

Dell Unity™-Produktreihe Benutzerhandbuch zur Unisphere® Befehlszeilenschnittstelle

Version 5.x

Hinweise, Vorsichtshinweise und Warnungen

 **ANMERKUNG:** Eine ANMERKUNG macht auf wichtige Informationen aufmerksam, mit denen Sie Ihr Produkt besser einsetzen können.

 **VORSICHT:** Ein VORSICHTSHINWEIS warnt vor möglichen Beschädigungen der Hardware oder vor Datenverlust und zeigt, wie diese vermieden werden können.

 **WARNUNG:** Mit WARNUNG wird auf eine potenziell gefährliche Situation hingewiesen, die zu Sachschäden, Verletzungen oder zum Tod führen kann.

Weitere Ressourcen.....	16
Kapitel 1: Einleitung.....	17
Überblick.....	17
Speichertypen.....	17
Verwenden der CLI in Skripten.....	17
Einrichten des Unisphere-CLI-Clients.....	18
Installieren des Unisphere-CLI-Clients.....	18
Starten des Unisphere-CLI-Clients.....	18
Zertifikatsüberprüfung.....	18
Unisphere-CLI-Syntax.....	19
Befehl.....	19
Befehlszeilenoptionen.....	19
Objekte.....	19
Objektqualifizierer.....	20
Aktionen.....	20
Aktionsqualifizierer.....	20
Größenqualifizierer.....	21
Geschwindigkeitsqualifizierer.....	21
Aktionsbefehle.....	21
Aktionsbefehl „create“.....	21
Aktionsbefehl „set“.....	22
Aktionsbefehl „show“.....	22
Aktionsbefehl „delete“.....	24
Hilfe.....	24
Hilfe zum Unisphere-CLI-Client.....	24
Hilfe zu übergeordneten Objekttypen.....	25
Hilfe zu untergeordneten Objekttypen.....	25
Hilfe zu Aktionen.....	26
Managen von SSL-Zertifikaten.....	26
Konfigurieren einer Zertifikats-Policy.....	27
Anzeigen von Zertifikaten.....	27
Löschen von Zertifikaten.....	27
Löschen sämtlicher Zertifikate.....	27
Importieren von Zertifikaten.....	28
Anzeigen der Befehlszeilenoptionen.....	28
Zugreifen auf das System.....	33
Hochladen eines Upgradekandidaten.....	34
Ausblenden von Kopfzeileninformationen.....	35
Speichern von Unisphere CLI-Einstellungen.....	35
Kapitel 2: Managen des Systems.....	36
Konfigurieren allgemeiner Systemeinstellungen.....	36
Anzeigen von Systemeinstellungen.....	37

Ändern der allgemeinen Systemeinstellungen.....	38
Manuelles Failback von NAS-Servern.....	39
Durchführen einer Systemintegritätsprüfung.....	39
Konfigurieren von Systeminformationen.....	40
Anzeigen von Systeminformationen.....	40
Konfigurieren oder Ändern der Systemkontaktinformationen.....	41
Verwalten von Softwareversionen.....	42
Anzeigen der Systemsoftwareversion.....	42
Vorbereiten der Systemsoftware für die Installation.....	44
Anzeigen fehlerhafter Speicherressourcen.....	45
Upgrade des Systems.....	45
Erstellen von Upgradesitzungen.....	46
Anzeigen von Upgradesitzungen.....	47
Wiederaufnehmen der Upgradesitzung.....	48
Abbrechen einer Upgradesitzung.....	49
Management der Sicherheitseinstellungen.....	49
Anzeigen von Sicherheitseinstellungen.....	50
Ändern von Sicherheitseinstellungen.....	50
Managen der Systemzeit.....	52
Anzeigen der Systemzeit.....	52
Ändern der Systemzeit.....	52
Zeitzone des Zeitplans verwalten.....	53
Zeitzone des Zeitplans anzeigen.....	53
Zeitzone des Zeitplans ändern.....	54
Managen von Supportkonfigurations- und Proxyservereinstellungen.....	55
Anzeigen von Supportkonfigurations- und Proxyservereinstellungen.....	56
Konfigurieren oder Ändern der Einstellungen für Support und Proxyserver.....	56
Managen von Supportverträgen.....	57
Anzeigen von Supportverträgen.....	58
Aktualisieren von Supportverträgen.....	58
Managen von Centralized ESRS.....	59
Anzeigen der Centralized ESRS-Konfiguration.....	59
Aktivieren oder Ändern von Centralized ESRS.....	60
Prüfen der Netzwerkverbindung von Centralized ESRS.....	61
Testen des Centralized EMC Secure Remote Support.....	61
Managen von SupportAssist (nur physische Bereitstellungen).....	62
Anzeigen der SupportAssist-Konfiguration.....	63
Initialisieren von SupportAssist.....	64
Prüfen der SupportAssist-Netzwerkverbindung.....	65
Ändern von SupportAssist.....	66
SupportAssist CallHome testen.....	67
Managen von Connect Home.....	67
Anzeigen von Connect Home.....	68
Ändern der Connect Home-Konfigurationseinstellungen.....	68
Testen von Connect Home.....	69
Managen von Benutzerrollen.....	69
Anzeigen von Benutzerrollen.....	70
Managen von Benutzerkonten.....	71
Erstellen eines Benutzerkontos.....	71
Anzeigen von Benutzerkonten.....	72

Ändern von Benutzerkonten.....	73
Löschen von Benutzerkonten.....	74
Verwalten von Benutzerkontoeinstellungen.....	75
Konfigurieren von Benutzerkontoeinstellungen.....	76
Anzeigen von Benutzerkontoeinstellungen.....	78
Managen von Supportanmeldedaten.....	79
Anzeigen der Supportanmeldedaten.....	79
Konfigurieren oder Ändern der Supportanmeldedaten.....	80
Löschen von Supportanmeldedaten.....	80
Managen von Systemlimits.....	80
Anzeigen von Systembegrenzungen.....	81
Anzeigen der Lizenzen für installierte Funktionen.....	82
Anzeigen von Lizenzen.....	82
Lesen und Akzeptieren der Endbenutzer-Lizenzvereinbarung.....	83
Anzeigen der EULA.....	83
Akzeptieren der EULA.....	84
Managen der Remoteprotokollierung.....	84
Erstellen der Konfiguration für Remoteprotokollierung.....	85
Anzeigen von Einstellungen für die Remote-Protokollierung.....	86
Ändern der Konfiguration für Remoteprotokollierung.....	87
Löschen der Konfiguration für Remoteprotokollierung.....	88
Managen der Systemzertifikate.....	89
Anzeigen von Informationen zum Zertifikat.....	90
Löschen eines Systemzertifikats.....	91
Managen von Snapshot-Schutzplänen.....	91
Anzeigen von Schutzplänen.....	92
Löschen von Schutzplänen.....	93
Managen von Aufgabenregeln.....	93
Erstellen von Aufgabenregeln.....	94
Anzeigen von Aufgabenregeln.....	97
Einstellungen für Aufgabenregeln ändern.....	99
Löschen von Aufgabenregeln.....	101
Managen von Jobs.....	102
Anzeigen der Liste der Jobs.....	103
Wiederaufnehmen eines Jobs.....	104
Abbrechen eines Jobs.....	104
Löschen von Jobs.....	105
Managen von Jobschritten.....	105
Anzeigen einer Liste der Schritte in einem Job.....	106
Kapitel 3: Konfigurieren der Netzwerkkommunikation.....	108
Managen von NAS-Servern.....	108
Erstellen eines NAS-Servers.....	111
Anzeigen von NAS-Servern.....	113
Ändern von NAS-Servereinstellungen.....	115
Löschen von NAS-Servern.....	118
Prüfen und Aktualisieren von Benutzerzuordnungen für Multiprotokoll-NAS-Server.....	119
Managen von FTP-Einstellungen.....	120
Managen von LDAP-Einstellungen eines NAS-Servers.....	126
Managen von NAS-Schnittstellen.....	132

Managen von NAS-Routen.....	138
Managen der Kerberos-Einstellungen.....	142
Managen von VLANs.....	144
Anzeigen von VLANs.....	144
Managen von Mandanten.....	145
Erstellen eines Mandanten.....	145
Anzeigen von Mandanten.....	146
Ändern von Mandanteneinstellungen.....	147
Löschen eines Mandanten.....	148
Managen von CIFS-Servern.....	148
Erstellen eines CIFS-Servers.....	149
Anzeigen eines CIFS-Servers.....	150
Ändern von CIFS-Servereinstellungen.....	150
Löschen eines CIFS-Servers	151
Managen von NFS-Servern.....	152
Erstellen eines NFS-Servers.....	153
Anzeigen eines NFS-Servers.....	155
Ändern von NFS-Servereinstellungen.....	155
Löschen eines NFS-Servers.....	157
Managen von Common Anti Virus Agent (CAVA).....	157
Anzeigen von CAVA-Einstellungen.....	158
Ändern von CAVA-Einstellungen.....	158
Managen von Konfigurationseinstellungen für Ereignisveröffentlichung.....	159
Anzeigen von CEPA-Konfigurationseinstellungen.....	160
Ändern der CEPA-Konfigurationseinstellungen.....	161
Managen von Konfigurationseinstellungen für CEPA-Pools.....	162
Erstellen eines CEPA-Pools.....	164
Anzeigen von CEPA-Pooleinstellungen.....	165
Ändern der Einstellungen für CEPA-Pools.....	165
Löschen eines CEPA-Pools.....	166
Managen von VMware-NAS-Protokollendpunktservern.....	167
Erstellen von Protokollendpunktservern.....	167
Anzeigen der VMware-Protokollendpunktserver.....	168
Löschen von Protokollendpunktservern.....	169
Managen des gegenseitigen CHAP für die gegenseitige CHAP-Authentifizierung.....	169
Festlegen von gegenseitigen CHAP-Schlüsseinstellungen.....	170
Anzeigen von gegenseitigen CHAP-Schlüsseinstellungen.....	170
Einrichten des iSNS für iSCSI-Speicher.....	171
Erstellen von iSNS-Serverdatensätzen.....	171
Anzeigen von iSNS-Serverdatensätzen.....	172
Löschen von iSNS-Serverdatensätzen.....	172
Ändern der iSNS-Serverdatensatz-Einstellungen.....	172
Managen der iSCSI-Konfiguration.....	173
Anzeigen der iSCSI-Konfiguration.....	173
Ändern der iSCSI-Konfiguration.....	174
Managen von iSCSI-Nodes (iSCSI-Servern).....	174
Anzeigen von iSCSI-Nodes.....	175
Ändern der Einstellungen von iSCSI-Nodes.....	176
Managen von Ethernetports.....	177
Anzeigen von Ethernetport-Einstellungen.....	178

Ändern von Ethernetport-Einstellungen.....	179
Managen von SAS-Ports (nur physische Bereitstellungen).....	180
Anzeigen von SAS-Einstellungen.....	180
Managen von FC-Ports.....	181
Anzeigen von FC-Porteinstellungen.....	182
Ändern von Porteinstellungen.....	182
Managen von nicht aktivierten Ports.....	183
Anzeigen nicht aktivierter Ports.....	184
Managen von Management-Netzwerkschnittstellen.....	185
Anzeigen von Managementoberflächen.....	185
Ändern der Schnittstelleneinstellungen.....	186
Management von Netzwerkschnittstellen.....	187
Erstellen von Schnittstellen.....	188
Anzeigen von Schnittstellen.....	188
Ändern der Schnittstelleneinstellungen.....	190
Löschen von Schnittstellen.....	191
Managen statischer IP-Routen.....	191
Erstellen von IP-Routen.....	192
Anzeigen von IP-Routen.....	193
Managen von IP-Routen.....	194
Löschen von IP-Routen.....	195
Managen von Verbindungsbündelungen.....	195
Erstellen von Linkzusammenfassungen.....	197
Anzeigen von Verbindungsbündelungen.....	197
Ändern von Linkzusammenfassungen.....	198
Löschen von Linkzusammenfassungen.....	199
Managen von Failsafe-Netzwerkfunktionen (nur physische Bereitstellungen).....	200
Erstellen eines FSN.....	201
Anzeigen von FSN-Einstellungen.....	201
Ändern eines FSN.....	202
Löschen eines FSN.....	203
Managen von DNS-Einstellungen.....	204
Konfigurieren der Einstellungen für DNS.....	205
Anzeigen von Standard-DNS-Adressen.....	205
Anzeigen von DNS-Serverdomains.....	206
Konfigurieren einer DNS-Domain.....	206
Managen von NTP-Servereinstellungen.....	207
Erstellen eines NTP-Serverdatensatzes.....	208
Anzeigen von NTP-Servereinstellungen.....	208
Konfigurieren von NTP-Servereinstellungen.....	209
Löschen von NTP-Servereinstellungen.....	209
Managen von NIS-Serverdomain.....	210
Anzeigen von NIS-Serverdomains.....	211
Ändern von NIS-Serverdomains.....	211
Managen von SMTP-Servereinstellungen.....	212
Anzeigen von SMTP-Servereinstellungen.....	213
Konfigurieren von SMTP-Servereinstellungen.....	213
Managen von NDMP-Servereinstellungen.....	214
Anzeigen von NDMP-Servereinstellungen.....	215
Konfigurieren von NDMP-Servereinstellungen	215

Managen von LDAP-Einstellungen.....	216
Konfigurieren von LDAP-Einstellungen.....	218
LDAP-Einstellungen anzeigen.....	220
Ändern von LDAP-Einstellungen.....	221
Überprüfen von LDAP-Einstellungen.....	223
Aktualisieren der automatisch erkannten LDAP-Serveradressliste.....	223
Löschen von LDAP-Einstellungen.....	224
Dienstprogrammbeefehle.....	224
Pingen.....	224
Verfolgen der Route.....	225
Managen von Distributed Hierarchical Storage Management.....	226
Anzeigen der DHSM-Einstellungen.....	226
Ändern der Distributed Hierarchical Storage Management-Einstellungen.....	227
Managen der DHSM-Verbindung.....	227
Erstellen einer DHSM-Verbindung.....	228
Anzeigen der Einstellungen für DHSM-Verbindung.....	229
Ändern der Einstellungen für DHSM-Verbindung.....	231
Löschen einer DHSM-Verbindung.....	232
Managen des Tie-Breaker-Node (nur virtuelle Dual-SP-Bereitstellungen).....	233
Anzeigen der grundlegenden Informationen zum Tie-Breaker-Node.....	234
Managen der Konfiguration eines Tie-Breaker-Node (nur virtuelle Dual-SP-Bereitstellungen).....	234
Anzeigen der Einstellungen für die Tie-Breaker-Node-Konfiguration.....	234
Ändern der Einstellungen für die Tie-Breaker-Node-Konfiguration.....	235
Kapitel 4: Hosts verwalten.....	237
Managen von Hostkonfigurationen.....	237
Erstellen von Hostkonfigurationen.....	239
Anzeigen von Hostkonfigurationen.....	241
Ändern der Hostkonfigurationseinstellungen.....	242
Löschen von Hostkonfigurationen.....	243
Managen von Host-LUNs.....	244
Anzeigen von Host-LUN-Konfigurationen.....	245
Ändern der Host-LUN-Konfigurationseinstellungen.....	246
Hostgruppen managen.....	246
Erstellen einer Hostgruppe.....	247
Eine Hostgruppe anzeigen.....	248
Hostgruppen ändern.....	249
Hostgruppe löschen.....	251
Hostgruppen-LUNs managen.....	252
Managen von Hostinitiatoren.....	253
Initiatoren erstellen.....	255
Anzeigen von Initiatoren.....	256
Ändern von Initiatoreinstellungen.....	257
Managen von Hostinitiatorpfaden.....	258
Initiatorpfade anzeigen.....	260
Managen von iSCSI-CHAP-Konten für die einseitige CHAP-Authentifizierung.....	260
Erstellen von iSCSI-CHAP-Konten.....	261
Anzeigen von iSCSI-CHAP-Konten.....	262
Ändern der Einstellungen für iSCSI-CHAP-Konten.....	262
Löschen von iSCSI-CHAP-Konten.....	263

Verwalten von iSCSI-Verbindungen.....	263
Erstellen einer iSCSI-Verbindung.....	264
Anzeigen von iSCSI-Verbindungseinstellungen.....	264
Ändern der iSCSI-Verbindungseinstellungen.....	265
Löschen einer iSCSI-Verbindung.....	266
Verwalten der iSCSI-Verbindungspfade.....	266
Erstellen eines iSCSI-Verbindungspfads.....	267
Anzeigen von iSCSI-Verbindungspfadeinstellungen.....	268
Löschen eines iSCSI-Verbindungspfads.....	268
Managen von Remotespeichersystemen.....	269
Erstellen von Konfigurationen für Remotesysteme.....	271
Prüfen der Einstellungen für Remotespeichersysteme.....	272
Anzeigen von Einstellungen für Remotespeichersysteme.....	273
Ändern der Einstellungen für Remotespeichersysteme.....	274
Löschen von Konfigurationen für Remotesysteme.....	275
Ungeplantes Failover auf Rack-Ebene von Replikationssitzungen.....	275
Anhalten von Replikationssitzungen.....	276
Fortsetzen von Replikationssitzungen.....	277
Managen von VMware vCenter.....	278
Erstellen von VMware vCenter.....	278
Festlegen der Anmeldedaten oder der Beschreibung eines vorhandenen vCenter-Servers.....	279
Löschen eines vorhandenen vCenter-Servers.....	280
Anzeigen aller vCenter-Server.....	281
Aktualisieren aller vCenter-Server.....	281
Managen von ESXi-Hosts.....	282
Erstellen eines ESXi-Hosts.....	282
Ändern von Anmeldedaten für ESXi-Host.....	283
Löschen der ESXi-Hostanmeldedaten.....	284
Anzeigen aller vorhandenen ESXi-Hosts.....	285
Erkennen aller ESXi-Hosts.....	285
Aktualisieren eines ESXi-Hosts.....	286
Virtuelle Maschine.....	287
Anzeigen aller vorhandenen virtuellen Maschinen.....	287
VM-Festplatte.....	288
Anzeigen aller Festplatten.....	288
Kapitel 5: Managen von Hardwarekomponenten.....	290
Managen des Speicherprozessors (SP).....	290
Anzeigen des Speicherprozessors.....	291
Managen der Festplatte.....	292
Anzeigen der Festplatte.....	293
Neues Einlesen von Festplatten (nur virtuelle Bereitstellungen).....	295
Ändern der Festplatteneinstellungen (nur virtuelle Bereitstellungen).....	295
Managen des Akkus (nur physische Bereitstellungen).....	296
Anzeigen des Akkus.....	296
Managen des Netzteils (nur physische Bereitstellungen).....	297
Anzeigen des Netzteils.....	297
Managen der Link Control Card (LCC) (nur physische Bereitstellungen).....	298
Anzeigen der Link Control Card.....	298
Managen von SSD (nur physische Bereitstellungen).....	299

Anzeigen der SSD.....	299
Managen des Disk Array Enclosure (DAE).....	300
Anzeigen eines Disk Array Enclosure.....	300
Managen des Disk Processor Enclosure (DPE).....	301
Anzeigen des Disk Processor Enclosure.....	302
Managen des Speichermoduls (nur physische Bereitstellungen).....	302
Anzeigen des Speichermoduls.....	303
Managen der System Status Card (nur physische Bereitstellungen).....	303
Anzeigen der SSC.....	304
Managen von Lüftermodulen (nur physische Bereitstellungen).....	304
Anzeigen des Lüftermoduls.....	305
Managen von I/O-Modulen, integrierten Modulen und Karten mit 4 Ports (nur physische Bereitstellungen)....	306
Commit ausführen für I/O-Module, integrierte Module und Karten mit 4 Ports.....	307
Anzeigen von I/O-Modulen, integrierten Modulen und Karten mit 4 Ports.....	307

Kapitel 6: Managen von Speicher..... 309

Automatisches Konfigurieren von Pools	309
Starten der automatischen Poolkonfiguration.....	310
Anzeigen von Konfigurationseinstellungen für die automatische Erstellung von Pools.....	311
Konfigurieren benutzerdefinierter Pools.....	312
Erstellen von Pools.....	314
Ändern von Pooleinstellungen.....	318
Hinzufügen von Laufwerken zum Speicherpool.....	319
Anzeigen von Pools.....	321
Löschen von Pools.....	324
Managen von FAST VP-Pooleinstellungen.....	325
Managen von Pool-Tiers.....	329
Anzeigen von Storage Tiers.....	330
Anzeigen von Poolressourcen	331
Managen von allgemeinen FAST VP-Einstellungen.....	333
Ändern von allgemeinen FAST VP-Einstellungen.....	334
Anzeigen von allgemeinen FAST VP-Einstellungen.....	335
Managen von FAST Cache (nur unterstützte physische Bereitstellungen).....	336
Erstellen von FAST Cache.....	336
Anzeigen von FAST Cache-Einstellungen.....	337
Erweitern von FAST Cache.....	337
Verkleinern des FAST Cache.....	338
Löschen von FAST Cache.....	338
Managen von FAST Cache-Speicherobjekten (nur physische Bereitstellungen).....	339
Anzeigen von FAST Cache-Speicherobjekten.....	339
Anzeigen von Speicherprofilen (nur physische Bereitstellungen).....	340
Managen von Laufwerksgruppen (nur physische Bereitstellungen).....	343
Anzeigen von Laufwerksgruppen.....	343
Anzeigen empfohlener Konfigurationen für Laufwerksgruppen.....	345
Managen von Speichersystemkapazität-Einstellungen.....	345
Anzeigen von Systemkapazitätseinstellungen.....	346
Managen von System-Tier-Kapazitätseinstellungen.....	347
Anzeigen der System-Tier-Kapazität.....	347
Managen von Dateisystemen.....	347
Erstellen von Dateisystemen.....	354

Anzeigen von Dateisystemen.....	357
Ändern der Dateiseinstellungen.....	359
Löschen von Dateisystemen.....	363
Managen von Benutzer-Quotas für Dateisysteme und Quota-Strukturen.....	363
Erstellen einer Benutzerquote auf einem Dateisystem oder einer Quotenstruktur.....	364
Anzeigen von Benutzerquoten.....	366
Ändern von Quotenlimits für einen bestimmten Benutzer.....	367
Aktualisieren von Benutzerquoten.....	368
Managen von Quotenstrukturen.....	369
Erstellen einer Quotenstruktur.....	369
Anzeigen von Quotenstrukturen.....	370
Festlegen von Quotenlimits für eine bestimmte Quotenstruktur.....	371
Aktualisieren einer Quotenstruktur auf einem Dateisystem.....	372
Löschen von Quota-Strukturen.....	373
Managen von Quota-Einstellungen.....	374
Konfigurieren von Quota-Einstellungen.....	375
Anzeigen von Quotenkonfigurationseinstellungen.....	377
Managen von NFS-Netzwerk-Shares.....	378
Erstellen von NFS-Netzwerk-Freigaben.....	380
Anzeigen von Einstellungen für NFS-Freigaben.....	383
Ändern von Einstellungen für NFS-Freigaben.....	384
Löschen von NFS-Netzwerk-Shares.....	387
Managen von SMB-Netzwerkfreigaben.....	387
Erstellen von CIFS-Netzwerk-Freigaben.....	389
Anzeigen von Einstellungen für CIFS-Freigaben.....	390
Ändern der Einstellung von CIFS-Freigaben.....	391
Löschen von CIFS-Netzwerk-Freigaben.....	393
Managen von LUNs.....	393
Erstellen von LUNs.....	396
Anzeigen von LUNs.....	399
Ändern von LUNs.....	401
Löschen von LUNs.....	404
Aktualisieren von Thin Clones einer LUN.....	404
Managen von Consistency Groups.....	405
Erstellen einer Consistency Group.....	408
Anzeigen von Consistency Groups.....	409
Ändern von Consistency Groups.....	411
Löschen von Consistency Groups.....	413
Aktualisieren von Thin Clones einer Consistency Group.....	414
Managen von VMware NFS-Datenspeichern.....	415
Erstellen von NFS-Dataspaces.....	420
Anzeigen von NFS-Datenspeichern.....	423
Ändern der Einstellungen für NFS-Datenspeicher.....	425
Löschen von NFS-Datenspeichern.....	428
Managen von VMware-VMFS-Datenspeichern.....	429
Erstellen von VMware VMFS-Datenspeichern.....	432
Anzeigen von VMware VMFS-Datenspeichern.....	435
Ändern der Einstellungen für VMware-VMFS-Datenspeicher.....	437
Löschen von VMware VMFS-Datenspeichern.....	440
Aktualisieren von Thin Clones eines VMFS-Datenspeichers.....	441

Managen von VMware-Protokollendpunkten.....	441
Anzeigen von Protokollendpunkten.....	442
Ändern des VMware-Protokollendpunkts.....	443
vVol-Datenspeicher managen.....	444
vVol-Datenspeicher erstellen.....	445
vVol-Datenspeicher anzeigen.....	446
vVol-Datenspeicher ändern.....	447
vVol-Datenspeicher löschen.....	448
vVol-Datenspeicherzuweisung managen.....	449
vVol-Objekte managen.....	450
vVol-Objekte anzeigen.....	452
vVol-Objekte löschen.....	453
vVol-Snapshots erstellen.....	454
vVol-Snapshots wiederherstellen.....	454
Managen von Funktionsprofilen.....	455
Erstellen eines Funktionsprofils.....	458
Anzeigen von Funktionsprofilen.....	458
Ändern von Funktionsprofilen.....	459
Löschen von Funktionsprofilen.....	460
Managen von I/O-Limits.....	460
Erstellen einer I/O-Begrenzungs-Policy.....	462
Löschen einer I/O-Limit-Policy.....	464
Ändern einer I/O-Limit-Policy.....	465
Anzeigen von I/O-Limit-Policies.....	466
Managen der I/O-Limitkonfiguration.....	467
Anzeigen der I/O-Limit-Konfigurationseinstellung.....	467
Durchsetzen der Verwendung der I/O-Limit-Konfigurationseinstellung	468
Kapitel 7: Schützen von Daten.....	469
Management von Snapshots.....	469
Erstellen von Snapshots.....	471
Anzeigen von Snapshots.....	473
Anhängen von Snapshots an Hosts.....	475
Aktualisieren von Snapshots.....	476
Replizieren von Snapshots.....	476
Trennen von Snapshots.....	478
Wiederherstellen einer Speicherressource mithilfe eines Snapshot.....	478
Löschen eines Snapshot.....	479
Kopieren von Snapshots.....	480
Ändern von Snapshots.....	481
Managen von Snapshot-NFS-Shares.....	483
Erstellen von NFS-Snapshots.....	484
Anzeigen von Snapshot-NFS-Freigaben.....	485
Einrichten von Snapshot-NFS-Freigaben.....	486
Löschen von Snapshot-NFS-Shares.....	488
Managen von Snapshot-CIFS-Freigaben.....	489
Erstellen eines CIFS-Snapshot.....	490
Anzeigen von Snapshot-CIFS-Freigaben.....	491
Einrichten von Snapshot-CIFS-Shares.....	491
Löschen von Snapshot-CIFS-Freigaben.....	493

Managen von Replikationssitzungen.....	493
Erstellen von Replikationssitzungen.....	498
Anzeigen von Replikationssitzungen.....	503
Ändern der Einstellungen für Replikationssitzungen.....	504
Anhalten von Replikationssitzungen.....	507
Fortsetzen von Replikationssitzungen.....	507
Manuelles Synchronisieren von Replikationssitzungen.....	509
Löschen einer Replikationssitzung.....	509
Failover von Replikationssitzungen.....	510
Failback von Replikationssitzungen.....	511
Beibehalten von asynchronen Replikationssitzungen.....	513
Erneutes Erstellen einer Replikationssitzung.....	513
Managen von virtuellen RecoverPoint-Appliances-CHAP-Konten.....	515
Zeigen Sie das RPA-CHAP-Konto an.....	516
Ändern eines RPA-CHAP-Kontos.....	516
Managen der Data-at-Rest-Verschlüsselung (nur physische Bereitstellungen).....	517
Anzeigen der Einstellungen der Data-at-Rest-Verschlüsselung (nur physische Bereitstellungen).....	518
Ändern der Verschlüsselungseinstellung für KMIP-Support (nur physische Bereitstellungen).....	518
Managen von KMIP-Support (nur physische Bereitstellungen).....	519
Anzeigen von KMIP-Einstellungen (nur physische Bereitstellungen).....	519
Ändern der Einstellungen für KMIP-Support (nur physische Bereitstellungen).....	520
Überprüfen von KMIP-Einstellungen (nur physische Bereitstellungen).....	521

Kapitel 8: Datenmobilität..... 522

Managen von VNX-Importsitzungen.....	522
Anzeigen von Importsitzungen.....	524
Managen von VNX-Importsitzungen für Block.....	525
Erstellen einer Blockimportsitzung.....	526
Änderung der Importsitzungseinstellungen für Block.....	527
Umstellung von Importsitzungen für Block.....	528
Abbrechen einer Blockimportsitzung.....	529
Anzeigen von Importsitzungen für Block.....	530
Managen von VNX-Importsitzungen für File.....	530
Erstellen einer NAS-Importsitzung.....	533
Änderung der Importsitzungseinstellungen für File.....	537
Umstellen von Importsitzungen für File.....	539
Commit von Importsitzungen für File.....	540
Abbrechen einer NAS-Importsitzung.....	541
Anzeigen von Importsitzungen für File.....	542
Anzeigen von Importsitzungselementen.....	543
Verwalten generischer Blockressourcen-Importsitzungen.....	545
Erstellen einer generischen Importsitzung.....	546
Anzeigen der Einstellungen der generischen Importsitzung.....	548
Ändern der Einstellungen der generischen Importsitzung.....	549
Anhalten einer generischen Importsitzung.....	550
Wiederaufnehmen einer generischen Importsitzung.....	551
Abbrechen einer generischen Importsitzung.....	551
Neustarten einer generischen Importsitzung.....	552
Löschen einer generischen Importsitzung.....	553
Common-Base-Snapshots.....	553

Eine Vorabprüfung für vorhandene Common-Base-Snapshots durchführen.....	554
Managen von LUN-Verschiebungssitzungen.....	555
Erstellen einer Sitzung zum Verschieben einer LUN.....	556
Anzeigen einer LUN-Verschiebungssitzung.....	557
Ändern der Einstellungen für die LUN-Verschiebungssitzung.....	558
Löschen einer LUN-Verschiebungssitzung.....	559
Abbrechen einer Sitzung zum Verschieben einer LUN.....	559
Kapitel 9: Management von Ereignissen und Warnmeldungen.....	561
Anzeigen von Ereignisprotokollen und Warnmeldungen.....	561
Anzeigen von Ereignisdatensätzen.....	562
Anzeigen von Warnmeldungs-Verlaufsinformationen.....	563
Bestätigen von Warnmeldungen.....	565
Löschen von Warnmeldungen.....	565
Warnmeldungen deaktivieren.....	566
Konfigurieren von Warnmeldungseinstellungen.....	566
Anzeigen von Warnmeldungseinstellungen.....	567
Warnmeldungseinstellungen ändern.....	568
Konfigurieren der Einstellungen für Warnmeldungen per E-Mail.....	569
Konfigurieren von SNMP-Zielen für Warnmeldungen.....	572
Erstellen von SNMP-Zielen.....	573
Anzeigen von SNMP-Zielen.....	574
Ändern der Einstellungen für das SNMP-Ziel.....	575
Löschen von SNMP-Zielen.....	576
Kapitel 10: Warten des Systems.....	577
Ändern des Servicepassworts.....	577
Wartung des Systems.....	578
Neustarten der Managementsoftware.....	578
Herunterfahren des Systems.....	578
Erneutes Initialisieren des Systems.....	579
Sammeln von Serviceinformationen.....	579
Managen von Core-Speicherauszugsdateien.....	580
Anzeigen von Core-Speicherauszügen.....	580
Löschen von Core-Speicherauszügen.....	581
Managen von Serviceinformationen.....	581
Anzeigen der Liste „Serviceinformationsdatei“.....	581
Managen des SSH-Zugriffs.....	582
Einrichten von SSH-Zugriff.....	582
Anzeigen von SSH-Einstellungen.....	583
Warten des Speicherprozessors (SP).....	583
Starten des Servicemodus.....	583
Reboot.....	584
Neues Image erstellen.....	584
Kapitel 11: Messwerte managen.....	585
Service zum Managen von Messwerten.....	585
Messwertserviceeinstellungen anzeigen.....	585
Messwertservice konfigurieren.....	586

Managen von Messwerteinstellungen.....	586
Anzeigen von Messwerteinstellungen.....	587
Werte von Verlaufsmesswerten managen.....	589
Anzeigen von Verlaufsmesswerteinstellungen.....	590
Echtzeitmesswerte managen.....	595
Anzeigen von Echtzeitmesswerteinstellungen.....	595
Kapitel 12: Anwendungsbeispiele.....	598
Pool-Anwendungsbeispiele.....	598
Automatisches Konfigurieren von Pools.....	598
Erstellen eines Pools mithilfe von Laufwerken mit spezifischen Merkmalen.....	600
Konfigurieren eines dynamischen Speicherpools.....	601
Konfigurieren eines herkömmlichen Speicherpools für ein All-Flash-Modell.....	602
Hinzufügen von Festplatten zu einem vorhandenen Pool.....	603
Anwendungsbeispiele für die Dateifreigabe.....	604
Erstellen eines NAS-Servers mit Multiprotokoll-Dateifreigabe.....	604
Konfigurieren von LDAP und Hochladen des Zertifikats der Zertifizierungsstelle.....	605
Konfigurieren von SMB für den NAS-Server.....	606
Gemeinsames Nutzen des Dateisystems von NFS und SMB.....	607
Erzeugen und Überprüfen des Benutzerzuordnungsberichts.....	607
Anwendungsbeispiele für Ressourcenkonfiguration.....	607
Identifizieren der Poolkapazität und Konfigurieren einer Ressource.....	608
Anwendungsbeispiel für Replikationskonfiguration.....	609
Lokale Replikation konfigurieren.....	609
Konfigurieren der asynchronen Replikation.....	610
Konfigurieren der synchronen Replikation.....	610
Erstellen einer Replikationsschnittstelle.....	611
Erstellen einer Replikationsverbindung.....	613
Erstellen einer Replikationssitzung für Blockspeicher.....	613
Erstellen einer asynchronen Replikationssitzung für Dateispeicherung.....	614
Erstellen einer synchronen Replikationssitzung für Dateispeicherung.....	615
Anzeigen von Replikationssitzungen.....	615
Anhang A: Referenz.....	617
Health details.....	617

Es werden regelmäßig neue Software- und Hardwareversionen veröffentlicht, um das Produkt kontinuierlich zu verbessern. Aus diesem Grund werden einige in diesem Dokument beschriebene Funktionen eventuell nicht von allen Versionen der von Ihnen verwendeten Software oder Hardware unterstützt. In den Versionshinweisen zum Produkt finden Sie aktuelle Informationen zu Produktfunktionen. Wenden Sie sich an Ihren Experten für technischen Support, wenn ein Produkt nicht ordnungsgemäß oder nicht wie in diesem Dokument beschrieben funktioniert.

Hier erhalten Sie Hilfe

Auf Support, Produkt- und Lizenzierungsinformationen kann wie folgt zugegriffen werden:

Produktinformationen

Dokumentationen oder Versionshinweise zum Produkt und zu Funktionen finden Sie in der Technischen Dokumentaktion von Unity unter dell.com/unitydocs.

Fehlerbehebung:

Informationen über Produkte, Softwareupdates, Lizenzierung und Service finden Sie auf der Supportwebsite (Registrierung erforderlich) unter: dell.com/support. Melden Sie sich an und suchen Sie die entsprechende Produktseite.

Einleitung

Themen:

- Überblick
- Einrichten des Unisphere-CLI-Clients
- Unisphere-CLI-Syntax
- Aktionsbefehle
- Hilfe
- Managen von SSL-Zertifikaten
- Anzeigen der Befehlszeilenoptionen
- Zugreifen auf das System
- Hochladen eines Upgradekandidaten
- Ausblenden von Kopfzeileninformationen
- Speichern von Unisphere CLI-Einstellungen.

Überblick

In der Unisphere-CLI können Sie Befehle über eine Eingabeaufforderung auf einem Microsoft Windows- bzw. UNIX-/Linux-Host auf einem System ausführen. Unisphere® ermöglicht das Management eines Systems. Die Unisphere-CLI richtet sich an fortgeschrittene Benutzer, die Befehle in Skripten zur Automatisierung von Routineaufgaben einsetzen möchten.

Mit der Unisphere-CLI können Sie ein System managen. Hierzu gehören die folgenden Aufgaben:

- Konfigurieren und Überwachen des Systems
- Verwalten von Benutzern
- Bereitstellen von Speicherplatz
- Schützen von Daten
- Steuern des Hostzugriffs auf den Speicher

Speichertypen

Die Unisphere-CLI unterstützt die Bereitstellung und das Management von Netzwerkblock- und dateibasiertem Storage, z. B.

- Dateisystemspeicher, der eine oder mehrere Freigaben enthält. Hier können Clients Daten speichern und problemlos auf Dateisysteme und Freigaben zugreifen, die sich nahtlos in folgende Umgebungen integrieren lassen:
 - Windows-Umgebungen, die das SMB-Protokoll zur Dateifreigabe, Microsoft Active Directory zur Authentifizierung und Windows-Verzeichniszugriff für Ordnerberechtigungen verwenden.
 - Linux-/UNIX-Umgebungen, in denen über das NFS-Protokoll Dateien freigegeben werden und Ordnerberechtigungen über POSIX-Zugriffssteuerungslisten aufgerufen werden.
- LUN-Speicher, über Fibre Channel (FC)- oder iSCSI-Protokoll. Sie können eine einzelne LUN oder eine LUN-Gruppe haben, die eine oder mehrere LUNs enthält. Hier wird Hosts und Anwendungen, die über das FC- oder iSCSI-Protokoll auf Speicher zugreifen, in Form von LUNs Speicher auf Blockebene bereitgestellt.
- Storage für virtuelle VMware-Maschinen über NFS-, VMFS- und vVol (Virtual Volume)-Datenspeicher.

Verwenden der CLI in Skripten

Mit Skripten können Sie in der Unisphere-CLI Routineaufgaben automatisieren, beispielsweise die Bereitstellung von Speicher oder die Planung von Snapshots zum Schutz gespeicherter Daten. Sie können beispielsweise ein Skript erstellen, in dem ein Snapshot einer iSCSI-LUNs erstellt wird und anschließend die älteren, zuvor erstellten Snapshots gelöscht werden. Customer Service stellt keine Beispielskripte oder Support für benutzerdefiniertes Skripting bereit.

Einrichten des Unisphere-CLI-Clients

Sie können den Unisphere-CLI-Client auf einem Computer mit Microsoft Windows oder UNIX/Linux installieren und starten. Befehle werden in der Unisphere-CLI über das sichere HTTPS-Protokoll an das System gesendet.

Installieren des Unisphere-CLI-Clients

Info über diese Aufgabe

So installieren Sie den Unisphere-CLI-Client:

Schritte

1. Rufen Sie die Supportwebsite auf.
2. Laden Sie den Unisphere-CLI-Client für Ihr Betriebssystem herunter.
3. Gehen Sie je nach Betriebssystem wie folgt vor:
 - Doppelklicken Sie in Windows auf die Installationsdatei, und befolgen Sie die Anweisungen. Der Standardinstallationspfad lautet wie folgt:
 - 64-Bit-Systeme: C:\Program Files (x86)\Dell EMC\Unity\Unisphere CLI
 - 32-Bit-Systeme: C:\Program Files\Dell EMC\Unity\Unisphere CLI
 -  **ANMERKUNG:** Das Installationsverzeichnis wird zur Systemvariablen PATH hinzugefügt.
 - Geben Sie unter UNIX/Linux Folgendes ein: `rpm -ihv <filename>`, wobei `filename` der Name der Installationsdatei ist. Der Standardinstallationsort ist: `/opt/emc/uemcli-<version>/bin/`, wobei `version` die Version des installierten Clients ist.

Starten des Unisphere-CLI-Clients

Info über diese Aufgabe

Nachdem Sie den Unisphere-CLI-Client installiert haben, können Sie ihn auf einem Microsoft Windows- bzw. UNIX-/Linux-Computer starten.

Geben Sie zum Starten des Unisphere-CLI-Clients je nach Betriebssystem Folgendes in die Befehlseingabeaufforderung ein:

Schritte

1. Wenn Sie ein Windows-Betriebssystem haben, geben Sie Folgendes ein:
`uemcli.exe`
2. Wenn Sie ein UNIX-/Linux-Betriebssystem haben, geben Sie Folgendes ein:
`/usr/bin/uemcli`

Zertifikatsüberprüfung

Für die Herstellung einer sicheren Verbindung zwischen der UEMCLI und dem Back-end-Server wird eine Public Key Infrastructure (PKI) verwendet. Eine wichtige Komponente von PKI ist die Zertifikatsüberprüfung. Die Zertifikatsüberprüfung bietet einem Benutzer die Möglichkeit, den Back-end-Server zu überprüfen, mit dem eine Verbindung hergestellt wird.

Wenn die UEMCLI mit einem Server eine Verbindung herstellt und eine sichere Verbindung anfordert, sendet der Server seine Identifikation in Form eines digitalen Zertifikats zurück. Das Zertifikat enthält in der Regel Folgendes:

- Servername
- Vertrauenswürdige Zertifizierungsstelle (Certificate Authority, CA)
- Öffentlicher Verschlüsselungsschlüssel des Servers

Der UEMCLI-Client kontaktiert ggf. den Server, der das Zertifikat ausgestellt hat (die vertrauenswürdige CA), um die Gültigkeit des Zertifikats vor dem Herstellen einer Verbindung zu verifizieren. Sobald das Zertifikat verifiziert wurde, stellen die UEMCLI und der Back-end-Server eine Verbindung her und tauschen Daten aus.

Stufe der Zertifikatsüberprüfung

Mit dem Skript `setlevel.sh` wird die Stufe der Zertifikatsüberprüfung auf niedrig oder mittel gesetzt, nachdem das RPM-Paket installiert wurde:

low	Der Zertifikatsüberprüfungsprozess wird nicht verwendet, um auf das Array zuzugreifen.
medium (Standard)	Der Zertifikatsüberprüfungsprozess wird verwendet, um auf das Array zuzugreifen.

Führen Sie den folgenden Befehl aus:

```
/opt/emc/uemcli/bin/setlevel.sh (low|medium|l|m)
```

Befolgen Sie anschließend die Anweisungen. Das Tool führt Sie durch die Schritte zur Festlegung der Sicherheitsstufe.

Weitere Informationen finden Sie im Abschnitt [Managen von SSL-Zertifikaten](#).

Unisphere-CLI-Syntax

Im Folgenden ist die Syntax einer Beispiel-Befehlszeile aufgeführt:

```
uemcli [<switches>] <object path> [<object qualifier>] <action> [<action qualifiers>]
```

Befehl

Sämtliche Befehlszeilen beginnen mit dem Befehl `uemcli`. Wenn Sie nicht jede Befehlszeile mit dem Befehl `uemcli` beginnen, wird der Befehl nicht ausgeführt und Sie müssen ihn erneut ausführen. Wenn Sie nur `uemcli` ohne Optionen und weitere Befehle eingeben, wird eine Liste angezeigt, in der die einzelnen Optionen beschrieben sind.

Befehlszeilenoptionen

Mit lokalen Befehlszeilenoptionen können Sie die Unisphere-CLI konfigurieren und die Verbindung zu einem System herstellen. Geben Sie die Optionen unmittelbar hinter dem Befehl `uemcli` ein. Wenn Sie mehrere Optionen in einer Befehlszeile eingeben, trennen Sie sie durch ein Leerzeichen voneinander ab. Am Anfang einer Option steht jeweils ein Bindestrich (-).

Details zu sämtlichen verfügbaren Optionen finden Sie unter [Anzeigen der Befehlszeilenoptionen](#).

Objekte

Objekte ermöglichen die Festlegung des Objekttyps, für den eine Aktion durchgeführt wird. Hierbei kann es sich um einen Benutzer oder Host, eine LDAP-Einstellung oder um das gemanagte System handeln. Alle Objekte sind in Typen kategorisiert und als übergeordnetes/untergeordnetes Element verschachtelt, um einen Pfad zum tatsächlichen Objekt zu bilden, für das eine Aktion durchgeführt werden soll (ähnlich wie bei der Suche einer Datei in einem Dateisystem). Bei einem Objekttyp kann es sich um ein übergeordnetes Element oder ein untergeordnetes Element handeln. Nicht alle übergeordneten Objekttypen haben untergeordnete Objekte.

Bei sämtlichen Aktionen muss der vollständig qualifizierte Pfad zum Objekt angegeben werden. Die einzige Ausnahme bildet die Option `-help`, die für Objekte in jeder Ebene eines Pfads gilt. [Hilfe](#) erläutert, wie die Option `-help` zu verwenden ist.

Das Objekt, für das Sie eine Aktion durchführen, wird durch eine ID mit der Bezeichnung „Objektqualifizierer“ bestimmt. Informationen hierzu finden Sie unter [Objektqualifizierer](#).

Beispiel 1

Im folgenden Beispiel zur Erstellung eines Benutzerkontos lauten die beiden Objekttypen `user` und `account`:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /user/account create -name user1 -type local -passwd Password789! -role operator
```

Beispiel 2

Im folgenden Beispiel zur Anzeige sämtlicher Benutzerkonten im System lauten die Objekttypen `user` und `account`. Es wird keine Objekt-ID angegeben, daher wird die Aktion „show“ auf „account“ angewendet, und es wird eine Liste sämtlicher Benutzerkonten angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /user/account show
```

Objektqualifizierer

Bei Objektqualifizierern handelt es sich um eindeutige Kennungen für Objekte im System. Das Format lautet wie folgt:

```
-<identifizier> <value>
```

Hierbei gilt:

- `identifizier` – Typ des Objektqualifizierers. Die gängigste Kennung lautet `-id`.
- `value` – Tatsächlicher Wert des Objektqualifizierers.

Bei der Erstellung von Objekten, wie etwa Benutzern oder Netzwerkschnittstellen, werden IDs – die Objektqualifizierer für das Objekt – vergeben. Bei der Durchführung von Aktionen wie dem Anzeigen, Ändern oder Löschen von Objekten geben Sie den Objektqualifizierer an. Die häufigste Kennung ist der Parameter `-id`. Der Qualifizierer ist nur im Bereich des angegebenen Objekttyps garantiert eindeutig. Am Anfang eines Objektqualifizierers steht jeweils ein Bindestrich (-).

Beispiel

Im folgenden Beispiel zur Änderung des Passworts für ein Benutzerkonto lautet der Objektqualifizierer `local_user`:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /user/account -id local_user set -passwd NewPassword456! -oldpasswd password123
```

Aktionen

Bei Aktionen handelt es sich um die an einem Objekt oder Objekttyp durchgeführten Operationen wie das Erstellen, Ändern, Anzeigen und Löschen. Aktionen sind immer erforderlich. [Aktionsbefehle](#) führt Details zu jedem der Aktionsbefehle auf.

Beispiel

Im folgenden Beispiel zur Änderung des Passworts für ein Benutzerkonto lautet die Aktion `set`:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /user/account -id local_user set -passwd NewPassword456! -oldpasswd password123
```

Aktionsqualifizierer

Aktionsqualifizierer sind Parameter für bestimmte Aktionen, beispielsweise Attribute oder Einstellungen, die bei der Änderung von Objekten modifiziert werden müssen. Am Anfang eines Aktionsqualifizierers steht jeweils ein Bindestrich (-).

Beispiel

Im folgenden Beispiel zur Änderung einer Rolle und eines Passworts für ein Benutzerkonto lauten die Aktionsqualifizierer `-passwd`, `-oldpasswd` und `-role`:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /user/account -id local_user set -passwd newpassword -oldpasswd password123 -role administrator
```

Größenqualifizierer

Mit den Größenqualifizierern können Sie eine bestimmte Größe bzw. Kapazität angeben. Bruchteile werden in Dezimalschreibweise eingegeben. Geben Sie beispielsweise „2,4T“ ein, um eine Größe von 2,4 Terabyte festzulegen. In der Ausgabe des Größenwerts werden die genaue Byte-Zahl und die angegebene Größe angezeigt:

```
Size = 1209462790557 (1.1TB)
```

In der folgenden Tabelle sind die Größenqualifizierer aufgeführt: Bei den Qualifizierern wird zwischen Groß- und Kleinschreibung unterschieden.

Tabelle 1. Größenqualifizierer

Qualifizierer	Einheit
K	Kilobyte
M	Megabyte
G	Gigabyte
T	Terabyte
P	Petabyte

Geschwindigkeitsqualifizierer

Die folgenden Qualifizierer sind für die Geschwindigkeitswerte definiert. Bei den Qualifizierern wird nicht zwischen Groß- und Kleinschreibung unterschieden.

Tabelle 2. Geschwindigkeitsqualifizierer

Qualifizierer	Einheit
Kbps, Kb/s	1.000 Bit pro Sekunde
Mbps, Mb/s	1.000.000 Bit pro Sekunde
Gbps, Gb/s	1.000.000.000 Bit pro Sekunde
KBps, KB/s	1.000 Byte pro Sekunde
MBps, MB/s	1.000.000 Byte pro Sekunde
GBps, GB/s	1.000.000.000 Byte pro Sekunde

Aktionsbefehle

In der Unisphere-CLI gibt es vier primäre Aktionsbefehle, die Sie an Objekttypen oder Objekten durchführen können: „Erstellen“, „Ändern/Konfigurieren“, „Anzeigen“ und „Löschen“. In diesem Abschnitt werden diese vier Aktionsbefehle erläutert. [Unisphere-CLI-Syntax](#) erläutert die Beziehung zwischen Aktionsbefehlen, Objekttypen und Objekten.

Aktionsbefehl „create“

Mit dem Aktionsbefehl `create` wird im System ein Objekt auf Grundlage des angegebenen Pfads erstellt. Bei erfolgreichem Befehl erhält das neue Objekt einen Objektqualifizierer bzw. eine ID, mit dem/der es im System identifiziert wird.

Format

```
<object> create [<action qualifiers>]
```

Beispiel

Im folgenden Beispiel wird mit dem Aktionsbefehl `create` ein lokales Benutzerkonto erstellt. Das neue Benutzerkonto erhält die ID `local_user`:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /user/account create -name local_user -type local -passwd Password789! -role operator
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = local_user
Operation completed successfully.
```

Aktionsbefehl „set“

Mit dem Aktionsbefehl `set` können Sie einen Objekttyp oder ein Objekt durch Angabe von Pfad und Objektqualifizierer ändern. Einige Optionen für bestimmte Objekte können bei der Erstellung des Objekts nicht konfiguriert werden, sie können jedoch konfiguriert werden, nachdem das Objekt mithilfe des Befehls `set` erstellt wurde. Dieser Leitfaden bezieht sich häufig auf diese Aktionen als **Konfiguration**. Wenn das von dem Objektqualifizierer angegebene Objekt nicht vorhanden ist, wird eine Fehlermeldung angezeigt.

Format

```
<object path> set <object qualifier> [<action qualifiers>]
```

Beispiel

Im folgenden Beispiel wird mit dem Aktionsbefehl `set` das Passwort eines Benutzerkontos geändert. Durch den Pfad `/user/account` wird angegeben, dass es sich beim Objekttyp um ein Benutzerkonto handelt. Der Objektqualifizierer `-id` identifiziert `local_user` als das zu ändernde Benutzerkonto:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /user/account -id local_user set -passwd NewPassword456! -oldpasswd OldPassword456!
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = local_user
Operation completed successfully.
```

Aktionsbefehl „show“

Mit dem Aktionsbefehl `show` werden eine Liste mit Objekten im System und die Attribute dieser Objekte angezeigt. Sie können einen Objektqualifizierer angeben, um die Attribute für ein einzelnes Objekt anzuzeigen. Der Aktionsbefehl `show` bietet Qualifizierer zur Änderung der Ausgabedarstellung, einschließlich des Formats der einzuschließenden Attribute. Folgende Ausgabeformate sind verfügbar: Name-Wert-Paar-Dateien (NVP), Tabellen und Dateien mit durch Kommas getrennten Werten (CSV).

Format

```
uemcli [<switches>] <object> [<object qualifier>] show [{-detail | -brief | -filter <value>}]
[-output {nvp | table [-wrap] | csv}]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
<code>-output -o</code>	Geben Sie das Ausgabeformat an. Folgende Werte sind möglich: <ul style="list-style-type: none"><code>nvp</code> : Im NVP-Format wird die Ausgabe als <code>name=value</code> dargestellt. Das Name-Wert-Paar-Format enthält ein Beispiel für das NVP-Format.<code>table</code> : Im Tabellenformat wird die Ausgabe als Tabelle mit Spaltenüberschriften und Zeilen dargestellt. Werte, die nicht in die Spalte passen, werden standardmäßig abgeschnitten. Wenn Sie den Tabellenqualifizierer um ein durch ein Komma abgetrenntes <code>-wrap</code> ergänzen, erfolgt innerhalb der Tabellenspalten ein Zeilenumbruch. Das Tabellenformat enthält ein Beispiel für das Tabellenformat.<code>csv</code> : Das CSV-Format entspricht dem Tabellenformat, aber die Namen und Werte sind durch Kommas voneinander getrennt. Das Format Comma-Separated Values enthält ein Beispiel für das CSV Format.
<code>-detail</code>	Hiermit werden sämtliche Attribute angezeigt.
<code>-brief</code>	Hiermit werden nur die grundlegenden Attribute angezeigt (Standard).
<code>-filter</code>	Durch Kommas getrennte Liste der Attribute, die in der Befehlsausgabe enthalten sind.

NVP-Format

```
1:   ID           = 1a0_SPA
     SP           = SPA_
     Ports        = eth0_SPA,eth1_SPA
     Health state = OK (5)

2:   ID           = 1a0_SPB
     SP           = SPB_
     Ports        = eth0_SPB,eth1_SPB
     Health state = OK (5)
```

Tabellenformat

```
ID      | SP  | Ports                | Health state
-----+-----+-----+-----
1a0_SPA | SPA | eth0_SPA,eth1_SPA | OK (5)
1a0_SPB | SPB | eth0_SPB,eth1_SPB | OK (5)
```

CSV-Format

```
ID,SP,Ports,Health state
1a0_SPA,SPA,"eth0_SPA,eth1_SPA",OK (5)
1a0_SPB,SPB,"eth0_SPB,eth1_SPB",OK (5)
```

Beispiel

Mit dem folgenden Befehl wird der Attributsatz in der Aktionsausgabe `show` verändert. Wenn Sie zum Beispiel `-filter "ID,ID,ID,ID"` zum Befehl hinzufügen, werden in der Ausgabe vier Zeilen mit dem Attribut „ID“ für jede aufgeführte Instanz angezeigt:

```
1:  ID = 1a_0
    ID = 1a_0
    ID = 1a_0
    ID = 1a_0
```

```
uemcli /net/nas/server show -filter "ID, SP, Health state, ID, Name"
```

Filterformat

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
1:      ID          = nas_1
        SP          = SPA
        Health state = OK (5)
        ID          = nas_1
        Name        = Mynas1

2:      ID          = nas_2
        SP          = SPA
        Health state = OK (5)
        ID          = nas_2
        Name        = Mynas2
```

Aktionsbefehl „delete“

Mit dem Aktionsbefehl `delete` wird ein Objekt unter Angabe von Objekt und Objektqualifizierer aus dem System gelöscht.

Format

```
<object path> <object qualifier> delete
```

Beispiel

Mit dem folgenden Befehl wird das Benutzerkonto „local_user1“ gelöscht:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /user/account -id local_user1 delete
```

Hilfe

Hilfe zum Verwenden der CLI, wie etwa Informationen über die Syntax, einen Objekttyp, ein bestimmtes Objekt oder einen bestimmten Aktionsbefehl, erhalten Sie über die Optionen `-help`, `-h` oder `-?`.

Hilfe zum Unisphere-CLI-Client

Hilfe zum Client, wie etwa Anwendungsbeispiele, Optionen und Systemanforderungen, erhalten Sie, wenn Sie „uemcli“ oder zusätzlich zum Befehl die Option `-help` | `-?` eingeben. [Anzeigen der Befehlszeilenoptionen](#) bietet Einzelheiten zu sämtlichen verfügbaren Optionen.

Beispiel

Mit dem folgenden Befehl werden Informationen zur Syntax und zu den Befehlszeilenoptionen angezeigt:

```
uemcli -?
```

```
[Get help on client options]
uemcli -help
  {CMDHELP|CMD|-upload|-download|-version|-saveUser|-removeUser|-removeAllUsers|-default|-
  certList|-certClear|-certDel|-certImport}

[Get help on objects or actions]
uemcli [-d <address>] [-port <number>] [-u <user_name>] [-p <password>] [-sslPolicy
  {interactive|reject|accept|store}] [-t <seconds>] [-silent] [-noHeader] [-cmdTime] <object>
  [<action>] -help
```

```

[Perform an action on an object on the destination system]
uemcli [-d <address>] [-port <number>] [-u <user_name>] [-p <password>] [-sslPolicy
{interactive|reject|accept|store}] [-s <name>[:<version>]] [-gmtoff [-|+]<HH>[:<MM>]] [-t
<seconds>] [-silent] [-noHeader] [-cmdTime] <object> [<qualifiers>] <action> [<qualifiers>]

[Upload a file to the destination system]
uemcli [-d <address>] [-port <number>] [-u <user_name>] [-p <password>]
[-sslPolicy {interactive|reject|accept|store}] [-t <seconds>] [-silent] [-noHeader]
-upload -f <file_path> <type> [-<parameter> <value> ...] [<action>]

[Download a file from the destination system]
uemcli [-d <address>] [-port <number>] [-u <user_name>] [-p <password>] [-sslPolicy
{interactive|reject|accept|store}] [-t <seconds>] [-silent] [noHeader] -download {-d
<directory>|-f <file_path>} <type> [-<parameter> <value> ...] [<action>]

[Display the version of this client]
uemcli -version

[Save access credentials for the destination system locally]
uemcli [-d <address>] [-port <number>] -u <user_name> -p <password> [-silent] -saveUser

[Remove access credentials for the destination system from this client]
uemcli [-d <address>] [-port <number>] [-silent] -removeUser

[Remove all stored access credentials from this client]
uemcli [-silent] -removeAllUsers

[Save the destination address as the default for this client]
uemcli -d <address> -port <number> [-silent] -default
[List certificates saved for this client]
uemcli [-silent] -certList

[Delete a certificate from this client]
uemcli [-silent] -certDel <certificate_id>

[Delete all certificates from this client]
uemcli [-silent] -certClear

[Import an SSL certificate from a file]
uemcli [-silent] -certImport <file>

```

Hilfe zu übergeordneten Objekttypen

Hilfe zu übergeordneten Objekttypen, die in der Regel untergeordnete Objekttypen enthalten, erhalten Sie, wenn Sie den Objekttyp gefolgt von der Option `-help` eingeben, um die enthaltenen Objekttypen anzuzeigen.

Beispiel

Der folgende Befehl zeigt eine Liste der DNS-Objekttypen: `/net /dns` ist der übergeordnete Objekttyp und `[config]` und `[domain]` sind die untergeordneten Objekttypen. In der Ausgabe sind die Elemente in Klammern die Objekte, an denen die Aktionen wie Erstellen und Ändern durchgeführt werden.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/dns -help
```

```

+- /net/dns/
    +- [config]
    +- [domain]

```

 **ANMERKUNG:** Um Hilfe zu allen Objekttypen zu erhalten, geben Sie nur einen Schrägstrich ein (`/`). Zum Beispiel `/ -help`.

Hilfe zu untergeordneten Objekttypen

Wenn Sie Hilfe zu untergeordneten Objekttypen benötigen, geben Sie den Objekttyp gefolgt von der Option `-help-help` ein. Daraufhin wird eine Liste mit den unterstützten Aktionsbefehlen angezeigt.

Beispiel

Mit dem folgenden Befehl werden die Aktionsbefehle zur Festlegung (Änderung) und Anzeige einer DNS-Servereinstellung aufgerufen: `/net /dns` ist der übergeordnete Objekttyp und `[config]` ist der untergeordnete Objekttyp. In der Ausgabe sind die Elemente in Klammern die Aktionen (wie Erstellen und Ändern), die Sie für die angegebenen Objekttypen durchführen können:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/dns/config -?
```

```
Configure system DNS client settings.
Actions:
[Set]
/net/dns/config set -nameServer <value>

[Show]
/net/dns/config show [-output {nvp|csv|table[-wrap]}] [{-brief|-detail}]
```

Hilfe zu Aktionen

Wenn Sie Hilfe zu einem Aktionsbefehl aufrufen möchten, geben Sie den vollständig qualifizierten Objektparameter gefolgt vom Aktionsqualifizierer `-help` ein.

Beispiel

Mit dem folgenden Befehl wird die Liste der Schnittstellenattribute, die Sie ändern können, angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/if set -?
```

```
Storage system address: 127.0.0.1
Storage system port: 443
HTTPS connection

/net/if -id <value> set [ -vlanId <value> ] [ -addr <value> ] [ -netmask <value> ] [ -gateway
<value> ]
Modify an existing interface.

Where:
-id <value>
Specify the ID of an interface (eg. if_0, if_3)

[Optional] -vlanId <value>
Specify the virtual LAN (VLAN) ID for the interface. The interface uses the ID to accept
packets that have VLAN tags. The value range is 1 to 4095. If the value is empty string, VLAN
tagging will be disabled.
[Optional] -addr <value>
Specify the IP address for the interface.

[Optional] -netmask <value>
Specify the subnet mask for the IPv6 interface.

[Optional] -gateway <value>
Specify the gateway for the interface.
```

Managen von SSL-Zertifikaten

Bei der Anmeldung beim System über die Unisphere-CLI sorgen Secure Socket Layer (SSL)-Zertifikate für eine sichere Kommunikation zwischen dem CLI-Client und dem System. Sie können diese Zertifikate managen und eine Policy konfigurieren, die von der Unisphere-CLI beim Eingang unbekannter Zertifikate genutzt werden soll. Sämtliche heruntergeladenen Zertifikate werden in der sicheren lokalen Lockbox auf dem Clientsystem gespeichert. [Speichern von Unisphere CLI-Einstellungen](#) erläutert, wie die Einstellungen gespeichert werden.

Konfigurieren einer Zertifikats-Policy

Legen Sie in einer Zertifikats-Policy fest, wie die Unisphere-CLI auf unbekannte SSL-Zertifikate reagieren soll, die aus dem System heruntergeladen werden.

Format

`-sslPolicy <value>`

Option

Option	Beschreibung
<code>-sslPolicy</code>	Folgende Werte sind möglich: <ul style="list-style-type: none">• <code>interactive</code>: Der Benutzer wird vom Client zur Aktion aufgefordert (Standard).• <code>reject</code>: Die Zertifikate werden automatisch abgelehnt.• <code>accept</code>: Die Zertifikate werden automatisch akzeptiert.• <code>store</code>: Die Zertifikate werden automatisch akzeptiert und in der Lockbox gespeichert.

Anzeigen von Zertifikaten

Zeigen Sie eine Liste aller in der Lockbox gespeicherten SSL-Zertifikate an.

 **ANMERKUNG:** Aktionsbefehl „show“ erläutert, wie das Ausgabeformat geändert wird.

Format

`-certList`

Löschen von Zertifikaten

Mit diesem Befehl werden SSL-Zertifikate aus der Lockbox gelöscht.

Format

`-certDel <certificate IDs>`

Option

Option	Beschreibung
<code>-certDel</code>	Geben Sie eine Liste mit den zu löschenden Zertifikat-IDs ein. Trennen Sie die einzelnen IDs mit Komma voneinander ab.  ANMERKUNG: Mit der Option <code>-certList</code> können Sie eine Liste der gespeicherten Zertifikate samt ID aufrufen.

Löschen sämtlicher Zertifikate

Löschen Sie sämtliche SSL-Zertifikate aus der Lockbox.

Format

`-certClear`

Importieren von Zertifikaten

Importieren Sie ein SSL-Zertifikat aus einer Datei.

Format

`-certImport <file>`

Option

Option	Beschreibung
<code>-certImport</code>	Geben Sie den Pfad und den Namen der zu importierenden Datei an. Folgende Formate werden unterstützt: <ul style="list-style-type: none">• Privacy Enhanced Mail (PEM)• Distinguished Encoding Rules (DER)• Cryptographic Message Syntax (PKCS #7)

Anzeigen der Befehlszeilenoptionen

Die Unisphere-CLI-Befehlszeilenoptionen gelten nur für Ihren installierten Unisphere-CLI-Client. Mit den Optionen können Sie auf ein System zugreifen, Dateien in das System hochladen und Sicherheitszertifikate managen.

Format

`uemcli [{"-help|-h|-?}"]`

Die folgende Tabelle beschreibt jede der Optionen:

Tabelle 3. Befehlszeilenoptionen

Option	Beschreibung
<code>-destination -d</code>	Die IP-Adresse (IPv4 oder IPv6) bzw. der Netzwerkname des Zielsystems. Wenn Sie diese Option nicht angeben, verwendet der Client die für <code>-default</code> angegebenen Adressen. Wenn dort keine Adresse angegeben ist, wird die localhost-Adresse 127.0.0.1 verwendet.
<code>-port</code>	Die Portnummer im System.
<code>-user -u</code>	Der Benutzername für die Anmeldung beim System.
<code>-password -p</code>	Das Passwort für die Anmeldung beim System.
<code>-securePassword</code>	Gibt das Passwort im sicheren Modus an – der Benutzer wird aufgefordert, das Passwort einzugeben.
<code>-timeout -t</code>	Die Zeitüberschreitung (in Sekunden), nach der Sie automatisch beim System abgemeldet werden, wenn keine Benutzeraktivität festgestellt wurde oder ein Systemproblem aufgetreten ist. Der Standardwert beträgt 600 Sekunden (10 Minuten).
<code>-sslPolicy</code>	Policy für den Umgang mit aus dem System heruntergeladenen unbekanntem SSL-Zertifikaten. Gültige Werte: <ul style="list-style-type: none">• <code>interactive</code> (Standard) – Fordern Sie den Benutzer auf, die Zertifikate für die aktuelle Sitzung zu akzeptieren.• <code>reject</code> : Die Zertifikate werden automatisch abgelehnt.• <code>accept</code> : Die Zertifikate werden automatisch akzeptiert.

Tabelle 3. Befehlszeilenoptionen (fortgesetzt)

Option	Beschreibung
	<ul style="list-style-type: none"> • <code>store</code> : Die Zertifikate werden automatisch akzeptiert und gespeichert.
-certList	Liste sämtlicher in der Lockbox lokal gespeicherten Zertifikate.
-certClear	Sämtliche in der Lockbox lokal gespeicherten Zertifikate werden gelöscht.
-certDel	<p>Es werden ausgewählte Zertifikate aus der Lockbox gelöscht. Geben Sie die IDs der zu löschenden Zertifikate ein. Trennen Sie die einzelnen IDs mit Komma voneinander ab.</p> <p>i ANMERKUNG: Mit der Option <code>-certList</code> können Sie eine Liste der gespeicherten Zertifikate samt ID aufrufen.</p>
-certImport	<p>Es wird ein Zertifikat aus einer Datei importiert. Folgende Formate werden unterstützt:</p> <ul style="list-style-type: none"> • Privacy Enhanced Mail (PEM) • Distinguished Encoding Rules (DER) • Cryptographic Message Syntax (PKCS #7)
-syntax -s	Name und Version der für den Client zu verwendenden Syntax (optional). Trennen Sie den Namen und die Version mit einem Doppelpunkt voneinander ab. Mit der folgenden Option wird beispielsweise die Syntax von UEM-Version 1.5 angewendet: <code>-syntax uem:1.5</code>
-upload	<p>Es wird eine Datei in das System hochgeladen. Geben Sie den Dateityp und den Speicherort im folgenden Format ein:</p> <pre>{-help <type> -help {-f -file} <file> <type> [<parameter>=<value>...]}</pre> <p>Hierbei gilt:</p> <ul style="list-style-type: none"> • <code>-help</code> : Hiermit wird eine Liste der Dateitypen angezeigt, die Sie in das System hochladen können. • <code>type -help</code> : Hiermit werden Informationen zu einem Dateityp angezeigt. Folgende Werte sind möglich: <ul style="list-style-type: none"> ○ <code>license</code> : Eine Lizenzdatei. Beim Upload wird die Lizenz auf dem System installiert. ○ <code>upgrade</code> : Eine Kandidatendatei für das Upgrade der Systemsoftware. Wenn Sie eine Kandidatendatei für das Upgrade in das System hochgeladen haben, wird die vorherige Version ersetzt. Auf dem System können sich nicht mehrere Upgradekandidaten gleichzeitig befinden. ○ <code>/net/nas/ldap</code> : Ein benutzerdefiniertes LDAP-Schema oder ein Zertifikat der Zertifizierungsstelle (CA) für den NAS-Server, identifiziert durch den erforderlichen Parameter <code>-server</code>. Durch das Hochladen eines gültigen LDAP-Schemas ändert sich die LDAP-Konfiguration. Dies führt zu Änderungen an Dateisystemen beim Zugriff auf den spezifischen NAS-Server. ○ <code>/net/nas/server</code> : Eine Datei mit benutzerdefinierten Nutzerzuordnungsregeln für den spezifischen NAS-Server, der von dem erforderlichen Parameter <code>-id</code> identifiziert wird. Der obligatorische <code>-type</code> Parameter gibt den entsprechenden Typ der hochgeladenen Konfigurationsdatei an. Gültige Werte: <ul style="list-style-type: none"> ▪ <code>userMapping</code> ▪ <code>passwd</code> ▪ <code>group</code> ▪ <code>hosts</code> ▪ <code>netgroup</code> ▪ <code>homedir</code> ○ <code>/net/nas/cava</code> — Eine Antivirus-Konfigurationsdatei mit Parametern des CAVA-Dienstes. ○ <code>/net/nas/kerberos</code> — Eine Kerberos-Schlüsseltabellendatei (Keytab), die für sicheres NFS mit einem benutzerdefinierten UNIX- oder Linux-Kerberos-KDC erforderlich ist. Sie enthält SPNs (Service Principal Names), Verschlüsselungsmethoden und Schlüssel für den sicheren NFS-Service.

Tabelle 3. Befehlszeilenoptionen (fortgesetzt)

Option	Beschreibung
	<ul style="list-style-type: none"> ○ /sys/cert — Eine Zertifikatsdatei eines bestimmten Typs für den spezifischen Dienst, der durch obligatorisch gekennzeichnet ist <code>-type</code> und <code>-service</code>-Parameter. Gültige obligatorische <code>-type</code>-Parameter sind: <ul style="list-style-type: none"> ▪ CA ▪ Server ▪ Client ▪ TrustedPeer Gültige obligatorische <code>-service</code>-Parameter sind: <ul style="list-style-type: none"> ▪ Mgmt_LDAP ▪ Mgmt_KMIP ▪ VASA_HTTP ▪ vSphere <p>i ANMERKUNG: Der optionale <code>-scope</code>-Parameter gibt an, ob das Zertifikat einen globalen oder lokalen Umfang hat. Wenn er lokal ist, muss die ID des Umfangs angegeben werden. Zum Beispiel: Wenn der Umfang des Zertifikats NAS-Server „nas_1“ ist, dann ist der Wert des Umfangattributs „nas_1“. Der optionale <code>-passphrase</code>-Parameter gibt die Passphrase für Servertypzertifikate an. Die ID des Zertifikats wird angezeigt, wenn die Zertifikatsdatei erfolgreich hochgeladen wurde.</p> <ul style="list-style-type: none"> ● <code>-f file file type</code>: Geben Sie für <code>file</code> Pfad und Name der hochzuladenden Datei ein. Geben Sie für <code>type</code> den Dateityp der hochzuladenden Datei ein. ● <code>parameter = value</code>: Optionale Parameter/Wert-Paare, mit denen Sie beim Upload bestimmte Parameter hinzufügen können. <p>i ANMERKUNG: Mit dem folgenden Befehl rufen Sie eine Liste der unterstützten Dateitypen auf: <code>-upload -help</code></p>
<p><code>-download</code></p>	<p>Laden Sie eine Datei aus dem System herunter. Geben Sie den Dateityp und den Speicherort im folgenden Format ein:</p> <pre>{-help <type> -help {-d <folder> -f <file>} <type> [-<parameter> <value> ...]}</pre> <p>Hierbei gilt:</p> <ul style="list-style-type: none"> ● <code>-help</code>: Hiermit wird eine Liste der Dateitypen angezeigt, die Sie aus dem System herunterladen können. ● <code>type -help</code>: Hiermit werden Informationen zu einem Dateityp angezeigt. Folgende Werte sind möglich: <ul style="list-style-type: none"> ○ <code>serviceInfo</code> — Laden Sie die Dienstinformationsdatei herunter. Wenn keine ID angegeben ist, wird die zuletzt erzeugte Serviceinformationsdatei heruntergeladen. Ihr Serviceprovider kann die gesammelten Informationen zur Analyse Ihres Systems nutzen. Diese Aktion sollte mit Servicebenutzer-Anmeldedaten ausgeführt werden. Zum Herunterladen von Serviceinformationen sollten Sie diese zuerst mithilfe des Befehls <code>uemcli /service/system collect -serviceInfo</code> zusammenstellen. <p>i ANMERKUNG: Wenden Sie sich an Ihren Serviceanbieter, um zu bestimmen, ob diese Informationen gesammelt werden müssen, und um einen Prozess zum Senden der Datei an den Customer Service einzurichten.</p> <ul style="list-style-type: none"> ○ <code>config</code>: Hiermit werden Details zu den Konfigurationseinstellungen des Speichersystems in einer Datei gespeichert. Mithilfe dieser Datei können Servicemitarbeiter Sie bei der Neukonfiguration Ihres Systems nach einem schwerwiegenden Systemfehler oder bei einer Neuinitialisierung des Systems unterstützen. Diese Aktion sollte mit Servicebenutzer-Anmeldedaten ausgeführt werden. Die Datei enthält lediglich Details zur Konfiguration Ihres Systems. Eine Systemwiederherstellung ist auf der Grundlage dieser Datei nicht möglich. Diese Aktion sollte mit Servicebenutzer-Anmeldedaten ausgeführt werden.

Tabelle 3. Befehlszeilenoptionen (fortgesetzt)

Option	Beschreibung
	<p>i ANMERKUNG: Es wird empfohlen, nach jeder wichtigen Änderung der Systemkonfiguration die Datei an einem Remotestandort zu speichern, damit Sie in jedem Fall auf ein Exemplar der Datei zugreifen können.</p> <ul style="list-style-type: none"> ○ <code>/net/nas/ldap</code> : Ein benutzerdefiniertes LDAP-Schema für den NAS-Server, der durch den erforderlichen Parameter <code>-server</code> identifiziert wird. Sobald Sie LDAP-Einstellungen für einen NAS-Server konfigurieren, können Sie die automatisch erzeugte LDAP-Schemadatei herunterladen, um weitere Änderungen vorzunehmen. ○ <code>/net/nas/server</code> : Eine Datei mit benutzerdefinierten Nutzerzuordnungsregeln für den spezifischen NAS-Server, der von dem erforderlichen Parameter <code>-id</code> identifiziert wird. Der obligatorische <code>-type</code> Parameter gibt den entsprechenden Typ der hochgeladenen Konfigurationsdatei an. Gültige Werte: <ul style="list-style-type: none"> ▪ <code>userMapping</code> ▪ <code>passwd</code> ▪ <code>group</code> ▪ <code>hosts</code> ▪ <code>netgroup</code> ▪ <code>homedir</code> ○ <code>/net/nas/cava</code> — Eine CAVA-Konfigurationsdatei. ○ <code>/net/nas/kerberos</code> — Kerberos-Schlüsseltabellendatei (Keytab), die für sicheres NFS mit benutzerdefiniertem UNIX- oder Linux-Kerberos-KDC erforderlich ist. Sie enthält SPNs (Service Principal Names), Verschlüsselungsmethoden und Schlüssel für sicheren NFS-Service. ○ <code>/import/session/nas</code> — Ein detaillierter Dateiimportstatusbericht, der Fehlerinformationen für eine VDM-zu-NAS-Importsitzung enthalten kann, die durch das obligatorische <code>.</code> gekennzeichnet ist <code>-id</code>-Parameter. ○ <code>/sys/cert</code> — Eine Zertifikatsdatei, die auf dem Speichersystem vorhanden ist, das durch das obligatorische <code>-id</code>-Parameter <code>.</code> gekennzeichnet ist. ○ <code>encryption</code> — Drei Arten von Data-at-Rest-Verschlüsselungsdateien (D@RE) stehen zum Herunterladen mit dem obligatorischen <code>-type</code>-Parameter zur Verfügung. Gültige Werte: <ul style="list-style-type: none"> ▪ <code>backupKeys</code> - Wenn eine Kopie des Keystores angefordert wird, sind keine zusätzlichen Parameter erforderlich. Es wird empfohlen, dass eine Kopie des Keystore immer dann heruntergeladen und gespeichert wird, wenn sich die bereitgestellte oder Hardwarekonfiguration des Speichersystems ändert. ▪ <code>auditLog</code> - Wenn eine Kopie von <code>auditlog</code> wird angefordert, die obligatorische <code>-entries</code> Parameter muss angegeben werden, wobei es zwei Möglichkeiten gibt: <code>all</code> oder <code>JJJJ-MM</code>. Alle Einträge können angefordert werden oder ein bestimmtes Jahr und Monat der Einträge. Die heruntergeladene Datei hat eine maximale Größe von 100 MB. Passen nicht alle Einträge in diese Dateigröße, wird der Kopf des Speichersystems <code>auditlog</code> zurückgegeben. Der Rest von <code>auditlog</code> kann mit der Option Jahr und Monat abgerufen werden. <p>i ANMERKUNG: Wenn <code>auditlog</code> angefordert wird, wird auch seine Prüfsummendatei mit heruntergeladen.</p> <ul style="list-style-type: none"> ▪ <code>cksum</code> - Fordert eine neu generierte Prüfsummendatei für ein zuvor heruntergeladenes <code>auditlog</code>-Datei an. In diesem Fall ist die Pflicht, dass <code>-logName <auditlog filename></code> -Parameter angegeben werden muss. <p>i ANMERKUNG: Dies muss der genaue Dateiname eines zuvor heruntergeladenen <code>auditlog</code>-Datei sein.</p> <ul style="list-style-type: none"> ○ <code>/service/system/dump</code> — Core-Dump-Dateien werden nach einem SP-Fehler generiert. Laden Sie diese Dateien herunter, um sie an Ihren Serviceanbieter zu senden. Sie können hilfreich sein beim Troubleshooting und dem Lösen von Problemen mit dem System. Servicekontoanmeldedaten sind erforderlich. ● <code>{-d <folder> -f <file>} <type></code> : Zielverzeichnis oder Pfad zur Zieldatei. Geben Sie anstelle von <code><type></code> den Typ der herunterzuladenden Datei ein.

Tabelle 3. Befehlszeilenoptionen (fortgesetzt)

Option	Beschreibung
	<ul style="list-style-type: none"> • [-<parameter> <value>...] [<action>]: Hiermit wird eine Datei aus dem Speichersystem heruntergeladen. • <type>: Dateityp • [-<parameter> <value> ...]: Optionale Schlüsselwertpaare, die an das Speichersystem über URL-verschlüsselte und durch Leerzeichen getrennte Parameter übermittelt werden. • [<action>]: Optionale Aktion, die angibt, was auf der heruntergeladenen Datei ausgeführt werden soll.
-gmtoff	<p>Hier wird der Zeitunterschied zur Greenwich Mean Time (GMT) festgelegt. Der Wert wird zur Umwandlung der Uhrzeit auf dem System in die Uhrzeit auf dem Clientsystem verwendet. Mit dem Befehl auto wird der Zeitunterschied des aktuellen Clientsystems gesendet. Geben Sie Folgendes ein, um den Zeitunterschied festzulegen:</p> <p>[- +] <HH> [: <MM>]</p> <p>Hierbei gilt:</p> <ul style="list-style-type: none"> • - + : Geben Sie ein, ob die Zeitzone auf die GMT-Zone folgt (-) oder ihr vorausgeht (+). Das Pluszeichen kann bei der Eingabe weggelassen werden. • HH : Geben Sie ein, wie viele Stunden der Zeitunterschied beträgt. • MM : Geben Sie ein, wie viele Minuten der Zeitunterschied beträgt (optional). Die Minuten- und Stundenangaben müssen durch einen Doppelpunkt voneinander getrennt werden.
-help -h -?	Mit dieser Option rufen Sie Informationen zur Syntax und den Optionen auf.
-saveUser	<p>Mit dieser Option werden die Zugangsdaten für die Optionen <code>-user</code> und <code>-password</code> in einer lokalen Sicherheitsdatei in der Lockbox gespeichert. Die gespeicherten Zugangsdaten werden bei jedem Befehl automatisch von der Unisphere-CLI auf das angegebene Paar aus Systemziel und Port angewendet.</p> <p>ANMERKUNG: Es kann nur jeweils ein Satz Anmeldedaten für das System gespeichert werden. Dies bedeutet, dass Sie mit dem Service-Benutzerkonto nicht auf die CLI zugreifen können, wenn sich das Service-Passwort vom Admin-Passwort von <code>-saveUser</code> unterscheidet.</p>
-removeUser	Hiermit wird das angegebene Benutzerkonto aus der Lockbox entfernt.
-default	Speichern Sie das Paar aus Ziel und Port als Standardsystem. In diesem Fall wird ein von Ihnen eingegebener Befehl von der Unisphere-CLI auf dem Standardsystem ausgeführt. In der Unisphere-CLI wird das angegebene Paar aus Ziel und Port in einer lokalen Sicherheitsdatei in der Lockbox gespeichert. Wenn Sie die Option <code>-default</code> angeben, überschreibt die Unisphere-CLI das bislang gespeicherte Paar aus Ziel und Port mit dem neuen Paar. Wenn Sie die Option <code>-port</code> angeben, wird der angegebene Portwert zusammen mit dem Wert für <code>-destination</code> in der lokalen Sicherheitsdatei gespeichert.
-silent	Mit dieser Option wird festgelegt, dass ein Befehl zu Ende ausgeführt wird, ohne dass eine Ausgabe angezeigt oder eine Bestätigung durch den Benutzer angefordert wird. Dies ist hilfreich bei der Ausführung von Skripten.
-noHeader	Mit dieser Option wird die Kopfzeile der Befehlsausgabe (IP-Adresse des Systems, Portnummer usw.) ausgeblendet.
-v -version	Hiermit wird die Version Ihrer Unisphere-CLI angezeigt.
-cmdTime	Hiermit wird die aktuelle Zeit des Zielsystems angezeigt.
-enableStdErr	Schreiben Sie Fehlermeldungen an <code>stderr</code> statt an <code>stdout</code> .
-flatten	Mit diesem Parameter werden alle Objektnamen zum Anzeigen von Hilfeinformationen in einem abgeflachten Format anstatt in einer Baumstruktur dargestellt.

Zugreifen auf das System

Um über die Unisphere-CLI auf ein System zugreifen und Befehle ausführen zu können, müssen Sie den Netzwerknamen bzw. die Management-IP-Adresse des Systems, Ihren Benutzernamen und Ihr Passwort angeben.

ANMERKUNG: In der Unisphere-CLI gibt es keinen Sitzungsmodus, in dem Sie sich ein Mal beim System anmelden und anschließend Befehle ausführen können. Das Zielsystem, der Benutzername und das Passwort müssen bei jeder Befehlsausführung neu eingegeben werden. Wenn Sie einen Befehl eingeben, erfolgt also zuerst die Anmeldung beim System, dann wird der Befehl ausgeführt, und anschließend werden Sie wieder beim System abgemeldet. Um die Anmeldedaten nicht bei jedem Befehl neu eingeben zu müssen, können Sie mit der Option `-saveUser` den Benutzernamen und das Passwort für das angegebene Paar aus Zielsystem und Port speichern. Der Switch `-saveUser` unterstützt nur einen Satz gespeicherter Anmeldedaten für das System. Dies bedeutet, dass dieser Switch nicht aktiviert werden sollte, wenn das Administrator- und Servicepasswort unterschiedlich ist, da hierdurch eine erfolgreiche Anmeldung des Servicekontos bei der CLI verhindert wird.

Format

```
[{-d|-destination} <value>] [{-u|-user} <user_name>] [{-p|-password} <password>]
```

Switche

Qualifizierer	Beschreibung
<code>-destination -d</code>	Die IP-Adresse bzw. der Netzwerkname des Zielsystems. Wenn Sie diese Option nicht einschließen, verwendet der Client die für <code>-default</code> angegebenen Adressen. Wenn keine Standardadresse existiert, verwendet der Client die localhost-Adresse 127.0.0.1.
<code>-user -u</code>	Die Domain und der Benutzername für die Anmeldung beim System. Beispiel: Local/joe.
<code>-password -p</code>	Das Passwort für die Anmeldung beim System.
<code>-securePassword</code>	Gibt das Passwort im sicheren Modus an – der Benutzer wird aufgefordert, das Passwort einzugeben.
<code>-port</code>	Geben Sie die Portnummer ein, über die Sie auf das System zugreifen. ANMERKUNG: Wenn Sie die Option <code>-port</code> nicht angeben, greift die Unisphere-CLI über den Standardport 443 auf das System zu.
<code>-default</code>	Speichern Sie das Paar aus Ziel und Port als Standardsystem. In diesem Fall wird ein von Ihnen eingegebener Befehl von der Unisphere-CLI auf dem Standardsystem ausgeführt. In der Unisphere-CLI wird das angegebene Paar aus System und Port in einer lokalen Datei gespeichert. Wenn Sie die Option <code>-default</code> angeben, überschreibt die Unisphere-CLI das bislang gespeicherte Paar aus Ziel und Port mit dem neuen Paar. ANMERKUNG: Wenn Sie den Switch <code>-port</code> einbeziehen, wird der angegebene Portwert mit dem Wert <code>-destination</code> gekoppelt und in der lokalen Datei gespeichert. Unter Ausblenden von Kopfzeileninformationen wird erläutert, wie die Anmeldedaten des Nutzerkontos auf dem lokalen Clientsystem gespeichert werden.
<code>-saveUser</code>	Hiermit werden die für die Optionen <code>-user</code> und <code>-password</code> angegebenen Zugangsdaten in einer lokalen Datei gespeichert. Die gespeicherten Zugangsdaten werden bei jedem Befehl automatisch von der Unisphere-CLI auf das angegebene Paar aus Ziel und Port angewendet. Ausblenden der Kopfzeileninformation erläutert, wie die Anmeldedaten des Benutzerkontos auf dem lokalen Clientsystem gespeichert werden.
<code>-removeUser</code>	Hiermit werden die gespeicherten Zugangsdaten für das Paar aus Ziel und Port entfernt.

Beispiel 1

Im folgenden Beispiel greift der Benutzer Local/joe mit dem Passwort 12345 auf das Ziel-Speichersystem 10.0.0.1 zu:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456!
```

Beispiel 2

Im folgenden Beispiel werden die Zugangsdaten für den angegebenen Benutzer gespeichert:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! -saveUser
```

Beispiel 3

Im folgenden Beispiel wird das Zielsystem als Standard festgelegt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! -default
```

Beispiel 4

Im folgenden Beispiel wird auf das Standardsystem zugegriffen:

```
uemcli -u Local/joe -p MyPassword456!
```

Beispiel 5

Im folgenden Beispiel werden die gespeicherten Zugangsdaten vom Zielsystem 10.0.0.1 entfernt:

```
uemcli -d 10.0.0.1 -removeUser
```

Hochladen eines Upgradekandidaten

Um ein Upgrade der Systemsoftware durchzuführen, laden Sie eine Kandidatendatei für das Upgrade hoch, die Sie von der Supportwebsite herunterladen können, und verwenden Sie den Qualifizierer `-upload`. Starten Sie nach dem Hochladen der Kandidatendatei in das System den Upgradeprozess mit einer Upgradesitzung. [Erstellen von Upgradesitzungen](#) erläutert die Konfiguration von Upgradesitzungen.

Voraussetzungen

Sie können den jeweils aktuellen Softwareupgradekandidaten von der Supportwebsite herunterladen.

Format

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! -upload -f <file> upgrade
```

Optionen

Qualifizierer	Beschreibung
-f	Geben Sie den Pfad und Dateinamen der Kandidatendatei für das Upgrade ein, die hochgeladen werden soll. Stellen Sie Pfad und Dateiname in Anführungszeichen.

Beispiel

Im folgenden Beispiel wird eine Kandidatendatei für das Upgrade in das System hochgeladen:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! -upload -f "upgrade-2.0.0.12190-MAGNUM-RETAIL.tgz.bin" upgrade
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection  
  
Operation completed successfully.
```

Ausblenden von Kopfzeileninformationen

Wenn Sie eine Option oder einen Befehl ausführen, wird in der Befehlsausgabe eine Kopfzeile angezeigt, in der das Zielsystem, die Portnummer des Systems, die Syntax und das verwendete Kommunikationsprotokoll (HTTPS) angegeben sind. Beispiel:

```
Storage system address: 127.0.0.1  
Storage system port: 443  
HTTPS connection
```

Mit der Option `-noHeader` können Sie die Kopfzeile ausblenden:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! -noHeader /sys/general show
```

```
1:   System name           = Vorpai  
    Model                 = EMC Storage Systems 12GB RAM WM PHTM  
    Platform type        = EMC Storage System  
    Product serial number = FNM00102000154  
    Auto failback        = on  
    Health state         = Degraded/Warning (10)
```

Speichern von Unisphere CLI-Einstellungen.

Sie können die folgenden Einstellungen auf dem Host speichern, auf dem die Unisphere-CLI ausgeführt wird:

- Benutzerzugangsdaten (Benutzername und Passwort) für jedes System, auf das Sie zugreifen. Weitere Informationen finden Sie in `-saveUser` unter [Anzeigen der Befehlszeilenoptionen](#).
- Aus dem System importierte SSL-Zertifikate. [Weitere Informationen zu SSL-Zertifikaten finden Sie unter](#)
- Informationen zum Standardsystem, auf das über die Unisphere-CLI zugegriffen wird, einschließlich des Systemnamens bzw. der IP-Adresse und der Portnummer des Systems. Weitere Informationen finden Sie in `-default` unter [Anzeigen der Befehlszeilenoptionen](#).

In der Unisphere-CLI werden die Einstellungen in einer sicheren Lockbox gespeichert, die sich lokal auf dem Host befindet, auf dem die Unisphere-CLI installiert ist. Die gespeicherten Daten stehen nur auf dem Host, auf dem sie gespeichert wurden, und dem Benutzer, der die Speicherung veranlasst hat, zur Verfügung. Die Lockbox befindet sich hier:

- Unter Windows XP: `C:\Documents and Settings\\Local Settings\Application Data\.emc\uemcli`
- Unter Windows 7 und Windows 10: `C:\Users\${user_name}\AppData\Local\.emc\uemcli`
- Unter UNIX/Linux: `<home_directory>/\.emc/uemcli`

Die Dateien `cps.clb` und `csp.clb.FCD` sind Lockbox-bezogen. Bei der Deinstallation der Unisphere-CLI werden diese Verzeichnisse und Dateien nicht gelöscht und können optional aufbewahrt werden. Sie können diese Dateien aus Sicherheitsgründen jedoch löschen.

Managen des Systems

Themen:

- Konfigurieren allgemeiner Systemeinstellungen
- Konfigurieren von Systeminformationen
- Verwalten von Softwareversionen
- Anzeigen fehlerhafter Speicherressourcen
- Upgrade des Systems
- Management der Sicherheitseinstellungen
- Managen der Systemzeit
- Zeitzone des Zeitplans verwalten
- Managen von Supportkonfigurations- und Proxyservereinstellungen
- Managen von Supportverträgen
- Managen von Centralized ESRS
- Managen von SupportAssist (nur physische Bereitstellungen)
- Managen von Connect Home
- Managen von Benutzerrollen
- Managen von Benutzerkonten
- Verwalten von Benutzerkontoeinstellungen
- Managen von Supportanmeldedaten
- Managen von Systemlimits
- Anzeigen der Lizenzen für installierte Funktionen
- Lesen und Akzeptieren der Endbenutzer-Lizenzvereinbarung
- Managen der Remoteprotokollierung
- Managen der Systemzertifikate
- Managen von Snapshot-Schutzplänen
- Managen von Aufgabenregeln
- Managen von Jobs
- Managen von Jobschritten

Konfigurieren allgemeiner Systemeinstellungen

Konfigurieren Sie allgemeine Einstellungen im System, wie zum Beispiel:

- Aktivieren bzw. Deaktivieren des automatischen Failbacks für SPs
- Manuelles Failback von NAS-Servern
- Durchführen einer Prüfung der Systemintegrität
- Ändern des Namens des Systems

i ANMERKUNG: Zu einem Failover kommt es, wenn bei einem SP ein Hardware- oder Softwareproblem auftritt. Beim Failover wechseln sämtliche auf diesem SP ausgeführten NAS-Server auf den anderen SP. Die Unterbrechung fällt dabei für die angeschlossenen Hosts so gering wie möglich aus. Sobald der SP repariert ist, findet bei Aktivierung der entsprechenden Option ein automatisches Failback aller NAS-Server auf ihren ursprünglichen SP statt.

In der folgenden Tabelle sind die allgemeinen Systemattribute aufgeführt:

Tabelle 4. Allgemeine Systemattribute

Merkmale	Beschreibung
System name	Name des Systems.

Tabelle 4. Allgemeine Systemattribute (fortgesetzt)

Merkmale	Beschreibung
<code>UUID base</code>	Basiswert, der zur Generierung von UUIDs in der Hostumgebung verwendet wird (wie z. B. OVMS-Hosts).
<code>Model</code>	Das Systemmodell.
<code>System UUID</code> (nur virtuelle Bereitstellungen)	System-UUID (Universally Unique Identifier) für ein virtuelles System.
<code>License activation key</code> (nur virtuelle Bereitstellungen)	Ein Schlüssel, der bestätigt, dass das System lizenziert ist und dass die Software legal erworben wurde.
<code>Product serial number</code>	Die Seriennummer des Systems.
<code>Auto failback</code>	Hier ist angegeben, ob für den SP automatisches Failback aktiviert ist. Gültige Werte: <ul style="list-style-type: none"> • <code>on</code> • <code>off</code>
<code>Health state</code>	Der aktuelle Integritätsstatus des Systems. Der Integritätsstatuscode wird in Klammern angezeigt. Gültige Werte: <ul style="list-style-type: none"> • <code>Unknown (0)</code> : Status ist unbekannt. • <code>OK (5)</code> : Funktioniert ordnungsgemäß. • <code>OK BUT (7)</code> : Funktioniert ordnungsgemäß, aber es könnte ein Problem vorliegen. • <code>Degraded/Warning (10)</code> : Funktioniert und führt alle Funktionen aus, die Performance ist jedoch eventuell nicht optimal. • <code>Minor failure (15)</code> : Funktioniert und führt alle Funktionen aus, aber die Gesamtperformance ist eingeschränkt. Diese Bedingung hat geringe Auswirkungen auf das System, und das Problem sollte in der näheren Zukunft angegangen werden, aber eine unmittelbare Lösung ist nicht erforderlich. • <code>Major failure (20)</code> : Im System sind Fehler aufgetreten, und einige oder alle Funktionen funktionieren nur noch eingeschränkt oder gar nicht mehr. Dieser Zustand hat erhebliche Auswirkungen auf das System und muss sofort beseitigt werden. • <code>Critical failure (25)</code> : Es ist ein Fehler aufgetreten; eine Recovery ist eventuell nicht möglich. Diese Bedingung hat zu Datenverlusten geführt. Der Fehler muss umgehend behoben werden. • <code>Non-recoverable error (30)</code> : Das System ist komplett ausgefallen und kann nicht wiederhergestellt werden.
<code>Health details</code>	Zusätzliche Integritätsinformationen. Weitere Informationen zur Integrität finden Sie im Anhang A, Referenz.
<code>Power (Present)</code> (nur physische Bereitstellungen)	Derzeitiger Stromverbrauch des Systems
<code>Power (Rolling Average)</code> (nur physische Bereitstellungen)	Durchschnittlicher Stromverbrauch des Systems (in der letzten Stunde mit 30-Sekunden-Sampling-Rate)
<code>Supported SP upgrades</code> (nur physische Bereitstellungen)	Liste der Storage-Prozessornamen, auf die das aktuelle System ein Upgrade durchführen kann.

Anzeigen von Systemeinstellungen

Zeigen Sie die aktuellen Systemeinstellungen an.

 **ANMERKUNG:** Aktionsbefehl „show“ erläutert, wie das Ausgabeformat geändert wird.

Format

```
/sys/general show
```

Beispiel 1 (nur physische Bereitstellungen)

Mit dem folgenden Befehl werden die allgemeinen Einstellungen für ein physisches System angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/general show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:   System name           = demo
     Model                = Unity 300
     UUID Base            = 0
     System UUID          =
     Product serial number = demo
     Auto failback        = on
     Health state         = OK (5)
     Health details       = "The system is operating normally."
     Power (Present)      = 572 watts
     Power (Rolling Average) = 573 watts
     Supported SP upgrades = SP400, SP500, SP600
```

Beispiel 2 (nur virtuelle Bereitstellungen)

Mit dem folgenden Befehl werden die allgemeinen Einstellungen für ein virtuelles System angezeigt:

 **ANMERKUNG:** UUID Base wird nicht angezeigt, wenn die Option `-detail` nicht angegeben ist.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/general show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:   System name           = Demo
     Model                = UnityVSA
     System UUID          = 421D3F1B-6D79-52A1-9AC7-67AE794E520E
     License activation key = CQPZQ0DJJQHR0X
     Product serial number = VIRT14349BPJEP
     Health state         = OK (5)
```

Ändern der allgemeinen Systemeinstellungen

Ändern Sie den Namen des Systems bzw. die Einstellung für das automatische Failback.

Format

```
/sys/general set [-name <value>] [-uuidBase <value>] [-autoFailback {on|off}]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-name	Geben Sie einen Namen für das System ein.

Qualifizierer	Beschreibung
-uuidBase	Geben Sie den UUID-Basiswert ein.
-autoFailback	Hiermit wird das automatische Failback aktiviert bzw. deaktiviert. Gültige Werte: <ul style="list-style-type: none"> • on • off

Beispiel

Mit dem folgenden Befehl deaktivieren Sie das automatische Failback:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/general set -autoFailback off
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Manuelles Failback von NAS-Servern

Führen Sie nach einem Failover manuell ein Failback aller NAS-Server auf ihren ursprünglichen SP durch. Wenn das automatische Failback aktiviert ist, muss es nicht manuell eingeleitet werden.

Format

```
/sys/general failback
```

Beispiel

Mit dem folgenden Befehl wird ein Failback aller NAS-Server durchgeführt, auf denen es vorher zu einem Failover gekommen ist:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/general failback
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Durchführen einer Systemintegritätsprüfung

Führen Sie eine Integritätsprüfung des gesamten Systems durch. Eine Integritätsprüfung umfasst mehrere Untersuchungen zum Status des Systems, damit eventuelle verborgene Probleme ausgeschlossen werden können.

ANMERKUNG: Vor dem Upgrade der Systemsoftware muss eine Systemintegritätsprüfung durchgeführt werden. Damit die Systemsoftware aktualisiert werden kann, müssen sämtliche Systemkomponenten die Integritätsprüfung bestehen. Wenn eine Systemkomponente eine herabgesetzte Leistungsfähigkeit aufweist, schlägt das Update fehl.

Format

```
/sys/general healthcheck
```

Beispiel

Mit dem folgenden Befehl führen Sie eine Systemintegritätsprüfung durch:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/general healthcheck
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1: Error code = Error: The health check has failed. An internal error is preventing
the health check from completing successfully. Record the error code and search the
EMC Online Support website for available support options.
[Error Code: platform::check_boot_control_status_2]

Operation completed successfully.
```

ANMERKUNG:

- Die Ergebnisse der Integritätsprüfung enthalten möglicherweise Fehler und Warnungen, aber eine Meldung von `Operation completed successfully.` wird in der Ausgabe angezeigt. Dies ist nur ein Hinweis, dass die Integritätsprüfung durchgeführt wurde, nicht, dass sie erfolgreich ohne Fehler und Warnungen abgeschlossen wurde. Versuchen Sie, alle Fehler zu beheben und führen Sie die Integritätsprüfung erneut durch.
- Wenn Fehler auftreten, ist ein Softwareupgrade des Systems nicht zulässig. Wenn Warnungen auftreten, können sie während des Upgradeverfahrens umgangen werden.

Konfigurieren von Systeminformationen

Konfigurieren Sie Systeminformationen über den Standort und Benutzer des Systems.

In der folgenden Tabelle sind die Attribute der Systeminformationen aufgeführt:

Tabelle 5. Attribute der Systeminformationen

Attribut	Beschreibung
Location name	Speicherortname
Address 1	Adresse des Ansprechpartners für das System
City	Name des Ortes
State	Name des Bundeslands oder Kantons
Country	Zweistelliger Ländercode
Postal Code	Postleitzahl
Contact first name	Vorname des Benutzers
Contact last name	Nachname des Benutzers
Contact mobile phone	Mobiltelefonnummer des Benutzers
Contact company	Unternehmen des Benutzers
Site ID	Interne ID zur Identifizierung des Standorts, an dem das System installiert ist.
Contact email address	E-Mail-Adresse der Kontaktperson für das System
Contact phone number	Telefonnummer der Kontaktperson für das System

Anzeigen von Systeminformationen

Zeigen Sie die aktuellen Systeminformationen an.

 **ANMERKUNG:** Aktionsbefehl „show“ erläutert, wie das Ausgabeformat geändert wird.

Format

```
/sys/info show
```

Beispiel

Mit dem folgenden Befehl werden die allgemeinen Einstellungsinformationen für das System angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/info show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:   Contact first name   = Zach
     Contact last name  = Arnold
     Contact company    = EMC
     Contact email address = something@somemail.com
     Contact phone number = 123456789
```

Konfigurieren oder Ändern der Systemkontaktinformationen

Geben Sie die Attribute für System und Kontaktinformationen ein oder ändern Sie sie.

Format

```
/sys/info set [-location <value>] [-contactFirstName <value>] [-contactLastName <value>] [-contactEmail <value>] [-contactPhone <value>] [-contactMobilePhone <value>]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-location	Geben Sie einen aktualisierten Standortnamen an.
-contactEmail	Geben Sie die neue E-Mail-Adresse des Ansprechpartners für das System an.
-contactPhone	Geben Sie die neue Telefonnummer des Ansprechpartners für das System an.
-contactMobilePhone	Geben Sie die neue mobile Telefonnummer des Ansprechpartners für das System an.
-contactFirstName	Geben Sie den neuen Vornamen des Ansprechpartners für das System an.
-contactLastName	Geben Sie den neuen Nachnamen des Ansprechpartners für das System an.

Beispiel

Mit dem folgenden Befehl können Sie die folgenden Systeminformationen ändern:

- Kontakt – Vorname
- Kontakt – Nachname
- E-Mail-Adresse der Kontaktperson
- Telefonnummer der Kontaktperson
- Standort des Systems
- Kontakt – Mobiltelefon

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/info set -contactFirstName Zach
-contactLastName Arnold -contactEmail something@someemail.com -contactPhone 1233456789 -location
here -contactMobilePhone 987654321
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
Operation completed successfully.
```

Verwalten von Softwareversionen

Sie können Details zu den Systemsoftwareversionen aufrufen, die manuell von einem Benutzer in das System hochgeladen wurden oder die vom Support automatisch in das System übertragen wurden.

 **ANMERKUNG:** Der Support überträgt nur Software-Images auf das System, wenn der Benutzer vorher seine Einwilligung gegeben hat.

Tabelle 6. Attribute der Systemsoftware

Attribut	Beschreibung
ID	ID der Systemsoftware.
Type	Art der Systemsoftware. Folgende Werte sind möglich: <ul style="list-style-type: none"> • installed : das aktuell auf dem System installierte Software-Image • candidate : in das System hochgeladener Kandidat zum Upgrade der Systemsoftware • downloaded: Software-Image, das vom Support automatisch in das System übertragen wurde
Version	Die Softwareversion.
Release date	Das Datum, an dem die Software veröffentlicht wurde.
Full version	Vollversion der Software.  ANMERKUNG: Dieser Wert ist für heruntergeladene Software-, Firmware- und Sprachpakete leer.
Reboot required	Hier ist angegeben, ob ein Neustart für dieses Softwareupgradepaket erforderlich ist. Die Werte lauten: <ul style="list-style-type: none"> • yes • no
Pause allowed	Hier ist angegeben, ob das Softwareupgradepaket dem Benutzer das Anhalten des Upgrades und das Auswählen des gewünschten Disruptive Upgrade-Fensters ermöglicht. Die Werte lauten: <ul style="list-style-type: none"> • yes • no
Image filename	Der Dateiname des Software-Image.

Anzeigen der Systemsoftwareversion

Zeigen Sie die Version des in das System hochgeladenen Kandidaten für das Upgrade der installierten Systemsoftware an. [Upgrade des Systems](#) erläutert, wie Sie ein Upgrade der Systemsoftware durchführen.

Format

```
/sys/soft/ver [{"-id <value>|"-type {installed|candidate|downloaded}}] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID der Systemsoftware ein.
-type	Geben Sie den Softwaretyp ein. Folgende Werte sind möglich: <ul style="list-style-type: none">● <code>installed</code> : Es wird die Version der installierten Systemsoftware angezeigt.● <code>candidate</code> : Es wird die Version des in das System hochgeladenen Kandidaten für das Upgrade der Systemsoftware angezeigt.● <code>downloaded</code> : Software-Image, das vom Support automatisch in das System übertragen wurde.

Beispiel

Mit dem folgenden Befehl werden Details zur installierten Systemsoftware und einem hochgeladenen Upgradekandidaten angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/soft/ver show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:   ID           = INST_1
     Type        = installed
     Version     = 5.2.0.0.5.001
     Release date = 2020-08-26 08:32:30
     Full version = Unity 5.2.0.0 (Release, Build 001, 2020-08-26 08:32:30,
5.2.0.0.5.001)
     Image type  =
     Reboot required =
     Pause allowed =
     Image filename =

2:   ID           = CAND_1
     Type        = candidate
     Version     = 5.2.0.0.5.002
     Release date = 2020-08-28 07:26:51
     Full version = Unity 5.2.0.0 (Release, Build 002, 2020-08-28 07:26:51,
5.2.0.0.5.002)
     Image type  = software
     Reboot required = yes
     Pause allowed = yes
     Image filename = Unity-upgrade-5.2.0.0.5.002-5.2.0.0.5.002-GNOSIS_RETAIL.tgz.bin

3:   ID           = ASD_1
     Type        = downloaded
     Version     = 4.2.0.9215195
     Release date =
     Full version =
     Image type  = software
     Reboot required =
     Pause allowed =
     Image filename = Unity-merlin_dev_qiand2-
upgrade-4.2.0.9215195.9215195-4.2.0.9215195.9215195-GNOSIS_DEBUG.tgz.bin.gpg

4:   ID           = ASD_2
     Type        = downloaded
     Version     = V2-Dec-19-2016
     Release date =
     Full version =
     Image type  = firmware
     Reboot required =
     Pause allowed =
     Image filename = Unity-Drive-Firmware-V2-Dec-19-2016.tgz.bin.gpg
```

Vorbereiten der Systemsoftware für die Installation

Sie können ein automatisch heruntergeladenes Software-Image für die Installation vorbereiten.

ANMERKUNG: Der Support überträgt nur Software-Images auf das System, wenn der Benutzer vorher seine Einwilligung gegeben hat.

Format

```
/sys/soft/ver -id <value> prepare
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID der automatisch heruntergeladenen Systemsoftware ein.

Beispiel 1

Mit dem folgenden Befehl wird das automatisch heruntergeladene Software-Image „ASD_1“ für die Installation vorbereitet:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/soft/ver -id ASD_1 prepare
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
Operation completed successfully.
```

Beispiel 2

Bei folgendem Befehl wird eine Fehlermeldung zurückgegeben, da er sich auf ein nicht automatisch heruntergeladenes Software-Image bezieht:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/soft/ver -id CAND_1 prepare
```

```
Operation failed. Error code: 0x6000cd5
The specified image ID is invalid. The current action can only be performed on downloaded
images. Obtain the image ID with '/sys/soft/ver -type downloaded show' and try again with
correct image ID. (Error Code:0x6000cd5)
```

ANMERKUNG: Mit dem Befehl `/sys/soft/ver show` können Sie IDs der automatisch heruntergeladenen Software-Images auf dem System abrufen. Unter „Type“ muss „downloaded“ stehen, wie im folgenden Beispiel gezeigt:

```
ID = ASD_1
Type = downloaded
Version = 4.2.0.9215195
Release date =
Image type = software
Reboot required =
Pause allowed =
Image filename = Unity-_dev_001-upgrade-4.2.0.9215195.9215195-4.2.0.9215195.9215195-
GNOSIS_DEBUG.tgz.bin.gpg
```

Anzeigen fehlerhafter Speicherressourcen

Mit diesem Befehl wird eine Liste der Speicherressourcen angezeigt, die sich in einem fehlerhaften Status befinden, einschließlich ihres Integritätsstatus.

Format

```
/sys/res/health/fault
```

Beispiel

Im folgenden Beispiel werden die Speicherressourcen aufgeführt, die sich in einem fehlerhaften Status befinden, sowie die Art der Ressource und die entsprechenden Informationen zum Integritätsstatus.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/res/health/fault show
```

```
Storage system address: 10.64.75.201
Storage system port: 443
HTTPS connection

1:      ID           = pool_1
      Type          = pool
      Health state  = Degraded/Warning (10)

2:      ID           = sv_2
      Type          = lun
      Health state  = Minor failure (15)
```

Upgrade des Systems

Erstellen Sie eine Upgradesitzung, um das System zu aktualisieren oder vorhandene Upgradesitzungen anzuzeigen. In der Upgradesitzung wird ein Upgradekandidat installiert, der in das System hochgeladen wurde. Sie können den jeweils aktuellen Upgradekandidaten von der Supportwebsite herunterladen. Mit der Option `-upload` laden Sie den Kandidaten vor Beginn der Upgradesitzung in das System hoch.

Der aktuelle Software-Upgradekandidat enthält alle verfügbaren Hotfixes. Wenn Sie ein Hotfix auf Ihr System angewendet haben, wird es im aktuellen Upgradekandidat integriert.

i ANMERKUNG: Damit das System aktualisiert werden kann, müssen sämtliche Systemkomponenten die Integritätsprüfung bestehen. Wenn eine Systemkomponente heruntergestuft wird, schlägt das Update fehl. [Durchführen einer Systemintegritätsprüfung](#) erläutert, wie Sie eine Integritätsprüfung auf dem System ausführen.

In der folgenden Tabelle sind die Attribute für Upgradesitzungen aufgeführt.

Tabelle 7. Attribute von Upgradesitzungen

Attribut	Beschreibung
Status	Aktueller Status der Upgradesitzung. Folgende Werte sind möglich: <ul style="list-style-type: none">• <code>running</code>: Die Systemsoftware wird aktualisiert.• <code>completed</code>: Das Upgrade der Systemsoftware ist abgeschlossen.• <code>paused</code>: Die Upgradesitzung wurde angehalten, bevor die Speicherprozessoren neu gestartet wurden.• <code>failed</code>: Bei der Upgradesitzung ist ein Fehler aufgetreten.
Progress	Aktueller Fortschritt der Upgradesitzung.
Creation time	Datum und Uhrzeit der Erstellung der Upgradesitzung.
Elapsed time	Bisherige Ausführungsdauer der Upgradesitzung.
Estimated time left	Für den Abschluss der Upgradesitzung erforderliche geschätzte Zeit

Tabelle 7. Attribute von Upgradesitzungen (fortgesetzt)

Attribut	Beschreibung
Percent complete	Zeigt den Fortschritt des Upgrades in Prozent an.
Type	Der Typ des durchgeführten Upgrade: Softwareupgrade oder Upgrade des Speicherprozessors. Für Softwareupgrade sind Details über <code>/sys/soft/ver show</code> verfügbar.
Additional info	Weitere Informationen zum Status des Upgrades.

Erstellen von Upgradesitzungen

Erstellt eine neue Upgradesitzung. Dies könnte ein Upgrade von Software oder Hardware sein, das von einer Sitzung überwacht wird.

ANMERKUNG: Verwenden Sie Unisphere oder die Unisphere-CLI nicht, um das System während eines Softwareupdates zu managen oder zu konfigurieren.

Format

```
/sys/upgrade create -type {software [-candId <value>] [-pauseBeforeReboot] | sp -newSPModel <value>} [-offline]} [-pauseBetweenReboots]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-candId	Geben Sie die ID des hochzuladenden Upgradekandidaten ein. Systemsoftwareversionen anzeigen erläutert, wie Sie die ID des hochgeladenen Softwarekandidaten anzeigen. ANMERKUNG: Dieses Argument ist optional. Wenn kein Wert angegeben wird, sucht das System den Upgradekandidaten.
-pauseBeforeReboot	Geben Sie an, ob die Ausführung aller Aufgaben während des Upgrades angehalten werden soll, bevor die SPs neu starten. ANMERKUNG: Diese Option wird ignoriert für Sprachpakete, Hotfixes und ODFU-Updates.
-newSPModel	Starten Sie ein Upgrade des Speicherprozessors mit dem angegebenen Zielmodell. Die möglichen Werte für dieses System werden mit <code>/sys/general show</code> identifiziert.
-offline	Optionaler Parameter, mit dem ein Offlineupgrade des Speicherprozessors und kein Onlineupgrade (Standardeinstellung) durchgeführt wird.
-pauseBetweenReboots	Optionaler Parameter für die Software- oder Online-DIP-Updates (Data in Place). Sofern angegeben, wird das System angehalten, nachdem das Upgrade für den ersten SP durchgeführt wurde und bevor das Upgrade für den zweiten SP durchgeführt wird. Dadurch wird das Upgrade unterbrochen und Sie können es manuell mit <code>/sys/upgrade resume</code> fortsetzen.

Beispiel 1

Mit dem folgenden Befehl wird eine Sitzung für das Upgrade der Systemsoftware erstellt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/upgrade create -type software
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

ANMERKUNG: Alle Warnmeldungen (sofern vorhanden) werden angezeigt, wenn Sie den Upgradeprozess zum ersten Mal ausführen. Führt ein potenzielles Problem zu einer Warnmeldung, stoppt der Aktualisierungsvorgang. Wenn Sie die Warnmeldung gelesen haben, führen Sie den Befehl erneut aus, um mit dem Upgrade fortzufahren. Dieses Mal führt der Upgradeprozess die Prüfungen erneut aus, aber hält für Warnmeldungen nicht an. Der Upgradeprozess hält nur an, wenn ein Fehler auftritt.

Beispiel 2

Mit dem folgende Befehl wird eine Sitzung erstellt, um ein Upgrade für den Speicherprozessor durchzuführen:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/upgrade create -type sp -newSPModel SP500
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Beispiel 3

Mit dem folgenden Befehl wird ein DIP-Offlineupgrade initiiert.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/upgrade create -type sp -newSPModel SP500 -offline
```

```
Storage system address: 10.64.75.201
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Beispiel 4

Mit dem folgenden Befehl wird ein Softwareupgrade initiiert, das nach den ersten SP-Neustarts angehalten wird.

```
uemcli /sys/upgrade create -type software -pauseBetweenReboots
```

```
Storage system address: 10.64.75.201
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Anzeigen von Upgradesitzungen

Zeigen Sie Details einer vorhandenen Sitzung zum Upgrade an.

ANMERKUNG: Aktionsbefehl „show“ erläutert, wie das Ausgabeformat geändert wird.

Format

```
/sys/upgrade show
```

Beispiel 1

Mit dem folgenden Befehl werden Details zur Hardwareupgradesitzung angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/upgrade show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      Type                = SP
      Status                = Running
      Status message       =
      Creation time        = 2015-11-09 19:43:08
      Elapsed time         = 01h 3m 08s
      Estimated time left  = 01h 70m 00s
      Progress              = Task 2 of 5 (Running health checks)
      Percent complete     = 5%
```

Beispiel 2

Mit dem folgenden Befehl werden Details zur Softwareupgradesitzung angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/upgrade show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      Type                = Software
      Status                = Failed
      Status message       = Stopping c4 stack on SPA timeout expired
      Creation time        = 2009-11-09 18:04:12
      Elapsed time         = 00h 20m 08s
      Estimated time left  =
      Progress              = Task 5 of 25 (Stopping c4 stack on SPA)
      Percent complete     = 15%
```

Beispiel 3

Mit dem folgenden Befehl wird ein Problem mit der Integritätsprüfung vor dem Upgrade in `Additional info` angezeigt.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/upgrade show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      Type                = Software
      Status                = Failed
      Creation time        = 2009-11-09 18:04:12
      Elapsed time         = 00h 20m 08s
      Estimated time left  =
      Progress              =
      Percent complete     = 5%
      Additional info      = "Error: The health check has failed. An internal error
is preventing the health check from completing successfully. Record the error code
and search the EMC Online Support website for available support options. [Error
Code: platform::check_boot_control_status_2]","Error: One or more LUNs are in degraded
state. Record the error code and contact your service provider. [Error Code:
flr::check_if_lun_recovery_is_required_2]"
```

Wiederaufnahmen der Upgradesitzung

Nehmen Sie eine bestehende Upgradesitzung wieder auf, die angehalten wurde oder fehlgeschlagen ist.

Format

```
/sys/upgrade resume
```

Beispiel

Der folgende Befehl setzt das Upgrade fort:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/upgrade resume
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
Operation completed successfully.
```

Abbrechen einer Upgradesitzung

Brechen Sie eine Upgradesitzung ab, die fehlgeschlagen ist oder angehalten wurde. Bei einem Ausfall mit Sperre (spätere Schritte bei Betriebssystem- oder Speicherprozessorupgrade) kann das Upgrade nicht abgebrochen werden und muss stattdessen wiederaufgenommen werden.

Format

```
/sys/upgrade cancel
```

Beispiel

Mit dem folgenden Befehl wird die Upgradesitzung abgebrochen.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/upgrade cancel
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
Operation completed successfully.
```

Management der Sicherheitseinstellungen

Management von Sicherheitseinstellungen für das System

In der folgenden Tabelle sind die Attribute der Systeminformationen aufgeführt:

Tabelle 8. Attribute der Sicherheitseinstellungen

Merkmale	Beschreibung
FIPS 140 mode	Zeigt an, ob das System im FIPS-Modus arbeitet. Gültige Werte: <ul style="list-style-type: none">• enabled• disabled  ANMERKUNG: Der Standardwert ist „disabled“.
TLS mode	Zeigt die niedrigste Version des TLS-Protokolls an, die das System für die SSL-Kommunikation unterstützt. Gültige Werte: <ul style="list-style-type: none">• TLSv1.0 and above• TLSv1.1 and above

Tabelle 8. Attribute der Sicherheitseinstellungen (fortgesetzt)

	<ul style="list-style-type: none"> • TLSv1.2 and above <p>ANMERKUNG: Der Standardwert ist TLSv1.0 and above.</p>
Restricted shell mode	<p>Gibt an, ob für das Servicekonto die eingeschränkte Shell auf dem Speicherprozessor aktiviert ist. Gültige Werte:</p> <ul style="list-style-type: none"> • enabled • disabled <p>ANMERKUNG: Der Standardwert ist „enabled“.</p>

Anzeigen von Sicherheitseinstellungen

Zeigt aktuelle Sicherheitseinstellungen für das System an.

Format

```
/sys/security show
```

Beispiel

Mit dem folgenden Befehl werden die Sicherheitseinstellungen für das System angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/security show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:  FIPS 140 mode           = disabled
    TLS mode                = TLSv1.0 and above
    Restricted shell mode = enabled
```

Ändern von Sicherheitseinstellungen

Ändern Sie die Sicherheitseinstellungen für das System.

Format

```
/sys/security set {-fips140Enabled {yes | no} | -tlsMode {TLSv1.0 | TLSv1.1 | TLSv1.2} |
-restrictedShellEnabled {yes | no}}
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-fips140Enabled	<p>Aktiviert oder deaktiviert den FIPS 140 Compliance-Modus. Gültige Werte:</p> <ul style="list-style-type: none"> • yes • no
-tlsMode	<p>Gibt die niedrigste Version des TLS-Protokolls an, die das System für die SSL-Kommunikation unterstützt. Gültige Werte:</p> <ul style="list-style-type: none"> • TLSv1.0

Qualifizierer	Beschreibung
	<ul style="list-style-type: none"> • TLSv1.1 • TLSv1.2 <p>ANMERKUNG: Die Angabe von TLS 1.1 oder TLS 1.2 kann sich auf vorhandene Clientanwendungen auswirken, die nicht mit den entsprechenden TLS-Protokollen kompatibel sind. Die folgenden Funktionen können nicht verwendet werden, wenn TLS 1.1 angegeben ist:</p> <ul style="list-style-type: none"> • Die Replikation von oder auf OE-Versionen vor 4.3 wird nicht unterstützt. • Wenn für Unisphere ein Browser auf die Verwendung von TLS 1.0 eingeschränkt ist und der <code>tlsMode</code> auf dem System entweder TLS 1.1 oder TLS 1.2 unterstützt, wird die Unisphere Anmeldeseite nicht geladen und es wird ein Sicherheitsfehler angezeigt. <p>Die folgenden Funktionen können nicht verwendet werden, wenn TLS 1.2 angegeben ist:</p> <ul style="list-style-type: none"> • Die Replikation von oder auf OE-Versionen vor 4.3 wird nicht unterstützt. • Wenn für Unisphere ein Browser auf die Verwendung von TLS 1.1 eingeschränkt ist und der <code>tlsMode</code> auf dem System TLS 1.2 unterstützt, wird die Unisphere Anmeldeseite nicht geladen und es wird ein Sicherheitsfehler angezeigt. • Alle vorhandenen Unisphere CLI-Client-Versionen (d. h. Unisphere CLI-Client-Version 5.2.3 und früher) unterstützen TLS 1.2 nicht. Wenn Sie Unisphere CLI-Clients verwenden und TLS 1.1 deaktivieren, können Unisphere CLI-Clients keine Verbindung mit Unity herstellen. In diesem Fall müssen Sie die Unisphere CLI-Client Version 5.0.3 installieren, um eine Verbindung mit Unity herzustellen.
<code>-restrictedShellEnabled</code>	Aktiviert oder deaktiviert für das Servicekonto die eingeschränkte Shell auf dem Speicherprozessor. Gültige Werte: <ul style="list-style-type: none"> • <code>yes</code> • <code>no</code>

Beispiele

Mit dem folgenden Befehl werden die Sicherheitseinstellungen des Systems für den FIPS-140-Modus geändert:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/security set -fips140Enabled yes
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
The system will reboot one SP at a time for this change to take effect. Do you want to
continue?
yes / no: yes
```

Operation completed successfully.

Mit dem folgenden Befehl werden die Sicherheitseinstellungen des Systems für den TLS-Modus geändert:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/security set -tlsMode TLSv1.1
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
Please refer to the Security Configuration Guide for backward compatibility.
This change may impact running operations (e.g. replication) and the management services will
be automatically restarted for the change to take effect.
Do you want to continue?
yes / no: yes
```

Operation completed successfully.

ANMERKUNG: Der Befehl `security set -tlsMode` aktualisiert nicht die unterstützten TLS-Protokollversionen für einen NAS-Server. Verwenden Sie das `svc_nas` Serviceskript, um die unterstützten TLS-Protokollversionen für einen NAS-Server zu

konfigurieren. Weitere Informationen zu diesem Serviceskript finden Sie im Dokument *Dell Unity Family Service Commands Technical Notes*.

Mit dem folgenden Befehl wird die Systemsicherheitseinstellung für die Einstellung „restricted shell enabled“ geändert:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/security set -restrictedShellEnabled no
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
This action will disable restricted shell for service account on the storage processor. Do
you want to continue?
yes / no: yes

Operation completed successfully.
```

Managen der Systemzeit

In der folgenden Tabelle sind die Systemzeitattribute aufgeführt:

Tabelle 9. Attribute der Systemzeit

Merkmale	Beschreibung
Time	Systemzeit – ohne Verzögerung bei der Verarbeitung des Befehls. Die Differenz zwischen der erforderlichen und der tatsächlichen Zeit kann aufgrund der Verzögerung bei der Verarbeitung des Befehls bis zu einer Minute betragen.  ANMERKUNG: <code>-gmt off</code> hat Auswirkungen auf die Systemzeit.

Anzeigen der Systemzeit

Zeigen Sie die aktuelle Systemzeit an.

Format

```
/sys/time show
```

Beispiel

Mit dem folgenden Befehl wird die Systemzeit angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/time show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1: Time      = 2011-01-01 03:00:00
```

Ändern der Systemzeit

Ändern Sie die Systemzeit.

Format

```
/sys/time set {-clientTime | -utc <value>} [-force {noreboot | allowreboot | allowdu}]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-clientTime	Gibt an, dass die Systemzeit mit der Zeit des Systems synchronisiert werden soll, von dem aus die CLI ausgeführt wird. i ANMERKUNG: Die Differenz zwischen der Client-Zeit und der tatsächlichen Systemzeit kann aufgrund der Verzögerung bei der Verarbeitung des Befehls bis zu einer Minute betragen.
-utc	Geben Sie die im System einzustellende Zeit an (im UTC-Format). Format: <YYYY>-<MM>-<DD><hh>:<mm>:<ss> i ANMERKUNG: Die Differenz zwischen der erforderlichen und der tatsächlichen Zeit kann aufgrund der Verzögerung bei der Verarbeitung des Befehls bis zu einer Minute betragen.
-force	Geben Sie an, ob der für die Zeitänderung eventuell erforderliche Systemneustart akzeptiert oder abgelehnt werden soll. Wenn Sie nichts angeben, werden Sie gegebenenfalls zur Bestätigung des Neustarts aufgefordert. Gültige Werte: <ul style="list-style-type: none">• noreboot• allowreboot• allowdu i ANMERKUNG: allowdu wird verwendet, wenn sich das System in einem heruntergestuften Zustand befindet oder einen SP aufweist (während des Neustarts sind die Daten nicht verfügbar). Andernfalls fortfahren mit allowreboot. Im unbeaufsichtigten Modus wird das System bei Bedarf neu gestartet.

Beispiel

Mit dem folgenden Befehl können Sie den Systemneustart akzeptieren:

```
uemcli /sys/time set -utc "2011-05-17 14:26:20" -force allowreboot
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully
```

Zeitzone des Zeitplans verwalten

In der folgenden Tabelle sind die Attribute der Zeitzone des Zeitplans aufgeführt:

i **ANMERKUNG:** Die Zeitzone des Zeitplans bezieht sich nur auf die Planung von Snapshots und die Zeitplanung der asynchronen Replikationsdrosselung. Es handelt sich nicht um eine allgemeine Einstellung der Systemzeitzone.

Tabelle 10. Attribute der Zeitzone des Zeitplans

Merkmale	Beschreibung
Name	Name der Zeitzone des Zeitplans.

Zeitzone des Zeitplans anzeigen

Zeigt die aktuelle Zeitzone des Zeitplans an.

Format

```
/sys/schedtimezone show
```

Beispiel

Mit dem folgenden Befehl wird die Zeitzone des Zeitplans angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/schedtimezone show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1: Name      = (UTC-05:00) Eastern Time (US & Canada)

Operation completed successfully.
```

Zeitzone des Zeitplans ändern

Ändern Sie die Zeitzone für Zeitpläne.

Format

```
/sys/schedtimezone set -name <timezone_string>
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-name	Gibt den Namen der Zeitzone des Zeitplans an, der in doppelte Anführungszeichen gesetzt sein sollte, wenn ein Leerzeichen im Namen enthalten ist.  ANMERKUNG: Wenn Sie die Zeitzone auf UTC Legacy festlegen, wird die Auswirkung der Zeitzone gelöscht.

Beispiel 1

Mit dem folgenden Befehl wird die Zeitzone für den Snapshot-Zeitplan auf den der lokalen Zeitzone für Eastern Time (USA und Kanada) festgelegt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/schedtimezone set -name "(UTC-05:00) Eastern Time (US & Canada)"
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Be aware of the following possible impacts of changing time zone:
 1. Existing snapshot schedule is not updated to the same absolute time when the time zone
    is changed. Check whether your snapshot schedule needs to be updated after changing the time
    zone.
 2. If the time zone is changed at the same time a scheduled snapshot is created, the
    scheduled snapshot may not be created properly. Avoid changing the time zone at the same time
    a scheduled snapshot is created.
Do you want to continue to change time zone? Input yes to continue or no to abort.
yes / no / y / n: yes

Operation completed successfully.
```

Mit dem folgenden Befehl werden alle unterstützten Zeitzonen angezeigt, die in der Namensliste abgerufen werden können:

```
uemcli /sys/schedtimezone set -h
```

Beispiel 2

Mit dem folgenden Befehl wird die Zeitzone für den Snapshot-Zeitplan auf den der lokalen Zeitzone für Eastern Time (USA und Kanada) festgelegt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/schedtimezone set -name "UTC Legacy"
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

Be aware of the following possible impacts of changing time zone:

1. Existing snapshot schedule is not updated to the same absolute time when the time zone is changed. Check whether your snapshot schedule needs to be updated after changing the time zone.
2. If the time zone is changed at the same time a scheduled snapshot is created, the scheduled snapshot may not be created properly. Avoid changing the time zone at the same time a scheduled snapshot is created.

Do you want to continue to change time zone? Input yes to continue or no to abort.

yes / no / y / n: yes

Operation completed successfully.

Mit dem folgenden Befehl werden alle unterstützten Zeitzonen angezeigt, die in der Namensliste abgerufen werden können:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/schedtimezone set -h
```

Managen von Supportkonfigurations- und Proxyservereinstellungen

Managen Sie die Einstellungen der Supportkonfiguration im System, wie zum Beispiel:

- Name der IP-Adresse des Proxyserver.
- Portnummer des Proxyserver.
- Name des Kontos auf dem Proxyserver.
- Passwort des Kontos.
- Gibt an, ob die Liste der Supportverträge automatisch wöchentlich aktualisiert wird.
- Gibt an, ob Cloudmanagement für Services wie Cloud IQ aktiviert ist.

In der folgenden Tabelle sind die Attribute der Supportkonfiguration aufgeführt:

Tabelle 11. Attribute der Supportkonfiguration

Merkmale	Beschreibung
Support proxy server address	Name oder IP-Adresse des Support-Services-Proxyserver.
Support proxy server port	Portnummer des Supportservices-Proxyserver
Support proxy server user name	Name des Kontos auf dem Support-Proxyserver.
Support proxy server password	Passwort des Kontos auf dem Support-Proxyserver.
Automatic support contracts update enabled	Gibt an, ob das System seine Serviceverträge automatisch einmal wöchentlich aktualisiert.
Cloud management enabled	Gibt an, ob Cloudmanagement aktiviert ist. Mögliche Werte sind: <ul style="list-style-type: none">• enabled• disabled (Standard)

Anzeigen von Supportkonfigurations- und Proxyservereinstellungen

Zeigen Sie die aktuellen Informationen der Supportkonfiguration an.

Format

```
/sys/support/config show
```

Beispiel 1

Mit dem folgenden Befehl wird die Support-Konfiguration angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/config show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:   Support proxy server enabled = yes
     Support proxy server address = 10.0.0.1
     Support proxy server port    = 1080
```

Beispiel 2

Mit dem folgenden Befehl wird die Support-Konfiguration angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/config show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:   Support proxy server enabled           = no
     Support proxy server address         =
     Support proxy server port            = 0
     Support proxy user name              =
     Support proxy protocol                = Unknown
     Automatic support contracts update enabled = no
     Cloud management enabled             = no
```

Konfigurieren oder Ändern der Einstellungen für Support und Proxyserver

Ändern Sie die Attribute der Supportkonfiguration.

Format

```
/sys/support/config set [-enableSupportProxy {yes | no}] [-supportProxyAddr <value>]
[-supportProxyPort <value>] [-supportProxyUser <value> {-supportProxyPasswd <value> |-
supportProxyPasswdSecure}] [-supportProxyProtocol {http | socks}] [-autoUpdateContracts {yes |
no}] [-enableCloudMgmt {yes | no}]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-enableSupportProxy	Gibt an, ob der Proxyserver aktiviert oder deaktiviert werden soll. Gültige Werte:

Qualifizierer	Beschreibung
	<ul style="list-style-type: none"> • yes • no
-supportProxyAddr	Geben Sie den Namen oder die IP-Adresse des Support-Services-Proxyservers an.
-supportProxyPort	Geben Sie den Port des Support-Services-Proxyservers an.
-supportProxyUser	Geben Sie den Benutzernamen eines Kontos auf dem Support-Services-Proxyserver an.
-supportProxyPasswd	Geben Sie das Passwort für das Konto des Support-Services-Proxyservers an.
-supportProxyPasswdSecure	Gibt das Passwort im sicheren Modus an – der Benutzer wird aufgefordert, das Passwort einzugeben.
-supportProxyProtocol	Geben Sie für die Kommunikation mit dem Support-Services-Proxyserver das verwendete Protokoll an. Gültige Werte: <ul style="list-style-type: none"> • http • socks <i>i</i> ANMERKUNG: Bei den Werten wird zwischen Groß- und Kleinschreibung unterschieden.
-autoUpdateContracts	Geben Sie an, ob das System seine Serviceverträge automatisch einmal pro Woche aktualisiert. Gültige Werte: <ul style="list-style-type: none"> • yes • no <i>i</i> ANMERKUNG: Bei den Werten wird zwischen Groß- und Kleinschreibung unterschieden.
-enableCloudMgmt	Geben Sie an, ob das Senden von Daten an CloudIQ auf dem System aktiviert ist. Gültige Werte: <ul style="list-style-type: none"> • yes • no <i>i</i> ANMERKUNG: Bei den Werten wird zwischen Groß- und Kleinschreibung unterschieden.

Beispiel

Mit dem folgenden Befehl können Sie die Parameter des Supportservices-Proxyservers angeben:

```
uemcli /sys/support/config set -supportProxyAddr 10.0.0.1 -supportProxyPort 8080
-supportProxyUser user1 -supportProxyPasswd password123 -supportProxyProtocol http
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
Operation completed successfully.
```

Managen von Supportverträgen

Managen Sie Supportverträge im System.

In der folgenden Tabelle sind die Attribute der Supportverträge aufgeführt:

Tabelle 12. Attribute von Supportverträgen

Merkmale	Beschreibung
ID	Kennung des Supportvertrags.
Status	Status des Supportvertrags. Folgende Werte sind möglich: <ul style="list-style-type: none"> • active • about to expire

Tabelle 12. Attribute von Supportverträgen (fortgesetzt)

Merkmale	Beschreibung
	<ul style="list-style-type: none">• expired
Service type	Typ des Supportvertrags.
Start date	Startdatum des Supportvertrags.
Expiration date	Ablaufdatum des Supportvertrags.

Anzeigen von Supportverträgen

Zeigen Sie die verfügbaren Supportverträge an.

Format

```
/sys/support/contract [-id <value>] show
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-id	Identifiziert die Supportverträge

Beispiel

Mit dem folgenden Befehl werden die Supportverträge angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/contract show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1: ID           = contract1
   Status       = active
   Service type = software
   Expiration date = 2012/12/31
```

Aktualisieren von Supportverträgen

Aktualisieren Sie die Liste von Supportverträgen von einem Supportserver.

Format

```
/sys/support/contract refresh
```

Beispiel

Mit dem folgenden Befehl werden die Supportverträge angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/contract refresh
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

Operation completed successfully.

Managen von Centralized ESRS

ANMERKUNG: Das Management von Centralized ESRS ist nur für UnityVSA-Version 5.3 oder höher relevant. Centralized ESRS wird in physischen Bereitstellungen mit Unity-Betriebsumgebung (OE) Version 5.3 oder höher nicht unterstützt.

Centralized ESRS werden auf einem Gatewayserver ausgeführt. Wenn Sie diese Option auswählen, wird Ihr Speichersystem zu anderen Speichersystemen in einem ESRS-Cluster hinzugefügt. Das Cluster befindet sich hinter einer einzigen, gemeinsamen, (zentralen) sicheren Verbindung zwischen den EMC Servern und einem arrayexternen ESRS Gateway. Das ESRS Gateway ist der zentrale Eingangs- und Ausgangspunkt für alle IP-basierten ESRS-Aktivitäten für die Storage-Systeme, die mit dem Gateway verknüpft sind.

Das ESRS Gateway ist eine Lösung für Remotesupport, die auf einem oder mehreren vom Kunden bereitgestellten dedizierten Servern installiert ist. Das ESRS Gateway fungiert als Kommunikations-Broker zwischen den damit verbundenen Speichersystemen, dem Policy-Manager und den Proxy-Servern (optional) sowie EMC. Verbindungen zum Policy Manager und zu zugehörigen Proxyservern werden über die ESRS Gateway-Schnittstelle konfiguriert, ebenso wie das Hinzufügen (Registrieren), Ändern, Löschen (Aufheben der Registrierung) und Abfragen von Statusfunktionen, die ESRS-Clients verwenden können, um sich beim ESRS Gateway zu registrieren.

ANMERKUNG: Bevor Centralized ESRS verwendet werden kann, müssen gültige Supportanmeldedaten angegeben werden.

In der folgenden Tabelle sind die Attribute für Centralized ESRS aufgelistet:

Tabelle 13. Attribute für Centralized ESRS

Merkmale	Beschreibung
Enabled	Gibt an, ob der Centralized ESRS-Service aktiviert ist. Gültige Werte: <ul style="list-style-type: none">• yes• no
Address	Gibt die IP-Adresse des Centralized ESRS-Servers an.
Port	Gibt die Portnummer des Centralized ESRS-Servers an.
Secondary Address	Gibt die IP-Adresse des sekundären Centralized ESRS-Servers an.
Secondary Port	Gibt die Portnummer des sekundären Centralized ESRS-Servers an.

Anzeigen der Centralized ESRS-Konfiguration

Zeigen Sie Details zur Centralized ESRS-Konfiguration an.

Format

```
/sys/support/esrsc show
```

Beispiel

Mit dem folgenden Befehl wird die Centralized ESRS-Konfiguration angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/esrsc show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:   Enabled           = yes
     Address          = 10.10.10.123
     Port             = 9443
```

```
Secondary Address = 10.10.10.124
Secondary Port    = 9443
```

Aktivieren oder Ändern von Centralized ESRS

Aktivieren oder ändern Sie die Konfiguration von Centralized ESRS.

Format

```
/sys/support/esrsc set -enable { yes | no } [ -address <value> ] [ -port <value>] [-secondAddress <value>] [-secondPort <value>]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-enable	Gibt an, ob Centralized ESRS aktiviert oder deaktiviert werden soll. Gültige Werte: <ul style="list-style-type: none">• yes• no  ANMERKUNG: Wenn ESRS deaktiviert ist, können andere Parameter nicht geändert werden.
-address	Gibt die IP-Adresse des Centralized ESRS VE-Servers an, mit dem die Verbindung hergestellt wird.
-port	Gibt die Nummer des Ports an, der für eine Verbindung zum Centralized ESRS verwendet wird.
-secondAddress	Geben Sie den Netzwerknamen oder die IP-Adresse des sekundären Centralized ESRS VE-Servers an.
-secondPort	Geben Sie die Nummer des Ports an, der für eine Verbindung zum primären Centralized ESRS VE-Server verwendet wird.  ANMERKUNG: Das sekundäre Gateway muss sich im selben Cluster wie der primäre Gateway befinden.

Beispiel 1

Der folgende Befehl spezifiziert die Parameter des Centralized ESRS:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/esrsc set -enable yes -address 10.10.22.22
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

Operation completed successfully.

Beispiel 2

Im folgenden Beispiel wird die Centralized ESRS VE mit einem sekundären Gateway für hohe Verfügbarkeit konfiguriert.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/esrsc set -enable yes -address 10.10.22.22 -secondAddress 10.10.22.32
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

Operation completed successfully.

Prüfen der Netzwerkverbindung von Centralized ESRS

Prüfen Sie die Netzwerkverbindung von Centralized ESRS, bevor Sie ESRS konfigurieren.

Prüfen Sie die Netzwerkverbindung von Centralized ESRS zu den Dell Servern. Wenn ein Fehler auftritt, kann Centralized ESRS nicht aktiviert werden.

Format

```
/sys/support/esrsc checkNetwork -address <value> [-port <value>]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-address	Geben Sie die IP-Adresse von Centralized ESRS VE ein.
-port	Geben Sie die Portnummer für Centralized ESRS VE ein.

Beispiel

Dieses Beispiel zeigt, wann die Prüfung der Netzwerkverbindung für Centralized ESRS fehlschlägt.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/esrsc checkNetwork -address 10.100.10.7
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection
```

```
Operation failed. Error code: 0x6400be8
```

```
The centralized ESRS network connectivity check failed. Please check your firewall configuration and whether the centralized ESRS server is operating normally. (Error Code:0x6400be8)
```

Testen des Centralized EMC Secure Remote Support

Wenn Centralized EMC Secure Remote Support bereits konfiguriert wurde, können Sie mit diesem Befehl die Verbindung zwischen Ihrem System und der EMC Secure Remote Support-Datenbank testen. Mit dem Befehl `checkNetwork` wird die Konnektivität Ihres lokalen Netzwerks geprüft und mit dem Befehl `test` die Verbindung zurück zu Dell.

Format

```
/sys/support/esrsc test
```

Beispiel 1

Das folgende Beispiel zeigt die Ergebnisse der Ausführung dieses Befehls, wenn Centralized EMC Secure Remote Support noch nicht konfiguriert wurde.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/esrsc test
```

```
Operation failed. Error code: 0x6400c06  
Not supported since Centralized Secure Remote Support is not enabled. (Error Code:0x6400c06)
```

Beispiel 2

Das folgende Beispiel zeigt die erfolgreiche Ausführung dieses Befehls.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/esrsc test
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection  
  
Operation completed successfully.
```

ANMERKUNG: Ein erfolgreicher Vorgang weist darauf hin, dass der Test erfolgreich durchgeführt wurde und nicht, dass die Verbindung selbst erfolgreich war. Anders gesagt: Es wird darauf hingewiesen, dass CallHome gesendet wurde, aber nicht, ob es vom EMC Secure Remote Support-Server empfangen wurde. Zum Prüfen des Status des tatsächlichen Tests melden Sie sich bei Service 360 an, um die aktuellen Service-Requests (SRs) einzusehen. Wenn CallHome vom EMC Secure Remote Support-Server empfangen wurde, wird der Verbindungstest als automatisch geschlossener CallHome-SR angezeigt.

Managen von SupportAssist (nur physische Bereitstellungen)

ANMERKUNG: Diese Funktion ist in Ihrer Implementierung möglicherweise nicht verfügbar. SupportAssist wird auf UnityVSA nicht unterstützt und das zentralisierte ESRS-Verhalten auf UnityVSA bleibt mit der Unity-Betriebsumgebungsversion 5.2 oder früher identisch. Verwenden Sie in diesem Fall den Befehl `/sys/support/esrsc`, um die zentralisierten ESRS zu managen.

SupportAssist ist eine Remoteüberwachungs- und -Supportfunktion, die autorisierten Mitarbeitern Remotezugriffsfunktionen von DELL auf Stagesysteme über einen sicheren und verschlüsselten Tunnel bereitstellt. Der sichere Tunnel, den SupportAssist zwischen dem Stagesystem und den Systemen im DELL Netzwerk herstellt, ermöglicht es dem Stagesystem, direkt mit dem DELL Supportservice zu kommunizieren.

Die Option `set -acceptEula` sollte der erste Befehl sein, der ausgeführt wird, wenn SupportAssist zum ersten Mal aktiviert wird, und er muss nur einmal ausgeführt werden. Wenn die EULA nicht akzeptiert wird, kann SupportAssist nicht aktiviert werden. Sobald die EULA akzeptiert wurde, kann der `checkNetwork`-Befehl jederzeit ausgeführt werden und prüft die Netzwerkverbindung zwischen Unity und dem Supportservice.

ANMERKUNG: Nachdem SupportAssist aktiviert ist, bleiben die Eigenschaften `EULA accepted` und `Initialized` auf `yes` eingestellt, unabhängig davon, ob die NutzerInnen die SupportAssist-Einstellungen ändern oder SupportAssist sogar deaktivieren. Außerdem sollte der Befehl `checkNetwork` nach dem Aktivieren von SupportAssist und vor dem Ausführen des `set`-Befehls erneut ausgeführt werden, um Änderungen an der SupportAssist-Konfiguration vorzunehmen. Stellen Sie sicher, dass dieselben Parameter, die im `set`-Befehl angegeben sind, auch im `checkNetwork`-Befehl angegeben sind und dass die Netzwerkprüfung erfolgreich ist.

Auf einem neuen Unity-Stagesystem der Version 5.3 lautet der Standardstatus `initialized = yes`. Der `initialize`-Befehl ist nur dann auszuführen, wenn die `show`-Ausgabe `initialized = no` anzeigt. Beispiel: Wenn ESRS vor dem Upgrade eines Unity-Stagesystems von Version 5.2 oder früher auf Unity-Version 5.3 nicht aktiviert ist und nach dem Upgrade nicht versucht wurde, SupportAssist zu aktivieren, sollte der Standardstatus `initialized = no` angezeigt werden. Erzeugen Sie vor dem Ausführen des `initialize`-Befehls einen Zugriffsschlüssel, der von der Seriennummer des Systems und einer nutzerdefinierten 4-stelligen PIN abgeleitet ist, auf der Produktsupportseite der Dell Website. Der generierte Zugriffsschlüssel und die PIN müssen im `initialize`-Befehl enthalten sein.

`set -connectionType`, `set -enableRemoteAccess` und `set -rscEnabled` werden verwendet, um einen anderen Verbindungstyp anzugeben. Wenn Sie für den Verbindungstyp die direkte oder Gateway-Verbindung festlegen, wird SupportAssist aktiviert. Die Aktivierung des Remotezugriffs ermöglicht sowohl ausgehenden Netzwerkverkehr zu als auch eingehenden Netzwerkverkehr vom Dell Support. Das Deaktivieren des Remotezugriffs erlaubt nur ausgehenden Datenverkehr an den Dell Support. Remote Secure Credentials (RSC) ermöglicht es autorisierten Dell Servicemitarbeitern, sich bei einem System zu authentifizieren, ohne zuvor ein Kennwort mit dem Eigentümer der Appliance zu vereinbaren. Wenn RSC aktiviert ist, meldet sich ein Supportmitarbeiter bei Unity mit einem dynamischen RSA-Passcode von einem streng kontrollierten Back-end-Portal an. Der RSC-Passcode ist ein Einmal-Passcode, der nach einem bestimmten Zeitraum abläuft. Für jede RSC-Anmeldung und -Abmeldung zu Auditzwecken wird ein Auditprotokoll aufbewahrt. Um RSC zu aktivieren, müssen die folgenden Bedingungen erfüllt sein:

- Die SupportAssist-EULA ist akzeptiert.
- Die Netzwerkprüfung ist erfolgreich.

- SupportAssist ist initialisiert.
- Der Remotezugriff ist aktiviert.

Der `Testcallhome`-Befehl kann erst verwendet werden, nachdem SupportAssist aktiviert wurde und getestet hat, ob die SupportAssist CallHome-Funktion funktioniert.

In der folgenden Tabelle sind die Attribute für SupportAssist aufgeführt.

Tabelle 14. SupportAssist-Attribute

Attribut	Beschreibung
Connection type	Gibt an, wie Unity eine Verbindung zum Supportservice herstellt. Gültige Werte: <ul style="list-style-type: none"> • Disabled - Remote-Verbindungsservice ist auf dem Stagesystem deaktiviert • Direct - Direkte Verbindung zum Supportservice • Gateway - Herstellen einer Verbindung zum Supportservice über das Gateway (sicheres Verbindungsgateway Version 5.12.00.10 oder höher)
Primary gateway	Zeigt die Netzwerkinformationen des primären Gateways an.
Secondary gateway	Zeigt die Netzwerkinformationen des sekundären Gateways an.
Remote access enabled	Zeigt an, ob der Remotezugriff aktiviert ist. Gültige Werte: <ul style="list-style-type: none"> • yes • no
RSC enabled	Gibt an, ob RSC (Remote Secure Credential) aktiviert ist. RSC ermöglicht Ihrem Serviceanbieter den Zugriff auf das Stagesystem mit sicheren Remote-Anmeldedaten. Gültige Werte: <ul style="list-style-type: none"> • yes • no
Status	Zeigt den SupportAssist-Konnektivitätsstatus an.
EULA accepted	Gibt an, ob die SupportAssist-Endnutzer-Lizenzvereinbarung (EULA) akzeptiert wurde. Gültige Werte: <ul style="list-style-type: none"> • yes • no <p> ANMERKUNG: Wenn die EULA nicht akzeptiert wird, kann SupportAssist auch nicht konfiguriert werden.</p>
Initialized	Gibt an, ob SupportAssist initialisiert ist. Gültige Werte: <ul style="list-style-type: none"> • yes • no
Follow support proxy	Gibt an, ob der in der Supportkonfiguration (<code>/sys/support/config</code>) definierte Proxyserver verwendet werden soll, wenn er aktiviert ist. Gültige Werte: <ul style="list-style-type: none"> • yes • no (Standardwert)

Anzeigen der SupportAssist-Konfiguration

Zeigen Sie Details zur SupportAssist-Konfiguration an.

Format

```
/sys/support/assist show
```

Beispiel

Mit dem folgenden Befehl wird die SupportAssist-Konfiguration angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/assist show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      Connection type           = Gateway
        Primary gateway          = 10.123.45.67:9443
        Secondary gateway        = 10.123.45.68:9443
        Remote Access enabled    = yes
        RSC enabled              = no
        Status                   = OK
        EULA accepted            = yes
        Initialized               = yes
        Follow support proxy      = no
```

Initialisieren von SupportAssist

ANMERKUNG: Dieser Befehl gilt nur, wenn SupportAssist nicht initialisiert ist. Normalerweise wird dieser Befehl verwendet, wenn das Unity-System von einer früheren Version auf Version 5.3.0 oder höher aktualisiert wird und EMC Secure Remote Service deaktiviert ist.

Der Befehl wird verwendet, um SupportAssist über den Dell Supportservice zu initialisieren. NutzerInnen müssen den Zugriffsschlüssel auf der Produktsupportseite der Dell Website generieren. Der Schlüssel wird aus der aktuellen Unity-Systemseriennummer und einer 4-stelligen PIN erzeugt, die der/die NutzerIn angibt. Der/die NutzerIn muss den generierten Zugriffsschlüssel und die zugehörige nutzerdefinierte PIN in diesen Befehl aufnehmen. Der/die NutzerIn kann über **Support > Produktportal > Unity-Portal** in Unisphere auf die Produktsupportseite zugreifen. Wenn Gateway-Informationen bereitgestellt werden, stellt der Befehl eine Verbindung zu Dell über ein sicheres Verbindungsgateway der Version 5.12.00.10 oder höher her. Andernfalls wird eine direkte Verbindung zu Dell hergestellt.

Format

```
/sys/support/assist initialize -accessKey <value> -pin <value> [-primaryGwAddr <value> [-primaryGwPort <value>] [-secondaryGwAddr <value> [-secondaryGwPort <value>]]]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-accessKey	Gibt den Zugriffsschlüssel für SupportAssist an. Ein gültiger Wert ist eine 8-Bit-ASCII-Zeichenfolge aus Zahlen und Buchstaben. ANMERKUNG: Der Zugriffsschlüssel kann von der Produktsupportseite auf der Dell Website generiert werden. Sie können die Seite von Support > Produktportal > Unity-Portal in Unisphere aus aufrufen.
-pin	Gibt die vom Nutzer/von der Nutzerin beim Generieren des Zugriffsschlüssels eingegebene zufällige, nutzerdefinierte vierstellige Zahl an.
-primaryGwAddr	Gibt die Netzwerkadresse des primären Gateways an.
-primaryGwPort	Gibt den Netzwerkport des primären Gateways an. Der Standardwert ist 9443.
-secondaryGwAddr	Gibt die Netzwerkadresse des sekundären Gateways an.
-secondaryGwPort	Gibt den Netzwerkport des sekundären Gateways an. Der Standardwert ist 9443.

Beispiel 1

Das folgende Beispiel zeigt die Ergebnisse der Ausführung dieses Befehls, wenn keine Gateway-Informationen bereitgestellt wurden:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/assist initialize -accessKey 123a456b -pin 2021
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection  
  
Operation completed successfully.
```

Beispiel 2

Der folgende Befehl zeigt die Ergebnisse der Ausführung dieses Befehls, wenn Gateway-Informationen bereitgestellt wurden:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/assist -accessKey 789c012d -pin 2021 -primaryGwAddr 10.1.2.3
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection  
  
Operation completed successfully.
```

Prüfen der SupportAssist-Netzwerkverbindung

Prüfen Sie die Netzwerkverbindung vom SupportAssist-Client zu den Dell Servern. Wenn ein Fehler auftritt, kann SupportAssist nicht aktiviert werden.

 **ANMERKUNG:** Sobald die EULA akzeptiert wurde, kann dieser Befehl jederzeit ausgeführt werden.

Format

```
/sys/support/assist checkNetwork
```

Beispiel 1

Das folgende Beispiel zeigt die erfolgreiche Ausführung dieses Befehls.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/assist checkNetwork -remoteAccess no -connectionType direct -followProxy no
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection  
  
Operation completed successfully.
```

Beispiel 2

Mit dem folgenden Befehl werden die Ergebnisse der Ausführung dieses Befehls angezeigt, wenn vor der Aktivierung von SupportAssist kein DNS-Server konfiguriert wurde:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/assist checkNetwork -remoteAccess no -connectionType direct -followProxy no
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection  
  
Operation failed. Error code: 0x6400c27
```

DNS server is not configured. Please config dns server before enabling Support Assist.
(Error Code:0x6400c27)

Ändern von SupportAssist

Ändern Sie die SupportAssist-Konfiguration.

Format

```
/sys/support/assist set [-acceptEula yes][-connectionType {direct|gateway|disabled}][-enableRemoteAccess {yes|no}][-primaryGwAddr <value> [-primaryGwPort <value>][-secondaryGwAddr <value> [-secondaryGwPort <value>]]][-enable Rsc {yes|no}][-followProxy {yes|no}]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-connectionType	Gibt an, wie Unity eine Verbindung zum Supportservice herstellt. Gültige Werte: <ul style="list-style-type: none">• direkt• Gateway• disabled <p> ANMERKUNG: Gateway erfordert das sichere Verbindungsgateway Version 5.12.00.10 oder höher. Wenn gateway angegeben ist, muss die primäre Gatewayadresse einen Wert haben. Der Wert für die sekundäre Gatewayadresse ist optional.</p>
-primaryGwAddr	Gibt die Netzwerkadresse des primären Gateways an.
-primaryGwPort	Gibt den Netzwerkport des primären Gateways an.
-secondaryGwAddr	Gibt die Netzwerkadresse des sekundären Gateways an.
-secondaryGwPort	Gibt den Netzwerkport des sekundären Gateways an.
-enableRemoteAccess	Gibt an, ob der Remotezugriff aktiviert ist. Gültige Werte: <ul style="list-style-type: none">• yes – bidirektionale Verbindung (ausgehende und eingehende; vollständige SupportAssist-Funktionen werden bereitgestellt)• no – einseitige Verbindung (nur ausgehende; nur partielle SupportAssist-Funktionen werden bereitgestellt)
-enableRSC	Gibt an, ob der Remote Secure Credential-Zugriff aktiviert werden soll. Gültige Werte: <ul style="list-style-type: none">• yes• no
-acceptEula	Gibt an, ob die Endnutzer-Lizenzvereinbarung (EULA) von SupportAssist akzeptiert werden soll. Gültige Werte: <ul style="list-style-type: none">• yes• no <p> ANMERKUNG: Wenn die EULA nicht akzeptiert wird, kann SupportAssist auch nicht konfiguriert werden.</p>
-followProxy	Gibt an, ob der in der Supportkonfiguration (/sys/support/config) definierte Proxyserver verwendet werden soll, wenn er aktiviert ist. Gültige Werte: <ul style="list-style-type: none">• yes• no

Beispiel

Mit dem folgenden Befehl wird die EULA akzeptiert, der Verbindungstyp als Gateway festgelegt, der Remotezugriff mit bidirektionaler Verbindung aktiviert, es werden die IP-Adresse und die Portinformationen des primären und sekundären Gateways angegeben und die vorhandenen Proxyservereinstellungen befolgt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/assist set -acceptEula yes
-connectionType gateway -enableRemoteAccess yes -primaryGwAddr 10.1.2.3 -primaryGwPort 9443
-secondaryGwAddr 10.1.2.4 -secondaryGwPort 9443 -followProxy yes
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
Operation completed successfully.
```

SupportAssist CallHome testen

Wenn SupportAssist konfiguriert ist, können Sie mit diesem Befehl die Verbindung zwischen Ihrem System und dem Dell Supportservice testen. Während der Befehl `checkNetwork` die Verbindung zurück zu Dell überprüft, prüft dieser `testcallhome`-Befehl die End-to-End-CallHome-Funktion basierend auf dem sicheren Verbindungskanal.

Format

```
/sys/support/assist testcallhome
```

Beispiel 1

Das folgende Beispiel zeigt die erfolgreiche Ausführung dieses Befehls.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/assist testcallhome
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
Operation completed successfully.
```

i ANMERKUNG: Ein erfolgreicher Vorgang weist darauf hin, dass der Test erfolgreich durchgeführt wurde und nicht, dass die Verbindung selbst erfolgreich war. Anders gesagt: Es wird darauf hingewiesen, dass CallHome gesendet wurde, aber nicht, ob es vom Dell Server empfangen wurde. Zum Prüfen des Status des tatsächlichen Tests melden Sie sich bei Service 360 an, um die aktuellen Service-Requests (SRs) einzusehen. Wenn CallHome vom Dell Server empfangen wurde, wird der Verbindungstest als automatisch geschlossener CallHome-SR angezeigt.

Beispiel 2

Das folgende Beispiel zeigt die Ergebnisse der Ausführung dieses Befehls, wenn SupportAssist nicht aktiviert ist.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/assist testcallhome
```

```
Operation failed. Error code: 0x6400c40
Please enable SupportAssist before testing callhome. (Error Code:0x6400c40)
```

Managen von Connect Home

Konfigurieren Sie Connect Home so, dass Systeminformationen direkt an den Support gesendet werden, wenn kritische Warnmeldungen auftreten.

Connect Home verwendet Simple Mail Transport Protocol (SMTP), um Systeminformationen automatisch per E-Mail an den Support zu senden. Diese E-Mail-Nachrichten enthalten Systemereignis- und Fehlerverläufe, die der Dell Support zur Diagnose und Behebung von Problemen verwenden kann.

Connect Home ist eine Alternative zu SupportAssist/ESRS, bietet aber nur eine unidirektionale Verbindung vom Unity-System zum Support.

Tabelle 15. Connect Home-Attribute

Attribut	Beschreibung
Enabled	Gibt an, ob Connect Home aktiviert ist. Gültige Werte: <ul style="list-style-type: none"> • yes • no
SMTP server	Die IP-Adresse des SMTP-Servers, der für Connect Home konfiguriert ist.
E-mail from address	Die E-Mail-Adresse, von der aus Connect Home-E-Mails an den Support gesendet werden.
E-mail to address	Die Ziel-E-Mail-Adresse, an die Connect Home-E-Mails gesendet werden.

Anzeigen von Connect Home

Mit diesem Befehl werden die Konfigurationseinstellungen für Connect Home angezeigt.

Zeigen Sie die aktuellen Connect Home-Konfigurationseinstellungen an.

Format

```
/sys/support/connecthome show
```

Beispiel

Mit dem folgenden Befehl werden die Konfigurationseinstellungen für Connect Home angezeigt.

```
uemcli -d 10.0.0.1 -u admin -p Password /sys/support/connecthome show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      Enabled           = yes
        SMTP server      = 10.10.10.123
        E-mail from address = bs-xxxx@emc.com
        E-mail to address  = emailalertesg@emc.com
```

Ändern der Connect Home-Konfigurationseinstellungen

Mit diesem Befehl werden die Konfigurationseinstellungen für Connect Home geändert.

Ändern der Konfigurationseinstellungen für Connect Home

Format

```
/sys/support/connecthome set [-enable {yes | no}] [-smtpServer <value>] [-emailFromAddr <value>]
```

Tabelle 16. Aktionsqualifizierer

Qualifizierer	Beschreibung
-enable	Geben Sie an, ob Connect Home aktiviert werden soll. Gültige Werte: <ul style="list-style-type: none"> • yes • no
-smtpServer	Geben Sie die IP-Adresse des SMTP-Servers an, über den Connect Home E-Mails sendet.
-emailFromAddr	Geben Sie die E-Mail-Adresse an, von der aus Connect Home-E-Mails an den Support gesendet werden. Wenn nicht angegeben, wird ein Standardwert formatiert als <arrayname>@emc.com verwendet. <p>i ANMERKUNG: Ab Unity OE 5.3 sind Connect Home-Konnektivitätsbenachrichtigungen mit <serialNumber>@emc.com nicht mehr die Standardeinstellung. Bei der Konfiguration der Connect Home-Konnektivität müssen Sie eine E-Mail-Adresse mit dem Domainnamen Ihres Systems angeben oder eine E-Mail-Adresse, die die Authentifizierung von Ihrem eigenen SMTP-Server weiterleiten kann.</p>

Beispiel

In diesem Beispiel wird Connect Home aktiviert und festgelegt, dass es SMTP-Server 10.10.22.22 verwendet.

```
uemcli -d 10.0.0.1 -u local/joe -p Password /sys/support/connecthome set -enable yes -smtpServer 10.10.22.22
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Testen von Connect Home

Mit diesem Befehl wird eine erfolgreiche Übertragung von Warnmeldungen per E-Mail mit Connect Home getestet.

Testen Sie, ob Connect Home erfolgreich eine E-Mail-Warnmeldung an den Support mithilfe des angegebenen SMTP-Servers senden kann.

Format

```
/sys/support/connecthome test
```

Beispiel

Dieses Beispiel zeigt die Ergebnisse einer Test-E-Mail-Warnmeldung mit den angegebenen Connect Home-Konfigurationseinstellungen.

```
uemcli -d 10.0.0.1 -u local/joe -p Password /sys/support/connecthome test
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Managen von Benutzerrollen

Sie können die unterstützten Benutzerrollen im System sowie die Arten von Aktionen anzeigen lassen, die die Benutzer ausführen können.

In der folgenden Tabelle sind die Attribute für Benutzerrollen aufgeführt:

Tabelle 17. Attribute der Benutzerrollen

Merkmale	Beschreibung
Name	<p>Der Name der Benutzerrolle. Folgende Werte sind möglich:</p> <ul style="list-style-type: none"> • <code>administrator</code>: Administratorrolle: Administratoren können Systemdaten anzeigen, Systemeinstellungen ändern und sämtliche wichtigen Administrationsfunktionen ausführen. • <code>storageadmin</code>: Speicheradministratorrolle: Speicheradministratoren können Systemdaten anzeigen und Einstellungen ändern. Speicheradministratoren können keine Benutzerkonten oder Hostkonfigurationen hinzufügen, keine anfängliche Systemkonfiguration vornehmen, keine Netzwerkeinstellungen ändern, keine NAS-Server erstellen oder löschen und keine Upgrades von Systemsoftware vornehmen. • <code>operator</code> : Operatorrolle: Die Bediener können System- und Speicherinformationen anzeigen, aber keine Systemeinstellungen ändern. Für diese Rolle gelten lediglich Anzeigerechte. • <code>securityadministrator</code>: Rolle des Sicherheitsadministrators: System- und Speicherstatusinformationen können angezeigt werden, aber nur sicherheitsbezogene Aufgaben können ausgeführt werden. Nicht alle Vorgänge können ausgeführt werden. • <code>vmadmin</code>: VMware-Administratorrolle: Wird nur verwendet, um das System als VASA-Anbieter in vCenter hinzuzufügen.
Description	Kurze Beschreibung der Benutzerrolle.

Anzeigen von Benutzerrollen

Zeigen Sie eine Liste mit Rollen an, die Sie den Benutzern zuweisen können. Sie können eine Filterung nach dem Rollennamen durchführen.

Format

```
/user/role [-name <value>] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-name	<p>Geben Sie den Namen der Benutzerrolle ein. Folgende Werte sind möglich:</p> <ul style="list-style-type: none"> • <code>administrator</code>: Administratorrolle • <code>storageadmin</code> : Speicheradministratorrolle • <code>operator</code>: Operatorrolle (nur Ansicht) • <code>securityadministrator</code>: Rolle des Sicherheitsadministrators • <code>vmadmin</code>: VMware Administrator (nur verwendet, um das System als VASA-Anbieter in vCenter zu registrieren)

Beispiel

Mit dem folgenden Befehl wird eine Liste der Benutzerrollen im System angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /user/role show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```

1:   Name      = administrator
    Description = User is allowed to perform security tasks.

2:   Name      = storageadmin
    Description = User has access to all administrative and management interfaces and
data.

3:   Name      = operator
    Description = User is allowed to see all storage system data but not to perform any
storage management operations.

4:   Name      = securityadministrator
    Description = User is allowed only to perform security tasks and is able to see all
storage system data, but cannot perform any operations.

5:   Name      = vmadmin
    Description = Can only be used to establish a VASA connection from vCenter to the
storage system.

```

Managen von Benutzerkonten

Steuern Sie den Benutzerzugriff auf das System und die Funktionen, indem Sie Benutzerkonten für die einzelnen Manager bzw. Administratoren erstellen, die das System konfigurieren und überwachen müssen. Die Konten mit eindeutigen Benutzernamen und Passwort stehen für eine bestimmte Rolle und Aufgabe. Wenn Benutzer sich beim System über die CLI oder die Unisphere-Benutzeroberfläche anmelden, fordert das System sie auf, ihren Benutzernamen und ihr Passwort einzugeben, um Zugriff zu erhalten.

Tabelle 18. Attribute von Benutzerkonten

Merkmale	Beschreibung
ID	Kennung des Benutzerkontos.
Name	Kontoname.
Role	Geben Sie den Rollentyp für das Benutzerkonto ein.
Type	Der Kontotyp (Umfang). Mögliche Werte sind: <ul style="list-style-type: none"> • local • ldapuser • ldapgroup
Password	Passwort für das lokale Konto.
Password expiration status	Informationen zum Ablauf des Passworts. Mögliche Werte sind: <ul style="list-style-type: none"> • <code><value> days remaining</code> • Expired • Ein leerer Wert, was bedeutet, dass das Passwort für dieses Benutzerkonto nicht abläuft. Beispiel: Benutzerkonten mit dem type ldapuser oder ldapgroup.

Erstellen eines Benutzerkontos

Legen Sie ein Konto für einen Benutzer oder eine Benutzergruppe an, und weisen Sie dem Konto eine Rolle zu. Die Berechtigungen der Benutzer hängen von der Rolle ab. Die Benutzer können lokal beim System angemeldet sein oder über LDAP authentifiziert werden. Benutzergruppen können nur über LDAP authentifiziert werden.

Die einzelnen Benutzerkonten erhalten eigene IDs.

Format

```

/user/account create -name <value> -type {local {-passwd <value> | -passwdSecure} | ldapuser |
ldapgroup} -role <value>

```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-name	Geben Sie einen Namen für das Konto ein. Geben Sie für LDAP-Nutzer und -Gruppen nur den Nutzernamen an, ohne den Domainnamen zu berücksichtigen. Beim LDAP-Nutzer- oder Gruppennamen muss die Groß-/ Kleinschreibung beachtet werden. Verwenden Sie die gleiche Groß-/Kleinschreibung wie im LDAP-Server für den LDAP-Nutzer/die LDAP-Gruppe angegeben.  ANMERKUNG: .
-type	Geben Sie den Benutzer- bzw. Benutzergruppentyp ein. Folgende Werte sind möglich: <ul style="list-style-type: none">• local: Lokaler Nutzer.• ldapuser: Nutzer hat ein LDAP-Konto.• ldapgroup : Gruppe hat ein LDAP-Konto.
-passwd	Geben Sie bei lokalen Benutzern das Benutzerpasswort ein. Für Benutzerkonten gelten die folgenden Passwortanforderungen: <ul style="list-style-type: none">• Die Kennwörter müssen zwischen 8 und 40 Zeichen lang sein und Leerzeichen sind nicht zulässig.• Das Kennwort muss mindestens einen Großbuchstaben, einen Kleinbuchstaben und eine Zahl enthalten.• Kennwörter dürfen keine einfachen Anführungszeichen (') oder Et-Zeichen (&) enthalten.• Beim Wechsel des Kennworts darf nicht auf die drei unmittelbar zuvor verwendeten Kennwörter zurückgegriffen werden.
-passwdSecure	Gibt das Kennwort im sicheren Modus an – der Nutzer wird aufgefordert, das Kennwort und die Kennwortbestätigung einzugeben.
-role	Geben Sie den Namen der Rolle für das Konto ein. Folgende Werte sind möglich: <ul style="list-style-type: none">• administrator: Administrator• storageadmin: Speicheradministrator• operator: Operator (nur Ansicht)• securityadministrator: Sicherheitsadministrator• vmadmin: VMware-Administrator Der Befehl <code>/user/role show -detail</code> gibt eine Liste aller verfügbaren Nutzerrollen aus. Attribute der Nutzerrollen enthält eine detaillierte Beschreibung der einzelnen Nutzerrollen.

Beispiel

Mit dem folgenden Befehl wird ein Benutzerkonto angelegt, mit dem user1 als lokalem Benutzer die Rolle des Bedieners zugewiesen wird.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /user/account create -name user1 -type local -passwd Password987! -role operator
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = user_user1
Operation completed successfully.
```

Anzeigen von Benutzerkonten

Zeigen Sie eine Liste der Benutzerkonten an. Sie können nach Konto-ID filtern.

Format

```
/user/account [-id <value>] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID eines Benutzerkontos ein.

Beispiel

Mit dem folgenden Befehl wird eine Liste aller Benutzerkonten im System angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /user/account show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:   ID    = user_user1
     Name = user1
     Role = administrator
     Type = local

2:   ID    = ldapuser_ldapdomain.com/ldapUser
     Name = ldapdomain.com/ldapUser
     Role = operator
     Type = ldapuser

3:   ID    = ldapgroup_ldapdomain.com/ldapGroup
     Name = ldapdomain.com/ldapGroup
     Role = storagadmin
     Type = ldapgroup
```

Ändern von Benutzerkonten

Aktualisieren Sie ein Benutzerkonto anhand der neuen Einstellungen.

Format

```
/user/account -id <value> set [ {-passwd <value> | -passwdSecure} { {-oldpasswd <value> |
-oldpasswdSecure} | -force}] [ -role <value>] [-locked {yes | no}]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des zu ändernden Benutzerkontos ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-passwd	Geben Sie bei lokalen Benutzern das Benutzerpasswort ein. Für Benutzerkonten gelten die folgenden Passwortanforderungen: <ul style="list-style-type: none">• Die Kennwörter müssen zwischen 8 und 40 Zeichen lang sein und Leerzeichen sind nicht zulässig.• Das Kennwort muss mindestens einen Großbuchstaben, einen Kleinbuchstaben und eine Zahl enthalten.• Kennwörter dürfen keine einfachen Anführungszeichen (') oder Et-Zeichen (&) enthalten.• Beim Wechsel des Kennworts darf nicht auf die drei unmittelbar zuvor verwendeten Kennwörter zurückgegriffen werden.

Qualifizierer	Beschreibung
-passwdSecure	Gibt ein Passwort im sicheren Modus an. Der Benutzer wird aufgefordert, das Passwort einzugeben und zu bestätigen.
-oldpasswd	Geben Sie das alte Passwort ein, damit Sie das neue Passwort festlegen können.
-oldpasswdSecure	Gibt ein Passwort im sicheren Modus an. Der Nutzer wird aufgefordert, das Kennwort anzugeben.
-force	Hiermit wird das Passwort zurückgesetzt.  ANMERKUNG: Dieser Qualifizierer kann nur von Administratoren verwendet werden.
-role	Geben Sie den Namen der Rolle für das Konto ein. Folgende Werte sind möglich: <ul style="list-style-type: none"> • administrator: Administrator • storageadmin: Speicheradministrator • operator: Operator (nur Ansicht) • securityadministrator: Sicherheitsadministrator • vmadmin: VMware-Administrator Der Befehl <code>/user/role show -detail</code> gibt eine Liste aller verfügbaren Nutzerrollen aus. Attribute der Benutzerrollen bietet eine Beschreibung jeder einzelnen Benutzerrolle.
-locked	Gibt an, ob das Benutzerkonto gesperrt oder entsperrt werden soll. Gültige Werte: <ul style="list-style-type: none"> • yessperrt das Benutzerkonto. • noentsperrt das Benutzerkonto.  ANMERKUNG: Diese Option kann nur von Benutzern festgelegt werden, die die Administrator- oder Sicherheitsadministrator-Rolle haben, und auch nur auf STIG-fähigen Systemen.

Beispiel

Mit dem folgenden Befehl wird das Kennwort für das Nutzerkonto `user_user1` geändert:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /user/account -id user_user1 set -passwd NewPassword456! -oldpasswd OldPassword456!
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = user_user1
Operation completed successfully.
```

Löschen von Benutzerkonten

Löschen Sie ein Benutzerkonto.

Format

```
/user/account -id <value> delete
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des zu löschenden Benutzerkontos ein.

Beispiel

Mit dem folgenden Befehl wird das Benutzerkonto „user_user1“ gelöscht:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /user/account -id user_user1 delete
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully
```

Verwalten von Benutzerkontoeinstellungen

Sie können detaillierte Kontoeinstellungen für die Benutzer im System verwalten.

 **ANMERKUNG:** Dieser Befehl ist nur für STIG-fähige Systeme verfügbar.

Tabelle 19. Attribute der Benutzerkontoeinstellungen

Merkmale	Beschreibung
Enabled	<p>Gibt an, ob die Funktion für die Nutzerkontoeinstellungen aktiviert ist. Mögliche Werte sind:</p> <ul style="list-style-type: none">• yes• no <p> ANMERKUNG: Wenn der Wert <code>yes</code> ist, aber keine detaillierten Kontoeinstellungen angegeben sind, wird der „Default enabled value“, wie unten angegeben, für jede Einstellung verwendet.</p> <p>Wenn dieser Wert <code>no</code> ist, wird der „Disabled value“ für jede Einstellung verwendet.</p>
Password minimum size	<p>Gibt eine Mindestanzahl von Zeichen für das Kennwort ein. Der gültige Wertebereich ist 8–64. Die Standardwerte sind:</p> <ul style="list-style-type: none">• Standardwert bei Aktivierung: 15• Wert bei Deaktivierung: 8
Number of previous passwords	<p>Gibt die Anzahl der vergangenen Passwörter an, die nicht wiederverwendet werden dürfen, bis der Zyklus zurückgesetzt wurde. Der gültige Wertebereich ist 3–12. Die Standardwerte sind:</p> <ul style="list-style-type: none">• Standardwert bei Aktivierung: 5• Wert bei Deaktivierung: 3
Password period	<p>Der Zeitraum (in Tagen), bis ein Passwort abläuft. Der gültige Wertebereich ist 1–180 Tage. Ein leerer Wert gibt an, dass das Kennwort nie abläuft. Die Standardwerte sind:</p> <ul style="list-style-type: none">• Standardwert bei Aktivierung: 60• Wert bei Deaktivierung: kein Ablaufdatum (leer)
Maximum failed logins	<p>Die Anzahl der aufeinanderfolgenden fehlgeschlagenen Anmeldeversuche, die innerhalb des unter „failed login period“ angegebenen Zeitraums zulässig sind, bis das Konto gesperrt wird. Ein leerer Wert gibt an, dass keine Begrenzung festgelegt ist. Der gültige Wertebereich ist 1–10. Die Standardwerte sind:</p> <ul style="list-style-type: none">• Standardwert bei Aktivierung: 3• Wert bei Deaktivierung: unbegrenzt (leer)

Tabelle 19. Attribute der Benutzerkontoeinstellungen (fortgesetzt)

Merkmale	Beschreibung
	<p> ANMERKUNG: Maximum failed logins, Failed login period und Account lockout period müssen entweder alle leer sein oder alle einen Wert enthalten.</p>
Failed login period	<p>Der Zeitraum (in Sekunden), in dem höchstens die unter „Maximum failed logins“ angegebenen Anmeldeversuche auftreten dürfen, da es ansonsten zu einer Kontosperrung kommt. Der gültige Wertebereich ist 1–3600 Sekunden. Ein leerer Wert gibt an, dass es keinen Zeitraum für die Zählung von fehlgeschlagenen Anmeldeversuchen gibt. Die Standardwerte sind:</p> <ul style="list-style-type: none"> • Standardwert bei Aktivierung: 900 • Wert bei Deaktivierung: kein Zeitraum für die Zählung von fehlgeschlagenen Anmeldeversuchen (leer) <p>Wenn die maximal möglichen fehlgeschlagenen Anmeldeversuche nicht während des unter Failed login period angegebenen Zeitraums aufgetreten sind, wird der Zähler für Maximum failed logins zurückgesetzt.</p> <p> ANMERKUNG: Failed login period, Maximum failed logins und Account lockout period müssen entweder alle leer sein oder alle einen Wert enthalten.</p>
Account lockout period	<p>Der Zeitraum (in Sekunden), für den ein Konto gesperrt bleibt, bevor sich der Nutzer wieder anmelden kann. Der gültige Wertebereich ist 1–86400 Sekunden. Die Standardwerte sind:</p> <ul style="list-style-type: none"> • Standardwert bei Aktivierung: 3600 • Wert bei Deaktivierung: Das Konto wird nie gesperrt (leer). <p> ANMERKUNG: Account lockout period, Maximum failed logins und Failed login period müssen entweder alle leer sein oder alle einen Wert enthalten.</p>
Session idle timeout	<p>Zeitraum ohne Aktivität (in Sekunden), nach dem für die Anmeldesitzung ein Timeout auftritt. Der gültige Wertebereich ist 1–3600 Sekunden. Die Standardwerte sind:</p> <ul style="list-style-type: none"> • Standardwert bei Aktivierung: 600 • Wert bei Deaktivierung: 3600 <p> ANMERKUNG: Ein leerer Wert bedeutet, dass bei Sitzungen nie ein Timeout aufgrund von Inaktivität auftritt.</p>
Default admin lockout enabled	<p>Gibt an, ob die Kontosperrung für Administratorbenutzer aktiviert ist. Mögliche Werte sind:</p> <ul style="list-style-type: none"> • yes • no <p>Die Standardwerte sind:</p> <ul style="list-style-type: none"> • Standardwert bei Aktivierung: no • Wert bei Deaktivierung: no

Konfigurieren von Benutzerkontoeinstellungen

Konfigurieren Sie die Kontoeinstellungen für ein STIG-fähiges System. Wenn die Option `-enabled yes` lautet, können alle nachfolgenden Optionen angegeben werden. Wenn die nachfolgenden Optionen nicht angegeben werden, obwohl die Benutzerkontoeinstellung `-enabled yes` lautet, wird jeweils der Standardwert bei Aktivierung, wie unten angegeben, verwendet. Der „disabled“-Wert für diese Optionen, wenn die Benutzerkontoeinstellung `-enabled no` lautet, wird in der Attributtabelle unter [Verwalten von Benutzerkontoeinstellungen](#) im Detail erläutert.

 **ANMERKUNG:** Dieser Befehl ist nicht gültig für Systeme, die nicht STIG-fähig sind.

Format

```
/user/account/settings set [-enabled {yes | no}] [-passwdMinSize <value>] [-passwdCount <value>]
[{-passwdPeriod <value> | -noPasswdPeriod}] [{-maxFailedLogins <value> | -noMaxFailedLogins}]
[{-failedLoginPeriod <value> | -noFailedLoginPeriod}] [{-lockoutPeriod <value> |
-noLockoutPeriod | -manualUnlock}] [{-sessionIdleTimeout <value> | -noSessionIdleTimeout}] [-
defaultAdminLockoutEnabled {yes | no}]
```

Tabelle 20. Aktionsqualifizierer

Qualifizierer	Beschreibung
-enabled	Gibt an, ob Benutzerkontoeinstellungen aktiviert oder deaktiviert werden sollen. Gültige Werte: <ul style="list-style-type: none"> • yes • no
-passwdMinSize	Gibt an, wie viele Zeichen das Passwort mindestens enthalten soll: Der gültige Wertebereich ist 8–64. Wird nichts angegeben, lautet der Standardwert bei „enabled“ 15.
-passwdCount	Gibt die Anzahl von Passwörtern an, die erneut verwendet werden können. Gültiger Bereich: 3 –12. Wird nichts angegeben, lautet der Standardwert bei „enabled“ 5.
-passwdPeriod	Gibt den Zeitraum (in Tagen) an, bis ein Passwort abläuft. Der gültige Wertebereich ist 1–180 Tage. Wird weder dieser Wert noch -noPasswdPeriod angegeben, lautet der Standardwert bei „enabled“ 60. ANMERKUNG: Diese Einstellung gilt nicht für lokale Admin-Nutzerkonten.
-noPasswdPeriod	Gibt an, dass das Passwort bei lokalen Benutzerkonten nicht abläuft.
-maxFailedLogins	Gibt die Anzahl der aufeinanderfolgenden fehlgeschlagenen Anmeldeversuche an, die innerhalb des unter „failed login period“ angegebenen Zeitraums zulässig sind, bis das Konto gesperrt wird. Der gültige Wertebereich ist 1–10. Wird weder dieser Wert noch -noMaxFailedLogins angegeben, lautet der Standardwert 3. ANMERKUNG: Wenn diese Option angegeben wird, müssen die Optionen -failedLoginPeriod und -lockoutPeriod ebenfalls angegeben werden.
-noMaxFailedLogins	Gibt an, dass keine maximale Begrenzung für die Anzahl der aufeinanderfolgenden fehlgeschlagenen Anmeldeversuchen vorhanden ist. ANMERKUNG: Wenn diese Option angegeben wird, müssen die Optionen -noFailedLoginPeriod und -noLockoutPeriod ebenfalls angegeben werden.
-failedLoginPeriod	Gibt den Zeitraum (in Sekunden) an, in dem höchstens die unter „Maximum failed logins“ angegebenen Anmeldeversuche auftreten dürfen, da es ansonsten zu einer Kontosperrung kommt. Der gültige Wertebereich ist 1–3600 Sekunden. Wird weder dieser Wert noch -noFailedLoginPeriod angegeben, lautet der Standardwert bei „enabled“ 900. ANMERKUNG: Wenn diese Option angegeben wird, müssen die Optionen -maxFailedLogins und -lockoutPeriod ebenfalls angegeben werden. Wenn die maximal möglichen fehlgeschlagenen Anmeldeversuche nicht während des unter Failed login period angegebenen Zeitraums aufgetreten sind, wird der Zähler für Maximum failed logins zurückgesetzt.
-noFailedLoginPeriod	Gibt an, dass die innerhalb eines bestimmten Zeitraums aufeinanderfolgenden fehlgeschlagenen Anmeldeversuche nicht gezählt werden. ANMERKUNG: Wenn diese Option angegeben wird, müssen die Optionen -noMaxFailedLogins und -noLockoutPeriod ebenfalls angegeben werden.
-lockoutPeriod	Gibt den Zeitraum (in Sekunden) an, für den ein Konto gesperrt bleibt, bevor sich der Nutzer wieder anmelden kann. Der gültige Wertebereich ist 1–86400 Sekunden. Wird

Tabelle 20. Aktionsqualifizierer (fortgesetzt)

Qualifizierer	Beschreibung
	weder dieser Wert noch <code>-noLockoutPeriod</code> angegeben, lautet der Standardwert bei „enabled“ 3600. <i>i</i> ANMERKUNG: Wenn diese Option angegeben wird, müssen die Optionen <code>-maxFailedLogins</code> und <code>-failedLoginPeriod</code> ebenfalls angegeben werden.
<code>-noLockoutPeriod</code>	Gibt an, dass lokale Nutzerkonten nicht gesperrt werden, wenn sie die Anzahl von <code>-maxFailedLogins</code> innerhalb des unter <code>-failedLoginPeriod</code> angegebenen Zeitraums erreichen. <i>i</i> ANMERKUNG: Wenn diese Option angegeben wird, müssen die Optionen <code>-noMaxFailedLogins</code> und <code>-noFailedLoginPeriod</code> ebenfalls angegeben werden.
<code>-manualUnlock</code>	Gibt an, dass das Konto gesperrt bleibt, bis es von einem Administrator manuell entsperrt wird.
<code>-sessionIdleTimeout</code>	Gibt den Zeitraum ohne Aktivität (in Sekunden) an, nach dem für die Anmeldesitzung ein Timeout auftritt. Der gültige Wertebereich ist 1–3600 Sekunden. Wird weder dieser Wert noch <code>-noSessionIdleTimeout</code> angegeben, lautet der Standardwert bei „enabled“ 600.
<code>-noSessionIdleTimeout</code>	Gibt an, dass bei Sitzungen nie ein Timeout aufgrund von Inaktivität auftreten soll.
<code>-defaultAdminLockoutEnabled</code>	Gibt an, ob die Kontosperrung für Administratorbenutzer aktiviert ist. Mögliche Werte sind: <ul style="list-style-type: none"> • yes • no Wird dieser Wert nicht angegeben, lautet der Standardwert bei „enabled“ no.

Beispiel 1

Mit dem folgenden Befehl werden die Nutzerkontoeinstellungen mit allen „enabled“-Standardwerten in Kraft gesetzt (bei einer vorherigen Festlegung von „disabled“):

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /user/account/settings set -enabled yes
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Beispiel 2

Mit dem folgenden Befehl werden die Benutzerkontoeinstellungen deaktiviert, sodass sie auf die Werte vor der Aktivierung zurückgesetzt werden:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /user/account/settings set -enabled no
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Anzeigen von Benutzerkontoeinstellungen

Sie können die Kontoeinstellungen aller Benutzer im System aufrufen.

Format

```
/user/account/settings show
```

Beispiel

Hiermit werden die Benutzerkontoeinstellungen für alle Benutzer im System angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /user/account/settings show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:   Enabled                               = yes
     Password minimum size                 = 15
     Number of previous passwords          = 5
     Password period                       = 60
     Maximum failed logins                 = 3
     Failed login period                   = 900
     Account lockout period                = 3600
     Session idle timeout                  = 600
     Default admin lockout enabled         = no
```

Managen von Supportanmeldedaten

Managen Sie die Einstellungen der Support-Anmeldedaten im System, wie zum Beispiel:

- Benutzername des Benutzerkontos
- Passwort des Benutzerkontos

In der folgenden Tabelle sind die Attribute der Supportanmeldedaten aufgeführt:

Tabelle 21. Attribute der Supportanmeldedaten

Merkmale	Beschreibung
Support user name	Name des Benutzerkontos
Support password	Passwort des Benutzerkontos

Anzeigen der Supportanmeldedaten

Zeigen Sie die aktuellen Supportanmeldedaten an.

Format

```
/sys/support/account show
```

Beispiel

Mit dem folgenden Befehl werden die Supportanmeldedaten angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/account show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:   Support user name = user1
```

Konfigurieren oder Ändern der Supportanmeldedaten

Konfigurieren oder ändern Sie die Attribute der Supportkontoanmeldedaten, die mit dem System verknüpft sind.

Format

```
/sys/support/account set -user <value> {-passwd <value> | -passwdSecure}
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-user	Geben Sie den Benutzernamen für das Konto des Supports an.
-passwd	Geben Sie das neue Passwort für das Konto des Supports an.
-passwdSecure	Gibt das Passwort im sicheren Modus an – der Benutzer wird aufgefordert, das Passwort einzugeben.

Beispiel

Mit dem folgenden Befehl geben Sie das neue Passwort für das Konto des Supports an:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/account set -user user1 -passwd Password123
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection  
  
Operation completed successfully.
```

Löschen von Supportanmeldedaten

Löschen Sie die Supportanmeldedaten.

Format

```
/sys/support/account delete
```

Beispiel

Mit dem folgenden Befehl können Sie Support-Anmeldedaten löschen:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/account delete
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection  
  
Operation completed successfully.
```

Managen von Systemlimits

Dieser CLI-Befehl zeigt die Limits des Systems und verschiedener Speicherressourcen an.

Systemlimits zeigen die Limits für Größe, Kapazität und Anzahl verschiedener Systemkomponenten oder Speicherressourcen an. Einige dieser Limits sind Schwellenwerten für Warnmeldungen zugeordnet. Wenn dieser Schwellenwert überschritten wird, erzeugt das System eine Warnmeldung. Bestimmte Limits sind lizenzabhängig.

Tabelle 22. Attribute von Systemlimits

Attribut	Beschreibung
ID	Kennung des Limits
Name	Name des Limits
Description	Beschreibung des Limits
Limit value	Obere Grenze des Limits, die nicht überschritten werden kann
Threshold value	Schwellenwert des angegebenen Limits, oberhalb dessen das System eine Warnmeldung erzeugt
License	Lizenzkennung in Bezug auf das gegebene Limit. Einige Systemlimits hängen vom Typ der installierten Lizenz ab.

Anzeigen von Systembegrenzungen

Mit diesem Befehl können Sie Systembegrenzungen, Schwellenwerte, die damit verbundene Warnmeldungen auslösen, und Limits, die auf Produktfunktionslizenzen basieren, anzeigen.

Zeigen Sie Details zu Systembegrenzungen an.

Format

```
/sys/limits [{"-id <value> | -license <value>}] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die Kennung des Limits ein.
-license	Geben Sie eine angegebene Lizenz ein, für die zugeordnete Limits angezeigt werden sollen.

Beispiel

Mit dem folgenden Befehl wird eine Liste aller Funktionslizenzen im System angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/limit show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:   ID           = Limit_Pool_MaxCapacityInTotal
     Name        = Max Storage Capacity
     Description = The maximum allowed capacity of all storage pools in total.
     Limit value = 17179869184 (16.0 TB)
     Threshold value = 15032385536 (14.0 TB)
     License     = STORAGE_CAPACITY_LIMIT

2:   ID           = Limit_Pool_MaxCount
     Name        = Max Storage Pool Count
     Description = The maximum allowed number of storage pools on the system.
     Limit value = 10
     Threshold value = 8
     License     =
```

```

3: ID = Limit VirtualDisk MinSize
   Name = Min Virtual Disk Size
   Description = The minimum allowed size of a virtual disk.
   Limit value = 10737418240 (10.0 GB)
   Threshold value =
   License =

```

Anzeigen der Lizenzen für installierte Funktionen

Zeigen Sie Details zu den Lizenzen für erworbene Funktionen an. Diese Lizenzen wurden zusammen mit dem System erworben. Sie müssen Lizenzen auf Ihrem System installieren, bevor Sie bestimmte Funktionen nutzen oder Aufgaben wie die Erstellung von Speicher ausführen können.

Verwenden Sie zur Installation einer Lizenz die Option `-upload`, um sie in das System hochzuladen. [Anzeigen der Befehlszeilenoptionen](#) enthält Details zu sämtlichen verfügbaren Optionen. Die folgende Tabelle führt die Attribute für Produktlizenzen auf und beschreibt sie.

Tabelle 23. Lizenzattribute

Attribut	Beschreibung
ID	Kennung der Lizenz
Name	Name der Lizenz.
Description	Beschreibung der Lizenz
Installed	Hier ist angegeben, ob eine Funktion mit der Lizenz installiert ist. Gültige Werte sind „yes“ und „no“.
Version	Version der Lizenz.
Issued	Datum, an dem die Lizenz zur Verfügung gestellt wurde.
Expires	Datum, bis zu dem die Lizenz gültig ist.
Health state	Der Integritätsstatus der Lizenz. Der Statuscode wird in Klammern angezeigt. Folgende Werte sind möglich: <ul style="list-style-type: none"> • <code>OK (5)</code>: Die Lizenz ist aktiv. • <code>Degraded/Warning (10)</code>: Die Lizenz läuft bald ab. • <code>Major failure (20)</code>: Die Lizenz ist abgelaufen. Rufen Sie zur Aktualisierung einer Lizenz, die bereits abgelaufen ist oder in Kürze abläuft, in Unisphere die Seite Lizenzen managen auf.
Health details	Zusätzliche Integritätsinformationen. In Anzeigen der Befehlszeilenoptionen finden Sie Einzelheiten zu den Integritätsinformationen.

Anzeigen von Lizenzen

Zeigen Sie Details zu installierten Lizenzen an.

 **ANMERKUNG:** Aktionsbefehl „show“ erläutert, wie das Ausgabeformat geändert wird.

Format

```
/sys/lic [-id <value>] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Identifizieren Sie die Lizenz.

Beispiel

Mit dem folgenden Befehl wird eine Liste aller Funktionslizenzen im System angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/lic show
```

```
1:      ID           = ISCSI
      Name          = Internet Small Computer System Interface (iSCSI)
      Description   = This license enables you to use the iSCSI
      protocol for  = block storage.
      Installed     = yes
      Version       = 1.1
      Issued        = 2009-11-09
      Expires       = 2010-11-09
      Health state  = OK (5)

2:      ID           = CIFS
      Name          = Common Internet File System (CIFS)
      Description   = This license enables you to configure and
      manage file  = shares that are exposed using the CIFS protocol.
      Installed     = yes
      Version       = 1.1
      Issued        = 2009-01-19
      Expires       = Never
      Health state  = OK (5)
```

Lesen und Akzeptieren der Endbenutzer-Lizenzvereinbarung

Zeigen Sie die Endbenutzer-Lizenzvereinbarung (EULA) an. Sie müssen die EULA akzeptieren, bevor Sie Produktlizenzen hochladen oder das System konfigurieren können.

Anzeigen der EULA

Zeigen Sie die EULA als Textdatei an. Die Ausgabe zeigt eine URL an, über die Sie auf die Textdatei zugreifen können.

 **ANMERKUNG:** Aktionsbefehl „show“ erläutert, wie das Ausgabeformat geändert wird.

Format

```
/sys/eula show
```

Beispiel

Mit dem folgenden Befehl wird der Vereinbarungsstatus der EULA sowie eine URL zur Anzeige der EULA als Textdatei angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/eula show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
1: Agree = yes
   URL = https://10.0.0.1/eula.txt
```

Akzeptieren der EULA

Akzeptieren Sie die EULA, bevor Sie Produktlizenzen installieren und das System konfigurieren.

Format

```
/sys/eula set -agree yes
```

Beispiel

Mit dem folgenden Befehl akzeptieren Sie die EULA:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/eula set -agree yes
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Managen der Remoteprotokollierung

Protokollieren Sie Systemmeldungen auf maximal fünf Remotehosts. Erstellen Sie eine Einstellung für die Remoteprotokollierung für jeden Host, bei der Folgendes angegeben wird:

- das System, auf dem die Protokolle erstellt werden
- der Netzwerkname bzw. die IP-Adresse des Remotehosts, auf dem die Protokolldaten gespeichert werden
- die Schweregrade, die an den Remotehost gesendet werden

Auf die Remotehosts muss vom System aus zugegriffen werden können. Die Sicherheit der Protokollinformationen muss über die Kontrolle des Netzwerkzugriffs oder über die Systemsicherheitsfunktionen am Remote-Host gewährleistet werden. Sie können die Methode zur Übertragung des Protokolls (UDP bzw. TCP) und den vom System zu verwendenden Hostport konfigurieren. Bei der Standardkonfiguration werden Protokollinformationen auf Port 514 über das UDP-Protokoll übertragen.

Meldungen werden in Flat-Dateien protokolliert. Die Systemmeldungen auf Benutzerebene werden in englischer Sprache aufgezeichnet. Sie können jedoch eine Stelle angeben, mit der Sie den in den Protokollen enthaltenen Informationstyp gemäß der ausgebenden Systemkomponente sowie die Sprache für das Protokoll auswählen können.

[Anzeigen von Ereignisprotokollen und Warnmeldungen](#) erläutert, wie Sie Details zu den aktuellen Systemprotokollen und -warnmeldungen anzeigen.

In der folgenden Tabelle sind die Attribute für die Remotesystemprotokollierung aufgeführt.

Tabelle 24. Attribute für die Remoteprotokollierung

Attribut	Beschreibung
ID	Kennung des Remotesystemprotokolls.
Enabled	Hier ist angegeben, ob die Remote-Protokollierung zurzeit aktiviert ist. Gültige Werte sind folgende (keine Unterscheidung zwischen Groß- und Kleinschreibung): <ul style="list-style-type: none">• yes• no
Host	Die IP-Adresse bzw. der Netzwerkname des Remote-Hosts.
Port	Portnummer auf dem Remote-Host. Der Standardwert ist 514.

Tabelle 24. Attribute für die Remoteprotokollierung (fortgesetzt)

Attribut	Beschreibung
Protocol	Das Protokoll zur Übertragung des Protokolls. Gültige Werte sind folgende (keine Unterscheidung zwischen Groß- und Kleinschreibung): <ul style="list-style-type: none"> • tcp • udp
Facility	Das System, auf dem das Protokoll verarbeitet wird. Es gilt einer der folgenden Werte (keine Unterscheidung zwischen Groß- und Kleinschreibung): <ul style="list-style-type: none"> • KERN - Kernel-Nachrichten. • USER (Standard) - Nachrichten auf Benutzerebene. • Syslog - Nachricht intern von syslogd generiert.
Severity	Die geringsten Schweregrade, die an den Remotehost gesendet werden. Gültige Werte sind folgende (keine Unterscheidung zwischen Groß- und Kleinschreibung): <ul style="list-style-type: none"> • emergency • alert • critical • error • warning • notice • info • debug

Erstellen der Konfiguration für Remoteprotokollierung

Erstellen Sie die Konfiguration für die Remoteprotokollierung.

Format

```
/sys/rlog create [-enabled {yes|no}] [-host <value>] [-port <value>] [-protocol {udp|tcp}] [-facility {KERN | USER | Syslog}] [-severity {emergency | alert | critical | error | warning | notice | info | debug}]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-enabled	Mit dieser Option wird die Protokollierung auf einem Remote-System aktiviert. Gültige Werte sind folgende (keine Unterscheidung zwischen Groß- und Kleinschreibung): <ul style="list-style-type: none"> • yes • no Bei Angabe von yes muss -host <value> verwendet werden. Hierbei steht „value“ für die IP-Adresse des Ziel-Remotehosts, auf dem die Protokolle gespeichert werden.
-host	Geben Sie die IP-Adresse bzw. den Netzwerknamen des Remotehosts ein, auf dem die Protokolldateien gespeichert werden sollen. Folgende Werte sind möglich: <ul style="list-style-type: none"> • <IPv4-Adresse> • <IPv6-Adresse> • <Netzwerkname> ⓘ ANMERKUNG: Die neue Kombination aus IP-Adresse und Port darf nicht mit einer vorhandenen Remotehostadresse identisch sein.

Qualifizierer	Beschreibung
-port	Geben Sie die Portnummer ein, mit der der Host die übertragenen Protokollinformationen empfängt. Der Standardwert ist 514.
-protocol	Geben Sie das Protokoll für die Übertragung der Protokolldateien an. Gültige Werte sind folgende (keine Unterscheidung zwischen Groß- und Kleinschreibung): <ul style="list-style-type: none"> • tcp • udp
-facility	Geben Sie an, welches System die Protokolldateien verarbeitet. Es gilt einer der folgenden Werte (keine Unterscheidung zwischen Groß- und Kleinschreibung): <ul style="list-style-type: none"> • KERN: Kernel-Meldungen. • USER (Standardeinstellung): Meldungen auf Nutzerebene. • Syslog: Intern von syslog erzeugte Meldung.
-severity	Geben Sie die geringsten Schweregrade der Protokolldateien ein, die an den Remotehost gesendet werden. Es gilt einer der folgenden Werte (keine Unterscheidung zwischen Groß- und Kleinschreibung): <ul style="list-style-type: none"> • emergency • alert • critical • error • warning • notice • info • debug <p> ANMERKUNG: Beispielsweise ist der Standardschweregrad. Wenn dieser Wert eingegeben wird, werden alle Nutzer-/Auditprotokolle an den Remotehost gesendet. Wenn eingegeben wird, werden nur Protokolle mit dem Schweregrad „emergency“ an den Remotehost gesendet.</p>

Beispiel

Mit dem folgenden Befehl wird die Protokollierung auf einem Remotesystem mit den folgenden Einstellungen konfiguriert:

- Remotezielhost: 10.10.10.10
- Hostport: 8181
- Verwendet Protokoll: tcp.
- Verwendet das syslog-System.
- Schweregrad:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/rlog set -enabled yes -host 10.10.10.10
-port 8181 -protocol TCP -facility syslog -severity notice
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
Operation completed successfully.
```

Anzeigen von Einstellungen für die Remote-Protokollierung

Zeigen Sie Einstellungen für die Remote-Protokollierung an.

Format

```
/sys/rlog show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID ein, die den Remotehost identifiziert. Optional, wenn nur ein Remotehost konfiguriert ist.

Beispiel

Mit dem folgenden Befehl werden die Einstellungen für die Protokollierung auf Remote-Systemen angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/rlog show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      ID          = RemoteSysLogPort_0
      Enabled    = yes
      Host       = 10.0.0.1
      Port       = 514
      Protocol   = UDP
      Facility   = KERN
      Severity   = DEBUG
```

Ändern der Konfiguration für Remoteprotokollierung

Aktualisieren Sie die Konfiguration für Remoteprotokollierung mit neuen Einstellungen.

Format

```
/sys/rlog [-id <value>] set [-enabled {yes|no}] [-host <value>] [-port <value>] [-protocol {udp|tcp}] [-facility {KERN | USER | Syslog}] [-severity {emergency | alert | critical | error | warning | notice | info | debug}]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID ein, die den Remotehost identifiziert. Optional, wenn nur ein Remotehost konfiguriert ist.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-enabled	Mit dieser Option wird die Protokollierung auf einem Remote-System aktiviert. Gültige Werte sind folgende (keine Unterscheidung zwischen Groß- und Kleinschreibung): <ul style="list-style-type: none">• yes• no Bei Angabe von yes muss -host <value> verwendet werden. Hierbei steht „value“ für die IP-Adresse des Ziel-Remotehosts, auf dem die Protokolle gespeichert werden.
-host	Geben Sie die IP-Adresse bzw. den Netzwerknamen des Remotehosts ein, auf dem die Protokolldateien gespeichert werden sollen. Folgende Werte sind möglich: <ul style="list-style-type: none">• <IPv4-Adresse>• <IPv6-Adresse>• <Netzwerkname>

Qualifizierer	Beschreibung
	 ANMERKUNG: Die neue Kombination aus IP-Adresse und Port darf nicht mit einer vorhandenen Remotehostadresse identisch sein.
-port	Geben Sie die Portnummer des Remotehosts ein. Der Standardwert ist <i>514</i> .
-protocol	Geben Sie das Protokoll für die Übertragung der Protokolldateien an. Gültige Werte sind folgende (keine Unterscheidung zwischen Groß- und Kleinschreibung): <ul style="list-style-type: none"> • tcp • udp
-facility	Geben Sie an, welches System die Protokolldateien verarbeitet. Es gilt einer der folgenden Werte (keine Unterscheidung zwischen Groß- und Kleinschreibung): <ul style="list-style-type: none"> • KERN - Kernel-Nachrichten. • USER - Nachrichten auf Benutzerebene. • Syslog - Meldung intern von Syslog generiert.
-severity	Geben Sie die geringsten Schweregrade der Protokolldateien ein, die an den Remotehost gesendet werden. Es gilt einer der folgenden Werte (keine Unterscheidung zwischen Groß- und Kleinschreibung): <ul style="list-style-type: none"> • emergency • alert • critical • error • warning • notice • info • debug  ANMERKUNG: Zum Beispiel, debug ist der Standard-Schweregrad. Wenn dieser Wert eingegeben wird, werden alle Nutzer-/Auditprotokolle an den Remotehost gesendet. Wenn <i>emergency</i> eingegeben wird, werden nur Protokolle mit Notfall-Schweregrad an den Remote-Host gesendet.

Beispiel

Mit dem folgenden Befehl wird die Protokollierung auf einem Remotesystem mit den folgenden Einstellungen konfiguriert:

- Remotezielhost: 10.64.74.12
- Hostport: 514
- Verwendet Protokoll: udp.
- Verwendet das KERN-System.
- Verwendet die *critical*-Schwere.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/rlog set -enabled yes -host 10.64.74.12
-port 514 -protocol UDP -facility KERN -severity critical
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = RemoteSysLogPort_0
Operation completed successfully.
```

Löschen der Konfiguration für Remoteprotokollierung

Löschen Sie eine Konfiguration für Remoteprotokollierung.

 **ANMERKUNG:** Wenn nur ein Remoteziel vorhanden ist, dürfen Sie es nicht löschen.

Format

```
/sys/rlog -id <value> delete
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des zu löschenden Remotehosts ein.

Beispiel

Mit dem folgenden Befehl wird der Remotehost „RemoteSysLogPort_1“ gelöscht:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/rlog -id RemoteSysLogPort_1 delete
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
Operation completed successfully.
```

Managen der Systemzertifikate

Schnittstelle für das Management von Zertifikaten für verschiedene Komponenten auf dem Speichersystem.

In der folgenden Tabelle sind die Attribute für Zertifikate aufgeführt:

Tabelle 25. Zertifikatattribute

Attribut	Beschreibung
ID	Zertifikatkennung
Type	Zertifikattyp Gültige Zertifikattypen sind: <ul style="list-style-type: none">• CA• Server• Client• TrustedPeer
Service	Service, mit dem das Zertifikat verknüpft ist. Die unterstützten Services sind: <ul style="list-style-type: none">• Mgmt_LDAP• Mgmt_KMIP• VASA_HTTP• vSphere
Scope	Umfang des Zertifikats. Das Zertifikat kann lokalen oder globalen Umfang haben. Wenn er global ist, hat er keinen Wert. Wenn er lokal ist, ist der Wert die Kennung des Umfangs. Zum Beispiel: Wenn der Umfang des Zertifikats, das dem Service Mgmt_LDAP zugeordnet ist, NAS-Server „nas01“ ist, dann ist der Wert der Eigenschaft „nas01“.
Trust anchor	Gibt an, ob das Zertifikat als vertrauenswürdig gilt als „End-of-Chain“ für Peer-Zertifikatüberprüfung. Gültige Werte: <ul style="list-style-type: none">• yes• no
Version	Zertifikatversion
Serial number	Seriennummer des Zertifikats
Signature algorithm	Signaturalgorithmus des Zertifikats

Tabelle 25. Zertifikatattribute (fortgesetzt)

Attribut	Beschreibung
Issuer name	Name der Zertifikatausgabestelle.
Valid from	Datum und Uhrzeit des Beginns der Gültigkeit des Zertifikats
Valid to	Datum und Uhrzeit des Ablaufs des Zertifikats
Subject name	Betreff des Zertifikats
Subject alternative name	Alternativer Name des Betreffs des Zertifikats
Public key algorithm	Algorithmus des öffentlichen Schlüssels des Zertifikats
Key length	Schlüssellänge des Zertifikats
Thumbprint algorithm	Fingerabdruckalgorithmus des Zertifikats
Thumbprint	Fingerabdruck des Zertifikats
Private key available	Gibt an, ob das Zertifikat mit einem privaten Schlüssel verbunden ist. Je nach Verfügbarkeit sind gültige Werte: <ul style="list-style-type: none"> • yes • no

Anzeigen von Informationen zum Zertifikat

Zeigen Sie Details zu einem Zertifikat an.

Format

```
/sys/cert [ -type { CA | Server | Client | TrustedPeer } ] [ -service {Mgmt_LDAP | Mgmt_KMIP | VASA_HTTP | vSphere} [ -scope <value> ] ] [ -id <value> ] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Identifiziert das Zertifikat.
-type	Identifiziert den Typ des Zertifikats.
-service	Identifiziert den Service. Gültige Werte: <ul style="list-style-type: none"> • Mgmt_LDAP • Mgmt_KMIP • VASA_HTTP • vSphere
-scope	Identifiziert den Herausgeber des Zertifikats.

Beispiel

Mit dem folgenden Befehl werden Informationen über ein VASA-HTTP-Zertifikat angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/cert -id vasa_http-vc1-cacert-1 show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```

1: ID = vasa_http-vc1-cacert-1
   Type = CA
   Service = VASA_HTTP
   Scope =
   Trust anchor = no
   Version = 2
   Serial number = 04:00:00:00:00:01:21:58:53:08:A2
   Signature algorithm = SHA256WithRSAEncryption
   Issuer name = CN = GlobalSign O = GlobalSign OU = GlobalSign Root CA - R3
   Valid from = 2009-03-18 10:00:00
   Valid to = 2029-03-18 10:00:00
   Subject name = CN = GlobalSign O = GlobalSign OU = GlobalSign Root CA - R3
   Subject alternative name =
   Public key algorithm = RSA
   Key length = 2048
   Thumbprint algorithm = SHA1
   Thumbprint = d6 9b 56 11 48 f0 1c 77 c5 45 78 c1 09 26 df 5b 85 69 76 ad
   Private key available = no

```

Löschen eines Systemzertifikats

Löscht ein X509-Zertifikat.

Format

```
/sys/cert -id <value> delete
```

Objektqualifizierer

Objekt	Beschreibung
-id	Identifiziert das Zertifikat.

Beispiel

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/cert -id vasa_http-vc1-servercert-1 delete
```

```

Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.

```

Managen von Snapshot-Schutzplänen

Zur Planung der Snapshot-Erstellung weisen Sie der Speicherressource, von der Snapshots erstellt werden sollen, einen Schutzplan zu. Die Pläne bestehen aus mindestens einer Regel, mit der der Zeitpunkt und die Häufigkeit der Erstellung von Speicherressourcen-Snapshots festgelegt werden. Wenn Sie eine Regel erstellen, können Sie sie einem vorhandenen Plan zuweisen. Ansonsten wird sie automatisch einem neuen Plan zugewiesen. [Managen von Aufgabenregeln](#) erläutert, wie Aufgabenregeln eingerichtet werden. [Management von Snapshots](#) erläutert, wie Sie manuell Snapshots erstellen und vorhandene Snapshots managen.

Die einzelnen Schutzpläne sind durch jeweils eigene IDs gekennzeichnet.

In der folgenden Tabelle sind die Attribute für Schutzpläne aufgeführt.

Tabelle 26. Attribute für Schutzpläne

Attribut	Beschreibung
ID	Die ID des Plans

Tabelle 26. Attribute für Schutzpläne (fortgesetzt)

Attribut	Beschreibung
Name	Der Name des Plans
Type	Der Plantyp. Folgende Werte sind möglich: <ul style="list-style-type: none"> • system: Vom System definiert • user: Von einem Benutzer definiert
Rules	Liste der IDs für jede einzelne Aufgabenregel im Plan. Managen von Aufgabenregeln bietet Einzelheiten zu Planregeln.
Sync replicated	Der Zustand, der dem Nutzer anzeigt, ob der Zeitplan synchron auf dem Remotesystem repliziert wird. Folgende Werte sind möglich: <ul style="list-style-type: none"> • no: Der Zeitplan wird lokal erstellt und wird nicht repliziert. • yes: Der Zeitplan ist synchron mit dem Remotesystem.
Last modified time	Der Zeitpunkt der letzten Änderung des Zeitplans

Anzeigen von Schutzplänen

Zeigen Sie Details zu den Schutzplänen an. Sie können nach der Plan-ID filtern.

 **ANMERKUNG:** Aktionsbefehl „show“ erläutert, wie das Ausgabeformat geändert wird.

Format

```
/sys/task/sched [-id <value>] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID eines Plans ein.

Beispiel

Mit dem folgenden Befehl werden Details zu sämtlichen Plänen (benutzer- und systemdefiniert) im System angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/task/sched show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:   ID           = LessProtectionID
     Name        = Less Protection
     Type        = System
     Rules       = RULE_1, RULE2
     Sync replicated = no

2:   ID           = DefaultProtectionID
     Name        = Default Protection
     Type        = System
     Rules       = RULE_3
     Sync replicated = no

3:   ID           = MySchedID
     Name        = MySched1
     Type        = User
```

```
Rules           = RULE_4
Sync replicated = yes
```

Löschen von Schutzplänen

Löschen Sie einen benutzerdefinierten Schutzplan. Vom System definierte Pläne oder Pläne, die mit Speicherressourcen verbunden oder ihnen zugewiesen sind, können nicht gelöscht werden.

ANMERKUNG: Beim Löschen eines Plans werden sämtliche damit verknüpften Regeln ebenfalls gelöscht.

Format

```
/sys/task/sched [-id <value>] delete
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des zu löschenden Plans ein.

Beispiel

Mit dem folgenden Befehl wird der Plan „MySchedID“ gelöscht:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/task/sched -id MySchedID delete
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
Operation completed successfully.
```

Managen von Aufgabenregeln

In Aufgabenregeln wird festgelegt, wann und wie häufig eine Aufgabe, beispielsweise die Erstellung eines Snapshots, ausgeführt wird. Wenn Sie eine Regel erstellen, können Sie sie einem vorhandenen Schutzplan zuweisen. Ansonsten wird sie automatisch einem neuen Plan zugewiesen. Anschließend weisen Sie den Plan der Speicherressource zu, auf der Snapshots geplant sind. [Managen von Snapshot-Schutzplänen](#) erläutert, wie Sie Schutzpläne anzeigen und löschen können.

In der folgenden Tabelle sind die Attribute für Aufgabenregeln aufgeführt.

Tabelle 27. Attribute für Aufgabenregeln

Attribut	Beschreibung
ID	Die ID der Regel.
Type	Die Art der Regel, mit der angegeben wird, wann eine Aufgabe ausgeführt wird. Gültige Werte: <ul style="list-style-type: none">• <code>hoursinterval</code>: Die Aufgabe wird in einem in Stunden bzw. Minuten angegebenen Intervall ausgeführt.• <code>hourslist</code>: Die Aufgabe wird jeden Tag zu einer bestimmten Stunde und optional zu einer bestimmten Minute innerhalb dieser Stunde ausgeführt.• <code>daysinterval</code>: Die Aufgabe wird in einem in Tagen angegebenen Intervall und optional zu einer bestimmten Stunde am angegebenen Tag ausgeführt.

Tabelle 27. Attribute für Aufgabenregeln (fortgesetzt)

Attribut	Beschreibung
	<ul style="list-style-type: none"> • <code>weekdayslist</code>: Die Aufgabe wird am angegebenen Tag der Woche oder zur angegebenen Stunde an jedem angegebenen Tag ausgeführt. • <code>monthdayslist</code> : Die Aufgabe wird jeden Monat an einem bestimmten Tag zu einer bestimmten Uhrzeit ausgeführt.
Frequency	Die Häufigkeit, in der eine Aufgabe ausgeführt wird.
Keep for	Der Zeitraum, den ein Snapshot aufbewahrt wird, bevor er gelöscht wird.
Allow auto-delete	Für Snapshots; gibt an, ob der Snapshot automatisch gelöscht werden kann. Gültige Werte: <ul style="list-style-type: none"> • <code>yes</code>: Das System kann den Snapshot automatisch löschen. • <code>no</code> : Das System kann den Snapshot nicht automatisch löschen.
Access	Für Snapshots; gibt an, ob der von dieser Planung erstellte Snapshot ein Kontrollpunkt ist oder auf „Lesen/Schreiben“ eingestellt ist. Gültige Werte: <ul style="list-style-type: none"> • <code>ckpt</code> : Der Snapshot ist ein schreibgeschützter Kontrollpunkt. • <code>share</code>: Der Snapshot ist auf „Lesen/Schreiben“ eingestellt, damit Benutzer CIFS (SMB)-Freigaben oder NFS-Exporte erstellen können.

Erstellen von Aufgabenregeln

Erstellen Sie eine Aufgabenregel und fügen Sie sie einem vorhandenen Zeitplan hinzu. Wenn ein Zeitplan nicht vorhanden ist, wird ein neuer erstellt.

 **ANMERKUNG:** `gmtoff` Switch kann nicht verwendet werden, wenn der Nutzer die Zeitzone des Zeitplans bereits konfiguriert hat.

Format

```
/sys/task/rule create {-schedId <value> | -schedName <value>} -type {hoursinterval -every <value> [-at <value>] | hourslist -hours <value> [-at <value>] | daysinterval -every <value> [-at <value>] | weekdayslist -days <value> [-at <value>] | monthdayslist -days <value> [-at <value>]} [{-keepFor <value> | -allowAutoDelete {yes | no}}] [-access {ckpt | share}] [-syncRep {yes | no}]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
<code>-schedId</code>	Geben Sie die ID eines vorhandenen Schutzplans an, dem Sie die Regel zuweisen. Anzeigen von Schutzplänen erläutert, wie Sie Details zu vorhandenen Plänen und ihren IDs anzeigen können.
<code>-schedName</code>	Geben Sie einen Namen für den neuen Schutzplan ein, dem Sie die Regel zuweisen möchten.
<code>-type</code>	Geben Sie den Regeltyp und damit die Häufigkeit an, mit der die Aufgabe ausgeführt wird. Gültige Werte: <ul style="list-style-type: none"> • <code>hoursinterval</code> : Die Aufgabe wird in einem in Stunden bzw. Minuten angegebenen Intervall ausgeführt. • <code>hourslist</code> : Die Aufgabe wird jeden Tag zu einer bestimmten Stunde und optional zu einer bestimmten Minute innerhalb dieser Stunde ausgeführt. Unterstützt bis zu zwei angegebene Stunden. • <code>daysinterval</code> : Die Aufgabe wird in einem in Tagen angegebenen Intervall und optional zu einer bestimmten Stunde am angegebenen Tag ausgeführt.

Qualifizierer	Beschreibung
	<ul style="list-style-type: none"> • <code>weekdayslist</code>: Die Aufgabe wird am angegebenen Tag der Woche oder zur angegebenen Stunde an jedem angegebenen Tag ausgeführt. Unterstützt bis zu sieben angegebene Werte, einschließlich aller Tage in der Woche. • <code>monthdayslist</code>: Die Aufgabe wird jeden Monat an einem bestimmten Tag zu einer bestimmten Uhrzeit ausgeführt. Unterstützt nur einen Tag-Wert.
<code>-every</code> (verwendet mit <code>-type</code>)	<p>Wenn der Wert von <code>-typehoursinterval</code> oder <code>daysinterval</code> ist, geben Sie das Zeitintervall für die Aufgabenausführung ein. Gültige Werte:</p> <ul style="list-style-type: none"> • <code>hoursinterval</code> : Anzahl der Stunden im Bereich von 1 bis 24. • <code>daysinterval</code> : Anzahl der Tage im Bereich von 1 bis 31.
<code>-hours</code> (verwendet mit <code>-type</code>)	<p>Wenn der Wert von <code>-typehourslist</code> ist, geben Sie eine durch Komma getrennte Liste der Stunden des Tages für die Aufgabenausführung ein. Der Wertebereich liegt zwischen 0 und 23.</p>
<code>-at</code> (verwendet mit <code>-type</code>)	<p>Geben Sie die Minutenzahl innerhalb einer Stunde bzw. an einem Tag ein, wenn die Aufgabe auf Basis des Werts von <code>-type</code> ausgeführt wird. Gültige Werte:</p> <ul style="list-style-type: none"> • <code>hoursinterval</code> oder <code>hourslist</code>: Geben Sie die Zahl der Minuten nach der Stundenangabe im Bereich zwischen 0 und 59 ein. Der Standardwert ist 0. • <code>daysinterval</code>, <code>weekdayslist</code> oder <code>monthdayslist</code> : Geben Sie die Uhrzeit für den Tag im folgenden Format ein: <code><HH>[:MM]</code> wobei <code>HH</code> die Stunde und <code>MM</code> die Minuten innerhalb der angegebenen Stunde repräsentiert. Der Wertebereich erstreckt sich von 0:00 bis 23:59. Der Standardwert ist 0:00.
<code>-days</code> (verwendet mit <code>-type</code>)	<p>Wenn der Wert von <code>-typeweekdayslist</code> oder <code>monthdayslist</code> ist, geben Sie die Wochentage oder den Tag des Monats ein, an denen die Aufgabe ausgeführt werden soll:</p> <ul style="list-style-type: none"> • <code>weekdayslist</code>: Geben Sie eine durch Komma getrennte Liste der Wochentage ein. Gültige Werte: <ul style="list-style-type: none"> ○ <code>mon</code> : Montag ○ <code>tue</code> : Dienstag ○ <code>wed</code> : Mittwoch ○ <code>thu</code> : Donnerstag ○ <code>fri</code> : Freitag ○ <code>sat</code> : Samstag ○ <code>sun</code> : Sonntag • <code>monthdayslist</code> : Geben Sie den Tag des Monats innerhalb des Bereichs zwischen 1 und 31 ein. <p> ANMERKUNG: Für <code>monthdayslist</code> können Sie nur einen Tag im Monat angeben.</p>
<code>-keepFor</code>	<p>Geben Sie ein, wie viele Tage oder Stunden ein Snapshot vom System aufbewahrt werden soll, bevor er gelöscht wird. Verwenden Sie das folgende Format: <code><value>[<qualifier>]</code>. Hierbei gilt:</p> <ul style="list-style-type: none"> • <code>value</code>: Geben Sie die Zahl der Stunden bzw. Tage ein. Folgende Werte können verwendet werden: <ul style="list-style-type: none"> ○ <code>hours</code> : Anzahl der Stunden im Bereich von 1 bis 8760. ○ <code>days</code> : Anzahl der Tage im Bereich von 1 bis 365. • <code>qualifier</code>: Geben Sie den Qualifizierer für den Wert ein. Folgende Werte sind möglich: <ul style="list-style-type: none"> ○ <code>h</code> : Gibt die Stunden an. ○ <code>d</code> : Gibt die Tage an. <p>Der Standardwert beträgt 1h (1 Stunde).</p>
<code>-allowAutoDelete</code>	<p>Geben Sie an, ob das System automatisch den Snapshot oder Snapshot-Satz löschen kann. Gültige Werte:</p> <ul style="list-style-type: none"> • <code>yes</code> (Standard) • <code>no</code>
<code>-access</code>	<p>Geben Sie an, ob der Snapshot ein schreibgeschützter Kontrollpunkt ist oder „Lesen/Schreiben“ für CIFS (SMB)-Freigaben oder NFS-Exporte eingestellt ist. Gültige Werte:</p> <ul style="list-style-type: none"> • <code>ckpt</code> (Standard) • <code>share</code>
<code>-syncRep</code>	<p>Geben Sie an, ob dieser Zeitplan synchron repliziert wird. Alle Änderungen, die an dem replizierten Zeitplan auf dem lokalen System vorgenommen werden, gelten automatisch und umgekehrt für das Remotesystem. Gültige Werte:</p> <ul style="list-style-type: none"> • <code>yes</code>

Qualifizierer	Beschreibung
	<ul style="list-style-type: none"> no <p> ANMERKUNG: Wenn eine synchrone Remoteverbindung hergestellt wird, ist der Standardwert <code>yes</code> sonst ist er <code>no</code>.</p>

Beispiel 1

Mit dem folgenden Befehl wird eine Aufgabenregel mit den folgenden Einstellungen erstellt:

- Die Regel wird dem neuen Schutzplan „MyScheduleID“ zugewiesen.
- Alle 12 Stunden und 30 Minuten wird ein Snapshot erstellt.
- Hiermit wird der Snapshot 10 Stunden lang aufbewahrt und erst dann gelöscht.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/task/rule create -schedName MyScheduleID
-type hoursinterval -every 12 -at 30 -keepFor 10h
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = RULE_1
Schedule ID = MyScheduleID
Operation completed successfully.
```

Beispiel 2

Mit dem folgenden Befehl wird eine Aufgabenregel mit den folgenden Einstellungen erstellt:

- Hiermit wird die Regel dem vorhandenen Schutzplan „MySchedID“ zugewiesen.
- Es wird jeden Tag ein Snapshot um 8.30 Uhr und 20.30 Uhr erstellt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/task/rule create -schedId MySchedID -type
hourslist -hours "8,20" -at 30
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = RULE_2
Operation completed successfully.
```

Beispiel 3

Mit dem folgenden Befehl wird eine Aufgabenregel mit den folgenden Einstellungen erstellt:

- Hiermit wird die Regel dem vorhandenen Schutzplan „MySchedID“ zugewiesen.
- Alle zwei Tage wird um 13.20 Uhr ein Snapshot erstellt.
- Der Snapshot wird erst nach 1 Woche (7 Tagen) gelöscht:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/task/rule create -schedId MySchedID -type
daysinterval -every 2 -at 13:20 -keepFor 7d
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = RULE_3
Operation completed successfully.
```

Beispiel 4

Mit dem folgenden Befehl wird eine Aufgabenregel mit den folgenden Einstellungen erstellt:

- Hiermit wird die Regel dem vorhandenen Schutzplan „MySchedID“ zugewiesen.
- Jeden Montag-, Mittwoch- und Freitagmorgen um 6.00 Uhr wird ein Snapshot erstellt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/task/rule create -schedId MySchedID -type weekdayslist -days "Mon,Wed,Fri" -at 6
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = RULE_4
Operation completed successfully.
```

Beispiel 5

Mit dem folgenden Befehl wird eine Aufgabenregel mit den folgenden Einstellungen erstellt:

- Hiermit wird die Regel dem vorhandenen Schutzplan „MySchedID“ zugewiesen.
- Es wird an jedem Monatsersten um 12.00 Uhr ein Snapshot erstellt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/task/rule create -schedId MySchedID -type monthdayslist -days 1
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = RULE_5
Operation completed successfully.
```

Beispiel 6

Mit dem folgenden Befehl wird eine Aufgabenregel mit den folgenden Einstellungen erstellt:

- Hiermit wird die Regel dem vorhandenen Schutzplan „MySchedID“ zugewiesen.
- Es wird an jedem Monatsersten um 12.00 Uhr ein Snapshot erstellt. zum bestehenden Zeitplan mithilfe des `gmtoff`-Switch:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! -gmtoff -4 /sys/task/rule create -schedId MySchedID -type monthdayslist -days 1
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
Operation failed. Error code: 0x6401f5e
"-gmtoff" is not allowed when schedule time zone is configured. Either remove it or clear
schedule time zone. (Error Code:0x6401f5e)
```

Anzeigen von Aufgabenregeln

Zeigen Sie Details zu Aufgabenregeln an. Sie können nach der ID einer Regel filtern oder die ID eines Schutzplans eingeben, damit nur die diesem Plan zugewiesenen Regeln angezeigt werden.

ANMERKUNG: Aktionsbefehl „show“ erläutert, wie das Ausgabeformat geändert wird. Der `gmtoff` -Switch kann nicht verwendet werden, wenn der Nutzer die Zeitzone des Zeitplans bereits konfiguriert hat. Der Grund dafür ist, dass das Attribut „Frequenz“ mit der Zeitzone des Zeitplans angezeigt wird.

Format

```
/sys/task/rule [{"-id <value> | -sched<value>}] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID einer Regel ein.
-sched	Geben Sie die ID eines Schutzplans ein, um die damit verbundenen Regeln anzuzeigen.

Beispiel 1

Mit dem folgenden Befehl werden die Details sämtlicher Aufgabenregeln, die mit Schutzplan SCHED_3 verknüpft sind, aufgeführt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/task/rule -sched SCHED_3 show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:   ID           = RULE_1
     Type        = HoursInterval
     Frequency   = Every 12h at 30m after the hour
     Keep for    = 10h
     Allow auto-delete = no
     Access      =

2:   ID           = RULE_2
     Type        = HoursList
     Frequency   = Every day at 0:20, 8:20, 20:20
     Keep for    = 1h
     Allow auto-delete = no
     Access      = ckpt

3:   ID           = RULE_3
     Type        = DaysInterval
     Frequency   = Every 2d at 13:20
     Keep for    = 7d
     Allow auto-delete = no
     Access      = share

4:   ID           = RULE_4
     Type        = WeekDaysList
     Frequency   = Every Mon, Wed, Fri at 6:00
     Keep for    = 1h
     Allow auto-delete = no
     Access      =

5:   ID           = RULE_5
     Type        = MonthDaysList
     Frequency   = Every 1st, 2nd, 3rd day of month at 0:00
     Keep for    = 1h
     Allow auto-delete = no
     Access      =
```

Beispiel 2

Mit dem folgenden Befehl werden Details sämtlicher Aufgabenregeln aufgelistet, die dem Schutzplan SCHED_3 für (UTC-05:00) Detroit, Iqaluit, Marengo, New York, Vincennes verknüpft sind, aufgeführt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/task/rule -sched SCHED_3 show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      ID              = RULE_1
      Type              = HoursInterval
      Frequency         = Every 12h at 30m after the hour ((UTC-05:00) Detroit, Iqaluit,
Marengo, New York, Vincennes)
      Keep for          = 10h
      Allow auto-delete = no
      Access            =

2:      ID              = RULE_2
      Type              = HoursList
      Frequency         = Every day at 0:20, 8:20, 20:20 ((UTC-05:00) Detroit, Iqaluit,
Marengo, New York, Vincennes)
      Keep for          = 1h
      Allow auto-delete = no
      Access            = ckpt

3:      ID              = RULE_3
      Type              = DaysInterval
      Frequency         = Every 2d at 13:20 ((UTC-05:00) Detroit, Iqaluit, Marengo, New
York, Vincennes)
      Keep for          = 7d
      Allow auto-delete = no
      Access            = share

4:      ID              = RULE_4
      Type              = WeekDaysList
      Frequency         = Every Mon, Wed, Fri at 6:00 ((UTC-05:00) Detroit, Iqaluit,
Marengo, New York, Vincennes)
      Keep for          = 1h
      Allow auto-delete = no
      Access            =

5:      ID              = RULE_5
      Type              = MonthDaysList
      Frequency         = Every 1st, 2nd, 3rd day of month at 0:00 ((UTC-05:00) Detroit,
Iqaluit, Marengo, New York, Vincennes)
      Keep for          = 1h
      Allow auto-delete = no
      Access            =
```

Beispiel 3

Mit dem folgenden Befehl werden Details sämtlicher Aufgabenregeln, die dem Schutzplan SCHED_3 zugewiesen sind, und versuchen, den `gmtoff`-Switch zu verwenden, aufgeführt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! -gmtoff -4 /sys/task/rule -sched SCHED_3 show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation failed. Error code: 0x6401f5e
"-gmtoff" is not allowed when schedule time zone is configured. Either remove it or clear
schedule time zone. (Error Code:0x6401f5e)
```

Einstellungen für Aufgabenregeln ändern

Ändern Sie die Einstellungen für vorhandene Aufgabenregeln mit Ausnahme des Regeltyps.

Format

```
/sys/task/rule -id <value> set [-frequency {[-every <value>] [-at <value>] | [-hours <value>]
[-at <value>] | [-days <value>] [-at <value>]]} [-access {ckpt|share}] [{-keepFor <value> |
-allowAutoDelete {yes|no}}]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID ein, die die Zeitplanregel identifiziert.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-frequency	Markierung, die die Häufigkeit der Regel angibt.  ANMERKUNG: Der Typ der Regel kann nicht geändert werden. Geben Sie die korrekten Parameter gemäß dem Regeltyp an.
-every (basierend auf dem Regeltyp)	Geben Sie das Zeitintervall an. Wenn der Wert von <code>-typehoursinterval</code> oder <code>daysinterval</code> ist, geben Sie das Zeitintervall für die Aufgabenausführung ein. Gültige Werte: <ul style="list-style-type: none"> Für <code>hoursinterval</code>: Anzahl der Stunden im Bereich von 1 bis 24. Für <code>daysinterval</code>: Anzahl der Tage im Bereich von 1 bis 31.
-hours (basierend auf dem Regeltyp)	Wenn der Wert von <code>-typehourslist</code> ist, geben Sie eine durch Komma getrennte Liste der Stunden des Tages für die Aufgabenausführung ein. Der Wertebereich liegt zwischen 0 und 23.
-at (basierend auf dem Regeltyp)	Geben Sie die Minutenzahl innerhalb einer Stunde bzw. an einem Tag ein, wenn die Aufgabe auf Basis des Werts von <code>-type</code> ausgeführt wird. Gültige Werte: <ul style="list-style-type: none"> <code>hoursinterval</code> oder <code>hourslist</code>: Geben Sie die Zahl der Minuten nach der Stundenangabe im Bereich zwischen 0 und 59 ein. Der Standardwert ist 0. <code>daysinterval</code>, <code>weekdayslist</code> oder <code>monthdayslist</code>: Geben Sie die Uhrzeit für den Tag im folgenden Format ein: <code><HH>[:MM]</code> wobei <code>HH</code> die Stunde und <code>MM</code> die Minuten innerhalb der angegebenen Stunde repräsentiert. Der Wertebereich erstreckt sich von 0:00 bis 23:59. Der Standardwert ist 0:00.
-days (basierend auf dem Regeltyp)	Wenn der Wert von <code>-typeweekdayslist</code> oder <code>monthdayslist</code> ist, geben Sie die Wochentage oder den Tag des Monats ein, an denen die Aufgabe ausgeführt werden soll: <ul style="list-style-type: none"> <code>weekdayslist</code>: Geben Sie eine durch Komma getrennte Liste der Wochentage ein. Gültige Werte: <ul style="list-style-type: none"> <code>mon</code>: Montag <code>tue</code>: Dienstag <code>wed</code>: Mittwoch <code>thu</code>: Donnerstag <code>fri</code>: Freitag <code>sat</code>: Samstag <code>sun</code>: Sonntag <code>monthdayslist</code>: Geben Sie den Tag des Monats innerhalb des Bereichs zwischen 1 und 31 ein.  ANMERKUNG: Für <code>monthdayslist</code> können Sie nur einen Tag im Monat angeben.
-keepFor	Geben Sie ein, wie viele Tage oder Stunden ein Snapshot vom System aufbewahrt werden soll, bevor er gelöscht wird. Verwenden Sie das folgende Format: <code><value>[<qualifier>]</code> . Hierbei gilt: <ul style="list-style-type: none"> <code>value</code>: Geben Sie die Zahl der Stunden bzw. Tage ein. Folgende Werte können verwendet werden: <ul style="list-style-type: none"> <code>hours</code>: Anzahl der Stunden im Bereich von 1 bis 8760. <code>days</code>: Anzahl der Tage im Bereich von 1 bis 365. <code>qualifier</code>: Geben Sie den Qualifizierer für den Wert ein. Folgende Werte sind möglich:

Qualifizierer	Beschreibung
	<ul style="list-style-type: none"> ○ h : Gibt die Stunden an. ○ d : Gibt die Tage an. Der Standardwert beträgt 1h (1 Stunde).
-allowAutoDelete	Geben Sie an, ob das System automatisch den Snapshot oder Snapshot-Satz löschen kann. Gültige Werte: <ul style="list-style-type: none"> ● yes (Standard) ● no
-access	Geben Sie an, ob der Snapshot ein schreibgeschützter Kontrollpunkt ist oder „Lesen/Schreiben“ für CIFS (SMB)-Freigaben oder NFS-Exporte eingestellt ist. Gültige Werte: <ul style="list-style-type: none"> ● ckpt (Standard) ● share

Beispiel 1

Mit folgendem Befehl wird die Regel `SchedRule_37` so geändert, dass alle 12 Stunden und 30 Minuten ein Snapshot erstellt und 10 Stunden lang aufbewahrt wird:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/task/rule -id SchedRule_37 set -type hoursinterval -every 12 -at 30 -keepFor 10h
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = RULE_1
Schedule ID = MyScheduleID
Operation completed successfully.
```

Beispiel 2

Mit folgendem Befehl wird die ursprüngliche Regel `SchedRule_37` durch nicht übereinstimmende Parameter geändert:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/task/rule -id SchedRule_37 -set -frequency -hours "8,20" -at 30
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
Operation failed. Error code: 0x6000c59
```

```
Invalid syntax for frequency parameter. Recheck the type of the schedule rule. (Error Code:0x6000c59)
```

Löschen von Aufgabenregeln

Löschen Sie eine Aufgabenregel.

 **ANMERKUNG:** Sie können keine Regeln löschen, die mit einem systemdefinierten Plan verknüpft sind, sondern nur Regeln im Zusammenhang mit einem benutzerdefinierten Plan. Wenn Sie die letzte Regel eines Plans löschen, wird der Plan ebenfalls gelöscht.

Format

```
/sys/task/rule -id <value> delete
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID der zu löschenden Regel ein.

Beispiel

Mit dem folgenden Befehl wird die Regel RULE_1 gelöscht:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/task/rule -id RULE_1 delete
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection
```

```
Operation completed successfully.
```

Managen von Jobs

Managen Sie die Operationen, die im Hintergrund ausgeführt werden.

In der folgenden Tabelle sind die Attribute für Jobs aufgeführt.

Tabelle 28. Attribute für Jobs

Attribut	Beschreibung
ID	Jobkennung
Type	Jobtyp. Folgende Werte sind möglich: <ul style="list-style-type: none">• Provisioning• Snapshot• Snapshot schedule
Title	Jobtitel
State	Jobstatus. Folgende Werte sind möglich: <ul style="list-style-type: none">• Queued• Running• Suspended• Completed• Completed with problems• Failed• Rolling back
Result description	Beschreibt das Ergebnis des Schritts.
Step	Aktueller Schritt
User	Benutzer, der den Job gestartet hat
Start time	Zeitpunkt, zu dem der Job gestartet wurde
Elapsed time	Verstrichene Zeit für den aktuellen Job
Estimated time left	Verbleibende Zeit bis zum Abschluss des aktuellen Jobs
Percent complete	Jobfortschritt in Prozent
Associated object	Objekt oder Speicherressource, das/die von diesem Job betroffen ist. Nur ein Objekt ist mit jedem Job verknüpft. Format wird wie folgt angezeigt:

Tabelle 28. Attribute für Jobs (fortgesetzt)

Attribut	Beschreibung
	<id> (<object type>)

Anzeigen der Liste der Jobs

Zeigen Sie die Liste der vorhandenen Jobs an.

Format

```
/sys/task/job [{"-id <value> | -active | -failed | -completed}] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Identifiziert den Job.
-active	Zeigt nur nicht abgeschlossene Jobs an (Queued, Running, Suspended, Rolling back).
-failed	Zeigt nur fehlgeschlagene Jobs an.
-completed	Zeigt nur erfolgreich abgeschlossene Jobs und mit Problemen abgeschlossene Jobs an.

Beispiel 1

Mit dem folgenden Befehl wird eine Liste aller Jobs angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/task/job show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:   ID           = N-26
     Type        = Provisioning
     Title       = Create or modify storage resource
     State       = Completed
     Step        = 2 of 2 (Apply iSCSI hosts)
     Percent complete = 100%
```

Beispiel 2

Mit dem folgenden Befehl wird eine Liste aller Jobs angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/task/job show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:   ID           = N-11
     Type        = Storage resource provisioning
     Title       = Create storage resource
     State       = Completed
     Result description = Success
     User        = Local/admin
     Step        =
     Start time   = 2016-06-17 09:47:36
     Elapsed time = 1m 26s
```

```
Estimated time left =  
Percent complete = 100%  
Associated object = fs_3 (/stor/prov/fs)
```

Wiederaufnahmen eines Jobs

Nimmt einen vorhandenen Job wieder auf. Kann nur auf den unterbrochenen Job angewendet werden.

Format

```
/sys/task/job -id <value> resume
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Identifiziert den Job.

Beispiel

Mit dem folgenden Befehl wird ein vorhandener Job abgebrochen.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/task/job -id N-23564 resume
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection  
  
Operation completed successfully.
```

Abbrechen eines Jobs

Bricht einen vorhandenen Job ohne Rollback ab. Kann nur auf den unterbrochenen oder in Warteschlange gestellten Job angewendet werden.

Format

```
/sys/task/job -id <value> cancel
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Identifiziert den Job.

Beispiel

Mit dem folgenden Befehl wird ein vorhandener Job abgebrochen.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/task/job -id N-23654 cancel
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection
```

```
Operation completed successfully.
```

Löschen von Jobs

Löscht einen Job oder eine Jobgruppe. Aktive Jobs können nicht gelöscht werden.

Format

```
/sys/task/job {-id <value> | -failed | -completed} delete
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Identifiziert den Job.
-failed	Identifiziert Jobs, die fehlgeschlagen sind
-completed	Identifiziert Jobs, die erfolgreich oder mit Problemen abgeschlossen wurden

Beispiel

Mit dem folgenden Befehl wird ein vorhandener Job gelöscht.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/task/job -id N-23654 delete
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection
```

```
Operation completed successfully.
```

Managen von Jobschritten

Managen Sie die Schritte des angegebenen Jobs.

In der folgenden Tabelle sind die Attribute für Jobschritte aufgeführt.

Tabelle 29. Attribute für Jobschritte

Attribut	Beschreibung
Title	Titel des Schritts
Status	Status des Schritts. Folgende Werte sind möglich: <ul style="list-style-type: none">• Queued• Running• Completed• Failed
Execution result code	Der Fehlercode der Operation
Execution result description	Die Fehlermeldung der Operation
Rollback result code	Der Fehlercode des Rollback
Rollback result description	Die Fehlermeldung des Rollback
Details	Zusätzliche Informationen Format: key: „value“, key: „value“, ...

Tabelle 29. Attribute für Jobschritte (fortgesetzt)

Attribut	Beschreibung
Associated object	Objekt oder Speicherressource, das/die von diesem Job betroffen ist. Nur ein Objekt ist mit jedem Jobschritt verknüpft. Format wird wie folgt angezeigt: <id> (<object type>)

Anzeigen einer Liste der Schritte in einem Job

Zeigt eine Liste der Schritte des angegebenen Jobs an.

Format

```
/sys/task/job/step -jobId <value> show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-jobId	Identifiziert den Job.

Beispiel 1

Mit dem folgenden Befehl wird eine Liste der Schritte des angegebenen Jobs angezeigt.

```
uemcli /sys/task/job/step -jobId N-23654 show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1: Title           = Extend storage pool
   Status          = Completed
   Execution result code = 0
   Execution result description =
   Rollback result code = 0
   Rollback result description =
   Details         = ID: "local_pool_8"; Name: "SASx6_2"

2: Title           = Create application
   Status          = Completed
   Execution result code = 0
   Execution result description =
   Rollback result code = 0
   Rollback result description =
   Details         = ID: "local_pool_8"; Name: "SASx6_2"

3: Title           = Create file system
   Status          = Running
   Execution result code = 0
   Execution result description =
   Rollback result code = 0
   Rollback result description =
   Details         = ID: fs_99; Name: JobTest11

4: Title           = Create NFS share
   Status          = Queued
   Execution result code = 0
   Execution result description =
   Rollback result code = 0
   Rollback result description =
   Details         = ID: nfs_45; Name: JobTest11
```

```

5: Title = Finalize allocation
   Status = Queued
   Execution result code = 0
   Execution result description =
   Rollback result code = 0
   Rollback result description =
   Details = ID: local_pool_8; Name: SASx6_2

```

Beispiel 2

Mit dem folgenden Befehl wird eine detaillierte Liste der Schritte des angegebenen Jobs angezeigt.

```
uemcli /sys/task/job/step -jobId N-11 show -detail
```

```

Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1: Title = Create storage resource
   Status = Completed
   Execution result code = 0
   Execution result description =
   Rollback result code = 0
   Rollback result description =
   Details = ID: "res_3"; Name: "testFS3"
   Associated object =

2: Title = Create file system
   Status = Completed
   Execution result code = 0
   Execution result description =
   Rollback result code = 0
   Rollback result description =
   Details = ID: "fs_3"; Name: "testFS3"
   Associated object = fs_3 (/stor/prov/fs)

3: Title = Add filesystem to storage resource
   Status = Completed
   Execution result code = 0
   Execution result description =
   Rollback result code = 0
   Rollback result description =
   Details = ID: "res_3, fs_3"
   Associated object =

```

Konfigurieren der Netzwerkkommunikation

Themen:

- Managen von NAS-Servern
- Managen von VLANs
- Managen von Mandanten
- Managen von CIFS-Servern
- Managen von NFS-Servern
- Managen von Common Anti Virus Agent (CAVA)
- Managen von Konfigurationseinstellungen für Ereignisveröffentlichung
- Managen von Konfigurationseinstellungen für CEPA-Pools
- Managen von VMware-NAS-Protokollendpunktservern
- Managen des gegenseitigen CHAP für die gegenseitige CHAP-Authentifizierung
- Einrichten des iSNS für iSCSI-Speicher
- Managen der iSCSI-Konfiguration
- Managen von iSCSI-Nodes (iSCSI-Servern)
- Managen von Ethernetports
- Managen von SAS-Ports (nur physische Bereitstellungen)
- Managen von FC-Ports
- Managen von nicht aktivierten Ports
- Managen von Management-Netzwerkschnittstellen
- Management von Netzwerkschnittstellen
- Managen statischer IP-Routen
- Managen von Verbindungsbündelungen
- Managen von Failsafe-Netzwerkfunktionen (nur physische Bereitstellungen)
- Managen von DNS-Einstellungen
- Managen von NTP-Servereinstellungen
- Managen von NIS-Serverdomain
- Managen von SMTP-Servereinstellungen
- Managen von NDMP-Servereinstellungen
- Managen von LDAP-Einstellungen
- Dienstprogrammbeefehle
- Managen von Distributed Hierarchical Storage Management
- Managen der DHSM-Verbindung
- Managen des Tie-Breaker-Node (nur virtuelle Dual-SP-Bereitstellungen)
- Managen der Konfiguration eines Tie-Breaker-Node (nur virtuelle Dual-SP-Bereitstellungen)

Managen von NAS-Servern

NAS-Server sind Softwarekomponenten im System, die Vorgänge für über SMB- oder NFS-Protokolle übertragene Daten managen. Sie müssen mindestens einen NAS-Server konfigurieren, bevor Sie gemeinsamen Netzwerkspeicher erstellen können. Sie können einen NAS-Server so konfigurieren, dass Windows-Netzwerk-Shares (SMB) und/oder Linux/UNIX-Netzwerk-Shares unterstützt werden.

NAS-Server werden auf jedem SP ausgeführt und kommunizieren mit Netzwerkhosts über SP-Ports. Nach der Konfiguration eines NAS-Servers können Sie Dateisysteme erstellen, aus denen Sie NFS- oder SMB-Netzwerk-Shares exportieren. Auf konfigurierten Hosts werden Netzwerk-Freigaben für den Zugriff auf den Dateisystemspeicher zugeordnet oder gemountet.

Die einzelnen NAS-Server verfügen über eigene IDs.

In der folgenden Tabelle sind die Attribute für NAS-Server aufgeführt.

Tabelle 30. NAS-Server-Attribute

Merkmale	Beschreibung
ID	ID des NAS-Servers.
Name	Name des NAS-Servers
Health state	Integritätsstatus des NAS-Servers. Der Integritätsstatuscode wird in Klammern angezeigt. Folgende Werte sind möglich: <ul style="list-style-type: none"> • Unknown (0) : Status ist unbekannt. • OK (5) : Funktioniert ordnungsgemäß. • OK BUT (7) : Die Konfiguration ist unvollständig. • Degraded/Warning (10) : Funktioniert und führt alle Funktionen aus, die Performance ist jedoch eventuell nicht optimal. • Minor failure (15) : NAS-Server ist defekt. • Major failure (25) : Es ist ein Fehler aufgetreten; eine Recovery ist eventuell nicht möglich. Diese Bedingung hat zu Datenverlusten geführt. Der Fehler muss umgehend behoben werden.
Health details	Zusätzliche Integritätsinformationen. Weitere Einzelheiten finden Sie in Anhang A, Referenz.
SP	Primärer SP, auf dem der NAS-Server ausgeführt wird. <i>i</i> ANMERKUNG: Wenn der primäre SP heruntergestuft wird oder ausgefallen ist, führt der Server ein Failover zum anderen SP aus. Der aktuelle SP, den der Server verwendet, wird in Klammern angezeigt. Beispiel: SPA (Failover zu SPB).
Storage pool	Zugehörige Speicherpoolkennung.
Tenant	Kennung und Name des Mandanten.
Interface	ID der Netzwerkschnittstelle des NAS-Servers, der die Server-IP-Adresse definiert und dem Server die Kommunikation mit dem Netzwerk und den Hosts ermöglicht. Management von Netzwerkschnittstellen erläutert, wie die Netzwerkschnittstellen im System konfiguriert werden. <i>i</i> ANMERKUNG: Es ist zulässig, die letzte Schnittstelle des Servers zu entfernen.
CIFS enabled	Gibt an, ob SMB-Dateisysteme auf dem NAS-Server aktiviert sind. Gültige Werte sind „yes“ und „no“. Der Standardwert ist „no“. SMB-Dateisysteme bieten Unterstützung für SMB-Netzwerk-Shares.
Multiprotocol sharing enabled	Gibt an, ob die Multiprotokoll-Share für alle Dateisysteme auf dem NAS-Server aktiviert ist. Gültige Werte: <ul style="list-style-type: none"> • yes • no
Unix directory service	Verzeichnisdienst, der für die Abfrage von Identitätsinformationen für Unix, wie etwa UIDs, GIDs, Netzgruppen usw. verwendet wird. Gültige Werte: <ul style="list-style-type: none"> • local • nis • ldap • localThenNis • localThenLdap • none (Standard) <i>i</i> ANMERKUNG: Ein anderer Wert als der Standardwert ist für eine genaue Multiprotokollfreigabe von Dateien zwischen Unix- und Windows-Benutzern erforderlich.
Auto user mapping enabled	Gilt, wenn der Multiprotokoll-Freigabemodus aktiviert ist. Gibt an, ob ein Windows-Benutzer, dem kein bekannter Unix-/Linux-Benutzername zugeordnet ist, auf die Dateien auf dem NAS-Server zugreifen darf. <ul style="list-style-type: none"> • yes: Das System erzeugt eine interne UID für den Windows-Benutzer und ermöglicht den Zugriff auf die NAS-Serverdateien über Windows.

Tabelle 30. NAS-Server-Attribute (fortgesetzt)

Merkmale	Beschreibung
	<ul style="list-style-type: none"> no (Standardeinstellung): Die Windows-Authentifizierung schlägt fehl, wenn kein Unix-Standardnutzernamen konfiguriert ist.
Default Unix username	<p>Unix-Standardbenutzername oder Unix-ID, durch den bzw. die der Dateizugriff im Multiprotokoll-Freigabemodus gewährt wird. Dieser Benutzername wird für Windows-Benutzer verwendet, wenn der entsprechende Unix/Linux-Benutzername nicht vom Zuordnungsmechanismus gefunden wird.</p> <p>Das Unix-ID-Format lautet „@uid=xxxx,gid=yyyy@“, wobei xxxx und yyyy die Zahlenwerte der UID bzw. der primären GID sind. Wenn Sie diese ID verwenden, muss der Benutzer nicht im UDS definiert sein.</p>
Default Windows username	<p>Windows-Standardbenutzername, der den Dateizugriff im Multiprotokoll-Freigabemodus erlaubt. Dieser Benutzername wird für Unix-Benutzer verwendet, wenn der entsprechende Windows-Benutzername nicht vom Zuordnungsmechanismus gefunden wird.</p>
Replication type	<p>Zeigt an, an welcher asynchronen Replikation dieser NAS-Server teilnimmt. Gültige Werte:</p> <ul style="list-style-type: none"> none local remote mixed
Synchronous replication type	<p>Zeigt an, an welcher synchronen Replikation dieser NAS-Server teilnimmt. Gültige Werte:</p> <ul style="list-style-type: none"> none remote
Replication destination	<p>Gibt an, ob der NAS-Server ein Replikationsziel ist. Gültige Werte:</p> <ul style="list-style-type: none"> yes no <p>i ANMERKUNG: Dieses Attribut gilt nicht für den Replikationsstatus der zugehörigen Dateisysteme. Verwenden Sie den Befehl <code>stor/prov/fs show</code>, um den Replikationsstatus der Dateisysteme anzuzeigen.</p>
Backup only	<p>Zeigt an, ob der NAS-Server für Sicherungszwecke zum Einsatz kommt. Dieses Attribut zeigt an, dass der NAS-Server nicht der Produktionsstandort sein kann. Dies bedeutet, dass sowohl geplantes Failover als auch ungeplantes Failover in der mit dem NAS-Server verbundenen Replikationssitzung nur zur Sicherung nicht zulässig sind.</p>
Migration destination	<p>Gibt an, ob der NAS-Server ein Ziel für eine NAS-Importsitzung ist. Gültige Werte:</p> <ul style="list-style-type: none"> yes no
Username translation	<p>Gibt an, ob eine Benutzernamenszuordnung (Unix zu/von Windows) aktiviert ist. Gültige Werte:</p> <ul style="list-style-type: none"> yes no
Packet Reflect enabled	<p>Gibt an, ob die Spiegelung der ausgehenden Pakete (Antwort) über dieselbe Schnittstelle wie eingehende Pakete (Anforderung) aktiviert ist. Gültige Werte:</p> <ul style="list-style-type: none"> yes no (Standard)
Preferred production interfaces overridden	<p>Gibt an, ob die bevorzugten Schnittstellen für die Produktion auf dem Replikationsziel außer Kraft gesetzt sind.</p>
Preferred production IPv4 interface	<p>Gibt die Einstellungen für die bevorzugte IPv4-Schnittstelle für die Produktion an. Gültige Werte:</p> <ul style="list-style-type: none"> <Schnittstellen-ID> auto

Tabelle 30. NAS-Server-Attribute (fortgesetzt)

Merkmale	Beschreibung
Preferred production IPv6 interface	Gibt die Einstellungen für die bevorzugte IPv6-Schnittstelle für die Produktion an. Gültige Werte: <ul style="list-style-type: none"> • <Schnittstellen-ID> • auto
Preferred backup IPv4 interface	Gibt die Einstellungen für die bevorzugte IPv4-Schnittstelle für Backup und Disaster-Recovery-Test an. Gültige Werte: <ul style="list-style-type: none"> • <Schnittstellen-ID> • auto
Preferred backup IPv6 interface	Gibt die Einstellungen für die bevorzugte IPv6-Schnittstelle für Backup und Disaster-Recovery-Test an. Gültige Werte: <ul style="list-style-type: none"> • <Schnittstellen-ID> • auto
Source preferred production IPv4 interface	Gibt die Einstellungen der replizierten bevorzugten IPv4-Schnittstelle für die Produktion auf dem Replikationsziel an. Wenn es überschrieben ist, unterscheidet es sich möglicherweise von der Preferred production IPv4 interface. Gültige Werte: <ul style="list-style-type: none"> • <Schnittstellen-ID> • auto
Source preferred production IPv6 interface	Gibt die Einstellungen der replizierten bevorzugten IPv6-Schnittstelle für die Produktion auf dem Replikationsziel an. Wenn es überschrieben ist, unterscheidet es sich möglicherweise von der Preferred production IPv6 interface. Gültige Werte: <ul style="list-style-type: none"> • <Schnittstellen-ID> • auto
File space used	Zeigt den gesamten Dateispeicherplatz an, der für den angegebenen NAS-Server verwendet wird.
Data Reduction space saved	Gibt die eingesparte Größe an, wenn für diesen NAS-Server eine Datenreduzierung verwendet wird.
Data Reduction percent	Gibt den Prozentsatz des eingesparten Speichers an, wenn eine Datenreduzierung verwendet wird, im Vergleich zu der von diesem NAS-Server verwendeten Gesamtgröße.
Data Reduction ratio	Gibt das Verhältnis der Einsparungen zwischen Daten ohne Datenreduzierung und Daten nach der Datenreduzierung für diesen NAS-Server an.

Erstellen eines NAS-Servers

Erstellen Sie einen NAS-Server.

 **ANMERKUNG:** Das NFSv3-Protokoll ist standardmäßig aktiviert, wenn ein NAS-Server erstellt wird.

Format

```
/net/nas/server create -name <value> -sp <value> {-pool <value> | -poolName <value>}
[-tenant <value>] [-mpSharingEnabled {no | yes [-autoUserMappingEnabled {yes | no}]} [-
unixDirectoryService {local | ldap | nis | localThenNis | localThenLdap | none}] [-
defaultUnixUser <value>] [-defaultWindowsUser <value>]] [-replDest {yes [-backupOnly {yes |
no}] | no}] [-enablePacketReflect {yes | no}]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-name	Gibt den NAS-Servernamen an.

Qualifizierer	Beschreibung
	<p>i ANMERKUNG: NAS-Servernamen können alphanumerische Zeichen sowie einen Gedankenstrich und einen Unterstrich enthalten. Servernamen dürfen keine Leerzeichen aufweisen oder mit einem Gedankenstrich beginnen oder enden. Sie können NAS-Servernamen in vier Teilen erstellen, die durch Punkte getrennt sind (Beispiel: aa.bb.cc.dd). Namen können bis zu 255 Zeichen lang sein; der erste Teil des Namens (vor dem ersten Punkt) ist auf 15 Zeichen begrenzt.</p>
-sp	Gibt den übergeordneten SP für den NAS-Server an. Der Wert lautet „SPA“ oder „SPB“.
-pool	Gibt die ID des Speicherpools für den NAS-Server an.
-poolName	Gibt den Namen des Speicherpools für den NAS-Server an.
-tenant	Gibt die Kennung des Mandanten an. i ANMERKUNG: Wenn kein Mandant angegeben wird, wird der NAS-Server im standardmäßigen Netzwerk-Namespace erstellt.
-mpSharingEnabled	Gibt an, ob der Multiprotokoll-Share-Modus aktiviert ist. Gültige Werte sind „yes“ und „no“ (Standardeinstellung).
-unixDirectoryService	Verzeichnisdienst, der für die Suche nach Identitätsinformationen für Unix (wie etwa UIDs, GIDs, Netzgruppen usw.) verwendet wird. Gültige Werte: <ul style="list-style-type: none"> • nis • ldap • local • none (Standardeinstellung) • localThenNis • localThenLdap
-autoUserMappingEnabled	Gibt an, ob ein Windows-Benutzer, dem kein bekannter Unix-/Linux-Benutzername zugeordnet ist, auf die Dateien auf dem NAS-Server zugreifen darf. Gültige Werte: <ul style="list-style-type: none"> • yes: Das System erzeugt eine interne UID für den Windows-Benutzer und ermöglicht den Zugriff auf die NAS-Serverdateien über Windows. • no (Standardeinstellung): Die Windows-Authentifizierung schlägt fehl, wenn kein Unix-Standardbenutzername konfiguriert ist.
-defaultUnixUser	Unix-Standardbenutzername oder Unix-ID, durch den bzw. die der Dateizugriff im Multiprotokoll-Freigabemodus gewährt wird. Dieser Benutzername bzw. diese ID wird verwendet, wenn mit dem Zuordnungsmechanismus kein Unix-/Linux-Benutzername bzw. keine Unix-/Linux-ID gefunden wird. Das Unix-ID-Format lautet „@uid=xxxx,gid=yyyy@“, wobei xxxx und yyyy die Zahlenwerte der UID bzw. der primären GID sind. Wenn Sie diese ID verwenden, muss der Benutzer nicht im UDS definiert sein.
-defaultWindowsUser	Windows-Standardbenutzername, der den Dateizugriff im Multiprotokoll-Freigabemodus erlaubt. Dieser Benutzername wird verwendet, wenn der entsprechende Windows-Benutzername durch den Zuordnungsmechanismus nicht gefunden wird.
-replDest	Replikationszieleinstellungen für den NAS-Server. Wenn diese Option auf yes festgelegt ist, sind möglicherweise nur obligatorische Parameter enthalten. Alle anderen optionalen Parameter werden vom Quell-NAS-Server übernommen. Gültige Werte: <ul style="list-style-type: none"> • yes • no (Standardeinstellung)
-backupOnly	Gibt an, ob der NAS-Server nur für Sicherungszwecke erstellt werden soll. Der NAS-Server nur für Sicherungszwecke kann kein Produktionsstandort sein. Das bedeutet, dass sowohl geplantes Failover als auch ungeplantes Failover in einer NAS-Server-Replikationssitzung nur für Sicherungszwecke nicht zulässig sind. Gültige Werte: <ul style="list-style-type: none"> • yes • no

Qualifizierer	Beschreibung
-enablePacketReflect	Gibt an, ob die Spiegelung der ausgehenden Pakete (Antwort) über dieselbe Schnittstelle wie eingehende Pakete (Anforderung) aktiviert ist. Gültige Werte: <ul style="list-style-type: none"> • yes (Standardeinstellung) • no

Beispiel

Mit dem folgenden Befehl wird ein NAS-Server mit den folgenden Einstellungen erstellt:

- Name: NasServer_1.
- Verknüpft mit SP A.
- Verknüpft mit Speicherpool pool_0.
- Die IP-Paketspiegelung ist aktiviert.
- Die ID des neuen NAS-Servers ist ID nas_1.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/server create -name NasServer_1 -sp
spa -pool pool_0 -enablePacketReflect yes
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = nas_1
Operation completed successfully.
```

Anzeigen von NAS-Servern

Zeigen Sie Details zu konfigurierten NAS-Servern an, z. B. ihren Namen, die ID, und ob Support für CIFS (SMB)-Dateisysteme oder NFS-Dateisysteme aktiviert ist. Sie können nach der NAS-Server-ID filtern.

 **ANMERKUNG:** Aktionsbefehl „show“ erläutert, wie das Ausgabeformat geändert wird.

Format

```
/net/nas/server [{-id <value> | -name <value> | -tenant {<value> | none}}] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID eines NAS-Servers ein.
-name	Geben Sie den NAS-Servernamen ein.
-tenant	Geben Sie die Mandantenkennung ein.

Beispiel 1

Mit dem folgenden Befehl werden alle Details einer Liste aller konfigurierten NAS-Server angezeigt.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/server show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
1:      ID          = nas_1
      Name         = MyFS1
```

```

NetBIOS name           = MyFS1
SP                     = spa
Storage pool           = pool_0
Tenant                 = tenant_1
Interface              = if_0,if_1
NFS enabled            = yes
NFSv4 enabled          = no
CIFS enabled           = no
Multiprotocol sharing enabled = no
Unix directory service = none
Health state           = OK_BUT (7)

2:  ID                 = nas_2
    Name               = MyFS2
    NetBIOS name       = MyFS2
    SP                 = spa
    Storage pool       = pool_1
    Tenant             = tenant_2
    Interface          = if_3
    NFS enabled        = yes
    NFSv4 enabled      = no
    CIFS enabled       = yes
    Multiprotocol sharing enabled = yes
    Unix directory service = ldap
    Health state       = OK (5)

```

Beispiel 2

Mit dem folgenden Befehl werden alle Details einer Liste aller konfigurierten NAS-Server angezeigt.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/server show -detail
```

```

Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:  ID                 = nas_1
    Name               = MyVDM1
    NetBIOS name       =
    SP                 = spa
    Storage pool       = pool_1
    Tenant             =
    Interface          =
    NFS enabled        = yes
    NFSv4 enabled      = no
    CIFS enabled       = no
    Workgroup          =
    Windows domain     =
    Multiprotocol sharing enabled = no
    Unix directory service = none
    Auto user mapping enabled =
    Default Unix username =
    Default Windows username =
    Extended Unix credentials enabled = no
    Credentials cache retention = 15m
    Username translation =
    Packet Reflect enabled = yes
    Health state       = OK (5)
    Health details     = "The component is operating normally. No action is required."

    Type               = 64
    Replication destination = no
    Backup only         = no
    Migration destination = no
    Preferred production interfaces overridden =
    Preferred production IPv4 interface = auto
    Preferred production IPv6 interface = auto
    Preferred backup and DR test IPv4 interface = auto
    Preferred backup and DR test IPv6 interface = auto
    Source preferred production IPv4 interface =
    Source preferred production IPv6 interface =

```

```

File space used           = 8945901568 (8.3G)
Data Reduction space saved = 0
Data Reduction percent    = 0%
Data Reduction ratio      = 1:1

```

Ändern von NAS-Servereinstellungen

Ändern Sie einen vorhandenen NAS-Server.

 **ANMERKUNG:** [Management von Netzwerkschnittstellen](#) erläutert, wie Sie die einem NAS-Server zugeordneten Netzwerkschnittstellen ändern.

Format

```

/net/nas/server {-id <value | -name <value > set [-name <value>] [-sp {spa |
spb}} [-mpSharingEnabled {yes | no}} [-unixDirectoryService {ldap | nis | none}} [-
autoUserMappingEnabled {yes | no}} [{"-defaultAccessDisabled | [-defaultUnixUser <value>] [-
defaultWindowsUser <value>}}] [-enablePacketReflect {yes | no }} [-replDest {yes | no }} [-
backupOnly {yes | no}} [-preferredProductionOverride { no | yes }}][-preferredProductionIPv4
{ auto | <value>}}] [-preferredProductionIPv6 { auto | <value>}}] [-preferredBackupIPv4 {auto |
<value>}}] [-preferredBackupIPv6 {auto | <value>}}

```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des zu ändernden NAS-Servers ein.
-name	Geben Sie den Namen des zu ändernden NAS-Servers ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-name	Name des Servers für freigegebene Ordner
-sp	Eigentümer-SP Gültige Werte: <ul style="list-style-type: none"> • spa • spb
-mpSharingEnabled	Gibt an, ob der Multiprotokoll-Share-Modus aktiviert ist. Gültige Werte: <ul style="list-style-type: none"> • yes • no  ANMERKUNG: Sie können die Multiprotokoll-Dateifreigabe für NAS-Server nach der Erstellung eines Dateisystems auf dem NAS-Server nicht deaktivieren.
-unixDirectoryService	Verzeichnisdienst, der für die Suche nach Identitätsinformationen für Unix (wie etwa UIDs, GIDs, Netzgruppen usw.) verwendet wird. Gültige Werte: <ul style="list-style-type: none"> • nis • ldap • local • none • localThenNis • localThenLdap
-defaultAccessDisabled	Deaktiviert den Dateizugriff, wenn kein Mechanismus zur Anwenderzuordnung gefunden wird.

Qualifizierer	Beschreibung
-autoUserMappingEnabled	Gibt an, ob ein Windows-Benutzer, dem kein bekannter Unix-/Linux-Benutzername zugeordnet ist, auf die Dateien auf dem NAS-Server zugreifen darf. Gültige Werte: <ul style="list-style-type: none"> • yes. Das System erzeugt eine interne UID für den Windows-Benutzer und ermöglicht den Zugriff auf die NAS-Serverdateien über Windows. • no (Standardeinstellung). Die Windows-Authentifizierung schlägt fehl, wenn kein Unix-Standardbenutzername konfiguriert ist.
-defaultUnixUser	Unix-Standardbenutzername oder Unix-ID, durch den bzw. die der Dateizugriff im Multiprotokoll-Freigabemodus gewährt wird. Dieser Benutzername bzw. diese ID wird verwendet, wenn mit dem Zuordnungsmechanismus kein Unix-/Linux-Benutzername bzw. keine Unix-/Linux-ID gefunden wird. Das Unix-ID-Format lautet „@uid=xxxx,gid=yyyy@“, wobei xxxx und yyyy die Zahlenwerte der UID bzw. der primären GID sind. Wenn Sie diese ID verwenden, muss der Benutzer nicht im UDS definiert sein.
-defaultWindowsUser	Windows-Standardbenutzername, der den Dateizugriff im Multiprotokoll-Freigabemodus erlaubt. Dieser Benutzername wird verwendet, wenn der entsprechende Windows-Benutzername -defaultWindowsUser nicht durch den Zuordnungsmechanismus gefunden wird.
-enablePacketReflect	Gibt an, ob die Spiegelung der ausgehenden Pakete (Antwort) über dieselbe Schnittstelle wie eingehende Pakete (Anforderung) aktiviert ist. Gültige Werte: <ul style="list-style-type: none"> • yes • no
-replDest	Replikationszieleinstellungen für den NAS-Server. Gültige Werte: <ul style="list-style-type: none"> • yes • no
-backupOnly	Zeigt an, ob der NAS-Server für Sicherungszwecke zum Einsatz kommt. Nur ein NAS-Replikationszielservers kann nur für Sicherungszwecke eingesetzt werden. Dieses Attribut zeigt an, dass der NAS-Server nicht der Produktionsstandort sein kann. Dies bedeutet, dass sowohl geplantes Failover als auch ungeplantes Failover in der mit dem NAS-Server verbundenen Replikationssitzung nur zur Sicherung nicht zulässig sind. Gültige Werte: <ul style="list-style-type: none"> • yes • no
-preferredProductionOverride	Setzen Sie die „bevorzugte Schnittstelle“-Einstellungen der replizierten Produktionsschnittstellen außer Kraft. Gültige Werte: <ul style="list-style-type: none"> • yes • no
-preferredProductionIPv4	Einstellungen für die bevorzugte Produktions-IPv4-Schnittstelle. Die Schnittstelle muss IPv4 sein und zu diesem Server gehören. Gültige Werte: <ul style="list-style-type: none"> • <Schnittstellen-ID> • auto
-preferredProductionIPv6	Einstellungen für die bevorzugte Produktions-IPv6-Schnittstelle. Die Schnittstelle muss IPv6 sein und zu diesem Server gehören. Gültige Werte: <ul style="list-style-type: none"> • <Schnittstellen-ID> • auto
-preferredBackupIPv4	Einstellungen für die bevorzugte Backup- und Disaster-Recovery-Test-IPv4-Schnittstelle. Die Schnittstelle muss IPv4 sein und zu diesem Server gehören. Gültige Werte: <ul style="list-style-type: none"> • <Schnittstellen-ID> • auto
-preferredBackupIPv6	Einstellungen für die bevorzugte Backup- und Disaster-Recovery-Test-IPv6-Schnittstelle. Die Schnittstelle muss IPv6 sein und zu diesem Server gehören. Gültige Werte: <ul style="list-style-type: none"> • <Schnittstellen-ID> • auto

Beispiel 1

Mit dem folgenden Befehl wird der NAS-Server nas_1 mit den folgenden Einstellungen aktualisiert:

- Aktiviert Multiprotokoll-Shares.
- Verwendet LDAP als Unix-Verzeichnisdienst.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/server -id nas_1 set -mpSharingEnabled yes -unixDirectoryService ldap
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = nas_1
Operation completed successfully.
```

Beispiel 2

Mit dem folgenden Befehl werden die Replikationseinstellungen für NAS-Server nas_1 geändert.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/server -id nas_1 set -replDest yes
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = nas_1
Operation completed successfully.
```

Beispiel 3

Der folgende Befehl ändert den Speicherprozessor in SPB für NAS-Server nas_1.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/server -id nas_1 set -sp spb
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
WARNING: Modifying the NAS server's SP disrupts any running NDMP jobs, and may also result
in data unavailability for some client configurations other than NFS (v3, v4, and v4.1) and
SMB3+CA. The NDMP jobs must be restarted after the SP modification is completed.
Are you sure you want to modify the default SP?
yes / no:yes
```

```
ID = nas_1
Operation completed successfully.
```

ANMERKUNG:

- Wenn der Speicherprozessor bearbeitet wird, wird das NAS-Server-Integritätsattribut zu INFO aktualisiert und das Attribut Integritätsdetails wird zu Transitioning to other Storage Processor aktualisiert. Wenn die Änderung des Speicherprozessors abgeschlossen ist, werden die NAS Server-Integrität und -Integritätsdetails auf die vorherigen Werte zurückgesetzt.
- Eine Änderung am Speicherprozessor kann nicht auf einem NAS-Server durchgeführt werden, der Teil eines aktiven VDM-Dateiimportvorgangs ist. Der Importvorgang muss abgeschlossen sein, bevor der Speicherprozessor geändert werden kann. Andernfalls tritt der folgende Fehler auf: Failed: Cannot complete the operation because the resource is under import. (Error Code:0x900012a).
- Eine Änderung am Speicherprozessor kann nicht auf einem NAS-Server durchgeführt werden, der Teil einer aktiven Replikationssitzung ist. Halten Sie die Replikationssitzung an, nehmen Sie die SP-Änderung vor und setzen Sie die Replikationssitzung dann fort. Andernfalls tritt der folgende Fehler auf: Cannot modify the NAS server's Storage

Processor when there are non-paused replication sessions on the NAS server or its file systems. (Error Code:0x6720665).

Löschen von NAS-Servern

Löschen Sie einen NAS-Server.

Voraussetzungen

Bevor Sie einen NAS-Server löschen können, müssen Sie zunächst alle verknüpften Speicherressourcen löschen.

ANMERKUNG: Durch Löschen eines NAS-Servers werden sämtliche Konfigurationen auf dem NAS-Server entfernt. Die ihn verwendenden Speicherressourcen werden jedoch nicht gelöscht. Ein NAS-Server kann nicht gelöscht werden, wenn ihm Speicherressourcen zugeordnet sind. Nach dem Löschen der Speicherressourcen können die Dateien und Ordner nicht aus Snapshots wiederhergestellt werden. Sichern Sie die Daten aus den Speicherressourcen, bevor Sie sie aus dem System löschen.

Format

```
/net/nas/server {-id <value> | -name <value>} delete [{ -cifsDomUser <value> {-cifsDomPwd <value> | -cifsDomPwdSecure} | -skipUnjoin}]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des zu löschenden NAS-Servers ein.
-name	Geben Sie den Namen des zu löschenden NAS-Servers ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-cifsDomUser	Name des Domainbenutzers. ANMERKUNG: Wenn der NAS-Server noch mit SMB (CIFS)-Servern verbunden ist, geben Sie den SMB-Domainbenutzer an, um ihn von Active Directory zu trennen, bevor Sie den NAS-Server löschen.
-cifsDomPwd	Passwort des Domainbenutzers. ANMERKUNG: Geben Sie das Benutzerpasswort an, wenn Sie den CIFS-Server von der Active-Directory-Domain trennen möchten, bevor Sie ihn löschen.
-cifsDomPwdSecure	Passwort des Domainbenutzers im sicheren Modus. Damit wird der Benutzer aufgefordert, das Passwort einzugeben.
-skipUnjoin	Trennt den SMB-Server nicht von der Active-Directory-Domain, bevor er gelöscht wird.

Beispiel

Mit dem folgenden Befehl wird der NAS-Server nas_1 gelöscht:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/server -id nas_1 delete
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

Operation completed successfully.

Prüfen und Aktualisieren von Benutzerzuordnungen für Multiprotokoll-NAS-Server

Eine Multiprotokollumgebung erfordert folgende Arten von Benutzerzuordnungen:

- Ein Windows-Benutzername, der einem entsprechenden Unix-Benutzernamen zugeordnet ist
- Ein Unix-Benutzername, der einem entsprechenden Windows-Benutzernamen zugeordnet ist, der NFS verwendet, um auf ein Dateisystem zuzugreifen, das mit einer Windows-Zugriffs-Policy konfiguriert ist
- Ein Unix-Benutzername, der keinem entsprechenden Windows-Benutzernamen zugeordnet ist und NFS verwendet, um auf ein Dateisystem zuzugreifen, das mit einer Unix- oder einer nativen Zugriffs-Policy konfiguriert ist

Bei diesem Befehl werden Informationen von LDAP, NIS oder lokalen Dateien verwendet, um alle dem NAS-Server zugeordneten Dateisysteme zu analysieren und die SID-/UID-Zuordnung in allen Nodes zu aktualisieren.

Format

```
/net/nas/server {-id <value> | -name <value>} update [-async] {-userMapping [-dryRun] | -confView}
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des zu aktualisierenden NAS-Servers ein.
-name	Geben Sie den Namen des zu aktualisierenden NAS-Servers ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang asynchron aus.
-userMapping	Für alle CIFS (SMB)-Dateisysteme auf dem NAS-Server, aktualisieren Sie die UID/GID und erzeugen Sie einen Benutzerzuordnungsbericht. Eine neue UID/GID wird von einem Unix-Verzeichnisdienst für den Benutzernamen des Objekteigentümers abgerufen. Der Benutzername wird von Active Directory von der Windows-SID aufgelöst. ANMERKUNG: Quotenmanagement und korrekter Multiprotokolldateizugriff erfordern korrekte Zuordnungen zwischen SIDs und UIDs/GIDs auf der Ebene des NAS-Servers. Da dieser Vorgang für große Dateisysteme sehr lange dauern kann, wird empfohlen, den Qualifizierer <code>-async</code> zu verwenden.
-dryRun	Erzeugen Sie einen Benutzerzuordnungsbericht zum Herunterladen. Wenn Benutzer auf eine Datei oder einen Ordner auf dem NAS-Server über das SMB-Protokoll zugreifen, wird ihre SID-zu-UID/GID-Zuordnung in einer internen Zuordnungsdatenbank gespeichert. Dieser Vorgang parst die Zuordnungsdatenbank und fragt für jeden zugeordneten Benutzer den vorhandenen Unix-Verzeichnisdienst und Active Directory-Domaincontroller ab, um alle Inkonsistenzen zwischen der UID/GID im Unix-Verzeichnisdienst und der in der Datenbank gespeicherten UID/GID zu berichten. Es wird empfohlen, dass Sie den Benutzerzuordnungsbericht erzeugen und überprüfen, bevor Sie Multiprotokoll aktivieren. Dadurch können Sie ermöglichen, dass Ihr Unix-Verzeichnisdienst eine UID/GID für jeden Benutzer zurückgeben kann, dessen Zuordnung inkonsistent ist. Andernfalls können Benutzer mit inkonsistenten Zuordnungen nach der Aktivierung von Multiprotokoll möglicherweise nicht auf Dateien zugreifen, da deren Berechtigungen nicht ermittelt werden können. Außerdem kann der Zugriff auf Objekte, die diese Benutzer über SMB/CIFS erstellt haben, nicht gewährt werden, da die Eigentümer Unix nicht zugeordnet werden können. Wenn die UID/GID-Zuordnung für alle NAS-Server-Dateisysteme aktualisiert werden, wird der Zuordnungsbericht automatisch erneut generiert.

Qualifizierer	Beschreibung
	 ANMERKUNG: Nachdem ein Benutzer erfolgreich auf eine Datei oder einen Ordner auf dem NAS-Server von Windows aus zugreift, wird die UID/GID in der Zuordnungsdatenbank für diesen Benutzer aktualisiert. Die UID/GID wird ebenfalls aktualisiert, wenn der Benutzer auf eine Datei von Unix aus für ein Dateisystem mit einer Windows-Zugriffs-Policy zugreift.
-confView	Erzwingen einer sofortigen Aktualisierung des Snapshot der NAS-Serverkonfiguration. Wenn der NAS-Server als Replikationsziel der synchronen Replikationssitzung fungiert, wird der Konfigurations-Snapshot standardmäßig alle 15 Minuten aktualisiert.

Beispiel 1

Der folgende Befehl erzeugt einen Benutzerzuordnungsbericht für den NAS-Server „nas_1“.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/server -id nas_1 update -async -userMapping
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
Job ID = 76
Job created successfully.
```

Beispiel 2

Mit dem folgenden Befehl wird eine sofortige Aktualisierung des Snapshot des NAS-Servers „nas_1“ erzwungen.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/server -id nas_1 update -confView
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = nas_1
Operation completed successfully.
```

Managen von FTP-Einstellungen

FTP (File Transfer Protocol) ist ein Client-/Serverprotokoll, das über TCP/IP funktioniert und die Dateifreigabe in heterogenen Systemen ermöglicht. SFTP (Secure File Transfer Protocol) bietet sichere Dateiübertragungs- und -bearbeitungsfunktionen durch Verwendung von SSH.

Sie können einen NAS-Server konfigurieren, um Dateien mithilfe des FTP- oder SFTP-Protokolls gemeinsam zu nutzen. Remoteclients können mithilfe eines Unix- oder Windows-Benutzernamens authentifiziert werden. Sie können den FTP-Service auch nutzen, um anonyme Benutzerauthentifizierung zu akzeptieren.

Tabelle 31. FTP- und SFTP-Attribute für einen NAS-Server

Attribut	Beschreibung
NAS server	Zugehöriger NAS-Server-Bezeichner.
FTP enabled	Zeigt an, ob das FTP-Protokoll aktiviert ist. Gültige Werte: <ul style="list-style-type: none"> • yes • no (Standardeinstellung)
SFTP enabled	Zeigt an, ob das SFTP-Protokoll aktiviert ist. Gültige Werte: <ul style="list-style-type: none"> • yes • no (Standardeinstellung)

Tabelle 31. FTP- und SFTP-Attribute für einen NAS-Server (fortgesetzt)

Attribut	Beschreibung
CIFS users enabled	Gibt an, ob Windows (SMB)-Benutzer durch den FTP- oder SFTP-Server authentifiziert werden können. Gültige Werte: <ul style="list-style-type: none"> • yes(Standard) • no
Unix users enabled	Gibt an, ob Unix-Anwender durch den FTP- oder SFTP-Server authentifiziert werden können. Gültige Werte: <ul style="list-style-type: none"> • yes(Standard) • no
Anonymous user enabled	Gibt an, ob der FTP-Server die Authentifizierung anonymer Benutzer unterstützt. Gültige Werte: <ul style="list-style-type: none"> • yes(Standard) • no
Home directory limitation enabled	Gibt an, ob authentifizierte FTP- oder SFTP-Benutzer auf ihre Benutzerverzeichnisse beschränkt sind. Gültige Werte: <ul style="list-style-type: none"> • yes(Standard) • no
Default home directory	Zeigt das Standardbenutzerverzeichnis für die FTP- oder SFTP-Benutzer ohne definiertes oder zugängliches Benutzerverzeichnis an.
Welcome message	Zeigt die Begrüßung an, die FTP- oder SFTP-Benutzern vor der Authentifizierung angezeigt wird.
Message of the day	Zeigt die MOTD an, die angezeigt wird, sobald sich die FTP- oder SFTP-Benutzer anmelden.
Audit enabled	Gibt an, ob der FTP- oder SFTP-Server Auditdateisammlung aktiviert hat. Gültige Werte: <ul style="list-style-type: none"> • yes • no
Audit files directory	Gibt das Verzeichnis an, in dem die Auditdateien für den FTP- oder SFTP-Server gespeichert werden.
Audit file maximum size	Gibt die maximale Dateigröße der Auditdateien an. Wenn der Höchstwert erreicht ist, wird eine neue Auditdatei erstellt.
Allowed hosts	Gibt eine durch Komma getrennte Liste von Host-IP-Adressen an, die auf den FTP- oder SFTP-Server zugreifen dürfen. Es kann sich um eine IPv4-, IPv6- oder Subnetzadresse handeln. Für Subnetze muss die folgende Notationskonvention verwendet werden: <ul style="list-style-type: none"> • 10.0.0.1/10 • 2000:DB1::/10 Netzwerknamen werden ignoriert. i ANMERKUNG: Wenn diese Option angegeben wird, sind FTP-/SFTP-Verbindungen nur für Clients zulässig, deren IP-Adressen sich in der Liste der zulässigen Hosts finden. Allen Clients, deren IP in dieser Liste nicht angegeben ist, wird der Zugriff verweigert. Wenn ein Subnetz in der Liste der zulässigen Hosts definiert ist, muss die Client-IP zu dem angegebenen Subnetz gehören, damit sie eine Verbindung zu dem NAS-Server herstellen darf. Wenn definiert, können abgelehnte Hosts nicht definiert werden.

Tabelle 31. FTP- und SFTP-Attribute für einen NAS-Server (fortgesetzt)

Attribut	Beschreibung
Allowed users	<p>Gibt eine durch Komma getrennte Liste von Benutzernamen an, die auf den FTP- oder SFTP-Server zugreifen dürfen (numerische Benutzer-IDs sind ungültig und werden ignoriert).</p> <p>i ANMERKUNG: Wenn diese Option angegeben wird, sind FTP-/SFTP-Verbindungen nur für die angegebenen Benutzer zulässig. Allen Benutzern, die in dieser Liste nicht aufgeführt sind, wird der Zugriff verweigert. Wenn definiert, können abgelehnte Benutzer nicht definiert werden.</p>
Allowed groups	<p>Gibt eine durch Komma getrennte Liste von Benutzergruppen an, die auf den FTP- oder SFTP-Server zugreifen dürfen. Geben Sie den Namen der Gruppe an (numerische Gruppen-IDs sind ungültig und werden ignoriert).</p> <p>i ANMERKUNG: Wenn diese Option angegeben wird, sind FTP-/SFTP-Verbindungen nur für die aufgeführten Gruppen zulässig. Allen Benutzergruppen, die in dieser Liste nicht aufgeführt sind, wird der Zugriff verweigert. Wenn definiert, können abgelehnte Gruppen nicht definiert werden.</p>
Denied hosts	<p>Gibt eine durch Komma getrennte Liste von Host-IP-Adressen an, die auf den FTP- oder SFTP-Server nicht zugreifen dürfen. Es kann sich um eine IPv4-, IPv6- oder Subnetzadresse handeln.</p> <p>Für Subnetze muss die folgende Notationskonvention verwendet werden:</p> <ul style="list-style-type: none"> • 10.0.0.1/10 • 2000:DB1::/10 <p>Netzwerknamen werden ignoriert.</p> <p>i ANMERKUNG: Wenn diese Option angegeben wird, werden FTP-/SFTP-Verbindungen nur für Clients verweigert, deren IP-Adressen oder Subnetzadressen in dieser Liste enthalten sind. Wenn definiert, können erlaubte Hosts nicht definiert werden.</p>
Denied users	<p>Gibt eine durch Komma getrennte Liste von Benutzernamen an, die auf den FTP- oder SFTP-Server nicht zugreifen dürfen (numerische Benutzer-IDs sind ungültig und werden ignoriert).</p> <p>i ANMERKUNG: Wenn diese Option angegeben wird, werden FTP-/SFTP-Verbindungen nur für die angegebenen Benutzer verweigert. Allen Benutzern, die in dieser Liste nicht aufgeführt sind, wird der Zugriff erlaubt. Wenn definiert, können erlaubte Benutzer nicht definiert werden.</p>
Denied groups	<p>Gibt eine durch Komma getrennte Liste von Benutzergruppen an, die auf den FTP- oder SFTP-Server nicht zugreifen dürfen. Geben Sie den Namen der Gruppe an (numerische Gruppen-IDs sind ungültig und werden ignoriert).</p> <p>i ANMERKUNG: Wenn diese Option angegeben wird, werden FTP-/SFTP-Verbindungen nur für die aufgeführten Gruppen verweigert. Allen Benutzergruppen, die in dieser Liste nicht aufgeführt sind, wird der Zugriff erlaubt. Wenn definiert, können erlaubte Gruppen nicht definiert werden.</p>

Anzeigen von FTP-Einstellungen

Zeigen Sie FTP- oder SFTP-Servereinstellungen für einen NAS-Server an.

Format

```
/net/nas/ftp [-server <value>] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-server	Geben Sie den Namen des zugehörigen NAS-Servers ein.

Beispiel

Mit dem folgenden Befehl werden die FTP-Servereinstellungen für einen NAS-Server angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/ftp show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:   NAS server           = nas_1
     FTP enabled         = yes
     SFTP enabled        = no
     CIFS users enabled  = yes
     Unix users enabled  = yes
     Anonymous user enabled = no
     Homedir limitation enabled = no
     Default home directory = /home/public
     Allowed hosts       = 1.2.3.10,1.2.3.11,192.168.0.0/16,2001:db8::/48
     Allowed users       =
     Allowed groups      =
     Denied hosts        =
     Denied users        = guest,jack,john
     Denied groups       = guests,group1
```

Ändern der FTP-Einstellungen

Ändern Sie vorhandene FTP- oder SFTP-Einstellungen eines NAS-Servers.

Format

```
/net/nas/ftp -server <value> set [-ftpEnabled <value>] [-sftpEnabled <value>] [-cifsUserEnabled <value>] [-unixUserEnabled <value>] [-anonymousUserEnabled <value>] [-homedirLimitEnabled <value>] [-defaultHomedir <value>] [-welcome <value>] [-motd <value>] [-auditEnabled {yes|no}] [-auditDir <value>] [-auditMaxSize <value>] {[[-allowHost <value>] | [-appendAllowHost <value>] | [-removeAllowHost <value>] | [-denyHost <value>] | [-appendDenyHost <value>] | [-removeDenyHost <value>]} {[[-allowUser <value>] | [-appendAllowUser <value>] | [-removeAllowUser <value>] | [-denyUser <value>] | [-appendDenyUser <value>] | [-removeDenyUser <value>]} {[[-allowGroup <value>] | [-appendAllowGroup <value>] | [-removeAllowGroup <value>] | [-denyGroup <value>] | [-appendDenyGroup <value>] | [-removeDenyGroup <value>]}]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-server	Geben Sie den Namen des NAS-Servers ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-ftpEnabled	Gibt an, ob der FTP-Server auf dem NAS-Server aktiviert ist. Gültige Werte: <ul style="list-style-type: none"> • yes • no
-sftpEnabled	Gibt an, ob der SFTP-Server auf dem NAS-Server aktiviert ist. Gültige Werte: <ul style="list-style-type: none"> • yes • no
-cifsUserEnabled	Gibt an, ob Windows (SMB)-Benutzer durch den FTP- oder SFTP-Server authentifiziert werden können. Gültige Werte: <ul style="list-style-type: none"> • yes • no
-unixUserEnabled	Gibt an, ob Unix-Anwender durch den FTP- oder SFTP-Server authentifiziert werden können. Gültige Werte: <ul style="list-style-type: none"> • yes • no
-anonymousUserEnabled	Gibt an, ob der FTP-Server die Authentifizierung anonymer Benutzer unterstützt. Gültige Werte: <ul style="list-style-type: none"> • yes • no
-homedirLimitEnabled	Gibt an, ob authentifizierte FTP- oder SFTP-Benutzer auf ihre Benutzerverzeichnisse beschränkt sind. Gültige Werte: <ul style="list-style-type: none"> • yes • no
-defaultHomedir	Geben Sie das Standard-Home-Verzeichnis für die FTP- oder SFTP-Benutzer ohne definiertes oder zugängliches Benutzerverzeichnis ein.
-welcome	Geben Sie die Begrüßung ein, die FTP- oder SFTP-Anwendern vor der Authentifizierung angezeigt wird.
-motd	Geben Sie die MOTD (Message of the day) ein, die angezeigt wird, sobald die FTP- oder SFTP-Benutzer sich anmelden.
-auditEnabled	Gibt an, ob das FTP-/SFTP-Auditing auf dem NAS-Server aktiviert ist. Gültige Werte: <ul style="list-style-type: none"> • yes • no
-auditDir	Geben Sie das Verzeichnis ein, in dem die Auditdateien gespeichert werden sollen.
-auditMaxSize	Geben Sie die maximale Größe für die Auditprotokolldatei ein. Wenn dieses Maximum überschritten wird, wird eine neue Auditdatei erstellt.
-allowHost	Geben Sie die durch Komma getrennte Liste der zulässigen Clienthost-IP-Adressen ein. Es kann sich um eine IPv4-, IPv6- oder Subnetzadresse handeln. Für Subnetze muss die folgende Notationskonvention verwendet werden: <ul style="list-style-type: none"> • 10.0.0.1/10 • 2000:DB1::/10 Netzwerknamen werden ignoriert.  ANMERKUNG: Wenn diese Option angegeben wird, sind FTP-/SFTP-Verbindungen nur für Clients zulässig, deren IP-Adressen sich in der Liste der zulässigen Hosts finden. Allen Clients, deren IP in dieser Liste nicht angegeben ist, wird der Zugriff verweigert. Wenn ein Subnetz in der Liste der zulässigen Hosts definiert ist, muss die Client-IP zu dem angegebenen Subnetz gehören, damit sie eine Verbindung zu dem NAS-FTP-/SFTP-Server herstellen darf. Wenn -allowHost definiert ist, kann -denyHost nicht definiert werden.
-appendAllowHost	Geben Sie eine oder mehrere durch Komma getrennte Host-IP-Adressen an, die an eine vorhandene Liste von zulässigen Host-IP-Adressen angehängt werden sollen.

Qualifizierer	Beschreibung
-removeAllowHost	Geben Sie eine oder mehrere durch Komma getrennte Host-IP-Adressen an, die von einer vorhandenen Liste von zulässigen Host-IP-Adressen entfernt werden sollen.
-denyHost	Geben Sie die durch Komma getrennte Liste der Clienthost IP-Adressen ein, denen der Zugriff auf den FTP-/SFTP-Server verweigert wird. Es kann sich um eine IPv4-, IPv6- oder Subnetzadresse handeln. Für Subnetze muss die folgende Notationskonvention verwendet werden: <ul style="list-style-type: none"> • 10.0.0.1/10 • 2000:DB1::/10 Netzwerknamen werden ignoriert. <i>i</i> ANMERKUNG: Wenn diese Option angegeben wird, werden FTP-/SFTP-Verbindungen nur den Clients verweigert, deren IP-Adressen auf dieser -denyHost-Liste aufgeführt sind. Allen Clients, deren IP in dieser Liste nicht angegeben ist, wird der Zugriff erlaubt. Wenn ein Subnetz in der Liste der abgelehnten Hosts definiert ist, wird Client-IP-Adressen, die zu dem angegebenen Subnetz gehören, der Zugriff auf den NAS-FTP-/SFTP-Server verweigert. Wenn -denyHost definiert ist, kann -allowHost nicht definiert werden.
-appendDenyHost	Geben Sie eine oder mehrere durch Komma getrennte Host-IP-Adressen an, die an eine vorhandene Liste von nicht zulässigen Host-IP-Adressen angehängt werden sollen.
-removeDenyHost	Geben Sie eine oder mehrere durch Komma getrennte Host-IP-Adressen an, die von einer vorhandenen Liste von nicht zulässigen Host-IP-Adressen entfernt werden sollen.
-allowUser	Geben Sie die durch Komma getrennte Liste von Benutzernamen an, die auf den FTP-/SFTP-Server zugreifen dürfen (numerische Benutzer-IDs sind ungültig und werden ignoriert). <i>i</i> ANMERKUNG: Wenn diese Option angegeben wird, sind FTP-/SFTP-Verbindungen nur für die angegebenen Benutzer zulässig. Allen Benutzern, die in dieser Liste nicht aufgeführt sind, wird der Zugriff verweigert. Wenn -allowUser definiert ist, kann -denyUser nicht definiert werden.
-appendAllowUser	Geben Sie einen oder mehrere durch Komma getrennte Benutzernamen an, die an eine vorhandene Liste von zulässigen Benutzern angehängt werden sollen.
-removeAllowUser	Geben Sie einen oder mehrere durch Komma getrennte Benutzernamen an, die von einer vorhandenen Liste von zulässigen Benutzern entfernt werden sollen.
-denyUser	Geben Sie die durch Komma getrennte Liste von Benutzernamen an, die auf den FTP-/SFTP-Server nicht zugreifen dürfen (numerische Benutzer-IDs sind ungültig und werden ignoriert). <i>i</i> ANMERKUNG: Wenn diese Option angegeben wird, werden FTP-/SFTP-Verbindungen nur für die angegebenen Benutzer verweigert. Allen Benutzern, die in dieser Liste nicht aufgeführt sind, wird der Zugriff verweigert. Wenn -denyUser definiert ist, kann -allowUser nicht definiert werden.
-appendDenyUser	Geben Sie einen oder mehrere durch Komma getrennte Benutzernamen an, die an eine vorhandene Liste von nicht zulässigen Benutzern angehängt werden sollen.
-removeDenyUser	Geben Sie einen oder mehrere durch Komma getrennte Benutzernamen an, die von einer vorhandenen Liste von nicht zulässigen Benutzern entfernt werden sollen.
-allowGroup	Geben Sie die durch Komma getrennte Liste von Benutzergruppennamen an, die auf den FTP-/SFTP-Server zugreifen dürfen (numerische Gruppen-IDs sind ungültig und werden ignoriert). <i>i</i> ANMERKUNG: Wenn diese Option angegeben wird, sind FTP-/SFTP-Verbindungen nur für die aufgeführten Gruppen zulässig. Allen Benutzergruppen, die in dieser Liste nicht aufgeführt sind, wird der Zugriff verweigert. Wenn -allowGroup definiert ist, kann -denyGroup nicht definiert werden.
-appendAllowGroup	Geben Sie einen oder mehrere durch Komma getrennte Benutzergruppennamen an, die an eine vorhandene Liste von zulässigen Gruppen angehängt werden sollen.
-removeAllowGroup	Geben Sie einen oder mehrere durch Komma getrennte Benutzergruppennamen an, die von einer vorhandenen Liste von zulässigen Gruppen entfernt werden sollen.
-denyGroup	Geben Sie die durch Komma getrennte Liste von Benutzergruppennamen an, die nicht auf den FTP-/SFTP-Server zugreifen dürfen (numerische Gruppen-IDs sind ungültig und werden ignoriert).

Qualifizierer	Beschreibung
	i ANMERKUNG: Wenn diese Option angegeben wird, werden FTP-/SFTP-Verbindungen nur für die aufgeführten Gruppen verweigert. Allen Benutzergruppen, die in dieser Liste nicht aufgeführt sind, wird der Zugriff erlaubt. Wenn <code>-denyGroup</code> definiert ist, kann <code>-allowGroup</code> nicht definiert werden.
<code>-appendDenyGroup</code>	Geben Sie einen oder mehrere durch Komma getrennte Benutzergruppennamen an, die an eine vorhandene Liste von nicht zulässigen Gruppen angehängt werden sollen.
<code>-removeDenyGroup</code>	Geben Sie einen oder mehrere durch Komma getrennte Benutzergruppennamen an, die von einer vorhandenen Liste von nicht zulässigen Gruppen entfernt werden sollen.

Beispiel 1

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/ftp -server nas_1 set -ftpEnabled
yes -sftpEnabled no -cifsUserEnabled yes -unixUserEnabled yes -anonymousUserEnabled no
-homedirLimitEnabled no -defaultHomedir /home/public -welcome "Welcome to this awesome server"
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
Operation completed successfully.
```

Beispiel 2

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/ftp -server nas_1 set -denyUser
"guest,jack,john" -appendAllowHost 1.2.3.4,1.2.3.5
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
Operation completed successfully.
```

Managen von LDAP-Einstellungen eines NAS-Servers

Das Lightweight Directory Access Protocol (LDAP) ist ein Anwendungsprotokoll zur Durchführung von Abfragen und Änderungen in Verzeichnisservices in TCP/IP-Netzwerken. LDAP ermöglicht ein zentrales Management zur Netzwerkauthentifizierung und zur Autorisierung, da das Benutzer- und Gruppenmanagement im gesamten Netzwerk zusammengefasst wird.

Sie können einen NAS-Server konfigurieren, um LDAP oder NIS als Unix-Verzeichnisdienst zu verwenden, um Benutzer zuzuordnen, Netzwerkgruppen abzurufen und um Unix-Anmeldedaten zu erstellen. Wenn eine anfängliche LDAP-Konfiguration angewendet wird, überprüft das System den Typ des LDAP-Servers. Er kann ein Active Directory-Schema (IDMU), IPLANET-Schema oder ein RFC 2307 (offenes LDAP)-Schema sein. Standardmäßig wird das RFC 2307-Schema erzeugt. Sobald das Schema erkannt wurde, wird es in einer Datei „ldap.conf“ gespeichert. Sie können dieses LDAP-Schema herunterladen, es basierend auf Ihren Anforderungen bearbeiten und es mithilfe der CLI-Befehle, die in diesem Abschnitt erwähnt wurden, erneut hochladen.

In der folgenden Tabelle sind die Attribute für LDAP-Einstellungen für einen NAS-Server aufgeführt.

Tabelle 32. LDAP-Einstellungen für einen NAS-Server

Attribut	Beschreibung
<code>NAS server</code>	Eindeutige Kennung des zugehörigen NAS-Servers. Das LDAP-Clientkonfigurationsobjekt wird durch die NAS-Server-ID identifiziert.
<code>Servers</code>	Geben Sie die IP-Adressen der zugehörigen LDAP-Server ein. Wenn Sie möchten, dass der NAS-Server die DNS-Serviceerkennung verwendet, um die IP-Adressen des LDAP-

Tabelle 32. LDAP-Einstellungen für einen NAS-Server (fortgesetzt)

Attribut	Beschreibung
	<p>Servers automatisch abzurufen, geben Sie keinen Wert für diese Option an.</p> <p>i ANMERKUNG: Damit dieser automatische Erkennungsprozess funktioniert, muss der DNS-Server Pointer für die LDAP-Server enthalten und die LDAP-Server müssen die gleichen Authentifizierungseinstellungen verwenden.</p>
Port	<p>Der TCP/IP-Port, den der NAS-Server verwendet, um sich mit dem LDAP-Server zu verbinden. Der Standardwert für LDAP ist 389 und der für LDAPS ist 636.</p>
Protocol	<p>Typ des LDAP-Protokolls. Gültige Werte:</p> <ul style="list-style-type: none"> • ldap • ldaps <p>Verwenden Sie ldaps für eine sichere SSL-Verbindung.</p>
Authentication type	<p>Authentifizierungstyp für den LDAP-Server. Gültige Werte:</p> <ul style="list-style-type: none"> • anonymous • kerberos • simple
Verify certificate	<p>Gibt an, ob das Zertifikat der Zertifizierungsstelle zum Überprüfen des LDAP-Serverzertifikats für sichere SSL-Verbindungen verwendet wird. Gültige Werte:</p> <ul style="list-style-type: none"> • yes • no <p>Der Wert wird als leer angezeigt, wenn das LDAP-Protokoll ausgewählt ist (ohne SSL). Der Wert ist standardmäßig „yes“, wenn das LDAPS-Protokoll verwendet wird.</p>
Use CIFS account (gilt für Kerberos-Authentifizierung)	<p>Gibt an, ob CIFS-Authentifizierung verwendet wird, um den LDAP-Server zu authentifizieren. Gültige Werte:</p> <ul style="list-style-type: none"> • yes: Zeigt an, dass die CIFS (SMB)-Einstellungen für die Kerberos-Authentifizierung verwendet werden. Diese Option wird häufig verwendet, wenn IDMU als ein Unix-Verzeichnisdienst konfiguriert wird. • no: Zeigt an, dass Kerberos seine eigenen Einstellungen verwendet. Siehe Konfigurieren von Kerberos-Einstellungen, um die Authentifizierung über den Kerberos-Bereich zu konfigurieren.
Principal (gilt für Kerberos-Authentifizierung)	<p>Gibt den prinzipiellen Namen für die Kerberos-Authentifizierung an.</p>
Realm (gilt für Kerberos-Authentifizierung)	<p>Gibt den Namen des Bereichs für die Kerberos-Authentifizierung an.</p>
Password (gilt für Kerberos-Authentifizierung)	<p>Gibt das zugehörige Passwort für die Kerberos-Authentifizierung an.</p>
Bind DN (gilt für einfache Authentifizierung)	<p>Gibt den Distinguished Name (DN) an, der beim Binden verwendet wird.</p>
Bind password (gilt für einfache Authentifizierung)	<p>Gibt das zugehörige Passwort an, das beim Binden verwendet wird.</p>
Base DN	<p>Gibt den DN des Root-Levels in der Verzeichnisstruktur in RFC-Notation an oder gibt den Domainnamen mit Punkten an.</p>
Profile DN	<p>Gibt für einen iPlanet LDAP-Server den DN des Eintrags mit dem Konfigurationsprofil an.</p>
Replication sync	<p>Gibt den Status der LDAP-Serveradressenliste in dem NAS-Server an, der als Replikationsziel fungiert. Wenn eine Liste replizierter</p>

Tabelle 32. LDAP-Einstellungen für einen NAS-Server (fortgesetzt)

Attribut	Beschreibung
	<p>LDAP-Server auf dem Quell-NAS-Server erstellt wird, wird sie automatisch auf dem Ziel synchronisiert. Gültige Werte:</p> <ul style="list-style-type: none"> • <code>Not replicated</code>: LDAP-Liste ist nicht auf dem Ziel repliziert. • <code>Auto synchronized</code>: LDAP-Liste wird automatisch auf dem Replikationsziel synchronisiert. Alle Änderungs- oder Löschvorgänge auf der Quelle werden automatisch auf dem Ziel wiedergegeben. • <code>Overridden</code>: LDAP-Liste wurde manuell geändert oder auf dem Replikationsziel außer Kraft gesetzt. Änderungen oder Löschungen von Adressen auf der LDAP-Liste auf dem Quell-NAS-Server haben keinen Einfluss auf die außer Kraft gesetzte LDAP-Liste auf dem Replikationsziel. <p>ANMERKUNG: Wenn eine LDAP-Liste deaktiviert oder von der Quelle gelöscht wird, kann eine außer Kraft gesetzte LDAP-Liste auf dem Ziel nicht automatisch deaktiviert oder gelöscht werden.</p>
Source servers	Liste der LDAP-Server-IP-Adressen, die auf der Replikationsquelle definiert sind.

Anzeigen von LDAP-Einstellungen eines NAS-Servers

Zeigen Sie LDAP-Einstellungen eines NAS-Servers an.

Format

```
/net/nas/ldap [-server <value>] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-server	Name des zugehörigen NAS-Servers.

Beispiel

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/ldap -server nas_1 show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1: NAS server      = nas_1
   IP address     = 10.64.74.64, 10.64.74.74
   Port          = 636
   Protocol      = ldaps
   Authentication = simple
   Use CIFS account =
   Principal     =
   Realm        =
   Bind DN       = cn=adminstrator,cn=User,dc=emc,dc=com
   Base DN       = dc=emc,dc=com
   Profile DN    =
   Replication sync = Not replicated
   Source servers =
```

Ändern der LDAP-Einstellungen eines NAS-Servers

Ändern Sie die LDAP-Einstellungen eines NAS-Servers.

Format

```
/net/nas/ldap -server <value> set {-enabled no | [ -ip <value>] [-addr <value>] [-port <value>]
[-protocol {ldap | ldaps}] [-verifyCert {yes | no}] [-authType {anonymous | kerberos {-
useCifsAccount | -principal <value> [-realm <value>] [{"-password <value> | -passwordSecure }]}
| simple [-bindDn <value> {-bindPasswd <value> | -bindPasswdSecure}]]} [-baseDn <value>] [-
profileDn <value>]} [-replSync {auto | overridden}]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-server	Identifiziert den zugehörigen NAS-Server.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-enabled	Geben Sie diese Option an, um LDAP für einen vorhandenen NAS-Server zu deaktivieren. Der gültige Wert lautet no.  ANMERKUNG: Wenn der Wert auf „no“ festgelegt wird, werden die LDAP-Einstellungen für einen vorhandenen NAS-Server entfernt.
-ip	Geben Sie die IP-Adressen (getrennt durch Komma) der zugehörigen LDAP-Server ein. Wenn Sie möchten, dass der NAS-Server die DNS-Serviceerkennung verwendet, um die IP-Adressen des LDAP-Servers automatisch abzurufen, geben Sie keinen Wert für diese Option an.  ANMERKUNG: Damit dieser automatische Erkennungsprozess funktioniert, muss der DNS-Server Pointer für die LDAP-Server enthalten und die LDAP-Server müssen die gleichen Authentifizierungseinstellungen verwenden.
-addr	Geben Sie die LDAP-Serveradresse ein, die entweder eine IP-Adresse oder ein vollständig qualifizierter Domainname (FQDN) sein kann.
-port	Geben Sie den Port ein, der dem LDAP-Server zugewiesen ist. Wenn LDAPS verwendet wird, ist die Standardeinstellung 636. Wenn LDAP verwendet wird, ist der Standardport 389.
-protocol	Verwenden Sie LDAPS für eine sichere SSL-Verbindung.
-verifyCert	Geben Sie an, dass hochgeladene Zertifikate der Zertifizierungsstelle (CA) verwendet werden sollen, um die Zertifikate von LDAP-Servern zur Herstellung sicherer SSL-Verbindungen zu verifizieren. Gültige Werte: <ul style="list-style-type: none"> • yes • no Dies gilt nur, wenn das Protokoll LDAPS ist. Der Wert wird leer angezeigt, wenn LDAP (ohne SSL) verwendet wird.
-authType	Geben Sie die Art der Authentifizierung für den LDAP-Server an. Gültige Werte: <ul style="list-style-type: none"> • anonymous • kerberos • simple
-bindDn (nur gültig, wenn die simple-Authentifizierung verwendet wird)	Geben Sie den Distinguished Name (DN) für die Anbindung an den Server ein.

Qualifizierer	Beschreibung
-bindPasswd (nur gültig, wenn die simple-Authentifizierung verwendet wird)	Geben Sie das zugehörige Passwort für die Anbindung an den Server ein.
-bindPasswdSecure (nur gültig, wenn die simple-Authentifizierung verwendet wird)	Geben Sie das Passwort im sicheren Modus ein. Sie werden aufgefordert, das Passwort gesondert einzugeben.
-useCifsAccount (nur gültig, wenn die kerberos-Authentifizierung verwendet wird)	Geben Sie an, ob Sie CIFS (SMB)-Authentifizierung verwenden möchten. Nur für Kerberos-Anmeldeauthentifizierung. Wird häufig verwendet, um NAS-Server so zu konfigurieren, dass sie IDMU als UNIX-Verzeichnisdienst verwenden. (Wählen Sie simple-Authentifizierung, um Active Directory authentifizieren, ohne ein CIFS-Konto zu verwenden.)
-principal (nur gültig, wenn die kerberos-Authentifizierung verwendet wird)	Geben Sie den Principal-Namen für die Kerberos-Authentifizierung ein.
-realm (nur gültig, wenn die kerberos-Authentifizierung verwendet wird)	Geben Sie den Bereichsnamen für die Kerberos-Authentifizierung ein.
-password (nur gültig, wenn die kerberos-Authentifizierung verwendet wird)	Geben Sie das zugehörige Passwort für die Kerberos-Authentifizierung ein.
-baseDn	Geben Sie den DN des Root-Levels in der Verzeichnisstruktur in RFC-Notation ein oder geben Sie den Domainnamen mit Punkten ein. Gültige Notationsformate: <ul style="list-style-type: none"> • RFC, z. B. <dc=nt2k80,dc=drm,dc=lab,dc=emc,dc=com> • Gepunkteter Domainname, z. B. <nt2k80.drm.lab.emc.com>
-profileDn	Geben Sie für einen iPlanet-LDAP-Server den DN des Eintrags mit dem Konfigurationsprofil ein.
-replSync	Status der LDAP-Serveradressenliste in dem NAS-Server, der als Replikationsziel fungiert. Gültige Werte: <ul style="list-style-type: none"> • auto • overridden

Beispiel

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/ldap -server nas_1 set -ip
10.64.74.64,10.64.74.74 -addr example.domain.com -port 636 -protocol ldaps -authType simple
-bindDn "cn=administrator,cn=User,dc=emc,dc=com" -bindPasswd "Ldap123!" -baseDn "dc=mec,dc=com"
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
Operation completed successfully.
```

Hochladen eines LDAP-Schemas

Sie können das LDAP-Schema für Ihren NAS-Server anpassen und die neue Schemadatei hochladen. Sobald das Schema hochgeladen ist, wird seine Gültigkeit überprüft. Wenn das Schema gültig ist, wird es angewendet, und die LDAP-Konfiguration Ihres NAS-Servers wird geändert.

Beispiel

```
uemcli -upload -f "LDAP_nas_1.conf" -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/ldap -server nas_1 -type config
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Herunterladen eines LDAP-Schemas

Wenn eine anfängliche LDAP-Konfiguration angewendet wird, überprüft das System den Typ des LDAP-Servers. Sobald das Schema erkannt wurde, wird es in einer `ldap.conf`-Datei gespeichert. Sie können dieses LDAP-Schema mithilfe der Option `-download` herunterladen und es nach Ihren Anforderungen anpassen. Weitere Informationen über Optionen finden Sie unter [Befehlszeilenoptionen](#).

Beispiel

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! -download /net/nas/ldap -server nas_1 -type config
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Hochladen eines Zertifikats der Zertifizierungsstelle

Sie können Zertifikate einer Zertifizierungsstelle (CA) für Ihre NAS-LDAP-Server hochladen. Nachdem Sie das CA-Zertifikat hochgeladen haben, kann es zur Validierung von Zertifikaten eines LDAP-Servers verwendet werden.

Beispiel

```
uemcli -upload -f "MyCert.pem" -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/ldap -server nas_1 -type CACertificate
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Herunterladen eines Zertifikats der Zertifizierungsstelle

Ein Zertifikat der Zertifizierungsstelle (CA) wird zur Validierung von Zertifikaten eines LDAP-Servers verwendet.

Beispiel

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! -download /net/nas/ldap -server nas_1 -type CACertificate
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Managen von NAS-Schnittstellen

NAS-Schnittstellen repräsentieren die Netzwerkschnittstelle, die auf einem Ethernetport für NAS-Server konfiguriert wurde.

Tabelle 33. Schnittstellenattribute

Attribut	Beschreibung
ID	Die ID der Schnittstelle.
NAS server	Kennung des NAS-Servers.
Preferred	<p>Stellt die Netzwerkschnittstelle als bevorzugte Quelle für ausgehenden Datenverkehr ein. Alle ausgehenden DNS- oder Active Directory-Anforderungen werden über diese Schnittstelle weitergeleitet und die IP-Adresse, die dieser Schnittstelle zugewiesen ist, wird als Quelladresse der Datenpakete verwendet. Für jeden NAS-Server können Sie eine einzige IP-Adresse als bevorzugt auswählen. Gültige Werte:</p> <ul style="list-style-type: none"> • yes • no <p> ANMERKUNG: Dieses Attribut gilt nur für Dateischnittstellen.</p>
Port	Die ID des physischen Ports bzw. der Verbindungsbündelung auf einem SP, auf dem die Schnittstelle ausgeführt wird. In der ID sind der Name des Ports und des SP enthalten.
VLAN ID	<p>Die ID des virtuellen lokalen Netzwerks (VLAN) der Schnittstelle. In der Schnittstelle wird diese ID zur Annahme von Paketen mit VLAN-Tags verwendet. Der Wertebereich erstreckt sich von 1 bis 4095.</p> <p>Für IP-Mehrmandantenfähigkeit muss die VLAN-ID einer NAS-Server-Schnittstelle mit dem Satz von VLAN-IDs übereinstimmen, die einem Mandanten zugewiesen sind, zu dem der NAS-Server gehört. Nur nicht zugewiesene VLAN-IDs sind für NAS-Server zulässig, die nicht zu einem Mandanten gehören.</p> <p> ANMERKUNG: Falls keine VLAN-ID angegeben ist (der Standardwert), verfügen die Pakete nicht über VLAN-Tags. Weitere Informationen zu VLANs finden Sie in der Unisphere-Onlinehilfe.</p>
VLAN MTU size	Aktuelle VLAN-MTU-Größe.
IP address	IPv4- oder IPv6-Adresse.
Subnet mask	IPv4-Subnetzmaske.
Gateway	IPv4- oder IPv6-Gateway.
MAC address	MAC-Adresse der Schnittstelle.
SP	SP, der die Schnittstelle verwendet.
Role	<p>Gibt die Verwendung der Dateischnittstelle an. Gültige Werte:</p> <ul style="list-style-type: none"> • production • backup <p>Backupschnittstellen sind nur für Backups über NFS- und NDMP-Protokolle verfügbar und nicht für das CIFS (SMB)-Protokoll. Schnittstellen, die NAS-Servern in einer Replikationssitzung zugeordnet sind, werden über die Replikationssitzung nicht repliziert. Sie können eine Backupschnittstelle auf dem Ziel-NAS-Server erstellen. Im Gegensatz zu Produktionsschnittstellen werden Backupschnittstellen sofort auf dem Ziel-NAS-Server aktiviert und ermöglichen Ihnen, Backup und Disaster Recovery per NFS-Share über den Snapshot zu testen.</p>
Replication sync	<p>Gilt für Produktionsschnittstellen, die über Replikationssitzungen repliziert werden. Gültige Werte:</p> <ul style="list-style-type: none"> • Not replicated • Auto synchronized: Gibt an, dass diese Schnittstelle automatisch über die Replikationssitzung auf dem Ziel synchronisiert wird. Alle Änderungs- und Löschvorgänge auf der Quelle werden automatisch auf dem Ziel wiedergegeben. • Overridden: Gibt an, dass diese Schnittstelle auf der Zielseite manuell geändert/außer Kraft gesetzt wird.

Tabelle 33. Schnittstellenattribute (fortgesetzt)

Attribut	Beschreibung
	<p>Wenn eine Replikationsproduktionschnittstelle auf dem Quell-NAS-Server erstellt wird, wird sie auf dem Ziel automatisch synchronisiert.</p> <p>i ANMERKUNG: Änderungen oder Löschungen von Netzwerkeinstellungen der entsprechenden Quell-IP-Schnittstellen haben keine Auswirkung auf eine außer Kraft gesetzte Schnittstelle auf dem Ziel. Wenn allerdings eine Schnittstelle auf der Quelle gelöscht wird, reagieren außer Kraft gesetzte Schnittstellen nicht mehr und die Integritätsstatuswerte solcher Schnittstellen werden herabgestuft oder/und es kommt zu Warnmeldungen. Dies liegt daran, dass die SMB/CIFS-Shares eng auf die Produktions-IP-Schnittstellen festgelegt sind und nach einem Failover nicht über außer Kraft gesetzte Schnittstellen funktionieren.</p>
Health state	<p>Ein numerischer Wert, der die Integrität des Systems angibt. Gültige Werte:</p> <ul style="list-style-type: none"> • Unknown (0) • OK (5) • OK BUT (7) • Degraded/Warning (10) • Minor failure (15) • Major failure (20)
Health details	Zusätzliche Integritätsinformationen.
Source VLAN ID	Gibt den Wert der entsprechenden VLAN-ID an, wie in einer Replikationssitzung auf dem Quell-NAS-Server definiert.
Source IP address	Gibt den Wert der entsprechenden IP-Adresse an, wie in einer Replikationssitzung auf dem Quell-NAS-Server definiert.
Source subnet mask	Gibt den Wert der entsprechenden Subnetzmaske an, wie in einer Replikationssitzung auf dem Quell-NAS-Server definiert.
Source gateway	Gibt den Wert des entsprechenden Gateways an, wie in einer Replikationssitzung auf dem Quell-NAS-Server definiert.

Erstellen einer NAS-Schnittstelle

Erstellen Sie eine NAS-Schnittstelle.

Format

```
/net/nas/if create [-vlanId <value>] {-server <value> | -serverName <value>} [-preferred] -port <value> -addr <value>] [-netmask <value>] [-gateway <value>] [-role {production | backup}]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-server	<p>Kennung des NAS-Servers.</p> <p>i ANMERKUNG: Ein NAS-Server darf nur eine IPv4-Schnittstelle und eine IPv6-Schnittstelle aufweisen.</p>
-serverName	<p>Name des NAS-Servers.</p> <p>i ANMERKUNG: Ein NAS-Server darf nur eine IPv4-Schnittstelle und eine IPv6-Schnittstelle aufweisen.</p>
-preferred	<p>Geben Sie diesen Qualifizierer an, um die Netzwerkschnittstelle als bevorzugte Quelle für ausgehenden Verkehr festzulegen. Das heißt, dass alle ausgehenden DNS- oder Active Directory-Anforderungen über die als bevorzugt gekennzeichnete Schnittstelle weitergeleitet werden, und dass die IP-Adresse, die dieser Schnittstelle zugewiesen ist, als Quelladresse der Datenpakete verwendet wird.</p>

Qualifizierer	Beschreibung
	<p>i ANMERKUNG: Für jeden NAS-Server können Sie eine IPv4- und eine IPv6-Schnittstelle als bevorzugte Schnittfläche wählen.</p>
-port	<p>Geben Sie die ID des SP-Ports bzw. der Linkzusammenfassung für die Schnittstelle ein.</p> <p>i ANMERKUNG: Bei Systemen mit zwei Speicherprozessoren wird eine Dateischnittstelle eher auf einem Paar symmetrischer Ethernetports (oder Linkzusammenfassungen) als auf einem einzelnen angegebenen Port erstellt. Der aktuelle Port wird durch den SP des NAS-Servers definiert und kann von dem angegebenen Port abweichen (z. B. wenn der Benutzer „spa_eth2“ angibt, aber der derzeitige SP des NAS-Servers SP B ist, dann wird die Schnittstelle stattdessen auf „spb_eth2“ erstellt).</p>
-vlanId	<p>Geben Sie die ID des virtuellen LAN (VLAN) für die Schnittstelle ein. In der Schnittstelle wird diese ID zur Annahme von Paketen mit VLAN-Tags verwendet. Der Wertebereich erstreckt sich von 1 bis 4.095.</p> <p>i ANMERKUNG: Falls keine VLAN-ID angegeben ist (Standardeinstellung), verfügen die Pakete nicht über VLAN-Tags. Weitere Informationen zu VLANs finden Sie in der Unisphere-Onlinehilfe.</p>
-addr	<p>Geben Sie die IP-Adresse für die Schnittstelle ein. Die Präfixlänge sollte an die IPv6-Adresse angehängt werden. Wenn sie ausgelassen wird, beträgt sie standardmäßig 64. Die Standardpräfixlänge für IPv4-Adressen ist 24. Die IPv4-Netzmaske kann im Adressenattribut nach dem Schrägstrich angegeben werden.</p>
-netmask	<p>Geben Sie die Subnetzmaske für die Schnittstelle an.</p> <p>i ANMERKUNG: Dieser Qualifizierer ist nicht erforderlich, wenn die Präfixlänge im Attribut -addr festgelegt ist.</p>
-gateway	<p>Geben Sie das Gateway für die Schnittstelle ein.</p> <p>i ANMERKUNG: Dieser Qualifizierer konfiguriert das Standardgateway für den angegebenen SP des Ports.</p>
-role	<p>Geben Sie die Rolle der Schnittstelle an. Gültige Werte:</p> <ul style="list-style-type: none"> • production (Standardeinstellung) • backup <p>i ANMERKUNG: Um eine Schnittstelle auf einem NAS-Server als Replikationsziel zu erstellen, geben Sie den Wert als backup an.</p>

Beispiel

Mit dem folgenden Befehl wird eine NAS-Schnittstelle erstellt. Die Schnittstelle erhält die ID IF_2:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/if create -server nas_1 -port eth0_SPA -addr 10.0.0.1 -netmask 255.255.255.0
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = IF_2
Operation completed successfully.
```

Anzeigen von NAS-Schnittstellen

Zeigen Sie eine Liste von NAS-Schnittstellen im System an. Sie können nach der Schnittstellen-ID filtern.

i **ANMERKUNG:** Aktionsbefehl „show“ erläutert, wie das Ausgabeformat geändert wird.

Format

```
/net/nas/if [ {-id <value> | -port <value> | -server <value> | -serverName <value>} ] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID einer Schnittstelle ein.
-port	Geben Sie den Port ein, mit dem die Schnittstelle verknüpft ist.
-server	Geben Sie den NAS-Server ein, mit dem die Schnittstelle verknüpft ist.
-serverName	Geben Sie den Namen des NAS-Servers ein, mit dem die Schnittstelle verknüpft ist.

Beispiel 1

Mit dem folgenden Befehl werden sämtliche NAS-Schnittstellen im System angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/if show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      ID                = if_0
      NAS server         = nas_0
      Preferred          = yes
      Port               = eth2_spa
      VLAN ID            =
      IP address         = 3ffe:80c0:22c:4e:a:0:2:7f/64
      Subnet mask        =
      Gateway            = fe80::20a8bff:fe5a:967c
      SP                 = SPA
      Health state       = OK (5)

2:      ID                = if_1
      NAS server         = nas_1
      Preferred          = yes
      Port               = eth3_spb
      VLAN ID            = 1
      IP address         = 192.168.1.2
      Subnet mask        = 255.255.255.0
      Gateway            = 192.168.1.254
      SP                 = SPA
      Health state       = OK (5)
```

Beispiel 2

Mit dem folgenden Befehl werden sämtliche NAS-Schnittstellen im System angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/if show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      ID                = if_0
      NAS server         = nas_0
      Preferred          = yes
      Port               = eth2_spa
      VLAN ID            =
      VLAN MTU size      =
      IP address         = 3ffe:80c0:22c:4e:a:0:2:7f/64
      Subnet mask        =
      Gateway            = fe80::20a8bff:fe5a:967c
      MAC address        = 00-0C-29-9C-B3-33
      SP                 = SPA
      Health state       = OK (5)
      Health details     =
```

```

Role = production
Replication sync = Not replicated
Source VLAN ID =
Source IP address =
Source subnet mask =
Source gateway =

2: ID = if_1
NAS server = nas_1
Preferred = yes
Port = eth3_spb
VLAN ID = 1
VLAN MTU size = 1500
IP address = 192.168.1.2
Subnet mask = 255.255.255.0
Gateway = 192.168.1.254
MAC address = 00-0C-29-9C-B3-34
SP = SPA
Health state = OK (5)
Health details =
Role = production
Replication sync = Overridden
Source VLAN ID = 1
Source IP address = 10.0.1.2
Source subnet mask = 255.255.255.0
Source gateway = 10.0.1.1

```

Ändern der Einstellungen der NAS-Schnittstelle

Ändern Sie die Einstellungen für eine NAS-Schnittstelle.

Format

```

/net/nas/if -id <value> set [-vlanId <value>] [-addr <value>] [-netmask <value>] [-gateway <value>] [-preferred] [-replSync {auto | overridden}]

```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID der zu ändernden Schnittstelle ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-vlanId	Geben Sie die ID des virtuellen LAN (VLAN) für die Schnittstelle an. In der Schnittstelle wird diese ID zur Annahme von Paketen mit VLAN-Tags verwendet. Der Wertebereich erstreckt sich von 1 bis 4095.  ANMERKUNG: Falls keine VLAN-ID angegeben ist (der Standardwert), verfügen die Pakete nicht über VLAN-Tags. Weitere Informationen zu VLANs finden Sie in der Unisphere-Onlinehilfe.
-addr	Geben Sie die IP-Adresse für die Schnittstelle an.  ANMERKUNG: Die Präfixlänge sollte an die IPv6-Adresse angehängt werden. Die IPv4-Netzmaske kann im Adressenattribut nach dem Schrägstrich angegeben werden.
-netmask	Geben Sie die IPv4-Subnetzmaske für die Schnittstelle an.
-gateway	Geben Sie das Gateway für die Schnittstelle an.  ANMERKUNG: Das Gateway ist für IPv4 und IPv6 optional. Dieser Qualifizierer konfiguriert das Standardgateway für den angegebenen SP des Ports.

Qualifizierer	Beschreibung
-preferred	Geben Sie diesen Qualifizierer an, um die Netzwerkschnittstelle als bevorzugte Quelle für ausgehenden Verkehr festzulegen. Für jeden NAS-Server können Sie eine IPv4- und eine IPv6-Schnittstelle als bevorzugte Schnittfläche wählen.  ANMERKUNG: Dieses Attribut gilt nur für Dateischnittstellen.
-replSync	Dies gilt nur für NAS-Server, die als Replikationsziel fungieren. Jede Änderung an der Netzwerkadresseninformation führt dazu, dass die Schnittstelle automatisch in den Modus „overridden“ wechselt. Gültige Werte: <ul style="list-style-type: none"> • auto • overridden Beachten Sie Folgendes: <ul style="list-style-type: none"> • Verwenden Sie diesen Qualifizierer, um eine Schnittstelle in den Synchronisationsmodus „auto“ zurückzusetzen und alle außer Kraft gesetzten Einstellungen zu löschen. • Wenn die entsprechende Schnittstelle auf der Quelle bereits gelöscht ist, wenn die Replikationssynchronisation auf „auto“ festgelegt wird, wird auch die Schnittstelle auf dem Ziel gelöscht. • Der Wert „overridden“ führt dazu, dass Netzwerkschnittstellen nicht mehr automatisch synchronisiert werden. Aktuelle Einstellungen auf dem Quellsystem werden „eingefroren“ und die automatische Weitergabe wird gestoppt.

Beispiel

Mit dem folgenden Befehl wird die Gatewayadresse von Schnittstelle IF_1 geändert:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/if -id IF_1 set -gateway 2001:db8:0:170:a:0:2:70
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = IF_1
Operation completed successfully.
```

Löschen von NAS-Schnittstellen

Löschen Sie eine NAS-Schnittstelle.

 **VORSICHT:** Durch das Löschen einer NAS-Schnittstelle kann die Verbindung zwischen den Systemen unterbrochen werden, die die Schnittstelle verwenden, zum Beispiel konfigurierte Hosts.

Format

```
/net/nas/if -id <value> delete
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID der zu löschenden Schnittstelle ein.

Beispiel

Mit dem folgenden Befehl wird die Schnittstelle IF_1 gelöscht:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/if -id IF_1 delete
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

Operation completed successfully.

Managen von NAS-Routen

Eine NAS-Route stellt eine Route dar, die für eine NAS-Schnittstelle konfiguriert ist.

Tabelle 34. Attribute für NAS-Routen

Attribut	Beschreibung
ID	ID der Route.
NAS server	Kennung des NAS-Servers.
Interface	ID der Schnittstelle zum Erreichen des Gateways.
Route type	Typ der Route. Gültige Werte sind Folgende (keine Unterscheidung zwischen Groß- und Kleinschreibung): <ul style="list-style-type: none">• <code>default</code>: Das System verwendet ein Standardgateway/eine Standardroute, wenn es keinen spezifischeren Host oder keine spezifischere Netzwerkroute zu einem bestimmten Ziel findet. Eine IPv4- und IPv6-Standardroute ist pro Schnittstelle zulässig.• <code>host</code>: erstellt eine Route zu einem Host.• <code>net</code>: erstellt eine Route zu einem Subnetz.
Target	Je nach Wert für <code>-type</code> IP-Adresse des Zielnetzwerk-Node. Der Wert ist einer der folgenden: <ul style="list-style-type: none">• Für eine Standardroute wird die für <code>-gateway</code> angegebene IP-Adresse verwendet.• Geben Sie für eine Hostroute die IP-Adresse eines Zielhosts an.• Geben Sie für eine Netzwerkroute die IP-Adresse eines Zielsubnetzes an. Schließen Sie den Qualifizierer <code>-netmask</code> für das Zielsubnetz ein.
Netmask	Subnetzmaske
Gateway	Gateway-Adresse
Replication sync	Wenn die Routenquelle eine Produktionsschnittstelle des NAS-Servers ist, ist dies eine Kopie des Attributs <code>Replication sync</code> für die verknüpfte Schnittstelle. (Die verknüpfte Schnittstelle ist im Attribut <code>Interface</code> angegeben.) Wenn die Routenquelle keine Produktionsschnittstelle des NAS-Servers ist, ist der Wert dieses Attributs leer.
Health state	Numerischer Wert, der die Integrität des Systems angibt. Gültige Werte: <ul style="list-style-type: none">• <code>Unknown (0)</code>• <code>OK (5)</code>• <code>OK BUT (7)</code>• <code>Degraded/Warning (10)</code>• <code>Minor failure (15)</code>• <code>Major failure (20)</code>
Health details	Zusätzliche Integritätsinformationen.
Use for external services access	Flag, das gibt, ob die Route für den Zugriff auf externe Services verwendet wird. Gültige Werte: <ul style="list-style-type: none">• <code>yes</code>• <code>no</code>

Erstellen einer NAS-Route

Erstellen Sie eine Route für ein NAS-Schnittstelle.

Format

```
/net/nas/route create -if <value> -type {default | host -target <value> | net -target <value> [-netmask <value>]} -gateway <value>
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-if	Geben Sie die Schnittstelle an, die mit der Route verknüpft ist. Jede Schnittstelle hat eine eigene Routing-Tabelle in Reaktion auf eingehende Service-Requests.
-type	Geben Sie den Typ der Route an. Gültige Werte sind folgende (keine Unterscheidung zwischen Groß- und Kleinschreibung): <ul style="list-style-type: none">• <code>default</code>: Das System verwendet die Standardroute/das Standardgateway, wenn eine spezifischere Route für Host oder Netzwerk nicht verfügbar ist. Eine IPv4- und IPv6-Standardroute ist pro Schnittstelle zulässig.• <code>host</code>: Erstellen Sie eine Route zu einem Host.• <code>net</code>: Erstellen Sie eine Route zu einem Subnetz.
-target	Geben Sie je nach dem Wert für <code>-type</code> die IP-Adresse des Zielnetzwerk-Node an: <ul style="list-style-type: none">• Geben Sie für eine Standardroute keinen Wert an.• Geben Sie für eine Hostroute die IP-Adresse eines Zielhosts an.• Geben Sie für eine Netzwerkroute die IP-Adresse eines Zielsubnetzes an. Schließen Sie den Qualifizierer <code>-netmask</code> für das Zielsubnetz ein.
-netmask	Geben Sie für eine Route zu einem Subnetz die Netzmaske des Zielsubnetzes an.
-gateway	Geben Sie das Gateway für die Route an.

Beispiel

Mit dem folgenden Befehl wird eine Netzwerkroute für Schnittstelle `if_1` zum Erreichen des Subnetzes `10.64.74.x` mit Gateway `10.64.74.1` erstellt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/route create -if if_1 -type net -target 10.64.200.10 -netmask 255.255.255.0 -gateway 10.64.74.1
```

```
Storage system address: 10.64.75.201
Storage system port: 443
HTTPS connection
```

```
ID = route_1
Operation completed successfully.
```

Ändern der NAS-Routeneinstellungen

Ändern Sie die Einstellungen für eine NAS-Route.

Format

```
/net/nas/route -id <value> set [-type {default | host | net}] [-target <value>] [-netmask <value>] [-gateway <value>]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Identifiziert das NAS-Routenobjekt.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-type	Geben Sie den Typ der Route an. Gültige Werte sind folgende (keine Unterscheidung zwischen Groß- und Kleinschreibung): <ul style="list-style-type: none">• default: Das System verwendet die Standardroute/das Standardgateway, wenn eine spezifischere Route für Host oder Netzwerk nicht verfügbar ist. Eine IPv4- und IPv6-Standardroute ist pro Schnittstelle zulässig.• host: Erstellen Sie eine Route zu einem Host.• net: Erstellen Sie eine Route zu einem Subnetz.
-target	Geben Sie je nach dem Wert für -type die IP-Adresse des Zielnetzwerk-Node an. Gültige Werte sind: <ul style="list-style-type: none">• Geben Sie für eine Standardroute keinen Wert an. Das System verwendet die für -gateway angegebene IP-Adresse.• Geben Sie für eine Hostroute die IP-Adresse eines Zielhosts an.• Geben Sie für eine Netzwerkroute die IP-Adresse eines Zielsubnetzes an. Schließen Sie den Qualifizierer -netmask für das Zielsubnetz ein.
-netmask	Geben Sie für eine Route zu einem Subnetz die Netzmaske des Zielsubnetzes an.
-gateway	Geben Sie das Gateway für die Route an.

Beispiel

Der folgende Befehl ändert die IP-Zieladresse in 10.64.200.11, die Netzmaske in 255.255.255.0 und das Gateway in 10.64.74.2 für NAS-Route route_1:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456!/net/nas/route -id route_1 set -target 10.64.200.11 -netmask 255.255.255.0 -gateway 10.64.74.2 uemcli
```

```
Storage system address: 10.64.75.201
Storage system port: 443
HTTPS connection

ID = route_1
Operation completed successfully.
```

Anzeigen von NAS-Routen

Zeigen Sie eine Liste der Routen für eine angegebene NAS-Schnittstelle oder für alle NAS-Schnittstellen auf dem System an.

 **ANMERKUNG:** Aktionsbefehl „show“ erläutert, wie das Ausgabeformat geändert wird.

Format

```
/net/nas/route [{-id <value> | -server <value> [-useForESAccess {yes | no}] | -if <value>}] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID der Route an.
-server	Geben Sie den NAS-Server an, für den Routen angezeigt werden sollen.
-useForESAccess	Geben Sie an, ob das System nur die Routen anzeigen soll, die für externe Services verwendet werden.
-if	Geben Sie an, ob das System nur die mit dem angegebenen NAS-Server verknüpften Routen anzeigen soll.

Beispiel

Mit dem folgenden Befehl werden sämtliche NAS-Routen im System angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/route show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:   ID                = route_1
    NAS server        = nas_1
    Type              = net
    Target            = 10.50.50.10
    Netmask           = 255.255.255.0
    Gateway           = 10.0.0.1
    Interface         = if_1
    Health state      = OK (5)
    Health details    = "The component is operating normally. action is
required."
    Replication sync  =
    Use for external services access = no

2:   ID                = route_2
    NAS server        = nas_1
    Type              = default
    Target            =
    Netmask           =
    Gateway           = 10.0.0.2
    Interface         = if_2
    Health state      = OK (5)
    Health details    = "The component is operating normally. No action is
required."
    Replication sync  =
    Use for external services access = no

3:   ID                = route_3
    NAS server        = nas_1
    Type              = host
    Target            = 10.50.50.168
    Netmask           =
    Gateway           = 10.0.0.3
    Interface         = if_3
    Health state      = OK (5)
    Health details    = "The component is operating normally. No action is
required."
    Replication sync  =
    Use for external services access = yes
```

Löschen von NAS-Routen

Löschen Sie eine NAS-Route.

 **VORSICHT:** Durch das Löschen einer NAS-Route kann die Verbindung zwischen den Systemen unterbrochen werden, die die Schnittstelle verwenden, zum Beispiel konfigurierte Hosts.

Format

```
/net/nas/route -id <value> delete
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID der zu löschenden Schnittstelle an.

Beispiel

Mit dem folgenden Befehl wird die Route `route_1` gelöscht:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/route -id route_1 delete
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection
```

```
Operation completed successfully.
```

Managen der Kerberos-Einstellungen

Einstellungen für angepasste Kerberos Key Distribution Center-Server.

Kerberos ist ein verteilter Authentifizierungsservice, der für eine starke Authentifizierung eine Verschlüsselung mit einem geheimen Schlüssel verwendet. Er funktioniert auf Basis von "Tickets", die es Nodes ermöglichen, über ein nicht sicheres Netzwerk zu kommunizieren, um ihre Identität auf sichere Weise nachzuweisen. Wenn der NFS-Server als sicherer NFS-Server konfiguriert wurde, verwendet dieser das Sicherheits-Framework RPCSEC_GSS und das Kerberos-Authentifizierungsprotokoll, um Benutzer und Services zu überprüfen. Sie können eine sichere NFS-Umgebung für einen Multiprotokoll-NAS-Server oder für einen Server, der nur Unix-Freigaben unterstützt, konfigurieren. In dieser Umgebung wird der Benutzerzugriff auf NFS-Dateisysteme basierend auf Kerberos-Prinzipalnamen gewährt.

Tabelle 35. Kerberos-Attribute

Attribut	Beschreibung
NAS server	Kerberos-Bereichsnamenkonfigurationsobjekt, wie durch die NAS-Server-ID identifiziert.
Realm	Name des Kerberos-Bereichs
Servers	Durch Komma getrennte Liste von DNS-Namen für die Kerberos Key Distribution Center (KDC)-Server
Port	TCP-Port des KDC-Servers Default: 88

Konfigurieren von Kerberos-Einstellungen

Legen Sie Kerberos-Einstellungen für einen NAS-Server fest.

Format

```
/net/nas/kerberos -server <value> set {-enabled no | [ -addr <value>] [-port <value>] [-realm <value>]}
```

Objektqualifizierer

Qualifizierer	Beschreibung
-server	Identifiziert den zugehörigen NAS-Server.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-enabled	Aktiviert Kerberos auf dem NAS-Server. Der Wert ist <code>yes</code> oder <code>no</code> .
-addr	Gibt die DNS-Namen der Kerberos-KDC-Server an, durch Komma getrennt.

Qualifizierer	Beschreibung
	 ANMERKUNG: Adressen über IP festzulegen und sie außer Kraft zu setzen wird in dieser Version nicht unterstützt. Ein vollständig qualifizierter DNS-Name wird erwartet.
-port	Gibt den TCP-Port des KDC-Servers an. Der Wert kann jeder TCP-Port sein.
-realm	Identifiziert den Kerberos-Bereich. Wenn nicht eindeutig für das System, gibt der Vorgang eine Fehlermeldung zurück.

Beispiel

Mit dem folgenden Befehl wird ein angepasster Kerberos-Bereich für NAS-Server „nas_1“ konfiguriert:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/kerberos -server nas_1 set -addr
"primary.mydomain.lab.emc.com,secondary.mydomain.emc.com" -realm "MYDOMAIN.LAB.EMC.COM"
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
Operation completed successfully.
```

Anzeigen von Kerberos-Einstellungen

Zeigen Sie Kerberos-Einstellungen an.

Format

```
/net/nas/kerberos [{-server <value> | -realm <value>}] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-server	Identifiziert den zugehörigen NAS-Server.
-realm	Identifiziert den zugehörigen Kerberos-Bereich.

Beispiel

Der folgende Befehl zeigt die Kerberos-Einstellungen für alle NAS-Server des Speichersystems an.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/kerberos show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
1:   NAS server = nas_2
     Realm     = TEST.LAB.EMC.COM
     Servers   = us67890.test.lab.emc.com
```

```
2:   NAS server = nas_1
     Realm     = TEST.LAB.EMC.COM
     Servers   = us12345.test.lab.emc.com
```

Managen von VLANs

Netzwerkpartitionierung wird über virtuelle LANs bereitgestellt. VLANs werden im System statisch zugewiesen und die einzigen zulässigen Aktionen sind das Zuweisen oder Aufheben der Zuweisung einer VLAN-ID zu oder von einem bestimmten Mandanten.

Die einzelnen VLANs verfügen über eigene IDs.

In der folgenden Tabelle sind die Attribute für VLANs aufgeführt.

Tabelle 36. VLAN-Attribute

Attribut	Beschreibung
ID	VLAN-Kennung.
Tenant	Mandantenkennung, wenn zugewiesen.
Interface	Liste der Netzwerkschnittstellen, die diese VLAN-ID für Netzwerk-Datenverkehr-Tagging verwenden.
MTU size	Liste der Ports und ihrer entsprechenden MTU-Größenpaare für das angegebene VLAN.

Anzeigen von VLANs

Zeigen Sie Details zu konfigurierten VLANs an. Sie können nach der VLAN-ID filtern.

Format

```
/net/vlan show {-id <value> | [-from <value>] [-count <value>] [-inUse {yes | no}] [-assigned {yes [-tenant <value>] | no}]}
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-id	Gibt die VLAN-ID an. Gültige Werte sind 1 bis 4095. Bei Angabe ist keine andere Auswahl von VLAN-ID-Bereich, Netzwerkschnittstelle oder Mandantenzuweisung zulässig.
-from	Gibt die untere Grenze des VLAN-Bereichs an, der angezeigt werden soll. Gültige Werte sind 1 bis 4095. Bei Auslassung ist der Standardwert 1.
-count	Gibt die Anzahl der anzuzeigenden Elemente an. Gültige Werte sind 1 bis 4095. Bei Auslassung ist der Standardwert 10.
-inUse	Gültige Werte: <ul style="list-style-type: none">• yes : Zeigt nur die VLANs an, die von einer Netzwerkschnittstelle verwendet werden. Diese virtuellen LANs können zu oder von einem anderen Mandanten verschoben werden.• no : Zeigt nur die VLANs an, die nicht von einer Netzwerkschnittstelle verwendet werden.
-assigned	Gültige Werte: <ul style="list-style-type: none">• yes : Zeigt nur die VLANs an, die einem Mandanten zugewiesen sind.• no : Zeigt nur die VLANs an, die nicht einem Mandanten zugewiesen sind.
-tenant	Identifiziert bei Angabe den Mandanten.

Beispiel

Der folgende Befehl zeigt Informationen zu verwendeten VLANs beginnend mit 100 an:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/vlan show -from 100 -inUse yes
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:   VLAN      = 1
     Tenant    = if_10
     Interface =
     MTU Size  = spa_iom_0_eth1(1300), spb_iom_0_eth1(1300)

2:   VLAN      = 2
     Tenant    =
     Interface = if_11
     MTU Size  = spa_eth2(1490), spa_eth3(1497), spa_iom_0_eth1(1496), spb_eth2(1490),
     spb_eth3(1497), spb_iom_0_eth1(1496)

3:   VLAN      = 3
     Tenant    =
     Interface = if_12
     MTU Size  = spa_iom_0_eth2(1500)
```

Managen von Mandanten

IP-Mehrmandantenfähigkeit bietet die Möglichkeit, mehrere Netzwerk-Namespaces zu den NAS-Servern auf einem Speicherprozessor zuzuweisen. Mandanten werden zum Erstellen von isolierten dateibasierten Speicherpartitionen (CIFS/NFS) verwendet. Dies ermöglicht kosteneffizientes Mandantenmanagement verfügbarer Ressourcen und stellt gleichzeitig sicher, dass die Sichtbarkeit und das Management des Mandanten nur auf die zugewiesenen Ressourcen beschränkt sind.

Jeder Mandant kann folgende Komponenten aufweisen:

- eigene VLAN-Domain
- eigene Routing-Tabelle
- eigene IP-Firewall
- eigene virtuelle Schnittstelle (Datenverkehr getrennt von virtuellem Gerät und Linux-Kernel-Schicht)
- eigener DNS-Server oder andere administrative Server (ermöglichen dem Mandanten eigene Authentifizierung und Sicherheitsvalidierung von der Protokollschicht)

Jeder Mandant wird durch einen Universally Unique Identifier (UUID) identifiziert.

In der folgenden Tabelle sind die Attribute für Mandanten aufgeführt.

Tabelle 37. Mandantenattribute

Attribut	Beschreibung
ID	Mandantenkennung
Name	Benutzerfreundlicher Name des Mandanten.
UUID	Universally Unique Identifier eines Mandanten.
VLAN	Durch Kommas getrennte Liste von VLAN-IDs für den Mandanten

Erstellen eines Mandanten

Erstellen Sie einen Mandanten.

Format

```
/net/tenant create -name <value> -uuid <value> [-vlan <value>]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-name	Geben Sie den Namen des Mandanten an.
-uuid	Geben Sie den Universally Unique Identifier eines Mandanten an.
-vlan	Geben Sie die durch Kommas getrennte Liste von VLAN-IDs an, die der Mandant verwenden kann.  ANMERKUNG: Gültige Werte sind 1 bis 4095; jedoch kann jede VLAN-ID einem Mandanten zugewiesen werden, wenn: <ol style="list-style-type: none">1. sie keinem anderen Mandanten zugewiesen ist.2. keine vorhandenen Netzwerkschnittstellen durch die VLAN-ID gekennzeichnet sind.

Beispiel

Mit dem folgenden Befehl wird ein Mandant mit den folgenden Einstellungen erstellt:

- Der Mandantename ist Mandant A.
- Die UUID ist b67cedd7-2369-40c5-afc9-9e8753b88dee.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/tenant create -name "Tenant A" -uuid b67cedd7-2369-40c5-afc9-9e8753b88dee
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection
```

```
ID = tenant_1  
Operation completed successfully.
```

Anzeigen von Mandanten

Zeigen Sie Details zu konfigurierten Mandanten an. Sie können nach der Mandanten-ID filtern.

Format

```
/net/tenant [-id <value>] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Identifiziert den Mandanten, der angezeigt werden soll.

Beispiel

Mit dem folgenden Befehl werden Informationen über Mandanten angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/tenant show
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection
```

```
1:      ID      = tenant_1  
       Name    = Tenant A  
       UUID   = b67cedd7-2369-40c5-afc9-9e8753b88dee  
       VLAN   = 102,103,104
```

Ändern von Mandanteneinstellungen

Ändern Sie die Einstellungen für einen Mandanten.

Format

```
/net/tenant -id <value> set [ -name <value> ] { [-vlan <value>] | [-addVlan <value>] | [-removeVlan <value>] }
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Identifiziert den Mandanten.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-name	Geben Sie den neuen Namen des Mandanten an.
-vlan	Geben Sie die durch Kommas getrennte Liste von VLAN-IDs an. i ANMERKUNG: Gültige Werte für VLAN-IDs sind 1 bis 4095. Der neue Satz von VLAN-IDs wird mit den VLAN-IDs verglichen, die diesem Mandanten bereits zugewiesen sind. Nichtübereinstimmungen werden so interpretiert, als ob die entsprechenden IDs an die Qualifizierer <code>-addVlan</code> oder <code>-removeVlan</code> weitergegeben worden wären. Beispiel: Wenn die VLANs 101,102 und 103 Mandant X zugewiesen werden, entspricht der Befehl: <pre>tenant -id X set -vlan 101,102,104</pre> Folgendem: <pre>tenant -id X set -removeVlan 103 tenant -id X set -addVlan 104</pre>
-addVlan	Geben Sie die VLAN-ID an, die dem Mandanten zugewiesen werden soll. i ANMERKUNG: Gültige Werte für VLAN-IDs sind 1 bis 4095; jedoch kann jede VLAN-ID einem Mandanten zugewiesen werden, wenn: <ol style="list-style-type: none">1. sie keinem anderen Mandanten zugewiesen ist.2. keine vorhandenen Netzwerkschnittstellen durch die VLAN-ID gekennzeichnet sind.
-removeVlan	Geben Sie die VLAN-ID an, die vom Mandanten entfernt werden soll. i ANMERKUNG: Die VLAN-ID kann nur entfernt werden, wenn sie nicht von einer Schnittstelle der NAS-Server dieses Mandanten verwendet wird.

Beispiel

Der folgende Befehl ändert die Mandanteneinstellungen für die Liste der VLAN-IDs:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/tenant -id tenant_1 set -vlan 101,102,104
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection
```

```
Operation completed successfully.
```

Löschen eines Mandanten

Löscht einen vorhandenen Mandanten. Wenn Sie einen vorhandenen Mandanten löschen, sind die diesem Mandanten zugeordneten VLANs für die Verwendung mit anderen Mandanten verfügbar.

Format

```
/net/tenant -id <value> delete
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Identifiziert den Mandanten.

Beispiel

Mit dem folgenden Befehl wird ein Mandant gelöscht.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/tenant -id tenant_1 delete
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection
```

```
ID = tenant_1  
Operation completed successfully.
```

Managen von CIFS-Servern

CIFS (SMB)-Server verwenden das CIFS-Protokoll zur Übertragung von Dateien. Ein CIFS-Server kann als Komponente einer Windows Active Directory-Domain agieren oder unabhängig von jeglicher Windows-Domain als eigenständiger CIFS-Server.

In der folgenden Tabelle sind die Attribute für CIFS-Server aufgeführt.

Tabelle 38. CIFS-Server-Attribute

Attribut	Beschreibung
ID	ID des CIFS-Servers.
NAS server	Verknüpfte NAS-Server-ID.
Name	Name des für den Beitritt zu Active Directory verwendeten CIFS-Serverkontos
Description	Beschreibung des CIFS-Servers
NetBIOS name	NetBIOS-Name des Servers.
Windows domain	Name der Windows-Serverdomain.
User name	Benutzername der Windows-Domain
Password	Passwort der Windows-Domain
Last used organization unit	Zuletzt verwendete Active Directory-Organisationseinheit
Workgroup	Arbeitsgruppenname
Workgroup administrator password	Arbeitsgruppen-Administratorpasswort

Erstellen eines CIFS-Servers

Erstellen Sie einen CIFS (SMB)-Server.

ANMERKUNG: Pro NAS-Server kann nur ein CIFS-Server erstellt werden.

Format

```
/net/nas/cifs create {-server <value> | -serverName <value>} [-name <value>] [-description <value>] [-netbiosName <value>] {-domain <value> -username <value> {-passwd <value> | -passwdSecure} [-orgUnit <value>] | -workgroup <value> {-adminPasswd <value> | -adminPasswdSecure}}
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-server	Gibt die NAS-Serverkennung an.
-serverName	Gibt den NAS-Servernamen an.
-name	Gibt den CIFS-Servernamen an. Standardmäßig entspricht dies dem Wert für serverName. Dieser Wert wird ignoriert, wenn der CIFS-Server eigenständig ist.
-description	Gibt die Beschreibung des CIFS-Servers an.
-netbiosName	Gibt den NetBIOS-Namen des CIFS-Servers an. Er wird standardmäßig automatisch basierend auf dem CIFS-Servernamen erstellt.
-domain(nur gültig, wenn der CIFS-Server Active Directory hinzugefügt wird)	Gibt den Windows Active Directory-Domainnamen an.
-username (nur gültig, wenn der CIFS-Server Active Directory hinzugefügt wird)	Gibt den Active Directory-Benutzer an, der verwendet wird, um den CIFS-Server Active Directory hinzuzufügen.
-passwd(nur gültig, wenn der CIFS-Server Active Directory hinzugefügt wird)	Gibt das Active Directory-Benutzerpasswort an.
-passwdSecure(nur gültig, wenn der CIFS-Server Active Directory hinzugefügt wird)	Gibt ein Passwort im sicheren Modus an. Der Benutzer wird aufgefordert, das Passwort einzugeben und zu bestätigen.
-orgUnit(nur gültig, wenn der CIFS-Server Active Directory hinzugefügt wird)	Active Directory-Organisationseinheit.
-workgroup (nur gültig, wenn ein eigenständiger CIFS-Servers konfiguriert wird)	Gibt die Arbeitsgruppe des eigenständigen CIFS-Servers -workgroup an.
-adminPasswd (nur gültig, wenn ein eigenständiger CIFS-Servers konfiguriert wird)	Gibt das Passwort für das lokale Administratorkonto des eigenständigen CIFS-Servers an.
-adminPasswdSecure (nur gültig, wenn ein eigenständiger CIFS-Servers konfiguriert wird)	Gibt ein Passwort im sicheren Modus an. Sie werden aufgefordert, das Passwort einzugeben und zu bestätigen.

Beispiel

Mit dem folgenden Befehl wird ein CIFS-Server erstellt.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/cifs create -server nas_0 -name CIFSserver1 -description "CIFS description" -domain domain.one.com -username user1 -passwd password1
```

```
Storage system address: 10.0.0.1
Storage system port: 443
```

```
HTTPS connection
```

```
ID = CIFS_0  
Operation completed successfully.
```

Anzeigen eines CIFS-Servers

Mit dem folgenden Befehl werden die CIFS (SMB)-Servereinstellungen aufgeführt.

Format

```
/net/nas/cifs [{-id <value> | -name <value> | -server <value> | -serverName <value>}] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des CIFS-Servers ein.
-name	Geben Sie den Namen des CIFS-Servers ein.
-server	Geben Sie die ID des zugehörigen NAS-Servers ein.
-serverName	Geben Sie den Namen des zugehörigen NAS-Servers ein.

Beispiel

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/cifs show
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection  
  
1:   ID           = CIFS_0  
    NAS server  = nas_0  
    Name        = CIFSserver1  
    Description = CIFS description  
    NetBIOS name = CIFSserv  
    Windows domain = domain.one.com
```

Ändern von CIFS-Servereinstellungen

Ändern Sie einen vorhandenen CIFS (SMB)-Server.

Wenn Sie einen CIFS-Server von einer Domain zu einer anderen verschieben, berücksichtigen Sie die folgenden Optionen:

- [-domain <value>]
- [-newUsername <value> {-newPasswd <value> | -newPasswdSecure}]

Beachten Sie, dass Sie den Benutzernamen und das Passwort der Domain angeben müssen, zu der der CIFS-Server zuvor hinzugefügt wurde, um ihn wieder trennen zu können. Sie müssen auch den Benutzernamen und das Passwort für die neue Domain angeben, der er hinzugefügt werden soll.

Format

```
/net/nas/cifs {-id <value> | -name <value>} set [-name <value>] [-description <value>] [-netbiosName <value>] [-currentUsername <value> {-currentPasswd <value> | -currentPasswdSecure} | -skipUnjoin] ] { [-domain <value>] [-newUsername <value> {-newPasswd <value> |
```

```
-newPasswdSecure} ] | [-orgUnit <value>] | -workgroup <value>] [ {-adminPasswd <value> |
-adminPasswdSecure} ] }
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des zu ändernden CIFS-Servers ein.
-name	Geben Sie den Namen des zu ändernden CIFS-Servers ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-name	Gibt den neuen CIFS-Servernamen an.
-description	Gibt die Beschreibung des CIFS-Servers an.
-netbiosName	Gibt den neuen NetBIOS-Namen des CIFS-Servers an.
-domain	Gibt den neuen Namen der Windows-Serverdomain an.
-orgUnit	Active Directory-Organisationseinheit.
-currentUsername	Gibt den aktuellen Domainbenutzer an.
-currentPasswd	Gibt das aktuelle Passwort des Domainbenutzers an.
-currentPasswdSecure	Gibt das aktuelle Passwort im sicheren Modus an – der Benutzer wird aufgefordert, das Passwort und die Passwortbestätigung einzugeben.
-skipUnjoin	Trennen Sie den CIFS-Server nicht von einer Active Directory-Domain.
-newUsername	Gibt den neuen Domainbenutzer an.
-newPasswd	Gibt das neue Passwort des Domainbenutzers an.
-newPasswdSecure	Gibt das neue Passwort im sicheren Modus an – der Benutzer wird aufgefordert, das Passwort und die Passwortbestätigung einzugeben.
-workgroup	Gibt die neue Arbeitsgruppe des eigenständigen CIFS-Servers an.
-adminPasswd	Gibt das neue lokale Administratorpasswort des eigenständigen CIFS-Servers an.
-adminPasswdSecure	Gibt das Passwort im sicheren Modus an – der Benutzer wird aufgefordert, das Passwort und die Passwortbestätigung einzugeben.

Beispiel

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/cifs -id CIFS_0 set -workgroup
MyWorkgroup -adminPasswd MyPassword
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = CIFS_0
Operation completed successfully.
```

Löschen eines CIFS-Servers

Löschen Sie einen vorhandenen CIFS (SMB)-Server.

ANMERKUNG: Wenn Sie einen vorhandenen CIFS-Server löschen oder ihn in eine eigenständige Konfiguration umwandeln, müssen Sie die aktuellen Anmeldedaten (Benutzername und Passwort) angeben, um ihn ordnungsgemäß von der Domain zu trennen und das Computerkonto aus Active Directory zu entfernen. Sie können die Option `-skipUnjoin` verwenden, um den CIFS-Server zu löschen, ohne das Computerkonto aus Active Directory zu entfernen. (Dies erfordert, dass der Administrator das Konto manuell aus AD entfernt.) Die Option `-skipUnjoin` kann auch verwendet werden, wenn AD nicht funktioniert oder nicht erreicht werden kann. Wenn Sie diesen Befehl ohne Benutzernamen und Passwort ausführen, werden Sie den CIFS-Server der Domain nicht wieder unter demselben Namen hinzufügen können. Um denselben CIFS-Server wieder mit der Domain zu verbinden, müssen Sie dann zunächst seinen Namen ändern.

Format

```
/net/nas/cifs {-id <value> | -name <value>} delete [ {-username <value> {-passwd <value> |
-passwdSecure} | -skipUnjoin} ]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des zu löschenden CIFS-Servers ein.
-name	Der Name des CIFS-Servers.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-username	Gibt den Domainbenutzernamen an. Nicht erforderlich für eigenständige CIFS-Server. ANMERKUNG: Geben Sie den Benutzernamen an, wenn Sie den CIFS-Server von der Active-Directory-Domain trennen möchten, bevor Sie ihn löschen.
-passwd	Gibt das Passwort des Domainbenutzers an. Nicht erforderlich für eigenständige CIFS-Server. ANMERKUNG: Geben Sie das Benutzerpasswort an, wenn Sie den CIFS-Server von der Active-Directory-Domain trennen möchten, bevor Sie ihn löschen.
-passwdSecure	Gibt ein Passwort im sicheren Modus an. Damit wird der Benutzer aufgefordert, das Passwort einzugeben.
-skipUnjoin	Trennt den CIFS-Server nicht von der Active-Directory-Domain, bevor er gelöscht wird.

Beispiel

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/cifs -id CIFS_0 delete
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = CIFS_0
Operation completed successfully.
```

Managen von NFS-Servern

NFS-Server verwenden das NFS-Protokoll zur Übertragung von Dateien.

In der folgenden Tabelle sind die Attribute für NAS-Server aufgeführt.

Tabelle 39. NFS-Server-Attribute

Attribut	Beschreibung
ID	ID des NFS-Servers
NAS server	Verknüpfte NAS-Server-ID.
Hostname	NFS-Server-Hostname Wenn ein SMB-Server mit einer Active Directory (AD)-Domain verbunden wird, wird der NFS-Server-Hostname standardmäßig zum Namen des SMB-Computers. Wenn Sie sicheres NFS konfigurieren, um einen angepassten Bereich für die Kerberos-Authentifizierung zu verwenden, kann dieser Hostname angepasst werden.
NFSv3 enabled	Gibt an, ob mit dem NFSv3-Protokoll auf NFS-Shares zugegriffen werden kann. Gültige Werte sind <code>yes</code> oder <code>no</code> (Standard ist <code>yes</code>).
NFSv4 enabled	Gibt an, ob auf NFS-Shares mit dem NFSv4-Protokoll zugegriffen werden kann. Gültige Werte sind <code>yes</code> oder <code>no</code> (Standard ist <code>no</code>).
Secure NFS enabled	Gibt an, ob sicheres NFS (mit Kerberos) aktiviert ist. Gültige Werte sind „yes“ und „no“.
Kerberos KDC type	Zeigt den Typ des KDC-Bereichs an, der für sicheres NFS verwendet werden soll. Folgende Werte sind möglich: <ul style="list-style-type: none"> <code>windows</code>: Verwenden Sie den Windows-Bereich, der dem auf dem NAS-Server konfigurierten SMB-Server zugeordnet ist. Wenn Sie sicheres NFS mit dieser Methode konfigurieren, kann der SMB-Support nicht vom NAS-Server gelöscht werden, während das sichere NFS aktiviert und für die Verwendung des Windows-Bereichs konfiguriert ist. <code>custom</code>: Konfigurieren Sie einen angepassten Bereich, um auf alle Arten von Kerberos-Bereichen zu verweisen. (Windows, MIT, Heimdal). Wenn Sie sicheres NFS mit dieser Methode konfigurieren, müssen Sie die Keytab-Datei auf den NAS-Server hochladen, der definiert wird. Weitere Informationen finden Sie unter Konfigurieren von Kerberos-Einstellungen.
Service principal name	Durch Komma getrennte Liste der Service-Principal-Namen, die zur Authentifizierung für den Kerberos-Bereich verwendet werden. Der Name wird automatisch aus dem NFS-Serverhostnamen und dem ausgewählten Bereich abgeleitet.
Extended Unix credentials enabled	Verwenden Sie mehr als 16 Unix-Gruppen. Gültige Werte sind „Yes“ und „No“ (Standard).
Credentials cache retention	Timeout für die Aktualisierung des Anmeldedatencaches, in Minuten.

Erstellen eines NFS-Servers

Erstellen Sie einen NFS-Server.

 **ANMERKUNG:** Pro NAS-Server kann nur ein NFS-Server erstellt werden.

Format

```
/net/nas/nfs create {-server <value> | -serverName <value>} [-hostname <value>] [-v3 {yes | no}] [-v4 {yes | no}] [-secure {no | yes [-kdcType {Windows | custom}]]] [-username <value> {-passwd <value> | -passwdSecure}] [-extendedUnixCredEnabled {yes|no}] [-credCacheRetention <value>]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-server	Gibt die NAS-Serverkennung an.
-serverName	Gibt den NAS-Servernamen an.
-hostname	Gibt den Hostnamen für den NFS-Server an. Dieser wird bei der Kerberos- und DNS-Registrierung verwendet, so dass der Client diesen Namen beim Mounten von Exporten angeben kann. Standardmäßig ist der Hostname identisch mit dem Namen des SMB-Computers oder des NAS-Servers.
-v3	Gibt an, ob auf NFS-Shares mit dem NFSv4-Protokoll zugegriffen werden kann. Gültige Werte sind „yes“ (Standardeinstellung) und „no“.
-v4	Gibt an, ob auf NFS-Shares mit dem NFSv4-Protokoll zugegriffen werden kann. Gültige Werte sind „Yes“ und „No“ (Standard).
-secure	Gibt an, ob sicheres NFS (mit Kerberos) aktiviert wird. Gültige Werte sind „Yes“ und „No“ (Standard). Zur Aktivierung von sicherem NFS müssen Sie auch das NAS-Server-Kerberos-Objekt konfigurieren, mithilfe des Qualifizierers -kdcType einen entsprechenden KDC-Typ angeben und die (mit Kadmind erzeugte) Keytab-Datei hochladen.
-kdcType	Gibt den Typ des KDC-Bereichs an, der für sicheres NFS verwendet wird. Folgende Werte sind möglich: <ul style="list-style-type: none"> • windows: Verwenden Sie den Windows-Bereich, der dem SMB-fähigen NAS-Server zugeordnet ist. Wenn Sie sicheres NFS mit dieser Methode konfigurieren, kann der SMB-Support nicht vom NAS-Server gelöscht werden, während das sichere NFS aktiviert und für die Verwendung des Windows-Bereichs konfiguriert ist. • custom: Konfigurieren Sie einen angepassten Bereich, um auf alle Arten von Kerberos-Bereichen zu verweisen. (Windows, MIT, Heimdal). Wenn Sie sicheres NFS mit dieser Methode konfigurieren, müssen Sie die Keytab-Datei auf den NAS-Server hochladen, der definiert wird. Weitere Informationen finden Sie unter Konfigurieren von Kerberos-Einstellungen.
-username	(Gilt, wenn -kdcType Windows ist) Gibt einen Benutzernamen mit Administrationsrechten an, um den Service-Principal in der Active Directory-Domain zu registrieren.
-passwd	(Gültig, wenn -kdcType Windows ist) Gibt das Administratorpasswort der Active Directory-Domain an.
-passwdSecure	Gibt ein Passwort im sicheren Modus an. Der Benutzer wird aufgefordert, das Passwort einzugeben und zu bestätigen.
-extendedUnixCredEnabled	Gibt an, ob mehr als 16 Unix-Gruppen vorhanden sind. Gültige Werte sind „yes“ und „no“ (Standard).
-credCacheRetention	Gibt die Zeitdauer (in Minuten) an, bis der Anmeldedaten-cache aktualisiert wird oder abläuft. Der Standardwert ist 15 Minuten.

Beispiel

Mit dem folgenden Befehl wird ein NFS-Server auf NAS-Server „nas_1“ mit der Kennung „nfs_1“ erstellt, der NFSv4 und sicheres NFS unterstützt.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/nfs create -server nas_1 -v4 yes -secure yes
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = nfs_1
Operation completed successfully.
```

Anzeigen eines NFS-Servers

Mit dem folgenden Befehl werden die NFS-Servereinstellungen aufgeführt.

Format

```
/net/nas/nfs [{"-id <value> | -server <value> | -serverName <value> | -hostname <value>}] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des anzuzeigenden NFS-Servers ein.
-server	Geben Sie die ID des zugehörigen NAS-Servers ein.
-serverName	Geben Sie den Namen des zugehörigen NAS-Servers ein.
-hostname	Geben Sie den Hostnamen für den NFS-Server ein. Der vollständig qualifizierte Domainname oder die Kurznamenformate werden unterstützt.

Beispiel

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/nfs show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      ID                = nfs_1
        NAS server        = nas_1
        Hostname           = SATURN
        NFSv3 enabled      = yes
        NFSv4 enabled      = yes
        Secure NFS enabled = yes
        Kerberos KDC type  = Windows
        Service principal name = nfs/SATURN.domain.lab.emc.com, nfs/SATURN
        Extended Unix credentials enabled = no
        Credentials cache retention = 15
```

Ändern von NFS-Servereinstellungen

Ändern Sie einen vorhandenen NFS-Server.

Format

```
/net/nas/nfs [{"-id <value>}] set [{"-hostname <value>"} [{"-v3 {yes | no}} [{"-v4 {yes | no}} [{"-secure {no | yes [{"-kdcType {Windows | custom}}]} [{"-username <value> [{"-passwd <value> | -passwdSecure}]} [{"-extendedUnixCredEnabled {yes | no}} [{"-credCacheRetention <value>}]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Identifiziert den zu ändernden NFS-Server.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-hostname	Gibt den neuen Hostnamen für den NFS-Server an. Dieser wird bei der Kerberos- und DNS-Registrierung verwendet, so dass der Client diesen Namen beim Mounten von Exporten angeben kann. Standardmäßig ist der Hostname identisch mit dem Namen des SMB-Computers oder des NAS-Servers.
-v3	Gibt an, ob mit dem NFSv3-Protokoll auf NFS-Shares zugegriffen werden kann. Gültige Werte sind <code>yes</code> oder <code>no</code> .
-v4	Gibt an, ob auf NFS-Shares mit dem NFSv4-Protokoll zugegriffen werden kann. Gültige Werte sind <code>yes</code> oder <code>no</code> .
-secure	Gibt an, ob sicheres NFS (mit Kerberos) aktiviert wird. Gültige Werte sind „yes“ und „no“. Zur Aktivierung von sicherem NFS müssen Sie auch das NAS-Server-Kerberos-Objekt konfigurieren, mithilfe des Qualifizierers <code>-kdcType</code> einen entsprechenden KDC-Typ angeben und die (mit Kadmin erzeugte) Keytab-Datei hochladen.
-kdcType	Gibt den Typ des KDC-Bereichs an, der für sicheres NFS verwendet wird. Folgende Werte sind möglich: <ul style="list-style-type: none"> <code>Windows</code>: Verwenden Sie den Windows-Bereich, der dem auf dem NAS-Server konfigurierten SMB-Server zugeordnet ist. Wenn Sie sicheres NFS mit dieser Methode konfigurieren, kann der SMB-Support nicht vom NAS-Server gelöscht werden, während das sichere NFS aktiviert und für die Verwendung des Windows-Bereichs konfiguriert ist. <code>custom</code>: Konfigurieren Sie einen benutzerdefinierten Bereich, um auf alle Typen von Kerberos-Bereichen (Windows, MIT, Heimdal) zu verweisen. Wenn Sie sicheres NFS mit dieser Methode konfigurieren, müssen Sie die Keytab-Datei auf den NAS-Server hochladen, der definiert wird. Weitere Informationen finden Sie unter Konfigurieren von Kerberos-Einstellungen.
-username	(Gilt, wenn <code>-kdcType Windows</code> ist) Gibt einen Benutzernamen mit Administrationsrechten an, um den Service-Principal in der Active Directory-Domain zu registrieren.
-password	(Gültig, wenn <code>-kdcType Windows</code> ist) Gibt das Administratorpassword der Active Directory-Domain an.
-passwdSecure	Gibt ein Passwort im sicheren Modus an. Der Benutzer wird aufgefordert, das Passwort einzugeben und zu bestätigen.
-skipUnjoin	(Gilt, wenn der KDC-Realm-Typ Windows ist) Löscht den NFS-Server, ohne automatisch die Registrierung der NFS-Service-Principals aus der Active Directory-Domain zu löschen.
-extendedUnixCredEnabled	Gibt an, ob mehr als 16 Unix-Gruppen vorhanden sind. Gültige Werte sind „yes“ oder „no“.
-credCacheRetention	Gibt die Zeitdauer (in Minuten) an, bis der Anmeldedaten-cache aktualisiert wird oder abläuft. Der Standardwert ist 15 Minuten.

Beispiel

Der folgende Befehl ändert die Kredit-Cache-Aufbewahrungsfrist für den NFS-Server „nfs_1“.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/nfs -id nfs_1 set -credCacheRetention 20
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = nfs_1
Operation completed successfully.
```

Löschen eines NFS-Servers

Löschen Sie einen vorhandenen NFS-Server. Der NFS-Server kann nicht gelöscht werden, wenn er zugeordnete Ressourcen, z. B. NFS-Shares, auf dem NAS-Server hat.

Format

```
/net/nas/nfs -id <value> delete [-username <value> {-passwd <value> | -passwdSecure}] [-skipUnjoin]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Identifiziert den zu löschenden NFS-Server.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-username (gilt, wenn der Typ des KDC-Bereichs Windows ist.)	Gibt einen Benutzernamen mit Administrationsrechten an, um die Registrierung des Service-Principals der Active Directory-Domain zu löschen.
-passwd (gilt, wenn der Typ des KDC-Bereichs Windows ist.)	Gibt das Administratorpasswort der Active Directory-Domain an.
-passwdSecure	Gibt ein Passwort im sicheren Modus an. Der Benutzer wird aufgefordert, das Passwort einzugeben und zu bestätigen.
-skipUnjoin (gilt, wenn der Typ des KDC-Bereichs Windows ist.)	Löscht den NFS-Server, ohne automatisch die Registrierung der NFS-Service-Principals aus der Active Directory-Domain zu löschen.

Beispiel

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/nfs -id nfs_1 delete
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection
```

```
Operation completed successfully.
```

Managen von Common Anti Virus Agent (CAVA)

In der folgenden Tabelle sind die Attribute für CAVA aufgeführt.

Tabelle 40. CAVA-Attribute

Attribut	Beschreibung
NAS server	Zugehöriger NAS-Server-Bezeichner.
Enabled	Gibt an, ob CAVA aktiviert ist. Gültige Werte: <ul style="list-style-type: none">• yes• no <p> ANMERKUNG: Bevor Sie CAVA aktivieren können, müssen Sie zunächst eine CAVA-Konfigurationsdatei auf den NAS-Server hochladen. Unter Anzeigen der Befehlszeilenoptionen</p>

Tabelle 40. CAVA-Attribute (fortgesetzt)

Attribut	Beschreibung
	finden Sie ausführliche Informationen zum Hochladen der Konfigurationsdatei.

Anzeigen von CAVA-Einstellungen

Zeigen Sie Details zu CAVA-Einstellungen an.

Format

```
/net/nas/cava [-server <value>] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-server	Identifiziert den zugehörigen NAS-Server.

Beispiel

Mit dem folgenden Befehl werden die CAVA-Einstellungen aufgeführt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/cava show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
1:   NAS server = nas_0
     Enabled    = yes
```

```
2:   NAS server = nas_1
     Enabled    = no
```

Ändern von CAVA-Einstellungen

Ändern Sie die CAVA-Einstellungen.

Format

```
/net/nas/cava -server <value> set -enabled {yes | no}
```

Objektqualifizierer

Qualifizierer	Beschreibung
-server	Identifiziert den zugehörigen NAS-Server.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-enabled	<p>Geben Sie an, ob CAVA aktiviert ist. Gültige Werte:</p> <ul style="list-style-type: none"> • yes • no <p>i ANMERKUNG: Bevor Sie CAVA aktivieren können, müssen Sie zunächst eine CAVA-Konfigurationsdatei auf den NAS-Server hochladen. Unter Anzeigen der Befehlszeilenoptionen finden Sie ausführliche Informationen zum Hochladen der Konfigurationsdatei.</p>

Beispiel

CAVA wird mit dem folgenden Befehl aktiviert:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/cava -server nas_1 set -enabled yes
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
Operation completed successfully.
```

Managen von Konfigurationseinstellungen für Ereignisveröffentlichung

Ereignisveröffentlichung erlaubt es Drittanbieteranwendungen, sich zu registrieren, um beim Zugriff auf Dateisysteme mithilfe von SMB- oder NFS-Protokollen Ereignisbenachrichtigungen und Kontext aus dem Speichersystem zu erhalten. Der Common Event Publishing Agent (CEPA) liefert der Anwendung sowohl eine Ereignisbenachrichtigung als auch zugehörigen Kontext in einer Nachricht. Der Kontext kann aus Metadaten der Datei oder Verzeichnismetadaten bestehen, die erforderlich sind, um die Unternehmens-Policy zu entscheiden.

Sie müssen mindestens eine Ereignisoption definieren (vor dem Ereignis, nach dem Ereignis oder Fehlerfolgeereignis), wenn Ereignisveröffentlichung aktiviert ist.

- Vor-Ereignis-Benachrichtigungen werden gesendet, bevor Sie eine SMB oder NFS-Client-Anforderung verarbeitet.
- Nach-Ereignis-Benachrichtigungen werden nach einer erfolgreichen SMB- oder NFS-Client-Anforderung gesendet.
- Fehlerfolgeereignis-Benachrichtigungen werden nach einer fehlgeschlagenen SMB- oder NFS-Client-Anforderung gesendet.

Tabelle 41. Attribute für Ereignisveröffentlichung

Merkmale	Beschreibung
NAS server	Identifiziert den zugehörigen NAS-Server.
Enabled	Identifiziert, ob Ereignisveröffentlichung auf dem NAS-Server aktiviert ist. Gültige Werte: <ul style="list-style-type: none"> • yes • no (Standardeinstellung)
Pre-event failure policy	Angewendete Policy, wenn eine Benachrichtigung vor einem Ereignis fehlschlägt. Gültige Werte: <ul style="list-style-type: none"> • ignore (Standardeinstellung): gibt an, dass eine fehlgeschlagene Benachrichtigung vor einem Ereignis als erfolgreich bestätigt wird. • deny: gibt an, dass bei einer fehlgeschlagenen Benachrichtigung vor einem Ereignis die Anforderung des SMB- oder NFS-Clients nicht vom Speichersystem ausgeführt wird. Der Client erhält eine „Ablehnung“.
Post-event failure policy	Angewendete Policy, wenn eine Benachrichtigung nach einem Ereignis fehlschlägt. Die Policy wird auch auf Ereignisse nach einem Fehler angewendet. Gültige Werte: <ul style="list-style-type: none"> • ignore (Standardeinstellung): fortfahren und verlorene Ereignisse tolerieren.

Tabelle 41. Attribute für Ereignisveröffentlichung (fortgesetzt)

Merkmale	Beschreibung
	<ul style="list-style-type: none"> • <code>accumulate</code>: fortfahren und Persistenzdatei als kreisförmigen Ereignispuffer für verloren gegangene Ereignisse verwenden. • <code>guarantee</code>: fortfahren und Persistenzdatei als kreisförmigen Ereignispuffer für verloren gegangene Ereignisse verwenden, bis der Puffer gefüllt ist, und dann den Zugriff auf Dateisysteme ablehnen, auf denen die Ereignisveröffentlichung aktiviert ist. • <code>deny</code>: bei CEPA-Konnektivitätsausfall Zugriff auf Dateisysteme ablehnen, auf denen die Ereignisveröffentlichung aktiviert ist.
<code>HTTP port</code>	HTTP-Portnummer für Konnektivität zum CEPA-Server. Der Standardwert ist 12228. Das HTTP-Protokoll wird für eine Verbindung zu CEPA-Servern verwendet. Es ist nicht durch einen Benutzernamen oder ein Passwort geschützt.
<code>HTTP enabled</code>	Identifiziert, ob die Verbindung zu CEPA-Servern unter Verwendung des HTTP-Protokolls aktiviert ist. Wenn sie aktiviert ist, wird zuerst eine Verbindung über HTTP verwendet. Wenn HTTP deaktiviert ist oder die Verbindung fehlschlägt, wird eine Verbindung über das MS-RPC-Protokoll hergestellt, wenn alle CEPA-Server durch einen vollständig qualifizierten Domainnamen (FQDN) definiert sind. Wenn ein SMB-Server in einem NAS-Server in der Active Directory (AD)-Domain definiert ist, wird das SMB-Konto des NAS-Servers verwendet, um eine MS-RPC-Verbindung herzustellen. Gültige Werte: <ul style="list-style-type: none"> • <code>yes</code> (Standardeinstellung) • <code>no</code>
<code>Username</code>	Bei Verwendung des MS-RPC-Protokolls Name eines Windows-Benutzers, der eine Verbindung zu CEPA-Servern herstellen darf.
<code>Password</code>	Bei Verwendung des MS-RPC-Protokolls Passwort des Windows-Benutzers (definiert durch den Benutzernamen).
<code>Heartbeat</code>	Zeitintervall (in Sekunden) zwischen dem Scannen der CEPA-Server, um ihren Online- oder Offlinezustand zu identifizieren. Der Standardwert beträgt 10 Sekunden. Der Bereich liegt zwischen 1 Sekunde und 120 Sekunden.
<code>Timeout</code>	Zeit in Millisekunden, um festzustellen, ob ein CEPA-Server offline ist. Der Standardwert beträgt 1000 ms. Der Bereich liegt zwischen 50 und 5000 ms.
<code>Health state</code>	Integritätsstatus der Ereignisveröffentlichung. Der Integritätsstatuscode wird in Klammern angezeigt. Gültige Werte: <ul style="list-style-type: none"> • <code>OK (5)</code>: Der Ereignisveröffentlichungsservice funktioniert normal. • <code>OK_BUT (7)</code>: Einige für den NAS-Server konfigurierten CEPA-Server sind nicht erreichbar. • <code>Minor failure (15)</code>: Der Ereignisveröffentlichungsservice funktioniert nicht. • <code>Major failure (20)</code>: Alle für den NAS-Server konfigurierten CEPA-Server sind nicht erreichbar.
<code>Health details</code>	Zusätzliche Integritätsinformationen. Weitere Einzelheiten finden Sie in Anhang A, Referenz.

Anzeigen von CEPA-Konfigurationseinstellungen

Zeigen Sie Details zu CEPA-Konfigurationseinstellungen an.

Format

```
/net/nas/event/config [-server <value>] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
<code>-server</code>	Identifiziert den zugehörigen NAS-Server.

Beispiel

Das folgende Beispiel zeigt die CEPA-Einstellungen.

```
uemcli /net/nas/event/config -server nas_1 show -detail
```

```
Storage system address: 10.1.2.100
Storage system port: 443
HTTPS connection

1:   NAS server           = nas_1
     Enabled             = yes
     Pre-event failure policy = ignore
     Post-event failure policy = ignore
     HTTP port           = 12228
     HTTP enabled        = yes
     Username            = user1
     Heartbeat           = 10s
     Timeout             = 1000ms
     Health state        = OK (5)
     Health details      = The Events Publishing Service is operating normally.
```

Ändern der CEPA-Konfigurationseinstellungen

Ändern Sie die Konfiguration der Ereignisveröffentlichung. Wenn Sie einen NAS-Server erstellen, wird automatisch ein Ereignisveröffentlichungs-Konfigurationsobjekt mit Standardwerten erstellt.

Format

```
/net/nas/event/config -server <value> set [-enabled {yes | no}] [-preEventPolicy {ignore | deny}] [-postEventPolicy {ignore | accumulate | guarantee | deny}] [-httpPort <value>] [-httpEnabled {yes | no}] [-username <value> {-passwd <value> | -passwdSecure}] [-heartbeat <value>] [-timeout <value>]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-server	Identifiziert den zugehörigen NAS-Server.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-enabled	Identifiziert, ob Ereignisveröffentlichung auf dem NAS-Server aktiviert ist. Gültige Werte: <ul style="list-style-type: none">• yes• no (Standardeinstellung)
-preEventPolicy	Identifiziert die angewendete Policy, wenn eine Benachrichtigung vor einem Ereignis fehlschlägt. Gültige Werte: <ul style="list-style-type: none">• ignore (Standardeinstellung): gibt an, dass eine fehlgeschlagene Benachrichtigung vor einem Ereignis als erfolgreich bestätigt wird.• deny: gibt an, dass eine fehlgeschlagene Benachrichtigung für ein Vorabereignis mit einer Ablehnung bestätigt wird.
-postEventPolicy	Identifiziert die angewendete Policy, wenn eine Benachrichtigung nach einem Ereignis fehlschlägt. Die Policy wird auch auf Ereignisse nach einem Fehler angewendet. Gültige Werte: <ul style="list-style-type: none">• ignore (Standardeinstellung): fortfahren und verlorene Ereignisse tolerieren.• accumulate: fortfahren und Persistenzdatei als kreisförmigen Ereignispuffer für verloren gegangene Ereignisse verwenden.

Qualifizierer	Beschreibung
	<ul style="list-style-type: none"> • <code>guarantee</code>: fortfahren und Persistenzdatei als kreisförmigen Ereignispuffer für verloren gegangene Ereignisse verwenden, bis der Puffer gefüllt ist, und dann den Zugriff auf Dateisysteme ablehnen, auf denen die Ereignisveröffentlichung aktiviert ist. • <code>deny</code>: bei CEPA-Konnektivitätsausfall Zugriff auf Dateisysteme ablehnen, auf denen die Ereignisveröffentlichung aktiviert ist.
<code>-httpPort</code>	HTTP-Portnummer für Konnektivität zum CEPA-Server. Der Standardwert ist 12228. Das HTTP-Protokoll wird für eine Verbindung zu CEPA-Servern verwendet. Es ist nicht durch einen Benutzernamen oder ein Passwort geschützt.
<code>-httpEnabled</code>	Gibt an, ob die Verbindung zu CEPA-Servern unter Verwendung des HTTP-Protokolls aktiviert ist. Wenn sie aktiviert ist, wird zuerst eine Verbindung über HTTP verwendet. Wenn HTTP deaktiviert ist oder die Verbindung fehlschlägt, wird eine Verbindung über das MS-RPC-Protokoll hergestellt, wenn alle CEPA-Server durch einen vollständig qualifizierten Domainnamen (FQDN) definiert sind. Das SMB-Konto des NAS-Servers in der Active Directory-Domain stellt die Verbindung mithilfe von MS-RPC her. Gültige Werte sind folgende (keine Unterscheidung zwischen Groß- und Kleinschreibung). <ul style="list-style-type: none"> • <code>yes</code> (Standardeinstellung) • <code>no</code>
<code>-username</code>	Name eines Windows-Benutzers, der eine Verbindung zu CEPA-Servern herstellen darf.  ANMERKUNG: Um sicherzustellen, dass eine sichere Verbindung (durch Verwendung des Microsoft-RPC-Protokolls) verwendet wird, müssen Sie HTTP durch Festlegen von <code>-httpEnabled=no</code> deaktivieren.
<code>-passwd</code>	Passwort des Windows-Benutzers, definiert durch den Benutzernamen.
<code>-passwdSecure</code>	Gibt ein Passwort im sicheren Modus an. Der Benutzer wird aufgefordert, das Passwort anzugeben.
<code>-heartbeat</code>	Zeitintervall (in Sekunden) zwischen dem Scannen der CEPA-Server, um ihren Online- oder Offlinestatus zu identifizieren. Der Standardwert beträgt 10 Sekunden. Der Bereich liegt zwischen 1 Sekunde und 120 Sekunden.
<code>-timeout</code>	Zeit in Millisekunden, um festzustellen, ob ein CEPA-Server offline ist. Der Standardwert beträgt 1000 ms. Der Bereich liegt zwischen 50 und 5000 ms.

Beispiel

Der folgende Befehl aktiviert die Ereignisveröffentlichung und legt die Policy nach einem Ereignis auf `accumulate` fest.

```
uemcli /net/nas/event/config -server nas_1 set -enabled yes -postEventPolicy accumulate
```

```
Storage system address: 10.1.2.100
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Managen von Konfigurationseinstellungen für CEPA-Pools

Ereignispools konfigurieren die Arten von Ereignissen, die vom NAS-Server veröffentlicht werden, und die Adressen der CEPA-Server.

Die Ereignisveröffentlichung muss für den NAS-Server und das Dateisystem aktiviert werden. Bestimmte Arten von Ereignissen können auf Dateisystembasis für das NFS-Protokoll, das SMB-Protokoll oder NFS und SMB aktiviert werden.

Tabelle 42. Attribute für CEPA-Pools

Merkmale	Beschreibung
ID	Identifiziert den Ereignisveröffentlichungspool.
NAS server	Identifiziert den zugehörigen NAS-Server.

Tabelle 42. Attribute für CEPA-Pools (fortgesetzt)

Merkmale	Beschreibung
Name	Identifiziert den Namen des Ereignisveröffentlichungspools.
Addresses	Adressen der CEPA-Server. Ein CEPA-Pool ermöglicht die Verwendung von IPv4-, IPv6- und FQDN-Adressen.
Replication sync	<p>Dies gilt nur, wenn der NAS-Server über eine Replikationssitzung repliziert wird. Gültige Werte:</p> <ul style="list-style-type: none"> • <code>Not replicated</code> • <code>Auto synchronized</code>: gibt an, dass die Liste der Server des Ereignisveröffentlichungspools automatisch über die Replikationssitzung auf dem Ziel synchronisiert wird. Alle Änderungs- und Löschvorgänge auf der Quelle werden automatisch auf dem Ziel wiedergegeben. • <code>Overridden</code>: gibt an, dass die Liste der Server des Ereignisveröffentlichungspools manuell auf der Zielseite geändert oder außer Kraft gesetzt wird. <p>Wenn eine Liste der Server des Ereignisveröffentlichungspools auf der Quelle einer Replikation erstellt wird, wird sie automatisch auf dem NAS-Zielservers synchronisiert.</p> <p>IP-Adressänderungen oder -löschungen in der Liste der Server des Ereignisveröffentlichungspools auf einem Quellserver für die Ereignisveröffentlichung haben keine Auswirkung auf das Außerkraftsetzen der Server des Ereignisveröffentlichungspools auf dem Ziel.</p>
Source addresses	Adressen der CEPA-Server, die für die Replikationsquelle definiert sind. Ein CEPA-Pool ermöglicht die Verwendung von IPv4-, IPv6- und FQDN-Adressen.
Pre-events	Listet die ausgewählten Vorabereignisse auf. Der NAS-Server sendet eine Anforderungsereignisbenachrichtigung an den CEPA-Server, bevor ein Ereignis auftritt, und verarbeitet die Antwort. Die gültigen Ereignisse werden in der folgenden Tabelle definiert.
Post-events	Listet die ausgewählten anschließenden Ereignisse auf. Der NAS-Server sendet eine Benachrichtigung, nachdem ein Ereignis auftritt. Die gültigen Ereignisse werden in der folgenden Tabelle definiert.
Post-error events	Listet die ausgewählten Ereignisse nach einem Fehler auf. Der NAS-Server sendet die Benachrichtigung, nachdem ein Ereignis einen Fehler generiert. Die gültigen Ereignisse werden in der folgenden Tabelle definiert.

Tabelle 43. Ereignisbeschreibungen

Wert	Definition	Protokoll
<code>OpenFileNoAccess</code>	Sendet eine Benachrichtigung, wenn eine Datei für eine Änderung, die kein Lese- oder Schreibzugriff ist (z. B. Lese- oder Schreibattribute auf der Datei) geöffnet wird.	<ul style="list-style-type: none"> • SMB/CIFS • NFS (v4)
<code>OpenFileRead</code>	Sendet eine Benachrichtigung, wenn eine Datei für den Lesezugriff geöffnet wird.	<ul style="list-style-type: none"> • SMB/CIFS • NFS (v4)
<code>OpenFileReadOffline</code>	Sendet eine Benachrichtigung, wenn eine Offlinedatei für den Lesezugriff geöffnet wird.	<ul style="list-style-type: none"> • SMB/CIFS • NFS (v4)
<code>OpenFileWrite</code>	Sendet eine Benachrichtigung, wenn eine Datei für den Schreibzugriff geöffnet wird.	<ul style="list-style-type: none"> • SMB/CIFS • NFS (v4)
<code>OpenFileWriteOffline</code>	Sendet eine Benachrichtigung, wenn eine Offlinedatei für den Schreibzugriff geöffnet wird.	<ul style="list-style-type: none"> • SMB/CIFS • NFS (v4)
<code>OpenDir</code>	Sendet eine Benachrichtigung, wenn ein Verzeichnis geöffnet wird.	SMB/CIFS
<code>FileRead</code>	Sendet eine Benachrichtigung, wenn ein Lesezugriff auf eine Datei über NFS empfangen wird.	NFS (v3/v4)
<code>FileWrite</code>	Sendet eine Benachrichtigung, wenn ein Schreibzugriff auf eine Datei über NFS empfangen wird.	NFS (v3/v4)
<code>CreateFile</code>	Sendet eine Benachrichtigung, wenn eine Datei erstellt wird.	<ul style="list-style-type: none"> • SMB/CIFS • NFS (v3/v4)

Tabelle 43. Ereignisbeschreibungen (fortgesetzt)

Wert	Definition	Protokoll
CreateDir	Sendet eine Benachrichtigung, wenn ein Verzeichnis erstellt wird.	<ul style="list-style-type: none"> • SMB/CIFS • NFS (v3/v4)
DeleteFile	Sendet eine Benachrichtigung, wenn eine Datei gelöscht wird.	<ul style="list-style-type: none"> • SMB/CIFS • NFS (v3/v4)
DeleteDir	Sendet eine Benachrichtigung, wenn ein Verzeichnis gelöscht wird.	<ul style="list-style-type: none"> • SMB/CIFS • NFS (v3/v4)
CloseModified	Sendet eine Benachrichtigung, wenn eine Datei vor dem Schließen geändert wird.	<ul style="list-style-type: none"> • SMB/CIFS • NFS (v4)
CloseUnmodified	Sendet eine Benachrichtigung, wenn eine Datei vor dem Schließen nicht geändert wird.	<ul style="list-style-type: none"> • SMB/CIFS • NFS (v4)
CloseDir	Sendet eine Benachrichtigung, wenn ein Verzeichnis geschlossen wird.	SMB/CIFS
RenameFile	Sendet eine Benachrichtigung, wenn eine Datei umbenannt wird.	<ul style="list-style-type: none"> • SMB/CIFS • NFS (v3/v4)
RenameDir	Sendet eine Benachrichtigung, wenn ein Verzeichnis umbenannt wird.	<ul style="list-style-type: none"> • SMB/CIFS • NFS (v3/v4)
SetAclFile	Sendet eine Benachrichtigung, wenn die Sicherheitsbeschreibung (ACL) für eine Datei geändert wird.	SMB/CIFS
SetAclDir	Sendet eine Benachrichtigung, wenn die Sicherheitsbeschreibung (ACL) für ein Verzeichnis geändert wird.	SMB/CIFS
SetSecFile	Sendet eine Benachrichtigung, wenn eine Änderung an der Dateisicherheit über NFS empfangen wird.	NFS (v3/v4)
SetSecDir	Sendet eine Benachrichtigung, wenn eine Änderung an der Verzeichnissicherheit über NFS empfangen wird.	NFS (v3/v4)

Erstellen eines CEPA-Pools

Erstellen Sie einen CEPA-Pool.

Format

```
/net/nas/event/pool create -server <value> -name <value> -addr <value> [-preEvents <value>] [-postEvents <value>] [-postErrEvents <value>]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-server	Identifiziert den zugehörigen NAS-Server.
-name	Gibt einen Namen für den CEPA-Pool an. Der Name muss für jeden NAS-Server eindeutig sein.
-addr	Gibt eine durch Kommas getrennte Liste der Adressen der CEPA-Server an. Sie können IPv4-, IPv6- und FQDN-Adressen angeben.
-preEvents	Gibt die durch Kommas getrennte Liste von Vorabereignissen an.
-postEvents	Gibt die durch Kommas getrennte Liste der anschließenden Ereignisse an.

Qualifizierer	Beschreibung
-postErrEvents	Gibt die durch Kommas getrennte Liste von Ereignissen nach einem Fehler an.

Beispiel

Der folgende Befehl erstellt einen CEPA-Pool und eine Liste der anschließenden Ereignisse, bei denen Sie benachrichtigt werden.

```
uemcli /net/nas/event/pool create -server nas_1 -name mypool1 -addr 10.1.2.100 -postEvents CreateFile,DeleteFile
```

```
Storage system address: 10.1.2.100
Storage system port: 443
HTTPS connection
```

```
ID = cepa_pool_1
Operation completed successfully.
```

Anzeigen von CEPA-Poleinstellungen

Zeigen Sie Details zu einem CEPA-Pool an.

Format

```
/net/nas/event/pool [{"-id <value> | -server <value> | -name <value>}] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Identifiziert den Ereignisveröffentlichungspool.
-server	Identifiziert den zugehörigen NAS-Server.
-name	Identifiziert den Namen des Ereignisveröffentlichungspools.

Beispiel

Mit dem folgenden Befehl werden detaillierte Informationen zu einem CEPA-Pool angezeigt.

```
uemcli /net/nas/event/pool -server nas_1 show
```

```
Storage system address: 10.1.2.100
Storage system port: 443
HTTPS connection
```

```
1:   ID           = cepa_pool_1
     NAS server  = nas_1
     Name        = MyCepaPool
     Addresses   = 10.1.2.2
     Pre-events  =
     Post-events = CreateFile, DeleteFile
     Post-error events =
```

Ändern der Einstellungen für CEPA-Pools

Ändern Sie die Einstellungen für einen vorhandenen Ereignisveröffentlichungspool.

Format

```
/net/nas/event/pool -id <value> set [-name <value>] [-addr <value>] [-preEvents <value>] [-postEvents <value>] [-postErrEvents <value>] [-replSync {auto | overridden}]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Identifiziert den Ereignisveröffentlichungspool.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-name	Gibt einen Namen für den CEPA-Pool an. Der Name ist für jeden angegebenen NAS-Server eindeutig.
-addr	Gibt eine durch Kommas getrennte Liste der Adressen der CEPA-Server an. Ein CEPA-Pool ermöglicht IPv4-, IPv6- und FQDN-Adressen.
-preEvents	Gibt die durch Kommas getrennte Liste von Vorabereignissen an.
-postEvents	Gibt die durch Kommas getrennte Liste der anschließenden Ereignisse an.
-postErrEvents	Gibt die durch Kommas getrennte Liste von Ereignissen nach einem Fehler an.
-replSync	<p>Dies gilt nur, wenn der NAS-Server als Replikationsziel fungiert. Die gültigen Werte sind folgende:</p> <ul style="list-style-type: none">• auto: gibt an, dass die Liste der Server des Ereignisveröffentlichungspools automatisch über die Replikationssitzung auf dem Ziel synchronisiert wird. Alle Änderungs- und Löschvorgänge auf der Quelle werden automatisch auf dem Ziel wiedergegeben.• overridden: gibt an, dass die Liste der Server des Ereignisveröffentlichungspools manuell auf der Zielseite geändert oder außer Kraft gesetzt wird. <p>Wenn eine Liste der replizierten Server des Ereignisveröffentlichungspools auf der Quelle einer Replikation erstellt wird, wird sie automatisch auf dem Ziel synchronisiert.</p> <p>IP-Adressänderungen oder -löschungen in der Liste der Server des Ereignisveröffentlichungspools in einem Quellservice für die Ereignisveröffentlichung haben keine Auswirkung auf das Außerkraftsetzen der Serverliste des Ereignisveröffentlichungspools auf dem Ziel.</p>

Beispiel

Mit dem folgenden Befehl wird der Name eines CEPA-Pools geändert:

```
uemcli /net/nas/event/pool -id cepa_pool_1 set -name TestCepaPool
```

```
Storage system address: 10.1.2.100
Storage system port: 443
HTTPS connection
```

```
ID = cepa_pool_1
Operation completed successfully.
```

Löschen eines CEPA-Pools

Löscht einen CEPA-Pool.

Bevor Sie beginnen

Der Ereignisveröffentlichungsservice erfordert mindestens einen CEPA-Pool. Wenn Sie den letzten CEPA-Pool löschen, wird der Ereignisveröffentlichungsservice deaktiviert.

Format

```
/net/nas/event/pool [{"-id <value> | -name <value>}] delete
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Identifiziert den Ereignisveröffentlichungspool.
-name	Identifiziert den Namen des Ereignisveröffentlichungspools.

Beispiel

Mit dem folgenden Befehl wird ein CEPA-Pool gelöscht.

```
uemcli /net/nas/event/pool -id cepa_pool_1 delete
```

```
Storage system address: 10.1.2.100  
Storage system port: 443  
HTTPS connection
```

```
Operation completed successfully.
```

Managen von VMware-NAS-Protokollendpunktservern

VMware-Protokollendpunktserver sind NFS-basierte NAS-Server, die aktiviert werden, um einen I/O-Pfad vom VMware-Host zum jeweiligen Datei-vVol-Datenspeicher auf dem Storage-System bereitzustellen.

Beim Erstellen eines NAS-Protokollendpunktservern können Sie die IP-Adresse, die der NAS-PE verwenden soll, aus der Liste der IP-Schnittstellen auswählen, die bereits für den NAS-Server erstellt wurden. Es wird empfohlen, dass Sie mindestens zwei NAS-Server für vVols aktivieren, einen auf jedem SP, um hohe Verfügbarkeit zu ermöglichen. Das System wird einen dieser NAS-PEs automatisch auswählen, basierend darauf, welcher den Durchsatz maximieren wird.

Tabelle 44. Attribute für Protokollendpunktserver

Attribut	Beschreibung
ID	Kennung des VMware-Protokollendpunkts
NAS server	Kennung des zugehörigen NAS-Servers für NAS-PEs
NAS server interface	Kennung der NAS-Server-IP-Schnittstelle, die vom VMware-NAS-Protokollendpunktserver verwendet werden soll.

 **ANMERKUNG:** Pro NAS-Server wird nur ein VMware-Protokollendpunktserver unterstützt.

Erstellen von Protokollendpunktservern

Erstellen Sie VMware-Protokollendpunktserver für Datei-vVols.

Format

```
/net/nas/vmwarepe create [-async] {-server <value> | -serverName <value>} -if <value>
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.
-server	Geben Sie die Kennung des NAS-Servers ein.
-serverName	Geben Sie den Namen des NAS-Servers ein.
-if	Geben Sie den Namen der Kennung für die NAS-IP-Schnittstelle ein, die vom VMware-Protokollendpunktserver verwendet werden soll.

Beispiel

Im folgenden Beispiel wird ein Protokollendpunktserver auf dem NAS-Server „nas_1“ mit der IP-Schnittstelle „if_1“ erstellt.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/vmwarepe create -server nas_1 -if if_1
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = PES_0
Operation completed successfully.
```

Anzeigen der VMware-Protokollendpunktserver

Zeigen Sie VMware-Protokollendpunktserver für Datei-vVols an.

Format

```
/net/nas/vmwarepe [{-id <value> | -server <value> | -serverName <value>}] show
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die Kennung des NAS-Protokollendpunktserver ein.
-server	Geben Sie die Kennung des zugehörigen NAS-Servers ein.
-serverName	Geben Sie den Namen des zugehörigen NAS-Servers ein.

Beispiel

Das folgende Beispiel zeigt die Details für alle VMware-Protokollendpunktserver auf dem System an.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/vmwarepe show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
1: ID = PES_0
   NAS server = nas_1
   NAS server interface = if_1
```

Löschen von Protokollendpunktservern

Löschen Sie einen VMware-Protokollendpunktserver.

Format

```
/net/nas/vmwarepe -id <value> delete [-async] [-force]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die Kennung des zu löschenden VMware-Protokollendpunktserver ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.
-force	Entfernt bedingungslos alle VMware-NAS-Protokollendpunkte, die den VMware-Protokollendpunktserver verwenden und hebt die Bindung aller virtuellen Volumes auf, die den Protokollendpunktserver verwenden.

Beispiel

Im folgenden Beispiel wird der VMware-NAS-Protokollendpunktserver „PES_0“ gelöscht.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/vmwarepe -id PES_0 delete
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Managen des gegenseitigen CHAP für die gegenseitige CHAP-Authentifizierung

Das Challenge Handshake Authentication Protocol (CHAP) ist ein Sicherheitsprotokoll, das eine Methode für die Authentifizierung von Hosts (Initiatoren) und iSCSI-Nodes (Zielen) definiert. Wenn das CHAP aktiviert ist, sendet ein iSCSI-Ziel einem Initiator, der versucht, eine Verbindung herzustellen, eine „Challenge“ zur Authentifizierung. Wenn der Initiator nicht mit einem gültigen Passwort (einem sogenannten Schlüssel) antwortet, verweigert das Ziel die Verbindung. Die CHAP-Authentifizierung kann einseitig sein, d. h., nur das Ziel authentifiziert den Initiator, oder gegenseitig, d. h., das Ziel und der Initiator authentifizieren sich gegenseitig. Im Vergleich zum einseitigen CHAP bietet das gegenseitige CHAP zusätzliche Sicherheit. Erstellen Sie zur Aktivierung der einseitigen CHAP-Authentifizierung ein iSCSI-CHAP-Konto für einen Host. [Managen von iSCSI-CHAP-Konten für die einseitige CHAP-Authentifizierung](#) erläutert die Befehle für die Konfiguration der einseitigen CHAP-Authentifizierung.

ANMERKUNG: Bei gegenseitiger CHAP-Authentifizierung gilt das Passwort für alle iSCSI-Nodes im System. Ferner muss sich der CHAP-Schlüssel für eine Hostkonfiguration vom Passwort für das gegenseitige CHAP für iSCSI-Nodes unterscheiden.

Das gegenseitige iSCSI-CHAP-Objekt managt den Benutzernamen/Schlüssel, den das Ziel (Speichersystem) verwendet, um auf eine Abfrage eines Initiators (Host) zu reagieren.

Festlegen von gegenseitigen CHAP-Schlüsseinstellungen

In der folgenden Tabelle sind die gegenseitigen iSCSI-CHAP-Attribute aufgeführt.

Tabelle 45. Gegenseitige iSCSI-CHAP-Attribute

Attribut	Beschreibung
Username	Der gegenseitige CHAP-Benutzername.
Secret	Der gegenseitige CHAP-Schlüssel (Passwort).
Secret format	Das Eingabeformat des gegenseitigen CHAP. Folgende Werte sind möglich: <ul style="list-style-type: none">• <code>ascii</code>: ASCII-Format• <code>hex</code>: Hexadezimaler Format

Legt den Benutzernamen und den Schlüssel für das gegenseitige CHAP fest.

Format

```
/net/iscsi/reversechap set { [-username <value>] {-secret <value> | -secretSecure} [-secretFormat { ascii | hex } ] | -noChap}
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
<code>-username</code>	Der gegenseitige CHAP-Benutzername.
<code>-secret</code>	Gibt das gegenseitige CHAP-Schlüsselpasswort an. ANMERKUNG: Einschränkungen: Beim CHAP-Schlüssel handelt es sich um eine ASCII-Zeichenfolge aus 12 bis 16 Zeichen. Hexadezimale Schlüssel bestehen aus 12 bis 16 Datenpaaren (24 bis 32 Zeichen).
<code>-secretSecure</code>	Gibt das Passwort im sicheren Modus an – der Benutzer wird aufgefordert, das Passwort einzugeben.
<code>-secretFormat</code>	Das Eingabeformat des gegenseitigen CHAP. Folgende Werte sind möglich: <ul style="list-style-type: none">• <code>ascii</code>: ASCII-Format• <code>hex</code>: Hexadezimaler Format
<code>-noChap</code>	Entfernen Sie die gegenseitigen CHAP-Anmeldedaten.

Beispiel

```
uemcli /net/iscsi/reversechap set -secret xyz0123456789
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
Operation completed successfully.
```

Anzeigen von gegenseitigen CHAP-Schlüsseinstellungen

Zeigen Sie an, ob ein Schlüsselpasswort für das gegenseitige CHAP für iSCSI-Nodes konfiguriert wurde.

ANMERKUNG: Aktionsbefehl „show“ erläutert, wie das Ausgabeformat geändert wird.

Format

```
/net/iscsi/reversechap show
```

Beispiel

Mit dem folgenden Befehl wird die aktuelle Einstellung für das gegenseitige CHAP angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/iscsi/reversechap show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      Username = ReverseChapUser
```

Einrichten des iSNS für iSCSI-Speicher

Das iSNS-Protokoll (iSNSP) ermöglicht das zentrale Management von iSCSI-Devices. Ein iSNS-Server kann Services wie Remote-Discovery und -Konfiguration für iSCSI-Nodes und -Hosts bereitstellen. Bei Verwendung von iSNSP müssen sowohl die iSCSI-Nodes (Ziele) als auch die Hosts (Initiatoren) im Netzwerk für die Verwendung des iSNS-Servers konfiguriert werden. Sie erstellen einen einzelnen iSNS-Serverdatensatz für das System. In der folgenden Tabelle sind die Attribute für iSNS-Serverdatensätze aufgeführt.

Tabelle 46. Attribute von iSNS-Serverdatensätzen

Attribut	Beschreibung
ID	Die ID des iSNS-Serverdatensatzes.
Server	Der Name bzw. die IP-Adresse eines iSNS-Servers.

Erstellen von iSNS-Serverdatensätzen

Erstellen Sie einen iSNS-Serverdatensatz, und geben Sie einen iSNS-Server für das System an. Wenn Sie einen iSNS-Serverdatensatz erstellen, wird der vorhandene Datensatz im System überschrieben.

Format

```
/net/iscsi/isns create -server <value>
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-server	Geben Sie den Namen bzw. die IP-Adresse des iSNS-Servers ein.

Beispiel

Mit dem folgenden Befehl wird ein iSNS-Serverdatensatz für die Server-IP-Adresse 10.5.2.128 erstellt. Der Serverdatensatz erhält die ID ISNS_10.5.2.128:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/iscsi/isns create -server 10.5.2.128
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = isns_0
Operation completed successfully.
```

Anzeigen von iSNS-Serverdatensätzen

Zeigen Sie Details zu konfigurierten iSNS-Serverdatensätzen an.

 **ANMERKUNG:** Aktionsbefehl „show“ erläutert, wie das Ausgabeformat geändert wird.

Format

```
/net/iscsi/isns show
```

Beispiel

Mit dem folgenden Befehl werden Details zum iSNS-Serverdatensatz angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/iscsi/isns show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = isns_0
Operation completed successfully.
```

Löschen von iSNS-Serverdatensätzen

Löschen Sie einen iSNS-Serverdatensatz.

Format

```
/net/iscsi/isns -id <value> delete
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des zu löschenden iSNS-Serverdatensatzes ein.

Beispiel

Mit dem folgenden Befehl wird der iSNS-Serverdatensatz isns_0 gelöscht:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/iscsi/isns -id isns_0 delete
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Ändern der iSNS-Serverdatensatz-Einstellungen

Ändern Sie einen bestehenden iSNS-Serverdatensatz.

Format

```
/net/iscsi/isns -id <value> set -server <value>
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des zu löschenden iSNS-Serverdatensatzes ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-server	Neue dem iSNS-Server zugeordnete IP-Adresse.

Beispiel

Mit dem folgenden Befehl wird der iSNS-Serverdatensatz geändert:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/iscsi/isns -id isns_0 set -server 10.5.2.130
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = isns_0
Operation completed successfully.
```

Managen der iSCSI-Konfiguration

In der folgenden Tabelle sind die Attribute für die iSCSI-Konfiguration aufgeführt.

Tabelle 47. Attribute für die iSCSI-Konfiguration

Attribut	Beschreibung
CHAP required	Gibt an, ob für den Zugriff auf den iSCSI-Speicher eine CHAP-Authentifizierung erforderlich ist. Gültige Werte: <ul style="list-style-type: none">• yes• no

Anzeigen der iSCSI-Konfiguration

Zeigen Sie Details zur iSCSI-Konfiguration an.

Format

```
/net/iscsi/config show
```

Beispiel

Mit dem folgenden Befehl werden Details zur iSCSI-Konfiguration angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/iscsi/config show
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection  
  
1: CHAP required = yes
```

Ändern der iSCSI-Konfiguration

Ändern Sie die iSCSI-Konfiguration.

Format

```
/net/iscsi/config set -chapRequired {yes | no}
```

Objektqualifizierer

Qualifizierer	Beschreibung
-chapRequired	Gibt an, ob eine CHAP-Authentifizierung erforderlich ist. Bei den Werten wird zwischen Groß- und Kleinschreibung unterschieden. Gültige Werte: <ul style="list-style-type: none">• yes• no

Beispiel

Mit dem folgenden Befehl wird der Hostzugriff ohne CHAP-Authentifizierung verweigert:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/iscsi/config set -chapRequired yes
```

```
Storage system address:10.0.0.1  
Storage system port: 443  
HTTPS connection  
  
Operation completed successfully.
```

Managen von iSCSI-Nodes (iSCSI-Servern)

iSCSI-Nodes oder iSCSI-Server sind Softwarekomponenten im System, die Vorgänge für über das iSCSI-Protokoll übertragene Daten managen. iSCSI-Nodes werden auf jedem Ethernetport ausgeführt und kommunizieren mit Netzwerkhosts über SP-Ports.

iSCSI-Nodes übernehmen die Aufgaben zur Erstellung und Überwachung von Speicher sowie zum Management von iSCSI-LUNs. Hosts stellen über iSCSI-Initiatoren eine Verbindung zur LUN her.

Die einzelnen iSCSI-Nodes verfügen über eigene IDs.

Unter [Managen des gegenseitigen CHAP für die gegenseitige CHAP-Authentifizierung](#) wird erläutert, wie die gegenseitige CHAP-Authentifizierung zwischen iSCSI-Hosts und -Nodes konfiguriert wird.

In der folgenden Tabelle sind die Attribute für iSCSI-Nodes aufgeführt.

Tabelle 48. Attribute für den iSCSI-Node

Attribut	Beschreibung
ID	Die ID des iSCSI-Nodes.
Alias	Der Name des iSCSI-Nodes.

Tabelle 48. Attribute für den iSCSI-Node (fortgesetzt)

Attribut	Beschreibung
IQN	Der iSCSI Qualified Name (IQN) des Nodes. Im iSCSI-Protokoll ist eine konkrete Adresssyntax für iSCSI-Geräte, die an der Datenübertragung im Netzwerk beteiligt sind, festgelegt. Die iSCSI-Adressen werden als IQNs bezeichnet. Die IQNs bestehen aus Feldern für Typ, Datum, Authority und Zeichenfolge. Beispiel: <code>iqn.1992-07.com.emc:apm000650039080000-3</code>
SP	Primärer SP, auf dem der Node ausgeführt wird.
Health state	Der Integritätsstatus des iSCSI-Nodes. Der Statuscode wird in Klammern angezeigt. Folgende Werte sind möglich: <ul style="list-style-type: none"> • <code>Unknown (0)</code>: Status ist unbekannt. • <code>OK (5)</code>: Funktioniert ordnungsgemäß. • <code>Degraded/Warning (10)</code>: Funktioniert und führt alle Funktionen aus, die Performance ist jedoch eventuell nicht optimal. • <code>Critical failure (25)</code>: Es ist ein Fehler aufgetreten; eine Recovery ist eventuell nicht möglich. Diese Bedingung hat zu Datenverlusten geführt. Der Fehler muss umgehend behoben werden.
Health details	Zusätzliche Integritätsinformationen. Weitere Informationen zur Integrität finden Sie im Anhang A, Referenz.
Port	Zugehörige Netzwerkportkennung.
Interfaces	ID der jeweils dem iSCSI-Node zugewiesenen Netzwerkschnittstellen. Über die Schnittstelle wird die IP-Adresse des Nodes definiert und damit die Kommunikation mit dem Netzwerk und den Hosts ermöglicht.  ANMERKUNG: Management von Netzwerkschnittstellen erläutert, wie die Netzwerkschnittstellen im System konfiguriert werden.

Anzeigen von iSCSI-Nodes

Zeigen Sie Details zu iSCSI-Nodes an. Sie können nach der ID des iSCSI-Nodes filtern.

 **ANMERKUNG:** Aktionsbefehl „show“ erläutert, wie das Ausgabeformat geändert wird.

Format

```
/net/iscsi/node [-id <value>] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID eines iSCSI-Nodes ein.

Beispiel

Mit dem folgenden Befehl werden sämtliche auf dem System vorhandenen iSCSI-Nodes aufgeführt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/iscsi/node show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      ID           = ISCSIN_1
      Alias         = MyISCSIserver1
      IQN           = iqn.1992-05.com.emc:fcnch0821001340000-1
      Health state = OK (5)
      SP           = SPA
      Port         = eth0_SPA
      Interfaces   = IF_1,IF_2

2:      ID           = ISCSIN_2
      Name          = MyISCSIserver2
      IQN           = iqn.1992-05.com.emc:fcnch0821001340001-1
      Health state = OK (5)
      SP           = SPA
      Port         = eth1_SPA
      Interfaces   = IF_3
```

Ändern der Einstellungen von iSCSI-Nodes

Ändern Sie den dem Node zugewiesenen Netzwerkschnittstellen-Alias.

Format

```
/net/iscsi/node -id <value> set -alias <value>
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des zu ändernden iSCSI-Nodes ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-alias	Benutzerfreundlicher Name zur Identifizierung des iSCSI-Nodes

Beispiel

Der folgende Befehl ordnet dem Node ISCSIN_1 einen Alias zu:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/iscsi/node -id ISCSIN_1 set -alias "My iSCSI node"
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = ISCSIN_1
Operation completed successfully.
```

Managen von Ethernetports

Sie können die Einstellungen für die Netzwerkports auf jedem SP anzeigen und ändern.

In der folgenden Tabelle sind die Attribute des Ports beschrieben.

Tabelle 49. Attribute des Netzwerkports

Attribut	Beschreibung
ID	ID des Ports.
Name	Name des Ports.
SP	Name des SP, auf dem sich der Port befindet. Der Wert lautet „SPA“ oder „SPB“.
Protocols	Arten von Protokollen, die der Port unterstützt. Folgende Werte sind möglich: <ul style="list-style-type: none"> ● <code>mgmt</code>: Managementoberfläche ● <code>file</code>: Netzwerkschnittstelle für Windows (SMB)- und Linux/UNIX (NFS)-Speicher. ● <code>iscsi</code>: iSCSI-Schnittstelle für iSCSI-Speicher Unter Management von Netzwerkschnittstellen wird die Konfiguration der Netzwerkschnittstellen im System erläutert.
MTU size	Paketgröße der maximalen Übertragungseinheit (Maximum Transmission Unit, MTU) des Ports (in Byte). Der Standardwert beträgt 1.500 Byte pro Paket.
Requested MTU size	Vom Benutzer eingestellte MTU-Größe.
Available MTU size	Liste verfügbarer MTU-Größen. i ANMERKUNG: Dies kann entweder als eine durch Komma getrennte Liste der exakten Werte angezeigt werden (wenn es eine iSCSI-Schnittstelle auf dem Port gibt) oder als ein Intervall, das durch die Minimal- und Maximalwerte definiert ist, zum Beispiel 1280-9216.
Speed	Aktuelle Verbindungsgeschwindigkeit des Ports.
Requested speed	Vom Benutzer eingestellte Verbindungsgeschwindigkeit.
Available speeds	Liste verfügbarer Geschwindigkeitswerte.
Health state	Integritätsstatus des Ports. Der Integritätsstatuscode wird in Klammern angezeigt. Folgende Werte sind möglich: <ul style="list-style-type: none"> ● <code>Unknown (0)</code>: Status ist unbekannt. ● <code>OK (5)</code>: Der Port funktioniert normal. ● <code>OK BUT (7)</code>: Kommunikation verloren, aber der Port wird nicht verwendet. ● <code>Minor failure (15)</code>: Kommunikation verloren. Prüfen Sie die Netzwerkverbindung und die Kabelanschlüsse. ● <code>Major failure (20)</code>: Der Port ist defekt. Tauschen Sie den SP, auf dem sich der Port befindet, aus.
Health details	Zusätzliche Integritätsinformationen. Weitere Informationen zur Integrität finden Sie im Anhang A, Referenz.
Aggregated port ID	Wenn der Port in einer Linkzusammenfassung ist, wird die ID der Linkzusammenfassung angezeigt. Managen von Verbindungsbündelungen erläutert, wie Linkzusammenfassungen auf den SP-Ports konfiguriert werden.
Connector type	Physischer Anschlusstyp. Gültige Werte: <ul style="list-style-type: none"> ● <code>unknown</code> ● <code>RJ45</code> ● <code>LC</code> ● <code>MiniSAS_HD</code> ● <code>CopperPigtail</code> ● <code>NoSeparableConnector</code>
MAC address	Eindeutige Kennung einem Netzwerkgerät für die Kommunikation in einem Netzwerksegment zugewiesen.

Tabelle 49. Attribute des Netzwerkports (fortgesetzt)

Attribut	Beschreibung
SFP supported speeds	Liste der unterstützten Geschwindigkeitswerte des eingesteckten SFP-Moduls (Small Form-factor-Pluggable).
SFP supported protocols	Liste der unterstützten Protokolle des eingesteckten SFP-Moduls (Small Form-factor-Pluggable). Gültige Werte: <ul style="list-style-type: none"> • unknown • FibreChannel • Ethernet • SAS

Anzeigen von Ethernetport-Einstellungen

Zeigen Sie Details zu den Netzwerkports an. Sie können nach der Port-ID filtern.

 **ANMERKUNG:** Aktionsbefehl „show“ erläutert, wie das Ausgabeformat geändert wird.

Format

```
/net/port/eth [-id <value>] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des Ports ein.

Beispiel

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/port/eth show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:   ID                = spa_eth2
     Name             = SP A Ethernet Port 2
     SP               = spa
     Protocols        = file, net, iscsi
     MTU size         = 4500
     Requested MTU size = 4500
     Available MTU sizes = 1280-9216
     Linux device name = eth2
     Speed            = 1 Gbps
     Requested speed   = auto
     Available speeds   = 1 Gbps, 10 Gbps, 100 Mbps, auto
     Health state      = OK (5)
     Health details    = "The port is operating normally."
     Aggregated port ID = None
     FSN port ID       = None
     Connector type    = RJ45
     MAC address       = 00:60:16:7A:7F:CF
     SFP supported speeds =
     SFP supported protocols =

2:   ID                = spa_eth3
     Name             = SP A Ethernet Port 3
     SP               = spa
     Protocols        = file, net, iscsi
```

```

MTU size = 1500
Requested MTU size = 1500
Available MTU sizes = 1500, 9000
Linux device name = eth3
Speed = 1 Gbps
Requested speed = auto
Available speeds = 1 Gbps, 10 Gbps, 100 Mbps, auto
Health state = OK (5)
Health details = "The port is operating normally."
Aggregated port ID = None
FSN port ID = None
Connector type = RJ45
MAC address = 00:60:16:7A:7F:CE
SFP supported speeds =
SFP supported protocols =

```

Ändern von Ethernetport-Einstellungen

ANMERKUNG: Die neuen Einstellungen werden auf ein Paar symmetrische Ports in Dual-Speicherprozessorsystemen angewendet.

Ändern Sie die Größe der Maximum Transmission Unit und die Portgeschwindigkeit für einen Ethernetport.

Format

```
/net/port/eth -id <value> set [-mtuSize <value>] [-speed <value>]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des Netzwerkports ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-mtuSize	<p>Geben Sie die MTU-Paketgröße (in Byte) für den Port ein.</p> <ul style="list-style-type: none"> • Wenn ein Ethernet-Port nur Dateischnittstellen enthält, kann die MTU-Größe auf einen angepassten Wert zwischen 1280 und 9216 eingestellt werden. • Wenn ein Ethernet-Port iSCSI-Schnittstellen enthält, sind die erlaubten MTU-Größen 1500 und 9000. <p>Spezifische I/O-Module können den zulässigen Bereich für den Wert der MTU-Größe auch einschränken. Die MTU-Größenwerte 1500 Byte (Standard) und 9000 Byte (Jumbo Frame) werden von allen Schnittstellen und I/O-Modulen unterstützt.</p>
-speed	<p>Geben Sie die Portgeschwindigkeit ein. Das Attribut „Verfügbare Geschwindigkeit“ enthält die Liste der gültigen Werte.</p> <p>ANMERKUNG: Der Port wird während der Anpassung der Geschwindigkeit vorübergehend verknüpft.</p>

Beispiel

Mit dem folgenden Befehl wird die MTU-Größe für Ethernetport 0 (eth0) auf SP A auf 9.000 Byte erhöht:

```
uemcli /net/port/eth -id spa_eth0 set -mtuSize 9000
```

```

Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = spa_eth0

```

```
ID = spb_eth0
Operation completed successfully.
```

Managen von SAS-Ports (nur physische Bereitstellungen)

Sie können die Einstellungen für die SAS-Ports auf jedem SP anzeigen. In der folgenden Tabelle sind die Attribute des Ports beschrieben.

Tabelle 50. SAS-Port-Attribute

Attribut	Beschreibung
ID	ID des Ports.
Name	Name des Ports.
SP	Name des SP, auf dem sich der Port befindet. Gültige Werte: <ul style="list-style-type: none">• spa• spb
Speed	Aktuelle Verbindungsgeschwindigkeit des Ports.
Health state	Integritätsstatus des Ports. Der Integritätsstatuscode wird in Klammern angezeigt. Gültige Werte: <ul style="list-style-type: none">• Unknown (0) : Status ist unbekannt.• OK (5) : Der Port funktioniert normal.• OK BUT (7) : Kommunikation verloren, aber der Port wird nicht verwendet.• Minor failure (15) : Kommunikation verloren. Prüfen Sie die Netzwerkverbindung und die Kabelanschlüsse.• Major failure (20) : Der Port ist defekt. Tauschen Sie den SP, auf dem sich der Port befindet, aus.
Health details	Zusätzliche Integritätsinformationen. In Health details finden Sie Einzelheiten zu den Integritätsinformationen.
Connector type	Physischer Anschlusstyp. Gültige Werte: <ul style="list-style-type: none">• unknown• RJ45• LC• MiniSAS_HD• CopperPigtail• NoSeparableConnector

Anzeigen von SAS-Einstellungen

Zeigen Sie Details zu den SAS-Ports an. Sie können nach der Port-ID filtern.

 **ANMERKUNG:** Aktionsbefehl „show“ erläutert, wie das Ausgabeformat geändert wird.

Format

```
/net/port/sas [-id <value>] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des Ports ein.

Beispiel

```
uemcli /net/port/sas show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:   ID           = spa_sas0
     Name        = SP A SAS Port 0
     SP          = spa
     Speed       =
     Health state = OK_BUT (7)

2:   ID           = spa_sas1
     Name        = SP A SAS Port 1
     SP          = spa
     Speed       = 6 Gbps
     Health state = OK (5)
```

Managen von FC-Ports

Sie können die Einstellungen für die FC-Ports auf jedem SP anzeigen und ändern.

In der folgenden Tabelle sind die Attribute des Ports beschrieben.

Tabelle 51. FC-Port-Attribute

Attribut	Beschreibung
ID	ID des Ports.
Name	Name des Ports.
SP	Name des SP, auf dem sich der Port befindet.
WWN	World Wide Name (WWN) des Ports.
Speed	Aktuelle Verbindungsgeschwindigkeit des Ports.
Requested speed	Vom Benutzer eingestellte Verbindungsgeschwindigkeit.
Available speed	Liste verfügbarer Geschwindigkeitswerte.
Health state	Integritätsstatus des Ports. Der Integritätsstatuscode wird in Klammern angezeigt. Folgende Werte sind möglich: <ul style="list-style-type: none">• Unknown (0): Status ist unbekannt.• OK (5) : Der Port funktioniert normal.• OK BUT (7): Kommunikation verloren, aber der Port wird nicht verwendet.• Minor failure (15): Kommunikation verloren. Prüfen Sie die Netzwerkverbindung und die Kabelanschlüsse.• Major failure (20): Der Port ist defekt. Tauschen Sie den SP, auf dem sich der Port befindet, aus.
Health details	Zusätzliche Integritätsinformationen. Weitere Informationen zur Integrität finden Sie im Anhang A, Referenz.
Connector type	Physischer Anschlusstyp. Gültige Werte: <ul style="list-style-type: none">• unknown• RJ45• LC• MiniSAS_HD• CopperPigtail• NoSeparableConnector

Tabelle 51. FC-Port-Attribute (fortgesetzt)

Attribut	Beschreibung
SFP supported speeds	Liste der unterstützten Geschwindigkeitswerte des eingesteckten SFP-Moduls (Small Form-factor-Pluggable).
SFP supported protocols	Liste der unterstützten Protokolle des eingesteckten SFP-Moduls (Small Form-factor-Pluggable). Gültige Werte: <ul style="list-style-type: none"> • unknown • FibreChannel • Ethernet • SAS
Replication capability	Typ der Replikationsfunktion. Gültige Werte: <ul style="list-style-type: none"> • Sync replication • RecoverPoint

Anzeigen von FC-Porteinstellungen

Zeigen Sie Details zu den FC-Ports an. Sie können nach der Port-ID filtern.

Format

```
/net/port/fc [-id <value>] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des Ports ein.

Beispiel

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/port/fc show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      ID           = spa_fc4
      Name         = SP A FC Port 4
      SP          = spa
      WWN         = 50:06:BD:01:60:05:8E:50:06:01:64:3D:E0:05:8E
      Speed       = 1 Gbps
      Requested speed = auto
      Available speeds = 4 Gbps, 8 Gbps, 16 Gbps, auto
      Health state  = OK (5)
      Health details = "The port is operating normally."
      SFP supported speeds = 4 Gbps, 8 Gbps, 16 Gbps
      SFP supported protocols = FibreChannel
      Replication capability = Sync replication
      SFP supported mode = Multimode
```

Ändern von Porteinstellungen

Ändern Sie die Geschwindigkeit für einen FC-Port.

Format

```
/net/port/fc -id <value> set -speed <value>
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des FC-Ports ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-speed	Geben Sie die Portgeschwindigkeit ein. Das Attribut „Verfügbare Geschwindigkeit“ enthält die Liste der gültigen Werte.  ANMERKUNG: Der Port wird während der Anpassung der Geschwindigkeit vorübergehend verknüpft.

Beispiel

Mit dem folgenden Befehl wird die Geschwindigkeit für FC-Port fc1 auf SP A auf 1 Gb/s festgelegt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/port/fc -id spa_fc1 set -speed 1Gbps
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection
```

```
ID = spa_fc1  
Operation completed successfully.
```

Managen von nicht aktivierten Ports

Mit diesem Befehl können nicht aktivierte Netzwerkports gemanagt werden.

Nicht aktivierte Ports müssen initialisiert werden, um vom System verwendet werden zu können. Verwenden Sie die Befehlszeilenoberfläche, um Informationen zu den nicht aktivierten und entfernten SFP-Systemports (Small Form-factor Pluggable) anzuzeigen.

Tabelle 52. Attribute nicht aktivierter Ports

Attribut	Beschreibung
ID	Portkennung.
Name	Portname.
SP	Speicherprozessor, auf dem sich der Port befindet
Health state	Aktueller Integritätsstatus des Ports Gültige Status sind: <ul style="list-style-type: none">● Unknown (0) : Status ist unbekannt.● OK (5) : Der nicht aktivierte Port ist nicht initialisiert. Er muss aktiviert werden, bevor er verwendet werden kann.● OK (5) : Das SFP-Modul (Small Form-factor Pluggable) in diesem nicht aktivierten Port wurde entfernt. Da der Port nicht verwendet wird, ist keine Aktion erforderlich.
Health details	Zusätzliche Integritätsinformationen.
Connector type	Physischer Anschlusstyp, der dem nicht aktivierten Port zugeordnet ist. Gültige Werte: <ul style="list-style-type: none">● unknown

Tabelle 52. Attribute nicht aktivierter Ports (fortgesetzt)

Attribut	Beschreibung
	<ul style="list-style-type: none"> • RJ45 • LC • MiniSAS_HD • CopperPigtail • NoSeparableConnector
SFP supported speeds	Liste der unterstützten Geschwindigkeitswerte des eingefügten SFP-Moduls.
SFP supported protocols	Liste der unterstützten Protokolle des eingefügten SFP-Moduls. Gültige Werte: <ul style="list-style-type: none"> • unknown • FibreChannel • Ethernet

Anzeigen nicht aktivierter Ports

Verwenden Sie diesen Befehl, um eine Liste von nicht aktivierten Ports auf dem System anzuzeigen.

Zeigen Sie Details zu nicht aktivierten Ports an.

Format

```
/net/port/unc [-id <value>] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des Ports ein.

Beispiel

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/port/unc show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:   ID           = spb_unc5
     Name        = SP B Uncommitted Port 5
     SP         = spb
     Health state = OK (5)
     Health details = "The Small Form-factor Pluggable (SFP) module in this
Uncommitted port has been removed. Since the port is not in use, no action is required."
     Connector type = LC
     SFP supported speeds =
     SFP supported protocols =

2:   ID           = spa_unc5
     Name        = SP A Uncommitted Port 5
     SP         = spa
     Health state = OK (5)
     Health details = "The Uncommitted port is uninitialized. It needs to be
committed before it can be used."
     Connector type = LC
     SFP supported speeds = 10 Gbps
     SFP supported protocols = Ethernet
```

```

3: ID = spb_iom_1_unc0
   Name = SP B I/O Module 1 Uncommitted Port 0
   SP = spb
   Health state = OK (5)
   Health details = "The Uncommitted port is uninitialized. It needs to be
committed before it can be used."
   Connector type = RJ45
   SFP supported speeds =
   SFP supported protocols =

```

Managen von Management-Netzwerkschnittstellen

Konfigurieren Sie Management-Netzwerkschnittstellen so, dass das System, das Netzwerk und konfigurierte Hosts remote gemanagt und überwacht werden. Geben Sie für die Schnittstelle die IP-Adresse und die IP-Adressen von Subnetzmaske und Gateway an. Zeigen Sie Details zu den vorhandenen Managementoberflächen an, die über Connection Utility im System konfiguriert wurden. Jede Managementoberfläche wird durch ihre IP-Protokollversion identifiziert. IPv4 und IPv6 können unabhängig voneinander gleichzeitig konfiguriert werden, sie können jedoch nicht gleichzeitig deaktiviert werden. Die Netzmaske kann mit der geeigneten Präfixlänge angegeben werden, durch „/“ getrennt von der IP-Adresse, z. B. 10.0.0.1/24. Dies ist für IPv4 optional, für IPv6 jedoch obligatorisch. Es können bis zu fünf IPv6-Adressen automatisch zugewiesen werden. Nur eine IPv6-Adresse kann manuell eingestellt werden.

In der folgenden Tabelle sind die Schnittstellenattribute aufgeführt und beschrieben.

Tabelle 53. Schnittstellenattribute

Attribut	Beschreibung
IP protocol version	IP-Protokollversion. Gültige Werte: <ul style="list-style-type: none"> • ipv4 • ipv6
Address origin	Ursprung der IP-Einstellungen. Gültige Werte: <ul style="list-style-type: none"> • disabled: Gibt an, dass die Schnittstelle deaktiviert ist. • automatic: Gibt an, dass die IP-Attribute automatisch von DHCP oder SLAAC eingestellt werden (nur bei IPv6). • static: Gibt an, dass die IP-Attribute manuell eingestellt werden.
IP address	IPv4- oder IPv6-Adresse.
Subnet mask	IPv4-Subnetzmaske.
Gateway	IPv4- oder IPv6-Gateway.
MAC address	Die mit der Schnittstelle verknüpfte MAC-Adresse.

Anzeigen von Managementoberflächen

Zeigen Sie eine Liste von Schnittstellen im System an. Sie können nach der Schnittstellen-ID filtern.

Format

```
/net/if/mgmt show
```

Beispiel

Mit dem folgenden Befehl werden sämtliche Managementoberflächen im System angezeigt.

```
uemcli /net/if/mgmt show
```

```

Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

```

```

1:      IP protocol version = ipv4
        Address origin     = static
        IP address         = 10.0.0.1
        Subnet mask        = 255.255.255.0
        Gateway            = 10.0.0.2

2:      IP protocol version = ipv6
        Address origin     = automatic
        IP address         = 3ffe:80c0:22c:4e:a:0:2:7f/64
        Subnet mask        =
        Gateway            = 3ffe

```

Ändern der Schnittstelleneinstellungen

Ändern Sie die Einstellungen für eine Schnittstelle.

Format

```

/net/if/mgmt set { -ipv4 | -ipv6 } {disabled | automatic | static [-addr <value>] [-netmask
<value>] [-gateway <value>] }

```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-ipv4	Gibt den IPv4-Ursprung an. Folgende Werte sind möglich: <ul style="list-style-type: none"> • disabled: Gibt an, dass die Schnittstelle deaktiviert ist. • automatic: Gibt an, dass die IP-Attribute automatisch von DHCP eingestellt werden. • static: Gibt an, dass die IP-Attribute manuell eingestellt werden.
-ipv6	Gibt den IPv6-Ursprung an. Folgende Werte sind möglich: <ul style="list-style-type: none"> • disabled: Gibt an, dass die Schnittstelle deaktiviert ist. • automatic: Gibt an, dass die IP-Attribute automatisch von DHCP oder SLAAC eingestellt werden. Mehrere Adressen sind möglich. • static: Gibt an, dass die IP-Attribute manuell eingestellt werden.
-addr	Gibt die IPv4- oder IPv6-Adresse der Schnittstelle an. Optional können Sie die Präfixlänge im folgenden Format angeben: <code><IP address>/<prefix length></code> .  ANMERKUNG: Die Standardpräfixlänge für IPv6 ist 64.
-netmask	Geben Sie die IPv4-Subnetzmaske für die Schnittstelle an.  ANMERKUNG: Dies ist optional, wenn Sie die Präfixlänge im -addr Attribut festlegen.
-gateway	Geben Sie den IPv4- oder IPv6 Gateway für die Schnittstelle an.

Beispiel

Mit dem folgenden Befehl werden die IP-Adresse, die Netzmaske und der Gateway für Schnittstelle IF_1 geändert:

```

uemcli /net/if/mgmt set -ipv4 static -addr 192.168.1.1 -netmask 255.255.255.0 -gateway
192.168.1.2

```

```

Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

```

```

Operation completed successfully.

```

Management von Netzwerkschnittstellen

Erstellen Sie Schnittstellen, um den Zugriff zwischen System, Netzwerk und konfigurierten Hosts zu aktivieren und zu steuern. Geben Sie für die Schnittstelle die IP-Adresse und die IP-Adressen von Subnetzmaske und Gateway an.

Sie können folgende Arten von Schnittstellen erstellen:

- iSCSI-Schnittstellen zur Steuerung des Zugriffs auf iSCSI-Speicher. Die Schnittstelle wird einem iSCSI-Node zugewiesen.
- Replikationsschnittstellen für replikationsbezogenen Daten- oder Managementverkehr.

Das System konfiguriert jede Schnittstelle auf einem Paar symmetrischer SP-Ports. Die Schnittstelle kann zwischen SPs verschoben werden. Sie können angeben, welchen SP die Schnittstelle verwenden soll. Dabei kann es sich um einem physischen Port oder einen Verbindungsbündelungs-Port handeln. Es besteht auch die Möglichkeit, die ID eines virtuellen LAN (VLAN) für die Kommunikation mit VLAN-Netzwerken anzugeben.

Die einzelnen Schnittstellen verfügen über eigene IDs.

In der folgenden Tabelle sind die Schnittstellenattribute aufgeführt und beschrieben.

Tabelle 54. Schnittstellenattribute

Attribut	Beschreibung
ID	Die ID der Schnittstelle.
Type	Die Art der Schnittstelle. Folgende Werte sind möglich: <ul style="list-style-type: none"> • <code>iscsi</code>: Schnittstelle für iSCSI-Speicher. • <code>replication</code>: Schnittstelle für replikationsbezogenen Daten- oder Managementverkehr.
Port	Die ID des physischen Ports bzw. der Verbindungsbündelung auf einem SP, auf dem die Schnittstelle ausgeführt wird. In der ID sind der Name des Ports und des SP enthalten.
VLAN ID	Die ID des virtuellen lokalen Netzwerks (VLAN) der Schnittstelle. In der Schnittstelle wird diese ID zur Annahme von Paketen mit VLAN-Tags verwendet. Der Wertebereich erstreckt sich von 1 bis 4095.  ANMERKUNG: Falls keine VLAN-ID angegeben ist (der Standardwert), verfügen die Pakete nicht über VLAN-Tags. Weitere Informationen zu VLANs finden Sie in der Unisphere-Onlinehilfe.
IP address	IPv4- oder IPv6-Adresse.
Subnet mask	IPv4-Subnetzmaske.
Gateway	IPv4- oder IPv6-Gateway.
MAC address	Die MAC-Adresse der Schnittstelle.
SP	Der SP, der die Schnittstelle verwendet.
Health state	Ein numerischer Wert, der die Integrität des Systems angibt. Folgende Werte sind möglich: <ul style="list-style-type: none"> • Unknown (0) • OK (5) • OK BUT (7) • Degraded/Warning (10) • Minor failure (15) • Major failure (20)
Health details	Zusätzliche Integritätsinformationen.

Erstellen von Schnittstellen

Erstellen Sie eine Schnittstelle.

Format

```
/net/if create [ -async ] [-vlanId <value>] -type { iscsi | replication} -port <value> -addr <value> [-netmask <value>] [-gateway <value>]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Erstellungsvorgang im asynchronen Modus aus.
-type	Geben Sie den Schnittstellentyp an. Folgende Werte sind möglich: <ul style="list-style-type: none">• <code>iscsi</code>: Schnittstelle für iSCSI-Speicher.• <code>replication</code>: Schnittstelle für replikationsbezogenen Daten- oder Managementverkehr.
-port	Geben Sie die ID des SP-Ports bzw. der Linkzusammenfassung für die Schnittstelle an. ANMERKUNG: Bei Systemen mit zwei SPs wird eine Dateischnittstelle eher auf einem Paar symmetrischer Ethernetports als auf einem einzelnen angegebenen Port erstellt. Der aktuelle Port wird durch NAS-Server-SP definiert und kann vom angegebenen Port abweichen. Wenn der Benutzer beispielsweise Port <code>spa_eth2</code> angibt, sich der NAS-Server aber auf SP B befindet, wird die Schnittstelle auf Port <code>spb_eth2</code> erstellt.
-vlanId	Geben Sie die ID des virtuellen LAN (VLAN) für die Schnittstelle an. In der Schnittstelle wird diese ID zur Annahme von Paketen mit VLAN-Tags verwendet. Der Wertebereich erstreckt sich von 1 bis 4095. ANMERKUNG: Falls keine VLAN-ID angegeben ist (Standardeinstellung), verfügen die Pakete nicht über VLAN-Tags. Weitere Informationen zu VLANs finden Sie in der Unisphere-Onlinehilfe.
-addr	Geben Sie die IP-Adresse für die Schnittstelle an. Die Präfixlänge sollte an die IPv6-Adresse angehängt werden. Wenn sie ausgelassen wird, beträgt sie standardmäßig 64. Die Standardpräfixlänge für IPv4-Adressen ist 24. Die IPv4-Netzmaske kann im Adressenattribut nach dem Schrägstrich angegeben werden.
-netmask	Geben Sie die Subnetzmaske für die Schnittstelle an. ANMERKUNG: Dieser Qualifizierer ist nicht erforderlich, wenn die Präfixlänge im Attribut <code>-addr</code> festgelegt ist.
-gateway	Geben Sie das Gateway für die Schnittstelle an. ANMERKUNG: Dieser Qualifizierer konfiguriert das Standardgateway für den angegebenen SP des Ports.

Beispiel

Mit dem folgenden Befehl wird eine Replikationsschnittstelle erstellt. Die Schnittstelle erhält die ID `IF_1`:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/if create -type replication -port eth1_spb -addr 10.0.0.1 -netmask 255.255.255.0 -gateway 10.0.0.1
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = IF_1
Operation completed successfully.
```

Anzeigen von Schnittstellen

Zeigen Sie eine Liste von Schnittstellen im System an. Sie können nach der Schnittstellen-ID filtern.

Format

```
/net/if [ {-id <value> | -port <value> | -type <value>} ] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID einer Schnittstelle ein.
-port	Geben Sie den Port ein, mit dem die Schnittstelle verknüpft ist.
-type	Geben Sie den Typ der Schnittstelle an. Gültige Werte: <ul style="list-style-type: none">• iscsi• replication

Beispiel

Mit dem folgenden Befehl werden die Details zu sämtlichen Schnittstellen im System angezeigt.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/if show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      ID                = if_0
      Type                = file
      NAS server          = nas_0
      Port                = eth0_spa
      VLAN ID             =
      VLAN MTU size      =
      IP address          = 3ffe:80c0:22c:4e:a:0:2:7f/64
      Subnet mask         =
      Gateway             = fe80::20a8bff:fe5a:967c
      IPv4 mode           =
      IPv4 address        =
      IPv4 subnet mask    =
      IPv4 gateway        =
      IPv6 mode           = static
      IPv6 address        = 3ffe:80c0:22c:4e:a:0:2:7f/64
      IPv6 link-local address =
      IPv6 gateway        = fe80::20a8bff:fe5a:967c
      MAC address         = EA:3E:22:3F:0C:62
      SP                  = spa
      Preferred           = yes

2:      ID                = if_1
      Type                = file
      NAS server          = nas_1
      Port                = eth1_spb
      VLAN ID             = 1
      VLAN MTU size      = 1500
      IP address          = 192.168.1.2
      Subnet mask         = 255.255.255.0
      Gateway             = 192.168.1.254
      IPv4 mode           = static
      IPv4 address        = 192.168.1.2
      IPv4 subnet mask    = 255.255.255.0
      IPv4 gateway        = 192.168.1.254
      IPv6 mode           =
      IPv6 address        =
      IPv6 link-local address =
      IPv6 gateway        =
      MAC address         = EA:3E:22:21:7A:78
      SP                  = spa
      Preferred           = yes
```

```

3:      ID          = if_2
      Type         = replication
      NAS server   =
      Port        = eth1_spb
      VLAN ID     =
      VLAN MTU size =
      IP address   = 10.103.75.56
      Subnet mask  = 255.255.248.0
      Gateway     = 10.103.72.1
      IPv4 mode    = static
      IPv4 address = 10.103.75.56
      IPv4 subnet mask = 255.255.248.0
      IPv4 gateway = 10.103.72.1
      IPv6 mode    =
      IPv6 address =
      IPv6 gateway =
      MAC address  = EA:3E:22:6D:BA:40
      SP          = spb
      Preferred   = no

```

Ändern der Schnittstelleneinstellungen

Ändern Sie die Einstellungen für eine Schnittstelle.

Format

```
/net/if -id <value> set [-vlanId <value>] [-addr <value>] [-netmask <value>] [-gateway <value>]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID der zu ändernden Schnittstelle ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-vlanId	Geben Sie die ID des virtuellen LAN (VLAN) für die Schnittstelle an. In der Schnittstelle wird diese ID zur Annahme von Paketen mit VLAN-Tags verwendet. Der Wertebereich erstreckt sich von 1 bis 4095.  ANMERKUNG: Falls keine VLAN-ID angegeben ist (der Standardwert), verfügen die Pakete nicht über VLAN-Tags. Weitere Informationen zu VLANs finden Sie in der Unisphere-Onlinehilfe.
-addr	Geben Sie die IP-Adresse für die Schnittstelle an.  ANMERKUNG: Die Präfixlänge sollte an die IPv6-Adresse angehängt werden. Die IPv4-Netzmaske kann im Adressenattribut nach dem Schrägstrich angegeben werden.
-netmask	Geben Sie die IPv4-Subnetzmaske für die Schnittstelle an.
-gateway	Geben Sie das Gateway für die Schnittstelle an.  ANMERKUNG: Das Gateway ist für IPv4 und IPv6 optional. Dieser Qualifizierer konfiguriert das Standardgateway für den angegebenen SP des Ports.

Beispiel

Mit dem folgenden Befehl wird die Gatewayadresse von Schnittstelle IF_1 geändert:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456!/net/if -id IF_1 set -gateway 2001:db8:0:170:a:0:2:70
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection
```

```
ID = IF_1  
Operation completed successfully.
```

Löschen von Schnittstellen

Löschen Sie eine Schnittstelle.

ANMERKUNG: Durch das Löschen einer Schnittstelle kann die Verbindung zwischen den Systemen unterbrochen werden, die die Schnittstelle verwenden (zum Beispiel konfigurierten Hosts).

Format

```
/net/if -id <value> delete
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID der zu löschenden Schnittstelle ein.

Beispiel

Mit dem folgenden Befehl wird die Schnittstelle IF_1 gelöscht:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/if -id IF_1 delete
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection
```

```
Operation completed successfully.
```

Managen statischer IP-Routen

Eine Route bestimmt, wohin ein Paket, dessen Ziel ein nicht lokales Subnetz ist, weitergeleitet wird, um sein Ziel (Netzwerk oder Host) zu erreichen. Eine statische IP-Route ist eine Host-, Netzwerk- oder Standardroute, die manuell konfiguriert ist.

Das System wählt wie folgt eine Route in der Reihenfolge von der konkretesten zur allgemeinsten aus:

1. Host (konkreteste)
2. Netzwerk
3. Standard (allgemeinste)

ANMERKUNG: Bei einer IP-Route wird eine Schnittstelle (IP-Adresse) über ein Gateway mit einem größeren Netzwerk verbunden. Ohne die Route ist die Schnittstelle außerhalb des unmittelbaren Subnetzes nicht mehr zugänglich. Daher stehen mit der Schnittstelle verknüpfte Netzwerk-Shares und Exporte Clients außerhalb des unmittelbaren Subnetzes nicht mehr zur Verfügung.

Die einzelnen Routen verfügen über eigene IDs.

In der folgenden Tabelle sind die Attribute für statische IP-Routen erläutert.

Tabelle 55. Attribute statischer IP-Routen

Attribut	Beschreibung
ID	ID der Route.
Interface ID	ID der Schnittstelle, über die die Route das Gateway erreicht. Die Schnittstelle ist mit einem SP verknüpft. Anzeigen von Schnittstellen erläutert, wie die IDs der Netzwerkschnittstellen angezeigt werden.
Route type	Art der Route. Gültige Werte: <ul style="list-style-type: none"> • <code>default</code>: Das Standardgateway, das verwendet wird, wenn die Route zu einem angeschlossenen Node nicht gefunden wird • <code>host</code>: Statische IP-Route zu einem bestimmten Host • <code>net</code>: Statische Route zu einer Subnetz-IP-Adresse
Target	IP-Adresse des Netzwerk-Node auf der Basis des angegebenen Routentyps. Gültige Werte: <ul style="list-style-type: none"> • Bei der Einstellung „default“ gibt es keinen Wert, da die angegebene IP-Adresse des Gateways verwendet wird. • Bei der Einstellung „host“ wird die IP-Adresse des Hosts als Wert verwendet. • Bei der Einstellung „net“ ist der Wert eine Subnetz-IP-Adresse.
Netmask	Bei einer Subnetzroute ist dies die IP-Adresse der Subnetzmaske.
Gateway	IP-Adresse des Gateways.
Health state	Ein numerischer Wert, der die Integrität des Systems angibt. Gültige Werte: <ul style="list-style-type: none"> • Unknown (0) • OK (5) • OK BUT (7) • Degraded/Warning (10) • Minor failure (15) • Major failure (20)
Health details	Zusätzliche Integritätsinformationen. Weitere Informationen zur Integrität finden Sie im Anhang A, Referenz.

Erstellen von IP-Routen

Erstellen Sie eine IP-Route.

 **ANMERKUNG:** Wenn Sie eine Route ändern möchten, löschen Sie sie, und erstellen Sie sie mit geänderten Einstellungen neu.

Format

```
/net/route create -if <value> -type {default | host -target <value> | net -target <value> [-netmask <value>]} [-gateway <value>]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
<code>-if</code>	Geben Sie die ID der Schnittstelle ein, über die die Route das Gateway erreicht. Anzeigen von Schnittstellen erläutert, wie die IDs der Netzwerkschnittstellen angezeigt werden.  ANMERKUNG: Die für die Route eingegebene Schnittstelle wird unter Umständen nicht verwendet. Die beste Schnittstelle für die Route wird automatisch bestimmt.
<code>-type</code>	Geben Sie die Art der Route ein. Folgende Werte sind möglich: <ul style="list-style-type: none"> • <code>default</code>: Das System verwendet das Standardgateway, wenn die Route zu einem angeschlossenen Node nicht gefunden wird.

Qualifizierer	Beschreibung
	<ul style="list-style-type: none"> • <code>host</code>: Erstellen Sie eine Route zu einem Host. • <code>net</code>: Erstellen Sie eine Route zu einem Subnetz.
<code>-target</code>	Geben Sie je nach dem Wert für <code>-type</code> die IP-Adresse des Ziel-Netzwerk-Node an. Der Wert ist einer der folgenden: <ul style="list-style-type: none"> • Bei „default“ wird die für <code>-gateway</code> angegebene IP-Adresse verwendet. • Bei „host“ wird die IP-Adresse eines Zielhosts angegeben. • Bei „net“ wird die IP-Adresse eines Zielsubnetzes angegeben. Schließen Sie den Qualifizierer <code>-netmask</code> mit ein, um die IP-Adresse der Subnetzmaske anzugeben.
<code>-netmask</code>	Geben Sie für die Route zu einem Subnetz die IP-Adresse der Subnetzmaske ein.
<code>-gateway</code>	Geben Sie die Gateway-IP-Adresse der Route ein.

Beispiel

Mit dem folgenden Befehl wird eine Netzwerkroute für Schnittstelle `if_1` zum Erreichen des Subnetzes `10.64.74.x` mit Gateway `10.64.74.1` erstellt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/route create -if IF_1 -type net -target 10.64.200.10 netmask 255.255.255.0 -gateway 10.64.74.1
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = RT_1
Operation completed successfully.
```

Anzeigen von IP-Routen

Zeigen Sie Details zu IP-Routen an. Sie können nach der Routen-ID filtern.

 **ANMERKUNG:** Aktionsbefehl „`show`“ erläutert, wie das Ausgabeformat geändert wird.

Format

```
/net/route [ {-id <value> | -if <value>} ] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
<code>-id</code>	Gibt die ID einer Route an.
<code>-if</code>	Gibt die Netzwerkschnittstelle, für die Sie die Routen zurückgeben möchten.

Beispiel

Mit dem folgenden Befehl werden Details zu den IP-Routen `RT_1`, `RT_2` und `RT_3` angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/route show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
1:      ID          = RT_1
      Type         = net
```

```

Target      = 10.64.74.10
Netmask     = 255.255.255.0
Gateway     = 10.0.0.1
Interface   = IF_1
Health state = OK (5)

2:  ID      = RT_2
    Type    = default
    Target  =
    Netmask =
    Gateway = 10.64.74.2
    Interface = IF_2
    Health state = OK (5)

3:  ID      = RT_3
    Type    = host
    Target  = 10.64.74.168
    Netmask =
    Gateway = 10.0.0.3
    Interface = IF_3
    Health state = OK (5)

```

Managen von IP-Routen

Ändern Sie eine vorhandene IP-Route.

Format

```

/net/route set route -id <value> set [-type {default | host | net}] [-target <value> [-netmask <value>]] [-gateway <value>]

```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Identifiziert das Routenobjekt.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-type	<p>Geben Sie den Typ der Route an. Es ist nur eine standardmäßige IPv4-Routeninstanz zulässig. Gültige Werte sind folgende (keine Unterscheidung zwischen Groß- und Kleinschreibung):</p> <ul style="list-style-type: none"> • <i>default</i>: Das System verwendet das Standardgateway, wenn keine spezifischere Route für Host oder Netzwerk verfügbar ist. • <i>host</i>: Erstellen Sie eine Route zu einem Host. • <i>net</i>: Erstellen Sie eine Route zu einem Subnetz.
-target	<p>Geben Sie die IP-Zieladresse oder einen Bereich von IP-Adressen an. Wenn der Routentyp</p> <ul style="list-style-type: none"> • <i>host</i> ist, ist der Wert eine IP-Adresse des Hosts. • <i>net</i> ist, ist der Wert eine Subnetz-IP-Adresse im folgenden Format: <IPv4 address>/ [<prefix length>] oder <IPv6 address>/ [<prefix length>]. <p>Die Standardpräfixlänge ist 24 für IPv4 address und 64 für IPv6 address.</p> <p>Gültige Werte:</p> <ul style="list-style-type: none"> • Für eine Standardroute verwendet das System die für -gateway angegebene IP-Adresse. • Geben Sie für eine Hostroute die IP-Adresse eines Zielhosts an. • Geben Sie für eine Netzwerkroute die IP-Adresse eines Zielsubnetzes an. Schließen Sie den Qualifizierer -netmask mit ein, um die IP-Adresse der Subnetzmaske anzugeben.

Qualifizierer	Beschreibung
-netmask	Geben Sie für die Route zu einem Subnetz die IP-Adresse der Subnetzmaske ein.
-gateway	Geben Sie die Gateway-IP-Adresse der Route an.

Beispiel

Der folgende Befehl ändert die IP-Zieladresse in 10.64.200.11, die Netzmaske in 255.255.255.0 und das Gateway in 10.64.74.2 für IP-Route RT_1:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/route -id RT_1 set -target 10.64.200.11 -netmask 255.255.255.0 -gateway 10.64.74.2
```

```
Storage system address: 10.64.75.201
Storage system port: 443
HTTPS connection
```

```
ID = RT_1
Operation completed successfully.
```

Löschen von IP-Routen

Löschen Sie eine IP-Route.

Format

```
/net/route -id <value> delete
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID der zu löschenden Route ein.

Beispiel

Mit dem folgenden Befehl wird die Route RT_1 gelöscht:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/route -id RT_1 delete
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
Operation completed successfully.
```

Managen von Verbindungsbündelungen

Mit der Verbindungsbündelung können Sie zwei physische Ports (z. B. Port 0 und Port 1) auf einem SP zu einem einzelnen logischen Port verknüpfen. Auf dem SP können auf diese Weise bis zu vier Ethernetports eingesetzt werden. Wenn Sie bei einem System mit zwei SPs zwei physische Ports zusammenfassen, werden aus Redundanzgründen die gleiche Ports auf beiden SPs miteinander verknüpft. Wenn Sie beispielsweise die Ports 0 und 1 miteinander verknüpfen, wird jeweils eine Verbindungsbündelung für diese beiden Ports auf SP A und auf SP B erstellt.

Eine ID wird verwendet, um jede Verbindungsbündelung zu identifizieren.

i ANMERKUNG: Damit die Verbindungsbündelung konfiguriert werden kann, muss die Verkabelung bei SP A mit der bei SP B identisch sein.

Die Verbindungsbündelung bietet die folgenden Vorteile:

- Der Gesamtdurchsatz wird erhöht, weil zwei physische Ports in einem logischen Port kombiniert werden.
- Zwischen den verknüpften Ports findet ein grundlegender Lastenausgleich statt, da der Netzwerkverkehr zwischen mehreren physischen Ports aufgeteilt wird.
- Es werden redundante Ports bereitgestellt, sodass beim Ausfall eines Ports in einem verknüpften Portpaar die Systemverbindung nicht abbricht.

i ANMERKUNG: Ports müssen dieselbe MTU-Größe aufweisen, damit sie aggregiert werden können. Verknüpfte Anschlüsse müssen mit demselben logischen Switch verbunden sein. Der Switch muss die Verwendung des IEEE 802.3ad LACP (Dynamic Link Aggregation Control Protocol) unterstützen und dafür konfiguriert sein, das Fehlertoleranz und Lastenausgleich bietet. In diesem LACP-Modus aggregiert das System Schnittstellen zu Gruppen, die die gleiche Geschwindigkeit und Duplexeinstellungen haben. Weitere Informationen zu LACP finden Sie in der Dokumentation zum Switch.

In der folgenden Tabelle sind die Attribute für die Linkzusammenfassung beschrieben.

Tabelle 56. Attribute für die Verbindungsbündelung

Attribut	Beschreibung
ID	Die ID der Verbindungsbündelung. Die ID ist eine Kombination aus der Link-ID und dem SP mit den verknüpften Ports.
Ports	Die IDs der verknüpften physischen Ports. Der Portname umfasst den Namen des SP, der die Ports enthält.
SP	Der Name des SP, auf dem die Ports miteinander verknüpft sind. Gültige Werte: <ul style="list-style-type: none"> • SPA • SPB
MTU size	Die MTU-Paketgröße (in Byte) für die verknüpften Ports. Der Standardwert beträgt 1.500 Byte pro Paket.
Linux device name	Name des Linux-Netzwerkgeräts.
FSN port ID	ID des FSN-Ports, zu dem die Linkzusammenfassung gehört, wenn sie Teil eines FSN ist.
Available MTU size	Liste verfügbarer MTU-Größen. i ANMERKUNG: Diese Option wird als Intervall angezeigt, das durch die Mindest- und Höchstwerte definiert ist, zum Beispiel: 1280-9216.
Health state	Der Integritätsstatus der Verbindungsbündelung. Der Integritätsstatuscode wird in Klammern angezeigt. Folgende Werte sind möglich: <ul style="list-style-type: none"> • Unknown (0) – Status ist unbekannt. • OK (5) – Funktioniert ordnungsgemäß. • OK BUT (7) – Die Verbindung ist unterbrochen, aber die Verbindungsbündelung wird nicht verwendet. • Degraded/Warning (10) – Funktioniert und führt alle Funktionen aus, die Performance ist jedoch eventuell nicht optimal. • Minor failure (15) – Funktioniert und führt alle Funktionen aus, aber die Gesamtperformance ist eingeschränkt. Diese Bedingung hat geringe Auswirkungen auf das System, und das Problem sollte in der näheren Zukunft angegangen werden, aber eine unmittelbare Lösung ist nicht erforderlich. • Major failure (20) – Im System sind Fehler aufgetreten, und einige oder alle Funktionen funktionieren nur noch eingeschränkt oder gar nicht mehr. Dieser Zustand hat

Tabelle 56. Attribute für die Verbindungsbündelung (fortgesetzt)

Attribut	Beschreibung
	<p>erhebliche Auswirkungen auf das System und muss sofort beseitigt werden.</p> <ul style="list-style-type: none"> • <code>Critical failure (25)</code> – Es ist ein Fehler aufgetreten; eine Recovery ist eventuell nicht möglich. Diese Bedingung hat zu Datenverlusten geführt. Der Fehler muss umgehend behoben werden. • <code>Non-recoverable error (30)</code> – Das System ist komplett ausgefallen und kann nicht wiederhergestellt werden.
Health details	Weitere Integritätsinformationen.

Erstellen von Linkzusammenfassungen

Erstellen Sie eine Verbindungsbündelung, indem Sie zwei physische Ports auf einem SP zu einem logischen Port miteinander verbinden.

Format

```
/net/la create -ports <value> [-mtuSize <value>]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
<code>-ports</code>	Geben Sie die IDs der physischen Ports ein, die mit dem SP verknüpft werden sollen. Trennen Sie die IDs mit Komma voneinander ab. Geben Sie z. B. zur Verknüpfung der Ports 0 und 1 mit dem SP A Folgendes ein: <code>eth0_SPA,eth1_SPA</code> .
<code>-mtuSize</code>	Geben Sie die MTU-Größe (in Byte) für die verknüpften Ports ein. Die MTU-Größe kann auf einen Wert zwischen 1280 und 9216 eingestellt werden. Spezifische I/O-Module können den zulässigen Bereich für den Wert der MTU-Größe einschränken. Die MTU-Größenwerte 1500 Byte (Standard) und 9000 Byte (Jumbo Frame) werden von allen Schnittstellen und I/O-Modulen unterstützt.

Beispiel

Mit dem folgenden Befehl werden Port 0 und Port 1 auf SP A bei Standard-MTU-Größe miteinander verknüpft. Da das System über zwei SPs verfügt, werden Port 0 und Port 1 auf SP B ebenfalls verknüpft. Das Ergebnis sind zwei Verbindungsbündelungs-IDs:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/la create -ports "eth0_SPA,eth1_SPA"
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = la0_SPA
ID = la0_SPB
Operation completed successfully.
```

Anzeigen von Verbindungsbündelungen

Zeigen Sie Details zu den Verbindungsbündelungen an. Sie können nach der ID der Verbindungsbündelung filtern.

Format

```
/net/la [-id <value>] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID der Verbindungsbündelung ein.

Beispiel

Mit dem folgenden Befehl werden die Verbindungsbündelungen im System – in diesem Fall für SP A und SP B – angezeigt.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/la show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:   ID           = spa_la_0_2
     SP           = spa
     Ports        = spa_iom_0_eth2, spa_iom_0_eth3
     FSN port ID  = None
     MTU size     = 3456
     Available MTU sizes = 1280-9216
     Linux device name = bond12
     Health state  = OK (5)
     Health details = "The component is operating normally. No action is required."
     Operational status =

2:   ID           = spb_la_0_2
     SP           = spb
     Ports        = spb_iom_0_eth2, spb_iom_0_eth3
     FSN port ID  = None
     MTU size     = 3456
     Available MTU sizes = 1280-9216
     Linux device name = bond12
     Health state  = OK (5)
     Health details = "The component is operating normally. No action is required."
     Operational status =
```

Ändern von Linkzusammenfassungen

Ändern Sie die Einstellungen einer Verbindungsbündelung.

Format

```
/net/la -id <value> set [-ports <value>] [-mtuSize <value>]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID der zu ändernden Verbindungsbündelung ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-ports	Geben Sie die IDs der physischen Ports ein, die mit dem SP verknüpft werden sollen. Trennen Sie die IDs mit Komma voneinander ab. Geben Sie z. B. zur Verknüpfung der Ports 0 und 1 mit dem SP A Folgendes ein: eth0_SPA,eth1_SPA
-mtuSize	Geben Sie die MTU-Größe (in Byte) für die verknüpften Ports ein. Die MTU-Größe kann auf einen Wert zwischen 1280 und 9216 eingestellt werden. Spezifische I/O-Module können den zulässigen Bereich für den Wert der MTU-Größe einschränken. Die MTU-Größenwerte 1500 Byte (Standard) und 9000 Byte (Jumbo Frame) werden von allen Schnittstellen und I/O-Modulen unterstützt.

Beispiel

Mit dem folgenden Befehl wird die MTU-Größe für die Verbindungsbündelung la0_SPA in 9.000 Byte geändert. Das System verfügt über zwei SPs, d. h., die MTU-Größe wird bei beiden Verbindungsbündelungs-IDs aktualisiert:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/la -id la0_SPA set -mtuSize 9000
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection
```

```
ID = la0_SPA  
ID = la0_SPB  
Operation completed successfully.
```

Löschen von Linkzusammenfassungen

Löschen Sie eine Verbindungsbündelung.

Format

```
/net/la [-id <value>] delete
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID der zu löschenden Verbindungsbündelung ein.

Beispiel

Mit dem folgenden Befehl wird die Verbindungsbündelung la0_SPA gelöscht. Das System verfügt über zwei SPs, daher wird die Verbindungsbündelung la0_SPB ebenfalls gelöscht:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/la -id la0_SPA delete
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection
```

```
ID = la0_SPA  
ID = la0_SPB  
Operation completed successfully.
```

Managen von Failsafe-Netzwerkfunktionen (nur physische Bereitstellungen)

Hier finden Sie weitere Informationen zu Failsafe-Netzwerkfunktionen (FSN) und erfahren, welche Attribute zum Managen eines FSN in der CLI verwendet werden.

Ein Failsafe-Netzwerk (FSN) ist eine Hochverfügbarkeitsfunktion, mit der Link-Failover dank der Redundanz auf der Switchebene auf das Netzwerk ausgedehnt wird. Ein FSN wird als ein einziger Link mit einer einzigen MAC-Adresse und potenziell mehreren IP-Adressen angezeigt. Ein FSN kann ein Port, eine Linkzusammenfassung oder eine beliebige Kombination aus beidem sein. Ein FSN bietet gegenüber einer Linkzusammenfassung allein ein zusätzliches Maß an Verfügbarkeit. Linkzusammenfassungen sorgen für Verfügbarkeit bei einem Portausfall. FSNs stellen die Verfügbarkeit bei einem Switchausfall sicher. Jeder Port oder jede Linkzusammenfassung gilt als Einzelverbindung. In einem FSN ist jeweils nur eine Verbindung aktiv. Alle Verbindungen, aus denen das FSN besteht, nutzen gemeinsam eine einzige Hardwareadresse (MAC).

Wenn das System einen Ausfall der aktiven Verbindung erkennt, wechselt es automatisch zur Stand-by-Verbindung im FSN. Diese neue Verbindung nimmt die Netzwerkidentität der ausgefallenen Verbindung an, bis die primäre Verbindung wieder verfügbar ist. Sie können festlegen, welche Verbindung der primäre Port/die primäre Verbindung ist. Um bei einem Hardwareausfall für Konnektivität zu sorgen, erstellen Sie FSN-Geräte auf mehreren I/O-Modulen oder integrierten Ports. Die FSN-Komponenten sind mit unterschiedlichen Switchen verbunden. Wenn der Netzwerkschicht für die aktive Verbindung ausfällt, führt das FSN ein Failover zu einer Verbindung mit einem anderen Switch durch und dehnt so Link-Failover-Funktionen auf das Netzwerk aus.

Wenn Sie eine Replikation von einem Unity-System zu einem anderen durchführen, konfigurieren Sie das FSN als Best Practice auf beiden Systemen auf dieselbe Weise. Sie müssen das FSN manuell auf dem Ziel konfigurieren, bevor Sie die Replikation einrichten. Wenn Sie dagegen das FSN nach der Konfiguration der Replikation auf dem Ziel einrichten, müssen Sie die Option zum Außerkraftsetzen verwenden, um das FSN als Schnittstelle für den Ziel-NAS-Server auszuwählen.

i ANMERKUNG: Eine NAS-Server-IP-Schnittstelle muss auf dem logischen Gerät der höchsten Ebene erstellt werden. Wenn Sie einen Port oder eine Linkzusammenfassung neu verwenden möchten, der bzw. die derzeit als NAS-Server-IP-Schnittstelle für ein FSN genutzt wird, müssen Sie die IP-Schnittstelle vom NAS-Server entfernen, das FSN erstellen und die IP-Schnittstelle erneut dem FSN-Gerät zuweisen.

Tabelle 57. FSN-Attribute

Attribut	Beschreibung
ID	ID des Failsafe-Netzwerkports
SP	Speicherprozessor, auf dem sich das FSN befindet
MTU size	Größe der Maximum Transmission Unit (MTU)
Available MTU sizes	Liste verfügbarer MTU-Größen. i ANMERKUNG: Dies wird als Intervall angezeigt, das durch die Minimal- und Maximalwerte definiert ist, zum Beispiel: 1280-9216.
Linux device name	Name des Linux-Netzwerkgeräts
Primary port	ID des primären Ports, der im FSN verwendet wird. Der primäre Port kann nicht entfernt werden.
Secondary ports	Durch Kommas getrennte Liste der anderen sekundären Ports im FSN. Diese umfasst sowohl Linkzusammenfassungen als auch Ethernetports.
Active port	ID des aktiven Ports für das FSN
Health state	Integritätsstatus des FSN. Gültige Werte: <ul style="list-style-type: none"> OK (5) : Der FSN-Betrieb verläuft normal oder der aktive Port des FSN wurde geändert. Degraded/Warning (10) : Die Performance des FSN hat sich verschlechtert. Minor failure (15) : Eine FSN-Portverbindung ist nicht aktiv.

Tabelle 57. FSN-Attribute (fortgesetzt)

Attribut	Beschreibung
	<ul style="list-style-type: none"> • <code>Major failure (20)</code>: Einem FSN-Port fehlen Ports oder ein FSN-Port ist nicht symmetrisch.
Health details	Ausführliche Integritätsinformationen für das FSN

Erstellen eines FSN

Sie erstellen ein Failsafe-Netzwerk über die Befehlszeilenoberfläche.

Löschen Sie ein Failsafe-Netzwerk mit zwei oder mehr Ports oder Linkzusammenfassungen.

Format

```
/net/fsn create -primaryPort <value> -secondaryPorts <value> [-mtuSize <value>]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
<code>-primaryPort</code>	Geben Sie die ID des primären Ports für das FSN ein. Das kann entweder ein Ethernetport oder eine Linkzusammenfassung sein.
<code>-secondaryPorts</code>	Geben Sie die durch Kommas getrennte Liste zusätzlicher Port- oder Linkzusammenfassungs-IDs ein, die in das FSN eingefügt werden sollen.
<code>-mtuSize</code>	Geben Sie optional die MTU-Größe (Maximum Transmission Unit) für das FSN ein. Die MTU muss im zulässigen Bereich für alle im FSN enthaltenen Ports liegen. Die MTU-Größe kann auf einen Wert zwischen 1280 und 9216 eingestellt werden. Spezifische I/O-Module können den zulässigen Bereich für den Wert der MTU-Größe einschränken. Die MTU-Größenwerte 1500 Byte (Standard) und 9000 Byte (Jumbo Frame) werden von allen Schnittstellen und I/O-Modulen unterstützt.

Beispiel

Im folgenden Beispiel wird ein FSN erstellt, in dem der primäre Port ein einzelner Ethernetport ist und die sekundären Ports eine Linkzusammenfassung sowie einen zusätzlichen einzelnen Ethernetport enthalten.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/fsn create -primaryPort spa_eth0 -secondaryPorts "spa_la_2,spa_eth3"
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = spa_fsn_0
ID = spb_fsn_0

Operation completed successfully.
```

Anzeigen von FSN-Einstellungen

Hier erfahren Sie, wie Sie die Liste und Details aller FSNs auf dem System überprüfen.

Format

```
/net/fsn [-id <value>] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID für den FSN-Port ein, für den Sie Details anzeigen möchten. Geben Sie nicht an, Details zu allen FSNs auf dem System anzuzeigen.

Beispiel

Das folgende Beispiel zeigt die Details für alle FSNs im System an.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/fsn show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:   ID           = spa_fsn_0_1
     SP           = spa
     Primary port = spa_iom_0_eth1
     Secondary ports = spa_la_2
     Active port  = spa_iom_0_eth1
     MTU size     = 1500
     Available MTU sizes = 1500,9000
     Health state = OK (5)
     Health details = "FSN port is operating normally."

2:   ID           = spb_fsn_0_1
     SP           = spb
     Primary port = spb_iom_0_eth1
     Secondary ports = spb_la_2
     Active port  = spb_iom_0_eth1
     MTU size     = 1500
     Available MTU sizes = 1500,9000
     Health state = OK (5)
     Health details = "FSN port is operating normally."
```

Ändern eines FSN

Hier erfahren Sie, wie Sie Änderungen an einem vorhandenen FSN vornehmen.

Sie ändern ein Failsafe-Netzwerk, indem Sie die enthaltenen sekundären Ports oder die MTU-Größen ändern.

Format

```
/net/fsn -id <value> set [-secondaryPorts <value>] [-mtuSize <value>]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des FSN-Ports ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-secondaryPorts	Geben Sie die Liste der vollständigen IDs der physischen Ports und/oder Linkzusammenfassungsports für das FSN ein. Entfernen Sie alle Ports, die aus dem FSN gelöscht werden sollen, und fügen Sie alle Ports hinzu, die Sie einfügen möchten.
-mtuSize	Geben Sie die neue MTU-Größe (Maximum Transmission Unit) für das FSN ein. Die MTU muss im zulässigen Bereich für alle im FSN enthaltenen Ports liegen. Die MTU-Größe kann auf einen Wert zwischen 1280 und 9216 eingestellt werden. Spezifische I/O-Module können den zulässigen Bereich für den Wert der MTU-Größe einschränken. Die MTU-Größenwerte 1500 Byte (Standard) und 9000 Byte (Jumbo Frame) werden von allen Schnittstellen und I/O-Modulen unterstützt.

Beispiel 1

Im folgenden Beispiel wird die MTU-Größe des FSN „spa_fsn_0“ geändert.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/fsn -d spa_fsn_0 set -mtuSize 9000
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = spa_fsn_0
ID = spb_fsn_0

Operation completed successfully.
```

Beispiel 2

Das folgende Beispiel zeigt einen Versuch, den Ethernetport „spa_iom_0_eth2“ zum FSN „spa_fsn_0“ hinzuzufügen. Dieser Ethernetport wird jedoch bereits für eine andere Linkzusammenfassung verwendet und konnte dem FSN nicht unabhängig hinzugefügt werden.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/fsn -d spa_fsn_0 set -secondaryPorts spa_iom_0_eth2
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation failed. Error code: 0x6000851
One of the specified ports cannot be used to configure an FSN because to it is already
included in an FSN or link aggregation. (Error Code:0x6000851)
```

Löschen eines FSN

Hier erfahren Sie, wie Sie ein FSN aus dem System löschen.

Sie können ein Failsafe-Netzwerk löschen.

Format

```
/net/fsn -id <value> delete
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des FSN-Ports ein.

Beispiel

Im folgenden Beispiel wird das FSN „spa_fsn_0“ gelöscht.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/fsn -id spa_fsn_0 delete
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = spa_fsn_0
ID = spb_fsn_0

Operation completed successfully.
```

Managen von DNS-Einstellungen

Ein Domain Name Server (DNS) ist ein Netzwerkdienst, der für die Konvertierung von Domainnamen in ihre jeweiligen IP-Adressen zuständig ist. Im System werden die Netzwerknamen und IP-Adressen der benötigten Netzwerkservices (z. B. NTP- und SMTP-Server) über den DNS-Service aufgelöst. Auf diese Weise können die IP-Adressen von über Netzwerknamen statt direkt über die IP-Adresse adressierten Hosts ermittelt werden.

Bei der anfänglichen Systemkonfiguration müssen Sie die Netzwerkadresse von mindestens einem DNS-Server zur Auflösung von Hostnamen in IP-Adressen angeben. Die DNS-Servereinstellungen können zu einem späteren Zeitpunkt ergänzt, gelöscht oder geändert werden.

Sie können mehrere DNS-Serverdomains konfigurieren und so jede Domain und IP-Adresse der vom System zu verwendenden DNS-Server angeben. Standardmäßig wird der oberste Eintrag in der Liste als aktueller DNS-Server betrachtet. Die weitere Liste ist die Hierarchie der DNS-Server, die verwendet werden sollen, wenn der erste aufgeführte Server nicht zur Verfügung steht. Wenn der erste DNS-Server in der Liste nicht verfügbar ist, fährt das System mit dem nächsten Server in der Liste fort usw. Sie können auch Standard-DNS-Serveradressen angeben, die vom System zuerst verwendet werden sollen.

DNS-Domains ermöglichen das Konfigurieren von DNS-Serveradressen. Alle Adressen werden in benutzerdefinierten DNS-Serverdomains gruppiert. DNS-Einstellungen werden durch die Domain-ID des NAS-Servers identifiziert. DNS-Einstellungen des NAS-Servers sollten die DNS-Auflösung aller Namen innerhalb einer SMB-Serverdomain erlauben, damit das SMB-Protokoll in einer Active Directory-Domain normal funktioniert.

i ANMERKUNG: Sie müssen mindestens einen gültigen DNS-Servereintrag in der Domain für das System konfigurieren. Wenn der letzte DNS-Eintrag gelöscht wird, kann die Netzwerkkommunikation mit dem Gerät beeinträchtigt und möglicherweise die Kommunikation zwischen dem System und den Hosts, die dessen Speicherressourcen verwenden, unterbrochen werden.

In der folgenden Tabelle sind die Attribute für DNS-Domains aufgeführt.

Tabelle 58. DNS-Domain- und Serverattribute

Attribut	Beschreibung
NAS server	ID des zugehörigen NAS-Servers.
Name	Der Name der DNS-Domain.
Auto-configuration enabled	Gibt an, ob DNS-Adressen automatisch konfiguriert werden.
Name servers	Die Liste der IP-Adressen, die den Namensservern in der Domain entsprechen.
Replication sync	Gibt den Status der DNS-Liste in dem NAS-Server an, der als Replikationsziel fungiert. Wenn eine Liste replizierter DNS-Server auf dem Quell-NAS-Server erstellt wird, wird sie automatisch auf dem Ziel synchronisiert. Gültige Werte:

Tabelle 58. DNS-Domain- und Serverattribute (fortgesetzt)

Attribut	Beschreibung
	<ul style="list-style-type: none"> • <code>Not replicated</code>: DNS-Liste ist nicht auf dem Ziel repliziert. • <code>Auto synchronized</code>: DNS-Liste wird automatisch auf dem Replikationsziel synchronisiert. Alle Änderungs- oder Löschvorgänge auf der Quelle werden automatisch auf dem Ziel wiedergegeben. • <code>Overridden</code>: DNS-Liste wurde manuell geändert oder auf dem Replikationsziel außer Kraft gesetzt. Änderungen oder Löschungen von Adressen auf der DNS-Liste auf dem Quell-NAS-Server haben keinen Einfluss auf die außer Kraft gesetzte DNS-Liste auf dem Replikationsziel. <p>ANMERKUNG: Wenn eine DNS-Liste deaktiviert oder von der Quelle gelöscht wird, kann eine außer Kraft gesetzte DNS-Liste auf dem Ziel nicht automatisch deaktiviert oder gelöscht werden.</p>
<code>Source name servers</code>	Liste der IP-Adressen der Namensserver, die auf der Replikationsquelle definiert sind

Konfigurieren der Einstellungen für DNS

Überprüfen Sie die DNS-Einstellungen für das Speichersystem.

Format

```
/net/dns/config set {-nameServer <value> | -auto | -noNameServer}
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
<code>-nameServer</code>	Geben Sie eine Liste der DNS-Serveradressen ein, die als Standardadressen festgelegt werden sollen. Trennen Sie die Adressen mit Komma voneinander ab. Die Adressen werden vom System in der Reihenfolge, in der Sie sie eingeben, verwendet.
<code>-auto</code>	Legen Sie DNS-Adressen dynamisch fest.
<code>-noNameServer</code>	Löschen Sie die Liste der IP-Adressen.

Beispiel

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/dns/config set
-nameServer "128.222.132.29,128.222.132.32"
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
Operation completed successfully.
```

Anzeigen von Standard-DNS-Adressen

Zeigen Sie die als Standard zugewiesenen DNS-Serveradressen an.

Format

```
/net/dns/config show
```

Beispiel

Mit dem folgenden Befehl werden die DNS-Serveradressen angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/dns/config show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1. Auto-configuration enabled = no
   Name servers                = 10.5.3.29,10.5.3.32,2001:db8:170:9400:212:3fff:fe2a:8812
```

Anzeigen von DNS-Serverdomains

Zeigen Sie Details zu konfigurierten DNS-Serverdomains an.

 **ANMERKUNG:** Aktionsbefehl „show“ erläutert, wie das Ausgabeformat geändert wird.

Format

```
/net/nas/dns [-server <value>] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-server	Geben Sie die ID des zugehörigen NAS-Servers ein.

Beispiel

Mit dem folgenden Befehl werden sämtliche DNS-Serverdomains aufgeführt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/dns -server nas_1 show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:   NAS server           = nas_1
     Name                = domain.one.com
     Name servers        = 10.64.74.1,10.64.74.201
     Replication sync    = Overridden
     Source name servers = 10.64.74.1,10.64.74.201
```

Konfigurieren einer DNS-Domain

Konfigurieren Sie eine DNS-Serverdomain.

Format

```
/net/nas/dns -server <value> set { [-name <value>] [-nameServer <value>] [-enabled no] [-replSync {auto | overridden}]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-server	Geben Sie den Namen des zugehörigen NAS-Servers ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-name	Geben Sie den Namen des zugehörigen NAS-Servers ein.
-nameServer	Geben Sie die IP-Adressen der DNS-Server ein. Trennen Sie die Adressen mit Komma voneinander ab.
-enabled	Stellen Sie den Wert auf „no“, um DNS-Einstellungen für den NAS-Server zu löschen. Gültiger Wert ist „no“.
-replSync	Status der DNS-Liste in dem NAS-Server, der als Replikationsziel fungiert. Gültige Werte: <ul style="list-style-type: none">• auto• overridden

Beispiel

Mit dem folgenden Befehl wird die DNS-Domain domain.two.com gelöscht:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/dns -server nas_1 set  
-name "newdomain.one.com"
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection
```

```
Operation completed successfully.
```

Managen von NTP-Servereinstellungen

ANMERKUNG: NTP ist zwar nicht erforderlich, jedoch stehen einige Funktionen ohne es nicht zur Verfügung.

Im System wird das Network Time Protocol (NTP) als Standard für die Synchronisierung der Systemuhr mit anderen Nodes im Netzwerk verwendet. NTP bietet eine Methode zur Synchronisierung von Uhren in verteilten Systemen innerhalb von ca. einer Millisekunde. Ein Windows Active Directory-Domaincontroller kann als Zeitserver fungieren, wenn der Windows-Zeitdienst darauf ausgeführt wird.

Einige Anwendungen funktionieren nicht ordnungsgemäß, wenn die Uhren von System und angeschlossenen Hosts nicht synchronisiert werden. Konfigurieren Sie das System und die angeschlossenen Hosts so, dass der gleiche Zeitserver verwendet wird. Dies hat folgende Auswirkungen:

- Die Gefahr, dass es zwischen System und angeschlossenen Hosts zu Synchronisationsproblemen kommt, wird begrenzt.
- Es gibt weniger Probleme bei der Abstimmung von Zeitstempeln aus den Anmeldeinformationen der unterschiedlichen Systeme.

ANMERKUNG: Bei der Verwendung eines NAS-Servers für CIFS (SMB)-Netzwerkfreigaben kann nicht auf eine Active Directory-Domain zugegriffen werden, es sei denn, das System ist mit maximal fünf Minuten Abweichung vom Active Directory-Controller der Domain synchronisiert, auf der sich die Netzwerkfreigaben befinden.

Sie können insgesamt drei NTP-Serveradressen für das System konfigurieren. Sämtliche NTP-Serveradressen sind in einem einzelnen NTP-Serverdatensatz zusammengefasst. NTP ist zwar nicht erforderlich, jedoch stehen einige Funktionen ohne es nicht zur Verfügung.

In der folgenden Tabelle sind die Attribute für den NTP-Serverdatensatz aufgeführt.

Tabelle 59. Attribute für den NTP-Serverdatensatz

Attribut	Beschreibung
ID	Die ID des NTP-Serverdatensatzes.

Tabelle 59. Attribute für den NTP-Serverdatensatz (fortgesetzt)

Attribut	Beschreibung
Server	Name bzw. IP-Adresse des NTP-Servers.

Erstellen eines NTP-Serverdatensatzes

Erstellen Sie einen NTP-Server und geben Sie von jedem NTP-Server eine IP-Adresse an, die vom System verwendet wird.

 **ANMERKUNG:** Die erste eingegebene NTP-Serveradresse wird standardmäßig die primäre Adresse.

Format

```
/net/ntp/server create -server <value> [-force {noReboot | allowReboot | allowDU}]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-server	Geben Sie den Namen bzw. die IP-Adresse eines NTP-Servers ein.
-force	<p>Akzeptieren Sie den für die Zeitänderung eventuell erforderlichen Systemneustart oder lehnen Sie ihn ab. Wenn Sie nichts angeben, werden Sie gegebenenfalls zur Bestätigung des Neustarts aufgefordert. Gültige Werte:</p> <ul style="list-style-type: none"> • noReboot • allowReboot • allowDU <p> ANMERKUNG: Hinweis: allowDU wird verwendet, wenn sich das System in einem heruntergestuften Zustand befindet oder einen SP aufweist (während des Neustarts sind die Daten nicht verfügbar). Andernfalls wird allowReboot verwendet. Im unbeaufsichtigten Modus wird das System bei Bedarf neu gestartet.</p>

Beispiel

Mit dem folgenden Befehl wird ein NTP-Serverdatensatz mit der NTP-Serveradresse 0.north-america.pool.ntp.org erstellt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/ntp/server create -server 0.north-america.pool.ntp.org
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = NTP_0.north-america.pool.ntp.org
Operation completed successfully.
```

Anzeigen von NTP-Servereinstellungen

Zeigen Sie Details zum NTP-Server an.

 **ANMERKUNG:** Aktionsbefehl „show“ erläutert, wie das Ausgabeformat geändert wird.

Format

```
/net/ntp/server [-id <value>] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des NTP-Servers ein.

Beispiel

Mit dem folgenden Befehl wird der NTP-Serverdatensatz mit zwei NTP-Serveradressen angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/ntp/server show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      ID      = NTP_0.north-america.pool.ntp.org
      Server = 0.north-america.pool.ntp.org

2:      ID      = NTP_1.north-america.pool.ntp.org
      Server = 1.north-america.pool.ntp.org
```

Konfigurieren von NTP-Servereinstellungen

Konfigurieren Sie die NTP-Servereinstellung.

Format

```
/net/ntp/server set -addr <value>
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-addr	Geben Sie eine Liste mit einer oder mehreren IP-Adressen oder Netzwerknamen von jedem NTP-Server ein, die in der NTP-Servereinstellung enthalten sein sollen. Trennen Sie die Adressen mit Komma voneinander ab.

Beispiel

Mit dem folgenden Befehl werden der NTP-Servereinstellung zwei IP-Adressen hinzugefügt:

```
uemcli -d 10.0.0.1 -u Local/joe -p 12345 /net/ntp/server set -addr "10.64.75.55,10.64.75.44"
```

Löschen von NTP-Servereinstellungen

Löschen Sie einen NTP-Serverdatensatz, um die NTP-Einstellungen zu entfernen.

 **ANMERKUNG:** Wenn Sie den primären NTP-Serverdatensatz löschen, wird automatisch festgelegt, welcher NTP-Serverdatensatz verwendet wird.

Format

```
/net/ntp/server -id <value> delete
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID der zu löschenden NTP-Servereinstellung ein.

Beispiel

Der folgende Befehl löscht die NTP-Servereinstellung NTP_10.5.1.207:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/ntp/server -id NTP_10.5.1.207 delete
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
Operation completed successfully.
```

Managen von NIS-Serverdomain

Der NIS-Service (Network Information Service) besteht aus einem Verzeichnisserviceprotokoll zur Pflege und Verteilung von Systemkonfigurationsdaten wie Benutzer- und Gruppeninformationen, Hostnamen und E-Mail-Aliasnamen an Netzwerkhosts. Um beispielsweise Daten auf Dateisystem-Freigaben zu sichern, sind bei einigen NDMP-Produkten Informationen von NIS-Servern erforderlich.

Die Adressen der NIS-Server sind unter den jeweiligen Domain zusammengefasst und mit Domain-IDs gekennzeichnet.

In der folgenden Tabelle sind die Attribute für NIS-Serverdomains aufgeführt.

Tabelle 60. Attribute für NIS-Serverdomains

Attribut	Beschreibung
NAS server	ID des zugehörigen NAS-Servers.
Domain	Der Name der NIS-Serverdomain.
Servers	Liste der IP-Adressen der NIS-Server in der Domain.
Replication sync	Gibt den Status der NIS-Serveradressenliste in dem NAS-Server an, der als Replikationsziel fungiert. Wenn eine Liste replizierter NIS-Server auf dem Quell-NAS-Server erstellt wird, wird sie automatisch auf dem Ziel synchronisiert. Gültige Werte: <ul style="list-style-type: none">• <code>Not replicated</code>: NIS-Liste ist nicht auf dem Ziel repliziert.• <code>Auto synchronized</code>: NIS-Liste wird automatisch auf dem Replikationsziel synchronisiert. Alle Änderungs- oder Löschvorgänge auf der Quelle werden automatisch auf dem Ziel wiedergegeben.• <code>Overridden</code>: NIS-Liste wurde manuell geändert oder auf dem Replikationsziel außer Kraft gesetzt. Änderungen oder Löschungen von Adressen auf der NIS-Liste auf dem Quell-NAS-Server haben keinen Einfluss auf die außer Kraft gesetzte NIS-Liste auf dem Replikationsziel. <p>ANMERKUNG: Wenn eine NIS-Liste deaktiviert oder von der Quelle gelöscht wird, kann eine außer Kraft gesetzte NIS-Liste auf dem Ziel nicht automatisch deaktiviert oder gelöscht werden.</p>
Source servers	Liste der IP-Adressen für die NIS-Server, die auf der Replikationsquelle definiert sind.

Anzeigen von NIS-Serverdomains

Zeigen Sie Details zu NIS-Serverdomains an.

Format

```
/net/nas/nis [-server <value>] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-server	Geben Sie die ID des zugehörigen NAS-Servers ein.

Beispiel

Mit dem folgenden Befehl werden Details zur NIS-Serverdomain angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/nis show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:   NAS server      = nas_0
     Domain         = nis.one.com
     Servers        = nisserver1.one.com,10.64.74.1
     Replication sync = Overridden
     Source servers = 10.64.74.74,10.64.74.1
```

Ändern von NIS-Serverdomains

Fügen Sie einer NIS-Serverdomain NIS-Serveradressen hinzu.

Format

```
/net/nas/nis -server <value> set { [-domain <value>] [-ip <value>] | {-enabled no}} [-replSync {auto | overridden}]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-server	Geben Sie die ID des zugehörigen NAS-Servers ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-domain	Geben Sie den NIS-Domainnamen ein.
-ip	Geben Sie die IP-Adressen der NIS-Server an, die zur Domain gehören sollen. Trennen Sie die Adressen mit Komma voneinander ab.
-enabled	Legen Sie den Wert auf „no“ fest, um die NIS-Einstellungen für den NAS-Server zu löschen. Gültiger Wert ist „no“.

Qualifizierer	Beschreibung
-replSync	Status der NIS-Liste in dem NAS-Server, der als Replikationsziel fungiert. Gültige Werte: <ul style="list-style-type: none"> • auto • overridden

Beispiel

Mit dem folgenden Befehl wird der NIS-Serverdomain nis.two.com eine neue IP-Adresse hinzugefügt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/nis -id nis.two.com set -
ip "10.64.74.200"
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
Operation completed successfully.
```

Managen von SMTP-Servereinstellungen

Das System verwendet das Simple Mail Transport Protocol (SMTP), um E-Mail-Warnmeldungen zu Systemereignissen (basierend auf dem Schweregrad) an bestimmte E-Mail-Adressen und den EMC Support zu senden. Sobald Sie die IP-Adresse des zu verwendenden SMTP-Servers angegeben haben, können Sie die folgenden Funktionen im System aktivieren:

- E-Mail-Warnmeldungen: Das System sendet E-Mail-Warnmeldungen zu Systemereignissen an die angegebene IP-Adresse, wenn eine bestimmte Warn- oder Fehlerbedingung eintritt. Das System verwendet die erste angegebene IP-Adresse.

[Konfigurieren von Warnmeldungseinstellungen](#) behandelt die Angabe des Warnmeldungs-Schweregrades. Sämtliche IP-Adressen werden unter einer SMTP-Servereinstellung zusammengefasst.

In der folgenden Tabelle sind die Attribute für SMTP-Server-Einstellungen aufgeführt.

Tabelle 61. Attribute für SMTP-Server

Attribut	Beschreibung
ID	Die ID des SMTP-Servers.
Address	Die IP-Adresse des SMTP-Servers.
Port	Der Port des SMTP-Servers.
Encryption level	Verschlüsselungsstufe (SSL-Methode) für die Kommunikation mit dem SMTP-Server. Gültige Werte: <ul style="list-style-type: none"> • Keine • Start TLS • SSL
Authentication type	Art der Authentifizierung für die Anmeldung beim SMTP-Server. Gültige Werte: <ul style="list-style-type: none"> • None • Plain • Anmeldung • CRAM_MD5 • DIGEST_MD5
User name	Benutzername zur Anmeldung beim SMTP-Server.
Bypass proxy	Gibt an, ob die globalen Proxyeinstellungen umgangen werden oder nicht. <ul style="list-style-type: none"> • yes: Globale Proxyserver-Einstellungen werden ignoriert und der SMTP-Server wird direkt aufgerufen.

Tabelle 61. Attribute für SMTP-Server (fortgesetzt)

Attribut	Beschreibung
	<ul style="list-style-type: none"> no (Standardeinstellung): Globale Proxyserver-Einstellungen dienen zum Zugriff auf den SMTP-Server.

Anzeigen von SMTP-Servereinstellungen

Zeigen Sie die IP-Adressen der SMTP-Server an.

 **ANMERKUNG:** Aktionsbefehl „show“ erläutert, wie das Ausgabeformat geändert wird.

Format

```
/net/sntp [-id <value>] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID eines SMTP-Servers ein.

Beispiel

Mit dem folgenden Befehl werden die IP-Adressen der beiden SMTP-Server in der Einstellung aufgeführt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/sntp show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      ID          = default
      Address      = 192.168.0.15
      Port         = 25
      Encryption level = SSL
      Authentication type = Plain
      User name     = test
      Bypass proxy  = no
```

Konfigurieren von SMTP-Servereinstellungen

Geben Sie die IP-Adressen für die SMTP-Servereinstellung ein.

Format

```
/net/sntp -id <value> set -addr <value> [-port <value>] [-encryptLevel {none|startTLS|ssl}] [-authType {none|plain|login|cram_md5|digest_md5}] [-user <value> {-passwd <value> |-passwdSecure}] [-bypassproxy {yes|no}]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID eines SMTP-Servers ein, für den Sie eine IP-Adresse angeben möchten.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-addr	Geben Sie die IP-Adresse des SMTP-Servers an. Es kann sich entweder um eine IPv4- oder eine IPv6-Adresse handeln.
-port	Geben Sie den Port des SMTP-Servers ein.
-encryptLevel	Gibt die Verschlüsselungsstufe (SSL-Methode) des SMTP-Servers an. Gültige Werte: <ul style="list-style-type: none"> • none • startTLS • ssl
-authType	Gibt den Authentifizierungstyp des SMTP-Servers an. Gültige Werte: <ul style="list-style-type: none"> • none • plain • login • cram_md5 • digest_md5
-user	Gibt den Benutzernamen des SMTP-Servers an.
-passwd	Gibt das Passwort des SMTP-Servers an.
-passwdSecure	Gibt ein Passwort im sicheren Modus an. Der Benutzer wird aufgefordert, das Passwort einzugeben.
-bypassproxy	Gibt an, ob die globalen Proxyeinstellungen beim Zugriff auf den SMTP-Server umgangen werden. Gültige Werte: <ul style="list-style-type: none"> • yes: Ignoriert globale Proxyserver-Einstellungen, um direkt auf den SMTP-Server zuzugreifen. • no (Standardeinstellung): Verwendet die globalen Proxyserver-Einstellungen.

Beispiel

Mit dem folgenden Befehl wird die IP-Adresse des vom System verwendeten Standard-SMTP-Servers festgelegt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/smtp -id default set -addr 10.64.74.16 -port 25 -encryptLevel ssl -authType plain -user test -passwd test
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
Operation completed successfully.
```

Managen von NDMP-Servereinstellungen

Das Network Data Management Protocol (NDMP) bietet einen Standard zur Sicherung von Dateiservern in einem Netzwerk. Mit NDMP kann über zentrale Anwendungen ein Backup von Servern ausgeführt werden, die sich auf verschiedenen Plattformen bzw. Plattformversionen befinden. NDMP vermeidet Engpässe im Netz, indem der Steuerpfadverkehr vom Datenpfadverkehr isoliert wird. Dadurch werden zentral verwaltete und überwachte lokale Backup-Vorgänge möglich.

Aktivieren Sie NDMP, wenn Sie mit NDMP-Produkten Daten auf Dateisystemspeicher sichern und wiederherstellen möchten.

In der folgenden Tabelle sind die Attribute für NDMP-Server aufgeführt.

Tabelle 62. Attribute für NDMP-Server

Attribut	Beschreibung
NAS server	ID des zugehörigen NAS-Servers.
Enabled	Hier ist angegeben, ob NDMP aktiviert ist. Gültige Werte sind „yes“ und „no“.

Tabelle 62. Attribute für NDMP-Server (fortgesetzt)

Attribut	Beschreibung
Username	Der Benutzername für den Zugriff auf den NDMP-Server.
Password	Das Passwort für den Zugriff auf den NDMP-Server.

Anzeigen von NDMP-Servereinstellungen

Überprüfen Sie, ob NDMP aktiviert oder deaktiviert ist.

Format

```
/net/nas/ndmp [-server <value>] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-server	Geben Sie die ID des zugehörigen NAS-Servers ein.

Beispiel

Mit dem folgenden Beispiel werden die NDMP-Einstellungen angezeigt. Daraus geht hervor, dass NDMP aktiviert ist:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/ndmp show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
1:   NAS server = nas_0
     Enabled   = yes
```

```
2:   NAS server = nas_1
     Enabled   = no
```

Konfigurieren von NDMP-Servereinstellungen

Konfigurieren Sie die NDMP-Servereinstellungen. Dies umfasst auch die Aktivierung bzw. Deaktivierung von NDMP und die Änderung des Passworts für den Zugriff auf den NDMP-Server.

Format

```
/net/nas/ndmp -server <value> set -enabled {yes {-passwd <value> | -passwdSecure} | no}
```

Objektqualifizierer

Qualifizierer	Beschreibung
-server	Geben Sie die ID des zugehörigen NAS-Servers ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-enabled	Hiermit wird NDMP aktiviert. Gültige Werte sind „yes“ und „no“. Bei Auswahl von „yes“ muss das Passwort für den NDMP-Server eingegeben werden.
-passwd	Geben Sie das Passwort für den NDMP-Server ein. Das Passwort wird bei der Aktivierung von NDMP benötigt.
-passwdSecure	Geben Sie das Passwort im sicheren Modus an – der Benutzer wird aufgefordert, das Passwort und die Passwortbestätigung einzugeben.

Beispiel

NDMP wird mit dem folgenden Befehl aktiviert:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/ndmp -server nas_0 set -enabled yes -passwd "Password0123"
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
Operation completed successfully.
```

Managen von LDAP-Einstellungen

Das Lightweight Directory Access Protocol (LDAP) ist ein Anwendungsprotokoll zur Durchführung von Abfragen und Änderungen in Verzeichnisservices in TCP/IP-Netzwerken. LDAP ermöglicht ein zentrales Management zur Netzwerkauthentifizierung und zur Autorisierung, da das Benutzer- und Gruppenmanagement im gesamten Netzwerk zusammengefasst wird. Die Integration des Systems in eine vorhandene LDAP-Umgebung ermöglicht die Steuerung des Benutzer- und Benutzergruppenzugriffs auf das System über die Unisphere-CLI bzw. über Unisphere.

Nach der Konfiguration der LDAP-Einstellungen für das System können Sie aus dem Kontext einer etablierten LDAP-Verzeichnisstruktur heraus Benutzer und Benutzergruppen managen. Sie können beispielsweise der Unisphere-CLI Zugriffsberechtigungen auf der Grundlage vorhandener Benutzer und Gruppen zuweisen.

i ANMERKUNG: Die LDAP-Einstellungen werden nur zur einfacheren Steuerung der Unisphere-CLI und von Unisphere, nicht jedoch für den Zugriff auf Speicherressourcen verwendet.

In der folgenden Tabelle sind die Attribute für LDAP-Einstellungen aufgeführt.

i ANMERKUNG: Wenn Sie LDAP mit SSL verwenden möchten, müssen Sie das CA-Zertifikat des LDAP-Servers mit dem Befehl `-upload` in das System hochladen, bevor Sie die LDAP-Einstellungen konfigurieren. Beispiel:

```
uemcli -d 10.0.0.1 -u admin -p MyPwd -upload -f /tmp/myldapservercertificate.cer /sys/cert -type CA -service Mgmt_LDAP
```

Tabelle 63. Attribute für LDAP-Server

Attribut	Beschreibung
ID	Die ID des LDAP-Servers.
Auto discovery enabled	Gibt an, ob die LDAP-Servernamen mithilfe von DNS erstellt werden. Um diese Funktion nutzen zu können, muss der DNS-Server für die LDAP-Domain als der erste Server in der Liste der DNS-Server konfiguriert sein.
Name	Serverhostnamen oder IP-Adressen der LDAP-Server, angegeben als durch Komma getrennte Liste. Wenn IP-Adressen angegeben werden, muss der DNS-Server für die LDAP-Domain mit einer Rückwärtssuche konfiguriert werden, damit diese den vollständig

Tabelle 63. Attribute für LDAP-Server (fortgesetzt)

Attribut	Beschreibung
	qualifizierten Domainnamen für die angegebenen IP-Adressen bereitstellt.
Domain name	Der Domainname des LDAP-Servers.
Port	Die vom Verzeichnisserver für die LDAP-Kommunikation verwendete Portnummer. LDAP verwendet standardmäßig Port 389 und LDAPS (LDAP over SSL) verwendet Port 636. Geben Sie für die Forest-Level-Authentifizierung Port 3268 für LDAP oder Port 3269 für LDAPS an.
Protocol	Hiermit wird angegeben, ob das LDAP-Protokoll bei der sicheren Kommunikation im Netzwerk auf SSL zurückgreift. SSL bietet Verschlüsselungs- und Authentifizierungsfunktionen. Bei SSL werden Daten im Netzwerk verschlüsselt und Nachrichten sowie Server authentifiziert. Folgende Werte sind möglich: <ul style="list-style-type: none"> • <code>ldap</code> (Standard): LDAP ohne SSL • <code>ldaps</code> — LDAP mit SSL.
Bind DN	DN (Distinguished Name) für einen Benutzer mit Administratorrechten auf dem LDAP-Server. Der DN kann in mehreren Formaten ausgedrückt werden. Beispiel: <code>cn=Administrator, cn=Users, dc=mycompany, dc=com</code> <code>Administrator@mycompany.com</code> <code>mycompany.com/Administrator</code>
Bind password	Für die Anbindung an den LDAP-Server zu verwendendes Passwort. Dies ist das Passwort für den Benutzer, der in <code>Bind DN</code> -Attribut.
User search path	Pfad auf dem Verzeichnisserver, in dem nach Benutzern gesucht werden soll. Zum Beispiel: <code>ou=People, dc=lss, dc=emc, dc=com</code>  ANMERKUNG: Auf einem Active Directory-Server wird ein Standardsuchpfad verwendet.
Group search path	Pfad, in dem nach Gruppen auf dem Verzeichnisserver gesucht werden soll. Zum Beispiel: <code>uid=<name>, ou=people, dc=<domaincomponent>, oder dc=<domain component></code>  ANMERKUNG: Auf einem Active Directory-Server wird ein Standardsuchpfad verwendet.
User ID attribute	Der Name des LDAP-Attributs, dessen Wert auf die Benutzer-ID hinweist. Der Standardwert lautet „uid“. Geben Sie für die Forest-Level-Authentifizierung <code>userPrincipalName</code> an.
Group name attribute	Der Name des LDAP-Attributs, dessen Wert auf den Gruppennamen hinweist. Der Standardwert lautet „cn“.
User object class	LDAP-Objektklasse für Benutzer. Der Standardwert lautet „user“. In Active Directory werden Gruppen und Benutzer im gleichen hierarchischen Verzeichnispfad gespeichert, und die Klasse wird als Gruppe bezeichnet.
Group object class	LDAP-Objektklasse für Gruppen. Der Standardwert lautet „group“. In Active Directory werden Gruppen und Benutzer im gleichen Verzeichnispfad gespeichert und die Klasse wird Gruppe genannt.

Tabelle 63. Attribute für LDAP-Server (fortgesetzt)

Attribut	Beschreibung
Group member class	Der Name des LDAP-Attributs, dessen Wert die Namen der Mitglieder einer Gruppe enthält. Der Standardwert lautet „member“.
Certificate filepath	Pfad zu (Dateiname der) Datei des vertrauenswürdigen Zertifikat, das für die unidirektionale LDAP-Serverauthentifizierung verwendet wird. Die Kette darf nicht das Serverzertifikat enthalten.
LDAP timeout	Zeitüberschreitung des LDAP-Servers in Millisekunden. Falls das System nach der angegebenen Zeitüberschreitung keine Antwort vom LDAP-Server empfängt, werden keine weiteren Anforderungen gesendet. Der Standardwert beträgt 10.000 Millisekunden bzw. 10 Sekunden.

Konfigurieren von LDAP-Einstellungen

Konfigurieren Sie die LDAP-Einstellungen zur Steuerung des Benutzerzugriffs auf die Unisphere-CLI und Unisphere von einem LDAP-Server aus.

ANMERKUNG: Wenn Sie LDAP mit SSL verwenden möchten, müssen Sie das CA-Zertifikat des LDAP-Servers mit dem Befehl `-upload` in das System hochladen, bevor Sie die LDAP-Einstellungen konfigurieren. Beispiel:

```
uemcli -d 10.0.0.1 -u admin -p MyPwd -upload -f /tmp/myldapservercertificate.cer
/sys/cert -type CA -service Mgmt_LDAP
```

Format

```
/net/ldap create [{-name <value> | -autoDiscoveryEnabled}] -domain <value> [-port <value>]
[-protocol {ldap|ldaps -certFilePath <value>}] -bindDn <value> {-bindPasswd <value> |
-bindPasswdSecure} [-userSearchPath <value>] [-groupSearchPath <value>] [-userIdAttr <value>] [-
groupNameAttr <value>] [-userObjectClass <value>] [-groupObjectClass <value>] [-groupMemberAttr
<value>] [-timeout <value>]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-name	Geben Sie die LDAP-IP-Adressen oder Hostnamen als durch Komma getrennte Zeichenfolge ein. Wenn IP-Adressen angegeben werden, muss der DNS-Server für die LDAP-Domain mit einer Rückwärtssuche konfiguriert werden, damit diese den vollständig qualifizierten Domainnamen für die angegebene IP-Adresse bereitstellt.
-autoDiscoveryEnabled	Geben Sie an, ob das System die LDAP-Server-Adressen mithilfe von DNS erhalten soll. Um diese Funktion nutzen zu können, muss der DNS-Server für die LDAP-Domain als der erste Server in der Liste der DNS-Server konfiguriert sein. ANMERKUNG: <code>-autoDiscoveryEnabled</code> ist die Standardeinstellung, wenn Sie auch keinen <code>-name</code> angeben bzw. <code>-autoDiscoveryEnabled</code> .
-domain	Geben Sie den Domainnamen des LDAP-Servers ein.
-protocol	Geben Sie an, ob das LDAP-Protokoll für die sichere Netzwerkkommunikation auf SSL zurückgreift. SSL bietet Verschlüsselungs- und Authentifizierungsfunktionen. Bei SSL werden Daten im Netzwerk verschlüsselt und Nachrichten sowie Server authentifiziert. Gültige Werte: <ul style="list-style-type: none"> • <code>ldap</code> (Standard): LDAP ohne SSL • <code>ldaps</code> — LDAP mit SSL.

Qualifizierer	Beschreibung
-certFilePath	Pfad zu (Dateiname der) Datei des vertrauenswürdigen Zertifikat, das für die unidirektionale Serverauthentifizierung verwendet wird.  ANMERKUNG: Wenn der Wert von <code>-protocol ldaps</code> ist, dann ist dieser Qualifier erforderlich.
-port	Geben Sie die vom Verzeichnisserver für die LDAP-Kommunikation verwendete Portnummer ein. Standardmäßig wird für LDAP Port 389 verwendet; bei LDAP über SSL kommt Port 636 zum Einsatz. Geben Sie für die Forest-Level-Authentifizierung Port 3268 für LDAP oder Port 3269 für LDAPS an.
-bindDn	Geben Sie den DN (Distinguished Name) für einen Benutzer mit Administratorrechten auf dem LDAP-Server ein. Der DN kann in mehreren Formaten ausgedrückt werden. Beispiel: cn=Administrator, cn=Users, dc=mycompany, dc=com Administrator@mycompany.com mycompany.com/Administrator
-bindPasswd	Geben Sie das Passwort für die Anbindung an den LDAP-Server ein. Dies ist das Passwort für den Benutzer, der in Bind DN -Attribut.
-bindPasswdSecure	Geben Sie das Passwort im sicheren Modus an – der Benutzer wird aufgefordert, das Passwort einzugeben.
-userSearchPath	Geben Sie den Pfad auf dem Verzeichnisserver ein, in dem nach Benutzern gesucht werden soll. Zum Beispiel: ou=People, dc=lss, dc=emc, dc=com  ANMERKUNG: Auf einem Active Directory-Server wird ein Standardsuchpfad verwendet.
-groupSearchPath	Geben Sie den Pfad auf dem Verzeichnisserver ein, in dem nach Gruppen gesucht werden soll. Zum Beispiel: ai.uid=<name>, ou=people, dc=<domaincomponent>, oder dc=<domain component> .  ANMERKUNG: Auf einem Active Directory-Server wird ein Standardsuchpfad verwendet.
-userIdAttr	Geben Sie den Namen des LDAP-Attributs ein, dessen Wert auf die Benutzer-ID hinweist. Der Standardwert ist <code>uid</code> .
-groupNameAttr	Geben Sie die LDAP-Objektklasse für Benutzer ein. Der Standardwert lautet „user“. In Active Directory werden Gruppen und Benutzer im gleichen hierarchischen Verzeichnispfad gespeichert, und die Klasse wird als Gruppe bezeichnet.
-groupObjectClass	Geben Sie die LDAP-Objektklasse für Gruppen ein. Der Standardwert lautet „group“. In Active Directory werden Gruppen und Benutzer im gleichen Verzeichnispfad gespeichert und die Klasse wird Gruppe genannt.
-groupMemberAttr	Geben Sie den Namen des LDAP-Attributs ein, dessen Wert die Namen der Mitglieder einer Gruppe enthält. Der Standardwert ist <code>member</code> .
-timeout	Geben Sie die Zeitüberschreitung des LDAP-Servers in Millisekunden ein. Falls das System nach der angegebenen Zeitüberschreitung keine Antwort vom LDAP-Server empfängt, werden keine weiteren Anforderungen gesendet. Der Standardwert beträgt 10.000 Millisekunden, d. h. 10 Sekunden.

Beispiel 1: Erstellen einer LDAP-Konfiguration mit einer bestimmten angegebenen LDAP-Serveradresse

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/ldap create -name lpso242.lss.emc.com
-domain domain.example.com -port 389 -protocol ldap -bindDn "cn=Directory Manager"
-bindPasswd Password0123 -userSearchPath "ou=People, dc=lss, dc=emc, dc=com" -groupSearchPath
"ou=Groups, dc=lss, dc=emc, dc=com" -userIdAttr "uid" -groupNameAttr "cn" -userObjectClass
"interOrgPerson" -groupObjectClass "groupOfUniqueNames" -groupMemberAttr "uniqueMember" -timeout
40000
```

```
Storage system address: 10.64.75.201
Storage system port: 443
HTTPS connection
```

```
ID = LDAP_1
Operation completed successfully.
```

Beispiel 2: Erstellen einer LDAP-Konfiguration mit mehreren angegebenen LDAP-Serveradressen

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/ldap create -name
lpso242.lss.emc.com,lpso243.lss.emc.com -domain domain.example.com -port 389 -protocol
ldap -bindDn "cn=Directory Manager" -bindPasswd Password0123 -userSearchPath
"ou=People,dc=lss,dc=emc,dc=com" -groupSearchPath "ou=Groups,dc=lss,dc=emc,dc=com" -userIdAttr
"uid" -groupNameAttr "cn" -userObjectClass "interOrgPerson" -groupObjectClass
"groupOfUniqueNames" -groupMemberAttr "uniqueMember" -timeout 40000
```

```
Storage system address: 10.64.75.201
Storage system port: 443
HTTPS connection
```

```
ID = LDAP_1
Operation completed successfully
```

Beispiel 3: Erstellen einer LDAP-Konfiguration mit automatischer Erkennung über DNS zum Konfigurieren der Serveradressen

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/ldap create
-autoDiscoveryEnabled -domain domain.example.com -port 389 -protocol ldap -bindDn
"cn=Administratortor,ou=Users,dc=domain,dc=example,dc=com" -bindPasswd Password0123 -userSearchPath
"ou=Users,dc=domain,dc=example,dc=com" -groupSearchPath "ou=Groups,dc=domain,dc=example,dc=com"
-userIdAttr "uid" -groupNameAttr "cn" -userObjectClass "interOrgPerson" -groupObjectClass
"groupOfUniqueNames" -groupMemberAttr "uniqueMember" -timeout 40000
```

```
Storage system address: 10.64.75.201
Storage system port: 443
HTTPS connection
```

```
ID = LDAP_1
Operation completed successfully
```

LDAP-Einstellungen anzeigen

Zeigen Sie Details zu den konfigurierten LDAP-Einstellungen an.

 **ANMERKUNG:** Aktionsbefehl „show“ erläutert, wie das Ausgabeformat geändert wird.

Format

```
/net/ldap [-id <value>] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID der LDAP-Einstellung ein.

Beispiel

Mit dem folgenden Befehl werden die LDAP-Einstellungen angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/ldap show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      ID           = LDAP_1
      Server name    = lps0242.lss.emc.com
      Domain         = local
      Protocol       = ldap
      Port           = 389
```

Ändern von LDAP-Einstellungen

Aktualisieren Sie eine konfigurierte LDAP-Einstellung.

ANMERKUNG: Wenn Sie LDAP mit SSL verwenden möchten, müssen Sie das CA-Zertifikat des LDAP-Servers mit dem Befehl `-upload` in das System hochladen, bevor Sie die LDAP-Einstellungen konfigurieren. Beispiel:

```
uemcli -d 10.0.0.1 -u admin -p MyPwd -upload -f /tmp/myldapserversertificate.cer
/sys/cert -type CA -service Mgmt_LDAP
```

Format

```
/net/ldap -id <value> set [{-name <value> | -autoDiscoveryEnabled}] [-port <value>] [-
protocol {ldap | ldaps {-certFilePath <value>}}] [-bindDn <value>] [-bindPasswd <value> |
-bindPasswdSecure] [-userSearchPath <value>] [-groupSearchPath <value>] [-userIdAttr <value>] [-
groupNameAttr <value>] [-userObjectClass <value>] [-groupObjectClass <value>] [-groupMemberAttr
<value>] [-timeout <value>]
```

Objektqualifizierer

Qualifizierer	Beschreibung
<code>-id</code>	Geben Sie die ID der zu ändernden LDAP-Einstellung ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
<code>-name</code>	Geben Sie die IP-Adressen bzw. die Hostnamen der primären Verzeichnisserver für die Authentifizierung ein. Die eingegebenen Werte hängen vom Format des Eintrags für das Themenfeld in jedem Zertifikat des Verzeichnisservers ab. In der Regel ist ein Hostname erforderlich. Geben Sie die LDAP-IP-Adressen oder Hostnamen als durch Komma getrennte Zeichenfolge ein. Wenn IP-Adressen angegeben werden, muss der DNS-Server für die LDAP-Domain mit einer Rückwärtssuche konfiguriert werden, damit diese den vollständig qualifizierten Domainnamen für die angegebenen IP-Adressen bereitstellt.
<code>-autoDiscoveryEnabled</code>	Geben Sie an, ob das System die LDAP-Serveradressen oder Hostnamen mithilfe von DNS erhalten soll. DNS muss so konfiguriert sein, dass diese Option wirksam wird. ANMERKUNG: <code>-autoDiscoveryEnabled</code> ist die Standardeinstellung, wenn Sie auch nichts angeben <code>-name</code> oder <code>-autoDiscoveryEnabled</code> .
<code>-domain</code>	Geben Sie den Domainnamen des LDAP-Servers ein.

Qualifizierer	Beschreibung
-port	Geben Sie die vom Verzeichnisserver für die LDAP-Kommunikation verwendete Portnummer ein. Standardmäßig wird für LDAP Port 389 verwendet; bei LDAP über SSL kommt Port 636 zum Einsatz. Geben Sie für die Forest-Level-Authentifizierung Port 3268 für LDAP oder Port 3269 für LDAPS an.
-protocol	Geben Sie an, ob das LDAP-Protokoll für die sichere Netzwerkkommunikation auf SSL zurückgreift. SSL bietet Verschlüsselungs- und Authentifizierungsfunktionen. Bei SSL werden Daten im Netzwerk verschlüsselt und Nachrichten sowie Server authentifiziert. Folgende Werte sind möglich: <ul style="list-style-type: none"> • ldap (Standard): LDAP ohne SSL • ldaps — LDAP mit SSL.
-certFilePath	Pfad zu (Dateiname der) Datei des vertrauenswürdigen Zertifikat, das für die unidirektionale Serverauthentifizierung verwendet wird.  ANMERKUNG: Wenn der Wert von -protocol ist ldaps, dann ist dieser Qualifizierer erforderlich.
-bindDn	Geben Sie den DN (Distinguished Name) für einen Benutzer mit Administratorrechten auf dem LDAP-Server ein. Der DN kann in mehreren Formaten ausgedrückt werden. Beispiel: cn=Administrator, cn=Users, dc=mycompany, dc=com Administrator@mycompany.com mycompany.com/Administrator
-bindPasswd	Geben Sie das Passwort für die Anbindung an den LDAP-Server ein. Dies ist das Passwort für den im Attribut angegebenen Benutzer. Bind DN . Es ist erforderlich, wenn der Qualifier -bindDn enthalten ist.
-bindPasswdSecure	Gibt das Passwort im sicheren Modus an – der Benutzer wird aufgefordert, das Passwort einzugeben.
-userSearchPath	Geben Sie den Pfad auf dem Verzeichnisserver ein, in dem nach Benutzern gesucht werden soll. Zum Beispiel: ou=People,dc=lss,dc=emc,dc=com.  ANMERKUNG: Auf einem Active Directory-Server wird ein Standardsuchpfad verwendet.
-groupSearchPath	Geben Sie den Pfad auf dem Verzeichnisserver ein, in dem nach Gruppen gesucht werden soll. Zum Beispiel: uid=<name>,ou=people,dc=<domaincomponent>, oder dc=<domain component>.  ANMERKUNG: Auf einem Active Directory-Server wird ein Standardsuchpfad verwendet.
-userIdAttr	Geben Sie den Namen des LDAP-Attributs ein, dessen Wert auf die Benutzer-ID hinweist. Der Standardwert ist uid.
-groupNameAttr	Geben Sie den Namen des LDAP-Attributs ein, dessen Wert auf den Gruppennamen hinweist. Der Standardwert ist cn.
-userObjectClass	Geben Sie die LDAP-Objektklasse für Benutzer ein. Der Standardwert ist user. In Active Directory werden Gruppen und Benutzer im gleichen hierarchischen Verzeichnispfad gespeichert und die Klasse heißt group.
-groupObjectClass	Geben Sie die LDAP-Objektklasse für Gruppen ein. Der Standardwert ist group. In Active Directory werden Gruppen und Benutzer im gleichen Verzeichnispfad gespeichert und die Klasse heißt group.
-groupMemberAttr	Der Name des LDAP-Attributs, dessen Wert die Namen der Mitglieder einer Gruppe enthält. Der Standardwert ist member.
-timeout	Geben Sie die Zeitüberschreitung des LDAP-Servers in Millisekunden ein. Falls das System nach der angegebenen Zeitüberschreitung keine Antwort vom LDAP-Server empfängt, werden keine weiteren Anforderungen gesendet. Der Standardwert beträgt 10.000 Millisekunden, d. h. 10 Sekunden.

Beispiel

Mit dem folgenden Befehl können Sie die LDAP-Einstellungen aktualisieren:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/ldap -id LDAP_1 set -server  
lps0242.lss.emc.com -port 389
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection
```

```
ID = LDAP_1  
Operation completed successfully.
```

Überprüfen von LDAP-Einstellungen

Prüfen Sie die Verbindung mit dem LDAP-Server.

Format

```
/net/ldap -id <value> verify
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Identifiziert den LDAP-Server.

Beispiel

Der folgende Befehl prüft die Verbindung zum LDAP-Server:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/ldap -id LDAP_1 verify
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection
```

```
Operation completed successfully.
```

Aktualisieren der automatisch erkannten LDAP-Serveradressliste

Aktualisiert die automatisch erkannte Serveradressliste für die angegebene LDAP-Serverkonfiguration. Dies kann nur durchgeführt werden, wenn die automatische Erkennung aktiviert ist.

Format

```
/net/ldap -id <value> refresh
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Identifiziert den LDAP-Server.

Beispiel

Der folgende Befehl aktualisiert die automatisch erkannte LDAP-Serveradressliste für die LDAP_1-Serverkonfiguration:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/ldap -id LDAP_1 refresh
```

```
Storage system address: 10.64.75.201  
Storage system port: 443  
HTTPS connection  
  
Operation completed successfully.
```

Löschen von LDAP-Einstellungen

Löschen Sie eine LDAP-Einstellung.

Format

```
/net/ldap -id <value> delete
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID der zu löschenden LDAP-Einstellung ein.

Beispiel

Mit dem folgenden Befehl können Sie die Einstellung LDAP_1 löschen:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/ldap -id LDAP_1 delete
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection  
  
Operation completed successfully.
```

Dienstprogrammbefehle

Mit Ping können Sie die Konnektivität zwischen Ihrem System und einem Remotehost prüfen. Sie können die Schnittstelle auswählen, von der der Ping-Vorgang durchgeführt wird. Das System identifiziert den SP, zu dem die ausgewählte Schnittstelle gehört, automatisch.

Traceroute ermöglicht Ihnen das Überprüfen der Netzwerkroute von der angegebenen Schnittstelle zu einem Remotehost. Sie können die Schnittstelle und die Hostadresse auswählen, die die Endpunkte der Route darstellen sollen.

Pingen

Führen Sie einen Ping-Vorgang für einen Remotehost von der angegebenen NAS-Serverschnittstelle aus durch (-srcIf-Parameterwert)

Format

```
/net/util ping -srcIf <value> -addr <value>
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-srcIf	Identifiziert die NAS-Serverschnittstelle, von der das Paket gesendet wird. Der Wert ist eine Schnittstellenkennung. Verwenden Sie diesen Qualifizierer, wenn Sie testen möchten, ob eine bestimmte Schnittstelle des NAS-Servers auf einen Remotehost zugreifen kann.
-addr	Geben Sie die Zieladresse für das Senden des Pakets an.

Beispiel

Im folgenden Beispiel wird ein Ping-Vorgang für einen Remotehost gezeigt:

```
uemcli /net/util ping -srcIf if_0 -addr 10.0.0.1
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
Operation completed successfully
```

Verfolgen der Route

Zeigen Sie die Route von der angegebenen Schnittstelle zu einem Remotehost an.

Format

```
/net/util/traceroute -srcIf <value> -addr <value>
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-srcIf	Identifiziert die Schnittstelle, von der das Paket gesendet wird. Der Wert ist eine Schnittstellenkennung.
-addr	Geben Sie die Zieladresse für das Senden des Pakets an.

Beispiel

Das folgende Beispiel zeigt Route verfolgen zu einem Remotehost an:

```
uemcli /net/util/traceroute -srcIf if_0 -addr 10.0.0.1
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1: Result = traceroute to 10.0.0.1 (10.64.74.57), 30 hops max, 40 byte packets using UDP
2: Result = 1 10.64.76.2 (10.64.76.2) 0.944 ms 0.801 ms 0.808 ms
3: Result = 2 10.64.74.57 (10.64.74.57) 0.431 ms 0.473 ms 0.354 ms
```

Managen von Distributed Hierarchical Storage Management

Distributed Hierarchical Storage Management (DHSM) ist für die vCenter-Plug-in-Anwendung erforderlich. Durch die DHSM-Funktion können Benutzer des VCenter-Plug-ins erweiterte Dateisystemfunktionen ausführen.

ANMERKUNG: Diese Funktion wurde zuvor Advanced Storage Access (ASA) genannt.

In der folgenden Tabelle sind die Attribute für DHSM aufgeführt.

Tabelle 64. DHSM-Attribute

Attribut	Beschreibung
NAS server	NAS-Server-ID.
State	Status des DHSM-Service. Gültige Werte: <ul style="list-style-type: none">• disabled• enabled
Username	DHSM-Benutzername.
Password	DHSM-Benutzerpasswort.
HTTPS enabled	Gibt an, ob SSL (HTTPS) für DHSM-Anforderungen an diesen DHSM-Server erforderlich ist. Gültige Werte: <ul style="list-style-type: none">• yes (Standardeinstellung)• no

Anzeigen der DHSM-Einstellungen

Zeigt die DHSM-Einstellungen an.

Format

```
/net/nas/dhsm [-server <value>] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-server	Geben Sie die ID des zugehörigen NAS-Servers ein.

Beispiel

Mit dem folgenden Befehl werden die DHSM-Einstellungen angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/dhsm show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
1:   NAS server      = nas_0
     State          = Enabled
     Username       = Local/joe
     HTTPS enabled  = no
```

Ändern der Distributed Hierarchical Storage Management-Einstellungen

Ändert die Distributed Hierarchical Storage Management (DHSM)-Einstellungen.

Format

```
/net/nas/dhsm -server <value> set [-state {Disabled | Enabled}] [[-username <value>] {-passwd <value> | -passwdSecure}] [-enableHTTPS {yes|no}]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-server	Geben Sie die ID des zugehörigen NAS-Servers ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-state	Gibt an, ob der DHSM-Service aktiviert ist. Mögliche Werte: <ul style="list-style-type: none">• Disabled: DHSM-Service ist deaktiviert.• Enabled: DHSM-Service ist aktiviert.
-username	Gibt den DHSM-Benutzernamen an.
-passwd	Gibt das DHSM-Benutzerpasswort an.  ANMERKUNG: Dieses Attribut muss angegeben werden, wenn der aktuelle Status „Disabled“ in „EnabledPerHost“ oder „EnabledForAll“ geändert wird.
-passwdSecure	Gibt ein Passwort im sicheren Modus an. Der Benutzer wird aufgefordert, das Passwort anzugeben und zu bestätigen.
-enableHTTPS	Gibt an, ob SSL (HTTPS) für DHSM-Anforderungen an diesen DHSM-Server erforderlich ist. Gültige Werte: <ul style="list-style-type: none">• yes• no

Beispiel

Mit dem folgenden Befehl ändern Sie das DHSM-Passwort:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/dhsm -server nas_0 set -state Enabled -username newname -passwd newpassword
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
Operation completed successfully.
```

Managen der DHSM-Verbindung

Eine Distributed Hierarchical Storage Management (DHSM)-Verbindung ist für die Cloud Tiering Appliance (CTA)-Integration mit Unity erforderlich. Die DHSM-Verbindungsfunktion ermöglicht das Archivieren von Unity-Dateisystemdaten in der CTA und das Abrufen aus der CTA.

In der folgenden Tabelle sind die Attribute für die DHSM-Verbindung aufgeführt.

Tabelle 65. Attribute für DHSM-Verbindung

Attribut	Beschreibung
ID	Kennung der DHSM-Verbindung.
Secondary URL	Gibt das Protokoll (HTTP) und den Hostnamen des sekundären Speicherservers an. Gibt optional einen Teil des hierarchischen Namespace (veröffentlicht vom Webserver) an. IP-Adresse und vollständig qualifizierter Domainname (FQDN) können als Hostname angegeben werden, es wird jedoch empfohlen, den FQDN zu verwenden.
Secondary port	Port des sekundären Speicherservers.
Local port	Lokaler Port der DHSM-Verbindungen.
Secondary username	Benutzername, den das Speicherarray verwendet, wenn HTTP-Digest-Authentifizierung durch den sekundären Speicher erforderlich ist.
Timeout	Timeout in Sekunden, wenn die Verbindung zum sekundären Speicher hergestellt wird. Wenn innerhalb des angegebenen Timeout-Zeitraums kein Abruf erfolgt, verwendet der NAS-Server eine andere DHSM-Verbindung. Der Standardwert beträgt 30 Sekunden.
File system	Speicherressource des Dateisystems, auf der die Verbindung erstellt wird.
Mode	Modus der Verbindung. Gültige Werte: <ul style="list-style-type: none"> • Disabled: keine Erstellung von Stub-Dateien oder Migration von Daten. Für Daten auf dem NAS-Server sind Lese- und Schreibvorgänge möglich. • Enabled (Standardeinstellung): ermöglicht die Erstellung von Stub-Dateien und Datenmigration über Lese- und Schreibvorgänge. • Recall only: Die Policy Engine ist zum Erstellen von Stub-Dateien nicht zulässig, aber der Benutzer kann weiterhin die Datenmigration mithilfe einer Lese- oder Schreibanforderung vom sekundären Dateisystem zu Unity auslösen.
Read policy	Lese-Policy, wenn der NAS-Server Daten aus dem sekundären Speicher abruft. <ul style="list-style-type: none"> • Full: ruft die gesamte Datei auf den NAS-Server bei einer Leseanforderung ab, bevor die Daten zurückgegeben werden. • Passthrough: ruft Daten ab, ohne die Daten in Unity abzurufen. • Partial: ruft nur die Datenblöcke ab, die zur Erfüllung der Leseanforderung des Clients erforderlich sind. • None: verwendet die Lesemethodenoption, die in der Stub-Datei angegeben ist.

Erstellen einer DHSM-Verbindung

Erstellen Sie eine DHSM-Verbindung unter Verwendung des HTTP-Protokolls zwischen dem angegebenen primären Dateisystem von Unity und einem sekundären Dateisystem der CTA.

Format

```
/net/nas/dhsmconn create [-async] -fs <value> -secondaryUrl <value> [-secondaryPort <value>] [-localPort <value>] [-mode {enabled | disabled | recallOnly}] [-readPolicy {none | full | passthrough | partial}] [-secondaryUsername <value>] [-secondaryPassword <value>] [-timeout <value>]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-fs	Gibt die Speicherressourcen-ID des Dateisystems an.
-secondaryUrl	Gibt die URL des sekundären Remotespeichers an, einschließlich des Protokolls, des Hostnamens und optional eines Teils des veröffentlichten hierarchischen Namespace.

Qualifizierer	Beschreibung
-secondaryPort	Gibt die Remoteportnummer an, an die der NAS-Server die HTTP-Anforderung sendet. Wenn keine Nummer angegeben ist, gibt der Data Mover HTTP-Anforderungen an Port 80 auf dem HTTP-Server mit sekundärem Speicher aus.
-localPort	Gibt den lokalen Port der DHSM-Verbindung an.
-mode	Legt den Modus der Unity-DHSM-Vorgänge auf dem angegebenen Dateisystem fest. Gültige Werte: <ul style="list-style-type: none"> • <code>enabled</code> (Standardeinstellung): ermöglicht die Erstellung von Stub-Dateien und Datenmigration über Lese- und Schreibvorgänge. • <code>disabled</code>: Migration von Stub-Dateien und Daten nicht möglich. Lese- und Schreibvorgänge für Daten in Unity sind im deaktivierten Modus möglich. • <code>recallOnly</code>: Die Policy Engine ist zum Erstellen von Stub-Dateien nicht zulässig, aber der Nutzer kann weiterhin die Datenmigration mithilfe einer Lese- oder Schreibanforderung vom sekundären System zu Unity auslösen.
-readPolicy	Gibt die Migrationsmethodenoption an, die von Unity auf der Verbindungsebene verwendet wird, um die in der Stub-Datei verwendete Migrationsmethode zu überschreiben. Gültige Werte: <ul style="list-style-type: none"> • <code>none</code> (Standardeinstellung): gibt keine Überschreibung an. • <code>full</code>: ruft die gesamte Datei für Unity bei einer Leseanforderung ab, bevor die Daten zurückgegeben werden. • <code>passthrough</code>: ruft Daten ab, ohne die Daten in Unity abzurufen. • <code>partial</code>: ruft nur die Blöcke ab, die zur Erfüllung der Leseanforderung des Clients erforderlich sind.
-secondaryUsername	Definiert den Benutzernamen, den der HTTP-Client verwendet, wenn Digest-Authentifizierung durch den HTTP-Server mit sekundärem Speicher erforderlich ist.
-secondaryPassword	Gibt das Passwort des Benutzernamens an, das für den sekundären Speicherserver erforderlich ist. <p> ANMERKUNG: Das Kennwort muss 8 bis 64 Zeichen lang sein und mindestens einen Groß- und Kleinbuchstaben sowie einen numerischen Buchstaben enthalten. Das Kennwort darf kein einfaches Anführungszeichen ('), kaufmännisches und-Zeichen (&) oder Leerzeichen enthalten.</p>
-timeout	Gibt den Timeout-Wert in Sekunden an. Standardmäßig wartet der Unity-HTTP-Client 30 Sekunden auf eine Antwort vom HTTP-Server und wiederholt den Vorgang dann einmal.

Beispiel

Mit dem folgenden Befehl wird eine HTTP-Verbindung für das Dateisystem `fs_1` auf dem sekundären Dateisystem `/export/dhsm1` auf `http://10.1.0.115` erstellt.

```
uemcli /net/nas/dhsmconn create -filesystem fs_1 -secondaryUrl http://10.1.0.115/export/dhsm1
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = dhsmconn_1
Operation completed successfully.
```

Anzeigen der Einstellungen für DHSM-Verbindung

Zeigen Sie die Details für DHSM-Verbindungen an.

Format

```
/net/nas/dhsmconn [{-id <value> | -fs <value>}] show
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-id	Kennung der DHSM-Verbindung.
-fs	Gibt die Speicherressourcen-ID des Dateisystems an.

Beispiel 1

Mit dem folgenden Befehl werden sämtliche DHSM-Verbindungen für Dateisystem fs_1 aufgeführt.

```
uemcli /net/nas/dhsmconn -fs fs_1 show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1: ID                = dhsmconn_0
   File system       = fs_1
   Mode              = enabled
   Read policy       = none
   Secondary url     = http://172.24.102.115/export/dhsm1
   Secondary port    = 80
   Secondary username = admin
   Local port        = 80
   Timeout           = 60
```

Beispiel 2

Der folgende Befehl zeigt DHSM-Verbindung dhsmconn_1.

```
uemcli /net/nas/dhsmconn -id dhsmconn_1 show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1: ID                = dhsmconn_1
   File system       = fs_1
   Mode              = disabled
   Read policy       = full
   Secondary url     = http://www.myserver.com/export/dhsm1
   Secondary port    = 80
   Secondary username = admin
   Local port        = 80
   Timeout           = 60
```

Beispiel 3

Mit dem folgenden Befehl werden sämtliche auf dem Speichersystem vorhandenen DHSM-Verbindungen aufgeführt.

```
uemcli /net/nas/dhsmconn show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1: ID                = dhsmconn_0
   File system       = fs_1
   Mode              = enabled
   Read policy       = none
   Secondary url     = http://10.1.0.115/export/dhsm1
   Secondary port    = 80
   Secondary username = admin
```

```

Local port      = 80
Timeout        = 60

2: ID          = dhsmconn_1
File system    = fs_2
Mode          = disabled
Read policy   = full
Secondary url  = http://10.1.0.115/export/dhsm1
Secondary port = 80
Secondary username = admin
Local port    = 80
Timeout      = 60

3: ID          = dhsmconn_2
File system    = fs_3
Mode          = enabled
Read policy   = passthrough
Secondary url  = http://10.1.0.115/export/dhsm2
Secondary port = 80
Secondary username = admin
Local port    = 80
Timeout      = 60

```

Ändern der Einstellungen für DHSM-Verbindung

Ändern Sie die Einstellungen für eine vorhandene DHSM-Verbindung.

Format

```

/net/nas/dhsmconn -id <value> modify [-async] [-mode {enabled | disabled | recallOnly}] [-readPolicy {full | passthrough | partial | none}] [-secondaryServerName <value> [-secondaryPort <value>] [-localPort <value>] [-secondaryUsername <value> -secondaryPassword <value>] [-timeout <value>]

```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-id	Kennung der DHSM-Verbindung.
-mode	Legt den Modus der Unity-DHSM-Vorgänge auf dem angegebenen Dateisystem fest. Gültige Werte: <ul style="list-style-type: none"> • enabled (Standardeinstellung): ermöglicht die Erstellung von Stub-Dateien und Datenmigration über Lese- und Schreibvorgänge. • disabled: Migration von Stub-Dateien und Daten nicht möglich. Lese- und Schreibvorgänge für Daten in Unity sind im deaktivierten Modus möglich. • recallOnly: Die Policy Engine ist zum Erstellen von Stub-Dateien nicht zulässig, aber der Nutzer kann weiterhin die Datenmigration mithilfe einer Lese- oder Schreibanforderung vom sekundären System zu Unity auslösen.
-readPolicy	Gibt die Migrationsmethodenoption an, die von Unity auf der Verbindungsebene verwendet wird, um die in der Stub-Datei verwendete Migrationsmethode zu überschreiben. Gültige Werte: <ul style="list-style-type: none"> • none (Standardeinstellung): gibt keine Überschreibung an. • full: ruft die gesamte Datei für Unity bei einer Leseanforderung ab, bevor die Daten zurückgegeben werden. • passthrough: ruft Daten ab, ohne die Daten in Unity abzurufen. • partial: ruft nur die Blöcke ab, die zur Erfüllung der Leseanforderung des Clients erforderlich sind.
-secondaryServerName	Gibt den Namen oder die IP-Adresse des Remoteservers an.
-secondaryPort	Gibt die Remoteportnummer an, an die der NAS-Server die HTTP-Anforderung sendet. Wenn keine Nummer angegeben ist, gibt der NAS-Server HTTP-Anforderungen an Port 80 auf dem HTTP-Server mit sekundärem Speicher aus.

Qualifizierer	Beschreibung
-secondaryUsername	Definiert den Benutzernamen, den der HTTP-Client verwendet, wenn Digest-Authentifizierung durch den HTTP-Server mit sekundärem Speicher erforderlich ist.
-secondaryPassword	Gibt das Kennwort des Nutzernamens an, das für den sekundären Speicherserver erforderlich ist.  ANMERKUNG: Das Kennwort muss 8 bis 64 Zeichen lang sein und mindestens einen Groß- und Kleinbuchstaben sowie einen numerischen Buchstaben enthalten. Das Kennwort darf kein einfaches Anführungszeichen ('), kaufmännisches und-Zeichen (&) oder Leerzeichen enthalten.
-timeout	Gibt den Timeout-Wert in Sekunden an. Standardmäßig wartet der Unity-HTTP-Client 30 Sekunden auf eine Antwort vom HTTP-Server und wiederholt den Vorgang dann einmal.

Beispiel 1

Mit dem folgenden Befehl wird der Modus der Verbindung dhsmconn_1 geändert.

```
uemcli /net/nas/dhsmconn -id dhsmconn_1 modify -mode recallOnly
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTP connection

ID = dhsmconn_1
Operation completed successfully.
```

Beispiel 2

Mit dem folgenden Befehl wird die ReadPolicy-Einstellung für die Verbindung dhsmconn_1 geändert.

```
uemcli /net/nas/dhsmconn -id dhsmconn_1 modify -readPolicy passthrough
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTP connection

ID = dhsmconn_1
Operation completed successfully.
```

Löschen einer DHSM-Verbindung

Löscht eine vorhandene HTTP-Verbindung zwischen dem Dateisystem und dem sekundären Dateisystem.

Format

```
/net/nas/dhsmconn -id <value> delete [-async] [-recallPolicyOnDelete {fail | no | yes}]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-id	Kennung der DHSM-Verbindung.
-recallPolicyOnDelete	Gibt die Abruf-Policy für jede migrierte Datei während des Löschvorgangs an. Gültige Werte: <ul style="list-style-type: none"> fail (Standardeinstellung): durchsucht das Dateisystem nach Stub-Dateien, die abhängig von der Verbindung sind, und fällt bei der ersten aus. no: löscht die Verbindung ohne auf Stub-Dateien zu prüfen, die von der Verbindung abhängen. Wenn die Option no angegeben wird und Stub-Datei vorhanden sind, tritt ein I/O-Fehler auf, wenn die Datei gelesen wird, da die Verbindung nicht mehr vorhanden ist.

Qualifizierer	Beschreibung
	<ul style="list-style-type: none"> • <code>yes</code>: migriert die Dateien wieder zu Unity, bevor die Verbindung gelöscht wird.

Beispiel

Der folgende Befehl löscht die DHSM-Verbindung `dhsmconn_1` und gibt die Abruf-Policy für alle migrierten Dateien während des Löschvorgangs an.

```
uemcli /net/nas/dhsmconn -id dhsmconn_1 delete -recallPolicy no
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTP connection
```

```
Operation completed successfully.
```

Managen des Tie-Breaker-Node (nur virtuelle Dual-SP-Bereitstellungen)

Mit einem Tie-Breaker-Node (TBN) lässt sich die Verfügbarkeit Ihres Speichersystems verbessern. Weitere Informationen zum Aktivieren eines TBN finden Sie unter [Ändern der Einstellungen für die Tie-Breaker-Node-Konfiguration](#).

Tabelle 66. Attribute für die TBN-Konfiguration

Attribut	Beschreibung
ID	TBN-Kennung
Health state	<p>Integritätsstatus des TBN. Der Integritätsstatuscode wird in Klammern angezeigt. Folgende Werte sind möglich:</p> <ul style="list-style-type: none"> • <code>Unknown (0)</code>: Die Integrität des TBN kann nicht bestimmt werden. • <code>OK (5)</code>: TBN funktioniert normal. • <code>Degraded/Warning (10)</code>: TBN-Service funktioniert, aber es ist mindestens eines der folgenden Probleme aufgetreten: <ul style="list-style-type: none"> ○ TBN kann mit SPA nur über eine Netzwerk-Heartbeat-Verbindung kommunizieren, aber nicht über beide. Eine der Netzwerk-Heartbeat-Verbindungen zwischen ihnen wurde getrennt. ○ TBN kann mit SPB nur über eine Netzwerk-Heartbeat-Verbindung kommunizieren, aber nicht über beide. Eine der Netzwerk-Heartbeat-Verbindungen zwischen ihnen wurde getrennt. ○ TBN kann mit dem jeweiligen SP über eine Netzwerk-Heartbeat-Verbindung separat kommunizieren, aber nicht über beide Heartbeat-Verbindungen. Eine der Netzwerk-Heartbeat-Verbindungen zwischen dem TBN und SPA wurde getrennt. Eine der Heartbeat-Verbindungen zwischen dem TBN und SPB wurde getrennt. • <code>Minor failure (15)</code>: Es ist mindestens eines der folgenden Ereignisse eingetreten: <ul style="list-style-type: none"> ○ TBN wurde von SPA getrennt. Beide Netzwerk-Heartbeat-Verbindungen zwischen dem TBN und SPA wurden getrennt. ○ TBN wurde von SPB getrennt. Beide Netzwerk-Heartbeat-Verbindungen zwischen dem TBN und SPB wurden getrennt.

Tabelle 66. Attribute für die TBN-Konfiguration (fortgesetzt)

Attribut	Beschreibung
	<ul style="list-style-type: none"> • <i>Major failure</i> (20): TBN wurde von SPA und SPB getrennt. Alle Netzwerk-Heartbeat-Verbindungen zwischen dem TBN und SPA sowie zwischen dem TBN und SPB wurden getrennt.
Health details	Zusätzliche Integritätsinformationen. Weitere Informationen zur Integrität finden Sie im Anhang A, Referenz.
Active	Gibt an, ob der TBN-Service aktiv ist. Gültige Werte: <ul style="list-style-type: none"> • yes • no

Anzeigen der grundlegenden Informationen zum Tie-Breaker-Node

Zeigen Sie grundlegende Informationen zum Tie-Breaker-Node (TBN) an, einschließlich der TBN-Kennung und des Integritätsstatus eines aktiven TBN.

Format

```
/net/tbn [-id <value>] show
```

Beispiel

Mit dem folgenden Befehl werden grundlegende TBN-Informationen angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/tbn/ show
```

```
Storage system address: 10.64.75.201
Storage system port: 443
HTTPS connection

1:      ID                = 42389FCA-01D1-4491-7D77-8060373D67B8
      Health state       = OK (5)
      Active              = yes
```

Managen der Konfiguration eines Tie-Breaker-Node (nur virtuelle Dual-SP-Bereitstellungen)

Mit einem Tie-Breaker-Node (TBN) kann ein Dual-SP-UnityVSA-System Datenbeschädigungen verhindern, die aus einer „Split-Brain“-Situation resultieren. Diese tritt auf, wenn die beiden SPs nicht mehr miteinander kommunizieren und ihre Daten nicht mehr miteinander synchronisieren. Durch Aktivierung eines TBN lässt sich diese Situation verhindern und die Verfügbarkeit Ihres Speichersystems verbessern.

Tabelle 67. Attribute für die TBN-Konfiguration

Attribut	Beschreibung
Enabled	Zeigt an, ob der TBN aktiviert ist. Gültige Werte: <ul style="list-style-type: none"> • yes • no
Active TBN	TBN-Kennung

Anzeigen der Einstellungen für die Tie-Breaker-Node-Konfiguration

Zeigen Sie die Einstellungen für die Tie-Breaker-Node-Konfiguration an.

Format

```
/net/tbn/config show
```

Beispiel

Mit dem folgenden Befehl werden Details zur TBN-Konfiguration angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/tbn/config show
```

```
Storage system address: 10.64.75.201
Storage system port: 443
HTTPS connection

1:      Enabled          = yes
      Active TBN       = 42389FCA-01D1-4491-7D77-8060373D67B8
```

Ändern der Einstellungen für die Tie-Breaker-Node-Konfiguration

Ändern Sie die Konfiguration des Tie-Breaker-Node (TBN).

Format

```
/net/tbn/config set [-enabled {yes|no}] [-activeTbn <value>]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-enabled	Aktiviert oder deaktiviert einen Tie-Breaker-Node (TBN). Gültige Werte: <ul style="list-style-type: none">• yes• no
-activeTbn	Gibt die TBN-Kennung an: <ul style="list-style-type: none">• Verwenden Sie diesen Wert mit dem Qualifizierer -enabled, um den angegebenen TBN zu aktivieren.• Verwenden Sie diesen Wert ohne den Qualifizierer -enabled, um den angegebenen TBN zu aktivieren. Die TBN-Kennung wird nicht benötigt, wenn der Wert des Qualifizierers -enabled „no“ lautet.

Beispiel 1: TBN aktivieren

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/tbn/config set -enabled yes -activeTbn 42389FCA-01D1-4491-7D77-8060373D67B8
```

```
Storage system address: 10.64.75.201
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Beispiel 2: TBN deaktivieren

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/tbn/config set -enabled no
```

```
Storage system address: 10.64.75.201
Storage system port: 443
HTTPS connection

Operation completed successfully
```

Beispiel 3: Aktiven TBN ändern

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/tbn/config set -activeTbn  
42389FCA-01D1-4491-7D77-8060373D67B8
```

```
Storage system address: 10.64.75.201  
Storage system port: 443  
HTTPS connection
```

```
Operation completed successfully
```

Hosts verwalten

Themen:

- Managen von Hostkonfigurationen
- Managen von Host-LUNs
- Hostgruppen managen
- Managen von Hostinitiatoren
- Managen von Hostinitiatorpfaden
- Managen von iSCSI-CHAP-Konten für die einseitige CHAP-Authentifizierung
- Verwalten von iSCSI-Verbindungen
- Verwalten der iSCSI-Verbindungspfade
- Managen von Remotespeichersystemen
- Managen von VMware vCenter
- Managen von ESXi-Hosts
- Virtuelle Maschine
- VM-Festplatte

Managen von Hostkonfigurationen

Hosts sind die Clients bzw. Server im Netzwerk, die auf Speicher im System zugreifen. Hostkonfigurationen sind logische Verbindungen, über die Hosts oder Anwendungen auf Speicherressourcen zugreifen. Bevor ein Host auf Speicher zugreifen kann, müssen Sie eine Konfiguration definieren und sie mit einer Speicherressource verknüpfen. Sie können eine Hostkonfiguration für jeden Host, jedes Hostsubnetz oder jede Netzwerkgruppe erstellen, die auf Speicherressourcen im System zugreift.

Die folgenden Arten von Hostkonfigurationen können erstellt werden:

- Individuelle Hostkonfigurationen: Diese Konfigurationen ermöglichen Ihnen die Definition und Steuerung des Zugriffs auf Speicherressourcen für einzelne Hosts.
- Konfigurationen von Subnetzen und Netzwerkgruppen: Mit diesen Konfigurationen können Sie den Zugriff auf Speicherressourcen für mehrere Hosts bzw. Netzwerksegmente definieren und steuern.

Die einzelnen Hostkonfigurationen verfügen über eigene IDs.

In der folgenden Tabelle sind die Attribute für Hostkonfigurationen aufgeführt.

Tabelle 68. Attribute für die Hostkonfiguration

Attribut	Beschreibung
ID	ID der Hostkonfiguration.
Name	Name der Hostkonfiguration
Description	Kurze Beschreibung der Hostkonfiguration.
Tenant	Mandant, dem der Host zugeordnet ist.
Address	Der Hostname bzw. die mit dem Host verknüpfte IP-Adresse, die IP-Adresse des Subnetzes oder der Name der Netzwerkgruppe.  ANMERKUNG: Diese Informationen sind beim Anschluss von Hosts an Netzwerk-Freigaben auf dem System erforderlich.
Netmask	Subnetzmaske für den Host.
Type	Art der Hostkonfiguration. Folgende Werte sind möglich: <ul style="list-style-type: none"> • <code>host</code> : Der Zugriff auf Speicherressourcen wird für jeden Host einzeln definiert und gesteuert.

Tabelle 68. Attribute für die Hostkonfiguration (fortgesetzt)

Attribut	Beschreibung
	<ul style="list-style-type: none"> ● <code>subnet</code> : Ein Subnetz ist eine logische Gruppierung verbundener Netzwerkgeräte. Devices in einem Subnetz teilen sich zusammenhängende Bereiche von IP-Adressen. Mit einer Subnetzmaske bzw. Netzwerkmaske werden die Grenzen eines IP-Subnetzes definiert. Sie können eine Hostkonfiguration mit einer Subnetzmaske verknüpfen, um den Speicherzugriff für Hosts in einem bestimmten Netzwerksegment zu definieren und zu steuern. ● <code>netgroup</code> : Eine Netzwerkgruppe ist eine benannte Gruppe von Hosts, Benutzern oder Domains in einem Netzwerk. Netzwerkgruppen ermöglichen die kollektive Referenzierung von Gruppen von Linux-/UNIX-Hosts für den Speicherzugriff über NFS. Sie können eine Hostkonfiguration für eine Netzwerkgruppe erstellen und den Speicherzugriff für mehrere Linux-/UNIX-Hosts bzw. -Benutzer über eine zentrale Konfiguration definieren und steuern. <p>i ANMERKUNG: In der Regel kann auf Netzwerkgruppen nur über NIS zugegriffen werden. Falls NIS nicht ausgeführt wird, sind keine Netzwerkgruppen definiert. Managen von NIS-Serverdomain erläutert, wie die NIS-Serverkommunikation konfiguriert wird.</p>
OS type	<p>Typ des auf dem Host ausgeführten Betriebssystems. Sie können einen beliebigen Wert eingeben. Im Folgenden finden Sie Vorschläge für einige der gängigen Betriebssysteme:</p> <ul style="list-style-type: none"> ● <code>undefined</code> : Betriebssystem ist nicht angegeben (Standardeinstellung) oder unbekannt. ● <code>other</code> : Sonstige ● <code>win2003srv</code> : Windows Server 2003 ● <code>winxp</code> : Windows XP ● <code>win2008srv</code> : Windows Server 2008 ● <code>winvista</code> : Windows Vista ● <code>win2012srv</code> : Windows Server 2012 ● <code>esx</code> : VMware ESX ● <code>redhat</code> : Red Hat Enterprise Linux ● <code>sles</code> : SUSE Linux Enterprise ● <code>win7</code> : Windows 7 ● <code>hyperv</code> : Microsoft Hyper-V ● <code>solaris</code> : Solaris
Ignored address	<p>Ein durch Kommata getrennte Liste der Host-IP-Adressen, die vom Datenzugriff ausgeschlossen werden sollen.</p>
Health state	<p>Integritätsstatus des Hosts. Der Integritätsstatuscode wird in Klammern angezeigt. Folgende Werte sind möglich:</p> <ul style="list-style-type: none"> ● <code>Unknown (0)</code> : Status ist unbekannt. ● <code>OK (5)</code> : Funktioniert ordnungsgemäß. ● <code>OK BUT (7)</code> : Funktioniert ordnungsgemäß, aber es könnte ein Problem vorliegen. ● <code>Degraded/Warning (10)</code> : Funktioniert und führt alle Funktionen aus, die Performance ist jedoch eventuell nicht optimal. ● <code>Minor failure (15)</code> : Funktioniert und führt alle Funktionen aus, aber die Gesamtpformance ist eingeschränkt. Diese Bedingung hat geringe Auswirkungen auf das System, und das Problem sollte in der näheren Zukunft angegangen werden, aber eine unmittelbare Lösung ist nicht erforderlich. ● <code>Major failure (20)</code> : Im System sind Fehler aufgetreten, und einige oder alle Funktionen funktionieren nur noch eingeschränkt oder gar nicht mehr. Dieser Zustand hat erhebliche Auswirkungen auf das System und muss sofort beseitigt werden. ● <code>Critical failure (25)</code> : Es ist ein Fehler aufgetreten; eine Recovery ist eventuell nicht möglich. Diese Bedingung hat zu Datenverlusten geführt. Der Fehler muss umgehend behoben werden. ● <code>Non-recoverable error (30)</code> : Das System ist komplett ausgefallen und kann nicht wiederhergestellt werden.
Health details	<p>Zusätzliche Integritätsinformationen. Weitere Informationen zur Integrität finden Sie im Anhang A, Referenz.</p>
Management type	<p>Zeigt die Art und Weise des Hostmanagements an. Folgende Werte sind möglich:</p>

Tabelle 68. Attribute für die Hostkonfiguration (fortgesetzt)

Attribut	Beschreibung
	<ul style="list-style-type: none"> • <code>VMware</code> : Der Host wird durch VMware-Webservices gemanagt. • <code>Other</code> : Der Host wird automatisch im Speichersystem erstellt. • <code>Manual</code> : Der Host wird manuell erstellt.
<code>Accessible LUNs</code>	Eine kommasetrennte Liste von LUNs, auf die vom Host aus zugegriffen werden kann.
<code>Host LUN IDs</code>	Durch Komma getrennte Liste von HLU (Host LUN Identifiers), die die entsprechenden Hosts verwenden, um auf die LUN zuzugreifen.
<code>Host group</code>	Hostgruppe, in der sich der Host befindet.

Erstellen von Hostkonfigurationen

Erstellen Sie eine Hostkonfiguration, und stellen Sie eine Verbindung zwischen dem System und den Hosts, die auf das System zugreifen, her.

Format

```
/remote/host create -name <value> [-descr <value>] [-tenant <value>] -type {host [-addr <value>]
[-ignoredAddr <value>] [-osType <value> ] | subnet -addr <value> [-netmask <value>] | netgroup
-addr <value>}
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
<code>-name</code>	Gibt den Namen der Hostkonfiguration an.
<code>-descr</code>	Gibt eine kurze Beschreibung der Hostkonfiguration an.
<code>-type</code>	<p>Gibt die Art der Hostkonfiguration an. Folgende Werte sind möglich:</p> <ul style="list-style-type: none"> • <code>host</code> : Der Zugriff auf Speicherressourcen wird für jeden Host einzeln definiert und gesteuert. • <code>subnet</code> : Ein Subnetz ist eine logische Gruppierung verbundener Netzwerkgeräte. Devices in einem Subnetz teilen sich zusammenhängende Bereiche von IP-Adressen. Mit einer Subnetzmaske bzw. Netzwerkmaske werden die Grenzen eines IP-Subnetzes definiert. <p>Sie können eine Hostkonfiguration mit einer Subnetzmaske verknüpfen, um den Speicherzugriff für Hosts in einem bestimmten Netzwerksegment zu definieren und zu steuern.</p> <ul style="list-style-type: none"> • <code>netgroup</code> : Eine Netzwerkgruppe ist eine benannte Gruppe von Hosts, Benutzern oder Domains in einem Netzwerk. Netzwerkgruppen ermöglichen die kollektive Referenzierung von Gruppen von Linux-/UNIX-Hosts für den Speicherzugriff über NFS. <p>Sie können eine Hostkonfiguration für eine Netzwerkgruppe erstellen und den Speicherzugriff für mehrere Linux-/UNIX-Hosts bzw. -Benutzer über eine zentrale Konfiguration definieren und steuern.</p> <p>i ANMERKUNG: In der Regel kann auf Netzwerkgruppen nur über NIS zugegriffen werden. Wenn NIS nicht ausgeführt wird, werden keine Netzwerkgruppen definiert. Managen von NIS-Serverdomain erläutert, wie die NIS-Serverkommunikation konfiguriert wird.</p>
<code>-tenant</code>	<p>Gibt die Kennung des Mandanten an, dem der Host zugeordnet ist.</p> <p>i ANMERKUNG: Falls nicht angegeben, wird der Host im standardmäßigen Netzwerk-Namespaces erstellt und das Mandantenattribut ist leer.</p>
<code>-addr</code>	<p>Gibt die Hostnamen bzw. die mit dem Host verknüpften IP-Adressen, die IP-Adressen des Subnetzes oder den Namen der Netzwerkgruppe an. Trennen Sie die einzelnen Werte durch Kommas.</p> <ul style="list-style-type: none"> • Format: <code><IP-Adresse>/[<Präfixlänge>]</code>. • Standardpräfixlänge für IPv4-Adressen ist 24 und für IPv6-Adressen 64.

Qualifizierer	Beschreibung
	 ANMERKUNG: Diese Informationen sind beim Anschluss von Hosts an Netzwerk-Shares auf dem System erforderlich.
-ignoredAddr	Gibt eine Liste mit IP-Adressen an, die dem Host zugeordnet und vom Datenzugriff ausgeschlossen sind. Trennen Sie die einzelnen Werte durch Kommas.
-netmask	Gibt die Subnetzmaske für die Hostkonfiguration an.
-osType	Geben Sie die Art des Betriebssystems an, das auf dem Host ausgeführt wird. Sie können einen beliebigen Wert eingeben. Im Folgenden finden Sie Vorschläge für einige der gängigen Betriebssysteme: <ul style="list-style-type: none"> • undefined : Betriebssystem ist nicht angegeben (Standardeinstellung) oder unbekannt. • other: Sonstige • win2003srv: Windows Server 2003 • winxp: Windows XP • win2008srv: Windows Server 2008 • winvista: Windows Vista • win2012srv : Windows Server 2012 • esx: VMware ESX • redhat: Red Hat Enterprise Linux • sles : SUSE Linux Enterprise • win7: Windows 7 • hyperv : Microsoft Hyper-V • solaris: Solaris

Beispiel 1

Mit dem folgenden Befehl wird eine Hostkonfiguration für einen Host mit den folgenden Einstellungen erstellt:

- Name: MyHost.
- Beschreibung: accounting.
- IP-Adresse: 10.64.74.10
- Betriebssystem: Windows XP.

Die Hostkonfiguration erhält die ID Host_1014:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/host create -name MyHost -
descr "accounting" -type host -addr 10.64.74.10 -osType winxp
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = Host_1014
Operation completed successfully.
```

Beispiel 2

Mit dem folgenden Befehl wird eine Hostkonfiguration für ein Subnetz mit den folgenden Einstellungen erstellt:

- Name: MySubnet.
- Beschreibung: subnet1.
- IP-Adresse: 192.168.10.0.
- Subnetzmaske: 255.255.255.0.

Die Hostkonfiguration erhält die ID Subnet_1015:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/host create -name MySubnet -  
descr "subnet1" -type subnet -addr 192.168.10.0 -netmask 255.255.255.0
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection
```

```
ID = Subnet_1015  
Operation completed successfully.
```

Beispiel 3

Mit dem folgenden Befehl wird eine Hostkonfiguration für ein Subnetz mit den folgenden Einstellungen erstellt:

- Name: IPv6Subnet
- Beschreibung: V6_HE_Subnet.
- IPv6-Adresse: 2001:db8:c25:
- Präfixlänge: 48.

Die Hostkonfiguration erhält die ID NetGroup_1023:

```
uemcli -d 10.0.0.1 /remote/host create -name IPv6Subnet -descr "V6_HE_Subnet" -type subnet -addr  
2001:db8:c25::/48
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection
```

```
ID = NetGroup_1023  
Operation completed successfully.
```

Anzeigen von Hostkonfigurationen

Zeigen Sie Details zu einer Hostkonfiguration an. Sie können die ID der Hostkonfiguration oder des Hosttyps auswählen.

 **ANMERKUNG:** Aktionsbefehl „show“ erläutert, wie das Ausgabeformat geändert wird.

Format

```
/remote/host [{"-id <value> | -name <value>} | -type {host | subnet | netgroup}] -hostgroup  
<value> | -hostgroupName <value>}] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die Host-ID an.
-name	Geben Sie den Hostnamen an.
-type	Gibt die Art des Hosts an. Gültige Werte: <ul style="list-style-type: none">• host• subnet• netgroup
-hostgroup	Gibt die Hostgruppen-ID an, die als Filter verwendet werden soll.
-hostgroupName	Gibt den Namen der Hostgruppe an, die als Filter verwendet werden soll.

Beispiel

Mit dem folgenden Befehl werden sämtliche auf dem System vorhandenen Hostkonfigurationen aufgeführt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/host show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      ID           = 1014
        Name         = MyHost
        Description  = this is my host
        Tenant       = tenant_3
        Type         = host
        Address      = 10.64.74.10, 10.64.80.10
        Netmask      =
        OS type      = winxp
        Ignored address = 10.64.80.10
        Health state = OK (5)

2:      ID           = 1015
        Name         = MySubnet
        Description  = this is my subnet
        Tenant       =
        Type         = subnet
        Address      = 192.168.10.0
        Netmask      = 255.255.255.0
        OS type      =
        Ignored address =
        Health state = OK (5)
```

Ändern der Hostkonfigurationseinstellungen

Ändern Sie die Einstellungen für eine Hostkonfiguration.

Format

```
/remote/host {-id <value> | -name <value>} set [-name <value>] [-descr <value>] [-addr <value>]
[-ignoredAddr <value>] [-netmask <value>] [-osType <value>] [-addLuns <value> [-hlus <value> ]]
[-removeLuns <value>]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	ID der zu ändernden Hostkonfiguration.
-name	Name der zu ändernden Hostkonfiguration.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-name	Gibt den neuen Namen für die Hostkonfiguration an.
-desc	Gibt die neue Beschreibung der Hostkonfiguration an.
-addr	Gibt die Hostnamen bzw. die mit dem Host verknüpften IP-Adressen, die IP-Adressen des Subnetzes oder die Netzwerkadressen der Netzwerkgruppe an. Trennen Sie die einzelnen Werte durch Kommas. <ul style="list-style-type: none">• Gibt als Subnetztyp die neue IP-Adresse des Subnetzes an.• Gibt als Netzwerkgruppe den Netzwerknamen der neuen Netzwerkgruppe an.

Qualifizierer	Beschreibung
	<ul style="list-style-type: none"> • Format: <IP-Adresse>/[<Präfixlänge>]. • Standardpräfixlänge für IPv4-Adressen ist 24 und für IPv6-Adressen 64. <p> ANMERKUNG: Diese Informationen sind beim Anschluss von Hosts an Netzwerk-Shares auf dem System erforderlich.</p>
-ignoredAddr	Gibt eine Liste mit IP-Adressen an, die dem Host zugeordnet und vom Datenzugriff ausgeschlossen sind. Trennen Sie die einzelnen Werte durch Kommas.
-netmask	Geben Sie die Subnetzmaske einer Hostkonfiguration an.
-osType	<p>Geben Sie die Art des Betriebssystems an, das auf dem Host ausgeführt wird. Sie können einen beliebigen Wert eingeben. Im Folgenden finden Sie Vorschläge für einige der gängigen Betriebssysteme:</p> <ul style="list-style-type: none"> • undefined : Betriebssystem ist nicht angegeben oder unbekannt. • other: Sonstige • win2003srv: Windows Server 2003 • winxp: Windows XP • win2008srv: Windows Server 2008 • winvista: Windows Vista • win2012srv : Windows Server 2012 • esx: VMware ESX • redhat: Red Hat Enterprise Linux • sles : SUSE Linux Enterprise • win7: Windows 7 • hyperv : Microsoft Hyper-V • solaris: Solaris
-addLuns	Geben Sie eine kommasetrennte Liste von LUN-freundlichen IDs an, um LUNs dem Host hinzuzufügen.
-hlus	<p>Gibt die kommasetrennte Liste der Host-LUN-Identifikatoren an, die von den entsprechenden Hosts verwendet werden sollen, die in der Option <code>-lunHosts</code> angegeben wurden. Die Anzahl der Positionen in den beiden Listen muss übereinstimmen. Eine leere Zeichenfolge ist jedoch ein gültiger Wert für jedes Element der Liste der Host-LUN-Identifikatoren, sofern die Listenelemente durch Kommata getrennt sind. Ein solches leeres Element bedeutet, dass das System automatisch den Host-LUN-Identifikatorwert zuweisen sollte, mit dem der entsprechende Host auf die LUN zugreift.</p> <p>Wenn nicht angegeben, weist das System automatisch den Host-LUN-Identifikatorwert jedem Host zu, der in der Argumentliste <code>-lunHosts</code> angegeben ist.</p>
-removeLuns	Geben Sie eine kommasetrennte Liste von LUN-freundlichen IDs an, um LUNs vom Host zu entfernen.

Beispiel

Mit dem folgenden Befehl wird die Beschreibung der Hostkonfiguration 1014 so geändert, dass die Datenbank für Gehaltsabrechnungen enthalten ist.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/host -id 1014 set -descr "Accounting"
-osType winxp
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = 1014
Operation completed successfully.
```

Löschen von Hostkonfigurationen

Löschen Sie eine Hostkonfiguration.

ANMERKUNG: Durch das Löschen einer Hostkonfiguration werden die mit der Konfiguration verknüpften Verbindungen zu blockbasiertem (Fibre Channel- oder iSCSI-) Speicher getrennt. Hosts, die die Konfiguration von NFS-basierten Speicherverbindungen nutzen, z. B. NFS-Freigaben, greifen bei allen Speicherressourcen, auf die sie zugreifen können, auf die Standard-Zugriffsberechtigungen zurück.

Format

```
/remote/host {-id <value> | -name <value>} delete
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	ID der zu löschenden Hostkonfiguration.
-name	Name der zu löschenden Hostkonfiguration.

Beispiel

Mit dem folgenden Befehl wird die Hostkonfiguration 1014 gelöscht:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/host -id 1014 delete
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
Operation completed successfully.
```

Managen von Host-LUNs

Host-LUNs sind die Speicherressourcen, die zu den Hosts gehören, die mit dem Speichersystem verbunden sind.

Es gibt zwei Arten von Host-LUNs:

- Produktions-LUNs: Lesen-/Schreiben-LUNs, die für den Datenzugriff verwendet werden.
- Snapshot-LUNs: Schreibgeschützte Snapshots und Lesen-/Schreiben-Snapshots einer Produktions-LUN.

Die einzelnen LUNs verfügen über eigene IDs.

In der folgenden Tabelle sind die Attribute für Host-LUNs aufgeführt.

Tabelle 69. Host-LUN-Attribute

Attribut	Beschreibung
ID	Eindeutige Kennung der Host-LUN (HLU).
Host	ID des Hosts, zu dem die LUN gehört.
Host name	Name des Hosts, zu dem die LUN gehört.
LUN	Benutzerfreundliche ID der LUN.
LUN name	LUN-Name.
Snapshot	Snapshot-ID einer LUN oder Consistency Group.
Snapshot name	Snapshot-Name einer LUN oder Consistency Group.
LUN ID	Logische Einheitennummer auf dem Host oder die Host-LUN-ID.
Access	Zugriffsberechtigung für den Host. Gültige Werte: <ul style="list-style-type: none">• read-only

Tabelle 69. Host-LUN-Attribute (fortgesetzt)

Attribut	Beschreibung
	<ul style="list-style-type: none"> • read/write
LUN type	LUN-Typ. Gültige Werte: <ul style="list-style-type: none"> • snap • production

Anzeigen von Host-LUN-Konfigurationen

Zeigen Sie Details zu einer Host-LUN an. Sie können nach der ID des Hosts, der ID der LUN oder dem LUN-Typ filtern.

 **ANMERKUNG:** Aktionsbefehl „show“ erläutert, wie das Ausgabeformat geändert wird.

Format

```
/remote/host/hlu { -id <value> | -host <value> | -hostName <value> | -lun <value> | -lunName <value> | { -host <value> | -hostName <value> } { -lun <value> | -lunName <value> } } [-type { production | snap } ] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Gibt die Host-LUN-ID an.
-host	Gibt die Host-ID an.
-hostName	Gibt den Hostnamen an.
-lun	Gibt die LUN-ID an.
-lunName	Gibt den LUN-Namen an.
-type	Gibt den LUN-Typ an.

Beispiel

Mit dem folgenden Befehl werden alle Host-LUNs auf Host Host_3 aufgeführt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/host/hlu -host Host_3 show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:   ID           = Host_3_sv_2_prod
     Host        = Host_3
     Host name   = 10.0.0.2
     LUN         = sv_2
     LUN name    = joeslun
     Snapshot   =
     Snapshot name =
     LUN ID     = 1
     Access     = Read/write
     LUN type   = Production
```

Ändern der Host-LUN-Konfigurationseinstellungen

Ändern der Host-LUN-ID.

 **ANMERKUNG:** Dieser Vorgang schlägt fehl, wenn Sie versuchen, eine bereits verwendete LUN-ID zuzuweisen.

Format

```
/remote/host/hlu {-id <value>} set -lunid <value>
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Gibt die HLU an.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-lunid	Gibt die neue LUN-ID für die LUN auf dem ausgewählten Host an.

Beispiel

Der folgende Befehl ändert die ID Host_3_sv_2_prod in LUN 0:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/host/hlu -id Host_3_sv_2_prod set -lunid 0
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection
```

```
Operation completed successfully.
```

Hostgruppen managen

Hostgruppen umfassen mehrere Hosts, die Zugriff auf dieselben LUNs oder VMFS-Datenspeicher haben. Auf diese Weise wird der Blockzugriff für Hosts optimiert, da jeder Host in der Gruppe denselben Typ von Zugriff auf die ausgewählten Blockressourcen hat. Durch das Hinzufügen einer neuen LUN oder eines neuen VMFS-Datenspeichers zu einer Hostgruppe ist die Ressource für alle Hosts in dieser Gruppe zugänglich.

Tabelle 70. Attribute der Hostgruppen-Konfiguration

Attribut	Beschreibung
ID	Die ID der Hostgruppe.
Name	Vom Nutzer zugewiesener Name der Hostgruppe.
Description	Beschreibung der Hostgruppe.
Type	Hostgruppen-Typ. Mögliche Werte sind: <ul style="list-style-type: none">• General: Standard-Hostgruppen, die auf LUNs zugreifen.• ESX: VMware-Hostgruppen, die auf LUNs und VMFS-Datenspeicher zugreifen können.
Health state	Integritätsstatus der Hostgruppe Der Integritätsstatuscode wird in Klammern angezeigt. Folgende Werte sind möglich:

Tabelle 70. Attribute der Hostgruppen-Konfiguration (fortgesetzt)

Attribut	Beschreibung
	<ul style="list-style-type: none"> • <code>Unknown (0)</code> : Der Status der Hostgruppe kann nicht bestimmt werden. • <code>OK (5)</code> : Alle Hosts in der Gruppe funktionieren normal. • <code>Degraded/Warning (10)</code> : Die Hostgruppe hat einen oder mehrere Hosts, die herabgesetzt sind. • <code>Critical failure (25)</code> : Die Hostgruppe hat einen oder mehrere Hosts, die sich in einem kritischen Fehlerzustand befinden.
<code>Health details</code>	Zusätzliche Integritätsinformationen.
<code>Hosts</code>	Durch Kommas getrennte Liste der Hosts in der Gruppe.
<code>LUNs accessible by all hosts</code>	Durch Kommas getrennte Liste von LUNs, die für alle Hosts in der Hostgruppe zugänglich sind.
<code>LUNs accessible by some hosts</code>	Durch Kommas getrennte Liste von LUNs, auf die einige der Hosts in der Gruppe zugreifen können, auf die jedoch nicht die gesamte Hostgruppe zugreifen kann.
<code>VMFS Datastores accessible by all hosts</code>	Eine durch Kommas getrennte Liste von VMFS-Datenspeichern, auf die alle Hosts in der Hostgruppe zugreifen können.
<code>VMFS Datastores accessible by some hosts</code>	Eine durch Kommas getrennte Liste von VMFS-Datenspeichern, auf die der Host in der Hostgruppe, jedoch nicht die gesamte Hostgruppe zugreifen kann.

Erstellen einer Hostgruppe

Erstellen Sie eine Gruppe von Hosts, um den Storage-Zugriff zu rationalisieren.

Erstellen Sie eine Gruppe von Hosts und führen Sie optional den Zugriff auf vorhandene LUNs zusammen.

Format

```
/remote/hostgroup create [-async] -name <value> [-descr <value>] -hosts <value> [-mergeExistingAccessToLuns {yes | no} ] [-addLuns <value> [-hlus <value>]] [[--addVmfsDatastores <value>] -vmfsHlus <value>]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
<code>-async</code>	Führen Sie den Befehl im asynchronen Modus aus.
<code>-name</code>	Geben Sie den Namen der Hostgruppe ein.
<code>-description</code>	Geben Sie eine Beschreibung für die Hostgruppe ein.
<code>-hosts</code>	Geben Sie eine durch Kommas getrennte Liste aller Hosts ein, die Sie in die Hostgruppe aufnehmen möchten.
<code>-mergeExistingAccessToLuns</code>	Gibt an, ob der vorhandene LUN-Zugriff auf die Hosts, die der Hostgruppe hinzugefügt werden sollen, mit der Hostgruppe LUN-Zugriff zusammengeführt wird. Beispiel: Wenn Host 2 Zugriff auf LUN 4 hat und Host 2 der Hostgruppe hinzugefügt wird, hat die gesamte Hostgruppe Zugriff auf LUN 4. Gültige Werte: <ul style="list-style-type: none"> • <code>yes</code> • <code>no</code> (Standard)
<code>-addLuns</code>	Geben Sie eine durch Kommas getrennte Liste der IDs für alle zusätzlichen LUNs ein, die von der Hostgruppe zugänglich sein sollen.
<code>-hlus</code> (zur Verwendung mit der Option <code>-addLuns</code>)	Geben Sie eine durch Kommas getrennte Liste der Host-LUN-Kennungen für die entsprechenden LUNs an, die mithilfe der Option <code>-addLuns</code> hinzugefügt wurden. Die Anzahl der Elemente in der durch

Qualifizierer	Beschreibung
	<p>Kommas getrennten Liste für die Option <code>-addLuns</code> und <code>-hlus</code> muss übereinstimmen. Jedes Element in der Liste muss ein numerischer Wert sein. Die angegebenen Host LUN-IDs werden auf alle Hosts in der Hostgruppe angewendet.</p> <p>Wenn diese Option nicht angegeben wird, weist das System automatisch HLU-Werte für jede in der Liste <code>-addLuns</code> angegebene LUN zu.</p>
<code>-type</code>	<p>Geben Sie den Typ der Hostgruppe an. Gültige Werte:</p> <ul style="list-style-type: none"> • <code>General</code> (Standardeinstellung): Hostgruppen, die Zugriff auf LUNs haben. Dazu gehören sowohl die Standard- als auch die VMware (ESX)-Hosts. • <code>ESX</code>: VMware Hostgruppen, die auf LUNs und VMware VMFS-Datenspeicher zugreifen können. Dies kann nur aus ESX-Hosts bestehen.
<code>-addVmfsResources</code>	Geben Sie eine durch Kommas getrennte Liste der IDs für die VMFS-Datenspeicher ein, auf die Sie von der Hostgruppe aus zugreifen möchten.
<code>-vmfsHlus</code> (zur Verwendung mit der Option <code>--addVmfsDatastores</code>)	<p>Geben Sie mithilfe der Option <code>--addVmfsDatastores</code> eine durch Kommas getrennte Liste der Host-LUN-Kennungen für die entsprechenden VMFS-Datenspeicher an. Die Anzahl der Elemente in der durch Kommas getrennten Liste für die Option <code>--addVmfsDatastores</code> und <code>-vmfsHlus</code> muss übereinstimmen. Jedes Element in der Liste muss ein numerischer Wert sein. Die angegebenen Host LUN-IDs werden auf alle Hosts in der Hostgruppe angewendet.</p> <p>Wenn diese Option nicht angegeben wird, weist das System automatisch HLU-Werte für jeden VMFS-Datenspeicher zu, der in der Liste <code>--addVmfsDatastores</code> angegeben ist.</p>

Beispiel

Im folgenden Beispiel wird eine Hostgruppe für die Hosts `Host_1`, `Host_2` und `Host_3` erstellt. Es wurden keine zusätzlichen LUNs angegeben.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/hostgroup create -name MyHostGroup
-descr "this is my host group" -hosts Host_1,Host_2,Host_3
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = HostGroup_1
Operation completed successfully.
```

Eine Hostgruppe anzeigen

Zeigen Sie die Details einer oder mehrerer Hostgruppen an.

Format

```
/remote/hostgroup {-id <value> | -name <value>} [-async] show [-detail]
```

Objektqualifizierer

Qualifizierer	Beschreibung
<code>-id</code>	Geben Sie die ID der Hostgruppe ein.
<code>-name</code>	Geben Sie den Namen der Hostgruppe ein.

Beispiel

Das folgende Beispiel zeigt die Details für alle Hostgruppen im System an.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/hostgroup show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      ID                = HostGroup_1
      Name                = MyHostGroup
      Description         = this is my host group
      Type                = General
      Health state        = OK (5)
      Health details      = "The component is operating normally. No
action  is required."
      Hosts               = Host_1,Host_2,Host_3
      LUNs accessible by all hosts = sv_2,sv_3
      LUNs accessible by some hosts = sv_1
      VMFS Resources accessible by all hosts = res_5,res_6
      VMFS Resources accessible by some hosts = res_4

2:      ID                = HostGroup_2
      Name                = AnotherHostGroup
      Description         = this is host group only contains ESX host
      Type                = ESX
      Health state        = OK (5)
      Health details      = "The component is operating normally. No
action  is required."
      Hosts               = Host_4,Host_5
      LUNs accessible by all hosts = sv_2,sv_3
      LUNs accessible by some hosts =
      VMFS Datastores accessible by all hosts =
      VMFS Datastores accessible by some hosts =
```

Hostgruppen ändern

Ändern Sie die Einstellungen und Details einer vorhandenen Hostgruppe.

Format

```
/remote/hostgroup {-id <value> | -name <value>} set [-async] [-name <value>] [-descr <value>]
{[-addHosts <value> [-mergeAccessToLuns {fromHostGroup | toHostGroup | no }]] [-removeHosts
<value> [-removeAccessToLuns {fromHostGroup | no }]] | [-addLuns <value> [-hlus <value>]]
[-removeLuns <value>]|[--addVmfsDatastores <value> [-vmfsHlus <value>]] [-removeVmfsDatastores
<value>] | [-modifyHlusForLuns <value>[-modifyHlusForHosts <value>]] [-modifyHlus <value>] | [-
modifyHlusForVmfsDatastores <value> [-modifyVmfsHlusForHosts <value>]] [-modifyVmfsHlus <value>]}
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID der Hostgruppe ein.
-name	Geben Sie den Namen der Hostgruppe ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
<code>-async</code>	Führen Sie den Befehl im asynchronen Modus aus.
<code>-name</code>	Geben Sie den neuen Namen für die Hostgruppe ein.
<code>-desc</code>	Geben Sie die neue Beschreibung der Hostgruppe ein.
<code>-addHosts</code>	Geben Sie eine durch Kommas getrennte Liste von Hosts ein, die Sie der vorhandenen Hostgruppe hinzufügen möchten.
<code>-mergeAccessToLuns</code> (zur Verwendung mit der Option <code>-addHosts</code>)	Legen Sie fest, wie der Hostzugriff auf LUNs für neue Hosts zusammengeführt werden soll, wenn sie der bereits vorhandenen Hostgruppe hinzugefügt werden. Gültige Werte: <ul style="list-style-type: none"> • <code>fromHostGroup</code> (Standardeinstellung): LUNs, auf die alle Hosts in der vorhandenen Hostgruppe zugreifen können, sind auch für die neu hinzugefügten Hosts zugänglich. • <code>toHostGroup</code>: LUNs, auf die alle Hosts in der vorhandenen Hostgruppe zugreifen können, sind auch für die neu hinzugefügten Hosts zugänglich und die LUNs, auf die der neue Host bereits Zugriff hat, sind für alle vorhandenen Hosts in der Hostgruppe zugänglich. • <code>no</code>: Der Hostzugriff für die hinzugefügten Hosts ändert sich nicht.
<code>-removeHosts</code>	Geben Sie eine durch Kommas getrennte Liste von Hosts ein, die Sie aus der Hostgruppe entfernen möchten.
<code>-removeAccessToLuns</code> (zur Verwendung mit der Option <code>-removeHosts</code>)	Geben Sie an, ob der Zugriff auf LUNs für die Hosts, die aus der Hostgruppe entfernt wurden, mithilfe der Option <code>-removeHosts</code> entfernt werden soll. Gültige Werte: <ul style="list-style-type: none"> • <code>fromHostGroup</code>: LUNs, auf die alle Hosts in der vorhandenen Hostgruppe zugreifen können, sind nicht mehr für die entfernten Hosts zugänglich. • <code>no</code> (Standardeinstellung): Der Hostzugriff für die entfernten Hosts wird nicht geändert.
<code>-addLuns</code>	Geben Sie eine durch Kommas getrennte Liste von LUNs ein, die der Hostgruppe hinzugefügt werden sollen.
<code>-hlus</code> (zur Verwendung mit der Option <code>-addLuns</code>)	Geben Sie eine durch Kommas getrennte Liste der Host-LUN-Kennungen für die entsprechenden LUNs an, die mithilfe der Option <code>-addLuns</code> hinzugefügt wurden. Die Anzahl der Elemente in der durch Kommas getrennten Liste für die Option <code>-addLuns</code> und <code>-hlus</code> muss übereinstimmen. Jedes Element in der Liste muss ein numerischer Wert sein. Die angegebenen Host LUN-IDs werden auf alle Hosts in der Hostgruppe angewendet. Wenn diese Option nicht angegeben wird, weist das System automatisch HLU-Werte für jede in der Liste <code>-addLuns</code> angegebene LUN zu.
<code>-removeLuns</code>	Geben Sie eine durch Kommas getrennte Liste von LUNs ein, die Sie aus der Hostgruppe entfernen möchten.
<code>-addVmfsDatastores</code>	Geben Sie eine durch Kommas getrennte Liste von VMFS-Datenspeichern ein, die der Hostgruppe hinzugefügt werden sollen.
<code>-vmfsHlus</code>	Geben Sie eine durch Kommas getrennte Liste der Host-LUN-Kennungen für die entsprechenden VMFS-Datenspeicher an, die mithilfe der Option <code>-addVmfsDatastores</code> hinzugefügt werden. Die Anzahl der Elemente in der durch Kommas getrennten Liste für die Option <code>-addVmfsDatastores</code> und <code>-vmfsHlus</code> muss übereinstimmen. Jedes Element in der Liste muss ein numerischer Wert sein. Die angegebenen Host LUN-IDs werden auf alle Hosts in der Hostgruppe angewendet. Wenn diese Option nicht angegeben wird, weist das System automatisch HLU-Werte für jeden VMFS-Datenspeicher zu, der in der Liste <code>-addVmfsDatastores</code> angegeben ist.
<code>-removeVmfsDatastores</code>	Geben Sie eine durch Kommas getrennte Liste der VMFS-Datenspeicher ein, die Sie aus der Hostgruppe entfernen möchten.
<code>-modifyHlusForLuns</code>	Geben Sie eine durch Kommas getrennte Liste von LUN-IDs ein, für die Sie die HLUs in der Hostgruppe ändern möchten.
<code>-modifyHlusForHosts</code>	Geben Sie eine durch Kommas getrennte Liste der Host-IDs ein, für die Sie die HLUs in der Hostgruppe ändern möchten.

Qualifizierer	Beschreibung
<code>-modifyHlus</code> (zur Verwendung mit den Optionen <code>-modifyHlusForLuns</code> und/oder <code>-modifyHlusForHosts</code>)	Geben Sie die durch Kommas getrennte Liste für die HLU-IDs ein, die von den entsprechenden in der Option <code>-modifyHlusForLuns</code> angegebenen LUNs verwendet werden soll. Die Anzahl der Positionen in den beiden Listen muss übereinstimmen. Jedes Element muss numerisch sein. Diese Liste der HLU-IDs wird nur auf die Liste der Hosts angewendet, die in der Option <code>-modifyHlusForHosts</code> angegeben sind. Wenn <code>-modifyHlusForHosts</code> nicht angegeben wird, werden die HLU-IDs auf alle Hosts in der Gruppe angewendet.
<code>-modifyHlusForVmfsDatastores</code>	Geben Sie eine durch Kommas getrennte Liste von VMFS-Datenspeicher-IDs ein, für die Sie die HLU-IDs für in der Hostgruppe ändern möchten.
<code>-modifyVmfsHlusForHosts</code>	Geben Sie eine durch Kommas getrennte Liste der VMFS-Host-IDs ein, für die Sie die HLU-IDs in der Hostgruppe ändern möchten.
<code>-modifyVmfsHlus</code> (zur Verwendung mit den Optionen <code>-modifyHlusForVmfsDatastores</code> und/oder <code>-modifyHlusForHosts</code>)	Geben Sie die durch Kommas getrennte Liste für die HLU-IDs ein, die von den entsprechenden in der Option <code>-modifyHlusForDatastores</code> angegebenen LUNs verwendet werden soll. Die Anzahl der Positionen in den beiden Listen muss übereinstimmen. Jedes Element muss numerisch sein. Diese Liste der HLU-IDs wird nur auf die Liste der Hosts angewendet, die in der Option <code>-modifyVmfsHlusForHosts</code> angegeben sind. Wenn <code>-modifyVmfsHlusForHosts</code> nicht angegeben wird, werden die HLU-IDs auf alle VMFS-Hosts in der Gruppe angewendet.

Beispiel

Im folgenden Beispiel wird Host_8 zu vorhandenen HostGroup_1 hinzugefügt.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/hostgroup -id HostGroup_1 set
-addHosts Host_8
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = HostGroup_1
Operation completed successfully.
```

Hostgruppe löschen

Löschen Sie eine Hostgruppe. Wenn eine Hostgruppe gelöscht wird, werden die Hosts, die sich in der Gruppe befanden, zurück zu eigenständigen Hosts zurückgegeben und Ihr Hostzugriff auf LUNs wird beibehalten. Mit diesem Befehl werden keine Hosts oder LUNs gelöscht.

Format

```
/remote/hostgroup {-id <value> | -name <value>} delete [-async]
```

Objektqualifizierer

Qualifizierer	Beschreibung
<code>-id</code>	Geben Sie die ID der Hostgruppe ein.
<code>-name</code>	Geben Sie den Namen der Hostgruppe ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
<code>-async</code>	Führen Sie den Vorgang im asynchronen Modus aus.

Beispiel

Im folgenden Beispiel wird HostGroup_2 gelöscht:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/hostgroup -id HostGroup_2 delete
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Hostgruppen-LUNs managen

Überprüfen Sie die Konfigurationsdetails der Hostgruppen-LUNs.

Tabelle 71. Konfigurationsattribute der Hostgruppen-LUNs

Attribut	Beschreibung
ID	ID der Hostgruppen-LUN.
Host group	Hostgruppen-ID, zu der die Hostgruppen-LUN gehört.
Host group name	Name der Hostgruppe, zu der die Hostgruppen-LUN gehört.
LUN	ID der LUN.
LUN name	Name der LUN.
LUN type	Beschreibt den Typ der LUN. Mögliche Werte sind: <code>Production</code> .
Accessible hosts	Eine durch Kommas getrennte Liste von Hosts, die Zugriff auf die LUN haben.
Host LUN IDs	Durch Komma getrennte Liste von HLU (Host LUN Identifiers), die die entsprechenden Hosts verwenden, um auf die LUN zuzugreifen.
Inaccessible hosts	Eine durch Kommas getrennte Liste von Hosts in der Hostgruppe, die nicht auf die LUN zugreifen können.
Default Host LUN ID	Die ID der Standard-Host-LUN, die verwendet werden soll, wenn neue Hosts zur Hostgruppe hinzugefügt werden. Wenn kein Wert angezeigt wird, gibt es keine Standard-HLU-ID.

Hostgruppen-LUNs anzeigen

Sie können die Details einer oder mehrerer Hostgruppen-LUNs anzeigen.

Format

```
/remote/hostgroup/hglu {-id <value> | -hostgroup <value> | -hostgroupName <value>} show [-detail]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die HLU-ID an.
-hostgroup	Geben Sie die ID der Hostgruppe ein.
-hostgroupname	Geben Sie den Namen der Hostgruppe ein.

Beispiel

Das folgende Beispiel zeigt die Details aller Hostgruppen-LUNs für HostGroup_3 an.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/hostgroup/hglu -hostgroup HostGroup_3 show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:   ID                = HostGroup_1_sv_1_prod
     Host group       = HostGroup_1
     Host group name  = testhg
     LUN              = sv_1
     LUN name         = testLuns-1
     LUN type         = Production
     Accessible hosts = Host_1,Host_2
     Host LUN IDs     = 1,1
     Inaccessible hosts = Host_3
     Default Host LUN ID

2:   ID                = HostGroup_1_sv_2_prod
     Host group       = HostGroup_1
     Host group name  = testhg
     LUN              = sv_2
     LUN name         = testLuns-2
     LUN type         = Production
     Accessible hosts = Host_1,Host_2,Host_3
     Host LUN IDs     = 2,2,0
     Inaccessible hosts =

3:   ID                = HostGroup_1_sv_3_prod
     Host group       = HostGroup_1
     Host group name  = testhg
     LUN              = sv_3
     LUN name         = testLuns-3
     LUN type         = Production
     Accessible hosts = Host_1,Host_2,Host_3
     Host LUN IDs     = 3,3,1
     Inaccessible hosts =
```

Managen von Hostinitiatoren

Nachdem Sie eine Hostkonfiguration zur Steuerung des Hostzugriffs auf den Speicher im System erstellt haben, müssen Sie für jede Hostkonfiguration, die auf das Speichersystem zugreift, mindestens einen Initiator erstellen. Jeder Initiator steht für den Initiator auf dem Host, der eine Verbindung zum Speichersystem herstellt. Es gibt zwei Typen von Initiatoren, Fibre Channel (FC) und iSCSI.

Ein Fibre-Channel-Initiator enthält den WWN eines HBA auf dem Host. Dieser WWN ist nicht der WWN des Hosts.

Ein iSCSI-Initiator enthält den vom Host verwendeten IQN (iSCSI Qualified Name) und optional das mit dem Host verknüpfte Kennwort der CHAP-Authentifizierung. [Managen des gegenseitigen CHAP für die gegenseitige CHAP-Authentifizierung](#) erläutert, wie die gegenseitige CHAP-Authentifizierung im System konfiguriert wird.

Jeder Initiator wird über eine ID identifiziert.

In der folgenden Tabelle sind die Attribute für Initiatoren aufgeführt.

Tabelle 72. Attribute für Initiatoren

Attribut	Beschreibung
ID	Hostinitiator-ID
Host	Name des übergeordneten Hosts.
UID	FC WWN oder iSCSI IQN des Initiators.
Initiator type	Der Typ des Initiators. Folgende Werte sind möglich:

Tabelle 72. Attribute für Initiatoren (fortgesetzt)

Attribut	Beschreibung
	<ul style="list-style-type: none"> • FC • iSCSI
Ports logged in	Durch Kommata getrennte Liste der Array-Zielports, an denen der Initiator angemeldet ist.
Ignored	<p>Gibt an, ob der Initiator für den Datenzugriff auf den Host ignoriert wird. Folgende Werte sind möglich:</p> <ul style="list-style-type: none"> • Yes : Der Initiator wird ignoriert. • No : Der Initiator wird nicht ignoriert.
Health state	<p>Der aktuelle Integritätsstatus des Systems. Der Integritätsstatuscode wird in Klammern angezeigt. Folgende Werte sind möglich:</p> <ul style="list-style-type: none"> • Unknown (0) : Status ist unbekannt. • OK (5) : Funktioniert ordnungsgemäß. • OK BUT (7) : Funktioniert ordnungsgemäß, aber es könnte ein Problem vorliegen. • Degraded/Warning (10) : Funktioniert und führt alle Funktionen aus, die Performance ist jedoch eventuell nicht optimal. • Minor failure (15) : Funktioniert und führt alle Funktionen aus, aber die Gesamtpformance ist eingeschränkt. Diese Bedingung hat geringe Auswirkungen auf das System, und das Problem sollte in der näheren Zukunft angegangen werden, aber eine unmittelbare Lösung ist nicht erforderlich. • Major failure (20) : Im System sind Fehler aufgetreten, und einige oder alle Funktionen funktionieren nur noch eingeschränkt oder gar nicht mehr. Dieser Zustand hat erhebliche Auswirkungen auf das System und muss sofort beseitigt werden. • Critical failure (25) : Es ist ein Fehler aufgetreten; eine Recovery ist eventuell nicht möglich. Diese Bedingung hat zu Datenverlusten geführt. Der Fehler muss umgehend behoben werden. • Non-recoverable error (30) : Das System ist komplett ausgefallen und kann nicht wiederhergestellt werden.
Health details	Zusätzliche Integritätsinformationen. Weitere Informationen zur Integrität finden Sie im Anhang A, Referenz.
CHAP users	Liste der CHAP-Konten, die für den Initiator konfiguriert sind.
Source type	<p>Der Quelltyp des Initiators. Mögliche Werte sind:</p> <ul style="list-style-type: none"> • HPAutotrespass : HP mit automatischer Überschreitung • OpenNative : (Standardeinstellung): Offen nativ (z. B. CLARiiON Open) • SGI : Silicon Graphics • HPNoAutotrespass: HP ohne automatische Überschreitung • Dell • FujitsuSiemens • Tru64: Compaq Tru64
Failover mode	<p>Der Failover-Modus für den Initiator. Mögliche Werte sind:</p> <ul style="list-style-type: none"> • AutoTrespass: Jeder Medienzugriff auf den Speicherprozessor, der nicht Eigentümer ist, wird abgelehnt. • PassiveNotReady: Ein Befehlsausfall während I/O wird an den SP, der nicht Eigentümer ist, gesendet. • DMP: Automatisches Überschreiten bei I/O an Speicherprozessor, der nicht Eigentümer ist. • PassiveAlwaysReady: Einige Befehle, z. B. „Test Unit Ready“, geben den PAR-Status zurück. • ALUA(Standardeinstellung): Initiatoren dürfen I/O an eine LUN senden, unabhängig davon, welcher Speicherprozessor tatsächlich Eigentümer der LUN ist.
LUNZ enabled	<p>Gibt an, ob LUNZ aktiviert ist. Mögliche Werte sind:</p> <ul style="list-style-type: none"> • yes (Standard) • no

Tabelle 72. Attribute für Initiatoren (fortgesetzt)

Attribut	Beschreibung
Unit serial number	Gibt die Unity-Seriennummer an. Mögliche Werte sind: <ul style="list-style-type: none"> • Array (Standard) • LUN Bei SCSI-3-Schnittstellen finden Sie die Seriennummer des Arrays oder der LUN auf der Seite „Unity Serial Number“ („Vital Product Data“, Seitencode 0x80).

Initiatoren erstellen

Erstellen Sie einen FC- oder iSCSI-Initiator und weisen Sie ihn einer Hostkonfiguration zu.

Format

```
/remote/initiator create -host <value> -uid <value> -type {iscsi|fc} [-sourceType {HPAutotrespass | OpenNative | SGI | HPNoAutotrespass | Dell | FujitsuSiemens | Tru64}] [-failoverMode {AutoTrespass | PassiveNotReady | DMP | PassiveAlwaysReady | ALUA}] [-lunzEnabled {yes | no}] [-unitSerialNumber {Array | LUN}]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-host	Identifiziert die Hostkonfiguration, der der Initiator zugewiesen werden soll.
-uid	Gibt den FC WWN oder den iSCSI IQN des Hosts an, dem der Initiator zugewiesen werden soll.
-type	Gibt den Typ des Initiators an. Folgende Werte sind möglich: <ul style="list-style-type: none"> • iscsi • fc
-sourceType	Gibt den Quelltyp für den Initiator an. Gültige Werte: <ul style="list-style-type: none"> • HPAutotrespass: HP mit automatischer Überschreitung • OpenNative: (Standardeinstellung): Offen nativ (z. B. CLARiiON Open) • SGI: Silicon Graphics • HPNoAutotrespass: HP ohne automatische Überschreitung • Dell • FujitsuSiemens • Tru64: Compaq Tru64
-failoverMode	Gibt den Failover-Modus für den Initiator an. Gültige Werte: <ul style="list-style-type: none"> • AutoTrespass: Jeder Medienzugriff auf den Speicherprozessor, der nicht Eigentümer ist, wird abgelehnt. • PassiveNotReady: Ein Befehlsausfall während I/O wird an den SP, der nicht Eigentümer ist, gesendet. • DMP: Automatisches Überschreiten bei I/O an Speicherprozessor, der nicht Eigentümer ist. • PassiveAlwaysReady: Einige Befehle, z. B. „Test Unit Ready“, geben den PAR-Status zurück. • ALUA (Standardeinstellung): Initiatoren dürfen I/O an eine LUN senden, unabhängig davon, welcher Speicherprozessor tatsächlich Eigentümer der LUN ist.
-lunzEnabled	Legt fest, ob LUNZ aktiviert wird. Gültige Werte: <ul style="list-style-type: none"> • yes (Standard) • no
-unitSerialNumber	Geben Sie die Einheitenseriennummer an. Gültige Werte: <ul style="list-style-type: none"> • Array (Standard) • LUN

Qualifizierer	Beschreibung
	Bei SCSI-3-Schnittstellen finden Sie die Seriennummer des Arrays oder der LUN auf der Seite „Unity Serial Number“ („Vital Product Data“, Seitencode 0x80).

Beispiel 1

Mit dem folgenden Befehl wird ein FC-Initiator für Hostkonfiguration 1014 erstellt. Der Fibre-Channel-Initiator erhält die ID 1021:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/initiator create -host 1014 -uid "20:00:00:00:C9:29:0F:FD:10:00:00:00:C9:29:0F:FD" -type fc
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = 1021
Operation completed successfully.
```

Beispiel 2

Mit dem folgenden Befehl wird ein iSCSI-Initiator für Hostkonfiguration Host_3 erstellt. Der iSCSI-Initiator erhält die ID 1022:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! -sslPolicy accept /remote/initiator create -host Host_3 -uid iqn.1000-05.com.fancy:win-123456 -type iscsi
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = 1022
Operation completed successfully.
```

Beispiel 3

Mit dem folgenden Befehl wird ein iSCSI-Initiator für „Host_3“ erstellt mit:

- dem Quelltyp „OpenNative“
- dem Failover-Modus „PassiveAlwaysReady“
- deaktiviertem LUNZ
- und der Einheitenseriennummer „Array“

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/initiator create -host Host_3 -uid iqn.1993-08.com.microsoft:win -type iscsi -sourceType OpenNative -failoverMode PassiveAlwaysReady -lunzEnabled no -unitSerialNumber Array
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = HostInitiator_8
Operation completed successfully.
```

Anzeigen von Initiatoren

Zeigen Sie eine Liste der Initiatoren an. Sie können nach Initiator-ID, Host-ID oder nach der Registrierung des Initiators filtern.

Format

```
/remote/initiator [{-id <value> | -host <value> | -unregistered}] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Identifiziert den Initiator.
-host	Geben Sie die ID einer Hostkonfiguration ein, um die Initiatoren, die der Hostkonfiguration zugewiesen sind, anzuzeigen.
-unregistered	Gibt nicht registrierte Initiatoren an.

Beispiel

Mit dem folgenden Befehl werden die Details aller auf dem System vorhandenen Initiatoren aufgeführt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/initiator show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1: ID                = HostInitiator_7
   Host              = Host_4
   UID               = iqn.1991-05.com.microsoft:cnenfanw411c.corp.emc.com
   Initiator type    = iscsi
   Ports logged in   = spb_eth2,spa_eth2
   Ignored           = no
   Health State      = OK (5)
   Health Details    = "The component is operating normally. No action is required."
   CHAP users        =
   Source type       = Open_Native
   Failover mode     = ALUA
   LUNZ              = yes
   Unit serial number = Array
```

Ändern von Initiatoreinstellungen

Ändern Sie einen bereits erstellten Initiator.

Format

```
/remote/initiator -id <value> set [-ignored {yes | no}] [-host <value>] [-sourceType {HPAutotrespass | OpenNative | SGI | HPNoAutotrespass | Dell | FujitsuSiemens | Tru64}] [-failoverMode {AutoTrespass | PassiveNotReady | DMP | PassiveAlwaysReady | ALUA}] [-lunzEnabled {yes | no}] [-unitSerialNumber {Array | LUN}]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Gibt die ID des Initiators an.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-ignored	Gibt an, ob der Initiator für den Datenzugriff auf den Host ignoriert wird. Gültige Werte: <ul style="list-style-type: none">• yes: Der Initiator wird ignoriert.• no: Der Initiator wird nicht ignoriert.

Qualifizierer	Beschreibung
-host	Gibt die Hostkonfiguration an, der der Initiator zugewiesen ist. In Anzeigen von Hostkonfigurationen wird erläutert, wie Sie die IDs der Hostkonfigurationen im System anzeigen können.
-sourceType	Gibt den Quelltyp für den Initiator an. Gültige Werte: <ul style="list-style-type: none"> • HPAutotrespass: HP mit automatischer Überschreitung • OpenNative: Offen nativ (z. B. CLARiiON Open) • SGI: Silicon Graphics • HPNoAutotrespass: HP ohne automatische Überschreitung • Dell • FujitsuSiemens • Tru64: Compaq Tru64
-failoverMode	Gibt den Failover-Modus für den Initiator an. Gültige Werte: <ul style="list-style-type: none"> • AutoTrespass: Jeder Medienzugriff auf den Speicherprozessor, der nicht Eigentümer ist, wird abgelehnt. • PassiveNotReady: Ein Befehlsausfall während I/O wird an den SP, der nicht Eigentümer ist, gesendet. • DMP: Automatisches Überschreiten bei I/O an Speicherprozessor, der nicht Eigentümer ist. • PassiveAlwaysReady: Einige Befehle, z. B. „Test Unit Ready“, geben den PAR-Status zurück. • ALUA: Initiatoren dürfen I/O an eine LUN senden, unabhängig davon, welcher Speicherprozessor tatsächlich Eigentümer der LUN ist.
-lunzEnabled	Legt fest, ob LUNZ aktiviert wird. Gültige Werte: <ul style="list-style-type: none"> • yes • no
-unitSerialNumber	Geben Sie die Einheitenseriennummer an. Gültige Werte: <ul style="list-style-type: none"> • Array • LUN Bei SCSI-3-Schnittstellen finden Sie die Seriennummer des Arrays oder der LUN auf der Seite „Unity Serial Number“ („Vital Product Data“, Seitencode 0x80).
-force	Sie können angeben, dass die Prüfung der Festlegung eines neuen Hosts umgangen werden soll, wenn bereits Speicherressourcen mit dem Host verbunden und an den Initiator angehängt sind. Wenn Sie einen veralteten Initiator löschen möchten, für den der zugehörige Host LUN-Zugriff hat und als solche diese LUNs nicht gelöscht werden können, müssen Sie den zugehörigen Host ignorieren, indem Sie mit dieser <code>-force</code> -Option den veralteten Initiator auf einen leeren Host festlegen.

Beispiel

Mit dem folgenden Befehl werden der Quelltyp, der Failover-Modus, die LUNZ-Einstellungen und die Einheitenseriennummer des Initiators geändert:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/initiator -id HostInitiator_6 set
-sourceType HPAutotrespass -failoverMode PassiveNotReady -lunzEnabled yes -unitSerialNumber
Array
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
Operation completed successfully.
```

Managen von Hostinitiatorpfaden

Das Speichersystem kommuniziert mit einem Hostinitiator über einen Hostinitiatorpfad. Das Speichersystem verwendet diesen Pfad, um die Hostinitiator-Konfigurationsinformationen zu identifizieren.

In der folgenden Tabelle sind die Attribute für einen Hostinitiatorpfad aufgeführt.

Tabelle 73. Attribute für Initiatorpfade

Attribut	Beschreibung
Initiator	Übergeordneter Initiator
Port	Die ID des Zielports.
Logged in	Gibt an, ob der Initiatorpfad angemeldet ist. Folgende Werte sind möglich: <ul style="list-style-type: none"> • Yes • No
Host	Die Host-ID, für die der Initiatorpfad registriert ist. Wenn in diesem Feld kein Wert enthalten ist, ist der Initiator bei keinem Host registriert. <i>i</i> ANMERKUNG: Diese Host-ID kann sich von der des Initiators unterscheiden, wenn die Auto-Push-Registrierungs- und die Initiatorregistrierungsinformationen nicht identisch sind. Auf diese Weise erzeugt das Speichersystem eine Warnmeldung.
Registration method	Gibt an, wie der Initiatorpfad registriert ist. Folgende Werte sind möglich: <ul style="list-style-type: none"> • Unknown: Der Initiator wurde von einer anderen Methode als ESX-Push registriert. • ESX: ESX hat die Initiatorregistrierung per Push an das Speichersystem weitergeleitet.
Session IDs	Durch Kommata getrennte Liste der Sitzungs-IDs für diesen Pfad.
Health state	Der aktuelle Integritätsstatus des Systems. Der Statuscode wird in Klammern angezeigt. Folgende Werte sind möglich: <ul style="list-style-type: none"> • Unknown (0): Status ist unbekannt. • OK (5) : Funktioniert ordnungsgemäß. • OK BUT (7): Funktioniert ordnungsgemäß, aber es könnte ein Problem vorliegen. • Degraded/Warning (10): Funktioniert und führt alle Funktionen aus, die Performance ist jedoch eventuell nicht optimal. • Minor failure (15): Funktioniert und führt alle Funktionen aus, aber die Gesamtperformance ist eingeschränkt. Diese Bedingung hat geringe Auswirkungen auf das System, und das Problem sollte in der näheren Zukunft angegangen werden, aber eine unmittelbare Lösung ist nicht erforderlich. • Major failure (20): Im System sind Fehler aufgetreten, und einige oder alle Funktionen funktionieren nur noch eingeschränkt oder gar nicht mehr. Dieser Zustand hat erhebliche Auswirkungen auf das System und muss sofort beseitigt werden. • Critical failure (25) : Es ist ein Fehler aufgetreten; eine Recovery ist eventuell nicht möglich. Diese Bedingung hat zu Datenverlusten geführt. Der Fehler muss umgehend behoben werden. • Non-recoverable error (30) : Das System ist komplett ausgefallen und kann nicht wiederhergestellt werden.
Health details	Zusätzliche Integritätsinformationen. In Health details finden Sie Einzelheiten zu den Integritätsinformationen.

Initiatorpfade anzeigen

Zeigen Sie eine Liste der Initiatoren an. Sie können nach der Initiator-ID filtern.

 **ANMERKUNG:** Aktionsbefehl „show“ erläutert, wie das Ausgabeformat geändert wird.

Format

```
/remote/initiator/path [-initiator <value>] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-initiator	Geben Sie die ID des Initiators ein, zu die zugeordneten Pfade anzuzeigen.

Beispiel

Mit dem folgenden Befehl werden alle auf dem System vorhandenen Initiatorpfade aufgeführt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/initiator/path show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:   Initiator           = 1043
     Port               = eth1_SPB
     Logged in          = Yes
     Registration method = ESX
     Host               = 1014
     Health state       = OK (5)
```

Managen von iSCSI-CHAP-Konten für die einseitige CHAP-Authentifizierung

Im System wird ein CHAP-Konto zur Authentifizierung eines Hosts (Initiators) verwendet, der versucht, auf eine iSCSI-Speicherressource (Ziel) zuzugreifen. Es werden die folgenden Arten von CHAP-Authentifizierung unterschieden:

- Einseitig, d. h., es wird nur der Initiator vom Ziel authentifiziert. Erstellen Sie zur Festlegung der einseitigen CHAP-Authentifizierung ein CHAP-Konto für eine Hostkonfiguration, bei der auf iSCSI-Speicher zugegriffen wird.
- Gegenseitig, d. h., Ziel und Initiator authentifizieren sich gegenseitig. Im Vergleich zum einseitigen CHAP bietet das gegenseitige CHAP zusätzliche Sicherheit. Zur Festlegung von gegenseitigem CHAP geben Sie ein entsprechendes Schlüsselpasswort an. [Managen des gegenseitigen CHAP für die gegenseitige CHAP-Authentifizierung](#) erläutert, wie Sie die gegenseitige CHAP-Authentifizierung konfigurieren.

Die einzelnen CHAP-Konten verfügen über eigene IDs.

In der folgenden Tabelle werden die Attribute für CHAP-Konten aufgeführt.

Tabelle 74. Attribute von CHAP-Konten

Attribut	Beschreibung
ID	Die ID des CHAP-Kontos.
IQN	Die IQN-Adresse des Hosts (Initiators).

Tabelle 74. Attribute von CHAP-Konten (fortgesetzt)

Attribut	Beschreibung
Wildcard	Gibt an, ob es sich um den Platzhalter CHAP handelt, bei dem alle Initiatoren vom Speichersystem authentifiziert werden können. Gültige Werte: <ul style="list-style-type: none"> • <code>yes</code>: Alle Initiatoren können vom Speichersystem authentifiziert werden. • <code>no</code>: Die Authentifizierung erfolgt einzeln für jeden Initiator.
Username	CHAP-Benutzername.
Secret	Das CHAP-Schlüsselpasswort.
Secret format	Das CHAP-Eingabeformat. Gültige Werte: <ul style="list-style-type: none"> • <code>ascii</code>: ASCII-Format • <code>hex</code>: Hexadezimalformat

Erstellen von iSCSI-CHAP-Konten

Erstellen Sie ein iSCSI-CHAP-Konto für einen Host (Initiator).

Format

```
/remote/iscsi/chap create {-iqn <value> | -wildcard} [-username <value>] {-secret <value> | -secretSecure} [ -secretFormat { ascii | hex } ]
```

Objektqualifizierer

Qualifizierer	Beschreibung
<code>-iqn</code>	Gibt die IQN-Adresse des Hosts (Initiator) an.
<code>-wildcard</code>	Gibt an, ob es sich um einen Platzhalter CHAP handelt, bei dem alle Initiatoren vom Speichersystem authentifiziert werden können.
<code>-username</code>	Gibt den CHAP-Benutzernamen an.
<code>-secret</code>	Gibt das CHAP-Schlüsselpasswort an.
<code>-secretSecure</code>	Gibt den CHAP-Schlüssel im sicheren Modus an – der Benutzer wird aufgefordert, das Passwort einzugeben.
<code>-secretFormat</code>	Gibt das CHAP-Eingabeformat an. Gültige Werte: <ul style="list-style-type: none"> • <code>ascii</code> (Standard): ASCII-Format • <code>hex</code>: Hexadezimalformat

Beispiel

Mit dem folgenden Befehl wird ein iSCSI-CHAP-Konto für einen Host erstellt. Das Konto erhält die ID `CHAP_1`:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/iscsi/chap create -iqn iqn.1991-05.com.microsoft:cpc7745 -secret opqrstuvwxyz
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = CHAP_1
Operation completed successfully.
```

Anzeigen von iSCSI-CHAP-Konten

Zeigen Sie Details zu den iSCSI-CHAP-Konten im System an.

 **ANMERKUNG:** Aktionsbefehl „show“ erläutert, wie das Ausgabeformat geändert wird.

Format

```
/remote/iscsi/chap [-id <value>] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Identifiziert das iSCSI-CHAP-Konto.

Beispiel

Mit dem folgenden Befehl werden sämtliche iSCSI-CHAP-Konten im System angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/iscsi/chap show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:   ID       = CHAP_1
     IQN      = iqn.1991-05.com.microsoft:cpc7745
     Wildcard = no
     Username = iqn.1991-05.com.microsoft:cpc7745

2:   ID       = CHAP_2
     IQN      =
     Wildcard = yes
     Username = globalChapUserName
```

Ändern der Einstellungen für iSCSI-CHAP-Konten

Ändern Sie die Einstellungen eines iSCSI-CHAP-Kontos, wie z. B. das Schlüsselpasswort.

Format

```
/remote/iscsi/chap -id <value> set [-username <value>]{-secret <value> | -secretSecure} [ -secretFormat { ascii | hex } ]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Identifiziert das zu ändernde iSCSI-CHAP-Konto.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-username	Gibt den CHAP-Benutzernamen an.

Qualifizierer	Beschreibung
-secret	Gibt das CHAP-Schlüsselpasswort an.
-secretSecure	Gibt den CHAP-Schlüssel im sicheren Modus an – der Benutzer wird aufgefordert, das Passwort einzugeben.
-secretFormat	Gibt das CHAP-Eingabeformat an. Folgende Werte sind möglich: <ul style="list-style-type: none"> • ascii: ASCII-Format • hex: Hexadezimaales Format

Beispiel

Mit dem folgenden Befehl wird das Schlüsselpasswort für iSCSI-CHAP-Konto CHAP_1 aktualisiert:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/iscsi/chap -id CHAP_1 set -secret abcdef123456
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Löschen von iSCSI-CHAP-Konten

Löschen Sie ein iSCSI-CHAP-Konto.

 **ANMERKUNG:** Wenn Sie ein iSCSI-CHAP-Konto löschen, wird der Host, der das Konto verwendet hat, beim Versuch des Zugriffs auf den iSCSI-Speicher nicht mehr authentifiziert.

Format

```
/remote/iscsi/chap -id <value> delete
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des zu löschenden CHAP-Kontos ein.

Beispiel

Mit dem folgenden Befehl wird iSCSI-CHAP-Konto CHAP_1 gelöscht:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/iscsi/chap -id CHAP_1 delete
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Verwalten von iSCSI-Verbindungen

Identifiziert iSCSI-Verbindungen zwischen Ziel-Speicherprozessoren und Arrays mit dem Quellsystem, die für die Erstellung von iSCSI-Verbindungspfaden erforderlich sind.

ANMERKUNG: Es kann nur eine iSCSI-Verbindung gleichzeitig erstellt werden. Daher kann nur ein Quellsystem für einen Migrationsvorgang verwaltet werden. Wenn ein Migrationsvorgang bereits abgeschlossen ist, müssen Sie eine neue iSCSI-Verbindung mit neuen Pfaden erstellen.

In der folgenden Tabelle sind die Attribute für iSCSI-Verbindungen aufgeführt.

Tabelle 75. iSCSI-Verbindungsattribute

Attribut	Beschreibung
ID	ID der iSCSI-Verbindung.
Name	Name der iSCSI-Verbindung.
Description	Beschreibung der iSCSI-Verbindung.

Erstellen einer iSCSI-Verbindung

Erstellen Sie eine iSCSI-Verbindung.

ANMERKUNG: Es kann nur eine iSCSI-Verbindung gleichzeitig erstellt werden. Daher kann nur ein Quellsystem für einen Migrationsvorgang verwaltet werden. Wenn ein Migrationsvorgang bereits abgeschlossen ist, müssen Sie eine neue iSCSI-Verbindung mit neuen Pfaden erstellen.

Format

```
/remote/iscsi/connection create -name <value> [-descr <value>] [-async]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-name	Gibt den Namen der iSCSI-Verbindung an.
-descr	Gibt die Beschreibung der iSCSI-Verbindung an.
-async	Führen Sie den Vorgang im asynchronen Modus aus.

Beispiel

Mit dem folgenden Befehl wird eine iSCSI-Verbindung erstellt.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/iscsi/connection create -name myConn -descr "Connection for lun_1 importing"
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = iscsi_conn_1
Operation completed successfully.
```

Anzeigen von iSCSI-Verbindungseinstellungen

Zeigen Sie Details zu den bestehenden iSCSI-Verbindungen an.

Format

```
/remote/iscsi/connection [{-id <value> | -name <value>}] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID der iSCSI-Verbindung ein.
-name	Geben Sie den eindeutigen Namen der iSCSI-Verbindung ein.

Beispiel

Dieses Beispiel zeigt alle iSCSI-Verbindungen.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/iscsi/connection show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      ID              = iscsi_conn_1
      Name              = Old Array
      Description       = LUN 1 import
```

Ändern der iSCSI-Verbindungseinstellungen

Ändern Sie die aktuellen iSCSI-Verbindungseinstellungen.

Format

```
/remote/iscsi/connection {-id <value> | -name <value>} set -descr <value> [-async]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID der iSCSI-Verbindung ein.
-name	Geben Sie den eindeutigen Namen der iSCSI-Verbindung ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-descr	Geben Sie die Beschreibung der iSCSI-Verbindung ein.
-async	Führen Sie den Vorgang im asynchronen Modus aus.

Beispiel

Der folgende Befehl ändert die Beschreibung für die iSCSI-Verbindung.

```
uemcli uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/iscsi/connection -id iscsi_conn_1 set -descr copyconnection
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Löschen einer iSCSI-Verbindung

Löscht eine bestehende iSCSI-Verbindung.

ANMERKUNG: Wenn Sie eine iSCSI-Verbindung löschen, werden auch alle iSCSI-Verbindungspfade, die mit der iSCSI-Verbindung verbunden sind, gelöscht.

Format

```
/remote/iscsi/connection {-id <value> | -name <value>} delete [-async]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID der iSCSI-Verbindung ein, die Sie löschen möchten.
-name	Geben Sie den eindeutigen Namen der iSCSI-Verbindung ein, die Sie löschen möchten.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.

Beispiel

Der folgende Befehl löscht die iSCSI-Verbindung „iscsi_conn_1“.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/iscsi/connection -id iscsi_conn_1 delete
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
Operation completed successfully.
```

Verwalten der iSCSI-Verbindungspfade

Der iSCSI-Verbindungspfad zu einem Remotesystem umfasst IP-Adresse, TCP-Port und eine Liste von iSCSI-Schnittstellen auf dem Speichersystem, von dem aus ausgehende iSCSI-Verbindungen hergestellt werden. Auf einer iSCSI-Verbindung können ein oder mehrere iSCSI-Pfade konfiguriert sein.

ANMERKUNG: Wenn das Quellsystem eine iSCSI-Adresse hat, die CHAP-Anmeldeinformationen enthält, müssen Sie die CHAP-Anmeldeinformationen vor der Migration von der iSCSI-Adresse entfernen und dann die CHAP-Anmeldeinformationen wiederherstellen, sobald die Migration abgeschlossen ist.

In der folgenden Tabelle sind die Attribute für iSCSI-Verbindungspfade aufgeführt.

Tabelle 76. iSCSI-Verbindungspfadattribute

Attribut	Beschreibung
Index	Nummer des iSCSI-Pfades innerhalb der iSCSI-Verbindung.
iSCSI connection	ID der iSCSI-Verbindung.
iSCSI connection name	Name der iSCSI-Verbindung.

Tabelle 76. iSCSI-Verbindungspfadattribute (fortgesetzt)

Attribut	Beschreibung
iSCSI path description	Beschreibung des iSCSI-Pfades.
Remote iSCSI address	IP-Adresse des iSCSI-Ziels auf dem Remotesystem.
Remote iSCSI port	TCP-Port des iSCSI-Ziels auf dem Remotesystem.
Local iSCSI interfaces	Liste der Identifikatoren der iSCSI-Schnittstellen auf dem lokalen Speichersystem.

Erstellen eines iSCSI-Verbindungspfads

Erstellt einen neuen iSCSI-Pfad und fügt ihn zu einer bestimmten iSCSI-Verbindung hinzu.

Format

```
/remote/iscsi/connection/path create {-connection <value> | -connectionName <value>} [-descr <value>] -addr <value> [-port <value>] -if <value> [-async]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-connection	Geben Sie die ID der iSCSI-Verbindung ein, zu der Sie einen Pfad hinzufügen möchten.
-connectionName	Geben Sie den eindeutigen Namen der iSCSI-Verbindung ein, zu der Sie einen Pfad hinzufügen möchten.
-descr	Geben Sie die Beschreibung des iSCSI-Pfades ein.
-addr	Geben Sie die IP-Adresse des Remotesystem-iSCSI-Ziels ein. i ANMERKUNG: Geben Sie keine iSCSI-Portaladresse an, die die Verbindung nur an eine andere Adresse umleitet. Unity unterstützt keine iSCSI-Umleitungen.
-port	Der Standard-TCP-Port ist 3260. Wenn die Portnummer von der Standardeinstellung abweicht, geben Sie den TCP-Port des Remotesystem-iSCSI-Ziels ein.
-if	Geben Sie eine durch Komma getrennte Liste von iSCSI-Schnittstellen auf dem lokalen Quellsystem an. i ANMERKUNG: Sie können Informationen zu bestehenden iSCSI-Schnittstellen mithilfe des Befehls <code>/net/if show</code> finden. Wenn ein System zwei Speicherprozessoren hat, stellen Sie sicher, dass Sie iSCSI-Netzwerkschnittstellen für beide Speicherprozessoren angeben.
-async	Führen Sie den Vorgang im asynchronen Modus aus.

Beispiel

Der folgende Befehl erstellt einen iSCSI-Pfad für die iSCSI-Verbindung „iscsi_conn_1“.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/iscsi/connection/path create -connection iscsi_conn_1 -addr 10.0.0.4 -if if_1,if_2
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Anzeigen von iSCSI-Verbindungspfadeinstellungen

Zeigen Sie Details zu den bestehenden iSCSI-Verbindungspfaden an.

Format

```
/remote/iscsi/connection/path [{"-connection <value> | -connectionName <value>}] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-connection	Geben Sie die ID der iSCSI-Verbindung ein.
-connectionName	Geben Sie den eindeutigen Namen der iSCSI-Verbindung ein.

Beispiel

Dieses Beispiel zeigt alle iSCSI-Verbindungspfade.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/iscsi/connection/path -connection iscsi_conn_1 show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      Index                = 1
       iSCSI connection      = iscsi_conn_1
       iSCSI connection name = MyConn
       iSCSI path description = SP 2 node 1
       Remote iSCSI address  = 10.0.0.4
       Remote iSCSI port     = 3260
       Local iSCSI interfaces = IF_1,IF_2

2:      Index                = 2
       iSCSI connection      = iscsi_conn_1
       iSCSI connection name = MyConn
       iSCSI path description = SP 1 node 2
       Remote iSCSI address  = 10.0.0.6
       Remote iSCSI port     = 3260
       Local iSCSI interfaces = IF_1,IF_2
```

Löschen eines iSCSI-Verbindungspfads

Löscht einen bestehenden iSCSI-Verbindungspfad.

 **ANMERKUNG:** Wenn Sie eine iSCSI-Verbindung löschen, werden auch alle iSCSI-Verbindungspfade, die mit dieser iSCSI-Verbindung verbunden sind, gelöscht. Sie müssen die Pfade nicht manuell löschen.

Format

```
/remote/iscsi/connection/path {-connection <value> | -connectionName <value>} -index <value>
delete [-async]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-connection	Geben Sie die ID der iSCSI-Verbindung ein, die den Pfad hat, den Sie löschen möchten.
-connectionName	Geben Sie den eindeutigen Namen der iSCSI-Verbindung ein, die den Pfad hat, den Sie löschen möchten.
-index	Geben Sie die Nummer des iSCSI-Pfades ein, den Sie aus der iSCSI-Verbindung löschen möchten.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.

Beispiel

Der folgende Befehl löscht den Pfad „1“ von der iSCSI-Verbindung „iscsi_conn_1“.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/iscsi/connection/path -connection  
iscsi_conn_1 -index 1 delete
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection  
  
Operation completed successfully.
```

Managen von Remotespeichersystemen

Konfigurieren Sie Remotespeichersysteme, die sich mit dem System verbinden, an dem Sie angemeldet sind. Das System verwendet die Konfiguration, um auf das Remotesystem zuzugreifen und mit ihm zu kommunizieren. Um die Remotereplikation verwenden zu können, müssen Sie beispielsweise eine Konfiguration erstellen, in der das Remotesystem als Ziel für die Replikationssitzung angegeben ist.

Die einzelnen Konfigurationen des Remotesystems verfügen über eigene IDs.

In der folgenden Tabelle sind die Attribute für die Remotespeichersysteme aufgeführt.

Tabelle 77. Attribute für Remotesysteme

Attribut	Beschreibung
ID	Die ID des Remotesystems.
Name	Der Name des Remotesystems.
Address	Netzwerkname oder Management-IP-Adresse des Remotesystems.
Alternate management address	Eine alternative Management-IP-Adresse des Remotesystems.
Operational status	Betriebsstatus der Sitzung. Der Code des Betriebsstatus wird in Klammern angegeben. <ul style="list-style-type: none">● Unknown (0x0)● OK (0x2)● Lost Communication (0xD)● Update Needed (0x8406)● Updating (0x8407)● Failed to Validate (0x840C)● Lost sync Communication (0x840D)

Tabelle 77. Attribute für Remotesysteme (fortgesetzt)

Attribut	Beschreibung
Model	Modellnummer des Remotesystems.
Serial number	Seriennummer des Remotesystems
Health state	<p>Der Integritätsstatus der Speicherressource. Der Integritätsstatuscode wird in Klammern angezeigt. Folgende Werte sind möglich:</p> <ul style="list-style-type: none"> ● <code>OK (5)</code>: Die Ressource funktioniert normal. ● <code>Degraded/Warning (10)</code>: Funktioniert, aber es ist mindestens eines der folgenden Probleme aufgetreten: <ul style="list-style-type: none"> ○ Mindestens ein Speicherpool funktioniert nur eingeschränkt. ○ Die Replikationssitzung ist heruntergestuft. ○ Die Replikationssitzung ist fehlgeschlagen. ○ Die Kapazitätshöchstgrenze ist nahezu erreicht. Zur Vermeidung von Datenverlusten müssen Sie die Größe des primären Speichers erhöhen oder zusätzliche Ressourcen für die Speicherung der Daten anlegen. ● <code>Minor failure (15)</code>: Es ist mindestens eines der folgenden Ereignisse eingetreten: <ul style="list-style-type: none"> ○ Mindestens ein Speicherpool ist ausgefallen. ○ Der zugehörige iSCSI-Node ist ausgefallen. ● <code>Major (20)</code>: Es ist mindestens eines der folgenden Ereignisse eingetreten: <ul style="list-style-type: none"> ○ Die Ressource ist nicht verfügbar. ○ Mindestens einer der zugehörigen Speicherpools ist ausgefallen. ● <code>Critical failure (25)</code>: Es ist mindestens eines der folgenden Ereignisse eingetreten: <ul style="list-style-type: none"> ○ Mindestens ein Speicherpool ist nicht verfügbar. ○ Die Ressource ist nicht verfügbar. ○ Die volle Kapazität der Ressource ist erreicht. Zur Vermeidung von Datenverlusten müssen Sie die Größe des primären Speichers erhöhen oder zusätzliche Ressourcen für die Speicherung der Daten anlegen. ● <code>Non-recoverable error (30)</code>: Es ist mindestens eines der folgenden Ereignisse eingetreten: <ul style="list-style-type: none"> ○ Die Ressource ist nicht verfügbar. ○ Mindestens einer der zugehörigen Speicherpools ist nicht verfügbar.
Health details	Zusätzliche Integritätsinformationen.
Source user name	Für Speichersysteme, die in einer Replikationssitzung als Quelle fungieren, der Benutzername, der für den Zugriff auf das System verwendet wird.
Source user password	Für Speichersysteme, die in einer Replikationssitzung als Quelle fungieren, das Benutzerpasswort, das für den Zugriff auf das System verwendet wird.
Local interfaces	Die Liste der für die Erstellung einer Verbindung zwischen zwei Systemen verwendeten Kennungen der lokalen Schnittstellen.
Remote interfaces	Die Liste der für die Erstellung einer Verbindung zwischen zwei Systemen verwendeten Kennungen der Remoteschnittstellen.
Destination user name	Für Speichersysteme, die in einer Replikationssitzung als Ziel fungieren, der Benutzername, der für den Zugriff auf das System verwendet wird.
Destination user password	Bei Speichersystemen, die in einer Replikationssitzung als Ziel fungieren, das Benutzerpasswort, das für den Zugriff auf das System verwendet wird.
Connection type	<p>Der Typ der Verbindung zum Remotesystem. Gültige Werte:</p> <ul style="list-style-type: none"> ● <code>sync</code> ● <code>async</code> ● <code>both</code>
Synchronous FC ports	<p>Die für die synchrone Replikation aktivierten Fibre Channel-Ports</p> <p> ANMERKUNG: Bei einem lokalen-System (RS_0) wird dieses Feld nur dann leer angezeigt, wenn es keine FC-Ports gibt. Für Remotesysteme ist es leer, wenn der Verbindungstyp asynchron ist.</p>

Tabelle 77. Attribute für Remotesysteme (fortgesetzt)

Attribut	Beschreibung
Bandwidth schedules	Die Bandbreiten-Zeitpläne für asynchrone Replikationssitzungen mit Quellrolle, die über eine Datenübertragung aufgrund von RPO oder manueller Synchronisation auf diesem Remote-System verfügen. ANMERKUNG: Dieses Attribut wird nur für asynchrone oder beide Verbindungstypen verwendet. Wenn nicht konfiguriert, wird „nicht konfiguriert“ angezeigt. Für Synchronisationsverbindungstyp wird „-“ angezeigt.
Current bandwidth	Aktuelle Bandbreite berechnet anhand der konfigurierten Bandbreiten-Zeitplänen und der Zeitzone des Zeitplans für asynchrone Replikationen auf diesem Remote-System. ANMERKUNG: Dieses Attribut wird nur für asynchrone oder beide Verbindungstypen verwendet. Wenn keine Zeitpläne für die Bandbreite konfiguriert sind, wird „nutzt verfügbare Bandbreite“ angezeigt. Für Synchronisationsverbindungstyp wird „-“ angezeigt.

Erstellen von Konfigurationen für Remotesysteme

Konfiguriert ein Remotesystem, auf das das lokale System zugreift.

ANMERKUNG: Bei VNX-Quellsystemen mit zwei Control Stations muss das Stammverzeichnis des Sysadmin-Benutzers, das zum Konfigurieren der Importverbindung verwendet wird, auf der primären Control Station von VNX vorhanden sein.

Format

```
/remote/sys create -addr <value> [-type VNX] -srcUsername <value> {-srcPassword <value> | -srcPasswordSecure} -dstUsername <value> {-dstPassword <value> | -dstPasswordSecure} [-connectionType {sync | async | both}] [ -bandwidthSchedules <value> ]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-addr	Geben Sie den Netzwerknamen oder die IP-Adresse des Remotesystems ein.
-type	Geben Sie den Typ des Remotesystems ein. Gültige Werte: <ul style="list-style-type: none"> VNX
-srcUsername	Geben Sie bei Systemen, die in einer Replikation als Quelle fungieren, den Benutzernamen ein, der für den Zugriff auf das System verwendet wird.
-srcPassword	Geben Sie bei Systemen, die in einer Replikation als Quelle fungieren, das Benutzerpasswort ein, das für den Zugriff auf das System verwendet wird.
-srcPasswordSecure	Geben Sie das Passwort im sicheren Modus an. Nachdem Sie den Befehl mit diesem Qualifizierer ausgeführt haben, werden Sie aufgefordert, das Passwort separat einzugeben.
-dstUsername	Bei Systemen, die in einer Replikationssitzung als Ziel fungieren, oder VNX-Systemen in einer Importsitzung geben Sie den Benutzernamen an, der für den Zugriff auf das System verwendet wird.
-dstPassword	Bei Systemen, die in einer Replikationssitzung als Ziel fungieren, oder VNX-Systemen in einer Importsitzung geben Sie das Benutzerpasswort an, das für den Zugriff auf das System verwendet wird.
-dstPasswordSecure	Geben Sie das Passwort im sicheren Modus an. Nachdem Sie den Befehl mit diesem Qualifizierer ausgeführt haben, werden Sie aufgefordert, das Passwort separat einzugeben.
-connectionType	Geben Sie diesen Qualifizierer an, um die Art der Replikationsverbindung anzuzeigen. Gültige Werte: <ul style="list-style-type: none"> async sync both

Qualifizierer	Beschreibung
-bandwidthSchedules	(<i>async</i> oder <i>both</i> nur Verbindungstypen) Geben Sie einen Zeitplan für die Bandbreiteneinschränkung an. Geben Sie Folgendes ein, um den Zeitplan festzulegen [{ Sun Mon Tue Wed Thu Fri Sat }] [HH-HH] [/<bandwidth>], wobei Folgendes gilt: <ul style="list-style-type: none"> • Sun Mon Tue Wed Thu Fri Sat: Wochentage, an denen der Zeitplan ausgeführt werden soll • HH-HH: Start- und Endzeit für den Zeitplan • /<bandwidth>: Wert, an dem die Bandbreite eingeschränkt werden soll, in KBps

Beispiel

Mit dem folgenden Befehl wird eine Konfiguration für ein Remotesystem mit den folgenden Einstellungen erstellt:

- Netzwerkadresse: 10.60.10.10.
- Enthält Anmeldedaten für den Fall, dass das System als Ziel oder Quelle genutzt wird
- Begrenzt die Bandbreite auf 2.000 KB/s von 7:00 Uhr bis 18:00 Uhr Montag bis Freitag. Andernfalls ist die Bandbreite auf 8.000 KB/s beschränkt.

Das konfigurierte Remotesystem erhält die ID RS_1:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/sys create -addr 10.60.10.10
-srcUsername LocalAdmin -srcPassword LocalAdminPassword -dstUsername RemAdmin -dstPassword
RemAdminPassword -connectionType async -bandwidthSchedules MonTueWedThuFri7-18/2000,/8000
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = RS_1
Operation completed successfully.
```

Prüfen der Einstellungen für Remotespeichersysteme

Prüfen Sie die Konfigurationseinstellungen für ein Remotesystem, damit die Quell-Speicherressource eine Verbindung zur Remote-Speicherressource herstellen kann.

Format

```
/remote/sys -id <value> verify
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID einer Konfiguration für ein Remotesystem ein, um die Einstellungen zu prüfen.

Beispiel

Mit dem folgenden Befehl wird die Konfiguration des Remotesystems RS_1 geprüft:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/sys -id RS_1 verify
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
Operation completed successfully.
```

Anzeigen von Einstellungen für Remotespeichersysteme

Zeigen Sie die Konfiguration eines Remotesystems auf dem lokalen System an. Sie können nach der Konfigurations-ID des Remotesystems filtern.

 **ANMERKUNG:** Aktionsbefehl „show“ erläutert, wie das Ausgabeformat geändert wird.

Format

```
/remote/sys [-id <value>] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID einer Konfiguration für ein Remotesystem ein.

Beispiel

Mit dem folgenden Befehl werden sämtliche Konfigurationen für Remote-Speichersysteme aufgeführt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/sys show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:  ID                = RS_0
    Name              = FNM00151702099
    Address           = 10.245.252.229
    Model             = Unity 300 (Local System)
    Serial number     = FNM00151702099
    Connection type   = async
    Source interfaces = N/A
    Local interfaces  = N/A
    Remote interfaces = N/A
    Operational status = OK (0x2)
    Health state      = OK (5)
    Health details    = "Communication with the replication host is established. No
action is required."
    Synchronous FC ports = spa_fc4, spb_fc4
    Bandwidth schedules = MonTueWedThuFri7-18/2000,/8000
    Current bandwidth   = 8000

2:  ID                = RS_1
    Name              = FNM00151702100
    Address           = 10.244.205.127
    Model             = Unity 300
    Serial number     = FNM00151702100
    Connection type   = sync
    Source interfaces = 10.245.252.231, 10.245.252.232
    Local interfaces  = 10.245.252.231, 10.245.252.232
    Remote interfaces = 10.244.205.131, 10.244.205.132
    Operational status = OK (0x2)
    Health state      = OK (5)
    Health details    = "Communication with the replication host is established. No
action is required."
    Synchronous FC ports = spa_iom_0_fc0, spb_iom_0_fc0
    Bandwidth schedules = N/A
    Current bandwidth   = N/A
```

Ändern der Einstellungen für Remotespeichersysteme

Ändert die Konfigurationseinstellungen für ein Remotesystem.

i ANMERKUNG: Wenn eine Replikationsverbindung bereits vorhanden ist und Sie einen anderen Modus für die Dateireplikation hinzufügen möchten, müssen Sie keine neue Verbindung erstellen. Ändern Sie den Modus der vorhandenen Replikationsverbindung in „Beide“. Stellen Sie außerdem sicher, dass Sie die entsprechenden Schnittstellenarten so konfigurieren, dass die asynchrone Replikation (eth2, eth3) und die synchrone Replikation (Managementport für die synchrone Replikation) unterstützt werden.

Format

```
/remote/sys -id <value> set [-addr <value>] [-dstUsername <value> {-dstPassword <value> | -dstPasswordSecure}] [-connectionType {sync | async | both}] [-bandwidthSchedules <value>]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID der zu ändernden Konfiguration für das Remotesystem ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-addr	Geben Sie den Netzwerknamen bzw. die Management-IP-Adresse des Remotesystems ein.
-dstUsername	Geben Sie den Benutzernamen für den Zugriff auf das Remotesystem ein.
-dstPassword	Geben Sie das Benutzerpasswort für den Zugriff auf das Remotesystem ein.
-dstPasswordSecure	Geben Sie das Passwort im sicheren Modus an. Der Benutzer wird aufgefordert, das Passwort anzugeben.
-connectionType	Geben Sie diesen Qualifizierer an, um die Art der Replikationsverbindung anzuzeigen. Gültige Werte: <ul style="list-style-type: none">• async• sync• both
-bandwidthSchedules	(async oder both nur Verbindungstypen) Geben Sie einen Zeitplan für die Bandbreiteneinschränkung an. Geben Sie Folgendes ein, um den Zeitplan festzulegen [{Sun Mon Tue Wed Thu Fri Sat}] [HH-HH] [/<bandwidth>], wobei Folgendes gilt: <ul style="list-style-type: none">• Sun Mon Tue Wed Thu Fri Sat: Wochentage, an denen der Zeitplan ausgeführt werden soll• HH-HH: Start- und Endzeit für den Zeitplan• /<bandwidth>: Wert, an dem die Bandbreite eingeschränkt werden soll, in KBps Lassen Sie das Feld leer, um einen vorhandenen Bandbreitenzeitplan zu löschen.

Beispiel

Mit dem folgenden Befehl werden der Name, die IP-Adresse und die Anmeldedaten für die Konfiguration des Remotesystems RS_1 geändert:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/sys -id RS_1 set -addr "10.64.74.2" -dstUsername Local/joe -dstPassword Password456!
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = RS_1
```

```
Operation completed successfully.
```

Löschen von Konfigurationen für Remotesysteme

Löscht die Konfiguration für ein Remotesystem.

ANMERKUNG: Achten Sie vor dem Löschen der Konfiguration für ein Remotesystem darauf, dass sämtliche I/O-Vorgänge im System, wie aktive Replikationssitzungen, abgeschlossen sind, da sonst Datenverluste auftreten können.

Format

```
/remote/sys -id <value> delete
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID der zu löschenden Konfiguration für das Remotesystem ein.

Beispiel

Mit dem folgenden Befehl wird die Konfiguration des Remotesystems RS_1 gelöscht:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/sys -id RS_1 delete
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection
```

```
Operation completed successfully.
```

Ungeplantes Failover auf Rack-Ebene von Replikationssitzungen

Führen Sie ein Failover aller synchronen Replikationssitzungen eines NAS-Servers vom Remotesystem zum lokalen System (ungeplantes Failover) aus. Dieser Vorgang ist auch automatisch ein Failover der Replikationssitzungen von Dateisystemen, die auf den betroffenen NAS-Servern erstellt wurden.

Format

```
/remote/sys -id <value> failover [-force]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des Remotesystems ein, von dem aus das Failover der synchronen Replikationssitzungen des NAS-Servers durchgeführt werden soll.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-force	Gibt an, ob die Überprüfung der Netzwerkverbindung zum Remotesystem übersprungen werden soll. Erforderlich, wenn die Netzwerkverbindung fehlerfrei ist. Keine Werte sind zulässig.

Beispiel

Der folgende Befehl führt eine ungeplante Failover-Replikation auf Rack-Ebene für ein Unity-System aus:

```
uemcli /remote/sys -id RS_1 failover
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection
```

```
ID = RS_1  
Operation completed successfully.
```

ANMERKUNG: Nach einem ungeplanten Failover müssen die NAS-Server und Dateisysteme auf dem ursprünglichen Quellsystem entsprechend dem neuen Status aktualisiert werden. Bei einer großen Anzahl von NAS-Servern und Dateisystemen kann diese Änderung einige Minuten dauern. Während dieser Zeit funktionieren die Fortsetzungs- und Failback-Vorgänge der synchronen Replikationssitzungen nicht. Es wird empfohlen, alle Aktualisierungen abzuwarten, bevor Sie einen Fortsetzungs- oder Failback-Vorgang durchführen. Es gibt keine Auswirkungen auf den Datenzugriff während dieser Aktualisierung.

Anhalten von Replikationssitzungen

Halten Sie die Replikationssitzungen an, die vom lokalen System auf das ausgewählte Remotesystem und vom ausgewählten Remotesystem auf das lokale System repliziert werden.

Format

```
/remote/sys -id <value> pause [-async] [-sessionType {sync | async | both}]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Identifiziert das Remotesystem.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Ausführen einer Aktion im asynchronen Modus
-sessionType	Gibt den Typ der Replikationssitzungen an, die angehalten werden sollen. Wenn diese nicht angegeben sind, wird standardmäßig der Verbindungstyp des Remotesystems verwendet. Folgende Werte sind gültig (keine Unterscheidung zwischen Groß- und Kleinschreibung): <ul style="list-style-type: none">• sync• async• both

Beispiel

Mit dem folgenden Befehl wird eine angehaltene Replikationssitzung für ein Unity-System ausgeführt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/sys -id RS_1 pause -sessionType sync
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = RS_1
Operation completed successfully.
```

Fortsetzen von Replikationssitzungen

Setzen Sie die Replikationssitzungen fort, die vom lokalen System auf das ausgewählte Remotesystem und vom ausgewählten Remotesystem auf das lokale System repliziert werden. Für jede asynchrone Replikationssitzung und dateisynchrone Sitzung wird die Option `allowFullCopy` intern verwendet. Wenn weitere Fortsetzungsoptionen erforderlich sind, setzen Sie stattdessen die einzelne Replikationssitzung fort.

Format

```
/remote/sys -id <value> resume [-async] [-sessionType {sync | async | both}]
```

Objektqualifizierer

Qualifizierer	Beschreibung
<code>-id</code>	Identifiziert das Remotesystem.

Aktionsqualifizierer

Qualifizierer	Beschreibung
<code>-async</code>	Ausführen einer Aktion im asynchronen Modus
<code>-sessionType</code>	Gibt den Typ der fortzusetzenden Replikationssitzungen an. Wenn diese nicht angegeben sind, wird standardmäßig der Verbindungstyp des Remotesystems verwendet. Folgende Werte sind gültig (keine Unterscheidung zwischen Groß- und Kleinschreibung): <ul style="list-style-type: none">• <code>sync</code>• <code>async</code>• <code>both</code>

Beispiel

Mit dem folgenden Befehl wird eine fortgesetzte Replikationssitzung für ein Unity-System ausgeführt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/sys -id RS_1 resume -sessionType async
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = RS_1
Operation completed successfully.
```

Managen von VMware vCenter

Managen Sie VMware vCenter-Server.

In der folgenden Tabelle sind die Attribute für VMware vCenter aufgeführt.

Tabelle 78. Attribute für VMware vCenter

Attribut	Beschreibung
ID	ID des VMware Virtual Center
Address	Domainname oder IP-Adresse von VMware vCenter
User name	Name des Administratorkontos in VMware vCenter
Password	Passwort des Administratorkontos in VMware vCenter
Description	Beschreibung von VMware vCenter
VASA provider state	Gibt an, ob das System als ein VASA-Anbieter in vCenter registriert ist. Folgende Werte können verwendet werden: <ul style="list-style-type: none"> Registered Not registered Not supported <i>(i)</i> ANMERKUNG: Automatische VASA-Registrierung wird auf vSphere-Versionen vor 6.0 nicht unterstützt. Das Speichersystem kann als ein VASA-Anbieter mit jeweils nur einem vCenter registriert werden.
Local username	Der Benutzername des lokalen Kontos, das von vSphere verwendet wird, um das System als einen VASA-Anbieter zu registrieren. <i>(i)</i> ANMERKUNG: Es wird empfohlen, mit dem Befehl <code>/user/account</code> einen neuen Benutzer zu erstellen und die Rolle auf <code>vmadmin</code> festzulegen.
Local password	Das Passwort des lokalen Kontos, das von vSphere verwendet wird, um das System als einen VASA-Anbieter zu registrieren.

Erstellen von VMware vCenter

Fügt die vCenter-Anmeldedaten hinzu und erkennt jeden ESXi-Host, der von diesem vCenter gemanagt wird. Die vCenter-Anmeldedaten sind im Speichersystem gespeichert. Um diesen Befehl auszuführen, muss der Benutzer über ein Konto auf dem Speichersystem verfügen.

Format

```
/virt/vmw/vc create -addr <value> -username <value> {-passwd <value> | -passwdSecure} [-descr <value>] [-registerVasaProvider {yes -localUsername <value> {-localPasswd <value> | -localPasswdSecure} | no}]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-addr	Domainname oder IP-Adresse des VMware vCenter.
-username	Geben Sie den Benutzernamen des VMware-Administrators für den Zugriff auf VMware vCenter an.
-passwd	Geben Sie das Passwort des VMware-Administrators für den Zugriff auf VMware vCenter an.

Qualifizierer	Beschreibung
-passwdSecure	Geben Sie das Passwort im sicheren Modus an. Der Benutzer wird aufgefordert, das Passwort einzugeben.
-descr	Geben Sie die Beschreibung des VMware vCenter-Servers an.
-registerVasaProvider	Geben Sie dies an, um das System als einen VASA-Anbieter mit diesem vCenter-Server zu registrieren. Gültige Werte: <ul style="list-style-type: none"> • yes • no
-localUsername	Geben Sie den Benutzernamen des Systemkontos an, das von vCenter verwendet wird, um das System als einen VASA-Anbieter zu registrieren.  ANMERKUNG: Es wird empfohlen, mit dem Befehl <code>/user/account</code> einen neuen Benutzer zu erstellen und die Rolle auf <code>vmadmin</code> festzulegen. Das Speichersystem kann als ein VASA-Anbieter mit jeweils nur einem vCenter registriert werden.
-localPasswd	Geben Sie das Passwort des Systemkontos an, das von vCenter verwendet wird, um das System als einen VASA-Anbieter zu registrieren.
-localPasswdSecure	Geben Sie das VASA-Passwort im sicheren Modus an, wodurch der Benutzer das Passwort eingeben muss, wenn er dazu aufgefordert wird.

Beispiel 1

Mit dem folgenden Befehl werden Anmeldedaten für Virtual Center hinzugefügt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /virt/vmw/vc create -addr 10.11.11.111
-username administrator@vsphere.local -passwd xxx -descr "Add vCenter"
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = VC_1
Operation completed successfully
```

Beispiel 2

Der folgende Befehl fügt ein vCenter hinzu und registriert das Speichersystem als einen VASA-Anbieter.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /virt/vmw/vc create -address 10.11.11.111 -
username root -passwd xxx -descr "Add virtual center" -registerVasaProvider yes -localUsername
admin -localPasswd Password321
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = VC_1
Operation completed successfully
```

Festlegen der Anmeldedaten oder der Beschreibung eines vorhandenen vCenter-Servers

Ändert die Anmeldedaten oder die Beschreibung des vorhandenen vCenter-Servers. Um diesen Befehl auszuführen, muss der Benutzer über ein Konto auf dem Speichersystem verfügen.

Format

```
/virt/vmw/vc -id <value> set [-addr <value>] [-username <value> {-passwd <value> |  
-passwdSecure} ] [-descr <value>]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Identifiziert den VMware vCenter-Server.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-addr	Gibt die neue IP-Adresse oder den neuen Domainnamen des VMware vCenter-Servers an.
-username	Gibt den Benutzernamen des VMware-Administrators an.
-passwd	Gibt das Passwort des VMware-Administrators an.
-passwdSecure	Gibt das Passwort im sicheren Modus an – der Benutzer wird aufgefordert, das Passwort einzugeben.
-descr	Gibt die neue Beschreibung des VMware vCenter-Servers an.

Beispiel

Mit dem folgenden Befehl wird die neue Beschreibung des VMware vCenter-Servers angegeben:

```
uemcli /virt/vmw/vc -id VC_1 set -descr "This vCenter manages 2 ESXi hosts"
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection
```

```
ID = VC_1  
Operation completed successfully.
```

Löschen eines vorhandenen vCenter-Servers

Entfernt einen vorhandenen VMware vCenter-Server und seine zugehörigen ESXi-Hosts.

 **ANMERKUNG:** Wenn das Unity-System als VASA-Anbieter in vCenter registriert ist und Sie das vCenter aus Unity löschen, wird die Registrierung des Unity-Systems als VASA-Anbieter von vCenter aufgehoben.

Format

```
/virt/vmw/vc -id <value> delete
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Identifiziert den VMware vCenter-Server.

Beispiel

Im folgenden Beispiel wird ein vorhandener vCenter-Server und alle zugehörigen ESXi-Hosts gelöscht.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /virt/vmw/vc -id VC_1 delete
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully
```

Anzeigen aller vCenter-Server

Zeigt eine Liste der konfigurierten VMware vCenter-Server an.

Format

```
/virt/vmw/vc [-id <value>] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Identifiziert den VMware vCenter-Server.

Beispiel

Im folgenden Beispiel wird eine Liste aller vCenter-Server angezeigt.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /virt/vmw/vc show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      ID           = VC_1
      Address        = 10.1.1.1
      Description    = This vCenter manages 2 ESXi hosts
      VASA provider state = yes
```

Aktualisieren aller vCenter-Server

Lesen Sie die Details aller konfigurierten VMware vCenter-Server neu ein.

Format

```
/virt/vmw/vc refresh [-scanHardware]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des vCenter an. Wenn nicht angegeben, werden alle angeschlossenen vCenter aktualisiert.
-scanHardware	Hiermit können Sie Hardwareänderungen neu einlesen (dies nimmt zusätzliche Zeit in Anspruch).

Beispiel

Im folgenden Beispiel werden alle vCenters neu eingelesen.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /virt/vmw/vc refresh -scanHardware
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Managen von ESXi-Hosts

Managen Sie VMware ESXi-Hosts.

In der folgenden Tabelle sind die Attribute für ESXi-Hosts aufgeführt.

Tabelle 79. ESXi-Host-Attribute

Attribut	Beschreibung
ID	ID des ESXi-Hosts
Name	Name des ESXi-Hosts
Address	Domainname oder IP-Adresse des ESXi-Hosts
Virtual center	Kennung des VMware vCenter-Servers, der den ESXi-Host managt
Username	Name des Benutzerkontos auf dem ESXi-Host
Password	Passwort des Benutzerkontos auf dem ESXi-Host
Description	Beschreibung des ESXi-Hosts
NFSv4 supported	Gibt an, ob das NFSv4-Protokoll für den Host unterstützt wird. Gültige Werte: <ul style="list-style-type: none">• yes• no
NFS username	Zeigt die Informationen zur NFS-Benutzerauthentifizierung an, die für den ESXi-Host konfiguriert sind. Derselbe Benutzername sollte auf dem VMware NFS-Datenspeicher konfiguriert werden, um sicheren NFS-Zugriff mit Kerberos für diesen Datenspeicher zu ermöglichen.

Erstellen eines ESXi-Hosts

Fügt einen VMware ESXi-Host hinzu.

Format

```
/virt/vmw/esx create -addr <value> { -vc <value> | -username <value> {-passwd <value> | -passwdSecure} } [ -descr <value> ] [ -resolveConflicts { yes | no } ]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-addr	Domainname oder IP-Adresse des ESXi-Hosts
-vc	Identifiziert den VMware vCenter-Server.
-username	Gibt den Benutzernamen für den Zugriff auf den VMware ESXi-Host an.
-passwd	Gibt das Passwort für den Zugriff auf den VMware ESXi-Host an.
-passwdSecure	Gibt das Passwort im sicheren Modus an – der Benutzer wird aufgefordert, das Passwort einzugeben.
-descr	Gibt die Beschreibung des VMware ESXi-Hosts an.
-resolveConflicts	Gibt die Option zum interaktiven Lösen von IP-Adressen- oder Initiator Konflikten an. Gültige Werte sind Ja oder Nein (Standard).

Beispiel 1

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /virt/vmw/esx create -addr 10.1.1.1 -username root -passwd xxx -descr "My ESXi host"
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = ESX_1
Operation completed successfully
```

Beispiel 2

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /virt/vmw/esx create -addr 10.1.1.1 -vc VMwareVC_12 -resolveConflicts yes
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

The ESX host to be created has IP addresses and/or Initiators already present in an existing host.

```
The ID of the existing host is: Host_12
The IP addresses in conflict are: 10.14.12.219, 10.14.12.220
The Initiators in conflicts are: iqn.1998-01.com.vmware:test1-1,
iqn.1998-01.com.vmware:test1-2
```

WARNING, the existing host has IP addresses and/or Initiators not found in the ESX host to be created. If you continue with the ESX host creation, those IP addresses and/or Initiators will be removed and can no longer be used for storage access.

```
The IP address not in the ESX host are: 10.14.12.217, 10.14.12.218
The Initiators not in the ESX host are: iqn.1998-01.com.vmware:test1-3
```

```
Do you want to convert the existing host to the ESX host?
Yes / no:yes
```

```
ID = ESX_1
Operation completed successfully
```

Ändern von Anmeldedaten für ESXi-Host

Ändert die Anmeldedaten bzw. die Beschreibung für den ESXi-Host. Um diesen Befehl auszuführen, muss der Benutzer über ein Konto auf dem Speichersystem verfügen.

Format

```
/virt/vmw/esx -id <value> set [ -descr <value> ] [ -username <value> { -passwd <value> | -passwdSecure } ] [ -addr <value> ]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Identifiziert den VMware ESXi-Host.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-descr	Gibt den Kommentar oder die Beschreibung an.
-username	Gibt den Benutzernamen für den Zugriff auf den VMware ESXi-Host an.
-passwd	Gibt das Passwort für den Zugriff auf den VMware ESXi-Host an.
-passwdSecure	Gibt das neue Passwort im sicheren Modus an – der Benutzer wird aufgefordert, das Passwort einzugeben.
-addr	Gibt den Domainnamen oder die IP-Adresse des ESXi-Hosts an, damit Unisphere den ESXi-Host direkt kontaktieren kann.  ANMERKUNG: Dies gilt nur für eigenständige ESXi-Hosts.

Beispiel

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /virt/vmw/esx -id ESX_1 set -descr "Changing ESXi host description"
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection
```

```
ID = ESX_1  
Operation completed successfully.
```

Löschen der ESXi-Hostanmeldedaten

Löscht die ESXi-Hostanmeldedaten. Dadurch wird auch der Zugriff des angegebenen Hosts auf alle VMware-Datenspeicher oder Protokollendpunkte entfernt, die ihm zugeordnet sind.

Format

```
/virt/vmw/esx -id <value> delete
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Identifiziert den ESXi-Host.

Beispiel

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /virt/vmw/esx -id ESX_1 delete
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Anzeigen aller vorhandenen ESXi-Hosts

Zeigt eine Liste aller konfigurierten VMware ESXi-Hosts an.

Format

```
/virt/vmw/esx [{"-id <value> | -vc <value>}] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Identifiziert den VMware ESXi-Host.
-vc	Identifiziert den VMware vCenter-Server.

Beispiel

Das folgende Beispiel zeigt, wie alle ESXi-Hosts auf dem mit dem System verbundenen vCenter angezeigt werden können.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /virt/vmw/esx -vc VC_1 show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      ID           = ESX_1
      Name          = nlpC12240.aa.bb.com
      vCenter       = VC_1
      Address       = 10.10.10.100
      Description   =
      NFSv4 supported = yes
      NFS username  = root

2:      ID           = ESX_2
      Name          = nlpC12241.xx.yy.com
      vCenter       = VC_1
      Address       = 10.10.10.101
      NFSv4 supported = no
      NFS username  =
```

Erkennen aller ESXi-Hosts

Listet alle VMware ESXi-Hosts auf dem angegebenen VMware vCenter-Server auf.

Format

```
/virt/vmw/esx discover { -vc <value> | -vcAddr <value> -username <value> {-passwd <value> |  
-passwdSecure} } [ -createAll ]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-vc	Identifiziert den vorhandenen VMware vCenter-Server.
-vcAddr	IP-Adresse oder Domainname von VMware vCenter.
-username	Gibt den Namen von VMware vCenter an.
-passwd	Gibt das Passwort von VMware vCenter an.
-passwdSecure	Gibt das Passwort im sicheren Modus an – der Benutzer wird aufgefordert, das Passwort einzugeben.
-createAll	Fügt alle erkannten ESXi-Hosts automatisch hinzu.

Beispiel

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /virt/vmw/esx discover -vc VC_1
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection  
  
1:   Name   = nlpc12240.us.dg.com  
2:   Name   = nlpc12241.us.dg.com  
  
Operation completed successfully
```

Aktualisieren eines ESXi-Hosts

Liest die Details eines VMware ESXi-Hosts neu ein.

Format

```
/virt/vmw/esx [-id <value>] refresh [-scanHardware]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Identifiziert den ESXi-Host. Wenn keine ID angegeben wird, werden alle Virtualisierungsobjekte neu eingelesen.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-scanHardware	Hiermit können Sie auch Hardwareänderungen neu einlesen (dies nimmt zusätzliche Zeit in Anspruch).

Beispiel

Mit dem folgenden Befehl wird die Hardware erneut überprüft, um zusätzliche ESXi-Hosts zu erkennen.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /virt/vmw/esx refresh -scanHardware
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
Operation completed successfully.
```

Virtuelle Maschine

Managen Sie virtuelle VMware-Maschinen.

In der folgenden Tabelle sind die Attribute für virtuelle Maschinen aufgeführt.

Tabelle 80. Attribute für virtuelle Maschinen

Attribut	Beschreibung
ID	ID der virtuellen Maschine
Name	Name der virtuellen Maschine
Description	Beschreibung der virtuellen Maschine
ESX server	ESXi-Hosts, die die virtuelle Maschine enthalten
OS	Gastbetriebssysteme
State	Energiestatus der virtuellen Maschine Gültige Werte: <ul style="list-style-type: none">• Powered on• Powered off• Suspended

Anzeigen aller vorhandenen virtuellen Maschinen

Zeigt eine Liste aller vorhandenen virtuellen Maschinen auf vorhandenen ESXi-Hosts auf dem Unity-System an.

Format

```
/virt/vmw/vm [{"-id <value> | -esx <value>}] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Identifiziert die virtuelle Maschine.
-esx	Identifiziert den ESXi-Host.

Beispiel

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /virt/vmw/vm -esx ESX_1 show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
```

HTTPS connection

```
1:   ID       = VM_1
     Name    = WinVM1
     vCenter = VC_1
     ESX server = ESX_1
     State   = Powered On

2:   ID       = VM_2
     Name    = LinVM3
     vCenter = VC_1
     ESX server = ESX_1
     State   = Suspended
```

VM-Festplatte

Managen Sie die Festplatteneigenschaften für virtuelle VMware-Maschinen, die auf dem Unity-System gespeichert sind.

In der folgenden Tabelle sind die Attribute für VM-Festplatten aufgeführt.

Tabelle 81. Attribute für VM-Festplatten

Attribut	Beschreibung
Name	Name der Festplatte
Type	Art der VM-Festplatte
Capacity	Kapazität der VM-Festplatte
Datastore	Zugeordneter Datastore

Anzeigen aller Festplatten

Zeigt die Festplatteneigenschaften für eine angegebene virtuelle Maschine an, die auf dem Unity-System gespeichert ist.

Format

```
/virt/vmw/vmdevice -vm <value> show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-vmId	Identifiziert die virtuelle Maschine.

Beispiel

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /virt/vmw/vmdevice -vm VM_1 show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:   Name      = Hard disk 1
     Type      = VM Hard Disk
     Capacity = 107374182400 (100GB)
     Datastore = Storage1

2:   Name      = Hard disk 2
     Type      = VM Hard Disk
```

```
Capacity = 107374182400 (100GB)
Datastore = Storage1
```

Managen von Hardwarekomponenten

Themen:

- Managen des Speicherprozessors (SP)
- Managen der Festplatte
- Managen des Akkus (nur physische Bereitstellungen)
- Managen des Netzteils (nur physische Bereitstellungen)
- Managen der Link Control Card (LCC) (nur physische Bereitstellungen)
- Managen von SSD (nur physische Bereitstellungen)
- Managen des Disk Array Enclosure (DAE)
- Managen des Disk Processor Enclosure (DPE)
- Managen des Speichermoduls (nur physische Bereitstellungen)
- Managen der System Status Card (nur physische Bereitstellungen)
- Managen von Lüftermodulen (nur physische Bereitstellungen)
- Managen von I/O-Modulen, integrierten Modulen und Karten mit 4 Ports (nur physische Bereitstellungen)

Managen des Speicherprozessors (SP)

In der folgenden Tabelle sind die Werte des Integritätsstatus für den Speicherprozessor (SP) im Normalmodus aufgeführt.

Tabelle 82. Werte des Integritätsstatus des Speicherprozessors (Normalmodus)

Code	Integritätsstatus	Ursache(n)
0	Unknown	<ul style="list-style-type: none"> • Die Integrität der Komponente kann nicht bestimmt werden.
5	OK	<ul style="list-style-type: none"> • SP funktioniert normal.
10	Degraded/Warning	<ul style="list-style-type: none"> • Der Schreibcache ist auf dem SP deaktiviert. • Der SP wird gestartet.
20	Major failure	<ul style="list-style-type: none"> • Der SP ist defekt. • Der SP fehlt. • Der SP antwortet nicht.

In der folgenden Tabelle sind die Werte des Integritätsstatus für den Speicherprozessor im Service-/Rettungsmodus aufgeführt.

Tabelle 83. Werte des Integritätsstatus des Speicherprozessors (Service-/Rettungsmodus)

Code	Integritätsstatus	Ursache(n)
0	Unknown	<ul style="list-style-type: none"> • Die Integrität der Komponente kann nicht bestimmt werden.
10	Degraded/Warning	<ul style="list-style-type: none"> • Ein Benutzer hat den SP in den Servicemodus versetzt.
20	Major failure	<ul style="list-style-type: none"> • Die Systemsoftware auf diesem SP hat ein Problem festgestellt. • Die CPU im SP ist defekt. • I/O-Modul 0 im SP ist defekt. • I/O-Modul 1 im SP ist defekt. • Die CPU und das I/O-Modul 0 im SP sind defekt. • Die CPU und das I/O-Modul 1 im SP sind defekt. • Speicher-DIMM 0 im SP ist defekt. • Speicher-DIMM 0 und 1 im SP sind defekt. • Speicher-DIMM 1 im SP ist defekt. • Speicher-DIMM 2 im SP ist defekt.

Tabelle 83. Werte des Integritätsstatus des Speicherprozessors (Service-/Rettungsmodus) (fortgesetzt)

Code	Integritätsstatus	Ursache(n)
		<ul style="list-style-type: none"> • Speicher-DIMMs im SP sind defekt. • Der SP ist defekt. • Die SSD im SP ist defekt. • Das gesamte Blade im SP ist defekt. • Die Glasfaserkabelverbindung im SP ist defekt. • Das Gehäuse im SP ist defekt. • Ein I/O-Modul im SP ist nicht korrekt konfiguriert. • Ein unerwarteter Fehler ist im SP aufgetreten. • Ein Kabel befindet sich im falschen SAS-Port auf dem SP. • Kein SAS-Port auf dem SP gefunden. • Ungültige Festplattenkonfiguration auf dem SP. • Kein I/O zwischen einem I/O-Modul im SP und einer Link Control Card in einem Disk Array Enclosure. • Ein FLARE DB-Laufwerk im Speicherprozessor ist defekt. • Bei einem der ersten 4 Laufwerke weichen einige Typen ab. • Eines der ersten 4 Laufwerke weist eine ungültige Blockgröße auf. • Bei einem der ersten 4 Laufwerke weicht die Größe ab. • Bei DPE-Wiederaufnahme fehlt eine EMC Seriennummer.

Anzeigen des Speicherprozessors

Zeigen Sie die vorhandenen Speicherprozessoren (SPs) an.

Format

```
/env/sp [-id <value>] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Identifiziert den Speicherprozessor.

Beispiel 1 (nur physische Bereitstellungen)

Mit dem folgenden Befehl werden die vorhandenen SPs angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /env/sp show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:  ID           = spa
   DPE          = dpe
   Slot         = 0
   Name         = SP A
   Mode         = Normal
   Health state = OK (5)
   Health details = "The component is operating normally. No action is required."
   Model        = BC SP 57840B1 8009C1 12GB 4C
   Part number  = 110-223-000C-02
   Serial number = FCNBC130100113
   Memory size  = 25769803776 (24.0G)
```

```

2:  ID           = spb
    DPE         = dpe
    Slot        = 1
    Name        = SP B
    Mode        = Normal
    Health state = OK (5)
    Health details = "The component is operating normally. No action is required."
    Model       = BC SP 57840B1 8009C1 12GB 4C
    Part number = 110-223-000C-02
    Serial number = FCNBC130100104
    Memory size  = 25769803776 (24.0G)

```

Beispiel 2 (nur virtuelle Bereitstellungen)

Mit dem folgenden Befehl werden vorhandene SPs für ein virtuelles System angezeigt.

```
uemcli -d 10.0.0.2 -u Local/joe -p MyPassword456! /env/sp show -detail
```

```

Storage system address: 10.0.0.2
Storage system port: 443
HTTPS connection

1:  ID           = spa
    UUID         = 421DB2B2-6AAC-BB48-73DE-513390292444
    DPE         = dpe
    Slot        = 0
    Name        = SP A
    Mode        = Normal
    Health state = OK (5)
    Health details = "The component is operating normally. No action is required."
    Model       = VIRT SP 12GB
    Memory size  = 12884901888 (12.0G)

```

Managen der Festplatte

In der folgenden Tabelle sind die Werte des Integritätsstatus für das Laufwerk aufgeführt.

Tabelle 84. Werte des Integritätsstatus des physischen Laufwerks

Code	Integritätsstatus	Ursache(n)
0	Unknown	<ul style="list-style-type: none"> Die Integrität der Komponente kann nicht bestimmt werden.
5	OK	<ul style="list-style-type: none"> Das Laufwerk arbeitet normal. Der Laufwerkssteckplatz ist leer.
10	Degraded/Warning	<ul style="list-style-type: none"> Das Laufwerk wird erneut mit dem System synchronisiert. Das Laufwerk kann nicht verwendet werden, da das System die maximale Anzahl zulässiger Laufwerke überschritten hat.
15	Minor failure	<ul style="list-style-type: none"> Das Laufwerk wird in den falschen Steckplatz eingesetzt. Das Laufwerk wird entfernt. Das Laufwerk ist offline.
20	Major failure	<ul style="list-style-type: none"> Das Laufwerk ist defekt. Das Laufwerk wird nicht unterstützt.

Tabelle 85. Werte des Integritätsstatus des virtuellen Laufwerks

Code	Integritätsstatus	Ursache(n)
0	Unknown	<ul style="list-style-type: none"> Die Integrität der Komponente kann nicht bestimmt werden.
5	OK	<ul style="list-style-type: none"> Das virtuelle Laufwerk funktioniert normal.

Tabelle 85. Werte des Integritätsstatus des virtuellen Laufwerks (fortgesetzt)

Code	Integritätsstatus	Ursache(n)
7	OK_BUT	<ul style="list-style-type: none"> • Das virtuelle Laufwerk wurde ursprünglich für ein anderes Speichersystem konfiguriert. • Das virtuelle Laufwerk wurde ursprünglich für einen anderen Speicherpool konfiguriert.
20	Major failure	<ul style="list-style-type: none"> • Auf das virtuelle Laufwerk kann nicht zugegriffen werden. • Das virtuelle Laufwerk ist zu klein. • Das virtuelle Laufwerk ist zu groß. • Das virtuelle Laufwerk ist wegen eines System- oder I/O-Fehlers fehlgeschlagen.

Anzeigen der Festplatte

Zeigen Sie die vorhandenen Laufwerke an.

Format

```
/env/disk [{"-id <value> | -pool <value> | -fastcache | -unused}] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	ID des Laufwerks.
-pool	Zeigt die Laufwerke, die zum angegebenen Pool gehören.
-fastcache	Zeigt die in FAST Cache verwendeten Laufwerke.
-unused	Zeigt nicht verwendete Laufwerke.

Beispiel 1

Mit dem folgenden Befehl werden die grundlegenden Attribute aller Laufwerke in einer physischen Bereitstellung angezeigt.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /env/disk show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:   ID           = DISK_0
     Enclosure   = DAE_1
     Slot        = 0
     Health state = OK (5)
     User capacity = 2199023255552 (2T)
     Used by FAST Cache = no
     Pool ID      = pool_1

2:   ID           = DISK_1
     Enclosure   = DAE_1
     Slot        = 1
     Health state = OK (5)
     User capacity = 2199023255552 (2T)
     Used by FAST Cache = no
     Pool ID      = pool_1
```

Beispiel 2

Mit dem folgenden Befehl werden die Details zu sämtlichen Laufwerken in einer physischen Bereitstellung angezeigt.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /env/disk show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:   ID                = dae_1_2_disk_59
     Enclosure         = dae_1_2_
     Slot              = 59
     Bank slot         = C19
     Name              = Disk 59
     Health state      = OK (5)
     Health details    = "The component is operating normally. No action is required."
     Type              = SAS
     Tier              = performance
     Capacity          = 881132310528 (820.6G)
     Rotational speed  = 10000 rpm
     User capacity     = 797989670912 (743.1G)
     Used by FAST Cache = no
     Pool ID           = Unconfigured
     Pool              = Unconfigured
     Current speed     = 6 Gbps
     Maximum speed    = 6 Gbps
     Manufacturer      = SEAGATE
     Model             = ST990080 CLAR900
     Vendor capacity   = 966367641600 (900.0G)
     Part number       = 005049206PWR
     Serial number     = 6XS3A9CG
     Firmware revision = CS19
     WWN               = 06:00:00:00:05:00:00:00:01:00:00:00:00:00:00:03
     Days remaining to EOL = 1497
```

Beispiel 3

Mit dem folgenden Befehl werden die Details zu sämtlichen Laufwerken in einer virtuellen Einzel-SP-Bereitstellung angezeigt.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /env/disk show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:   ID                = vdisk_1
     SCSI ID          = 0:3
     Name             = Virtual Disk 1
     Health state     = OK (5)
     Health details   = "The component is operating normally. No action is required."
     Type             = virtual
     Tier             = capacity
     Capacity         = 268435456000 (250.0G)
     Rotational speed =
     User capacity    = 268435435520 (249.9G)
     Pool ID          = pool_1
     Pool             = StoragePool100
     Current speed    =
     Maximum speed    =
     Manufacturer     = VMware
     Model            = Virtual disk
     Vendor capacity  = 268435456000 (250.0G)
     WWN              = 06:00:00:00:05:00:00:00:04:00:00:00:00:00:00:03
```

Beispiel 4

Mit dem folgenden Befehl werden die Details zu sämtlichen Laufwerken in einer virtuellen Dual-SP-Bereitstellung angezeigt.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /env/disk show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      ID                = vdisk_1
       SCSI ID SPA       = 0:3
       SCSI ID SPB       = 0:4
       Name              = Virtual Disk 1
       Health state      = OK (5)
       Health details    = "The component is operating normally. No action is required."
       Type              = virtual
       Tier              = capacity
       Capacity          = 268435456000 (250.0G)
       Rotational speed  =
       User capacity     = 268435435520 (249.9G)
       Pool ID           = pool_1
       Pool              = StoragePool100
       Current speed     =
       Maximum speed     =
       Manufacturer     = VMware
       Model             = Virtual disk
       Vendor capacity   = 268435456000 (250.0G)
       WWN               = 06:00:00:00:05:00:00:00:04:00:00:00:00:00:00:03
```

Neues Einlesen von Festplatten (nur virtuelle Bereitstellungen)

Prüfen Sie das System erneut auf verfügbare virtuelle Laufwerke.

Format

```
/env/disk rescan [-async]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.

Beispiel

Mit dem folgenden Befehl wird das System erneut auf im laufenden Betrieb eingesetzte virtuelle Laufwerke gescannt.

```
uemcli -d 10.0.0.2 -u Local/joe -p MyPassword456! /env/disk rescan
```

```
Storage system address: 10.0.0.2
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Ändern der Festplatteneinstellungen (nur virtuelle Bereitstellungen)

Ändern Sie die Einstellungen einer vorhandenen Festplatte.

Format

```
/env/disk -id <value> set [-async] [-name <value>] [-tier <value>]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Festplattenkennung

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.
-name	Geben Sie den neuen Namen für die Festplatte an.
-tier	Geben Sie den neuen Tier an. Gültige Werte: <ul style="list-style-type: none">• Kapazität• Performance• extreme  ANMERKUNG: Festplatten ohne ein Tier können nicht für das Pool-Provisioning verwendet werden.

Beispiel

Mit dem folgenden Befehl wird der Name des virtuellen Laufwerks mit der Kennung „vdisk_1“ geändert.

```
uemcli -d 10.0.0.2 -u Local/joe -p MyPassword456! /env/disk -id vdisk_1 set -name "High-performance storage"
```

```
Storage system address: 10.0.0.2
Storage system port: 443
HTTPS connection
```

```
Operation completed successfully.
```

Managen des Akkus (nur physische Bereitstellungen)

In der folgenden Tabelle sind die Werte des Integritätsstatus für die Systemakkus aufgeführt.

Tabelle 86. Werte des Integritätsstatus des Akkus

Code	Integritätsstatus	Ursache
0	Unknown	<ul style="list-style-type: none">• Die Integrität der Komponente kann nicht bestimmt werden.
5	OK	<ul style="list-style-type: none">• Der Akku funktioniert normal.
10	Degraded/Warning	<ul style="list-style-type: none">• Der Akku wird aufgeladen.
20	Major failure	<ul style="list-style-type: none">• Der Akku ist defekt.• Der Akku fehlt.

Anzeigen des Akkus

Zeigen Sie eine Liste der Systemakkus an.

Format

```
/env/bat [-id <value>] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	ID des Akkus.

Beispiel

Mit dem folgenden Befehl wird eine Liste der Systemakkus angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /env/bat show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      ID          = Bat_0
       SP          = SPA_
       Slot        = 0
       Health state = OK (5)

2:      ID          = Bat_0
       SP          = SPA_
       Slot        = 1
       Health state = Degraded/Warning (10)
```

Managen des Netzteils (nur physische Bereitstellungen)

In der folgenden Tabelle sind die Werte des Integritätsstatus für die Systemnetzteile aufgeführt.

Tabelle 87. Werte des Integritätsstatus des Netzteils

Code	Integritätsstatus	Ursache
0	Unknown	<ul style="list-style-type: none">Die Integrität der Komponente kann nicht bestimmt werden.
5	OK	<ul style="list-style-type: none">Das Netzteil funktioniert normal.
20	Major failure	<ul style="list-style-type: none">Das Netzteil ist defekt.Das Netzteil wird nicht mit Strom versorgt.Das Netzteil wurde entfernt.

Anzeigen des Netzteils

Zeigen Sie eine Liste der Systemnetzteile an.

Format

```
/env/ps [-id <value>] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	ID des Netzteils.

Beispiel

Mit dem folgenden Befehl wird eine Liste der Systemnetzteile angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /env/ps show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      ID           = Pow_0
      Enclosure     = DPE
      SP            = SPA
      Slot          = 0
      Health state = OK (5)

2:      ID           = Pow_1
      Enclosure     = DPE
      SP            = SPA
      Slot          = 1
      Health state = OK(5)
```

Managen der Link Control Card (LCC) (nur physische Bereitstellungen)

In der folgenden Tabelle sind die Werte des Integritätsstatus für die Link Control Cards (LCCs) des Systems aufgeführt.

Tabelle 88. Werte des Integritätsstatus der Link Control Card

Code	Integritätsstatus	Ursache
0	Unknown	<ul style="list-style-type: none">Die Integrität der Komponente kann nicht bestimmt werden.
5	OK	<ul style="list-style-type: none">Die LCC funktioniert normal.
20	Major failure	<ul style="list-style-type: none">Die LCC ist defekt.Die LCC wurde entfernt.

Anzeigen der Link Control Card

Zeigen Sie eine Liste der LCCs an.

Format

```
/env/lcc [-id <value>] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	ID der LCC.

Beispiel

Mit dem folgenden Befehl wird eine Liste der LCCs des Systems angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /env/lcc show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
1: ID          = LCC_0
   DAE         = DAE_0
   Slot        = 0
   Health state = OK (5)

2: ID          = LCC_1
   DAE         = DAE_0
   Slot        = 1
   Health state = OK(5)
```

Managen von SSD (nur physische Bereitstellungen)

In der folgenden Tabelle sind die Werte des Integritätsstatus für die SSDs des Systems aufgeführt.

Tabelle 89. Werte des Integritätsstatus der SSDs

Code	Integritätsstatus	Ursache
0	Unknown	<ul style="list-style-type: none">Die Integrität der Komponente kann nicht bestimmt werden.
5	OK	<ul style="list-style-type: none">Die SSD funktioniert normal.
10	Degraded/Warning	<ul style="list-style-type: none">Die SSD fällt aus.
20	Major failure	<ul style="list-style-type: none">Die SSD ist defekt.Die SSD wurde entfernt.

Anzeigen der SSD

Zeigen Sie eine Liste der SSDs des Systems an.

Format

```
/env/ssd [-id <value>] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	ID der SSD.

Beispiel

Mit dem folgenden Befehl wird eine Liste der SSDs des Systems angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /env/ssd show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```

1:   ID           = spa_ssd_0
     SP           = spa
     Slot         = 0
     Name         = SP A Internal Disk 0
     Type         = SATA
     Health state = OK (5)
     Health details = "The component is operating normally. No action is required."
     Manufacturer =
     Model        = Intel DC 3500 Series SSDs M.2
     Part number  = INTEL SSDSCKHB080G4M          118000039
     Serial number = BTWM535008WA

```

Managen des Disk Array Enclosure (DAE)

In der folgenden Tabelle sind die Werte des Integritätsstatus für die Disk Array Enclosures (DAEs) des Systems aufgeführt.

Tabelle 90. Werte des Integritätsstatus des Disk Array Enclosure

Code	Integritätsstatus	Ursache
0	Unknown	<ul style="list-style-type: none"> Die Integrität der Komponente kann nicht bestimmt werden.
5	OK	<ul style="list-style-type: none"> Das DAE funktioniert normal.
7	OK_BUT	<ul style="list-style-type: none"> Das DAE passt die Kommunikationsgeschwindigkeit an.
10	Degraded/Warning	<ul style="list-style-type: none"> Die Performance des DAE wird heruntergestuft.
20	Major failure	<ul style="list-style-type: none"> Für DAE weichen Festplattenlaufwerk-Typen ab. Beim DAE ist ein Kommunikationsfehler aufgetreten. Das DAE ist defekt. Das DAE weist eine defekte LCC auf. Das DAE wurde falsch konfiguriert. Das DAE wurde falsch verkabelt. Das DAE wurde entfernt. Beim DAE ist ein Fehler bei der Stromversorgung aufgetreten. Das DAE ist mit einem defekten I/O-Modul verbunden.

Anzeigen eines Disk Array Enclosure

Zeigen Sie eine Liste der DAEs des Systems an.

Format

```
/env/dae [-id <value>] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	ID des DAE.

Beispiel

Mit dem folgenden Befehl wird eine Liste der DAEs des Systems angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /env/dae show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:  ID                = dae_0_1
    Name              = DAE_0_1
    Health state      = OK (5)
    Health details    = "The component is operating normally. No action is
required."
    Manufacturer      = USI
    Model             = 25 DRIVE 6G SAS DERRINGER DAE
    Part number       = 100-562-712
    Serial number     = US1D1102500097
    Power (Present)   = 232 watts
    Power (Rolling Average) = 231 watts
    Temperature (Present) = 84° F (29° C)
    Temperature (Rolling Average) = 84° F (29° C)
    Bus               = 0
    Enclosure number  = 1
```

Managen des Disk Processor Enclosure (DPE)

In der folgenden Tabelle sind die Werte des Integritätsstatus für die Disk Processor Enclosures (DPEs) des Systems aufgeführt.

Tabelle 91. Werte des Integritätsstatus des Disk Processor Enclosure

Code	Integritätsstatus	Ursache
0	Unknown	<ul style="list-style-type: none"> Die Integrität der Komponente kann nicht bestimmt werden.
5	OK	<ul style="list-style-type: none"> Das DPE funktioniert normal.
7	OK_BUT	<ul style="list-style-type: none"> Das DPE passt die Kommunikationsgeschwindigkeit an.
10	Degraded/Warning	<ul style="list-style-type: none"> Die Performance des DPE wird heruntergestuft.
20	Major failure	<ul style="list-style-type: none"> Für DPE weichen Festplattenlaufwerk-Typen ab. Beim DPE ist ein Kommunikationsfehler aufgetreten. Das DPE ist defekt. Das DPE weist eine defekte LCC auf. Das DPE wurde falsch konfiguriert. Das DPE wurde falsch verkabelt. Das DPE wurde entfernt. Beim DPE ist ein Fehler bei der Stromversorgung aufgetreten. Das DPE ist mit einem defekten I/O-Modul verbunden. Steuerungsfehler zwischen Prozessoren für DPE; DPE muss wiederhergestellt werden. Kommunikationsfehler zwischen Prozessoren für DPE; DPE muss wiederhergestellt werden.

Anzeigen des Disk Processor Enclosure

Zeigen Sie Details des DPE-Systems an.

Format

```
/env/dpe [-id <value>] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	ID des DPE.

Beispiel 1 (nur physische Bereitstellungen)

Mit dem folgenden Befehl werden Informationen zum System-DPE angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /env/dpe show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:   ID           = dpe
     Name        = DPE
     Health state = OK (5)
     Health details = "The component is operating normally. No action is
required."
     Manufacturer =
     Model        = BC DPE NO I/O DUAL SP 25 DRV 6C
     Part number  = 100-542-441-03
     Serial number = FCNBV131000114
     Power (Present) = 361 watts
     Power (Rolling Average) = 362 watts
     Temperature (Present) = 84° F (29° C)
     Temperature (Rolling Average) = 84° F (29° C)
```

Beispiel 2 (nur virtuelle Bereitstellungen)

Mit dem folgenden Befehl werden Informationen zum System-DPE angezeigt:

```
uemcli -d 10.0.0.2 -u Local/joe -p MyPassword456! /env/dpe show -detail
```

```
Storage system address: 10.0.0.2
Storage system port: 443
HTTPS connection

1:   ID           = dpe
     Name        = DPE
     Health state = OK (5)
     Health details = "The component is operating normally. No action is required."
     Manufacturer = VMware
     Model        = VIRT SINGLE SP DPE 16
```

Managen des Speichermoduls (nur physische Bereitstellungen)

In der folgenden Tabelle sind die Werte des Integritätsstatus für Systemspeichermodule aufgeführt.

Tabelle 92. Werte des Integritätsstatus der Speichermodule

Code	Integritätsstatus	Ursache
0	Unknown	<ul style="list-style-type: none"> Die Integrität der Komponente kann nicht bestimmt werden.
5	OK	<ul style="list-style-type: none"> Das Speichermodul funktioniert normal.
20	Major failure	<ul style="list-style-type: none"> Das Speichermodul ist defekt. Das Speichermodul wurde entfernt.

Anzeigen des Speichermoduls

Zeigen Sie eine Liste der Systemspeichermodule an.

Format

```
/env/mm [-id <value>] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	ID des Speichermoduls.

Beispiel

Mit dem folgenden Befehl wird eine Liste der Systemspeichermodule angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /env/mm show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:   ID           = MM_SPA_0
     SP          = SPÄ
     Slot        = 0
     Health state = OK (5)

2:   ID           = MM_SPA_1
     SP          = SPÄ
     Slot        = 1
     Health state = OK (5)
```

Managen der System Status Card (nur physische Bereitstellungen)

In der folgenden Tabelle sind die Werte des Integritätsstatus für System Status Cards (SSCs) aufgeführt.

Tabelle 93. Werte des SSC-Integritätsstatus

Code	Integritätsstatus	Ursache(n)
0	Unknown	<ul style="list-style-type: none"> Die Integrität der Komponente kann nicht bestimmt werden.
5	OK	<ul style="list-style-type: none"> Die SSC funktioniert normal.
20	Major failure	<ul style="list-style-type: none"> Die SSC ist defekt.

Tabelle 93. Werte des SSC-Integritätsstatus (fortgesetzt)

Code	Integritätsstatus	Ursache(n)
		<ul style="list-style-type: none"> Die SSC fehlt.

Anzeigen der SSC

Zeigen Sie eine Liste von System Status Cards (SSCs) an.

Format

```
/env/ssc [-id <value>] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	ID der SSC.

Beispiel

Mit dem folgenden Befehl werden die Details der Systemstatuskarte angezeigt.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /env/ssc show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:  ID           = dae_0_3_ssc
   Enclosure    = dae_0_3_
   Slot         = 0
   Name         = DAE 0 3 System Status Card
   Health state = OK (5)
   Health details = "The component is operating normally. No action is required."
   Manufacturer = EMC
   Model        = NAGA 120 DRIVE 12G SAS SSC FRU
   Part number  = 303-340-000C-00
   Serial number = CF2BW162200072
```

Managen von Lüftermodulen (nur physische Bereitstellungen)

In der folgenden Tabelle sind die Werte des Integritätsstatus für Systemlüftermodule aufgeführt.

Tabelle 94. Werte des Integritätsstatus des Systemlüftermoduls

Code	Integritätsstatus	Ursache
0	Unknown	<ul style="list-style-type: none"> Die Integrität der Komponente kann nicht bestimmt werden.
5	OK	<ul style="list-style-type: none"> Das Lüftermodul funktioniert normal.
10	Degraded/Warning	<ul style="list-style-type: none"> Das Lüftermodul wird heruntergestuft.
20	Major failure	<ul style="list-style-type: none"> Das Lüftermodul wurde entfernt. Das Lüftermodul ist defekt.

Anzeigen des Lüftermoduls

Zeigen Sie eine Liste aller Lüftermodule des Systems an.

Format

```
/env/fan [-id <value>] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Identifiziert das Lüftermodul.

Beispiel

Mit dem folgenden Befehl wird eine Liste der Cachekarten des Systems angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /env/fan show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:   ID           = dpe_fan_a0

     Enclosure    = dpe
     Slot         = 0
     Name         = DPE Cooling Module A0
     Health state = OK (5)
     Health details = "The component is operating normally. No action is required."
     Manufacturer =
     Model        =
     Part number  =
     Serial number =

2:   ID           = dae_0_1_fan_1

     Enclosure    = dae_0_1
     Slot         = 1
     Name         = DAE 0 1 Cooling Module 1
     Health state = OK (5)
     Health details = "The component is operating normally. No action is required."
     Manufacturer =
     Model        =
     Part number  =
     Serial number =

3:   ID           = dpe_fan_bm_a0

     Enclosure    = dpe
     Slot         = 0
     Name         = DPE Cooling Module BM A0
     Health state = OK (5)
     Health details = "The component is operating normally. No action is required."
     Manufacturer =
     Model        =
     Part number  =
     Serial number =
```

Managen von I/O-Modulen, integrierten Modulen und Karten mit 4 Ports (nur physische Bereitstellungen)

Je nach Typ der installierten Komponente bieten I/O-Module, integrierte Module und Karten mit 4 Ports eine Verbindung zwischen den SPs und dem Host oder zwischen den SPs und dem Disk Array Enclosure.

ANMERKUNG: Integrierte Module und Karten mit 4 Ports sind nur für Unity 480/480F-, Unity 680/680F- und Unity 880/880F- Systeme verfügbar.

Sie können die Details zu jedem im System installierten I/O-Modul, integrierten Modul oder Karte mit 4 Ports anzeigen, z. B. den Integritätsstatus. Setzen Sie eine neu hinzugefügte Komponente ein, um sie für die Verwendung durch das System zu konfigurieren. Die einzelnen Komponentendatensätze und Warnmeldungen sind mit einer ID gekennzeichnet. In der folgenden Tabelle sind die Attribute für I/O-Module, integrierte Module und Karten mit 4 Ports aufgeführt.

Tabelle 95. Komponentenattribute

Attribut	Beschreibung
ID	ID des I/O-Moduls, des integrierten Moduls oder der Karte mit 4 Ports.
SP	ID des SP, mit dem das I/O-Modul, das integrierte Modul oder die Karte mit 4 Ports verbunden ist.
Slot	DPE-Steckplatz (Disk Processor Enclosure), in dem das I/O-Modul, das integrierte Modul oder die Karte mit 4 Ports eingesteckt ist
Name	Name des I/O-Moduls, des integrierten Moduls oder der Karte mit 4 Ports.
Manufacturer	Hersteller des I/O-Moduls, des integrierten Moduls oder der Karte mit 4 Ports.
Model	Modell des I/O-Moduls, des integrierten Moduls oder der Karte mit 4 Ports.
Health state	<p>Integritätsstatus des I/O-Moduls, des integrierten Moduls oder der Karte mit 4 Ports Der Integritätsstatuscode wird in Klammern angezeigt. Folgende Werte sind möglich:</p> <ul style="list-style-type: none"> ● Unknown (0) : Integritätsstatus der Komponente kann nicht ermittelt werden. ● OK (5) — Komponente funktioniert normal. ● Degraded/Warning (10) — Komponente wurde nicht festgeschrieben (konfiguriert). Commit ausführen für I/O-Module, integrierte Module und Karten mit 4 Ports erklärt, wie ein E/A-Modul, ein eingebettetes Modul oder eine 4-Port-Karte festgeschrieben wird. ● Minor failure (15) : Es ist mindestens eines der folgenden Ereignisse eingetreten: <ul style="list-style-type: none"> ○ Die Komponente wurde nach einem Neustart des SP nicht eingesetzt (konfiguriert). ○ Die Komponente wurde in den falschen Steckplatz eingesetzt. ● Major failure (20) : Es ist mindestens eines der folgenden Ereignisse eingetreten: <ul style="list-style-type: none"> ○ Die Komponente wurde entfernt. Installieren Sie die Komponente neu. ○ Die Komponente ist defekt und muss ausgetauscht werden. In der Onlinehilfe zu Unisphere wird erläutert, wie Sie eine Austauschkomponente bestellen. ○ Komponente ist falsch konfiguriert. Setzen Sie die Komponente ein, um Sie erneut zu konfigurieren.

Tabelle 95. Komponentenattribute (fortgesetzt)

Attribut	Beschreibung
Health details	Zusätzliche Integritätsinformationen. Weitere Informationen zur Integrität finden Sie im Anhang A, Referenz.
Part number	Art.-Nr. des I/O-Moduls, des integrierten Moduls oder der Karte mit 4 Ports.
Serial number	Seriennummer des I/O-Moduls, des integrierten Moduls oder der Karte mit 4 Ports.

Commit ausführen für I/O-Module, integrierte Module und Karten mit 4 Ports

Wenn Sie ein neues I/O-Modul, ein integriertes Modul oder eine Karte mit 4 Ports zum System hinzugefügt haben, müssen Sie zuerst ein Commit ausführen, bevor es vom System verwendet werden kann. Das System führt für unkonfigurierte I/O-Module, integrierte Module und Karten mit 4 Ports Commits automatisch aus.

Format

```
/env/iomodule commit
```

Beispiel

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /env/iomodule commit
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
Operation completed successfully.
```

Anzeigen von I/O-Modulen, integrierten Modulen und Karten mit 4 Ports

Zeigen Sie Details zu I/O-Modulen, integrierten Modulen oder Karten mit 4 Ports im System an. Sie können nach der Komponenten-ID filtern.

 **ANMERKUNG:** Aktionsbefehl „show“ bietet weitere Details zur Änderung des Ausgabeformats.

Format

```
/env/iomodule [-id <value>] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID eines I/O-Moduls, eines integrierten Moduls oder einer Karte mit 4 Ports ein.

Beispiel 1

Mit dem folgenden Befehl werden Details zu den beiden I/O-Modulen im System angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /env/iomodule show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:   ID           = IO_SPA_0
     SP           = SP̄A
     Slot         = 0
     Health state = OK (5)

2:   ID           = IO_SPA_1
     SP           = SP̄A
     Slot         = 1
     Health state = Degraded/Warning (10)
```

Beispiel 2

Der folgende Befehl zeigt Details zu einem integrierten Modul und einer Karte mit 4 Ports in einem Unity 680-System an:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /env/iomodule show
```

```
1:   ID           = spb_iopm_0
     SP           = spb
     Slot         = 0
     Name         = SP B Embedded Module 0
     Health state = OK (5)
     Health details = "The component is operating normally. No action is required."
     Manufacturer =
     Model        = IOPM
     Part number  = 110-452-003C-00
     Serial number = FCNMD184200103

2:   ID           = spb_ocp_0
     SP           = spb
     Slot         = 0
     Name         = SP A 4-Port Card
     Health state = OK (5)
     Health details = "The component is operating normally. No action is required."
     Manufacturer = CELESTICA-CSS
     Model        = OCP Light Blade
     Part number  = 105-001-101-03
     Serial number = CETED184300069
```

Managen von Speicher

Themen:

- Automatisches Konfigurieren von Pools
- Konfigurieren benutzerdefinierter Pools
- Managen von Pool-Tiers
- Anzeigen von Poolressourcen
- Managen von allgemeinen FAST VP-Einstellungen
- Managen von FAST Cache (nur unterstützte physische Bereitstellungen)
- Managen von FAST Cache-Speicherobjekten (nur physische Bereitstellungen)
- Anzeigen von Speicherprofilen (nur physische Bereitstellungen)
- Managen von Laufwerksgruppen (nur physische Bereitstellungen)
- Managen von Speichersystemkapazität-Einstellungen
- Managen von System-Tier-Kapazitätseinstellungen
- Managen von Dateisystemen
- Managen von Benutzer-Quotas für Dateisysteme und Quota-Strukturen
- Managen von Quotenstrukturen
- Managen von Quota-Einstellungen
- Managen von NFS-Netzwerk-Shares
- Managen von SMB-Netzwerkfreigaben
- Managen von LUNs
- Managen von Consistency Groups
- Managen von VMware NFS-Datenspeichern
- Managen von VMware-VMFS-Datenspeichern
- Managen von VMware-Protokollendpunkten
- vVol-Datenspeicher managen
- vVol-Objekte managen
- Managen von Funktionsprofilen
- Managen von I/O-Limits
- Managen der I/O-Limitkonfiguration

Automatisches Konfigurieren von Pools

Pools sind die Gruppen von physischen Laufwerken oder virtuellen Festplatten (Festplattengruppen), auf denen Speicherressourcen erstellt werden. Das System kann durch die Auswahl der richtigen Festplattengruppen auf der Grundlage von Typ und Verfügbarkeit der Laufwerke im System automatisch Pools konfigurieren.

Die folgenden Kriterien müssen erfüllt sein, um Pools automatisch zu erstellen.

- Eine FAST VP/FAST Cache-Lizenz ist nicht installiert.
- Keine andere Pools wurden erstellt.
- Bei virtuellen Bereitstellungen wurde allen virtuellen Laufwerken ein Tier-Typ zugewiesen.

i ANMERKUNG: Unter [Konfigurieren benutzerdefinierter Pools](#) wird erläutert, wie benutzerdefinierte Pools konfiguriert werden. Vor dem Erstellen von Speicherressourcen (einschließlich NAS-Server) müssen Sie mindestens einen Pool konfigurieren.

i ANMERKUNG: Alle Festplatten im System werden für Speicherpools verwendet.

In der folgenden Tabelle sind die Attribute für die automatische Poolkonfiguration aufgeführt.

Tabelle 96. Attribute für die automatische Poolkonfiguration

Attribut	Beschreibung
Target	<p>Art der Laufwerkskonfiguration. Folgende Werte sind möglich:</p> <ul style="list-style-type: none"> • pool: In einem Pool konfigurierte Laufwerke. • spares: Den Pools als Reserve zugewiesene Laufwerke. Wie viele Reservelaufwerke einem Pool zugewiesen sind, hängt vom Laufwerks- und Pooltyp ab: <ul style="list-style-type: none"> ○ Bei Pools zur Steigerung der Kapazität sind keine Reservelaufwerke zugewiesen. ○ Bei Pools zur Steigerung der Performance wird jeweils 30 Laufwerken ein Reservelaufwerk zugewiesen. Für alle weiteren 30 Laufwerke wird jeweils ein weiteres Reservelaufwerk zugewiesen. ○ Bei Flash-Pools wird jeweils 30 Laufwerken ein Reservelaufwerk zugewiesen. Für alle weiteren 30 Laufwerke wird jeweils ein weiteres Reservelaufwerk zugewiesen.
Name	<p>Name des Pools. Den folgenden Pools werden je nach Typ und Eigenschaft der im System vorhandenen Festplatten vom System Laufwerke zugewiesen:</p> <ul style="list-style-type: none"> • Capacity: Von NL (Near-Line)-SAS (Serial Attached SCSI)-Laufwerken zugewiesener Speicher Dieser Speicher bietet eine hohe Kapazität, aber insgesamt eine geringere Performance gegenüber regulären SAS- und EFD-Laufwerken (Enterprise Flash Drive). Mit NL-SAS-Laufwerken können Sie äußerst wirtschaftlichen Speicher für Vorgänge bereitstellen, bei denen keine hohe I/O-Performance erforderlich ist, wie etwa Datenbackup. • Performance: Von SAS (Serial Attached SCSI)-Festplatten zugewiesener Speicher Der Speicher bietet eine Mischung aus Performance und Kapazität und eignet sich damit für Anwendungen, in denen eine Balance zwischen diesen beiden Eigenschaften gefragt ist. • Flash: Von Flash-Laufwerken zugewiesener Speicher Hierbei handelt es sich um Speicher mit äußerst hoher Performance, jedoch zu relativ hohen Kosten pro GB. Flash-Laufwerke eignen sich insbesondere in Anwendungen, in denen eine hohe I/O-Performance und Energieeffizienz erforderlich sind. <p>Je nach Typ des Pools werden unterschiedliche RAID-Gruppen konfiguriert und die Laufwerke den Pools als Reservelaufwerke zugewiesen. Weitere Einzelheiten zu Pools und Reservelaufwerken finden Sie in der Unisphere-Onlinehilfe.</p>
Drives (current)	Liste der zurzeit im Pool befindlichen Laufwerke.
Drives (new)	Liste der Laufwerke, die dem Pool hinzugefügt werden sollen.
RAID level (nur physische Bereitstellungen)	Angewandtes RAID-Level.
Stripe length(nur physische Bereitstellungen)	Kommagetrennte Liste der Laufwerke im Stripe.

Starten der automatischen Poolkonfiguration

Starten Sie die Konfiguration von Pools automatisch. [Anzeigen von Konfigurationseinstellungen für die automatische Erstellung von Pools](#) zeigt die Konfigurationseinstellungen an, die bei der Ausführung dieses Befehls angewendet werden.

 **ANMERKUNG:** Alle Festplatten im System werden verwendet, um Speicherpools automatisch zu konfigurieren. Sie müssen diesen Vorgang explizit bestätigen, um fortzufahren.

Format

`/stor/config/auto set`

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie die Aktion im asynchronen Modus aus.

Beispiel

Die automatische Konfiguration des Pools wird mit dem folgenden Befehl gestartet:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/auto set
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

All disks in the system will be used to configure pools. Do you want to proceed?
yes / no: yes
Operation completed successfully.
```

Anzeigen von Konfigurationseinstellungen für die automatische Erstellung von Pools

Rufen Sie die Einstellungen für die automatische Poolerstellung auf, die auf das System angewendet werden. Im Abschnitt [Initiieren der automatischen Storage-Pool-Konfiguration](#) wird erläutert, wie diese Einstellungen auf das System angewendet werden.

 **ANMERKUNG:** Der Aktionsbefehl „show“ erläutert, wie das Ausgabeformat geändert wird.

Format

```
/stor/config/auto show
```

Beispiel (nur physische Bereitstellungen)

Mit dem folgenden Befehl wird die automatische Konfiguration von Pools und Reservefestplatten auf dem System angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/auto show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      Target          = Pool
        Name           = Performance
        Drives (current) = 5 x 600GB SAS; 5 x 300GB SAS
        Drives (new)    = 5 x 600GB SAS
        RAID level      = 5
        Stripe length   = 5,9

2:      Target          = Pool
        Name           = Capacity
        Drives (current) = 10 x 1TB NL-SAS
        Drives (new)    = 2 x 1TB NL SAS
        RAID level      = 5
        Stripe length   = 5,9

3:      Target          = Pool
        Name           = Extreme Performance
        Drives (current) = 10 x 100GB EFD
        Drives (new)    = 10 x 100GB EFD
        RAID level      = 1
        Stripe length   = 2

4:      Target          = Spares
        Name           = Unused / Hot Spare Candidates
        Drives (current) = 1 x 600GB SAS; 1 x 300GB SAS; 1 x 1TB NL SAS
        Drives (new)    = 1 x 100GB EFD
        RAID level      =
        Stripe length   =
```

Konfigurieren benutzerdefinierter Pools

Pools sind die Gruppen von Laufwerken, auf denen Speicherressourcen erstellt werden. Sie können Pools auf der Grundlage des Speicherresourcentyps und der Verwendung des Pools konfigurieren, beispielsweise als Dateisystemspeicher, der für die Datenbanknutzung optimiert ist. Die Speichereigenschaften unterscheiden sich in den folgenden Kriterien:

- Verwendeter Laufwerkstyp für Bereitstellung des Speichers.
- (nur virtuelle Dual-SP-Bereitstellungen) Implementierte RAID-Ebene für den Speicher.

i ANMERKUNG: Vor dem Erstellen von Speicherressourcen müssen Sie mindestens einen Pool konfigurieren.

In der folgenden Tabelle sind die Attribute für Pools aufgeführt:

Tabelle 97. Benutzerdefinierte Poolattribute

Attribut	Beschreibung
ID	ID des Pools.
Name	Name des Pools.
Type	Speicherpooltyp Gültige Werte: <ul style="list-style-type: none"> • Dynamic • Herkömmlich
Description	Kurze Beschreibung des Pools.
Total space	Gesamtspeicherkapazität des Pools.
Current allocation	Menge des Speichers im Pool, die Speicherressourcen zugewiesen ist.
Preallocated space	Die Menge des Speicherplatzes, die für zukünftige Zwecke im Pool für Speicherressourcen reserviert ist, um Schreibvorgänge effizienter zu gestalten. Der Pool kann möglicherweise einen Teil dieses Speicherplatzes zurückgewinnen, wenn nur noch insgesamt wenig Poolspeicherplatz frei ist. Dieser Wert entspricht der Summe der <code>sizePreallocated</code> -Werte der jeweiligen Storage-Ressource im Pool.
Remaining space	Menge des Speichers im Pool, die Speicherressourcen nicht zugewiesen ist.
Subscription	Bei Thin Provisioning der Gesamtspeicherplatz, der vom Pool genutzt wird. Alle Pools unterstützen standardmäßig und mit Thin Provisioning bereitgestellte Speicherressourcen. Bei Standard-Speicherressourcen wird bei der Erstellung der Ressource die gesamte angeforderte Kapazität aus dem Pool zugewiesen. Bei Thin-Provisioning-Speicherressourcen werden immer nur Teile der Kapazität je nach tatsächlicher Nutzung zugewiesen. Da mittels Thin Provisioning bereitgestellte Storage-Ressourcen eine höhere Belegung aufweisen können, als ihnen tatsächlich an Speicher zugewiesen wurde, ist es möglich, für Pools ein übermäßiges Provisioning festzulegen, damit sie eine höhere Storage-Kapazität unterstützen können, als tatsächlich haben. i ANMERKUNG: Wenn 85 % der physischen Kapazität des Pools erreicht sind, wird automatisch eine Warnmeldung ausgegeben. Der Schwellenwert für die Warnmeldung wird mit <code>-alertThreshold</code> angegeben.
Subscription percent	Bei Thin Provisioning der Prozentsatz des im Pool verfügbaren Gesamtspeicherplatzes, der belegt ist.
Alert threshold	Schwellenwert, bei dem eine Warnmeldung gesendet wird, sobald ein bestimmter Prozentsatz des belegbaren Speicherplatzes aufgebraucht ist. Der Wert kann zwischen 50 und 85 % eingestellt werden.
Drives	Hierunter werden die Typen der Laufwerke im System und deren Anzahl im Pool aufgeführt. Wenn FAST VP installiert ist, können unterschiedliche Laufwerkstypen gemischt werden, um einen Tiered Pool zu erstellen. SAS Flash 4-Laufwerke müssen allerdings in einem homogenen Pool verwendet werden.
Number of drives	Gesamtzahl der Laufwerke im Pool.
Number of unused drives	Anzahl der nicht genutzten Laufwerke im Pool.

Tabelle 97. Benutzerdefinierte Poolattribute (fortgesetzt)

Attribut	Beschreibung
RAID level(nur physische Bereitstellungen)	RAID-Level der Laufwerke im Pool.
Stripe length(nur physische Bereitstellungen)	Anzahl der Laufwerke, auf die die Daten verteilt sind.
Rebalancing	Gibt an, ob ein Poolausgleich läuft. Gültige Werte: <ul style="list-style-type: none"> • yes • no
Rebalancing progress	Gibt den Fortschritt des Poolausgleichs in Prozent an.
System defined pool	Hier wird angegeben, ob der Pool automatisch konfiguriert wurde. Gültige Werte: <ul style="list-style-type: none"> • yes • no
Health state	Integritätsstatus des Pools. Der Integritätsstatuscode wird in Klammern angezeigt. Gültige Werte: <ul style="list-style-type: none"> • Unknown (0): Der Integritätsstatus ist unbekannt. • OK (5): Läuft normal. • OK BUT (7): Der Pool hat den nutzerdefinierten oder den vom System definierten Schwellenwert von 85 % überschritten. • Degraded/Warning (10): Der Pool ist in Betrieb, funktioniert aber aufgrund mindestens einer der folgenden Ursachen nur eingeschränkt: <ul style="list-style-type: none"> ○ Der Pool hat den benutzerdefinierten Schwellenwert überschritten. ○ Der Pool erreicht in Kürze die Kapazitätsgrenze. ○ Der Pool ist nahezu voll. ○ Die Poolperformance ist eingeschränkt. • Major failure (20): Aufgrund eines fehlerhaften Caches ist der Pool nicht mehr verfügbar. • Critical failure (25): Der Pool ist vollständig belegt. Fügen Sie dem Pool zur Vermeidung eines Datenverlusts Speicher hinzu, oder erstellen Sie weitere Pools. • Non-recoverable error (30): Im Pool sind mindestens 2 Laufwerke fehlerhaft; unter Umständen ist ein Datenverlust aufgetreten.
Health details	Zusätzliche Integritätsinformationen. Weitere Informationen zur Integrität finden Sie im Anhang A, Referenz.
FAST Cache enabled (nur physische Bereitstellungen)	Gibt an, ob FAST Cache im Pool aktiviert ist. Gültige Werte: <ul style="list-style-type: none"> • yes • no
Non-base size used	Menge an Speicher, der für Thin Clones und Snapshot-Daten verwendet wird.
Auto-delete state	Gibt den Status eines automatischen Löschvorgangs im Pool an. Gültige Werte: <ul style="list-style-type: none"> • Idle • Running • Could not reach LWM • Could not reach HWM <p>i ANMERKUNG: Wenn der automatische Löschvorgang den oberen Schwellenwert nicht erreichen kann und sich Snapshots im Pool befinden, setzt der automatische Löschvorgang den Status für diesen Schwellenwert auf <code>Could not reach HWM</code> und erzeugt eine Warnmeldung.</p> <ul style="list-style-type: none"> • Failed
Auto-delete paused	Gibt an, ob ein automatischer Löschvorgang angehalten wurde. Gültige Werte: <ul style="list-style-type: none"> • yes • no

Tabelle 97. Benutzerdefinierte Poolattribute (fortgesetzt)

Attribut	Beschreibung
Auto-delete pool full threshold enabled	Gibt an, ob das System den oberen Schwellenwert für automatische Löschung bei vollem Speicherpool prüft. Gültige Werte: <ul style="list-style-type: none"> • yes • no
Auto-delete pool full high water mark	Die obere Marke für vollen Pool.
Auto-delete pool full low water mark	Die Der untere Marke für vollen Pool.
Auto-delete snapshot space used threshold enabled	Gibt an, ob das System die obere Marke für die automatische Löschung nach verwendeten Snapshot-Speicherplatz prüft. Gültige Werte: <ul style="list-style-type: none"> • yes • no
Auto-delete snapshot space used high water mark	Obere Marke für den verwendeten Snapshot-Speicherplatz im Pool.
Auto-delete snapshot space used low water mark	Untere Marke für den verwendeten Snapshot-Speicherplatz im Pool.
Data Reduction space saved(nur physische Bereitstellungen)	Im Pool eingesparter Speicher durch die Datenreduzierung. <i>i</i> ANMERKUNG: Die Datenreduzierung ist für Thin-LUNs und Thin-Dateisysteme verfügbar. Die Thin-Dateisysteme müssen auf Unity-Systemen erstellt worden sein, auf denen Version 4.2.x oder höher ausgeführt wird.
Data Reduction percent(nur physische Bereitstellungen)	Im Pool eingesparter Speicher (in Prozent) durch die Datenreduzierung. <i>i</i> ANMERKUNG: Die Datenreduzierung ist für Thin-LUNs und Thin-Dateisysteme verfügbar. Die Thin-Dateisysteme müssen auf Unity-Systemen erstellt worden sein, auf denen Version 4.2.x oder höher ausgeführt wird.
Data Reduction ratio(nur physische Bereitstellungen)	Verhältnis der Einsparungen zwischen Daten ohne Datenreduzierung und Daten nach der Datenreduzierung. <i>i</i> ANMERKUNG: Die Datenreduzierung ist für Thin-LUNs und Thin-Dateisysteme verfügbar. Die Thin-Dateisysteme müssen auf Unity-Systemen erstellt worden sein, auf denen Version 4.2.x oder höher ausgeführt wird.
All flash pool	Gibt an, ob der Speicherpool nur Flash-Laufwerke enthält. Gültige Werte: <ul style="list-style-type: none"> • yes • no

Erstellen von Pools

Erstellen Sie einen dynamischen oder einen herkömmlichen Pool.

- Beim Erstellen eines Dynamic Pools mit NL-SAS-Laufwerken sind RAID 5, 6 und 10 zulässig.
- Sowohl herkömmliche als auch Dynamic Pools werden in der CLI und REST API für Unity-All-Flash-Modelle ab OE-Version 4.2.x und für Unity-Hybridmodelle ab OE-Version 5.2.x unterstützt. Der Standardspeicherpooltyp ist dynamisch.
- Herkömmliche Speicherpools werden in allen hybriden und virtuellen Unity-Modellen unterstützt. Sie werden auch in Unity-All-Flash-Modellen mit OE-Version 4.1.x oder früher unterstützt.
- Die minimale Anzahl der Laufwerke, die für einen dynamischen Pool verwendet werden soll, ist die ausgewählte RAID-Breite plus ein Laufwerk.

Format

```
/stor/config/pool create [-async] -name <value> [-type {dynamic [-hotSpareCapacity <value>] | traditional}] [-descr <value>] {-diskGroup <value> -drivesNumber <value> [-storProfile <value>] | -disk <value>} [-tier <value>] [-alertThreshold <value>] [-snapPoolFullThresholdEnabled {yes|no}]
```

```
no]] [-snapPoolFullHWM <value>] [-snapPoolFullLWM <value>] [-snapSpaceUsedThresholdEnabled {yes|no}] [-snapSpaceUsedHWM <value>] [-snapSpaceUsedLWM <value>]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus. i ANMERKUNG: Gleichzeitige Befehle, asynchron oder synchron, können fehlschlagen, wenn sie beim Versuch, dieselben Systemelemente zu managen, in Konflikt stehen.
-name	Geben Sie einen Namen für den Pool ein.
-type	(Verfügbar nur für Systeme, die dynamische Speicherpools unterstützen) Geben Sie den Typ des zu erstellenden Speicherpools an. Folgende Werte sind möglich: <ul style="list-style-type: none"> dynamic <ul style="list-style-type: none"> -hotSpareCapacity Legt die Hot-Spare-Kapazität für alle 32-Laufwerke von dynamischen Pools fest. Gültige Werte sind 1 (reservieren Sie 1 Laufwerkkapazität für alle 32-Laufwerke als Ersatzlaufwerk) oder 2 (reservieren Sie eine Kapazität von 2 Laufwerken für alle 32-Laufwerke als Ersatzlaufwerk). i ANMERKUNG: Die Einstellung -hotSpareCapacity wird für einen Tier verwendet. Das bedeutet, dass alle Festplattengruppen im selben Tier denselben Wert -hotSpareCapacity haben. <ul style="list-style-type: none"> traditional Der Standardwert ist dynamic.
-descr	Geben Sie eine kurze Beschreibung des Pools ein.
-storProfile(nur physische Bereitstellungen)	Geben Sie kommagetrennt die ID der Storage-Profile ein, die auf den Pool angewendet werden sollen. Wie das Profil aussieht, hängt von dem Typ der Storage-Ressource ab, die auf den Pool zugreift, und von der beabsichtigten Nutzung des Pools. Storage-Profile anzeigen (nur physische Bereitstellungen) erläutert, wie Sie die IDs der verfügbaren Storage-Profile im System anzeigen können. Wenn diese Option nicht angegeben wird, wird für jeden bestimmten Laufwerkstyp in der ausgewählten Laufwerksgruppe eine Standard-RAID-Konfiguration ausgewählt: NL-SAS (RAID 6 mit einer Stripe-Länge von 8), SAS (RAID 5 mit einer Stripe-Länge von 5) oder Flash (RAID 5 mit einer Stripe-Länge von 5).
-diskGroup(nur physische Bereitstellungen)	Geben Sie eine durch Komma getrennte Liste der IDs der Laufwerksgruppen ein, die im Speicherpool verwendet werden sollen. Durch die Angabe von Laufwerksgruppen mit verschiedenen Laufwerkstypen wird ein Multi-Tier-Pool erstellt. Laufwerksgruppen anzeigen erläutert, wie Sie die IDs der Laufwerksgruppen im System anzeigen können.
-drivesNumber(nur physische Bereitstellungen)	Geben Sie kommagetrennt an, wie viele Laufwerke jeweils aus den ausgewählten Laufwerksgruppen im Pool verwendet werden sollen. Wenn diese Option angegeben wird, wenn -storProfile nicht angegeben ist, wird der Vorgang möglicherweise fehlschlagen, wenn der Wert -drivesNumber nicht der Standard-RAID-Konfiguration für jeden Laufwerkstyp in der ausgewählten Laufwerksgruppe entspricht. i ANMERKUNG: Wenn Sie einen Dynamic Pool auf einem Hybrid-Flash-Array erstellen, können Sie keine System-Festplattenlaufwerke angeben. Bei der Erstellung eines herkömmlichen Pools können Sie System-Festplattenlaufwerke angeben.
-disk(nur virtuelle Bereitstellungen)	Geben Sie die Liste der Laufwerk-IDs durch Komma getrennt ein, die im Pool verwendet werden sollen. Bestimmte Laufwerke müssen zuverlässige Speicherobjekte sein, die keinen zusätzlichen Schutz erfordern.
-tier(nur virtuelle Bereitstellungen)	Geben Sie die kommagetrennte Liste der Tiers an, denen die Laufwerke zugewiesen werden. Wenn das Tier ausgelassen wird, wird es automatisch zugewiesen, sofern die

Qualifizierer	Beschreibung
	Tiering-Informationen für das zugehörige Laufwerk verfügbar sind. Folgende Werte sind möglich: <ul style="list-style-type: none"> • Kapazität • -Performance • extreme
-alertThreshold	Geben Sie bei Thin Provisioning den Schwellwert als Prozentsatz des verwendeten belegbaren Speicherplatzes an. Die Warnmeldung wird ausgegeben, sobald der Host den angegebenen Prozentsatz am belegbaren Speicherplatz verwendet. Der Wert kann zwischen 50 und 85 % eingestellt werden.
-FASTCacheEnabled(nur physische Bereitstellungen)	Geben Sie an, ob FAST Cache im Pool aktiviert werden soll. Folgende Werte sind möglich: <ul style="list-style-type: none"> • yes • no Der Standardwert ist yes.
-snapPoolFullThresholdEnabled	Geben Sie an, ob das System den oberen Schwellenwert für die automatische Löschung bei vollem Pool prüft. Folgende Werte sind möglich: <ul style="list-style-type: none"> • yes • no Der Standardwert ist yes.
-snapPoolFullHWM	Geben Sie die obere Marke für vollen Pool an. Gültige Werte sind 1 bis 99. Der Standardwert beträgt 95.
-snapPoolFullLWM	Geben Sie die untere Marke für vollen Pool an. Gültige Werte sind 0 bis 98. Der Standardwert beträgt 85.
-snapSpaceUsedThresholdEnabled	Geben Sie an, ob das System die obere Marke für verwendeten Snapshot-Speicherplatz für die automatische Löschung prüft. Folgende Werte sind möglich: <ul style="list-style-type: none"> • yes • no Der Standardwert ist yes.
-snapSpaceUsedHWM	Geben Sie die obere Marke für verwendeten Snapshot-Speicherplatz an, mit dem die automatische Löschung im Pool ausgelöst wird. Gültige Werte sind 1–99. Der Standardwert ist 95.
-snapSpaceUsedLWM	Geben Sie die untere Marke für verwendeten Snapshot-Speicherplatz an, mit dem die automatische Löschung im Pool ausgelöst wird. Gültige Werte sind 0–98. Der Standardwert ist 20.

ANMERKUNG: Verwenden Sie den Befehl [Festplatteneinstellungen ändern \(nur virtuelle Bereitstellungen\)](#), um die zugewiesenen Tiers für bestimmte Laufwerke zu ändern.

Beispiel 1 (nur physische Bereitstellungen)

Der folgende Befehl erstellt einen dynamischen Speicherpool. Dieses Beispiel verwendet die Speicherprofile profile_1 und profile_2, 6 Laufwerke von Laufwerksgruppe dg_2 und 10 Laufwerke von Laufwerksgruppe dg_28. Der konfigurierte Pool erhält die ID pool_2.

ANMERKUNG: Bevor Sie den Befehl `stor/config/pool create` verwenden, verwenden Sie den Befehl `/stor/config/profile show`, um die dynamischen Poolprofile und den Befehl `/stor/config/dg show` zum Anzeigen der Laufwerksgruppen anzuzeigen.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! uemcli /stor/config/pool create -name MyPool
-descr "dynamic pool" -diskGroup dg_2,dg_28 -drivesNumber 6,10 -storProfile profile_1,profile_2
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = pool_2
Operation completed successfully.
```

Beispiel 2 (nur physische Bereitstellungen)

Der folgende Befehl erstellt einen herkömmlichen Speicherpool in Modellen, die dynamische Speicherpools unterstützen. Dieses Beispiel verwendet die Speicherprofile tprofile_1 und tprofile_2, 5 Laufwerke von Laufwerksgruppe dg_3 und 9 Laufwerke von Laufwerksgruppe dg_28. Der konfigurierte Pool erhält die ID pool_6.

ANMERKUNG: Bevor Sie den Befehl `stor/config/pool create` verwenden, verwenden Sie den Befehl `/stor/config/profile -traditional show`, um die traditionellen Poolprofile (die mit „t“ beginnen) und den `/stor/config/dg` Befehl „Show“ zum Anzeigen der Laufwerksgruppen anzuzeigen.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/pool create -name MyPool -descr
"traditional pool" -diskGroup dg_3,dg_28 -drivesNumber 5,9 -storProfile tprofile_1,tprofile_2
-type traditional
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = pool_6
Operation completed successfully.
```

Beispiel 3 (nur physische Bereitstellungen)

Der folgende Befehl erstellt einen herkömmlichen Speicherpool in Modellen, die dynamische Speicherpools nicht unterstützen. Dieses Beispiel verwendet die Speicherprofile profile_19 und profile_20, 5 Laufwerke von Laufwerksgruppe dg_15 und 9 Laufwerke von Laufwerksgruppe dg_16. Der konfigurierte Pool erhält die ID pool_5.

ANMERKUNG: Bevor Sie den Befehl `stor/config/pool create` verwenden, verwenden Sie den Befehl `/stor/config/profile show`, um die traditionellen Poolprofile und den `/stor/config/dg show` Befehl zum Anzeigen der Laufwerksgruppen anzuzeigen.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/pool create -name MyPool -descr
"my big pool" -storProfile profile_19,profile_20 -diskGroup dg_15,dg_16 -drivesNumber 5,9
-FASTCacheEnabled yes
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = pool_5
Operation completed successfully.
```

Beispiel 4 (nur virtuelle Bereitstellungen)

Mit dem folgenden Befehl wird ein Storage-Pool mit 2 virtuellen Laufwerken, vdisk_0 und vdisk_2, im Tier für Extreme Performance erstellt. Der konfigurierte Pool erhält die ID pool_4.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/pool create -name vPool -descr
"my virtual pool" -disk vdisk_0,vdisk_2
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = pool_4
Operation completed successfully.
```

Beispiel 5 (nur physische Bereitstellungen)

Der folgende Befehl erstellt einen dynamischen Storage-Pool, wobei 7 Laufwerke von der Laufwerksgruppe dg_21 mit einer Hot-Spare-Kapazität von 1 Festplatte verwendet werden. 6 Laufwerke von der Laufwerksgruppe dg_31 mit einer Hot-Spare-Kapazität von 2 Laufwerken; und 7 Laufwerke von der Laufwerksgruppe dg_18 mit einer Hot-Spare-Kapazität von 2 Laufwerken:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/pool create -name pool -diskGroup dg_21,dg_31,dg_18 -drivesNumber 7,6,7 -type dynamic -hotSpareCapacity 1,2,2
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = pool_1
Operation completed successfully.
```

ANMERKUNG: Die Einstellung `-hotSpareCapacity` wird für einen Tier verwendet. Das bedeutet, dass alle Festplattengruppen im selben Tier denselben Wert `-hotSpareCapacity` haben. In diesem Beispiel gehören die Laufwerksgruppen dg_31 und dg_18 zum selben Tier und haben dieselbe `-hotSpareCapacity`-Einstellung von 2.

Ändern von Pooleinstellungen

Ändern Sie die Einstellungen für den Schwellenwert für die Abonnementwarnmeldung, FAST Cache und den Snapshot-Schwellenwert bei einem Pool.

Format

```
/stor/config/pool {-id <value> | -name <value>} set [-async] -name <value> [-descr <value>]
[-alertThreshold <value>] [-snapPoolFullThresholdEnabled {yes|no}] [-snapPoolFullHWM <value>] [-
snapPoolFullLWM <value>] [-snapSpaceUsedThresholdEnabled {yes|no}] [-snapSpaceUsedHWM <value>]
[-snapSpaceUsedLWM <value>] [-snapAutoDeletePaused no]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des zu ändernden Pools ein.
-name	Geben Sie den Namen des zu ändernden Pools ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus. ANMERKUNG: Gleichzeitige Befehle, asynchron oder synchron, können fehlschlagen, wenn sie beim Versuch, dieselben Systemelemente zu managen, in Konflikt stehen.
-name	Geben Sie einen Namen für den Pool ein.
-descr	Geben Sie eine kurze Beschreibung des Pools ein.
-alertThreshold	Geben Sie bei Thin Provisioning den Schwellenwert als Prozentsatz des verwendeten belegbaren Speicherplatzes an. Die Warnmeldung wird ausgegeben, sobald der Host den angegebenen Prozentsatz am belegbaren Speicherplatz verwendet. Der Wert kann zwischen 50 und 84 % eingestellt werden.
-FASTCacheEnabled(nur physische Bereitstellungen)	Geben Sie an, ob FAST Cache im Pool aktiviert werden soll. Folgende Werte sind möglich:

Qualifizierer	Beschreibung
	<ul style="list-style-type: none"> • yes • no
-snapPoolFullThresholdEnabled	Geben Sie an, ob das System die obere Marke für die automatische Löschung bei vollem Pool prüft. Folgende Werte sind möglich: <ul style="list-style-type: none"> • yes • no
-snapPoolFullHWM	Geben Sie die obere Marke für vollen Pool an. Gültige Werte sind 1–99. Der Standardwert ist 95.
-snapPoolFullLWM	Geben Sie die untere Marke für vollen Pool an. Gültige Werte sind 0–98. Der Standardwert ist 85.
-snapSpaceUsedThresholdEnabled	Geben Sie an, ob das System die obere Marke für verwendeten Snapshot-Speicherplatz für die automatische Löschung prüft. Folgende Werte sind möglich: <ul style="list-style-type: none"> • yes • no
-snapSpaceUsedHWM	Geben Sie die obere Marke für verwendeten Snapshot-Speicherplatz an, mit dem die automatische Löschung im Pool ausgelöst wird. Gültige Werte sind 1–99. Der Standardwert ist 95.
-snapSpaceUsedLWM	Geben Sie die untere Marke für verwendeten Snapshot-Speicherplatz an, mit dem die automatische Löschung im Pool ausgelöst wird. Gültige Werte sind 0–98. Der Standardwert ist 20.
-snapAutoDeletePaused	Geben Sie an, ob die automatische Snapshot-Löschung angehalten werden soll. Wenn Sie no angeben, wird der automatische Löschkvorgang fortgesetzt.

Beispiel

Mit dem folgenden Befehl wird der Schwellenwert für die Abonnementwarnmeldung für Pool pool_1 auf 70 % festgelegt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/pool -id pool_1 -set -alertThreshold 70 -FASTCacheEnabled no
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = pool_1
Operation completed successfully.
```

Hinzufügen von Laufwerken zum Speicherpool

Durch zusätzliche Laufwerke können Sie die Speicherkapazität des Pools erhöhen.

ANMERKUNG:

- Die minimale Anzahl der Laufwerke, die für einen dynamischen Pool verwendet werden soll, ist die ausgewählte RAID-Breite plus ein Laufwerk.
- Um einen Hybridpool zu erweitern, wenn die Datenreduzierung und erweiterte Deduplizierung für eine Storage-Ressource im Pool aktiviert sind, müssen im Pool mindestens 10 % Flash-Festplatten verfügbar sein.

Format

```
/stor/config/pool {-id <value> | -name <value>} extend [-async] {-diskGroup <value>
-driveNumber <value> [-storProfile <value>] | -disk <value> [-tier <value>]}
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des zu erweiternden Pools ein.
-name	Geben Sie den Namen des zu erweiternden Pools ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.
-diskGroup(nur physische Bereitstellungen)	Geben Sie kommagetrennt die IDs der Laufwerksgruppen ein, die dem Speicherpool hinzugefügt werden sollen.
-drivesNumber(nur physische Bereitstellungen)	Geben Sie kommagetrennt an, wie viele Laufwerke jeweils aus den angegebenen Laufwerksgruppen dem Speicherpool hinzugefügt werden sollen. Wenn diese Option angegeben wird, wenn -storProfile nicht angegeben ist, wird der Vorgang möglicherweise fehlschlagen, wenn der Wert -drivesNumber nicht der Standard-RAID-Konfiguration für jeden Laufwerkstyp in der ausgewählten Laufwerksgruppe entspricht.  ANMERKUNG: Wenn Sie einen Dynamic Pool auf einem Hybrid-Flash-Array erstellen, können Sie keine System-Festplattenlaufwerke angeben. Bei der Erstellung eines herkömmlichen Pools können Sie System-Festplattenlaufwerke angeben.
-storProfile(nur physische Bereitstellungen)	Geben Sie kommagetrennt die IDs der Speicherprofile ein, die auf den Pool angewendet werden sollen. Wenn diese Option nicht angegeben wird, wird für jeden bestimmten Laufwerkstyp in der ausgewählten Laufwerksgruppe eine Standard-RAID-Konfiguration ausgewählt: <ul style="list-style-type: none"> • NL-SAS (RAID 6 mit einer Stripe-Länge von 8) • SAS (RAID 5 mit einer Stripe-Länge von 5) • Flash (RAID 5 mit einer Stripe-Länge von 5)
-disk(nur virtuelle Bereitstellungen)	Geben Sie kommagetrennt die Liste der Laufwerke ein, die dem Pool hinzugefügt werden sollen. Bestimmte Laufwerke müssen zuverlässige Speicherobjekte sein, die keinen zusätzlichen Schutz erfordern.
-tier(nur virtuelle Bereitstellungen)	Geben Sie die kommagetrennte Liste der Tiers an, denen die hinzugefügten Laufwerke zugewiesen werden. Wenn ein Tier in dieser Liste nicht angegeben ist, wird es automatisch zugewiesen, wenn Tiering-Informationen für das zugehörige Laufwerk verfügbar sind. Gültige Werte: <ul style="list-style-type: none"> • Kapazität • -Performance • extreme

Beispiel 1 (nur physische Bereitstellungen)

Mit dem folgenden Befehl wird der Pool pool_1 um sieben Laufwerke aus der Laufwerksgruppe DG_1 erweitert:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/pool -id pool_1 extend -diskGroup dg_1 -drivesNumber 7 -storProfile profile_12
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = pool_1
Operation completed successfully.
```

Beispiel 2 (nur virtuelle Bereitstellungen)

Mit dem folgenden Befehl wird der Pool pool_1 erweitert, indem zwei virtuelle Laufwerke hinzugefügt werden, vdisk_1 und vdisk_5.

```
uemcli -d 10.0.0.2 -u Local/joe -p MyPassword456! /stor/config/pool -id pool_1 extend -disk vdisk_1,vdisk_5
```

```
Storage system address: 10.0.0.2
Storage system port: 443
HTTPS connection

ID = pool_1
Operation completed successfully.
```

Anzeigen von Pools

Zeigen Sie eine Liste der Pools an. Sie können nach der Pool-ID filtern.

 **ANMERKUNG:** Der Aktionsbefehl „show“ erläutert, wie das Ausgabeformat geändert wird.

Format

```
/stor/config/pool {-id <value> | -name <value>}] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID eines Pools ein.
-name	Geben Sie den Namen eines Pools ein.

Beispiel 1 (nur physische Bereitstellungen)

Mit dem folgenden Befehl rufen Sie die Details zu sämtlichen Speicherpools in einem hybriden System ab:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/pool show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1: ID = pool_13
   Type = Dynamic
   Name = Dynamic
   Description =
   Total space = 3815810007040 (3.4T)
   Current allocation = 940921012224 (876.3G)
   Preallocated = 97118896128 (90.4G)
   Remaining space = 2777770098688 (2.5T)
   Subscription = 1194021912576 (1.0T)
   Flash percent = 39%
   Subscription percent = 31%
   Alert threshold = 70%
   Drives = 6 x 600.0G SAS; 6 x 400.0G SAS
Flash 3
  Number of drives = 12
  RAID level = 5
  Stripe length = 5
  Rebalancing = no
  Rebalancing progress =
  Health state = OK (5)
  Health details = "The component is operating normally. No action is required."
  FAST Cache enabled = yes
  Protection size used = 21474836480 (20.0G)
  Non-base size used = 21474836480 (20.0G)
  Auto-delete state = Idle
```

```

Auto-delete paused = no
Auto-delete pool full threshold enabled = yes
Auto-delete pool full high water mark = 95%
Auto-delete pool full low water mark = 85%
Auto-delete snapshot space used threshold enabled = no
Auto-delete snapshot space used high water mark = 25%
Auto-delete snapshot space used low water mark = 20%
Data Reduction space saved = 18790481920 (17.5G)
Data Reduction Percent = 2%
Data Reduction Ratio = 1.0:1
All flash pool = no

2: ID = pool_14
Type = Traditional
Name = Traditional
Description =
Total space = 15750450380800 (14.3T)
Current allocation = 3999290327040 (3.6T)
Preallocated = 2376320188416 (2.1T)
Remaining space = 9374839865344 (8.5T)
Subscription = 14190303510528 (12.9T)
Flash percent = 0%
Subscription percent = 90%
Alert threshold = 70%
Drives = 5 x 4.0T NL-SAS
Number of drives = 5
RAID level = 5
Stripe length = 5
Rebalancing = no
Rebalancing progress =
Health state = OK (5)
Health details = "The component is operating
normally. No action is required."
FAST Cache enabled = yes
Protection size used = 0
Non-base size used = 0
Auto-delete state = Idle
Auto-delete paused = no
Auto-delete pool full threshold enabled = yes
Auto-delete pool full high water mark = 95%
Auto-delete pool full low water mark = 85%
Auto-delete snapshot space used threshold enabled = no
Auto-delete snapshot space used high water mark = 25%
Auto-delete snapshot space used low water mark = 20%
Data Reduction space saved = 0
Data Reduction Percent = 0%
Data Reduction Ratio = 1.0:1
All flash pool = no

```

Beispiel 2 (nur physische Bereitstellungen)

Das folgende Beispiel zeigt alle Speicherpools für ein Modell an, das dynamische Speicherpools unterstützt.

```
uemcli -d 10.0.0.2 -u Local/joe -p MyPassword456! /stor/config/pool show -detail
```

```

[Response]
Storage system address: 10.0.0.2
Storage system port: 443
HTTPS connection

1: ID = pool_3
Type = Traditional
Name = MyPool
Description = traditional pool
Total space = 14177955479552 (12.8T)
Current allocation = 0
Preallocated space = 38310387712 (35.6G)
Remaining space = 14177955479552 (12.8T)
Subscription = 0
Subscription percent = 0%
Alert threshold = 70%

```

```

    Drives = 9 x 1.6T SAS Flash 3; 5 x 400.0G
SAS Flash 2
    Number of drives = 14
    RAID level = 5
    Stripe length = Mixed
    Rebalancing = no
    Rebalancing progress =
    Health state = OK (5)
    Health details = "The component is operating
normally. No action is required."
    FAST Cache enabled = no
    Protection size used = 0
    Non-base size used = 0
    Auto-delete state = Idle
    Auto-delete paused = no
    Auto-delete pool full threshold enabled = yes
    Auto-delete pool full high water mark = 95%
    Auto-delete pool full low water mark = 85%
    Auto-delete snapshot space used threshold enabled = no
    Auto-delete snapshot space used high water mark = 25%
    Auto-delete snapshot space used low water mark = 20%
    Data Reduction space saved = 0
    Data Reduction percent = 0%
    Data Reduction ratio = 1:1
    All flash pool = yes

2: ID = pool_4
    Type = Dynamic
    Name = dynamicPool
    Description =
    Total space = 1544309178368 (1.4T)
    Current allocation = 0
    Preallocated space = 38310387712 (35.6G)
    Remaining space = 1544309178368 (1.4T)
    Subscription = 0
    Subscription percent = 0%
    Alert threshold = 70%
    Drives = 6 x 400.0G SAS Flash 2
    Number of drives = 6
    RAID level = 5
    Stripe length = 5
    Rebalancing = no
    Rebalancing progress =
    Health state = OK (5)
    Health details = "The component is operating
normally. No action is required."
    Protection size used = 0
    Non-base size used = 0
    Auto-delete state = Idle
    Auto-delete paused = no
    Auto-delete pool full threshold enabled = yes
    Auto-delete pool full high water mark = 95%
    Auto-delete pool full low water mark = 85%
    Auto-delete snapshot space used threshold enabled = no
    Auto-delete snapshot space used high water mark = 25%
    Auto-delete snapshot space used low water mark = 20%
    Data Reduction space saved = 0
    Data Reduction percent = 0%
    Data Reduction ratio = 1:1
    All flash pool = yes

```

Beispiel 3 (nur virtuelle Bereitstellungen)

Mit dem folgenden Befehl werden Details zu sämtlichen Pools in einem virtuellen System angezeigt:

```
uemcli -d 10.0.0.3 -u Local/joe -p MyPassword456! /stor/config/pool show -detail
```

```

Storage system address: 10.0.0.3
Storage system port: 443
HTTPS connection

```

```

1: ID = pool_1
   Name = Capacity
   Description =
   Total space = 4947802324992 (4.5T)
   Current allocation = 3298534883328 (3T)
   Preallocated space = 38310387712 (35.6G)
   Remaining space = 4947802324992 (1.5T)
   Subscription = 10995116277760 (10T)
   Subscription percent = 222%
   Alert threshold = 70%
   Drives = 1 x 120GB Virtual; 1 x 300GB
Virtual
  Number of drives = 2
  Health state = OK (5)
  Health details = "The component is operating
normally. No action is required."
  Non-base size used = 1099511625 (1G)
  Auto-delete state = Running
  Auto-delete paused = no
  Auto-delete pool full threshold enabled = yes
  Auto-delete pool full high water mark = 95%
  Auto-delete pool full low water mark = 85%
  Auto-delete snapshot space used threshold enabled = yes
  Auto-delete snapshot space used high water mark = 25%
  Auto-delete snapshot space used low water mark = 20%

```

Löschen von Pools

Löschen Sie einen Pool.

Format

```
/stor/config/pool {-id <value> | -name <value>} delete [-async]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des zu löschenden Pools ein.
-name	Geben Sie den Namen des zu löschenden Pools ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.  ANMERKUNG: Gleichzeitige Befehle, asynchron oder synchron, können fehlschlagen, wenn sie beim Versuch, dieselben Systemelemente zu managen, in Konflikt stehen.

Beispiel

Der folgende Befehl löscht den Pool pool_1:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/pool -id pool_1 delete
```

```

Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

```

Operation completed successfully.

Managen von FAST VP-Pooleinstellungen

Fully Automated Storage Tiering for Virtual Pools (FAST VP) ist eine Speichereffizienztechnologie, mit der Daten anhand von Datenzugriffsmustern automatisch zwischen Storage Tiers in einem Pool verschoben werden.

In der folgenden Tabelle sind die Attribute für FAST VP-Pooleinstellungen aufgeführt.

Tabelle 98. FAST VP-Poolattribute

Attribut	Beschreibung
Pool	Identifiziert den Pool.
Status	Identifiziert den Status der Datenverlagerung im Pool. Folgende Werte sind möglich: <ul style="list-style-type: none">• Not started: Die Datenverlagerung wurde noch nicht gestartet.• Paused : Die Datenverlagerung wurde unterbrochen.• Completed : Die Datenverlagerung ist abgeschlossen.• Stopped by user: Die Datenverlagerung wurde vom Benutzer angehalten.• Active: Die Datenverlagerung läuft.• Failed: Die Datenverlagerung ist fehlgeschlagen.
Relocation type	Typ der Datenverlagerung. Folgende Werte sind möglich: <ul style="list-style-type: none">• Manual: Die Datenverlagerung wurde vom Benutzer initiiert.• Scheduled oder rebalancing: Die Datenverlagerung wurde vom System initiiert, weil sie geplant war oder weil die Daten ausgeglichen wurden.
Schedule enabled	Identifiziert, ob der Pool entsprechend dem FAST VP-Plan des Systems ausgeglichen wird. Folgende Werte sind möglich: <ul style="list-style-type: none">• yes• no
Start time	Gibt die Zeit an, um die die aktuelle Datenverlagerung gestartet wurde.
End time	Gibt die Zeit an, zu der das Ende der aktuellen Datenverlagerung geplant ist.
Data relocated	Die Menge der Daten, die während einer laufenden Verlagerung verlagert werden, bzw. bei einer vorherigen Verlagerung verlagert wurden, wenn derzeit keine Datenverlagerung läuft. Das Format lautet wie folgt: <code><value> [suffix]</code> Hierbei gilt: <ul style="list-style-type: none">• value: Gibt die Größe der verlagerten Daten an.• suffix: Gibt an, dass der Wert sich auf die vorherige Verlagerungssitzung bezieht.
Rate	Identifiziert die Übertragungsrate für die Datenverlagerung. Folgende Werte sind möglich: <ul style="list-style-type: none">• Low: Geringste Auswirkung auf die Systemperformance• Medium: Mäßige Auswirkung auf die Systemperformance• High: Höchste Auswirkung auf die Systemperformance Der Standardwert ist „Medium“.  ANMERKUNG: Dieses Feld ist leer, wenn keine Datenverlagerung läuft.
Data to move up	Menge der Daten im Pool, deren Verschiebung auf einen höheren Storage Tier geplant ist.
Data to move down	Menge der Daten im Pool, deren Verschiebung auf einen niedrigeren Storage Tier geplant ist.

Tabelle 98. FAST VP-Poolattribute (fortgesetzt)

Attribut	Beschreibung
Data to move within	Menge der Daten im Pool, deren Verschiebung zum Ausgleich innerhalb desselben Storage Tier geplant ist.
Data to move up per tier	Menge der Daten pro Tier, deren Verschiebung auf einen höheren Tier geplant ist. Das Format lautet wie folgt: <code><tier_name>:[value]</code> Hierbei gilt: <ul style="list-style-type: none"> • tier_name: Gibt den Storage Tier an. • value: Gibt die Menge der Daten in diesem Tier an, die nach oben verschoben werden sollen.
Data to move down per tier	Die Menge der Daten pro Tier, deren Verschiebung auf einen niedrigeren Tier geplant ist. Das Format lautet wie folgt: <code><tier_name>:[value]</code> Hierbei gilt: <ul style="list-style-type: none"> • tier_name: Gibt den Storage Tier an. • value: Gibt die Menge der Daten in diesem Storage Tier an, die nach unten verschoben werden sollen.
Data to move within per tier	Die Menge der Daten pro Tier, deren Verschiebung innerhalb desselben Tier zum Ausgleich geplant ist. Das Format lautet wie folgt: <code><tier_name>:[value]</code> Hierbei gilt: <ul style="list-style-type: none"> • tier_name: Gibt den Storage Tier an. • value: Gibt die Menge der Daten in diesem Tier an, die ausgeglichen werden sollen.
Estimated relocation time	Gibt die geschätzte Zeitdauer an, die für die nächste Datenverlagerung erforderlich ist.

Ändern von FAST VP-Pooleinstellungen

Ändern Sie die FAST VP-Einstellungen in einem vorhandenen Pool.

Format

```
/stor/config/pool/fastvp {-pool <value> | -poolName <value>} set [-async] -schedEnabled {yes | no}
```

Objektqualifizierer

Qualifizierer	Beschreibung
-pool	Geben Sie die ID des Pools ein.
-poolName	Geben Sie den Namen des Pools ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.  ANMERKUNG: Gleichzeitige Befehle, asynchron oder synchron, können fehlschlagen, wenn sie beim Versuch, dieselben Systemelemente zu managen, in Konflikt stehen.

Qualifizierer	Beschreibung
-schedEnabled	Geben Sie an, ob der Pool entsprechend dem FAST VP-Plan des Systems ausgeglichen wird. Folgende Werte sind möglich: <ul style="list-style-type: none"> • yes • no

Beispiel

Im folgenden Beispiel wird der Ausgleichsplan für Pool pool_1 aktiviert:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/pool/fastvp -pool pool_1 set -schedEnabled yes
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Pool ID = pool_1
Operation completed successfully.
```

Anzeigen von FAST VP-Poleinstellungen

Zeigen Sie die FAST VP-Einstellungen für einen Pool an.

Format

```
/stor/config/pool/fastvp [{"-pool <value> | -poolName <value>}] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-pool	Geben Sie die ID des Pools ein.
-poolName	Geben Sie den Namen des Pools ein.

Beispiel

Mit dem folgenden Befehl werden die FAST VP-Einstellungen im Speichersystem aufgeführt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/pool/fastvp -show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1: Pool = pool_1
  Relocation type = manual
  Status = Active
  Schedule enabled = no
  Start time = 2013-09-20 12:55:32
  End time = 2013-09-20 21:10:17
  Data relocated = 100111454324 (100G)
  Rate = high
  Data to move up = 4947802324992 (4.9T)
  Data to move down = 4947802324992 (4.9T)
  Data to move within = 4947802324992 (4.9T)
  Data to move up per tier = Performance: 500182324992 (500G), Capacity:
1000114543245 (1.0T)
  Data to move down per tier = Extreme Performance: 1000114543245 (1.0T), Performance:
500182324992 (500G)
```

```
Data to move within per tier = Extreme Performance: 500182324992 (500G), Performance:
500182324992 (500G), Capacity: 500182324992 (500G)
Estimated relocation time = 7h 30m
```

Starten der Datenverlagerung

Starten Sie die Datenverlagerung in einem Pool.

Format

```
/stor/config/pool/fastvp {-pool <value> | -poolName <value>} start [-async] [-rate {low | medium
| high}] [-endTime <value>]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-pool	Geben Sie die ID des Pools ein, um die Datenverlagerung fortzusetzen.
-poolName	Geben Sie den Namen des Pools ein, um die Datenverlagerung fortzusetzen.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.  ANMERKUNG: Gleichzeitige Befehle, asynchron oder synchron, können fehlschlagen, wenn sie beim Versuch, dieselben Systemelemente zu managen, in Konflikt stehen.
-pool	Geben Sie die ID des Pools ein.
-endTime	Geben Sie die Zeit zum Anhalten der Datenverlagerung an. Das Format lautet wie folgt: [HH:MM] Hierbei gilt: <ul style="list-style-type: none"> ● HH: Stunde ● MM: Minute Der Standardwert sind acht Stunden nach der aktuellen Zeit.
-rate	Geben Sie die Übertragungsrate für die Datenverlagerung an. Folgende Werte sind möglich: <ul style="list-style-type: none"> ● Low: Geringste Auswirkung auf die Systemperformance ● Medium: Mäßige Auswirkung auf die Systemperformance ● High: Höchste Auswirkung auf die Systemperformance Der Standardwert ist auf Systemebene festgelegt.

Beispiel

Mit dem folgenden Befehl wird die Datenverlagerung in Pool pool_1 gestartet und angewiesen, um 04:00 zu enden:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/pool/fastvp -pool pool_1 start
-endTime 04:00
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
Operation completed successfully.
```

Anhalten der Datenverlagerung

Halten Sie die Datenverlagerung in einem Pool an.

Format

```
/stor/config/pool/fastvp {-pool <value> | -poolName <value>} stop [-async]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-pool	Geben Sie die ID des Pools ein.
-poolName	Geben Sie den Namen des Pools ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.

Beispiel

Mit dem folgenden Befehl wird die Datenverlagerung in Pool pool_1 gestoppt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/pool/fastvp -pool pool_1 stop
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
Operation completed successfully.
```

Managen von Pool-Tiers

Anhand von Storage Tiers können Benutzer Daten zwischen verschiedenen Laufwerkstypen in einem Pool verschieben, um die Speichereffizienz zu maximieren. Storage Tiers werden durch die folgenden Merkmale definiert:

- Laufwerksperformance
- Laufwerkskapazität

In der folgenden Tabelle sind die Attribute für Speicherprofile aufgeführt:

Tabelle 99. Attribute des Storage Tier

Attribut	Beschreibung
Name	Name des Storage Tier
Drives	Die Liste der Laufwerkstypen, und die Anzahl der Laufwerke jeden Typs im Storage Tier.
RAID level(nur physische Bereitstellungen)	RAID-Level des Storage Tier
Stripe length(nur physische Bereitstellungen)	Kommagetrennte Liste der Stripe-Längen der Laufwerke auf dem Storage Tier.
Total space	Gesamtkapazität des Storage Tier
Current allocation	Aktuell zugewiesener Speicherplatz

Tabelle 99. Attribute des Storage Tier (fortgesetzt)

Attribut	Beschreibung
Remaining space	Verbleibender Speicherplatz

Anzeigen von Storage Tiers

Zeigen Sie eine Liste der Storage Tiers an. Sie können nach der Pool-ID filtern.

 **ANMERKUNG:** Der Aktionsbefehl „show“ erläutert, wie das Ausgabeformat geändert wird.

Format

```
/stor/config/pool/tier {-pool <value> | -poolName <value>} show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-pool	Geben Sie die ID eines Pools ein.
-poolName	Geben Sie den Namen eines Pools ein.

Beispiel 1 (nur physische Bereitstellungen)

Mit dem folgenden Befehl werden Tier-Details über den angegebenen Pool angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/pool/tier -pool pool_1 show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:   Name           = Extreme Performance
     Drives         = 6 x 800.0G SAS Flash 2
     Drive type     = SAS Flash
     RAID level     = 5
     Stripe length  = 5
     Total space    = 3111972241408 (2.8T)
     Current allocation = 0
     Remaining space = 3111972241408 (2.8T)
     Spare space configuration = 1

2:   Name           = Performance
     Drives         = 6 x 600.0G SAS
     Drive type     = SAS
     RAID level     = 5
     Stripe length  = 5
     Total space    = 2317671727104 (2.1T)
     Current allocation = 0
     Remaining space = 2317671727104 (2.1T)
     Spare space configuration = 2
```

Beispiel 2 (nur virtuelle Bereitstellungen)

Mit dem folgenden Befehl werden Details zum angegebenen Pool in einem virtuellen System angezeigt.

```
uemcli -d 10.0.0.2 -u Local/joe -p MyPassword456! /stor/config/pool/tier -pool pool_1 show
-detail
```

```
Storage system address: 10.0.0.2
Storage system port: 443
HTTPS connection

1:  Name           = Extreme Performance
    Drives         =
    Total space    = 0
    Current allocation = 0
    Remaining space = 0

2:  Name           = Performance
    Drives         = 1 x 500GB Virtual
    Total space    = 631242752000 (500.0G)
    Current allocation = 12624855040 (10.0G)
    Remaining space = 618617896960 (490.0G)

3:  Name           = Capacity
    Drives         =
    Total space    = 0
    Current allocation = 0
    Remaining space = 0
```

Anzeigen von Poolressourcen

Dieser Befehl zeigt eine Liste der Speicherressourcen an, die in einem Pool zugewiesen werden. Dies können Speicherressourcen sein, die auf dem angegebenen Speicherpool bereitgestellt wurden, und NAS-Server, von denen Dateisysteme dem Speicherpool zugewiesen wurden.

In der folgenden Tabelle sind die Attribute für Poolressourcen aufgeführt.

Tabelle 100. Poolressourcen

Attribut	Beschreibung
ID	Speicherressourcenkennung
Name	Name der Speicherressource.
Resource type	Typ der Ressource Gültige Werte: <ul style="list-style-type: none"> • LUN • File system • LUN group • VMware NFS • VMware VMFS • NAS server
Pool	Name des Pools.
Total pool space used	Der gesamte Poolspeicherplatz, der von einer Speicherressource verwendet wird. Dies schließt die verwendete Größe der Primärdaten, die verwendete Größe des Snapshot und die Größe der Metadaten ein. Speicherplatz im Pool kann freigegeben werden, wenn Snapshots und Thin Clones für Speicherressourcen gelöscht werden oder abgelaufen sind.
Total pool space preallocated	Die gesamte Menge des Speicherplatzes, die für zukünftige Zwecke im Pool für Speicherressourcen reserviert ist, um Schreibvorgänge effizienter zu gestalten. Der Pool kann möglicherweise einen Teil dieses Speicherplatzes zurückgewinnen, wenn nur noch wenig Speicherplatz frei ist. Zusätzlicher Poolspeicherplatz kann freigegeben werden, wenn Snapshots und Thin Clones gelöscht werden oder abgelaufen sind und wenn die Datenreduzierung angewendet wird.

Tabelle 100. Poolressourcen (fortgesetzt)

Attribut	Beschreibung
Total pool non-base space used	Gesamter Speicherpoolplatz, der von Snapshots und Thin Clones verwendet wird.
Health state	Integritätsstatus des Dateisystems. Der Integritätsstatuscode wird in Klammern angezeigt.
Health details	Zusätzliche Integritätsinformationen. Weitere Informationen zur Integrität finden Sie im Anhang A, Referenz.

Format

```
/stor/config/pool/sr [{"-pool <value> | -poolName <value>"}] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-pool	Geben Sie die ID des Pools ein.
-poolName	Geben Sie den Namen des Pools ein.

Beispiel

Mit dem folgenden Befehl werden Details für alle Speicherressourcen angezeigt, die mit dem Pool pool_1 verknüpft sind:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/pool/sr -pool pool_1 show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      ID              = res_1
      Name              = File_System_1
      Resource type     = File_System
      Pool              = pool_1
      Total pool space used = 53024473088 (49.3G)
      Total pool preallocated = 15695003648 (14.6G)
      Total pool snapshot space used = 7179124736 (6.6G)
      Total pool non-base space used = 7179124736 (6.6G)
      Health state       = OK (5)
      Health details     = "The component is operating normally. No action is
required."
```

```
2:      ID              = sv_1
      Name              = AF_LUN_1
      Resource type     = LUN
      Pool              = pool_1
      Total pool space used = 14448566272 (13.4G)
      Total pool preallocated = 4610351104 (4.2G)
      Total pool snapshot space used = 4593991680 (4.2G)
      Total pool non-base space used = 4593991680 (4.2G)
      Health state       = OK (5)
      Health details     = "The LUN is operating normally. No action is
required."
```

```
3:      ID              = res_2
      Name              = File_System_2
      Resource type     = File_System
      Pool              = pool_1
      Total pool space used = 117361025024 (109.3G)
      Total pool preallocated = 3166494720 (2.9G)
      Total pool snapshot space used = 41022308352 (38.2G)
```

```

Total pool non-base space used = 41022308352 (38.2G)
Health state                    = OK (5)
Health details                  = "The component is operating normally. No action is
required."

4:      ID                      = sv_2
      Name                      = AF_LUN 2
      Resource type             = LUN
      Pool                      = pool_1
      Total pool space used     = 9500246016 (8.8G)
      Total pool preallocated   = 2579349504 (2.4G)
      Total pool snapshot space used = 0
      Total pool non-base space used = 0
      Health state              = OK (5)
      Health details            = "The LUN is operating normally. No action is
required."

5:      ID                      = res_3
      Name                      = CG1
      Resource type             = LUN group
      Pool                      = pool_1
      Total pool space used     = 892542287872 (831.2G)
      Total pool preallocated   = 8863973376 (8.2G)
      Total pool snapshot space used = 231799308288 (215.8G)
      Total pool non-base space used = 231799308288 (215.8G)
      Health state              = OK (5)
      Health details            = "The component is operating normally. No action is
required."

```

Managen von allgemeinen FAST VP-Einstellungen

Fully Automated Storage Tiering for Virtual Pools (FAST VP) ist eine Speichereffizienztechnologie, mit der Daten anhand von Datenzugriffsmustern automatisch zwischen Storage Tiers in einem Pool verschoben werden.

In der folgenden Tabelle sind die Attribute für allgemeine FAST VP-Einstellungen aufgeführt.

Tabelle 101. Allgemeine FAST VP-Attribute

Attribut	Beschreibung
Paused	Gibt an, ob die Datenverlagerung ausgesetzt ist. Folgende Werte sind möglich: <ul style="list-style-type: none"> • yes • no
Schedule-enabled	Identifiziert, ob der Pool entsprechend dem FAST VP-Plan des Systems ausgeglichen wird. Folgende Werte sind möglich: <ul style="list-style-type: none"> • yes • no
Frequency	Datenverlagerungszeitplan Das Format lautet wie folgt: Every <days_of_the_week> at <start_time> until <end_time> Hierbei gilt: <ul style="list-style-type: none"> • <days_of_the_week>: Listet die Tage der Woche auf, an denen die Datenverlagerung ausgeführt wird. • <start_time>: Startzeit der Datenverlagerung • <end_time>: Endzeit der Datenverlagerung
Rate	Identifiziert die Übertragungsrates für die Datenverlagerung. Folgende Werte sind möglich: <ul style="list-style-type: none"> • Low: Geringste Auswirkung auf die Systemperformance • Medium: Mäßige Auswirkung auf die Systemperformance • High: Höchste Auswirkung auf die Systemperformance Standardwert ist medium.  ANMERKUNG: Dieses Feld ist leer, wenn keine Datenverlagerung läuft.

Tabelle 101. Allgemeine FAST VP-Attribute (fortgesetzt)

Attribut	Beschreibung
Data to move up	Menge der Daten im Pool, deren Verschiebung auf einen höheren Storage Tier geplant ist.
Data to move down	Menge der Daten im Pool, deren Verschiebung auf einen niedrigeren Storage Tier geplant ist.
Data to move within	Menge der Daten im Pool, deren Verschiebung zum Ausgleich innerhalb desselben Storage Tier geplant ist.
Estimated scheduled relocation time	Gibt die geschätzte Zeitdauer an, die für die nächste Datenverlagerung erforderlich ist.

Ändern von allgemeinen FAST VP-Einstellungen

Ändern Sie die allgemeinen FAST VP-Einstellungen.

Format

```
/stor/config/fastvp set [-async] [-schedEnabled {yes | no}] [-days <value>] [-at <value>] [-until <value>] [-rate {low | medium | high}] [-paused {yes | no}]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.
-paused	Geben Sie an, ob die Datenverlagerung im Speichersystem angehalten werden soll. Gültige Werte: <ul style="list-style-type: none"> • yes • no
-schedEnabled	Geben Sie an, ob der Pool entsprechend dem FAST VP-Plan des Systems ausgeglichen wird. Gültige Werte: <ul style="list-style-type: none"> • yes • no
-days	Geben Sie eine kommasetrennte Liste der Wochentage an, an denen die Datenverlagerung geplant wird. Gültige Werte: <ul style="list-style-type: none"> • mon: Montag • tue: Dienstag • wed: Mittwoch • thu: Donnerstag • fri: Freitag • sat: Samstag • sun: Sonntag
-at	Geben Sie die Zeit zum Starten der Datenverlagerung an. Das Format lautet wie folgt: [HH:MM] Hierbei gilt: <ul style="list-style-type: none"> • HH: Stunde • MM: Minute Gültige Werte liegen zwischen 00:00 und 23:59. Der Standardwert ist 00:00.
-until	Geben Sie die Zeit zum Anhalten der Datenverlagerung an. Das Format lautet wie folgt: [HH:MM] Hierbei gilt: <ul style="list-style-type: none"> • HH: Stunde

Qualifizierer	Beschreibung
	<ul style="list-style-type: none"> MM: Minute Gültige Werte liegen zwischen 00:00 und 23:59. Der Standardwert ist acht Stunden nach der Uhrzeit, die mit dem Parameter <code>-at</code> angegeben wurde.
<code>-rate</code>	Geben Sie die Übertragungsrate für die Datenverlagerung an. Folgende Werte sind möglich: <ul style="list-style-type: none"> low: Geringste Auswirkung auf die Systemperformance medium: Mäßige Auswirkung auf die Systemperformance high: Höchste Auswirkung auf die Systemperformance Der Standardwert beträgt <code>medium</code> .

Beispiel

Mit dem folgenden Befehl wird der Datenverlagerungsplan geändert und die Ausführung auf Montag bis Freitag von 23:00 bis 07:00 festgelegt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/fastvp set -schedEnabled yes -days "Mon,Fri" -at 23:00 -until 07:00
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
Operation completed successfully.
```

Anzeigen von allgemeinen FAST VP-Einstellungen

Zeigen Sie die allgemeinen FAST VP-Einstellungen an.

Format

```
/stor/config/fastvp show -detail
```

Beispiel

Mit dem folgenden Befehl werden die allgemeinen FAST VP-Einstellungen angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/fastvp show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
1: Paused = no
   Schedule enabled = yes
   Frequency = Every Mon, Fri at 22:30 until 8:00
   Rate = high
   Data to move up = 4947802324992 (1.5T)
   Data to move down = 4947802324992 (1.5T)
   Data to move within = 4947802324992 (1.5T)
   Estimated scheduled relocation time = 7h 30m
```

Managen von FAST Cache (nur unterstützte physische Bereitstellungen)

FAST Cache ist eine Speichereffizienztechnologie, bei der Laufwerke genutzt werden, um die Cachekapazität des Speichersystems zu erweitern und die Performance zu verbessern.

In der folgenden Tabelle sind die Attribute für FAST Cache aufgeführt:

Tabelle 102. FAST Cache-Attribute

Attribut	Beschreibung
Capacity	Kapazität von FAST Cache.
Drives	Die Liste der Laufwerkstypen und die Anzahl der Laufwerke jeden Typs in FAST Cache.
Number of drives	Gesamtzahl der Laufwerke in FAST Cache.
RAID level	Auf die FAST Cache-Laufwerke angewandtes RAID-Level. Dieser Wert ist immer RAID 1 .
Health state	Integritätsstatus des FAST Cache. Der Integritätsstatuscode wird in Klammern angezeigt.
Health details	Zusätzliche Integritätsinformationen. Weitere Informationen zur Integrität finden Sie im Anhang A, Referenz.

Erstellen von FAST Cache

Konfigurieren Sie FAST Cache. Das Speichersystem gibt einen Fehler aus, wenn FAST Cache bereits konfiguriert ist.

Format

```
/stor/config/fastcache create [-async] -diskGroup <value> -drivesNumber <value> [-enableOnExistingPools {yes | no}]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.
-diskGroup	Geben Sie die Laufwerksgruppe an, die in FAST Cache eingeschlossen werden soll.  ANMERKUNG: Es können nur SAS Flash 2-Laufwerke in FAST Cache verwendet werden.
-drivesNumber	Geben Sie die Anzahl der Laufwerke an, die in FAST Cache eingeschlossen werden sollen.
-enableOnExistingPools	Geben Sie an, ob FAST Cache auf allen vorhandenen Pools aktiviert werden soll. Gültige Werte: <ul style="list-style-type: none">• yes• no

Beispiel

Mit dem folgenden Befehl wird FAST Cache mit sechs Laufwerken aus Laufwerksgruppe dg_2 konfiguriert und FAST Cache in vorhandenen Pools aktiviert:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/fastcache create -diskGroup dg_2 -drivesNumber 6 -enableOnExistingPools yes
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
Operation completed successfully.
```

Anzeigen von FAST Cache-Einstellungen

Zeigen Sie die FAST Cache-Parameter an.

Format

```
/stor/config/fastcache show
```

Beispiel

Mit dem folgenden Befehl werden die FAST Cache-Parameter für ein Flash-Laufwerk mit mittlerer Lebensdauer angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/fastcache show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      Total space           = 536870912000 (500G)
        Drives                = 6 x 200GB SAS Flash 2
        Number of drives      = 6
        RAID level            = 1
        Health state          = OK (5)
        Health details         = "The component is operating normally. No action is required."
```

Erweitern von FAST Cache

Erweitern Sie den FAST Cache durch Hinzufügen weiterer Laufwerke.

Format

```
/stor/config/fastcache extend [-async] -diskGroup <value> -drivesNumber <value>
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.
-diskGroup	Geben Sie die durch Komma getrennte Liste von SAS-Flash-Laufwerken an, um sie dem FAST Cache hinzuzufügen. Hinzugefügte Laufwerke müssen denselben Laufwerkstyp und dieselbe Laufwerksgröße wie die vorhandenen Laufwerke aufweisen.
-drivesNumber	Geben Sie die Anzahl der Laufwerke für jede entsprechende Laufwerksgruppe an, die FAST Cache hinzugefügt werden soll.

Beispiel

Mit dem folgenden Befehl werden sechs Laufwerke von der Laufwerksgruppe „dg_2“ dem FAST Cache hinzugefügt.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/fastcache extend -diskGroup dg_2 -drivesNumber 6
```

```
Storage system address: 10.0.0.1
Storage system port: 443
```

```
HTTPS connection
```

```
Operation completed successfully.
```

Verkleinern des FAST Cache

Verkleinern Sie den FAST Cache durch Entfernen von Speicherobjekten.

Format

```
/stor/config/fastcache shrink [-async] -so <value>
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.
-so	Geben Sie die durch Komma getrennte Liste von Speicherobjekten an, die aus dem FAST Cache entfernt werden sollen. Führen Sie den Befehl <code>/stor/config/fastcache/show</code> aus, um eine Liste aller Speicherobjekte zu erhalten, die sich derzeit im FAST Cache befinden.

Beispiel

Mit dem folgenden Befehl wird die Raid-Gruppe „RG_1“ aus dem FAST Cache entfernt.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/fastcache shrink -so rg_1
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection
```

```
Operation completed successfully.
```

Löschen von FAST Cache

Löschen Sie die FAST Cache-Konfiguration. Das Speichersystem gibt einen Fehler aus, wenn FAST Cache nicht im System konfiguriert ist.

Format

```
/stor/config/fastcache delete [-async]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.

Beispiel

Mit dem folgenden Befehl wird die FAST Cache-Konfiguration gelöscht:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/fastcache delete
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection
```

```
Operation completed successfully.
```

Managen von FAST Cache-Speicherobjekten (nur physische Bereitstellungen)

FAST Cache-Speicherobjekte enthalten die RAID-Gruppen und Laufwerke, die sich in FAST Cache befinden.

Tabelle 103. Attribute für FAST Cache-Speicherobjekte

Attribut	Beschreibung
ID	Kennung des Speicherobjekts.
Type	Typ des Speicherobjekts
RAID level	Auf das Speicherobjekt angewandtes RAID-Level
Drive type	Laufwerkstyp.
Number of drives	Anzahl der Laufwerke im Speicherobjekt.
Drives	Durch Komma getrennte Liste der Laufwerk-IDs für jedes Speicherobjekt.
Total space	Gesamter vom Speicherobjekt genutzter Speicherplatz
Device state	Status des FAST Cache-Geräts. Folgende Werte können verwendet werden: <ul style="list-style-type: none">• OK: Dieses Cachegerät funktioniert normal.• Degraded: Ein Laufwerk dieses Cachegeräts ist fehlerhaft.• Faulted: Dieses Cachegerät funktioniert nicht normal.• Expanding: Dieses Cachegerät wird erweitert.• Expansion Ready: Die Erweiterung dieses Cachegeräts ist abgeschlossen.• Expansion Failure : Dieses Cachegerät konnte nicht erweitert werden.• Shrinking: Dieses Cachegerät wird verkleinert.• Shrink Done : Dieses Cachegerät hat geleerte Seiten und wird aus FAST Cache entfernt.

Anzeigen von FAST Cache-Speicherobjekten

Zeigen Sie eine Liste aller Speicherobjekte, einschließlich RAID-Gruppen und Laufwerke, in FAST Cache an.

Format

```
/stor/config/fastcache/so [-id <value> ] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des Speicherobjekts im FAST Cache ein.

Beispiel 1

Das folgende Beispiel zeigt FAST Cache-Speicherobjekte auf dem System.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/fastcache/so show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
1:   ID           = rg_6
     Type        = RAID group
     Stripe length = 2
     RAID level   = 1
     Number of drives = 2
     Drive type   = SAS Flash 2
     Drives       = dae_0_1_disk_1, dae_0_1_disk_2
     Total space  = 195400433664 (181.9G)
     Device state = OK
```

Anzeigen von Speicherprofilen (nur physische Bereitstellungen)

Bei Speicherprofilen handelt es sich um vorab festgelegte Einstellungen zur Konfiguration von Pools auf folgender Grundlage:

- Der Art der Speicherressourcen, die auf die Pools zurückgreifen.
- Der beabsichtigten Verwendung des Pools.

Sie können beispielsweise einen Pool für Dateisystem-Speicherressourcen zur allgemeinen Verwendung erstellen. Geben Sie bei der Konfiguration eines Pools die ID des Speicherprofils an, das auf den Pool angewendet werden soll.

ANMERKUNG: Speicherprofile stellen im Hinblick auf die Speicherbereitstellung keine Einschränkung dar. Sie können beispielsweise aus einem Pool für FC- oder iSCSI-Datenbanken Speicherplatz für Dateisysteme bereitstellen. Die Eigenschaften des Speichers sollten jedoch so gut wie möglich an die Art und Nutzung der verwendeten Speicherressource angepasst sein.

Die einzelnen Speicherprofile verfügen über eine eindeutige ID.

In der folgenden Tabelle sind die Attribute für Speicherprofile aufgeführt.

Tabelle 104. Speicherprofil-Attribute

Attribut	Beschreibung
ID	Kennung des Speicherprofils.
Type	(Verfügbar nur für Systeme, die dynamische Pools unterstützen) Typ des Speicherpools, den das Profil erstellen kann. Folgende Werte sind möglich: <ul style="list-style-type: none">• Dynamic• Traditional
Description	Kurze Beschreibung des Speicherprofils.
Drive type	Art der Laufwerke für das Speicherprofil.
RAID level	Nummer der RAID-Ebene des Speicherprofils. Folgende Werte sind möglich: <ul style="list-style-type: none">• 1 : RAID-Level 1• 5 : RAID-Level 5• 6 : RAID-Level 6• 10 : RAID-Level 1+0
Maximum capacity	Maximale Speicherkapazität des Speicherprofils.
Stripe length	Anzahl der Laufwerke, auf die die Daten verteilt sind. ANMERKUNG: Für Profile mit bester Anpassung ist dieser Wert <code>Best fit</code> .
Disk group	Liste der für die Speicherpoolkonfigurationen des angegebenen Speicherprofils empfohlenen Laufwerksgruppen. Dies wird nur berechnet, wenn die Option <code>-configurable</code> angegeben ist.

Tabelle 104. Speicherprofil-Attribute (fortgesetzt)

Attribut	Beschreibung
Maximum drives to configure	Liste der maximalen Anzahl von Laufwerken, die für das angegebene Speicherprofil in den empfohlenen Laufwerksgruppen zulässig sind. Dies wird nur berechnet, wenn die Option <code>-configurable</code> angegeben ist.
Maximum capacity to configure	Liste der maximalen Menge der freien Kapazität der verfügbaren Festplatten zur Konfiguration für das Speicherprofil in den empfohlenen Laufwerksgruppen. Dies wird nur berechnet, wenn die Option <code>-configurable</code> angegeben ist.

 **ANMERKUNG:** Der Aktionsbefehl „show“ erläutert, wie das Ausgabeformat geändert wird.

Format

```
/stor/config/profile [-id <value> | -driveType <value> [-raidLevel <value>] | -traditional] [-configurable] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
<code>-id</code>	Geben Sie die ID eines Speicherprofils ein.
<code>-driveType</code>	Geben Sie den Typ des Laufwerks an.
<code>-raidLevel</code>	Geben Sie den RAID-Typ des Profils an.
<code>-traditional</code>	(Verfügbar nur für Systeme, die dynamische Pools unterstützen) Geben Sie diese Option an, um die Profile anzuzeigen, mit denen Sie herkömmliche Speicherpools erstellen können. Lassen Sie diese Option aus, um die Profile anzuzeigen, mit denen Sie dynamische Speicherpools erstellen können.
<code>-configurable</code>	Zeigen Sie nur Profile an, die konfiguriert werden können, das heißt, solche mit nicht leerer Laufwerksgruppeninformation. Wenn angegeben, werden die folgenden Laufwerksgruppeninformationen für jedes Profil berechnet: <ul style="list-style-type: none"> • <code>Disk group</code> • <code>Maximum drives to configure</code> • <code>Maximum capacity to configure</code> Wenn das Profil für einen dynamischen Speicherpool ist, geben die berechneten Informationen an, ob die Laufwerksgruppe genug Laufwerke für die Speicherpoolerstellung hat. Bei der Berechnung wird angenommen, dass der Speicherpool nur mit den Laufwerken in der angegebenen Laufwerksgruppe erstellt wird.

Beispiel 1

Der folgende Befehl zeigt Details für Speicherprofile an, mit denen dynamische Speicherpools erstellt werden können:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/profile -configurable show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:   ID                = profile_22
     Type              = Dynamic
     Description       = SAS Flash 2 RAID5 (4+1)
     Drive type        = SAS Flash 2
     RAID level        = 5
     Maximum capacity  = 4611148087296 (4.1T)
     Stripe length     = Maximum capacity
     Disk group        =
     Maximum drives to configure =
```

```

Maximum capacity to configure =
2:  ID              = profile_30
    Type            = Dynamic
    Description     = SAS Flash 2 RAID10 (1+1)
    Drive type      = SAS Flash 2
    RAID level      = 10
    Maximum capacity = 9749818597376 (8.8T)
    Stripe length   = 2
    Disk group      =
    Maximum drives to configure =
    Maximum capacity to configure =

3:  ID              = profile_31
    Type            = Dynamic
    Description     = SAS Flash 2 RAID10 (2+2)
    Drive type      = SAS Flash 2
    RAID level      = 10
    Maximum capacity = 9749818597376 (8.8T)
    Stripe length   = 4
    Disk group      =
    Maximum drives to configure =
    Maximum capacity to configure =

```

Beispiel 2

Der folgende Befehl zeigt Details für Speicherprofile an, mit denen herkömmliche Speicherpools in Modellen erstellt werden können, die dynamische Speicherpools unterstützen:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/profile -traditional -configurable show
```

```

Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:  ID              = tprofile_22
    Type            = Traditional
    Description     = SAS Flash 3 RAID5 (4+1)
    Drive type      = SAS Flash 3
    RAID level      = 5
    Maximum capacity = 4611148087296 (4.1T)
    Stripe length   = Maximum capacity
    Disk group      = dg_16
    Maximum drives to configure = 5
    Maximum capacity to configure = 1884243623936 (1.7T)

2:  ID              = tprofile_30
    Type            = Traditional
    Description     = SAS Flash 3 RAID10 (1+1)
    Drive type      = SAS Flash 3
    RAID level      = 10
    Maximum capacity = 9749818597376 (8.8T)
    Stripe length   = 2
    Disk group      = dg_13, dg_15
    Maximum drives to configure = 10, 10
    Maximum capacity to configure = 1247522127872 (1.1T), 2954304921600 (2.6T)

3:  ID              = tprofile_31
    Type            = Traditional
    Description     = SAS Flash 3 RAID10 (2+2)
    Drive type      = SAS Flsh 3
    RAID level      = 10
    Maximum capacity = 9749818597376 (8.8T)
    Stripe length   = 4
    Disk group      = dg_13, dg_15
    Maximum drives to configure = 8, 8
    Maximum capacity to configure = 2363443937280 (2.1T), 952103075840 (886.7G)

```

Managen von Laufwerksgruppen (nur physische Bereitstellungen)

Laufwerksgruppen sind Gruppen von Laufwerken im System mit gleichen Eigenschaften (Typ, Kapazität und Drehzahl). Bei der Konfiguration von Speicherpools wählen Sie die zu verwendende Laufwerksgruppe und die Zahl der Laufwerke aus der Gruppe, die dem Speicherpool hinzugefügt werden sollen.

Die einzelnen Laufwerksgruppen verfügen über eigene IDs.

In der folgenden Tabelle sind die Attribute der Laufwerksgruppen aufgeführt.

Tabelle 105. Laufwerksgruppenattribute

Attribut	Beschreibung
ID	ID der Laufwerksgruppe
Drive type	Typ der Laufwerke in der Laufwerksgruppe
FAST Cache	Gibt an, ob die Laufwerke der Laufwerksgruppe FAST Cache hinzugefügt werden können.
Drive size	Kapazität eines Laufwerks in der Laufwerksgruppe
Rotational speed	Drehzahl der Laufwerke in der Gruppe.
Number of drives	Gesamtzahl der Laufwerke in der Laufwerksgruppe
Unconfigured drives	Gesamtzahl der nicht in einem Speicherpool befindlichen Laufwerke in der Laufwerksgruppe
Capacity	Gesamtkapazität sämtlicher Laufwerke in der Laufwerksgruppe
Recommended number of spares	Anzahl der für diese Laufwerksgruppe empfohlenen Ersatzlaufwerke
Drives past EOL	Anzahl der abgelaufenen (past EOL, End of Life) Laufwerke in der Gruppe
Drives approaching EOL	Anzahl der Laufwerke, die EOL in 0-30 Tagen, 0-60 Tagen, 0-90 Tagen und 0-180 Tagen erreichen werden.

Anzeigen von Laufwerksgruppen

Zeigen Sie Details zu den Laufwerksgruppen im System an. Sie können nach den Laufwerksgruppen-ID filtern.

 **ANMERKUNG:** Der Aktionsbefehl „show“ erläutert, wie das Ausgabeformat geändert wird.

Format

```
/stor/config/dg [-id <value>] [-traditional] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID einer Laufwerksgruppe ein.
-traditional	(Verfügbar nur für Systeme, die dynamische Pools unterstützen) Geben Sie diesen Qualifizierer an, damit das System annimmt, dass die zu erstellenden Speicherpools herkömmliche Speicherpools sind.

Beispiel 1

Der folgende Befehl zeigt Informationen über alle Laufwerksgruppen, die zur Konfiguration von dynamischen Speicherpools verwendet werden können:

ANMERKUNG: Bei Dynamic Pools beinhaltet der Wert für nicht konfigurierte Laufwerke keine System-Festplattenlaufwerke.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/dg show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:   ID                = dg_11
     Drive type       = SAS
     FAST Cache      = no
     Drive size       = 1181778411520 (1.0T)
     Vendor size      = 1.2T
     Rotational speed = 10000 rpm
     Number of drives = 44
     Unconfigured drives = 40
     Capacity         = 51998250106880 (47.2T)
     Recommended number of spares = 0
     Drives past EOL  = 0
     Drives approaching EOL = 0 (0-30 days), 0 (0-60 days), 0 (0-90 days), 0 (0-180
days)

2:   ID                = dg_40
     Drive type       = SAS Flash 4
     FAST Cache      = no
     Drive size       = 1881195675648 (1.7T)
     Vendor size      = 1.9T
     Rotational speed = 0 rpm
     Number of drives = 18
     Unconfigured drives = 18
     Capacity         = 33861522161664 (30.7T)
     Recommended number of spares = 0
     Drives past EOL  = 0
     Drives approaching EOL = 1 (0-30 days), 2 (0-60 days), 2 (0-90 days), 3 (0-180
days)
```

Beispiel 2

Der folgende Befehl zeigt Informationen über alle Laufwerksgruppen, die verwendet werden können, um herkömmliche Speicherpools in Modellen zu konfigurieren, die dynamische Speicherpools unterstützen:

ANMERKUNG: Bei Dynamic Pools beinhaltet der Wert für nicht konfigurierte Laufwerke keine System-Festplattenlaufwerke. Bei herkömmlichen Pools beinhaltet der Wert für nicht konfigurierte Laufwerke System-Festplattenlaufwerke.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/dg -traditional show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:   ID                = dg_11
     Drive type       = SAS
     FAST Cache      = no
     Drive size       = 1181778411520 (1.0T)
     Vendor size      = 1.2T
     Rotational speed = 10000 rpm
     Number of drives = 44
     Unconfigured drives = 44
     Capacity         = 51998250106880 (47.2T)
     Recommended number of spares = 2

2:   ID                = dg_40
     Drive type       = SAS Flash 4
     FAST Cache      = no
```

```

Drive size           = 1881195675648 (1.7T)
Vendor size         = 1.9T
Rotational speed    = 0 rpm
Number of drives    = 18
Unconfigured drives = 18
Capacity           = 33861522161664 (30.7T)
Recommended number of spares = 1

```

Anzeigen empfohlener Konfigurationen für Laufwerksgruppen

Zeigen Sie die empfohlenen Laufwerksgruppen an, von denen aus einem Speicherpool auf der Grundlage eines angegebenen Speicherprofils oder Speicherpooltyps Laufwerke hinzugefügt werden.

 **ANMERKUNG:** Der Aktionsbefehl „show“ erläutert, wie das Ausgabeformat geändert wird.

Format

```
/stor/config/dg recom {-profile <value>| -pool <value> | -poolName <value>}
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-profile	Geben Sie die ID eines Speicherprofils ein. Die Ausgabe umfasst die Liste der für das angegebene Speicherprofil empfohlenen Laufwerksgruppen.
-pool	Geben Sie die ID eines Pools ein. Die Ausgabe umfasst die Liste der für den angegebenen Speicherpool empfohlenen Laufwerksgruppen.
-poolName	Geben Sie den Namen eines Pools ein. Die Ausgabe umfasst die Liste der für den angegebenen Speicherpool empfohlenen Laufwerksgruppen.

Beispiel 1

Mit dem folgenden Befehl werden die empfohlenen Laufwerksgruppen für Speicherpool pool_1 angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/dg recom -pool pool_1
```

```

Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      ID           = DG_1
      Drive type    = SAS
      Drive size    = 536870912000 (500GB)
      Number of drives = 8
      Allowed numbers of drives = 4,8
      Capacity      = 4398046511104 (4TB)

2:      ID           = DG_2
      Drive type    = SAS
      Drive size    = 268435456000 (250GB)
      Number of drives = 4
      Allowed numbers of drives = 4
      Capacity      = 1099511627776 (1TB)

```

Managen von Speichersystemkapazität-Einstellungen

In der folgenden Tabelle sind die allgemeinen Speichersystemkapazität-Attribute aufgeführt:

Tabelle 106. Attribute für allgemeine Speichersystemkapazität

Merkmale	Beschreibung
Free space	Gibt die Menge an freiem Speicherplatz (verfügbar zur Verwendung) in allen Speicherpools auf dem Speichersystem an.
Used space	Gibt die Menge an Speicherplatz an, der in allen Speicherpools auf dem Speichersystem verwendet wird.
Preallocated space	Für alle Pools im Speichersystem reservierter Speicherplatz. Dieser Speicherplatz ist für zukünftige Anforderungen von Speicherressourcen reserviert, wodurch die Effizienz von Schreibvorgängen gesteigert wird. Jeder Pool kann möglicherweise den vorab zugewiesenen Speicherplatz aus Speicherressourcen zurückgewinnen, wenn die Speicherressourcen nicht den Speicherplatz nutzen und der Poolspeicherplatz knapp wird.
Total space	Gibt die Gesamtmenge des Speicherplatzes (frei und genutzt) in allen Speicherpools auf dem Speichersystem an.
Data Reduction space saved	Gibt die Größe des eingesparten Speichers im gesamten System an, wenn Sie die Datenreduzierung verwenden. i ANMERKUNG: Die Datenreduzierung ist für Thin-LUNs und Thin-Dateisysteme verfügbar. Die Thin-Dateisysteme müssen auf Unity-Systemen erstellt worden sein, auf denen Version 4.2.x oder höher ausgeführt wird.
Data Reduction percent	Gibt den im gesamten System eingesparten Speicher in Prozent an, wenn Sie die Datenreduzierung verwenden. i ANMERKUNG: Die Datenreduzierung ist für Thin-LUNs und Thin-Dateisysteme verfügbar. Die Thin-Dateisysteme müssen auf Unity-Systemen erstellt worden sein, auf denen Version 4.2.x oder höher ausgeführt wird.
Data Reduction ratio	Gibt das Verhältnis der Einsparungen zwischen Daten ohne Datenreduzierung und Daten nach der Datenreduzierung an. i ANMERKUNG: Die Datenreduzierung ist für Thin-LUNs und Thin-Dateisysteme verfügbar. Die Thin-Dateisysteme müssen auf Unity-Systemen erstellt worden sein, auf denen Version 4.2.x oder höher ausgeführt wird.

Anzeigen von Systemkapazitätseinstellungen

Zeigen Sie die aktuellen Speichersystem-Kapazitätseinstellungen an.

Format

```
/stor/general/system show
```

Beispiel

Mit dem folgenden Befehl werden Details zur Speicherkapazität im System angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/general/system show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      Free space           = 4947802324992 (4T)
        Used space          = 4947802324992 (4T)
        Total space         = 9895604649984 (9T)
        Preallocated space  = 60505210880 (56.3G)
        Data Reduction space saved = 4947802324992 (4.5T)
        Data Reduction percent = 50%
        Data Reduction ratio = 1
```

Managen von System-Tier-Kapazitätseinstellungen

In der folgenden Tabelle sind die allgemeinen System-Tier-Kapazitätsattribute aufgeführt:

Tabelle 107. Attribute für allgemeine System-Tier-Kapazität

Merkmale	Beschreibung
Name	Name des Tier. Wählen Sie eine der folgenden Optionen aus: <ul style="list-style-type: none">• Hohe Performance• Performance• Kapazität
Free space	Gibt die Menge des freien Speicherplatzes (verfügbar zur Verwendung) im Tier an.
Used space	Gibt die Menge des Speicherplatzes an, der im Tier verwendet wird.
Total space	Gibt die Gesamtmenge des Speicherplatzes (frei und genutzt) im Tier an.

Anzeigen der System-Tier-Kapazität

Zeigen Sie die aktuellen System-Tier-Kapazitätseinstellungen an.

Format

```
/stor/general/tier show
```

Beispiel

Mit dem folgenden Befehl werden Details zur Storage Tier-Kapazität im System angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/general/tier show -detail
```

```
1:      Name          = Extreme Performance Tier
      Free space     = 4947802324992 (4T)
      Used space    = 4947802324992 (4T)
      Total space   = 9895604649984 (9T)

2:      Name          = Performance Tier
      Free space     = 0
      Used space    = 0
      Total space   = 0

3:      Name          = Capacity Tier
      Free space     = 4947802324992 (4T)
      Used space    = 4947802324992 (4T)
      Total space   = 9895604649984 (9T)
```

Managen von Dateisystemen

Dateisysteme sind logische Container im System, über die den Hosts dateibasierte Speicherressourcen bereitgestellt werden. Sie konfigurieren Dateisysteme auf NAS-Servern, die die Dateisysteme pflegen und managen. Sie erstellen im Dateisystem Netzwerk-Shares, über die angeschlossene Hosts auf den Dateisystemspeicher zugreifen. Bei der Erstellung eines Dateisystems können Sie Unterstützung für die folgenden Netzwerk-Shares aktivieren:

- SMB-Shares (zuvor als CIFS-Shares bezeichnet), die Speicherzugriff für Windows-Hosts bereitstellen.
- NFS (Network File System)-Shares, die Speicherzugriff für Linux-/UNIX-Hosts bereitstellen.

Eine ID identifiziert jedes Dateisystem.

In der folgenden Tabelle sind die Attribute für Dateisysteme aufgeführt:

Tabelle 108. Dateisystemattribute

Attribut	Beschreibung
ID	ID des Dateisystems.
Name	Name des Dateisystems.
Description	Beschreibung des Dateisystems.
Health state	<p>Integritätsstatus des Dateisystems. Der Integritätsstatuscode wird in Klammern angezeigt. Folgende Werte sind möglich:</p> <ul style="list-style-type: none"> ● OK (5): Das Dateisystem funktioniert normal. ● OK_BUT (7): Das Dateisystem funktioniert, aber es ist mindestens eines der folgenden Probleme aufgetreten: <ul style="list-style-type: none"> ○ Die Speicherressource wird initialisiert oder gelöscht. ○ Das Dateisystem für diese Speicherressource reicht in Kürze nicht mehr aus. Weisen Sie der Speicherressource mehr Speicherplatz zu. ● Degraded/Warning (10): Funktioniert, aber es ist mindestens eines der folgenden Probleme aufgetreten: <ul style="list-style-type: none"> ○ Mindestens ein Speicherpool funktioniert nur eingeschränkt. ○ Eine Replikationssitzung für die Speicherressource wird heruntergestuft. ○ Die Kapazitätshöchstgrenze ist nahezu erreicht. Zur Vermeidung von Datenverlusten sollten Sie die Größe des primären Storage erhöhen oder zusätzliche Dateisysteme für die Speicherung der Daten anlegen. Ändern der Dateisystemeinstellungen erläutert, wie die Primärspeichergröße geändert wird. ● Minor failure (15): Es ist mindestens eines der folgenden Ereignisse eingetreten: <ul style="list-style-type: none"> ○ Mindestens ein Speicherpool ist ausgefallen. ○ Der zugehörige NAS-Server ist ausgefallen. ● Major failure (20): Es ist mindestens eines der folgenden Ereignisse eingetreten: <ul style="list-style-type: none"> ○ Mindestens ein Speicherpool ist ausgefallen. ○ Das Dateisystem ist nicht verfügbar. ● Critical failure (25): Es ist mindestens eines der folgenden Ereignisse eingetreten: <ul style="list-style-type: none"> ○ Mindestens ein Speicherpool ist nicht verfügbar. ○ Das Dateisystem ist nicht verfügbar. ○ Die volle Kapazität des Dateisystems ist erreicht. Zur Vermeidung von Datenverlusten sollten Sie die Größe des primären Storage erhöhen oder zusätzliche Dateisysteme für die Speicherung der Daten anlegen. Ändern der Dateisystemeinstellungen erläutert, wie die Primärspeichergröße geändert wird. ● Non-recoverable error (30): Es ist mindestens eines der folgenden Ereignisse eingetreten: <ul style="list-style-type: none"> ○ Mindestens ein Speicherpool ist nicht verfügbar. ○ Das Dateisystem ist nicht verfügbar.
Health details	Zusätzliche Integritätsinformationen. Weitere Informationen zur Integrität finden Sie im Anhang A, Referenz.
File system	Kennung des Dateisystems. Ausgabe einiger Kennzahlbefehle zeigen nur die Dateisystem-ID an. Auf diese Weise können Sie das Dateisystem in der Ausgabe problemlos erkennen.
Server	Name des NAS-Servers, auf dem das Dateisystem gemountet ist.
Storage pool ID	ID des Speicherpools, der vom Dateisystem verwendet wird.
Storage pool	Name des vom Dateisystem verwendeten Speicherpools.
Format	Das Format des Dateisystems. Der Wert lautet UFS64.
Protocol	<p>Das zur Aktivierung von Netzwerk-Shares vom Dateisystem aus verwendete Protokoll. Folgende Werte sind möglich:</p> <ul style="list-style-type: none"> ● nfs: Protokoll für Linux-/Unix-Hosts ● cifs: Protokoll für Windows-Hosts ● multiprotocol: Protokoll für Unix- und Windows-Hosts

Tabelle 108. Dateisystemattribute (fortgesetzt)

Attribut	Beschreibung
Access policy	<p>(Gilt nur für Multiprotokolldateisysteme.) Option für Zugriffs-Policy für das Dateisystem. Folgende Werte sind möglich:</p> <ul style="list-style-type: none"> • <code>native</code> (Standardeinstellung): Wenn diese Policy ausgewählt ist, werden UNIX-Modusbits für UNIX/Linux-Clients und Windows-Berechtigungen (ACLs) für Windows-Clients verwendet. • <code>UNIX</code>: Wenn diese Policy ausgewählt ist, werden Unix-Modusbits verwendet, um den Zugriff auf jede Datei im Dateisystem zu gewähren. • <code>Windows</code>: Wenn diese Policy ausgewählt ist, gelten die Berechtigungen, die unter Windows-ACLs definiert wurden, sowohl für Windows- als auch für Unix/Linux-Clients. (Unix-Modusbits werden ignoriert.)
Folder rename policy	<p>(Gilt nur für Multiprotokolldateisysteme.) Option für die Ordnerumbenennungs-Policy für das Dateisystem. Diese Policy steuert die Bedingungen, unter denen NFS- und SMB-Clients ein Verzeichnis umbenennen können. Folgende Werte sind möglich:</p> <ul style="list-style-type: none"> • <code>forbiddenSmb</code> (Standardeinstellung): Nur NFS-Clients können ohne Einschränkungen Verzeichnisse umbenennen. Ein SMB-Client kann kein Verzeichnis umbenennen, wenn mindestens eine Datei im Verzeichnis oder in einem seiner Unterverzeichnisse geöffnet ist. • <code>allowedAll</code> : Alle NFS- und SMB-Clients können Verzeichnisse ohne Einschränkungen umbenennen. • <code>forbiddenAll</code>: NFS- und SMB-Clients können kein Verzeichnis umbenennen, wenn mindestens eine Datei im Verzeichnis oder in einem seiner Unterverzeichnisse geöffnet ist.
Locking policy	<p>(Gilt nur für Multiprotokolldateisysteme.) Option für Sperr-Policy für das Dateisystem. Diese Policy steuert, ob die NFSv4-Bereichssperre beachtet werden muss. Folgende Werte sind möglich:</p> <ul style="list-style-type: none"> • <code>mandatory</code> (Standardeinstellung): Verwendet die Protokolle KMU und NFSv4, um Bereichssperren für eine Datei zu managen, die von einem anderen Nutzer verwendet wird. Eine obligatorische Sperr-Policy verhindert Datenbeschädigung, wenn gleichzeitig auf dieselben gesperrten Daten zugegriffen werden kann. • <code>advisory</code> : Als Reaktion auf das Sperren von Anfragen wird gemeldet, dass es einen Konflikt bei der Bereichssperre gibt, der Zugriff auf die Datei wird jedoch nicht verhindert. Diese Policy ermöglicht es NFSv2- und NFSv3-Anwendungen, die nicht bereichssperrenkonform sind, die Arbeit fortzusetzen, riskiert jedoch Datenbeschädigung durch gleichzeitige Schreibvorgänge.
Size	Für primäre Daten reservierter Speicher
Size used	Die zurzeit für primäre Daten verwendete Speichermenge.
Maximum size	Maximale Größe, auf die die Kapazität des primären Speichers erweitert werden kann.
Thin provisioning enabled	<p>Gibt an, ob Thin Provisioning aktiviert ist. Der Wert ist <code>yes</code> oder <code>no</code>. Der Standardwert lautet <code>no</code>. Von allen Speicherpools werden mit herkömmlichen und mit Thin Provisioning bereitgestellte Speicherressourcen unterstützt. Bei Standard-Speicherressourcen wird bei der Erstellung der Ressource die gesamte angeforderte Kapazität aus dem Pool zugewiesen. Bei Thin-Provisioning-Speicherressourcen werden immer nur Teile der Kapazität je nach tatsächlicher Nutzung zugewiesen. Da Thin-Provisioning-Speicherressourcen eine höhere Belegung aufweisen können, als ihnen tatsächlich an Speicher zugewiesen ist, ist es möglich, für Speicherpools ein Über-Provisioning festzulegen, damit die Pools eine höhere Speicherkapazität unterstützen können, als sie aufweisen.</p> <p> ANMERKUNG: In der Unisphere-Onlinehilfe erfahren Sie mehr zu Thin Provisioning.</p>
Data Reduction enabled	<p>Gibt an, ob die Datenreduzierung für dieses Thin-Dateisystem aktiviert ist. Gültige Werte:</p> <ul style="list-style-type: none"> • <code>yes</code> • <code>no</code> (Standard) <p> ANMERKUNG: Die Thin-Dateisysteme müssen auf Unity-Systemen erstellt worden sein, auf denen Version 4.2.x oder höher ausgeführt wird.</p>
Data Reduction space saved	Eingesparter Gesamt Speicherplatz für dieses Thin-Dateisystem (in Gigabyte) durch Datenreduzierung.

Tabelle 108. Dateisystemattribute (fortgesetzt)

Attribut	Beschreibung
	<p>i ANMERKUNG: Die Thin-Dateisysteme müssen auf Unity-Systemen erstellt worden sein, auf denen Version 4.2.x oder höher ausgeführt wird.</p>
Data Reduction percent	<p>Eingesparter Gesamt-Storage für das Thin-Dateisystem (in Prozent) durch Datenreduzierung.</p> <p>i ANMERKUNG: Die Thin-Dateisysteme müssen auf Unity-Systemen erstellt worden sein, auf denen Version 4.2.x oder höher ausgeführt wird.</p>
Data Reduction ratio	<p>Verhältnis der Einsparungen zwischen Daten ohne Datenreduzierung und Daten nach der Datenreduzierung.</p> <p>i ANMERKUNG: Die Datenreduzierung ist für Thin-Dateisysteme verfügbar. Die Thin-Dateisysteme müssen auf Unity-Systemen erstellt worden sein, auf denen Version 4.2.x oder höher ausgeführt wird.</p>
Advanced deduplication enabled	<p>Gibt an, ob für dieses Dateisystem die erweiterte Deduplizierung aktiviert ist. Diese Option ist erst verfügbar, wenn die Datenreduzierung aktiviert wurde. Ein leerer Wert weist darauf hin, dass die erweiterte Deduplizierung für das Dateisystem nicht unterstützt wird. Gültige Werte:</p> <ul style="list-style-type: none"> • yes • no (Standard) <p>i ANMERKUNG: Die Thin-Dateisysteme müssen auf einem Unity-System erstellt werden, auf dem Version 4.2.x oder höher ausgeführt wird. Erweiterte Deduplizierung ist nur verfügbar auf:</p> <ul style="list-style-type: none"> • Dynamischen oder herkömmlichen Pools in Unity 380F-, 480F-, 680F- und 880F-Systemen • Dynamische Pools in Unity-All-Flash 450F-, 550F- und 650F-Systemen • All-Flash-Pools und Hybrid-Flash-Pools in Unity Hybrid-Systemen 380, 480, 680 und 880
Current allocation	<p>Wenn diese Option aktiviert ist, wird hier angezeigt, wie viel primärer Speicher zurzeit über Thin Provisioning bereitgestellt wird.</p>
Total pool space preallocated	<p>Der Speicherplatz, der für zukünftige Zwecke im Pool für das Dateisystem reserviert ist, um Schreibvorgänge effizienter zu gestalten. Der Pool kann möglicherweise einen Teil dieses Speicherplatzes zurückgewinnen, wenn nur noch wenig Poolspeicherplatz frei ist.</p>
Total pool space used	<p>Gesamter Poolspeicherplatz, den das Dateisystem im Pool einnimmt. Dazu gehören der zugewiesene Speicherplatz und Zuweisungen für Snapshots und Overhead. Dazu gehört nicht der vorab zugewiesene Speicherplatz.</p>
Minimum size allocated	<p>(Wird angezeigt für Dateisysteme, die auf einem Unity-System mit OE-Version 4.1 erstellt wurden.) Mindestmenge von durch Thin Provisioning zugeordnetem primären Speicher. Dateiverkleinerungsvorgänge können die Dateisystemgröße nicht unter diesen Wert reduzieren.</p>
Protection size used	<p>Aktuell mit Schutzdaten belegter Speicher.</p>
Protection schedule	<p>ID eines angewendeten Schutzplans. Anzeigen von Schutzplänen erläutert, wie Sie die IDs der Pläne im System anzeigen können.</p>
Protection schedule paused	<p>Gibt an, ob ein angewendeter Schutzplan zurzeit ausgesetzt ist. Gültige Werte sind „yes“ und „no“.</p>
FAST VP policy	<p>FAST VP-Tiering Policy für das Dateisystem. Diese Policy definiert sowohl die anfängliche Tier-Positionierung als auch das laufende automatisierte Tiering von Daten während den Datenverlagerungsvorgängen. Gültige Werte (nicht unterschieden nach Groß- und Kleinschreibung):</p> <ul style="list-style-type: none"> • startHighThenAuto (Standardeinstellung): Legt die anfängliche Datenplatzierung auf die Laufwerke mit der höchsten Performance und freiem Speicherplatz fest und verlagert dann Teile der Daten der Storage-Ressource basierend auf der I/O-Aktivität. • auto: Legt die anfängliche Datenplatzierung auf eine optimale, vom System bestimmte Einstellung fest und verlagert dann Teile der Daten der Speicherressource basierend auf Performancestatistiken der Speicherressource, sodass die Daten entsprechend der I/O-Aktivität auf die Tiers verlagert werden.

Tabelle 108. Dateisystemattribute (fortgesetzt)

Attribut	Beschreibung
	<ul style="list-style-type: none"> • highest: Legt die anfängliche Datenplatzierung und nachfolgende Datenverlagerung (falls zutreffend) auf die Laufwerke mit der höchsten Performance und freiem Speicherplatz fest. • lowest: legt die anfängliche Datenplatzierung und nachfolgende Datenverlagerung (falls zutreffend) auf die kosteneffizientesten Laufwerke mit freiem Speicherplatz fest.
FAST VP distribution	<p>Prozentsatz des Dateisystemspeichers, der jedem Tier zugewiesen ist. Das Format lautet wie folgt:</p> <pre><tier_name>:<value>%</pre> <p>Hierbei gilt:</p> <ul style="list-style-type: none"> • <code><tier_name></code> ist der Name des Storage Tier. • <code><value></code> ist der Prozentsatz des Storage in diesem Tier.
CIFS synchronous write	<p>Gibt an, ob die Option für synchrone SMB-Schreibvorgänge aktiviert ist. Der Wert ist <code>yes</code> oder <code>no</code>.</p> <ul style="list-style-type: none"> • Die Option für synchrone SMB-Schreibvorgänge bietet erweiterten Support für Anwendungen, in denen Datenbankdateien auf Windows-Netzwerk-Shares gespeichert und abgerufen werden. Bei den meisten SMB-Dateisystemen erfolgen Lesevorgänge synchron und Schreibvorgänge asynchron. Wenn Sie die Option für synchrone SMB-Schreibvorgänge für ein Windows (SMB)-Dateisystem aktivieren, werden die Schreibvorgänge beim Speichern im System sofort synchron durchgeführt – unabhängig davon, welcher Schreibvorgang im SMB-Protokoll festgelegt ist. • Durch die Aktivierung synchroner Schreibvorgänge können Sie Datenbankdateien (z. B. MySQL) auf SMB-Netzwerk-Shares speichern und darauf zugreifen. Diese Option sorgt dafür, dass sämtliche Schreibvorgänge auf den Freigaben synchron ablaufen. Damit sinkt das Risiko eines Datenverlusts oder einer Datenbeschädigung unter verschiedenen Szenarien, wie beispielsweise einem Stromausfall. <p>i ANMERKUNG: Synchrone SMB-Schreibvorgänge sollten nur aktiviert werden, wenn Sie die Windows-Dateisysteme als Speicher für Datenbankanwendungen einsetzen möchten.</p> <p>Weitere Informationen zu synchronen SMB-Schreibvorgängen finden Sie in der Unisphere-Onlinehilfe.</p>
CIFS oplocks	<p>Gibt an, ob Opportunistic File Locks (oplocks) für SMB-Netzwerk-Shares aktiviert sind. Der Wert ist <code>yes</code> oder <code>no</code>.</p> <ul style="list-style-type: none"> • Mit oplocks können SMB-Clients Dateidaten lokal zwischenspeichern, bevor sie sie an einen Server senden. SMB-Clients können anschließend lokal mit den Dateien arbeiten und regelmäßig Änderungen an das System weiterleiten. In diesem Fall muss nicht jede einzelne Operation über das Netzwerk übertragen werden. • Diese Funktion ist für Windows(SMB)-Dateisysteme standardmäßig aktiviert. Solange mit der Anwendung keine kritischen Daten verarbeitet werden oder andere konkrete Gründe gegen diesen Modus sprechen, sollte oplocks aktiviert bleiben. <p>Weitere Informationen zu CIFS-oplocks finden Sie in der Unisphere-Onlinehilfe.</p>
CIFS notify on write	<p>Gibt an, ob Schreibenbenachrichtigungen für SMB-Netzwerk-Shares aktiviert sind. Der Wert ist <code>yes</code> oder <code>no</code>. Bei Aktivierung erhalten Windows-Anwendungen eine Benachrichtigung, wenn ein Nutzer in eine Datei auf der KMU-Freigabe schreibt oder Änderungen vornimmt.</p> <p>i ANMERKUNG: Falls diese Option aktiviert ist, geht aus dem Wert für die KMU-Verzeichnistiefe die niedrigste Verzeichnisebene für die Benachrichtigungseinstellungen hervor.</p>
CIFS notify on access	<p>Gibt an, ob Dateizugriffsbenachrichtigungen für SMB-Shares aktiviert sind. Der Wert ist <code>yes</code> oder <code>no</code>. Bei Aktivierung erhalten Windows-Anwendungen eine Benachrichtigung, wenn ein Nutzer auf eine Datei auf der KMU-Freigabe zugreift.</p> <p>i ANMERKUNG: Falls diese Option aktiviert ist, geht aus dem Wert für die KMU-Verzeichnistiefe die niedrigste Verzeichnisebene für die Benachrichtigungseinstellungen hervor.</p>

Tabelle 108. Dateisystemattribute (fortgesetzt)

Attribut	Beschreibung
CIFS directory depth	Hier wird die zulässige Unterverzeichnistiefe für Dateibenachrichtigungen bei Schreib- und Zugriffsbenachrichtigungen auf SMB-Netzwerk-Shares festgelegt. Der Wert kann zwischen 1 und 512 eingestellt werden. Der Standardwert lautet 512.
Replication type	Gibt an, an welcher Art von asynchroner Replikation dieses Dateisystem teilnimmt. Gültige Werte: <ul style="list-style-type: none"> • none • local • remote
Synchronous replication type	Gibt an, an welcher Art von synchroner Replikation dieses Dateisystem teilnimmt. Gültige Werte: <ul style="list-style-type: none"> • none • remote
Replication destination	Gibt an, ob die Speicherressource ein Ziel für eine Replikationssitzung (lokal oder remote) ist. Gültige Werte: <ul style="list-style-type: none"> • yes • no
Migration destination	Gibt an, ob die Speicherressource ein Ziel für eine NAS-Importsitzung ist. Gültige Werte: <ul style="list-style-type: none"> • yes • no
Creation time	Datum und Uhrzeit der Dateisystemerstellung.
Last modified time	Datum und Uhrzeit der letzten Änderung der Dateisystemeinstellungen.
Snapshot count	Anzahl der im Dateisystem erstellten Snapshots.
Pool full policy	Zu befolgende Policy, wenn der Pool voll ist und es versucht wird, in das Dateisystem zu schreiben. Dieses Attribut ermöglicht es Ihnen, Snapshots auf dem Dateisystem beizubehalten, wenn ein Pool voll ist. Gültige Werte: <ul style="list-style-type: none"> • <code>Delete All Snaps</code> (Standardeinstellung für Thick-Dateisysteme): Snapshots, die mit dem Dateisystem verknüpft sind, werden gelöscht, wenn der Pool die volle Kapazität erreicht. • <code>Fail Writes</code> (Standardeinstellung für Thin-Dateisysteme): Schreibvorgänge an das System schlagen fehl, wenn der Pool die volle Kapazität erreicht. <p> ANMERKUNG: Dieses Attribut ist nur für vorhandene Dateisysteme verfügbar. Sie können dieses Attribut nicht festlegen, wenn Sie ein Dateisystem erstellen.</p>
Event publishing protocols	Liste der Dateisystem-Zugriffsprotokolle, die für die Ereignisveröffentlichung aktiviert sind. Standardmäßig ist die Liste leer. Gültige Werte: <ul style="list-style-type: none"> • <code>nfs</code>: Aktivieren Sie die Ereignisveröffentlichung für NFS. • <code>cifs</code>: Aktiviert die Ereignisveröffentlichung für SMB (CIFS).
FLR mode	Gibt an, welche FLR-Verison (File-Level Retention) aktiviert ist. Mögliche Werte sind: <ul style="list-style-type: none"> • <code>enterprise</code> • <code>compliance</code> • <code>disabled</code>
FLR has protected files	Gibt an, ob das Dateisystem geschützte Dateien enthält. Mögliche Werte sind: <ul style="list-style-type: none"> • <code>yes</code> • <code>no</code>
FLR clock time	Zeigt die Uhrzeit des Dateisystems an, um das Aufbewahrungsdatum nachzuverfolgen. Beispiel: 2019-02-20 12:55:32.
FLR max retention date	Maximales Datum und maximale Uhrzeit, die bzw. das für eine gesperrte Datei in einem FLR-fähigen Dateisystem festgelegt wurde. 2020-09-20 11:00:00
FLR min retention period	Gibt die kürzeste Aufbewahrungsfrist an, in der die Dateien in einem FLR-fähigen Dateisystem gesperrt und vor Löschung geschützt werden können. Das Format lautet (<code><integer> d m y</code>) <code>infinite</code> . Mögliche Werte sind:

Tabelle 108. Dateisystemattribute (fortgesetzt)

Attribut	Beschreibung
	<ul style="list-style-type: none"> • d: days • m: months • y: years (die Standardeinstellung ist 1 Tag 1d) • infinite <p>Alle begrenzten Werte plus das aktuelle Datum müssen unter der maximalen Aufbewahrungsfrist bis 7. Februar 2106 liegen.</p>
<p>FLR default retention period</p>	<p>Gibt die Standardaufbewahrungsfrist an, die in einem FLR-fähigen Dateisystem verwendet wird, wenn eine Datei gesperrt ist und keine Aufbewahrungsfrist auf Dateiebene angegeben wurde.</p> <p>Das Format lautet (<integer> d m y) infinite. Mögliche Werte sind:</p> <ul style="list-style-type: none"> • d: days • m: months • y: years (FLR-C compliance, Standardeinstellung ist 1 Jahr 1y) • infinite (FLR-E enterprise, Standardeinstellung) <p>Alle begrenzten Werte plus das aktuelle Datum müssen unter der maximalen Aufbewahrungsfrist bis 7. Februar 2106 liegen.</p>
<p>FLR max retention period</p>	<p>Gibt die längste Aufbewahrungsfrist an, in der die Dateien in einem FLR-fähigen Dateisystem gesperrt und vor Löschung geschützt werden können. Mögliche Werte sind:</p> <ul style="list-style-type: none"> • d: days • m: months • y: years • infinite (Standard) <p>Der Wert darf nicht größer als 1 Tag sein. Alle begrenzten Werte plus das aktuelle Datum müssen unter der maximalen Aufbewahrungsfrist bis 7. Februar 2106 liegen.</p>
<p>FLR auto lock enabled</p>	<p>Gibt an, ob alle Dateien in einem FLR-fähigen Dateisystem automatisch gesperrt werden sollen. Mögliche Werte sind:</p> <ul style="list-style-type: none"> • yes • no
<p>FLR auto delete enabled</p>	<p>Gibt an, ob gesperrte Dateien in einem FLR-fähigen Dateisystem automatisch gelöscht werden sollen, sobald die Aufbewahrungsfrist abgelaufen ist. Mögliche Werte sind:</p> <ul style="list-style-type: none"> • yes • no <p>i ANMERKUNG: Das System sucht alle sieben Tage nach abgelaufenen Dateien und löscht diese automatisch, wenn die automatische Löschfunktion aktiviert ist. Die siebentägige Frist beginnt am Tag nach der Aktivierung der automatischen Löschfunktion auf dem Dateisystem.</p>
<p>FLR policy interval</p>	<p>Wenn die automatische Sperrfunktion für neue Dateien aktiviert ist, gibt dies ein Zeitintervall an, wie lange nach der Änderung von Dateien gewartet werden soll, bevor sie automatisch in einem FLR-aktivierten Dateisystem gesperrt werden.</p> <p>Das Format ist <value><qualifier>, wobei der Wert eine Ganzzahl ist und der Qualifizierer folgenden Wert hat:</p> <ul style="list-style-type: none"> • m: Minuten • h: Stunden • d--days <p>Der Wert sollte größer als 1 Minute sein und weniger als 366 Tage betragen.</p>
<p>Error Threshold</p>	<p>Gibt den Schwellenwert für belegten Speicherplatz im Dateisystem als Prozentsatz an. Bei Überschreitung werden Fehlerwarnmeldungen erzeugt. Der Standardwert ist 95 %. Wenn der Schwellenwert auf 0 festgelegt ist, wird diese Warnmeldung deaktiviert. Diese Option muss auf einen Wert festgelegt werden, der größer ist als der Schwellenwert für Warnmeldung und Info.</p>

Tabelle 108. Dateisystemattribute (fortgesetzt)

Attribut	Beschreibung
Warning Threshold	Gibt den Schwellenwert für belegten Speicherplatz im Dateisystem als Prozentsatz an. Bei Überschreitung werden Warnmeldungen erzeugt. Der Standardwert ist 75 %. Wenn der Schwellenwert auf 0 festgelegt ist, wird diese Warnmeldung deaktiviert. Diese Option muss auf einen Wert festgelegt werden, der kleiner ist als der Fehlerschwellenwert und größer als oder gleich dem Info-Schwellenwert.
Info Threshold	Gibt den Schwellenwert für belegten Speicherplatz im Dateisystem als Prozentsatz an. Bei Überschreitung werden Informationswarnmeldungen erzeugt. Der Standardwert ist 0 (deaktiviert). Diese Option muss auf einen Wert festgelegt werden, der kleiner ist als der Schwellenwert für die Warnmeldung.

Erstellen von Dateisystemen

Erstellen Sie ein Multiprotokoll-Dateisystem, NFS-Dateisystem oder CIFS (SMB)-Dateisystem. Für jeden Share-Typ (NFS oder CIFS), den Sie erstellen möchten, muss ein Dateisystem erstellt werden. Sobald Sie ein Dateisystem erstellt haben, können Sie die NFS- bzw. CIFS-Netzwerk-Shares erstellen und anhand der ID des Dateisystems mit einer Share verknüpfen.

 **ANMERKUNG:** Größenqualifizierer bietet Einzelheiten zur Verwendung von Qualifizierern zur Angabe der Speichergröße.

Voraussetzungen

- Konfigurieren Sie mindestens einen Speicherpool für das Dateisystem und weisen Sie dem Pool mindestens ein Laufwerk zu. [Konfigurieren benutzerdefinierter Pools](#) erklärt, wie Sie benutzerdefinierte Pools erstellen.
- Konfigurieren Sie mindestens einen NAS-Server, der dem Dateisystem zugewiesen werden kann. [Erstellen eines NAS-Servers](#) erläutert die Konfiguration von NAS-Servern.

Format

```
/stor/prov/fs create [-async] -name <value> [-descr <value>] {-server <value> | -serverName <value>} {-pool <value> | -poolName <value>} -size <value> [-thin {yes | no}] [-dataReduction {yes [-advancedDedup {yes | no}] | no}] [-minSizeAllocated <value>] -type {{nfs | cifs | multiprotocol [-accessPolicy {native | Windows | Unix}] [-folderRenamePolicy {allowedAll | forbiddenSmb | forbiddenAll}] [-lockingPolicy {advisory | mandatory}]} [-cifsSyncWrites {yes | no}] [-cifsOpLocks {yes | no}] [-cifsNotifyOnWrite {yes | no}] [-cifsNotifyOnAccess {yes | no}] [-cifsNotifyDirDepth <value>] | nfs} [-fastvpPolicy {startHighThenAuto | auto | highest | lowest}] [-sched <value> [-schedPaused {yes | no}]] [-replDest {yes | no}][{-eventProtocols <value>} [-flr {disabled | {enterprise | compliance} [-flrMinRet <value>] [-flrDefRet <value>] [-flrMaxRet <value>}]]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.
-name	Geben Sie einen Namen für das Dateisystem ein.
-descr	Geben Sie eine kurze Beschreibung des Dateisystems ein.
-server	Geben Sie die ID des NAS-Servers ein, der der übergeordnete NAS-Server für das Dateisystem sein wird. Anzeigen von NAS-Servern erläutert, wie Sie die IDs der NAS-Server im System anzeigen können.
-serverName	Geben Sie den Namen des NAS-Servers ein, der als übergeordneter NAS-Server für das Dateisystem dient.
-pool	Geben Sie die ID des Pools ein, der für das Dateisystem verwendet werden soll.

Qualifizierer	Beschreibung
-poolName	Geben Sie den Namen des Pools ein, der für das Dateisystem verwendet werden soll. Bei diesem Wert wird die Groß-/Kleinschreibung nicht beachtet. Anzeigen von Pools erläutert, wie Sie die Namen der Speicherpools im System anzeigen können.
-size	Geben Sie ein, wie viel Speicher für das Dateisystem reserviert werden soll.
-thin	Hiermit wird Thin Provisioning auf dem Dateisystem aktiviert. Gültige Werte: <ul style="list-style-type: none"> • yes (Standard) • no
-dataReduction	Geben Sie an, ob eine Datenreduzierung für das Thin-Dateisystem aktiviert ist. Gültige Werte: <ul style="list-style-type: none"> • yes (Standard) • no <p>i ANMERKUNG: Die Thin-Dateisysteme müssen auf Unity-Systemen erstellt worden sein, auf denen Version 4.2.x oder höher ausgeführt wird.</p>
-advancedDedup	Gibt an, ob die erweiterte Deduplizierung für das Thin-Dateisystem aktiviert ist. Diese Option ist erst verfügbar, wenn die Datenreduzierung aktiviert wurde. Gültige Werte: <ul style="list-style-type: none"> • yes • no (Standard) <p>i ANMERKUNG: Die Thin-Dateisysteme müssen auf einem Unity-System erstellt werden, auf dem Version 4.2.x oder höher ausgeführt wird. Erweiterte Deduplizierung ist nur verfügbar auf:</p> <ul style="list-style-type: none"> • Dynamischen oder herkömmlichen Pools in Unity 380F-, 480F-, 680F- und 880F-Systemen • Dynamische Pools in Unity-All-Flash 450F-, 550F- und 650F-Systemen • All-Flash-Pools und Hybrid-Flash-Pools in Unity Hybrid-Systemen 380, 480, 680 und 880
-minSizeAllocated	(Option verfügbar auf einem Unity-System mit OE-Version 4.1.) Geben Sie die minimale Größe an, die dem Thin-Dateisystem zugewiesen werden soll. Automatische und manuelle Dateiverkleinerungsvorgänge können die Dateisystemgröße nicht unter diesen Wert reduzieren. Der Standardwert ist 3 GB, die minimale Größe des Thin-Dateisystems.
-type	Geben Sie an, welche Art von Netzwerk-Freigabe vom Dateisystem exportiert werden soll. Gültige Werte: <ul style="list-style-type: none"> • nfs : Netzwerk-Shares für Linux-/UNIX-Hosts • cifs : Netzwerk-Shares für Windows-Hosts • multiprotocol : Netzwerk-Shares für Multiprotokoll-Shares
-accessPolicy	(Gilt nur für Multiprotokolldateisysteme) Geben Sie die Zugriffs-Policy für dieses Dateisystem an. Gültige Werte: <ul style="list-style-type: none"> • native (Standard) • unix • windows
-folderRenamePolicy	(Gilt nur für Multiprotokolldateisysteme) Geben Sie die Umbenennungs-Policy für das Dateisystem an. Gültige Werte: <ul style="list-style-type: none"> • forbiddenSMB (Standard) • allowedAll • forbiddenAll
-lockingPolicy	(Gilt nur für Multiprotokolldateisysteme.) Geben Sie die Sperr-Policy für das Dateisystem an. Gültige Werte: <ul style="list-style-type: none"> • mandatory (Standard) • advisory
-cifsSyncWrites	Hiermit werden synchrone Schreibvorgänge für CIFS-Netzwerk-Shares aktiviert. Gültige Werte: <ul style="list-style-type: none"> • yes • no (Standard)
-cifsOpLocks	Hiermit werden Opportunistic File Locks (oplocks) für CIFS-Netzwerk-Shares aktiviert. Gültige Werte: <ul style="list-style-type: none"> • yes (Standard) • no

Qualifizierer	Beschreibung
-cifsNotifyOnWrite	Hiermit wird der Empfang von Benachrichtigungen bei Schreibvorgängen in einer CIFS-Share aktiviert. Gültige Werte: <ul style="list-style-type: none"> • yes • no (Standard)
-cifsNotifyOnAccess	Hiermit wird der Empfang von Benachrichtigungen bei Zugriffen auf einer CIFS-Share aktiviert. Gültige Werte: <ul style="list-style-type: none"> • yes • no (Standard)
-cifsNotifyDirDepth	Falls der Wert für -cifsNotifyOnWrite oder -cifsNotifyOnAccessyes (aktiviert) lautet, geben Sie die Unterverzeichnistiefe an, bis zu der die Benachrichtigungen gelten sollen. Zulässige Werte sind 1 bis 512. Der Standardwert lautet 512.
-folderRenamePolicy	Geben Sie dies zum Umbenennen des Policy-Typs für das angegebene Dateisystem an. Gültige Werte: <ul style="list-style-type: none"> • allowedAll • forbiddenSmb (Standard) • forbiddenAll
-lockingPolicy	Legen Sie die Sperr-Policy für diesen Typ des Dateisystems fest. Gültige Werte: <ul style="list-style-type: none"> • advisory • mandatory (Standard)
-fastvpPolicy	Geben Sie die FAST VP-Tiering Policy für das Dateisystem an. Diese Policy definiert sowohl die anfängliche Tier-Positionierung als auch das laufende automatisierte Tiering von Daten während den Datenverlagerungsvorgängen. Gültige Werte (nicht unterschieden nach Groß- und Kleinschreibung): <ul style="list-style-type: none"> • startHighThenAuto (Standardeinstellung): Legt die anfängliche Datenplatzierung auf die Laufwerke mit der höchsten Performance und freiem Speicherplatz fest und verlagert dann Teile der Daten der Storage-Ressource basierend auf der I/O-Aktivität. • auto : Legt die anfängliche Datenplatzierung auf eine optimale, vom System bestimmte Einstellung fest und verlagert dann Teile der Daten der Storage-Ressource basierend auf Performancestatistiken der Storage-Ressource, sodass die Daten entsprechend der I/O-Aktivität auf die Tiers verlagert werden. • highest : Legt die anfängliche Datenplatzierung und nachfolgende Datenverlagerung (falls zutreffend) auf die Laufwerke mit der höchsten Performance und freiem Speicherplatz fest. • lowest : legt die anfängliche Datenplatzierung und nachfolgende Datenverlagerung (falls zutreffend) auf die kosteneffizientesten Laufwerke mit freiem Speicherplatz fest.
-sched	Geben Sie die ID eines Schutzplans ein, der auf die Speicherressource angewendet werden soll. Anzeigen von Schutzplänen erläutert, wie Sie die IDs der Pläne im System anzeigen können.
-schedPaused	Geben Sie an, ob der für -sched angegebene Schutzplan ausgesetzt werden soll. Gültige Werte: <ul style="list-style-type: none"> • yes • no
-replDest	Gibt an, ob die Ressource ein Replikationsziel ist. Gültige Werte: <ul style="list-style-type: none"> • yes • no (Standard)
-eventProtocols	Gibt die durch Kommas getrennte Liste der Dateisystem-Zugriffsprotokolle an, die für die Ereignisveröffentlichung aktiviert sind. Standardmäßig ist die Liste leer. Gültige Werte: <ul style="list-style-type: none"> • nfs — Aktivieren Sie die Ereignisveröffentlichung für NFS. • cifs — Aktivieren Sie die Ereignisveröffentlichung für CIFS (SMB).
-flr	Gibt an, ob die Aufbewahrung auf Dateiebene (File-Level Retention, FLR) aktiviert ist und wenn ja, welche FLR-Version verwendet wird. Gültige Werte: <ul style="list-style-type: none"> • enterprise — Geben Sie an, um FLR-E zu aktivieren. • compliance — Geben Sie an, um FLR-C zu aktivieren. • disabled (Standard) — Geben Sie an, um FOR zu deaktivieren.
-flrMinRet	Gibt die kürzeste Aufbewahrungsfrist an, in der die Dateien in einem FLR-fähigen Dateisystem gesperrt und vor Löschung geschützt werden können. Gültige Werte:

Qualifizierer	Beschreibung
	<ul style="list-style-type: none"> • d: days (die Standardeinstellung ist 1 Tag 1d) • m: months • y: years • infinite
-flrDefRet	<p>Gibt die Standardaufbewahrungsfrist an, die in einem FLR-fähigen Dateisystem verwendet wird, wenn eine Datei gesperrt ist und keine Aufbewahrungsfrist auf Dateiebene angegeben wurde.</p> <p>Das Format lautet (<integer> d m y) infinite.</p> <ul style="list-style-type: none"> • d: days • m: months • y: years — FLR-C (compliance) Standard ist 1 Jahr--1y) • infinite — FLR-E (enterprise) Standard <p>Alle begrenzten Werte plus das aktuelle Datum müssen unter der maximalen Aufbewahrungsfrist bis 7. Februar 2106 liegen.</p> <p>Der Wert dieses Parameters muss größer sein als die Mindestaufbewahrungsdauer -flrMinRet.</p>
-flrMaxRet	<p>Gibt das maximale Datum und die maximale Uhrzeit an, die bzw. das für eine gesperrte Datei in einem FLR-fähigen Dateisystem festgelegt wurde. Mögliche Werte sind:</p> <ul style="list-style-type: none"> • d: days • m: months • y: years • infinite (Standard) <p>Der Wert darf nicht größer als 1 Tag sein. Alle begrenzten Werte plus das aktuelle Datum müssen unter der maximalen Aufbewahrungsfrist bis 7. Februar 2106 liegen.</p> <p>Der Wert dieses Parameters muss größer sein als die standardmäßige Aufbewahrungsfrist -flrDefRet.</p>

Beispiel

Mit dem folgenden Befehl wird ein Dateisystem mit den folgenden Einstellungen erstellt:

- Name: FileSystem01
- Die Beschreibung lautet „Multiprotocol file system“.
- Nutzt den Kapazitätsspeicherpool.
- Verwendet den NAS-Server „nas_2“ als übergeordneten NAS-Server.
- Größe des primären Speichers: 3 GB
- Unterstützt die Multiprotokoll-Netzwerkfreigaben.
- Verfügt über eine native Zugriffs-Policy.
- Ist ein Replikationsziel.

Das Dateisystem erhält die ID res_28:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/fs create -name FileSystem01
-descr "Multiprotocol file system" -server nas_2 -pool capacity -size 3G -type multiprotocol
-accessPolicy native -replDest yes
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = res_28
Operation completed successfully.
```

Anzeigen von Dateisystemen

Zeigen Sie Details zu einem Dateisystem an. Sie können nach der Dateisystem-ID filtern.

 **ANMERKUNG:** Aktionsbefehl „show“ erläutert, wie das Ausgabeformat geändert wird.

Format

```
/stor/prov/fs [{-id <value> | -name <value> | -server <value> | -serverName <value>}] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID eines Dateisystems ein.
-name	Geben Sie den Namen eines Dateisystems ein.
-server	Geben Sie die ID des NAS-Servers ein, für den die Dateisysteme angezeigt werden.
-serverName	Geben Sie den Namen des NAS-Servers ein, für den die Dateisysteme angezeigt werden.

Beispiel 1

Mit dem folgenden Befehl werden Details zu sämtlichen Dateisystemen im Speichersystem aufgeführt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/fs show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:   ID           = SF_1
     Name        = MyFS
     Description  = my file system
     Health state = OK (5)
     File system  = fs_1
     Server       = SFS_1
     Storage pool = Performance
     Format       = UFS64
     Protocol     = nfs
     Access policy = native
     Folder rename policy = allowedAll
     Locking policy = advisory
     Size         = 1099511627776 (1T)
     Size used    = 128849018880 (120G)
     Maximum size = 281474976710656 (256.0T)
     Protection size used = 1099511627776 (1T)
```

Beispiel 2

Mit dem folgenden Befehl werden Details zu sämtlichen Dateisystemen im Speichersystem aufgeführt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/fs -serverName MyNAS_1 show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:   ID           = SF_1
     Name        = MyFS
     Description  = my file system
     Health state = OK (5)
     File system  = fs_1
     Server       = nas_1
     Storage pool = Performance
```

```

Format                = UFS64
Protocol              = nfs
Access policy        = native
Folder rename policy = allowedAll
Locking policy       = advisory
Size                 = 1099511627776 (1T)
Size used            = 128849018880 (120G)
Maximum size        = 281474976710656 (256.0T)
Protection size used = 1099511627776 (1T)

2:  ID                = SF_2
    Name              = MyFS_2
    Description       = my file system
    Health state      = OK (5)
    File system       = fs_2
    Server            = nas_1
    Storage pool      = Performance
    Format            = UFS64
    Protocol          = nfs
    Access policy     = native
    Folder rename policy = allowedAll
    Locking policy    = advisory
    Size              = 1099511627776 (1T)
    Size used         = 128849018880 (120G)
    Maximum size     = 281474976710656 (256.0T)
    Protection size used = 1099511627776 (1T)

```

Ändern der Dateisystemeinstellungen

Ändern Sie die Einstellungen für ein Dateisystem.

ANMERKUNG: Größenqualifizierer erläutert die Verwendung der Größenqualifizierer bei der Festlegung der Speichergröße.

Format

```

/stor/prov/fs {-id <value> | -name <value>} set [-async] [-descr <value>] [-accessPolicy
{native | Unix | Windows}] [-folderRenamePolicy {allowedAll | forbiddenSmb | forbiddenAll}]
[-lockingPolicy {advisory | mandatory}] [-size <value>] [-minSizeAllocated <value>] [-
dataReduction {yes [-advancedDedup {yes | no}] | no}] [-cifsSyncWrites {yes | no}] [-
fastvpPolicy {startHighThenAuto | auto | highest | lowest | none}] [-cifsOpLocks {yes |
no}] [-cifsNotifyOnWrite {yes | no}] [-cifsNotifyOnAccess {yes | no}] [-cifsNotifyDirDepth
<value>] [{-sched <value> | -noSched}] [-schedPaused {yes | no}] [-replDest {yes | no}]
[-poolFullPolicy {deleteAllSnaps | failWrites}] [-eventProtocols <value>] [-flr [-flrMinRet
<value>] [-flrDefRet <value>] [-flrMaxRet <value>] [-flrAutoLock {yes | no}] [-flrAutoDelete
{yes | no}] [-flrPolicyInterval <value>]] [-errorThreshold <value>] [-warningThreshold <value>]
[-infoThreshold <value>]

```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des zu ändernden Dateisystems ein.
-name	Geben Sie den Namen des zu ändernden Dateisystems ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.
-descr	Geben Sie eine kurze Beschreibung des Dateisystems ein.

Qualifizierer	Beschreibung
-accessPolicy	(Gilt nur für Multiprotokolldateisysteme.) Geben Sie die Zugriffs-Policy für das Dateisystem an. Gültige Werte: <ul style="list-style-type: none"> • native • unix • windows
-folderRenamePolicy	(Gilt nur für Multiprotokolldateisysteme.) Geben Sie die Umbenennungs-Policy für das Dateisystem an. Gültige Werte: <ul style="list-style-type: none"> • forbiddenSMB (Standard) • allowedAll • forbiddenAll
-lockingPolicy	(Gilt nur für Multiprotokolldateisysteme.) Geben Sie die Sperr-Policy für das Dateisystem an. Gültige Werte: <ul style="list-style-type: none"> • mandatory (Standard) • advisory
-size	Geben Sie ein, wie viel Poolspeicher für das Dateisystem reserviert werden soll.
-minSizeAllocated	(Option verfügbar auf einem Unity-System mit OE-Version 4.1.) Geben Sie die minimale Größe an, die dem Thin-Dateisystem zugewiesen werden soll. Automatische und manuelle Dateiverkleinerungsvorgänge können die Dateisystemgröße nicht unter diesen Wert reduzieren. Der Standardwert ist 3 GB, die minimale Größe des Thin-Dateisystems.
-dataReduction	Aktivieren der Datenreduzierung auf dem Thin-Dateisystem. Gültige Werte: <ul style="list-style-type: none"> • yes • no <p> ANMERKUNG: Die Thin-Dateisysteme müssen auf Unity-Systemen erstellt worden sein, auf denen Version 4.2.x oder höher ausgeführt wird.</p>
-advancedDedup	Aktiviert die erweiterte Deduplizierung auf dem Thin-Dateisystem. Diese Option ist erst verfügbar, wenn die Datenreduzierung aktiviert wurde. Gültige Werte: <ul style="list-style-type: none"> • yes • no (Standard) <p> ANMERKUNG: Die Thin-Dateisysteme müssen auf einem Unity-System erstellt werden, auf dem Version 4.2.x oder höher ausgeführt wird. Erweiterte Deduplizierung ist nur verfügbar auf:</p> <ul style="list-style-type: none"> • Dynamischen oder herkömmlichen Pools in Unity 380F-, 480F-, 680F- und 880F-Systemen • Dynamische Pools in Unity-All-Flash 450F-, 550F- und 650F-Systemen • All-Flash-Pools und Hybrid-Flash-Pools in Unity Hybrid-Systemen 380, 480, 680 und 880
-cifsSyncWrites	Hiermit werden synchrone Schreibvorgänge für CIFS (SMB)-Netzwerk-Shares aktiviert. Gültige Werte: <ul style="list-style-type: none"> • yes • no
-cifsOpLocks	Hiermit werden Opportunistic File Locks (oplocks) für CIFS-Netzwerk-Shares aktiviert. Gültige Werte: <ul style="list-style-type: none"> • yes • no
-cifsNotifyOnWrite	Hiermit wird der Empfang von Benachrichtigungen bei Schreibvorgängen in einer CIFS-Share aktiviert. Gültige Werte: <ul style="list-style-type: none"> • yes • no
-cifsNotifyOnAccess	Hiermit wird der Empfang von Benachrichtigungen bei Zugriffen auf einer CIFS-Share aktiviert. Gültige Werte: <ul style="list-style-type: none"> • yes • no

Qualifizierer	Beschreibung
-cifsNotifyDirDepth	Falls der Wert für -cifsNotifyOnWrite oder -cifsNotifyOnAccessyes (aktiviert) lautet, geben Sie die Unterverzeichnistiefe an, bis zu der die Benachrichtigungen gelten sollen. Der Wert kann zwischen 1 und 512 eingestellt werden. Der Standardwert lautet 512.
-sched	Geben Sie die ID des Plans ein, der auf das Dateisystem angewendet werden soll. Anzeigen von Schutzplänen erläutert, wie Sie die IDs der Pläne im System anzeigen können.
-schedPaused	Setzen Sie den Plan für den Qualifizierer -sched aus. Gültige Werte: <ul style="list-style-type: none"> • yes • no
-noSched	Hebt die Schutzplanzuweisung auf.
-fastvpPolicy	Geben Sie die FAST VP-Tiering Policy für das Dateisystem an. Diese Policy definiert sowohl die anfängliche Tier-Positionierung als auch das laufende automatisierte Tiering von Daten während den Datenverlagerungsvorgängen. Gültige Werte (nicht unterschieden nach Groß- und Kleinschreibung): <ul style="list-style-type: none"> • startHighThenAuto (Standardeinstellung): Legt die anfängliche Datenplatzierung auf die Laufwerke mit der höchsten Performance und freiem Speicherplatz fest und verlagert dann Teile der Daten der Storage-Ressource basierend auf der I/O-Aktivität. • auto: Legt die anfängliche Datenplatzierung auf eine optimale, vom System bestimmte Einstellung fest und verlagert dann Teile der Daten der Speicherressource basierend auf Performancestatistiken der Speicherressource, sodass die Daten entsprechend der I/O-Aktivität auf die Tiers verlagert werden. • highest: Legt die anfängliche Datenplatzierung und nachfolgende Datenverlagerung (falls zutreffend) auf die Laufwerke mit der höchsten Performance und freiem Speicherplatz fest. • lowest: legt die anfängliche Datenplatzierung und nachfolgende Datenverlagerung (falls zutreffend) auf die kosteneffizientesten Laufwerke mit freiem Speicherplatz fest.
-replDest	Gibt an, ob die Ressource ein Replikationsziel ist. Gültige Werte: <ul style="list-style-type: none"> • yes • no
-poolFullPolicy	Gibt die Policy an, die befolgt werden soll, wenn der Pool voll ist und ein Schreibvorgang auf das System versucht wird. Dieses Attribut ermöglicht es Ihnen, Snapshots auf dem Dateisystem beizubehalten, wenn ein Pool voll ist. Gültige Werte: <ul style="list-style-type: none"> • deleteAllSnaps: Snapshots, die mit dem Dateisystem verknüpft sind, werden gelöscht, wenn der Speicherpool die volle Kapazität erreicht. • failWrites: Schreibvorgänge auf das System schlagen fehl, wenn der Speicherpool die volle Kapazität erreicht.
-eventProtocols	Gibt eine Liste der Dateisystem-Zugriffsprotokolle an, die für die Ereignisveröffentlichung aktiviert sind. Standardmäßig ist die Liste leer. Gültige Werte: <ul style="list-style-type: none"> • nfs: Aktivieren Sie die Ereignisveröffentlichung für NFS. • cifs: Aktivieren Sie die Ereignisveröffentlichung für CIFS (SMB).
-flrMinRet	Gibt die kürzeste Aufbewahrungsfrist an, in der die Dateien in einem FLR-fähigen Dateisystem gesperrt und vor Löschung geschützt werden können. Gültige Werte: <ul style="list-style-type: none"> • d: days (die Standardeinstellung ist 1 Tag 1d) • m: months • y: years • infinite
-flrDefRet	Gibt die Standardaufbewahrungsfrist an, die in einem FLR-fähigen Dateisystem verwendet wird, wenn eine Datei gesperrt ist und keine Aufbewahrungsfrist auf Dateiebene angegeben wurde. Das Format lautet (<integer> d m y) infinite. <ul style="list-style-type: none"> • d: days • m: months • y: years — FLR-C (compliance) Standard ist 1 Jahr--1y) • infinite — FLR-E (enterprise) Standard <p>Alle begrenzten Werte plus das aktuelle Datum müssen unter der maximalen Aufbewahrungsfrist bis 7. Februar 2106 liegen.</p>

Qualifizierer	Beschreibung
	Der Wert dieses Parameters muss größer sein als die Mindestaufbewahrungsdauer <code>-flrMinRet</code> .
<code>-flrMaxRet</code>	Gibt das maximale Datum und die maximale Uhrzeit an, die bzw. das für eine gesperrte Datei in einem FLR-fähigen Dateisystem festgelegt wurde. Mögliche Werte sind: <ul style="list-style-type: none"> • <code>d: days</code> • <code>m: months</code> • <code>y: years</code> • <code>infinite</code> (Standard) Der Wert darf nicht größer als 1 Tag sein. Alle begrenzten Werte plus das aktuelle Datum müssen unter der maximalen Aufbewahrungsfrist bis 7. Februar 2106 liegen. Der Wert dieses Parameters muss größer sein als die standardmäßige Aufbewahrungsfrist <code>-flrDefRet</code> .
<code>-flrAutoLock</code>	Gibt an, ob alle neuen Dateien in einem FLR-fähigen Dateisystem automatisch gesperrt werden sollen. Gültige Werte: <ul style="list-style-type: none"> • <code>yes</code> • <code>no</code>
<code>-flrAutoDelete</code>	Gibt an, ob gesperrte Dateien in einem FLR-fähigen Dateisystem nach Ablauf der Aufbewahrungsfrist automatisch gelöscht werden. Gültige Werte: <ul style="list-style-type: none"> • <code>yes</code> • <code>no</code>
<code>-flrPolicyInterval</code>	Wenn <code>-flrAutoLock</code> auf <code>yes</code> eingestellt ist, geben Sie ein Zeitintervall an, wie lange Dateien nach der Änderung automatisch in einem FLR-aktivierten Dateisystem gesperrt werden. Das Format ist <code><value><qualifier></code> , wobei der Wert eine Ganzzahl ist und der Qualifizierer folgenden Wert hat: <ul style="list-style-type: none"> • <code>m: Minuten</code> • <code>h: Stunden</code> • <code>d--days</code> Der Wert sollte größer als 1 Minute sein und weniger als 366 Tage betragen.
<code>-errorThreshold</code>	Geben Sie den Schwellenwert in Prozent an, bei dessen Überschreitung Fehlerwarnmeldungen generiert werden. Der Bereich liegt zwischen 0 und 99. Der Standardwert ist 95 %. Wenn der Schwellenwert auf 0 festgelegt ist, wird diese Warnmeldung deaktiviert. Diese Option muss auf einen Wert größer als der <code>-warningThreshold</code> festgelegt werden.
<code>-warningThreshold</code>	Geben Sie den Schwellenwert in Prozent an, bei dessen Überschreitung Warnmeldungen generiert werden. Der Bereich liegt zwischen 0 und 99. Der Standardwert ist 75 %. Wenn der Schwellenwert auf 0 festgelegt ist, wird diese Warnmeldung deaktiviert. Diese Option muss auf einen Wert festgelegt werden, der kleiner ist als der <code>-errorThreshold</code> -Wert und größer als oder gleich dem <code>-infoThreshold</code> -Wert.
<code>-infoThreshold</code>	Geben Sie den Schwellenwert in Prozent an, bei dessen Überschreitung Warnmeldungen zur Information generiert werden. Der Bereich liegt zwischen 0 und 99. Der Standardwert ist 0 (deaktiviert). Diese Option muss auf einen Wert festgelegt werden, der kleiner ist als der <code>-warningThreshold</code> -Wert.

Beispiel

Der folgende Befehl gibt Ereignisveröffentlichungsprotokolle an:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/fs -id res_1 set -eventProtocols nfs,cifs
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = res_1
Operation completed successfully.
```

Löschen von Dateisystemen

Löschen Sie ein Dateisystem.

- ANMERKUNG:** Beim Löschen werden sämtliche mit dem Dateisystem verknüpften Netzwerk-Freigaben und optional die ihm zugeordneten Snapshots aus dem System entfernt. Nach dem Löschen des Dateisystems können die Dateien und Ordner nicht aus Snapshots wiederhergestellt werden. Sichern Sie die Daten eines Dateisystems, bevor Sie es aus dem Speichersystem löschen.
- ANMERKUNG:** Sie können kein FLR-C-fähiges Dateisystem löschen, das derzeit über gesperrte und geschützte Dateien verfügt. Ein FLR-E-fähiges Dateisystem kann gelöscht werden, auch wenn es geschützte Dateien beinhaltet.

Format

```
/stor/prov/fs {-id <value> | -name <value>} delete [-deleteSnapshots {yes | no}] [-async]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des zu löschenden Dateisystems ein.
-name	Geben Sie den Namen des zu löschenden Dateisystems ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-deleteSnapshots	Gibt an, dass die Snapshots des Dateisystems zusammen mit dem Dateisystem selbst gelöscht werden können. Gültige Werte: <ul style="list-style-type: none">yesno(Standard)
-async	Führen Sie den Vorgang im asynchronen Modus aus.

Beispiel

Mit dem folgenden Befehl wird das Dateisystem FS_1 gelöscht:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/fs -id res_1 delete
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Managen von Benutzer-Quotas für Dateisysteme und Quota-Strukturen

Eine Benutzer-Quota begrenzt die Menge an Speicher, die durch einen einzelnen Benutzer, der Daten in einem Dateisystem oder in einer Quota-Struktur speichert, belegt werden kann.

In der folgenden Tabelle sind die Attribute für Benutzer-Quotas aufgeführt:

Tabelle 109. Attribute für Benutzer-Quotas

Attribut	Beschreibung
File system	Kennung für das Dateisystem, auf dem die Quota gelten soll. Das Dateisystem darf nicht schreibgeschützt oder ein Replikationsziel sein.
Path	Quotenstrukturpfad relativ zum Stamm des Dateisystems Wenn die Benutzerquote auf einem Dateisystem ist, verwenden Sie entweder diesen Qualifizierer nicht oder legen Sie seinen Wert auf / fest.
User ID	Benutzerkennung auf dem Dateisystem.
Unix name	Durch Komma getrennte Liste von Unix-Benutzernamen, die der Benutzer-Quota zugeordnet ist. Mehrere Unix-Namen können angezeigt werden, wenn das Dateisystem eines mit mehreren Protokollen ist und in der Konfigurationsdatei für die Benutzerzuordnung (ntxmap) mehrere Unix-Namen einem Windows-Namen zugeordnet sind.
Windows SIDs	Durch Komma getrennte Liste von Windows-SIDs, die der Nutzerquote zugeordnet ist.  ANMERKUNG: Die Anzahl der angezeigten SIDs ist auf 16 begrenzt. Wenn die Anzahl der SIDs über 16 liegt, werden nur die ersten 16 angezeigt.
Windows name	Durch Komma getrennte Liste von Windows-Benutzernamen, die der Benutzer-Quota zugeordnet ist. Mehrere Windows-Namen können angezeigt werden, wenn das Dateisystem eines mit mehreren Protokollen ist und in der Konfigurationsdatei für die Benutzerzuordnung (ntxmap) mehrere Windows-Namen einem Unix-Namen zugeordnet sind.  ANMERKUNG: Wenn die Anzahl der Windows-Namen über 16 liegt, werden nur die ersten 16 Windows-Namen angezeigt.
Space used	Genutzter Speicherplatz auf dem Dateisystem oder der Quota-Struktur durch den angegebenen Benutzer.
Soft limit	Bevorzugtes Limit für die Speichernutzung. Das System gibt eine Warnmeldung aus, wenn das weiche Limit erreicht ist.
Hard limit	Absolutes Limit für die Speichernutzung. Wenn das harte Limit für eine Benutzer-Quota auf einem Dateisystem oder in einer Quota-Struktur erreicht ist, kann der Benutzer keine Daten mehr in das Dateisystem oder die Struktur schreiben, bis mehr Speicherplatz verfügbar ist.
Grace period left	Zeitraum, für den das System einen Countdown der Tage beginnt, sobald das weiche Limit erreicht ist. Wenn die Toleranzperiode des Benutzers abläuft, können Benutzer nicht mehr in das Dateisystem oder die Quota-Struktur schreiben, bis mehr Speicherplatz verfügbar ist, selbst wenn das harte Limit nicht erreicht wurde.
State	Status der Benutzer-Quota. Gültige Werte: <ul style="list-style-type: none"> • OK • Soft limit exceeded • Soft limit exceeded and grace period expired • Hard limit exceeded

Erstellen einer Benutzerquote auf einem Dateisystem oder einer Quotenstruktur

Sie können Benutzerquoten auf einem Dateisystem oder einer Quotenstruktur erstellen:

- Erstellen Sie eine Benutzerquote auf einem Dateisystem, um die Menge des Speicherplatzes zu begrenzen oder nachzuverfolgen, die ein einzelner Benutzer auf diesem Dateisystem belegt. Beim Erstellen oder Ändern von Benutzerquoten auf einem Dateisystem haben Sie die Möglichkeit, standardmäßige harte und weiche Limits zu verwenden, die auf Ebene des Dateisystems festgelegt werden.
- Erstellen Sie eine Benutzerquote in einer Quotenstruktur, um die Menge des Speicherplatzes zu begrenzen oder zu verfolgen, die ein einzelner Benutzer in dieser Struktur belegt. Beim Erstellen von Benutzerquoten in einer Quotenstruktur haben Sie die Möglichkeit, standardmäßige harte und weiche Limits zu verwenden, die auf Ebene der Quotenstruktur festgelegt werden.

Format

```
/quota/user create [-async] {-fs <value> | -fsName <value>} [-path <value>] {-userId <value> | -unixName <value> | -winName <value>} {-default | [-softLimit <value>] [-hardLimit <value>]}
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.
-fs	Geben Sie die ID des Dateisystems an, für das die Quote gelten soll. Das Dateisystem darf nicht schreibgeschützt oder ein Replikationsziel sein.
-fsName	Geben Sie den Namen des Dateisystems an, für das die Quote gelten soll. Das Dateisystem darf nicht schreibgeschützt oder ein Replikationsziel sein.
-path	Legen Sie eines der Folgenden fest: <ul style="list-style-type: none"> • Wenn die Benutzerquote für ein Dateisystem ist, verwenden Sie entweder diesen Qualifizierer nicht oder legen Sie seinen Wert auf / fest. • Wenn die Benutzerquote für eine Quotenstruktur ist, geben Sie den Pfad zu der Quotenstruktur relativ zum Stamm des Dateisystems an.
-userId	Geben Sie die Benutzer-ID auf dem Dateisystem oder der Quotenstruktur an.
-unixName	Geben Sie den UNIX-Benutzernamen an, der der angegebenen Benutzer-ID zugeordnet ist.
-winName	Geben Sie den Windows-Benutzernamen an, der der angegebenen Benutzer-ID zugeordnet ist. Das Format lautet wie folgt: [<domain>\]<name>
-default	Übernehmen Sie die Standardeinstellungen der Quotenlimits für den Benutzer. Verwenden Sie zum Anzeigen der Standardlimits den folgenden Befehl: <code>/quota/config -fs <value> -path <value> show</code> Wenn kein weiches oder hartes Limit für den Benutzer angegeben wurde, wird das Standardlimit angewendet.
-softLimit	Geben Sie das bevorzugte Limit für die Speichernutzung durch den Benutzer an. Ein Wert 0 bedeutet keine Begrenzung. Wenn das harte Limit festgelegt ist und das weiche Limit nicht, gibt es keine weiche Begrenzung.
-hardLimit	Geben Sie das absolute Limit für die Speichernutzung durch den Benutzer an. Ein Wert 0 bedeutet keine Begrenzung. Wenn das weiche Limit festgelegt ist und das harte Limit nicht, gibt es keine harte Begrenzung.  ANMERKUNG: Das harte Limit sollte größer als das weiche Limit sein.

Beispiel

Mit dem folgenden Befehl wird eine Benutzerquote für Benutzer 201 auf Dateisystem „res_1“, Quotenstruktur „/qtree_1“, erstellt. Die neue Benutzerquote hat die folgenden Begrenzungen:

- Weiches Limit ist 20 GB.
- Hartes Limit ist 50 GB.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /quota/user create -fs res_1 -path /qtree_1 -userId 201 -softLimit 20G -hardLimit 50G
```

```
Storage system address: 10.64.75.201
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Anzeigen von Benutzerquoten

Sie können Informationen zu Speichernutzung und -begrenzung für Benutzerquoten auf einem Dateisystem oder einer Quotenstruktur anzeigen.

Da es auf einem Dateisystem oder einer Quotenstruktur eine große Menge von Benutzerquoten geben kann, aktualisiert das System die Benutzerquoten nur einmal alle 24 Stunden, um die Auswirkungen auf die Systemperformance zu reduzieren. Sie können die Daten mithilfe der Aktualisierungsaktion häufiger aktualisieren. Verwenden Sie den Befehl `/quota/config show`, um die Zeit für die Datenaktualisierung anzuzeigen.

ANMERKUNG: Die Werte für Unix-Name und Windows-Name werden nur zurückgegeben, wenn eine einzige Benutzerquote angezeigt wird.

ANMERKUNG: Aktionsbefehl „show“ erklärt, wie das Ausgabeformat geändert werden kann.

Format

```
/quota/user {-fs <value> | -fsName <value>} [-path <value>] [-userId <value> | -unixName <value> | -winName <value>] [-exceeded] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-fs	Geben Sie die ID des Dateisystems an.
-fsName	Geben Sie den Namen des Dateisystems an.
-path	Legen Sie eines der Folgenden fest: <ul style="list-style-type: none">• Wenn die Benutzerquote für ein Dateisystem ist, verwenden Sie entweder diesen Qualifizierer nicht oder legen Sie seinen Wert auf / fest.• Wenn die Benutzerquote für eine Quotenstruktur ist, geben Sie den Pfad zu der Quotenstruktur relativ zum Stamm des Dateisystems an.
-userId	Geben Sie die Benutzer-ID auf dem Dateisystem oder der Quotenstruktur an.
-unixName	Geben Sie den Unix-Namen des Benutzers an.
-winName	Geben Sie den Windows-Benutzernamen an. Das Format lautet wie folgt: [<domain>\]<name>
-exceeded	Zeigen Sie nur Benutzerquoten an, deren Status nicht OK ist.

Beispiel

Mit dem folgenden Befehl werden Speicherplatznutzungsinformationen für Benutzer „nasadmin“ auf dem Dateisystem „res_1“, Quotenstruktur „/qtree_1“ angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /quota/user -fs res_1 -path /qtree_1 unixName nasadmin show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:   User ID           = 201
     Unix name       = nasadmin
     Windows names   = dell\nasadmin, dell\nasad
     Windows SIDs    = S-1-5-32-544, S-1-5-32-545
     Space used      = 32768 (32K)
     Soft limit      = 16384 (16K)
     Hard limit      = 65536 (64K)
```

```
Grace period left    = 7d 3h
State                = Soft limit exceeded
```

Ändern von Quotenlimits für einen bestimmten Benutzer

Sie können Limits für Benutzerquoten auf einem Dateisystem oder einer Quotenstruktur ändern.

Format

```
/quota/user {-fs | -fsName <value>} [-path <value>] {-userId <value> | -unixName <value> | winName <value>} set [-async] {-default | [-softLimit <value>] [-hardLimit <value>]}
```

Objektqualifizierer

Qualifizierer	Beschreibung
-fs	Geben Sie die ID des Dateisystems an.
-fsName	Geben Sie den Namen des Dateisystems an.
-path	Legen Sie eines der Folgenden fest: <ul style="list-style-type: none">• Wenn die Benutzerquote für ein Dateisystem ist, verwenden Sie entweder diesen Qualifizierer nicht oder legen Sie seinen Wert auf / fest.• Wenn die Benutzerquote für eine Quotenstruktur ist, geben Sie den Pfad zu der Quotenstruktur relativ zum Stamm des Dateisystems an.
-userId	Geben Sie die Benutzer-ID auf dem Dateisystem oder der Quotenstruktur an.
-unixName	Geben Sie den UNIX-Benutzernamen an, der der angegebenen Benutzer-ID zugeordnet ist.
-winName	Geben Sie den Windows-Benutzernamen an, der der angegebenen Benutzer-ID zugeordnet ist. Das Format lautet wie folgt: [<domain>\]<name>

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.
-default	Übernehmen Sie die Standardeinstellungen der Quotenlimits für den Benutzer. Verwenden Sie zum Anzeigen des Standardlimits den folgenden Befehl: <code>config -fs <value> -path <value> show</code> Wenn kein weiches oder hartes Limit für den Benutzer angegeben wurde, wird das Standardlimit angewendet.
-softLimit	Geben Sie das bevorzugte Limit für die Speichernutzung durch den Benutzer an. Ein Wert 0 bedeutet keine Begrenzung. Wenn das harte Limit festgelegt ist und das weiche Limit nicht, gibt es keine weiche Begrenzung.
-hardLimit	Geben Sie das absolute Limit für die Speichernutzung durch den Benutzer an. Ein Wert 0 bedeutet keine Begrenzung. Wenn das weiche Limit festgelegt ist und das harte Limit nicht, gibt es keine harte Begrenzung.  ANMERKUNG: Das harte Limit sollte größer als das weiche Limit sein.

Beispiel

Der folgende Befehl nimmt die folgenden Änderungen an den Benutzerquoten für Benutzer 201 auf Dateisystem „res_1“, Quotenstrukturpfad „/qtree_1“, vor:

- Legt das weiche Limit auf 10 GB fest.

- Legt das harte Limit auf 20 GB fest.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /quota/user -fs res_1 -path /qtree_1 -userId 201 set -softLimit 10G -hardLimit 20G
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
Operation completed successfully.
```

Aktualisieren von Benutzerquoten

Da es auf einem Dateisystem oder einer Quotenstruktur eine große Menge von Benutzerquoten geben kann, aktualisiert das System die Benutzerquoten nur einmal alle 24 Stunden, um die Auswirkungen auf die Systemperformance zu reduzieren. Sie können die Daten mithilfe der Aktualisierungsaktion häufiger aktualisieren. Verwenden Sie den Befehl `/quota/config show`, um die Zeit für die Datenaktualisierung anzuzeigen.

Format

```
/quota/user {-fs <value> | -fsName <value>} [-path <value>] refresh [-updateNames] [-async]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-fs	Geben Sie die ID des Dateisystems an.
-fsName	Geben Sie den Namen des Dateisystems an.
-path	Legen Sie eines der Folgenden fest: <ul style="list-style-type: none"> • Wenn die Benutzerquote auf einem Dateisystem ist, verwenden Sie entweder diesen Qualifizierer nicht oder legen Sie seinen Wert auf / fest. • Wenn die Benutzerquote auf einer Quotenstruktur ist, geben Sie den Pfad zu der Quotenstruktur relativ zum Stamm des Dateisystems an.
-updateNames	Aktualisieren Sie die Nutzungsdaten der Nutzerquoten und die Windows-Nutzernamen, Windows-SIDs und Unix-Nutzernamen in einem Dateisystem oder einer Quotenstruktur. <p> ANMERKUNG:</p> Die Aktualisierung von Nutzernamen verursacht Latenz, weil das System die Namensserver abfragen muss. Verwenden Sie diesen Qualifizierer daher nicht so häufig. Das System aktualisiert Windows-Nutzernamen, Windows-SIDs und Unix-Nutzernamen für Nutzerquoten automatisch alle 24 Stunden.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.

Beispiel

Mit dem folgenden Befehl werden alle Benutzerquoten auf dem Dateisystem „res_1“, Quotenstruktur „tree_1“ aktualisiert:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /quota/user -fs res_1 -path /tree_1 refresh
```

```
[Response]
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

Operation completed successfully.

Managen von Quotenstrukturen

Eine Quotenstruktur ist ein Verzeichnis, auf das eine Quote angewendet wird, wodurch der gesamte verbrauchte Speicherplatz dieses Verzeichnisses begrenzt oder nachverfolgt wird. Die Einstellungen für hartes Limit, weiches Limit und Toleranzperiode, die Sie für eine Quotenstruktur definieren, werden als Standardwerte für die Benutzerquoten der Quotenstruktur verwendet. Sie können die Einstellungen für das harte und weiche Limit überschreiben, indem Sie diese Einstellungen bei der Erstellung oder Änderung einer Benutzer-Quota explizit angeben.

In der folgenden Tabelle sind die Attribute für Quotenstrukturen aufgeführt.

Tabelle 110. Attribute für Quotenstrukturen

Attribut	Beschreibung
File system	Kennung des Dateisystems.
Path	Quotenstrukturpfad relativ zum Stamm des Dateisystems
Description	Beschreibung der Quotenstruktur
Soft limit	Bevorzugtes Limit für die Speichernutzung. Das System gibt eine Warnmeldung aus, wenn das weiche Limit erreicht ist.
Hard limit	Absolutes Limit für die Speichernutzung. Wenn das harte Limit für eine Quotenstruktur erreicht ist, können Benutzer keine Daten mehr in die Struktur schreiben, bis mehr Speicherplatz verfügbar ist.
Grace period left	Zeitraum, in dem ein Countdown beginnt, sobald das weiche Limit erreicht ist. Wenn die Toleranzperiode der Quotenstruktur abläuft, können Benutzer nicht mehr in die Quotenstruktur schreiben, bis mehr Speicherplatz verfügbar ist, selbst wenn das harte Limit nicht erreicht wurde.
State	Status der Benutzerquote. Gültige Werte: <ul style="list-style-type: none">• OK• Soft limit exceeded• Soft limit exceeded and grace period expired• Hard limit exceeded

Erstellen einer Quotenstruktur

Erstellen Sie eine Quotenstruktur, um die Menge des verbrauchten Speichers auf einem Verzeichnis nachzuverfolgen oder einzuschränken. Sie können Quota-Strukturen verwenden für:

- das Festlegen von Speicherbegrenzungen auf Projektbasis. Beispielsweise können Sie Quota-Strukturen für ein Projektverzeichnis erstellen, in dem mehrere Benutzer Dateien gemeinsam verwenden und erstellen.
- Verfolgen Sie die Nutzung des Verzeichnisses nach, indem Sie das harte und das weiche Limit der Quotenstruktur auf 0 (null) festlegen.

Format

```
/quota/tree create [-async] { -fs <value> | -fsName <value>} -path <value> [-descr <value>] {-default | [-softLimit <value>] [-hardLimit <value>]}
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.
-fs	Geben Sie die ID des Dateisystems an, in dem sich die Quotenstruktur befindet. Das Dateisystem darf nicht schreibgeschützt oder ein Replikationsziel sein.
-fsName	Geben Sie den Namen des Dateisystems an, in dem sich die Quotenstruktur befindet. Das Dateisystem darf nicht schreibgeschützt oder ein Replikationsziel sein.
-path	Geben Sie den Pfad zur Quotenstruktur relativ zum Stamm des Dateisystems an.
-descr	Geben Sie eine Beschreibung der Quotenstruktur an.
-default	Geben Sie an, dass die Standardeinstellungen der Quotenlimits für die Struktur übernommen werden. Verwenden Sie zum Anzeigen dieser Standardlimits den folgenden Befehl: Anzeigen von Quotenstrukturen
-softLimit	Geben Sie das bevorzugte Limit für verbrauchten Speicherplatz auf der Quotenstruktur an. Ein Wert 0 bedeutet keine Begrenzung. Wenn das harte Limit festgelegt ist und das weiche Limit nicht, gibt es keine weiche Begrenzung.
-hardLimit	Geben Sie das absolute Limit für verbrauchten Speicherplatz auf der Quotenstruktur an. Ein Wert 0 bedeutet keine Begrenzung. Wenn das weiche Limit festgelegt ist und das harte Limit nicht, gibt es keine harte Begrenzung.  ANMERKUNG: Das harte Limit sollte größer als das weiche Limit sein.

Beispiel

Mit dem folgenden Befehl wird die Quotenstruktur „/qtree_1“ auf Dateisystem „res_1“ erstellt. Die neue Quotenstruktur hat die folgenden Eigenschaften:

- Weiches Limit ist 100 GB.
- Hartes Limit ist 200 GB.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /quota/tree create -fs res_1 -path /qtree_1 -softLimit 100G -hardLimit 200G
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Anzeigen von Quotenstrukturen

Sie können Informationen zur Speichernutzung und -begrenzung für alle Quotenstrukturen auf einem Dateisystem oder für eine einzige Quotenstruktur anzeigen.

Da es auf einem Dateisystem eine große Menge von Quotenstrukturen geben kann, aktualisiert das System die Quotendaten nur einmal alle 24 Stunden, um die Auswirkungen auf die Systemperformance zu reduzieren. Sie können die Daten mithilfe der Aktualisierungsaktion häufiger aktualisieren. Verwenden Sie den Befehl `/quota/config show`, um die Zeit für die Datenaktualisierung anzuzeigen.

 **ANMERKUNG:** Aktionsbefehl „show“ erläutert, wie das Ausgabeformat geändert wird.

Format

```
/quota/tree {-fs <value> | -fsName <value>} [-path <value>] [-exceeded] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-fs	Geben Sie die ID des Dateisystems an.
-fsName	Geben Sie den Namen des Dateisystems an.
-path	Geben Sie den Pfad zu der Quotenstruktur an, der relativ zum Stamm des Dateisystems ist.
-exceeded	Zeigen Sie nur Quotenstrukturen an, deren Status nicht OK ist.

Beispiel

Mit dem folgenden Befehl werden Informationen zur Speichernutzung für alle Quotenstrukturen auf dem Dateisystem „res_1“ aufgeführt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /quota/tree -fs res_1 show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:   Path           = /qtree_1
     Description    = this is tree 1
     Space used     = 32768 (32K)
     Soft limit     = 53687091200 (50G)
     Hard limit     = 107374182400 (100G)
     Grace period left = 7d
     State         = OK

2:   Path           = /qtree_2
     Description    =
     Space used     = 32768 (32K)
     Soft limit     = 16384 (16K)
     Hard limit     = 65536 (64K)
     Grace period left = 7d
     State         = Soft limit exceeded
```

Festlegen von Quotenlimits für eine bestimmte Quotenstruktur

Sie können angeben, dass eine bestimmte Quotenstruktur die Standardeinstellungen für das Quotenlimit des zugehörigen Dateisystems übernehmen soll, oder Sie können auf der Quotenstruktur manuell weiche und harte Limits festlegen.

Format

```
/quota/tree {-fs <value> | -fsName <value>} -path <value> set [-async] [-descr <value>] {-default | [-softLimit <value>] [-hardLimit <value>]}
```

Objektqualifizierer

Qualifizierer	Beschreibung
-fs	Geben Sie die ID des Dateisystems an.
-fsName	Geben Sie den Namen des Dateisystems an.
-path	Geben Sie den Pfad zu der Quotenstruktur an, der relativ zum Stamm des Dateisystems ist.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.
-descr	Beschreibung der Quotenstruktur
-default	Übernehmen Sie die Standardeinstellungen für das Quotenlimit aus dem zugeordneten Dateisystem. Verwenden Sie zum Anzeigen der Standardlimits den folgenden Befehl: <code>/quota/config -fs <value> -path <value> show</code>
-softLimit	Geben Sie das bevorzugte Limit für verbrauchten Speicherplatz auf der Quotenstruktur an. Ein Wert 0 bedeutet keine Begrenzung.
-hardLimit	Geben Sie das absolute Limit für verbrauchten Speicherplatz auf der Quotenstruktur an. Ein Wert 0 bedeutet keine Begrenzung.  ANMERKUNG: Das harte Limit sollte gleich oder größer als das weiche Limit sein.

Beispiel

Der folgende Befehl nimmt die folgenden Änderungen an der Quotenstruktur „/qtree_1“ in Dateisystem „res_1“ vor:

- Legt das weiche Limit auf 50 GB fest.
- Legt das harte Limit auf 100 GB fest.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /quota/tree -fs res_1 -path /qtree_1 set -softLimit 50G -hardLimit 100G
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
Operation completed successfully.
```

Aktualisieren einer Quotenstruktur auf einem Dateisystem

Da es auf einem Dateisystem eine große Menge von Quotenstrukturen geben kann, aktualisiert das System die Quotendaten nur einmal alle 24 Stunden, um die Auswirkungen auf die Systemperformance zu reduzieren. Sie können die Daten mithilfe der Aktualisierungsaktion häufiger aktualisieren. Zur Anzeige des Zeitpunkts der Datenaktualisierung siehe das Ausgabefeld „Tree quota update time“ für den Befehl `/quota/config show`.

Format

```
/quota/tree {-fs <value> | -fsName <value>} refresh [-async]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-fs	Geben Sie die ID des Dateisystems an.
-fsname	Geben Sie den Namen des Dateisystems an.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.

Beispiel

Mit dem folgenden Befehl wird die Quoteninformationen für alle Quotenstrukturen auf dem Dateisystem „res_1“ aktualisiert:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /quota/tree -fs res_1 refresh /
```

```
[Response]
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Löschen von Quota-Strukturen

Sie können alle Quotenstrukturen für ein Dateisystem oder eine bestimmte Quotenstruktur löschen.

Format

```
/quota/tree {-fs <value> | -fsName <value>} -path <value> delete [-async]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-fs	Geben Sie die ID des Dateisystems an.
-fsName	Geben Sie den Namen des Dateisystems an.
-path	Legen Sie eines der Folgenden fest: <ul style="list-style-type: none">• Verwenden Sie zum Löschen aller Quotenstrukturen für das Dateisystem entweder diesen Qualifizierer nicht oder legen Sie seinen Wert auf / fest.• Geben Sie zum Löschen einer bestimmten Quotenstruktur den Pfad zu der Quotenstruktur an, relativ zum Stamm des Dateisystems.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.

Beispiel

Mit dem folgenden Befehl wird die Quotenstruktur „/qtree_1“ auf Dateisystem „res_1“ gelöscht.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /quota/tree -fs res_1 -path /qtree_1 delete
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

Operation completed successfully.

Managen von Quota-Einstellungen

Zum Managen von Quota-Einstellungen gehört die Auswahl einer Quota-Policy für ein Dateisystem, das Festlegen von Standardgrenzwerten für ein Dateisystem oder eine Quota-Struktur, das Festlegen einer Standardtoleranzperiode und das Deaktivieren der Durchsetzung von Grenzwerten für die Speicherplatznutzung für eine Quota-Struktur und Benutzer-Quotas auf der Struktur.

In der folgenden Tabelle sind die Attribute für die Konfiguration der Quota-Funktion aufgelistet:

Tabelle 111. Attribute für die Konfiguration der Quota-Funktion

Attribut	Beschreibung
Path	Quota-Strukturpfad relativ zum Stamm des Dateisystems. Verwenden Sie dieses Attribut entweder nicht für ein Dateisystem oder legen Sie seinen Wert auf / fest.
Quota policy	<p>(Gilt für nur Dateisysteme) Quota Policy für das Dateisystem. Gültige Werte:</p> <ul style="list-style-type: none">• <code>blocks</code>. Berechnet die Speicherplatznutzung in Bezug auf Dateisystemblöcke (8-KB-Einheiten). Die Blocknutzung richtet sich ausschließlich nach der Anzahl der zu der Datei hinzugefügten oder aus ihr entfernten Byte. Jeder Vorgang, der in der Zuweisung oder Entfernung von Blöcken resultiert, wie das Erstellen, Erweitern oder Löschen eines Verzeichnisses, das Schreiben oder Löschen von Dateien oder das Erstellen oder Löschen symbolischer Links, ändert die Blocknutzung. <p>Bei Verwendung der Block-Policy kann ein Benutzer eine platzsparende Datei erstellen, deren Größe die Dateigröße übersteigt, die aber weniger Blöcke auf dem Laufwerk nutzt.</p> <p>Verwenden Sie optional diese Policy für Nur-NFS- und Multiprotokoll-Dateisysteme.</p> <ul style="list-style-type: none">• <code>filesize</code> (Standardeinstellung). Hierbei wird die Speicherplatznutzung in Bezug auf die logischen Dateigrößen berechnet und die Größe von Verzeichnissen und symbolischen Links wird ignoriert. Verwenden Sie die Datei-Policy in folgenden Fällen:<ul style="list-style-type: none">○ Wenn Sie ein Nur-SMB-Dateisystem haben.○ Wenn die Dateigrößen kritisch für Quoten sind, z. B. wenn die Benutzernutzung auf der Größe der erstellten Dateien basiert und eine Überschreitung der Größenbegrenzung unzulässig ist.
User quota	<p>(Gilt nur für Dateisysteme) Gibt an, ob Benutzer-Quotas auf dem Dateisystem durchgesetzt werden sollen. Gültige Werte:</p> <ul style="list-style-type: none">• <code>on</code>. Aktivieren der Durchsetzung von Benutzer-Quotas auf dem Dateisystem oder der Quota-Struktur• <code>off</code>. Deaktivieren der Durchsetzung von Benutzer-Quotas auf dem Dateisystem oder der Quota-Struktur <p>i ANMERKUNG: Weil diese Verfahren Auswirkungen auf die Systemperformance haben, wird empfohlen, sie nur außerhalb der Spitzenproduktionszeiten durchzuführen. Sobald die Durchsetzung von Nutzer-Quotas aktiviert ist, können Sie die Quotas-Einstellungen ohne Beeinträchtigung der Performance ändern.</p>
Deny access	<p>Gibt an, ob Quotas zur Begrenzung der Speicherplatznutzung für das Dateisystem durchgesetzt werden. Folgende Werte sind möglich:</p> <ul style="list-style-type: none">• <code>yes</code>. (Standardeinstellung) Quotas zur Begrenzung der Speicherplatznutzung für das Dateisystem oder die Quota-Struktur werden durchgesetzt. Wenn Sie diese Option auswählen, wird die Möglichkeit, Speicherplatz zuzuweisen, durch die Quota-Einstellungen festgelegt.• <code>no</code>. Quota-Funktion für das Dateisystem oder die Quota-Struktur wird nicht durchgesetzt. Wenn Sie diese Option auswählen, wird die Möglichkeit, Speicherplatz zuzuweisen, nicht abgelehnt, wenn eine Quota-Begrenzung überschritten wird.
Grace period	Zeitraum, für den das System einen Countdown der Tage beginnt, sobald das weiche Limit erreicht ist. Wenn die Toleranzperiode für ein Dateisystem oder eine Quota-Struktur abläuft, können Benutzer nicht mehr in das Dateisystem oder die Quota-Struktur schreiben, bis mehr Speicherplatz verfügbar ist, selbst wenn das harte Limit nicht überschritten wurde.

Tabelle 111. Attribute für die Konfiguration der Quota-Funktion (fortgesetzt)

Attribut	Beschreibung
	Die Toleranzperiode kann auf <code>infinite</code> festgelegt werden, damit IO fortgesetzt werden kann, nachdem das weiche Limit überschritten wurde (bis das harte Limit erreicht ist).
<code>Default soft limit</code>	Standardmäßig bevorzugtes Limit für die Speichernutzung für Benutzer-Quotas auf dem Dateisystem, Quota-Strukturen im Dateisystem und Benutzer-Quotas auf den Quota-Strukturen im Dateisystem. Das System gibt eine Warnmeldung aus, wenn das weiche Limit erreicht ist.
<code>Default hard limit</code>	Standardmäßig hartes Limit für die Speichernutzung für Benutzer-Quotas auf dem Dateisystem, Quota-Strukturen im Dateisystem und Benutzer-Quotas auf den Quota-Strukturen im Dateisystem. Wenn das harte Limit für ein Dateisystem oder eine Quota-Struktur erreicht ist, können Benutzer keine Daten mehr in das Dateisystem oder die Struktur schreiben, bis mehr Speicherplatz verfügbar ist. Wenn das harte Limit für eine Benutzer-Quota auf einem Dateisystem oder in einer Quota-Struktur erreicht ist, kann dieser Benutzer keine Daten mehr in das Dateisystem oder die Struktur schreiben.
<code>Tree quota update time</code>	Zeitpunkt der Aktualisierung des Struktur-Quota-Berichts. Das Format für den Zeitpunkt lautet <code>JJJJ-MM-TT HH:MM:SS</code> .
<code>User quota update time</code>	Zeitpunkt der Aktualisierung des Benutzer-Quota-Berichts. Das Format für den Zeitpunkt lautet <code>JJJJ-MM-TT HH:MM:SS</code> .

Konfigurieren von Quota-Einstellungen

Sie können Quota-Konfigurationseinstellungen für ein Dateisystem oder eine Quota-Struktur konfigurieren.

Format

```
/quota/config {-fs <value> | -fsName <value>} [-path <value>] set [-async] {-policy {blocks | filesize} | [-userQuota {on | off | clear}] [-gracePeriod <value> | infinite] [-defaultSoft <value>] [-defaultHard <value>] [-denyAccess {yes | no}]}
```

Objektqualifizierer

Qualifizierer	Beschreibung
<code>-fs</code>	Geben Sie die ID des Dateisystems an, für das Sie Quoteneinstellungen konfigurieren möchten. Das Dateisystem darf nicht schreibgeschützt oder ein Replikationsziel sein.
<code>-fsname</code>	Geben Sie den Namen des Dateisystems an, für das Sie Quoteneinstellungen konfigurieren möchten. Das Dateisystem darf nicht schreibgeschützt oder ein Replikationsziel sein.
<code>-path</code>	Geben Sie den Pfad zu der Quotenstruktur an, relativ zum Stamm des Dateisystems. Verwenden Sie dieses Attribut entweder nicht für ein Dateisystem oder legen Sie seinen Wert auf <code>/</code> fest.

Aktionsqualifizierer

Qualifizierer	Beschreibung
<code>-async</code>	Führen Sie den Vorgang im asynchronen Modus aus.
<code>-userQuota</code>	Gibt an, ob Benutzer-Quotas auf dem Dateisystem oder der Quota-Struktur durchgesetzt werden sollen. Gültige Werte: <ul style="list-style-type: none"> <code>on</code> : Aktivieren der Durchsetzung von Nutzer-Quotas auf dem Dateisystem oder der Quota-Struktur <code>off</code> : Deaktivieren der Durchsetzung von Nutzer-Quotas auf dem Dateisystem oder der Quota-Struktur. Wenn Sie Benutzer-Quotas deaktivieren, bestehen die aktuellen Benutzer-Quota-Einstellungen nach wie vor, sofern Sie diese nicht löschen. Diese Einstellungen werden automatisch erneut angewendet, wenn Benutzer-Quotas erneut aktiviert werden.

Qualifizierer	Beschreibung
	<ul style="list-style-type: none"> • <code>clear</code> : Löschen von Nutzer-Quoteneinstellungen nach der Deaktivierung einer Nutzer-Quote <p>Weil das Aktivieren und Deaktivieren der Durchsetzung von Benutzer-Quotas Auswirkungen auf die Systemperformance haben, wird empfohlen, diese Verfahren nur außerhalb der Spitzenproduktionszeiten durchzuführen. Sobald die Durchsetzung von Benutzer-Quotas aktiviert ist, können Sie die Benutzer-Quota-Einstellungen ohne Beeinträchtigung der Performance ändern.</p>
<code>-policy</code>	<p>Geben Sie die Quota Policy für das Dateisystem an. Gültige Werte:</p> <ul style="list-style-type: none"> • <code>blocks</code> (Block-Policy): Hierbei wird die Speicherplatznutzung in Bezug auf die Dateisystemblöcke (8-KB-Einheiten) und die Laufwerksnutzung anhand von Verzeichnissen und symbolischen Links berechnet. • <code>filesize</code> (File-Policy): Hierbei wird die Speichernutzung in Bezug auf die logischen Dateigrößen berechnet und die Größe von Verzeichnissen und symbolischen Links wird ignoriert. <p>Weitere Informationen finden Sie unter Konfigurieren von Quota-Einstellungen</p>
<code>-gracePeriod</code>	<p>Geben Sie den Zeitraum an, für den das System einen Countdown der Tage beginnt, sobald das weiche Limit erreicht ist. Wenn die Toleranzperiode für eine Quota-Struktur abläuft, können Benutzer nicht mehr in die Quota-Struktur schreiben, bis mehr Speicherplatz verfügbar ist, selbst wenn das harte Limit nicht überschritten wurde. Wenn die Toleranzperiode für eine Benutzer-Quota auf einem Dateisystem oder einer Quota-Struktur abläuft, kann der einzelne Benutzer nicht mehr in das Dateisystem oder in die Quota-Struktur schreiben, bis für diesen Benutzer mehr Speicherplatz verfügbar ist. Standardmäßig beträgt die Schonfrist 7 Tage.</p> <p>Das Format lautet wie folgt:</p> <pre><value><qualifier></pre> <p>Hierbei gilt:</p> <ul style="list-style-type: none"> • <code>value</code>: Ein ganzzahliger Wert, je nach dem zugehörigen Qualifizierer: <ul style="list-style-type: none"> ○ Wenn der Qualifizierer „m“ (Minuten) ist, ist der zulässige Bereich von 1 bis 525600. ○ Wenn der Qualifizierer „h“ (Stunden) ist, ist der zulässige Bereich von 1 bis 8760. ○ Wenn der Qualifizierer „d“ (Tage) ist, ist der zulässige Bereich von 1 bis 365. • <code>qualifier</code>: einer der folgenden Wertqualifizierer (ohne Unterscheidung zwischen Groß- und Kleinschreibung): <ul style="list-style-type: none"> ○ <code>m</code> : Minuten ○ <code>h</code> : Stunden ○ <code>d</code> : Tage ○ <code>infinite</code> : Keine Begrenzung Auf diese Weise kann IO fortgesetzt werden, nachdem das weiche Limit überschritten wurde. <p>i ANMERKUNG: Wenn Sie einen Wert für die Toleranzperiode aktualisieren, wirkt sich der neue Wert nur auf die Quota oder Quotas aus, die das weiche Limit überschreiten, nachdem die Aktualisierung durchgeführt wurde. Alle vorhandenen Quotas, die mit dem älteren Wert für die Toleranzperiode gerechnet haben, sind nicht betroffen.</p>
<code>-defaultSoft</code>	<p>Gibt das standardmäßige bevorzugte Limit für die Speichernutzung für Benutzer-Quotas auf dem Dateisystem, den Quota-Strukturen im Dateisystem und Benutzer-Quotas auf den Quota-Strukturen im Dateisystem an. Das System gibt eine Warnmeldung aus, wenn das weiche Limit erreicht ist.</p>
<code>-defaultHard</code>	<p>Geben Sie das standardmäßig harte Limit für die Speichernutzung für Benutzer-Quotas auf dem Dateisystem, Quota-Strukturen im Dateisystem und Benutzer-Quotas auf den Quota-Strukturen im Dateisystem an. Wenn das harte Limit für eine Quota-Struktur erreicht ist, können Benutzer keine Daten mehr in das Dateisystem oder die Struktur schreiben, bis mehr Speicherplatz verfügbar ist. Wenn das harte Limit für eine Benutzer-Quota auf einem Dateisystem oder einer Quota-Struktur erreicht ist, kann dieser bestimmte Benutzer keine Daten mehr in das Dateisystem oder die Struktur schreiben.</p> <p>i ANMERKUNG: Das harte Limit sollte größer als das weiche Limit sein.</p>
<code>-denyAccess</code>	<p>Gibt an, ob Quota-Limits für das Dateisystem aktiviert werden. Gültige Werte:</p> <ul style="list-style-type: none"> • <code>yes</code> : Aktiviert die Quota-Funktion für das Dateisystem. Wenn Sie diese Option auswählen, wird die Möglichkeit, Speicherplatz zuzuweisen, durch die Quota-Einstellungen festgelegt. • <code>no</code> : Deaktiviert die Quota-Funktion für das Dateisystem. Wenn Sie diese Option auswählen, wird die Möglichkeit, Speicherplatz zuzuweisen, nicht abgelehnt, wenn eine Quota-Begrenzung erreicht wird.

Beispiel 1

Mit dem folgenden Befehl wird die Quota-Struktur „/qtree_1“ in Dateisystem „res_1“ wie folgt konfiguriert:

- Legt die standardmäßige Toleranzperiode auf 5 Tage fest.
- Legt das standardmäßige weiche Limit auf 10 GB fest.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /quota/config -fs res_1 -path /qtree_1 set -gracePeriod 5d -defaultSoft 10G
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Beispiel 2

Mit dem folgenden Befehl wird eine Quoten-Struktur für das Dateisystem fs1 in Pfad /dir1 auf eine Toleranzperiode eingestellt, die kein weiches Limit hat.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /quota/config -fsName fs1 -path /dir1 set -gracePeriod infinite
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Anzeigen von Quotenkonfigurationseinstellungen

Sie können die Quotenkonfigurationseinstellungen für ein Dateisystem, eine bestimmte Quotenstruktur, oder ein Dateisystem und alle zugehörigen Quotenstrukturen anzeigen.

Format

```
/quota/config {-fs <value> | -fsName <value>} [-path <value>] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-fs	Geben Sie die ID des Dateisystems an.
-fsname	Geben Sie den Namen des Dateisystems an.
-path	Geben Sie den Pfad zur Quotenstruktur relativ zum Stamm des Dateisystems an. Verwenden Sie dieses Attribut entweder nicht für ein Dateisystem oder legen Sie seinen Wert auf / fest. Wenn dieser Wert nicht angegeben wird, zeigt der Befehl die Quotenkonfiguration der Dateisystemebene und die Quotenkonfiguration aller Quotenstrukturen innerhalb des angegebenen Dateisystems an.

Beispiel

Mit dem folgenden Befehl werden Konfigurationsinformationen für die Quotenstruktur „/quota/config“ auf dem Dateisystem „res_1“ aufgeführt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /quota/config -fs res_1 show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
```

```

HTTPS connection

1:   Path                = /
     Quota policy        = blocks
     User quota          = on
     Deny access        = yes
     Grace period        = 7d
     User soft limit     = 53687091200 (50G)
     User hard limit     = 107374182400 (100G)
     Tree quota update time = 2014-10-31 13:17:28
     User quota update time = 2014-10-31 13:20:22

2:   Path                = /qtree_1
     Quota policy        = blocks
     User quota          = on
     Deny access        = yes
     Grace period        = 7d
     User soft limit     = 1073741824 (1G)
     User hard limit     = 10737418240 (10G)
     Tree quota update time =
     User quota update time =

```

Managen von NFS-Netzwerk-Shares

Netzwerk-Freigaben mit dem NFS (Network File System) bieten über das NFS-Protokoll einen Zugriffspunkt, über den konfigurierte Linux-/UNIX-Hosts bzw. IP-Subnetze auf Dateisystemspeicher zugreifen können. NFS-Netzwerk-Freigaben sind mit einem NFS-Dateisystem verknüpft.

Die einzelnen NFS-Freigaben verfügen über eine eindeutige ID.

In der folgenden Tabelle sind die Attribute für NFS-Netzwerk-Shares aufgeführt:

Tabelle 112. Attribute von NFS-Netzwerk-Freigaben

Attribut	Beschreibung
ID	Die ID der Freigabe.
Name	Der Name der Freigabe.
Description	Kurze Beschreibung der Freigabe.
Local path	Name des Pfads relativ zum Dateisystem des Verzeichnisses, auf das die Freigabe Zugriff bereitstellt. Standardmäßig ist das der Stamm des Dateisystems. Ein lokaler Pfad muss auf ein vorhandenes Verzeichnis im Dateisystem verweisen.
Export path	Der von den Hosts für die Verbindung mit der Freigabe verwendete Exportpfad.  ANMERKUNG: Der Exportpfad ist eine Kombination aus Netzwerkname oder IP-Adresse des zugehörigen NAS-Servers und dem Namen der Freigabe.
File system	ID des übergeordneten Dateisystems, das der NFS-Freigabe zugeordnet ist.
Default access	Die Standardeinstellung des gleichzeitigen Zugriffs für Hostkonfigurationen und nicht konfigurierte Hosts, die auf die Freigabe zugreifen können. Folgende Werte sind möglich: <ul style="list-style-type: none"> • <code>ro</code>: Hosts haben schreibgeschützten Zugriff auf den primären Storage und auf Snapshots, die der Freigabe zugeordnet sind. • <code>rw</code>: Hosts haben Schreibzugriff auf den primären Storage und auf Snapshots, die der Freigabe zugeordnet sind. • <code>roroot</code>: Hosts haben schreibgeschützten Zugriff auf den primären Storage und auf Snapshots, die der Freigabe

Tabelle 112. Attribute von NFS-Netzwerk-Freigaben (fortgesetzt)

Attribut	Beschreibung
	<p>zugeordnet sind, das Root-Verzeichnis des NFS-Clients verfügt jedoch über Root-Zugriff.</p> <ul style="list-style-type: none"> • <code>root</code>: Hosts haben Root-Schreibzugriff auf den primären Storage und auf Snapshots, die der Freigabe zugeordnet sind. Dies beinhaltet die Möglichkeit zur Einrichtung von Zugriffskontrollen, mit denen die Berechtigungen für andere Anmeldekonto eingeschränkt werden. • <code>na</code>: Hosts haben keinen Zugriff auf die Freigabe oder ihre Snapshots.
<code>Advanced host management</code>	<p>Gibt an, ob die in den Hostlisten aufgeführten Hosts mithilfe der <code>/remote/host</code>-Objekte definiert werden, z. B. mit ihrer Kennung. Werte sind (keine Unterscheidung zwischen Groß- und Kleinschreibung).</p> <ul style="list-style-type: none"> • <code>yes</code> (Standardeinstellung): Hostlisten enthalten die IDs der registrierten Hosts. • <code>no</code>: Hostlisten enthalten kommagetrennte Zeichenfolgen, wobei jede Zeichenfolge einen Hostnamen, eine IP-Adresse, ein Subnetz, eine Netzwerkgruppe oder eine DNS-Domain definiert.
<code>Read-only hosts</code>	<p>Durch Komma getrennte Liste von Hosts, die schreibgeschützten Zugriff auf die Freigabe und ihre Snapshots haben. Wenn erweitertes Hostmanagement aktiviert ist, ist dies eine Liste der IDs der registrierten Hosts. Andernfalls ist dies eine Liste von Netzwerkhostnamen, IPs, Subnetzen, Domains oder Netgroups.</p>
<code>Read/write hosts</code>	<p>Durch Kommas getrennte Liste von Hostkennungen mit Leseberechtigung. Andernfalls ist dies eine Liste von Netzwerkhostnamen, IPs, Subnetzen, Domains oder Netgroups.</p>
<code>Read-only root hosts</code>	<p>Durch Komma getrennte Liste von Hosts, die schreibgeschützten Root-Zugriff auf die Freigabe und ihre Snapshots haben. Wenn erweitertes Hostmanagement aktiviert ist, ist dies eine Liste der IDs der registrierten Hosts. Andernfalls ist dies eine Liste von Netzwerkhostnamen, IPs, Subnetzen, Domains oder Netgroups.</p>
<code>Root hosts</code>	<p>Durch Komma getrennte Liste von Hosts, die Lese-Schreib-Root-Zugriff auf die Freigabe und ihre Snapshots haben. Wenn erweitertes Hostmanagement aktiviert ist, ist dies eine Liste der IDs der registrierten Hosts. Andernfalls ist dies eine Liste von Netzwerkhostnamen, IPs, Subnetzen, Domains oder Netgroups.</p>
<code>No access hosts</code>	<p>Durch Komma getrennte Liste von Hosts, die keinen Zugriff auf die Freigabe oder ihre Snapshots haben. Wenn erweitertes Hostmanagement aktiviert ist, ist dies eine Liste der IDs der registrierten Hosts. Andernfalls ist dies eine Liste von Netzwerkhostnamen, IPs, Subnetzen, Domains oder Netgroups.</p>
<code>Allow SUID</code>	<p>Gibt an, ob es Nutzern erlaubt ist, die UNIX-Berechtigungsbits <code>setuid</code> und <code>setgid</code> festzulegen. Werte sind (keine Unterscheidung zwischen Groß- und Kleinschreibung).</p> <ul style="list-style-type: none"> • <code>yes</code> (Standardeinstellung): Nutzer können die Unix-Berechtigungsbits <code>setuid</code> und <code>setgid</code> festlegen. Dies ermöglicht es Benutzern, die ausführbare Datei mit den Rechten des Dateieigentümers auszuführen. • <code>no</code>: Nutzer können die Unix-Berechtigungsbits <code>setuid</code> und <code>setgid</code> nicht festlegen.
<code>Anonymous UID</code>	<p>(Gilt, wenn der Host keinen <code>allow root</code>-Zugriff darauf hat.) UID des anonymen Kontos. Dieses Konto ist Clientanfragen zugeordnet, die mit der Nutzer-ID 0 (Null) eingehen, die</p>

Tabelle 112. Attribute von NFS-Netzwerk-Freigaben (fortgesetzt)

Attribut	Beschreibung
	normalerweise mit dem Nutzernamen <code>root</code> verknüpft ist. Der Standardwert ist <code>4294967294 (-2)</code> , der in der Regel mit dem Nutzer <code>nobody</code> verknüpft ist (Root Squash).
<code>Anonymous GID</code>	(Gilt, wenn der Host keinen <code>allow root</code> -Zugriff darauf hat.) GID des anonymen Kontos. Dieses Konto ist Clientanfragen zugeordnet, die mit der Nutzer-ID 0 (Null) eingehen, die normalerweise mit dem Nutzernamen <code>root</code> verknüpft ist. Der Standardwert ist <code>4294967294 (-2)</code> , der in der Regel mit dem Nutzer <code>nobody</code> verknüpft ist (Root Squash).
<code>Creation time</code>	Der Zeitpunkt der Erstellung der Freigabe
<code>Last modified time</code>	Der Zeitpunkt der letzten Änderung der Freigabe
<code>Role</code>	Die spezifische Verwendung der Dateifreigabe. Folgende Werte sind möglich: <ul style="list-style-type: none"> <code>production</code>: Standardwert für NAS-Quellserver. <code>backup</code>: Standardwert für NAS-Zielserver. Automatisch für alle Freigaben eingestellt, die auf einem NAS-Server erstellt wurden, der als Replikationsziel fungiert. In anderen Fällen wird der Wert <code>production</code> automatisch als eine Rolle für die NFS-Freigabe festgelegt.
<code>Minimum security</code>	Gibt eine minimale Sicherheitsoption an, die vom Client für einen NFS-Mountvorgang (auf der Registerkarte „Dateisystem“) bereitgestellt werden muss. Der Wert kann einer der Folgenden sein, wobei das Sicherheitslevel immer weiter zunimmt: <ul style="list-style-type: none"> <code>sys</code>: Keine serverseitige Authentifizierung (Server verlässt sich auf NFS-Clientauthentifizierung) Ohne eine konfigurierte sichere NFS für den NAS-Server ist diese Einstellung Standard (auch bekannt als <code>AUTH_SYS</code>-Sicherheit). <code>krb5</code>: Kerberos V5-Authentifizierung. Standard, wenn sicheres NFS für den NAS-Server konfiguriert ist. <code>krb5i</code>: Kerberos V5-Authentifizierung und Integrität <code>krb5p</code>: Kerberos v5-Authentifizierung und Integrität; Verschlüsselung ist aktiviert.

Angabe von Hostlisten mithilfe einer Zeichenfolge

Wenn ein erweitertes Hostmanagement deaktiviert ist, kann eine Hostliste eine Kombination aus Netzwerk-Hostnamen, IP-Adressen, Subnetzen, Netgroups oder DNS-Domains enthalten. Es gelten folgende Formatierungsregeln:

- Eine IP-Adresse kann eine IPv4- oder IPv6-Adresse sein.
- Ein Subnetz kann eine IP-Adresse/Netzmaske oder IP-Adresse/Präfixlänge sein (z. B. `168.159.50.0/255.255.255.0` oder `168.159.50.0/24`).
- Das Format der DNS-Domain folgt dem UNIX/Linux-Format; zum Beispiel `*.example.com`. Wenn Sie Platzhalter in vollständig qualifizierten Domainnamen angeben, sind Punkte nicht im Platzhalter enthalten. Beispiel: `*.example.com` schließt `one.example.com` mit ein, `one.two.example.com` jedoch nicht.
- Um anzugeben, dass ein Name ein Netgroup-Name ist, stellen Sie dem Namen ein `@` voran. Ansonsten gilt der Name als Hostname.

Wenn ein erweitertes Hostmanagement aktiviert ist, enthalten die Hostlisten die Host-IDs der bestehenden Hosts. Sie können diese IDs mithilfe des Befehls `/remote/host` abrufen.

Erstellen von NFS-Netzwerk-Freigaben

Erstellen Sie eine NFS-Freigabe, um ein Dateisystem Ordner über das NFS-Protokoll zu exportieren.

ANMERKUNG: Freigabenzugriffseinstellungen für bestimmte Hosts werden nur wirksam, wenn die hostspezifische Einstellung weniger restriktiv ist als die Standardzugriffseinstellung für die Freigaben. Zudem hat die Zugriffseinstellung „Kein Zugriff“ für einen bestimmten Host immer Vorrang vor der Standardzugriffseinstellung.

- Beispiel 1: Wenn die Standardzugriffseinstellung für eine Freigabe „Schreibgeschützt“ und die Zugriffseinstellung für eine bestimmte Hostkonfiguration „Lesen/Schreiben“ lautet, so wird Letztere wirksam.
- Beispiel 2: Wenn die Standardzugriffseinstellung für eine Freigabe „Schreibgeschützt“ und die Zugriffseinstellung für eine bestimmte Hostkonfiguration „Kein Zugriff“ lautet, so kann der Host nicht auf die Freigabe zugreifen.
- Beispiel 3: Wenn die Standardzugriffseinstellung für eine Freigabe „Lesen/Schreiben“ und die Zugriffseinstellung für eine bestimmte Hostkonfiguration „Schreibgeschützt“ lautet, so erhält der Host nur Lesezugriff.

Voraussetzung

Konfigurieren Sie ein Dateisystem, das Sie mit den NFS-Netzwerk-Freigaben verknüpfen können. [Erstellen von Dateisystemen](#) erläutert, wie Sie Dateisysteme im System erstellen.

Format

```
/stor/prov/fs/nfs create [-async] -name <value> [-descr <value>] {-fs <value> | -fsName <value>}
-path <value> [-defAccess {ro | rw | roroot | root | na}] [-advHostMgmtEnabled {yes | no}]
[-roHosts <value>] [-rwHosts <value>] [-roRootHosts <value>] [-rootHosts <value>] [-naHosts
<value>] [-minSecurity {sys | krb5 | krb5i | krb5p}] [-allowSuid {yes | no}] [-anonUid <value>]
[-anonGid <value>]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.
-name	Geben Sie einen Namen für die Freigabe ein. Standardmäßig stellt dieser Wert zusammen mit dem Netzwerknamen oder der IP-Adresse des NAS-Servers den Exportpfad dar, über den Hosts auf die Freigabe zugreifen. Mit dem Schrägstrich (/) können Sie einen „virtuellen“ Namensraum erzeugen, der sich vom realen Pfadnamen der Freigabe unterscheidet. Beispiel: /fs1 und /fs2 können als vol/fs1 und vol/fs2 dargestellt werden. Beachten Sie die folgenden Überlegungen: <ul style="list-style-type: none"> • Sie können das Zeichen „/“ nicht als erstes Zeichen des Freigabennamens verwenden. • Ein NFSv4-Client kann keine Freigabe mit einem Namen mounten, der das Zeichen „/“ enthält. Stattdessen muss der Client den Freigabepfad verwenden. Um den Freigabepfad zu verwenden, müssen Sie den NAS-Serverparameter <code>nfs.showExportLevel</code> auf 0 oder 1 setzen.
-descr	Geben Sie eine kurze Beschreibung der Freigabe ein.
-fs	Geben Sie die ID des übergeordneten Dateisystems ein, das der NFS-Freigabe zugeordnet ist.
-fsName	Geben Sie den Namen des übergeordneten Dateisystems ein, das dem NFS-Share zugeordnet ist.
-path	Geben Sie den Namen des Systemverzeichnisses ein, in dem sich die Freigabe befindet. Der Pfad muss mit einem vorhandenen Verzeichnis-/Ordernamen in der Freigabe übereinstimmen, die auf Hostseite erstellt wurde. <ul style="list-style-type: none"> • Jede Freigabe muss über einen eigenen eindeutigen lokalen Pfad verfügen. Die erste Freigabe wird auf dem Stammverzeichnis des Dateisystems erstellt. • Bevor Sie zusätzliche Netzwerkfreigaben innerhalb eines NFS-Dateisystems erstellen können, müssen Sie Verzeichnisse innerhalb des Dateisystems erstellen. Stellen Sie eine Verbindung zu der ersten NFS-Freigabe von einem Host mit Zugriff auf die Freigabe her und legen Sie die Zugriffsberechtigungen entsprechend fest.
-defAccess	Geben Sie die Standardeinstellung des gleichzeitigen Zugriffs für Hostkonfigurationen und nicht konfigurierte Hosts an, die auf die Freigabe zugreifen können. Folgende Werte sind möglich: <ul style="list-style-type: none"> • <code>ro</code> : Hosts haben schreibgeschützten Zugriff auf den primären Storage und auf Snapshots, die der Freigabe zugeordnet sind.

Qualifizierer	Beschreibung
	<ul style="list-style-type: none"> • <code>rw</code> : Hosts haben Lese- und Schreibzugriff auf den primären Storage und auf Snapshots, die der Freigabe zugeordnet sind. • <code>rooroot</code> : Hosts haben schreibgeschützten Zugriff auf den primären Storage und auf Snapshots, die der Freigabe zugeordnet sind. Das Root-Verzeichnis des NFS-Clients verfügt über Root-Zugriff auf die Freigabe. • <code>root</code> : Hosts haben Lese- und Schreib-Root-Zugriff auf den primären Storage und auf Snapshots, die der Freigabe zugeordnet sind. Dies beinhaltet die Möglichkeit zur Einrichtung von Zugriffskontrollen, mit denen die Berechtigungen für andere Anmeldekonto eingeschränkt werden. • <code>na</code> (Standardeinstellung): Hosts haben keinen Zugriff auf die Freigabe oder ihre Snapshots.
<code>-advHostMgmtEnabled</code>	<p>Geben Sie an, ob Hostlisten durch die Angabe der IDs von registrierten Hosts oder durch die Verwendung einer Zeichenfolge konfiguriert werden. (Ein registrierter Host wird durch die Verwendung von <code>/remote/host</code> command definiert.) Werte sind (nicht unterschieden zwischen Groß- und Kleinschreibung):</p> <ul style="list-style-type: none"> • <code>yes</code> (Standardeinstellung): Hostlisten enthalten die IDs der registrierten Hosts. • <code>no</code> : Hostlisten enthalten durch Kommas getrennte Zeichenfolgen, wobei jede Zeichenfolge einen Hostnamen, IP, Subnetz, Netgroup oder DNS-Domain definiert. <p>Weitere Informationen über die Angabe von Hostlisten mithilfe einer Zeichenfolge finden Sie unter Angabe von Hostlisten mithilfe einer Zeichenfolge.</p>
<code>-roHosts</code>	Geben Sie die IDs von Hosts ein, die schreibgeschützten Zugriff auf die Freigabe und ihre Snapshots haben. Trennen Sie die IDs mit Komma voneinander ab. Wenn erweitertes Hostmanagement aktiviert ist, ist dies eine Liste der IDs der registrierten Hosts. Andernfalls ist dies eine Liste von Netzwerkhostnamen, IPs, Subnetzen, Domains oder Netgroups.
<code>-rwHosts</code>	Geben Sie die IDs von Hosts ein, die Lese-/Schreibzugriff auf die Freigabe und ihre Snapshots haben. Trennen Sie die IDs mit Komma voneinander ab. Wenn erweitertes Hostmanagement aktiviert ist, ist dies eine Liste der IDs der registrierten Hosts. Andernfalls ist dies eine Liste von Netzwerkhostnamen, IPs, Subnetzen, Domains oder Netgroups.
<code>-roRootHosts</code>	Geben Sie die IDs von Hosts ein, die schreibgeschützten Root-Zugriff auf die Freigabe und ihre Snapshots haben. Trennen Sie die IDs mit Komma voneinander ab. Wenn erweitertes Hostmanagement aktiviert ist, ist dies eine Liste der IDs der registrierten Hosts. Andernfalls ist dies eine Liste von Netzwerkhostnamen, IPs, Subnetzen, Domains oder Netgroups.
<code>-rootHosts</code>	Geben Sie die IDs von Hosts ein, die Lese-/Schreib-Root-Zugriff auf die Freigabe und ihre Snapshots haben. Trennen Sie die IDs mit Komma voneinander ab. Wenn erweitertes Hostmanagement aktiviert ist, ist dies eine Liste der IDs der registrierten Hosts. Andernfalls ist dies eine Liste von Netzwerkhostnamen, IPs, Subnetzen, Domains oder Netgroups.
<code>-naHosts</code>	Geben Sie die IDs der einzelnen Hostkonfigurationen ein, für die Sie den Zugriff auf die Freigabe und die zugehörigen Snapshots sperren möchten. Trennen Sie die IDs mit Komma voneinander ab. Wenn erweitertes Hostmanagement aktiviert ist, ist dies eine Liste der IDs der registrierten Hosts. Andernfalls ist dies eine Liste von Netzwerkhostnamen, IPs, Subnetzen, Domains oder Netgroups.
<code>-minSecurity</code>	<p>Geben Sie eine minimale Sicherheitsoption an, die vom Client für den NFS-Mountvorgang (in <code>fstab</code>) bereitgestellt werden muss. Der Wert kann einer der Folgenden sein, wobei das Sicherheitslevel immer weiter zunimmt: Alle höheren Sicherheitsstufen werden unterstützt und können vom Client in Verhandlungen für sicheren NFS-Zugriff durchgesetzt werden.</p> <ul style="list-style-type: none"> • <code>sys</code> : Keine serverseitige Authentifizierung (Server verlässt sich auf NFS-Clientauthentifizierung) Ohne eine konfigurierte sichere NFS für den NAS-Server ist diese Einstellung Standard. • <code>krb5</code> : Kerberos V5-Authentifizierung. Standard, wenn sicheres NFS für den NAS-Server konfiguriert ist. • <code>krb5i</code> : Kerberos v5-Authentifizierung und Integrität • <code>krb5p</code> : Kerberos v5-Authentifizierung und Integrität; Verschlüsselung ist aktiviert.
<code>-allowSuid</code>	<p>Gibt an, ob es Nutzern erlaubt ist, die UNIX-Berechtigungsbits <code>setuid</code> und <code>setgid</code> festzulegen. Werte sind (keine Unterscheidung zwischen Groß- und Kleinschreibung).</p> <ul style="list-style-type: none"> • <code>yes</code> (Standardeinstellung): Nutzer können die Unix-Berechtigungsbits <code>setuid</code> und <code>setgid</code> festlegen. Dies ermöglicht es Benutzern, die ausführbare Datei mit den Rechten des Dateieigentümers auszuführen. • <code>no</code> : Nutzer können die Unix-Berechtigungsbits <code>setuid</code> und <code>setgid</code> nicht festlegen.

Qualifizierer	Beschreibung
-anonUid	Geben Sie die UID des anonymen Kontos an.
-anonGid	Geben Sie die GID des anonymen Kontos an.

Beispiel 1

Mit dem folgenden Befehl wird die Ausgabe angezeigt für den Fall, dass der Pfad nicht gefunden wird, weil er mit nicht mit „/“ beginnt, und die Freigaben nicht erfolgreich erstellt werden.

```
uemcli -u admin -p Password123! /stor/prov/fs/nfs create -name testnfs112 -fs res_26 -path "mypath"
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation failed. Error code: 0x900a002
The system could not find the specified path. Please use an existing path. (Error
Code:0x900a002)
Job ID = N-1339
```

Beispiel 2

Mit dem folgenden Befehl wird die Ausgabe angezeigt für den Fall, dass der Pfad korrekt angegeben wird und die Freigaben erfolgreich erstellt werden. Die neue NFS-Freigabe hat die folgenden Einstellungen:

- Name der NFS-Freigabe ist „testnfs112“.
- Übergeordnetes Dateisystem ist „res_26“.
- Auf dem Verzeichnis „/mypath“

```
uemcli -u admin -p Password123! /stor/prov/fs/nfs create -name testnfs112 -fs res_26 -path "/mypath"
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = NFSShare_20
Operation completed successfully.
```

Anzeigen von Einstellungen für NFS-Freigaben

Zeigen Sie die Details zu einer NFS-Freigabe an. Sie können nach ID der NFS-Freigabe filtern oder die mit der ID eines Dateisystems verknüpften NFS-Netzwerk-Freigaben anzeigen.

 **ANMERKUNG:** Aktionsbefehl „show“ erläutert, wie das Ausgabeformat geändert wird.

Format

```
/stor/prov/fs/nfs [{-id <value> | -name <value> | -fs <value> | -fsName <value>}] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID einer NFS-Freigabe ein.
-name	Geben Sie den Namen eines NFS-Share ein.

Qualifizierer	Beschreibung
-fs	Geben Sie die ID eines NFS-Dateisystems ein, um die zugehörigen NFS-Netzwerk-Freigaben anzuzeigen.
-fsName	Geben Sie den Namen eines NFS-Dateisystems ein, um die zugehörigen NFS-Netzwerk-Shares anzuzeigen.

Beispiel

Mit dem folgenden Befehl werden Details zu sämtlichen NFS-Netzwerk-Freigaben im System aufgelistet:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/fs/nfs show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      ID                = NFSShare_1
      Name                = MyNFSshare1
      Description         = My nfs share
      File system         = res_26
      Local path          = /mypath
      Export path         = SATURN.domain.emc.com:/MyNFSshare1
      Default access      = na
      Advanced host mgmt. = yes
      Read-only hosts     = 1014, 1015
      Read/write hosts    = 1016
      Read-only root hosts =
      Root hosts         =
      No access hosts     =
      Creation time       = 2012-08-24 12:18:22
      Last modified time  = 2012-08-24 12:18:22
      Role                = production
      Minimum security    = krb5
      Allow SUID           = yes
      Anonymous UID       = 4294967294
      Anonymous GID       = 4294967294
```

Ändern von Einstellungen für NFS-Freigaben

Ändern Sie die Einstellungen einer NFS-Freigabe.

Format

```
/stor/prov/fs/nfs {-id <value> | -name <value>} set [-async] [-descr <value>] [-defAccess { ro
| rw | roroot | root | na }] [-advHostMgmtEnabled { yes | no }] [{"-roHosts <value>"} [-rwHosts
<value>"] [-roRootHosts <value>"] [-rootHosts <value>"] [-naHosts <value>"] [-addRoHosts <value>"]
[-addRwHosts <value>"] [-addRoRootHosts <value>"] [-addRootHosts <value>"] [-addNaHosts <value>"]
[-removeHosts <value>]] [-minSecurity {sys | krb5 | krb5i | krb5p}] [-allowSuid {yes | no}]
[-anonUid <value>] [-anonGid <value>]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID der zu ändernden NFS-Freigabe ein. Anzeigen von Einstellungen für NFS-Freigaben erläutert, wie Sie die IDs der NFS-Netzwerk-Shares im System anzeigen.
-name	Geben Sie den Namen des zu ändernden NFS-Share ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.
-descr	Geben Sie eine kurze Beschreibung der Freigabe ein.
-defAccess	Geben Sie die Standardeinstellung des gleichzeitigen Zugriffs für Hostkonfigurationen und nicht konfigurierte Hosts an, die auf die Freigabe zugreifen können. Folgende Werte sind möglich: <ul style="list-style-type: none"> • <code>ro</code>: Hosts haben schreibgeschützten Zugriff auf den primären Storage und auf Snapshots, die der Freigabe zugeordnet sind. • <code>rw</code>: Hosts haben Schreibzugriff auf den primären Storage und auf Snapshots, die der Freigabe zugeordnet sind. • <code>root</code>: Hosts haben schreibgeschützten Root-Zugriff auf den primären Storage und auf Snapshots, die der Freigabe zugeordnet sind. • <code>root</code>: Hosts haben Schreib-Root-Zugriff auf den primären Storage und auf Snapshots, die der Freigabe zugeordnet sind. Dieser Wert beinhaltet die Möglichkeit zur Einrichtung von Zugriffskontrollen, mit denen die Berechtigungen für andere Anmeldekonto eingeschränkt werden. • <code>na</code>: Hosts haben keinen Zugriff auf die Freigabe oder ihre Snapshots.
-advHostMgmtEnabled	Gibt an, ob die in den Hostlisten aufgeführten Hosts mithilfe der <code>/remote/host</code> -Objekte als ihre Kennung definiert werden (erweitertes Hostmanagement). Werte sind (keine Unterscheidung zwischen Groß- und Kleinschreibung). <ul style="list-style-type: none"> • <code>yes</code> (Standardeinstellung): Hostlisten enthalten die IDs der registrierten Hosts. • <code>no</code>: Hostlisten enthalten kommagetrennte Zeichenfolgen, wobei jede Zeichenfolge einen Hostnamen, eine IP-Adresse, ein Subnetz, eine Netzwerkgruppe oder eine DNS-Domain definiert. <p>Diese Einstellung kann nur aktualisiert werden, wenn die Liste der fünf Hosts unten leer ist.</p>
-roHosts	Gibt die kommagetrennte Liste von Kennungen der Hosts mit Leseberechtigung für die NFS-Freigabe an. Mit diesem Qualifizierer werden die vorhandenen schreibgeschützten Hosts überschrieben.
-rwHosts	Gibt die kommagetrennte Liste von Kennungen der Hosts mit Schreibberechtigung für die NFS-Freigabe an. Mit diesem Qualifizierer werden die vorhandenen Hosts mit Schreibzugriff überschrieben.
-roRootHosts	Gibt die kommagetrennte Liste von Kennungen der Hosts mit schreibgeschütztem Root-Zugriff auf die NFS-Freigabe an. Mit diesem Qualifizierer werden die vorhandenen schreibgeschützten Root-Hosts überschrieben.
-rootHosts	Gibt die kommagetrennte Liste von Kennungen der Hosts mit Root-Zugriff auf die NFS-Freigabe an. Dadurch werden die vorhandenen Root-Hosts mit Schreibberechtigung überschrieben.
-naHosts	Gibt die kommagetrennte Liste von Kennungen der Hosts ohne Zugriff auf die NFS-Freigabe an. Mit diesem Qualifizierer werden die vorhandenen Hosts ohne Zugriffsberechtigung überschrieben.
-addRoHosts	Gibt die kommagetrennte Liste der hinzuzufügenden Hosts mit schreibgeschütztem Zugriff auf die NFS-Freigabe an. Mit dieser Option können Sie inkrementell Hosts mit schreibgeschütztem Zugriff auf die NFS-Freigabe hinzufügen. Dadurch werden nicht alle vorhandenen schreibgeschützten Hosts überschrieben.
-addRwHosts	Gibt die kommagetrennte Liste der hinzuzufügenden Hosts mit Schreibzugriff auf die NFS-Freigabe an. Mit dieser Option können Sie inkrementell Hosts mit Schreibzugriff auf die NFS-Freigabe hinzufügen. Dadurch werden nicht alle vorhandenen Hosts mit Schreibzugriff überschrieben.
-addRoRootHosts	Gibt die kommagetrennte Liste von hinzuzufügenden Hosts mit schreibgeschütztem Root-Zugriff auf die NFS-Freigabe an. Mit dieser Option können Sie inkrementell Hosts mit schreibgeschütztem Root-Zugriff auf die NFS-Freigabe hinzufügen. Dadurch werden nicht alle vorhandenen schreibgeschützten Root-Hosts überschrieben.
-addRootHosts	Gibt die kommagetrennte Liste von Hosts an, die Schreib-Root-Zugriff auf die NFS-Freigabe erhalten. Mit dieser Option können Sie inkrementell Hosts mit Schreib-Root-Zugriff auf die NFS-Freigabe hinzufügen. Dadurch werden nicht alle vorhandenen Hosts mit Schreib-Root-Zugriff überschrieben.
-addNaHosts	Gibt die kommagetrennte Liste von Hosts ohne Zugriff auf die NFS-Freigabe an. Mit dieser Option können Sie inkrementell Hosts angeben, die keinen Zugriff auf die NFS-Freigabe haben. Dadurch werden nicht alle vorhandenen Hosts ohne Zugriffsberechtigung überschrieben.

Qualifizierer	Beschreibung
-removeHosts	Gibt die kommasetrennte Liste von Hosts an, denen der Zugriff auf die NFS-Freigabe entzogen wird. Mit dieser Option können Sie den Hostzugriff auf die NFS-Freigabe inkrementell entfernen.
-minSecurity	Gibt eine minimale Sicherheitsoption an, die vom Client für einen NFS-Mountvorgang bereitgestellt werden muss. Der Wert kann einer der Folgenden sein, wobei das Sicherheitslevel immer weiter zunimmt: Alle höheren Sicherheitsstufen werden unterstützt und können vom Client in Verhandlungen für sicheren NFS-Zugriff durchgesetzt werden. <ul style="list-style-type: none"> • <code>sys</code>: Keine serverseitige Authentifizierung (Server verlässt sich auf NFS-Clientauthentifizierung) Diese Option wird auch als <code>AUTH_SYS</code>-Sicherheit bezeichnet. • <code>krb5</code>: Kerberos V5-Authentifizierung • <code>krb5i</code>: Kerberos V5-Authentifizierung und Integrität • <code>krb5p</code>: Kerberos v5-Authentifizierung und Integrität; Verschlüsselung ist aktiviert
-allowSuid	Gibt an, ob es Nutzern erlaubt ist, die UNIX-Berechtigungsbits <code>setuid</code> und <code>setgid</code> festzulegen. Werte sind (keine Unterscheidung zwischen Groß- und Kleinschreibung). <ul style="list-style-type: none"> • <code>yes</code> (Standardeinstellung): Nutzer können die UNIX-Berechtigungsbits <code>setuid</code> und <code>setgid</code> festlegen. Dieser Wert ermöglicht Nutzern, die ausführbare Datei mit den Rechten des Dateieigentümers auszuführen. • <code>no</code>: Nutzer können die UNIX-Berechtigungsbits <code>setuid</code> und <code>setgid</code> nicht festlegen.
-anonUid	Geben Sie die UID des anonymen Kontos an.
-anonGid	Geben Sie die GID des anonymen Kontos an.

Beispiel 1

Mit dem folgenden Befehl wird festgelegt, dass bei NFS-Freigabe „NFSShare_1“ der Zugriff auf die Freigabe und die Snapshots für Host „HOST_1“ gesperrt wird:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/fs/nfs -id NFSShare_1 set
-descr "My share" -naHosts "HOST_1"
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = NFSShare_1
Operation completed successfully.
```

Beispiel 2

Mit dem folgenden Befehl wird festgelegt, dass mit der NFS-Freigabe NFSShare_1 schreibgeschützter Zugriff zur Freigabe und ihren Snapshots für Host HOST_3 hinzugefügt wird:

ANMERKUNG: HOST_2, HOST_4 und HOST_5 haben bereits schreibgeschützten Zugriff auf die Freigabe, aber die gesamte Liste der aktuellen schreibgeschützten Hosts muss immer angegeben werden, wenn Sie einen neuen schreibgeschützten Host entfernen oder hinzufügen.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/fs/nfs -id NFSShare_1 set -roHosts
HOST_2, HOST_3, HOST_4, HOST_5
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = NFSShare_1
Operation completed successfully.
```

Beispiel 3

Das folgende Beispiel zeigt Änderungen am Hostzugriff an NFSShare_2. Host_2 wird als schreibgeschützter Host hinzugefügt, Host_3 wird als Schreibhost hinzugefügt und der Zugriff wird für Host_1 entfernt:

```
uemcli /stor/prov/fs/nfs -id NFSShare_2 set -addRoHosts Host_2 -addRwHosts Host_3 -removeHosts Host_1
```

```
ID = NFSShare_2  
Operation completed successfully.
```

Löschen von NFS-Netzwerk-Shares

Löschen Sie einen NFS-Share.

Format

```
/stor/prov/fs/nfs {-id <value> | -name <value>} delete [-async]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des zu ändernden NFS-Share ein. In Anzeigen von Einstellungen für NFS-Freigaben wird erläutert, wie Sie die IDs der NFS-Netzwerk-Shares im System aufrufen können.
-name	Geben Sie den Namen des zu ändernden NFS-Share ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.

Beispiel

Mit dem folgenden Befehl wird der NFS-Share „NFSShare_1“ gelöscht:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/fs/nfs -id NFSShare_1 delete
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection  
  
Operation completed successfully.
```

Managen von SMB-Netzwerkfreigaben

SMB (Server Message Block)-Netzwerkfreigaben bieten über das SMB-Protokoll (zuvor als CIFS bezeichnet) einen Zugriffspunkt, über den konfigurierte Windows-Hosts bzw. IP-Subnetze auf Dateisystemspeicher zugreifen können. SMB-Netzwerkfreigaben sind mit einem SMB-Dateisystem verknüpft.

Die einzelnen SMB-Freigaben verfügen über eine eindeutige ID.

In der folgenden Tabelle sind die Attribute für SMB-Netzwerkfreigaben aufgeführt:

Tabelle 113. Attribute von SMB-Netzwerkfreigaben

Attribut	Beschreibung
ID	Die ID der Freigabe.
Name	Der Name der Freigabe.
Description	Kurze Beschreibung der Freigabe.
Local path	Name des Verzeichnisses innerhalb des Dateisystems, auf das die Freigabe Zugriff bietet.
Export path	Der von den Hosts für die Verbindung mit der Freigabe verwendete Exportpfad.  ANMERKUNG: Der Exportpfad ist eine Kombination aus Netzwerkname oder IP-Adresse des zugehörigen NAS-Servers und dem Namen der Freigabe.
File system	ID des übergeordneten Dateisystems, das der SMB-Freigabe zugeordnet ist.
Creation time	Der Zeitpunkt der Erstellung der Freigabe
Last modified time	Der Zeitpunkt der letzten Änderung der Freigabe
Availability enabled	Kontinuierlicher Verfügbarkeitsstatus.
Encryption enabled	SMB-Verschlüsselungsstatus
Umask	Gibt die Standard-Unix-Umask für neue Dateien an, die auf der Freigabe erstellt werden. Wenn nicht angegeben, wird die Umask standardmäßig auf 022 festgelegt.
ABE enabled	Gibt an, ob ein ABE-Filter (Access-Based Enumeration) aktiviert ist. Folgende Werte sind möglich: <ul style="list-style-type: none"> • <code>yes</code>: Filtert die Liste der verfügbaren Dateien und Ordner auf der Freigabe, sodass nur diejenigen angezeigt werden, auf die der anfragende Benutzer Zugriff hat. • <code>no</code>(Standard)
DFS enabled	Gibt an, ob DFS (Distributed File System) aktiviert ist. Folgende Werte sind möglich: <ul style="list-style-type: none"> • <code>yes</code>: Hiermit können Administratoren freigegebene Ordner gruppieren, die sich auf verschiedenen Freigaben befinden, indem sie sie transparent mit einem oder mehreren DFS-Namespaces verbinden. • <code>no</code>(Standard)
BranchCache enabled	Gibt an, ob BranchCache aktiviert ist. Folgende Werte sind möglich: <ul style="list-style-type: none"> • <code>yes</code>: Kopiert Inhalte von den Contentservern im Hauptgebäude oder der gehosteten Cloud und legt die Inhalte in Zwischenspeichern in Zweigstellen ab. Dadurch können Clientcomputer in Zweigstellen lokal auf Inhalte zugreifen anstatt über das WAN. • <code>no</code>(Standard)
Offline availability	Gibt an, ob Offlineverfügbarkeit aktiviert ist. Wenn diese Option aktiviert ist, können Benutzer mithilfe dieser Funktion auf ihren Computern mit freigegebenen Ordnern arbeiten, die auf einem Server gespeichert sind, auch wenn sie nicht mit dem Netzwerk verbunden sind. Folgende Werte sind möglich: <ul style="list-style-type: none"> • <code>none</code>: Verhindert, dass Clients Dokumente und Programme im Offline-Cache speichern. (Standard) • <code>documents</code>: Alle Dateien, die Clients aus der Freigabe öffnen, sind offline verfügbar.

Tabelle 113. Attribute von SMB-Netzwerkfreigaben (fortgesetzt)

Attribut	Beschreibung
	<ul style="list-style-type: none"> • <code>programs</code>: Alle Programme und Dateien, die Clients aus der Freigabe öffnen, sind offline verfügbar. Programme und Dateien werden vorzugsweise aus dem Offline-Cache geöffnet, auch wenn eine Verbindung zum Netzwerk besteht. • <code>manual</code>: Nur bestimmte Dateien sind offline verfügbar.

Erstellen von CIFS-Netzwerk-Freigaben

Erstellen Sie eine CIFS (SMB)-Freigabe, um ein Dateisystem über das CIFS-Protokoll zu exportieren.

Voraussetzung

Konfigurieren Sie ein Dateisystem, das Sie mit den CIFS-Netzwerk-Freigaben verknüpfen können. [Erstellen von Dateisystemen](#) erläutert, wie Sie Dateisysteme im System erstellen.

Format

```
/stor/prov/fs/cifs create [-async] -name <value> [-descr <value>] {-fs <value> | -fsName <value>} -path <value> [-enableContinuousAvailability {yes|no}] [-enableCIFSEncryption {yes|no}] [-umask <value> ] [-enableABE {yes | no} ] [-enableBranchCache {yes | no}] [-offlineAvailability {none | documents | programs | manual} ]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
<code>-async</code>	Führen Sie den Vorgang im asynchronen Modus aus.
<code>-name</code>	Geben Sie einen Namen für die Freigabe ein.  ANMERKUNG: Dieser Wert stellt zusammen mit dem Namen des NAS-Servers den Exportpfad dar, über den Hosts auf die Freigabe zugreifen.
<code>-descr</code>	Geben Sie eine kurze Beschreibung der Freigabe ein.
<code>-fs</code>	Geben Sie die Dateisystem-ID des übergeordneten Dateisystems ein, das der CIFS-Freigabe zugeordnet ist.
<code>-fsName</code>	Geben Sie den Namen des übergeordneten Dateisystems ein, das dem CIFS-Share zugeordnet ist.
<code>-path</code>	Geben Sie den Pfad zu dem Verzeichnis im Dateisystem an, das freigegeben wird. Der Pfad muss mit einem vorhandenen Verzeichnis-/Ordnernamen in der Freigabe übereinstimmen, die auf Hostseite erstellt wurde. Der standardmäßige Pfad ist das Stammverzeichnis des Dateisystems. Lokale Pfade müssen auf ein vorhandenes Verzeichnis im Dateisystem verweisen. <ul style="list-style-type: none"> • Die gleiche Pfad auf einem Dateisystem kann unbegrenzt oft freigegeben werden, aber jeder Freigabename muss eindeutig sein. Die erste Freigabe wird auf dem Stammverzeichnis des Dateisystems erstellt. • Bevor Sie zusätzliche Netzwerkfreigaben oder Unterverzeichnisse innerhalb eines NFS-Dateisystems erstellen können, müssen Sie darin Netzwerkfreigaben oder Unterverzeichnisse von einem an das Dateisystem angeschlossenen Windows-Host erstellen. Nachdem eine Freigabe von einem gemounteten Host aus erstellt wurde, können Sie eine entsprechende Freigabe im System erstellen und die Zugriffsberechtigungen entsprechend festlegen.

Qualifizierer	Beschreibung
	 ANMERKUNG: Wenn Sie die Freigabe im standardmäßigen Root-Pfad erstellen möchten, geben Sie für diese Option "/" ein.
-enableContinuousAvailability	Geben Sie an, ob die kontinuierliche Verfügbarkeit aktiviert ist.
-enableCIFSEncryption	Geben Sie an, ob die CIFS-Verschlüsselung aktiviert ist.
-umask	Geben Sie die Standard-Unix-Umask für neue Dateien ein, die auf der Freigabe erstellt werden.
-enableABE	Geben Sie an, ob Access-Based Enumeration (ABE) aktiviert ist. Gültige Werte: <ul style="list-style-type: none"> • yes • no (Standard)
-enableBranchCache	Geben Sie an, wenn BranchCache aktiviert ist. Gültige Werte: <ul style="list-style-type: none"> • yes • no (Standard)
-offlineAvailability	Geben Sie die Art der Offline-Verfügbarkeit an. Gültige Werte: <ul style="list-style-type: none"> • none (Standard): Verhindert, dass Clients Dokumente und Programme im Offline-Cache speichern. • documents : Erlaubt, dass alle Dateien, die Clients öffnen, offline verfügbar sind. • programs : Erlaubt, dass alle Programme und Dateien, die Clients öffnen, offline verfügbar sind. Programme und Dateien werden aus dem Offline-Cache geöffnet, auch wenn eine Verbindung zum Netzwerk besteht. • manual : Erlaubt nur bestimmten Dateien, offline verfügbar zu sein.

Beispiel

Mit dem folgenden Befehl wird eine CIFS-Freigabe mit den folgenden Einstellungen erstellt:

- Name: CIFSshare
- Beschreibung: My Share
- Im Zusammenhang mit Dateisystem fs1, das über die Dateisystem-ID res_20 verfügt.
- Der lokale Pfad im Dateisystem ist root "/".
 -  **ANMERKUNG:** Es ist nicht erforderlich, den vollständigen Pfad anzugeben, wenn der Pfad, in dem Sie die Freigabe erstellen möchten, bereits root ist. Geben Sie in diesem Fall "/" für den `-path` ein.
- Kontinuierliche Verfügbarkeit ist aktiviert.
- CIFS-Verschlüsselung ist aktiviert.

Die Freigabe erhält die ID „CIFSshare_1“:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/fs/cifs create -name CIFSshare
-descr "My share" -fs res_20 -path "/" -enableContinuousAvailability yes -enableCIFSEncryption
yes
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = CIFS_1
Operation completed successfully.
```

Anzeigen von Einstellungen für CIFS-Freigaben

Zeigen Sie die Details zu einer CIFS (SMB)-Freigabe an. Sie können nach ID der CIFS-Freigabe filtern oder die mit der ID eines Dateisystems verknüpfte CIFS-Netzwerk-Freigabe anzeigen.

-  **ANMERKUNG:** Aktionsbefehl „show“ erläutert, wie das Ausgabeformat geändert wird.

Format

```
/stor/prov/fs/cifs [{-id <value> | -name <value> | -fs <value> | -fsName <value>}]show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID einer CIFS-Freigabe ein.
-name	Geben Sie den Namen eines CIFS-Share ein.
-fs	Geben Sie die ID eines CIFS-Dateisystems ein, um die zugehörigen CIFS-Netzwerk-Shares anzuzeigen.
-fsName	Geben Sie den Namen eines CIFS-Dateisystems ein, um die zugehörigen CIFS-Netzwerk-Shares anzuzeigen.

Beispiel

Mit dem folgenden Befehl werden Details zu sämtlichen CIFS-Netzwerkfreigaben im System aufgelistet:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/fs/cifs show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      ID          = SMBShare_1
      Name         = fsmup
      Description  =
      File system  = res_1
      Local path   = /
      Export path  = \\sys-123.abc.xyz123.test.lab.emc.com\fsmup, \\10.0.0.0\fsmup

2:      ID          = SMBShare_2
      Name         = fsmup
      Description  =
      File system  = res_5
      Local path   = /
      Export path  = \\sys-123.abc.xyz123.test.lab.emc.com\fsmup, \\10.0.0.0\fsmup
```

Ändern der Einstellung von CIFS-Freigaben

Ändern Sie die Einstellungen einer CIFS (SMB)-Freigabe.

Format

```
/stor/prov/fs/cifs {-id <value> | -name <value>} set [-async] -name <value> [-descr <value>]
[-enableContinuousAvailability {yes|no}] [-enableCIFSEncryption {yes|no}] [-umask <value>] [-
enableABE {yes | no}] [-enableBranchCache {yes|no}] [-offlineAvailability {none| documents |
programs|manual}] [-advHostMgmtEnabled {yes | no}] [-defAccess { na | rw }] [-naHosts <value>]
[-rwHosts <value>]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID einer zu ändernden CIFS-Freigabe ein.
-name	Geben Sie den Namen eines zu ändernden CIFS-Share ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.
-descr	Gibt eine Beschreibung für die CIFS-Freigabe an.
-enableContinuousAvailability	Gibt an, ob die kontinuierliche Verfügbarkeit aktiviert ist.
-enableCIFSEncryption	Gibt an, ob die CIFS-Verschlüsselung aktiviert ist.
-umask	Geben Sie die Standard-UNIX-Umask für neue Dateien ein, die auf der Freigabe erstellt werden.
-enableABE	Geben Sie an, ob Access-Based Enumeration (ABE) aktiviert ist. Gültige Werte: <ul style="list-style-type: none"> • yes • no
-enableBranchCache	Geben Sie an, ob BranchCache aktiviert ist. Gültige Werte: <ul style="list-style-type: none"> • yes • no
-offlineAvailability	Geben Sie die Art der Offline-Verfügbarkeit an. Gültige Werte: <ul style="list-style-type: none"> • none: Verhindert, dass Clients Dokumente und Programme in einem Offline-Cache speichern. • documents: Erlaubt, dass alle Dateien, die Benutzer öffnen, offline verfügbar sind. • programs: Erlaubt, dass alle Programme und Dateien, die Nutzer öffnen, offline verfügbar sind. Diese Option umfasst Programme und Dateien, die aus einem Offline-Cache geöffnet werden, selbst wenn sie mit dem Netzwerk verbunden sind. • manual: Erlaubt nur bestimmten Dateien, offline verfügbar zu sein.
-advHostMgmtEnabled	Gibt an, ob die in den Hostlisten aufgeführten Hosts mithilfe der <code>using /remote/host</code> -Objekte definiert werden, z. B. mit ihrer Kennung (erweitertes Hostmanagement). Gültige Werte (nicht unterschieden nach Groß- und Kleinschreibung): <ul style="list-style-type: none"> • yes • no
-defAccess	Gibt die Standardzugriffsebene an. Gültige Werte sind folgende (keine Unterscheidung zwischen Groß- und Kleinschreibung): <ul style="list-style-type: none"> • rw • na
-rwHosts	Gibt die kommagetrennte Liste von Kennungen der Hosts mit Schreibberechtigung an. Mit dieser Option werden die vorhandenen Hosts mit Schreibzugriff überschrieben.
-naHosts	Gibt die durch Kommas getrennte Liste von Hostkennungen ohne Zugriffsberechtigung an. Mit dieser Option werden die vorhandenen Hosts ohne Zugriffsberechtigung überschrieben.

Beispiel

Mit dem folgenden Befehl wird die Beschreibung der CIFS-Freigabe „SMBShare_1“ auf `My share` festgelegt.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/fs/cifs -id SMBShare_1 set -descr "My share"
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = SMBShare_1
Operation completed successfully.
```

Löschen von CIFS-Netzwerk-Freigaben

Löschen Sie eine CIFS (SMB)-Freigabe.

Format

```
/stor/prov/fs/cifs {-id <value> | -name <value>} delete [-async]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des zu löschenden CIFS-Share ein.
-name	Geben Sie den Namen des zu löschenden CIFS-Share ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.

Beispiel

Mit dem folgenden Befehl wird die CIFS-Freigabe „CIFSShare_1“ gelöscht:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/fs/cifs -id CIFSShare_1 delete
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection
```

```
Operation completed successfully.
```

Managen von LUNs

Bei einer LUN handelt es sich um eine einzelne Speichereinheit, die für einen konkreten Speicherpool und eine bestimmte Menge von Fibre Channel(FC)- oder iSCSI-Speicher steht. Die LUNs haben einen Namen und eine Kennung für die Logical Unit Number (LUN-ID).

In der folgenden Tabelle sind die Attribute für LUNs aufgeführt.

Tabelle 114. LUN-Attribute

Attribut	Beschreibung
ID	ID der LUN.
Name	Name der LUN.
Description	Kurze Beschreibung der LUN.
Group	Name der Consistency Group, bei der die LUN Mitglied ist.
Storage pool ID	ID des Speicherpools, der von der LUN verwendet wird.
Storage pool	Name des Speicherpools, der von der LUN verwendet wird.
Type	Typ der LUN. Wert ist einer der folgenden (nicht unterschieden nach Groß- und Kleinschreibung): <ul style="list-style-type: none">• Primary

Tabelle 114. LUN-Attribute (fortgesetzt)

Attribut	Beschreibung
	<ul style="list-style-type: none"> Thin clone (tc bei Verwendung mit dem <code>-create</code>-Befehl.)
Base storage resource	(Gilt nur für Thin Clones) ID der Basis-LUN für den Thin Clone.
Source	(Gilt nur für Thin Clones) ID des Quell-Snapshot für den Thin Clone.
Original parent	(Gilt nur für Thin Clones) ID der übergeordneten LUN für den Thin Clone.
Health state	<p>Integritätsstatus der LUN Der Integritätsstatuscode wird in Klammern angezeigt. Folgende Werte sind möglich:</p> <ul style="list-style-type: none"> OK (5): Die LUN funktioniert normal. Degraded/Warning (10): Funktioniert, aber es ist mindestens eines der folgenden Probleme aufgetreten: <ul style="list-style-type: none"> Mindestens ein Speicherpool funktioniert nur eingeschränkt. Die Ressource ist heruntergestuft. Die Ressource hat zu wenig Speicherplatz und muss vergrößert werden. Minor failure (15): Es ist mindestens eines der folgenden Ereignisse eingetreten: <ul style="list-style-type: none"> Mindestens ein Speicherpool ist ausgefallen. Die Ressource ist nicht verfügbar. Major failure (20): Es ist mindestens eines der folgenden Ereignisse eingetreten: <ul style="list-style-type: none"> Mindestens ein Speicherpool ist ausgefallen. Die Ressource ist nicht verfügbar. Critical failure (25): Es ist mindestens eines der folgenden Ereignisse eingetreten: <ul style="list-style-type: none"> Mindestens ein Speicherpool ist nicht verfügbar. Die Ressource ist nicht verfügbar. Die Ressource hat keinen Speicherplatz mehr und muss vergrößert werden. Non-recoverable error (30): Es ist mindestens eines der folgenden Ereignisse eingetreten: <ul style="list-style-type: none"> Mindestens ein Speicherpool ist nicht verfügbar. Die Ressource ist nicht verfügbar.
Health details	Zusätzliche Integritätsinformationen.
Size	Aktuelle Größe der LUN.
Maximum size	Maximale Größe der LUN.
Thin provisioning enabled	<p>Gibt an, ob Thin Provisioning aktiviert ist. Gültige Werte:</p> <ul style="list-style-type: none"> yes no (Standard) <p>Von allen Speicherpools werden mit herkömmlichen und mit Thin Provisioning bereitgestellte Speicherressourcen unterstützt. Bei Standard-Speicherressourcen wird bei der Erstellung der Ressource die gesamte angeforderte Kapazität aus dem Pool zugewiesen. Bei Thin-Provisioning-Speicherressourcen werden immer nur Teile der Kapazität je nach tatsächlicher Nutzung zugewiesen. Da Thin-Provisioning-Speicherressourcen eine höhere Belegung aufweisen können, als ihnen tatsächlich an Speicher zugewiesen ist, ist es möglich, für Speicherpools eine Überbelegung festzulegen, damit die Pools eine höhere Speicherkapazität unterstützen können, als sie aufweisen.</p> <p> ANMERKUNG: In der Unisphere-Onlinehilfe erfahren Sie mehr zu Thin Provisioning.</p>
Data Reduction enabled	<p>Gibt an, ob die Datenreduzierung für eine Thin-LUN aktiviert ist. Gültige Werte:</p> <ul style="list-style-type: none"> yes no (Standard)
Data Reduction space saved	Eingesparter Gesamtspeicherplatz für die Thin-LUN (in Gigabyte) durch Datenreduzierung.
Data Reduction percent	Eingesparter Gesamt-Storage für die Thin-LUN (in Prozent) durch Datenreduzierung.

Tabelle 114. LUN-Attribute (fortgesetzt)

Attribut	Beschreibung
Data Reduction ratio	Verhältnis der Einsparungen zwischen Daten ohne Datenreduzierung und Daten nach der Datenreduzierung. i ANMERKUNG: Die Datenreduzierung ist für Thin-LUNs verfügbar.
Advanced deduplication enabled	Gibt an, ob für diese LUN die erweiterte Deduplizierung aktiviert ist. Diese Option ist erst verfügbar, wenn die Datenreduzierung aktiviert wurde. Ein leerer Wert weist darauf hin, dass die erweiterte Deduplizierung auf der LUN nicht unterstützt wird. Gültige Werte: <ul style="list-style-type: none"> • yes • no (Standard) i ANMERKUNG: Erweiterte Deduplizierung ist nur verfügbar auf: <ul style="list-style-type: none"> • Dynamischen oder herkömmlichen Pools in Unity 380F-, 480F-, 680F- und 880F-Systemen • Dynamische Pools in Unity-All-Flash 450F-, 550F- und 650F-Systemen • All-Flash-Pools und Hybrid-Flash-Pools in Unity Hybrid-Systemen 380, 480, 680 und 880
Current allocation	Bei aktiviertem Thin Provisioning die Menge an Primärspeicher, die zurzeit über Thin Provisioning bereitgestellt wird.
Total pool space preallocated	Der Speicherplatz, der für zukünftige Zwecke im Pool für die LUN reserviert ist, um Schreibvorgänge effizienter zu gestalten. Der Pool kann möglicherweise einen Teil dieses Platzes zurückgewinnen, wenn er ungenutzt ist und der Poolplatz knapp wird.
Total pool space used	Gesamtgröße des von der LUN genutzten Poolspeicherplatzes.
Non-base size used	(Gilt nur für Standard-LUNs) Menge des Speichers, der für die dieser LUN zugeordneten Snapshots und Thin Clones verwendet wird.
Family size used	(Gilt nur für Standard-LUNs) Menge des Speichers, der für die ganze LUN-Produktreihe verwendet wird.
Default snapshot mount point WWN	Der World Wide Name des standardmäßigen Snapshot-Einhängepunkts.
Snapshot count	Anzahl der in der LUN erstellten Snapshots.
Family snapshot count	(Gilt nur für Standard-LUNs) Anzahl der in der LUN-Produktreihe erstellten Snapshots, einschließlich aller abgeleiteten Snapshots.
Family thin clone count	(Gilt nur für Standard-LUNs) Anzahl der in der LUN-Produktreihe erstellten Thin Clones, einschließlich aller abgeleiteten Thin Clones.
Protection schedule	ID eines Schutzzeitplans, der auf die LUN angewendet wird. Anzeigen von Schutzplänen erläutert, wie Sie die IDs der Pläne im System anzeigen können.
Protection schedule paused	Gibt an, ob ein angewendeter Schutzplan zurzeit ausgesetzt ist.
WWN	World Wide Name der LUN.
Replication destination	Gibt an, ob die Speicherressource ein Ziel für eine Replikationssitzung (lokal oder remote) ist. Gültige Werte: <ul style="list-style-type: none"> • yes • no
Creation time	Der Zeitpunkt der Erstellung der Ressource.
Last modified time	Der Zeitpunkt der letzten Änderung der Ressource.
SP owner	Gibt den Standardeigentümer der LUN an. Der Wert ist SP A oder SP B.
Trespassed	Gibt an, ob die LUN an den Peer-SP umgeleitet wird. Gültige Werte: <ul style="list-style-type: none"> • yes • no

Tabelle 114. LUN-Attribute (fortgesetzt)

Attribut	Beschreibung
FAST VP policy	FAST VP-Tiering Policy für die LUN. Diese Policy definiert sowohl die anfängliche Tier-Positionierung als auch das laufende automatisierte Tiering von Daten während den Datenverlagerungsvorgängen. Gültige Werte (nicht unterschieden nach Groß- und Kleinschreibung): <ul style="list-style-type: none"> • startHighThenAuto (Standardeinstellung): Legt die anfängliche Datenplatzierung auf die Laufwerke mit der höchsten Performance und freiem Speicherplatz fest und verlagert dann Teile der Daten der Storage-Ressource basierend auf der I/O-Aktivität. • auto: Legt die anfängliche Datenplatzierung auf eine optimale, vom System bestimmte Einstellung fest und verlagert dann Teile der Daten der Speicherressource basierend auf Performancestatistiken der Speicherressource, sodass die Daten entsprechend der I/O-Aktivität auf die Tiers verlagert werden. • highest: Legt die anfängliche Datenplatzierung und nachfolgende Datenverlagerung (falls zutreffend) auf die Laufwerke mit der höchsten Performance und freiem Speicherplatz fest. • lowest: legt die anfängliche Datenplatzierung und nachfolgende Datenverlagerung (falls zutreffend) auf die kosteneffizientesten Laufwerke mit freiem Speicherplatz fest.
FAST VP distribution	Prozentsatz der LUN, der jedem Tier zugewiesen ist. Das Format lautet wie folgt: <tier_name>:<value>% Hierbei gilt: <ul style="list-style-type: none"> • <tier_name> ist der Name des Storage Tier. • <value> ist der Prozentsatz des Storage in diesem Tier.
LUN access hosts	Liste der Hosts, die über Berechtigungen zum Zugriff auf die LUN verfügen.
Host LUN IDs	Durch Komma getrennte Liste von HLUs (Host LUN Identifiers), die die entsprechenden Hosts verwenden, um auf die LUN zuzugreifen.
Snapshots access hosts	Liste der Hosts, die über Zugriff auf Snapshots der LUN verfügen.
IO limit	Name der angewendeten Host-I/O-Limit-Policy.
Effective maximum IOPS	Der effektive maximale I/O pro Sekunde für die LUN. Bei LUNs mit einer dichte-basierten IO-Limit-Policy entspricht dieser Wert dem Produkt von Maximum IOPS und Size der angehängten LUN.
Effective maximum KBPS	Die effektiven maximalen KB pro Sekunde für die LUN. Bei LUNs mit einer dichte-basierten IO-Limit-Policy entspricht dieser Wert dem Produkt von Maximum KBPS und Size der angehängten LUN.

Erstellen von LUNs

Erstellen Sie eine LUN, über die Hostinitiatoren auf Speicher zugreifen können.

Voraussetzungen

Konfigurieren Sie mindestens einen Storage-Pool für die LUN, und weisen Sie dem Pool mindestens ein Laufwerk zu. [Konfigurieren benutzerdefinierter Pools](#) erläutert, wie ein kundenspezifischer Storage-Pool im System erstellt wird.

Format

```
/stor/prov/luns/lun create [-async] -name <value> [-descr <value>] [-type {primary | tc {-source <value> | -sourceName <value>}}] [{-group <value> | groupName <value>}] [ {-pool <value> | -poolName <value>}] [-size <value>] [-thin {yes | no}] [-sched <value> [-schedPaused {yes | no}]] [-spOwner {spa | spb}] [-fastvpPolicy {startHighThenAuto | auto | highest | lowest}] [-lunHosts <value> [-hlus <value>]] [-snapHosts <value>] [-replDest {yes | no}] [-ioLimit <value>] [-dataReduction {yes [-advancedDedup {yes | no}] | no}]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.
-name	Geben Sie den Namen für die LUN ein.
-descr	Geben Sie eine kurze Beschreibung der LUN ein.
-type	Geben Sie den Typ der LUN an. Gültige Werte sind folgende (keine Unterscheidung zwischen Groß- und Kleinschreibung): <ul style="list-style-type: none"> • primary (Standard) • tc
-source	(Gilt nur für Thin Clones) Geben Sie die ID des Quellobjekts ein, das zur Erstellung von Thin Clones verwendet werden soll.
-sourceName	(Gilt nur für Thin Clones) Geben Sie den Namen des Quellobjekts ein, das zur Erstellung von Thin Clones verwendet werden soll.
-group	(Gilt nicht bei der Erstellung eines Thin Clone) Geben Sie die ID einer Konsistenzgruppe ein, der die neue LUN zugeordnet werden soll. Anzeigen von Consistency Groups erläutert, wie Informationen über Konsistenzgruppen angezeigt werden.  ANMERKUNG: Wenn keine Konsistenzgruppe für -group oder -groupName angegeben wird, wird die LUN keiner Konsistenzgruppe zugewiesen.
-groupName	(Gilt nicht bei der Erstellung eines Thin Clone) Geben Sie den Namen einer Consistency Group ein, der die neue LUN zugeordnet werden soll.  ANMERKUNG: Wenn keine Konsistenzgruppe für -group oder -groupName angegeben wird, wird die LUN keiner Konsistenzgruppe zugewiesen.
-pool	(Gilt nicht bei der Erstellung eines Thin Clone) Geben Sie die ID des Speicherpools ein, den die LUN verwenden soll.  ANMERKUNG: Beim Wert wird zwischen Groß- und Kleinschreibung unterschieden. Anzeigen von Pools erläutert, wie Sie die Namen der Speicherpools im System anzeigen können.
-poolName	(Gilt nicht bei der Erstellung eines Thin Clone) Geben Sie den Namen des Speicherpools ein, den die LUN verwenden soll.
-size	(Gilt nicht bei der Erstellung eines Thin Clone) Geben Sie die Menge des Speichers ein, der für die LUN zu reservieren ist.
-thin	(Gilt nicht bei der Erstellung eines Thin Clone) Aktivieren Sie Thin Provisioning für die LUN. Gültige Werte: <ul style="list-style-type: none"> • yes • no (Standard)
-sched	Geben Sie die ID eines Schutzplans ein, der auf die Speicherressource angewendet werden soll. Anzeigen von Schutzplänen erläutert, wie Sie die IDs der Pläne im System anzeigen können.
-schedPaused	Setzen Sie den Plan für den Qualifizierer -sched aus. Gültige Werte: <ul style="list-style-type: none"> • yes • no (Standard)
-spOwner	(Gilt nicht bei der Erstellung eines Thin Clone) Geben Sie den Standard-SP an, dem die LUN angehören wird. Das Speichersystem bestimmt den Standardwert. Gültige Werte: <ul style="list-style-type: none"> • spa • spb
-fastvpPolicy	(Gilt nicht bei der Erstellung eines Thin Clone) Geben Sie die FAST VP-Tiering Policy für die LUN an. Diese Policy definiert sowohl die anfängliche Tier-Positionierung als auch das laufende automatisierte Tiering von Daten während den Datenverlagerungsvorgängen. Gültige Werte (nicht unterschieden nach Groß- und Kleinschreibung):

Qualifizierer	Beschreibung
	<ul style="list-style-type: none"> • <code>startHighThenAuto</code> (Standardeinstellung): Legt die anfängliche Datenplatzierung auf die Laufwerke mit der höchsten Performance und freiem Speicherplatz fest und verlagert dann Teile der Daten der Storage-Ressource basierend auf der I/O-Aktivität. • <code>auto</code>: Legt die anfängliche Datenplatzierung auf eine optimale, vom System bestimmte Einstellung fest und verlagert dann Teile der Daten der Speicherressource basierend auf Performancestatistiken der Speicherressource, sodass die Daten entsprechend der I/O-Aktivität auf die Tiers verlagert werden. • <code>highest</code>: Legt die anfängliche Datenplatzierung und nachfolgende Datenverlagerung (falls zutreffend) auf die Laufwerke mit der höchsten Performance und freiem Speicherplatz fest. • <code>lowest</code>: legt die anfängliche Datenplatzierung und nachfolgende Datenverlagerung (falls zutreffend) auf die kosteneffizientesten Laufwerke mit freiem Speicherplatz fest.
<code>-lunHosts</code>	Geben Sie eine durch Komma getrennte Liste von Hosts mit Zugriff auf die LUN an.
<code>-hlus</code>	<p>Gibt die kommagetrennte Liste der Host-LUN-Kennungen an, die von den entsprechenden Hosts verwendet werden sollen, die in der Option <code>-lunHosts</code> angegeben wurden. Die Anzahl der Positionen in den beiden Listen muss übereinstimmen. Eine leere Zeichenfolge ist jedoch ein gültiger Wert für jedes Element der Liste der Host-LUN-Identifikatoren, sofern die Listenelemente durch Kommata getrennt sind. Ein solches leeres Element bedeutet, dass das System automatisch den Host-LUN-Identifikatorwert zuweisen sollte, mit dem der entsprechende Host auf die LUN zugreift.</p> <p>Wenn nicht angegeben, weist das System automatisch den Host-LUN-Kennungswert jedem Host zu, der in der Argumentliste <code>-lunHosts</code> angegeben ist.</p>
<code>-snapHosts</code>	Geben Sie eine durch Komma getrennte Liste von Hosts mit Zugriff auf Snapshots der LUN an.
<code>-replDest</code>	<p>(Gilt nicht bei der Erstellung eines Thin Clone) Gibt an, ob die Ressource ein Replikationsziel ist. Gültige Werte:</p> <ul style="list-style-type: none"> • <code>yes</code> • <code>no</code> (Standard)
<code>-ioLimit</code>	Geben Sie den Namen der anzuwendenden Host-I/O-Limit-Policy an.
<code>-dataReduction</code>	<p>(Gilt nicht bei der Erstellung eines Thin Clone) Geben Sie an, ob die Datenreduzierung für diese Thin-LUN aktiviert ist. Gültige Werte:</p> <ul style="list-style-type: none"> • <code>yes</code> • <code>no</code> (Standard) <p>i ANMERKUNG: Wenn die Datenreduzierung für eine Storage-Ressource in einem Hybridpool aktiviert ist, müssen im Pool mindestens 10 % Flash-Festplatten verfügbar sein.</p>
<code>-advancedDedup</code>	<p>Gibt an, ob die erweiterte Deduplizierung für diese LUN aktiviert ist. Diese Option ist erst verfügbar, wenn die Datenreduzierung aktiviert wurde. Ein leerer Wert weist darauf hin, dass die erweiterte Deduplizierung auf der LUN nicht unterstützt wird. Gültige Werte:</p> <ul style="list-style-type: none"> • <code>yes</code> • <code>no</code> (Standard) <p>Wenn die erweiterte Deduplizierung für eine Storage-Ressource in einem Hybridpool aktiviert ist, müssen im Pool mindestens 10 % Flash-Festplatten verfügbar sein.</p> <p>i ANMERKUNG: Erweiterte Deduplizierung ist nur verfügbar auf:</p> <ul style="list-style-type: none"> • Dynamischen oder herkömmlichen Pools in Unity 380F-, 480F-, 680F- und 880F-Systemen • Dynamische Pools in Unity-All-Flash 450F-, 550F- und 650F-Systemen • All-Flash-Pools und Hybrid-Flash-Pools in Unity Hybrid-Systemen 380, 480, 680 und 880

Beispiel 1

Mit dem folgenden Befehl wird eine LUN mit den folgenden Einstellungen erstellt:

- Name: MyLUN
- Beschreibung: My LUN
- Zugeordnet zur LUN-Konsistenzgruppe „res_1“
- Nutzt den Storage-Pool pool_1

- Größe des primären Speichers: 100 MB

Die LUN erhält die ID lun_1:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/luns/lun create -name "MyLUN"
-descr "My LUN" -type primary -group group_1 -pool pool_1 -size 100M
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = lun_1
Operation completed successfully.
```

Beispiel 2

Mit dem folgenden Befehl wird ein Thin Clone namens MyTC von SNAP_1 erstellt. Der Thin Clone erhält die ID lun_3.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/luns/lun create -name "MyTC" -descr
"My FC" -type tc -source SNAP_1
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = lun_3
Operation completed successfully.
```

Anzeigen von LUNs

Zeigen Sie die Liste der vorhandenen LUNs an.

 **ANMERKUNG:** Aktionsbefehl „show“ erläutert, wie das Ausgabeformat geändert wird.

Format

```
/stor/prov/luns/lun [{"-id <value> | name <value> | -group <value> | -groupName <value> |
-standalone}] [{"-type {primary | tc [{"-baseRes <value> | -baseResName <value> | -originalParent
<value> | -originalParentName <value> | -source <value> | -sourceName <value>}]}]} show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID für die LUN ein.
-name	Geben Sie den Namen für die LUN ein.
-group	Geben Sie die ID einer Consistency Group ein. Die Liste der LUNs in der angegebenen Consistency Group wird angezeigt.
-groupName	Geben Sie den Namen einer Consistency Group ein. Die Liste der LUNs in der angegebenen Consistency Group wird angezeigt.
-standalone	Zeigt nur LUNs an, die nicht zu einer Consistency Group gehören.
-type	Identifiziert den Typ der anzuzeigenden Ressourcen. Gültige Werte sind folgende (keine Unterscheidung zwischen Groß- und Kleinschreibung): <ul style="list-style-type: none"> • primary • tc

Qualifizierer	Beschreibung
-baseRes	(Gilt nur für Thin Clones) Geben Sie die ID einer Basis-LUN ein, nach der Thin Clones gefiltert werden sollen.
-baseResName	(Gilt nur für Thin Clones) Geben Sie den Namen einer Basis-LUN ein, nach der Thin Clones gefiltert werden sollen.
-originalParent	(Gilt nur für Thin Clones) Geben Sie die ID einer übergeordneten LUN ein, nach der Thin Clones gefiltert werden sollen.
-originalParentName	(Gilt nur für Thin Clones) Geben Sie den Namen einer übergeordneten LUN ein, nach der Thin Clones gefiltert werden sollen.
-source	(Gilt nur für Thin Clones) Geben Sie die ID eines Quell-Snapshot ein, nach dem Thin Clones gefiltert werden sollen.
-sourceName	(Gilt nur für Thin Clones) Geben Sie den Namen eines Quell-Snapshot ein, nach dem Thin Clones gefiltert werden sollen.

Beispiel 1

Mit dem folgenden Befehl werden Informationen zu sämtlichen LUNs und Thin Clones im System angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/luns/lun show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:  ID                = sv_1
   Name              = AF LUN 1
   Description       =
   Group            =
   Storage pool ID   = pool_1
   Storage pool      = Pool_1
   Type             = Primary
   Base storage resource = sv_1
   Source           =
   Original parent   =
   Health state      = OK (5)
   Health details    = "The LUN is operating normally. No action is required."
   Size             = 21474836480 (20.0G)
   Maximum size     = 281474976710656 (256.0T)
   Thin provisioning enabled = yes
   Data Reduction enabled = yes
   Data Reduction space saved = 5637144576 (5.2G)
   Data Reduction percent = 44%
   Data Reduction ratio = 1.8:1
   Advanced deduplication enabled = no
   Current allocation = 4606345216 (4.2G)
   Protection size used = 0
   Non-base size used = 0
   Family size used = 12079595520 (11.2G)
   Snapshot count    = 2
   Family snapshot count = 2
   Family thin clone count = 0
   Protection schedule = snapSch_1
   Protection schedule paused = no
   WWN               = 60:06:01:60:10:00:43:00:B7:15:A5:5B:B1:7C:01:2B
   Replication destination = no
   Creation time     = 2018-09-21 16:00:55
   Last modified time = 2018-09-21 16:01:41
   SP owner          = SPB
   Trespassed       = no
   LUN access hosts = Host_2
   Host LUN IDs     = 0
   Snapshots access hosts =
   IO limit         =
```

Effective maximum IOPS = N/A
 Effective maximum KBPS = N/A

Ändern von LUNs

Ändern Sie die Einstellungen für eine LUN.

Format

```
/stor/prov/luns/lun {-id <value> | -name <value>} set [-async] [-name <value>] [-descr <value>] [-size <value>] [{-group <value> | -groupName <value> | -standalone}] [{-sched <value> | -noSched}] [-schedPaused {yes | no}] [-spOwner {spa | spb}] [-fastvpPolicy {startHighThenAuto | auto | highest | lowest}] [{-lunHosts <value> [-hlus <value>]}] [-snapHosts <value>] | [-addHosts <value> [-hlus <value>]] [-removeHosts <value>] [-addSnapHosts <value>] [-removeSnapHosts <value>]] [-replDest {yes | no}] [{-ioLimit <value> | -noIoLimit}] [-dataReduction {yes [-advancedDedup {yes | no}] | no}]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID der zu ändernden LUN ein.
-name	Geben Sie den Namen der zu ändernden LUN ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.
-name	Geben Sie den Namen für die LUN ein.
-descr	Geben Sie eine kurze Beschreibung der LUN ein.
-group	(Gilt nicht für Thin Clones) Geben Sie die ID einer Konsistenzgruppe ein, der die neue LUN zugeordnet werden soll. Anzeigen von Consistency Groups erläutert, wie Informationen über Konsistenzgruppen angezeigt werden.  ANMERKUNG: Wenn keine Konsistenzgruppe für -group oder -groupName angegeben wird, wird die LUN keiner Konsistenzgruppe zugewiesen.
-groupName	(Gilt nicht für Thin Clones) Geben Sie den Namen einer Consistency Group ein, der die neue LUN zugeordnet werden soll.  ANMERKUNG: Wenn keine Konsistenzgruppe für -group oder -groupName angegeben wird, wird die LUN keiner Konsistenzgruppe zugewiesen.
-size	Geben Sie an, wie viel Speicher der LUN zugewiesen wird.
-standalone	(Gilt nicht für Thin Clones.) Entfernen Sie die LUN aus der Consistency Group.
-sched	Geben Sie die ID des Plans zur Anwendung der LUN ein. Anzeigen von Schutzplänen erläutert, wie Sie die IDs der Pläne im System anzeigen können.
-schedPaused	Setzen Sie den Plan für den Qualifizierer -sched aus. Gültige Werte: <ul style="list-style-type: none"> • yes • no
-noSched	Entfernt den Schutzplan aus der LUN.
-spOwner	(Gilt nicht für Thin Clones.) Geben Sie den Standardeigentümer der LUN an. Gültige Werte: <ul style="list-style-type: none"> • spa

Qualifizierer	Beschreibung
	<ul style="list-style-type: none"> • <code>spb</code>
<code>-fastvpPolicy</code>	<p>(Gilt nicht für Thin Clones.) Geben Sie die FAST VP-Tiering Policy für die LUN an. Diese Policy definiert sowohl die anfängliche Tier-Positionierung als auch das laufende automatisierte Tiering von Daten während den Datenverlagerungsvorgängen. Gültige Werte (nicht unterschieden nach Groß- und Kleinschreibung):</p> <ul style="list-style-type: none"> • <code>startHighThenAuto</code> (Standardeinstellung): Legt die anfängliche Datenplatzierung auf die Laufwerke mit der höchsten Performance und freiem Speicherplatz fest und verlagert dann Teile der Daten der Storage-Ressource basierend auf der I/O-Aktivität. • <code>auto</code>: Legt die anfängliche Datenplatzierung auf eine optimale, vom System bestimmte Einstellung fest und verlagert dann Teile der Daten der Speicherressource basierend auf Performancestatistiken der Speicherressource, sodass die Daten entsprechend der I/O-Aktivität auf die Tiers verlagert werden. • <code>highest</code>: Legt die anfängliche Datenplatzierung und nachfolgende Datenverlagerung (falls zutreffend) auf die Laufwerke mit der höchsten Performance und freiem Speicherplatz fest. • <code>lowest</code>: legt die anfängliche Datenplatzierung und nachfolgende Datenverlagerung (falls zutreffend) auf die kosteneffizientesten Laufwerke mit freiem Speicherplatz fest.
<code>-lunHosts</code>	<p>Geben Sie eine durch Komma getrennte Liste von Hosts mit Zugriff auf die LUN an.</p> <p> ANMERKUNG: Diese Liste muss alle Hosts enthalten, die Zugriff auf die LUN haben sollen. Wenn Sie Zugriff für neue Hosts hinzufügen, fügen Sie die Liste der vorhandenen Hosts in die durch Kommas getrennte Liste ein und hängen Sie die neuen Hosts an, die Zugriff haben sollen. Wenn Sie den Zugriff für Hosts entfernen, nehmen Sie die Liste der vorhandenen Hosts in die durch Komma getrennte Liste auf, aber schließen Sie die Hosts aus, denen Sie den Zugriff aus der Liste entfernen möchten.</p>
<code>-hlus</code>	<p>Gibt die kommagetrennte Liste der Host-LUN-Kennungen an, die von den entsprechenden Hosts verwendet werden sollen, die in der Option <code>-lunHosts</code> angegeben wurden. Die Anzahl der Positionen in den beiden Listen muss übereinstimmen. Eine leere Zeichenfolge ist jedoch ein gültiger Wert für jedes Element der Liste der Host-LUN-Identifikatoren, sofern die Listenelemente durch Kommata getrennt sind. Ein solches leeres Element bedeutet, dass das System automatisch den Host-LUN-Identifikatorwert zuweisen sollte, mit dem der entsprechende Host auf die LUN zugreift.</p> <p>Wenn nicht angegeben, weist das System automatisch den Host-LUN-Kennungswert jedem Host zu, der in der Argumentliste <code>-lunHosts</code> angegeben ist.</p>
<code>-replDest</code>	<p>Gibt an, ob die Ressource ein Replikationsziel ist. Gültige Werte:</p> <ul style="list-style-type: none"> • <code>yes</code> • <code>no</code> <p> ANMERKUNG: Dieser Wert muss <code>no</code> für einen Thin Clone sein.</p>
<code>-ioLimit</code>	Geben Sie den Namen der anzuwendenden Host-I/O-Limit-Policy an.
<code>-noIoLimit</code>	Geben Sie das Entfernen einer angewendeten Host-I/O-Limit-Policy an.
<code>-dataReduction</code>	<p>(Gilt nicht für Thin Clones) Gibt an, ob die Datenreduzierung für die Thin-LUN aktiviert ist. Gültige Werte:</p> <ul style="list-style-type: none"> • <code>yes</code> • <code>no</code>
<code>-advancedDedup</code>	<p>Gibt an, ob die erweiterte Deduplizierung für diese LUN aktiviert ist. Diese Option ist erst verfügbar, wenn die Datenreduzierung aktiviert wurde. Ein leerer Wert weist darauf hin, dass die erweiterte Deduplizierung auf der LUN nicht unterstützt wird. Gültige Werte:</p> <ul style="list-style-type: none"> • <code>yes</code> • <code>no</code> (Standard) <p> ANMERKUNG: Erweiterte Deduplizierung ist nur verfügbar auf:</p> <ul style="list-style-type: none"> • Dynamischen oder herkömmlichen Pools in Unity 380F-, 480F-, 680F- und 880F-Systemen • Dynamische Pools in Unity-All-Flash 450F-, 550F- und 650F-Systemen • All-Flash-Pools und Hybrid-Flash-Pools in Unity Hybrid-Systemen 380, 480, 680 und 880
<code>-addHosts</code>	Geben Sie den oder die hinzuzufügenden Hosts an, die Zugriff auf die LUN haben sollen. Sie müssen jeden Host mit Komma voneinander trennen. Mit dieser Option können Sie inkrementell Hosts hinzufügen, die auf die LUN zugreifen können. Dadurch werden nicht alle vorhandenen Hosts mit LUN-Zugriff überschrieben.

Qualifizierer	Beschreibung
-removeHosts	Geben Sie den Host oder die Hosts an, für die Sie den Zugriff auf die LUN entfernen möchten. Sie müssen jeden Host mit Komma voneinander trennen. Mit dieser Option können Sie inkrementell den Zugriff von Hosts auf die LUN entfernen. Dadurch werden nicht alle vorhandenen Hosts überschrieben, die Zugriff auf die LUN haben.
-addSnapHosts	Geben Sie den oder die hinzuzufügenden Hosts an, die Zugriff auf die LUN-Snapshots haben sollen. Sie müssen jeden Host mit Komma voneinander trennen. Mit dieser Option können Sie inkrementell Hosts hinzufügen, die auf die LUN-Snapshots zugreifen können. Dadurch werden nicht alle vorhandenen Hosts überschrieben, die auf die LUN-Snapshots zugreifen können.
-removeSnapHosts	Geben Sie den Host oder die Hosts an, für die Sie den Zugriff auf die LUN-Snapshots entfernen möchten. Sie müssen jeden Host mit Komma voneinander trennen.

Beispiel 1

Mit dem folgenden Befehl wird die LUN lun_1 mit den folgenden Einstellungen aktualisiert:

- Name: NewName.
- Beschreibung: My new description.
- Die Größe des primären Speichers beträgt 150 MB.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/luns/lun -id lun_1 set -name
NewName -descr "My new description" -size 150M
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = lun_1
Operation completed successfully.
```

Beispiel 2

Der folgende Befehl fügt Zugriff für zwei neue Hosts zu LUN „lun_2“ zusätzlich zu den vorhandenen Hosts hinzu:

- host13
- host14

i ANMERKUNG: Obwohl host1, host2 und host11 bereits Zugriff auf die LUN haben, muss die vollständige Liste der Hosts, die Zugriff auf die LUN haben sollten, angegeben werden, wenn Sie Änderungen am Hostzugriff vornehmen.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/luns/lun -id lun_2 set -lunHosts
host1, host2, host11, host13, host14
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = lun_2
Operation completed successfully.
```

Beispiel 3

Der folgende Befehl zeigt, wie Host_2 und Host_3 Zugriff auf LUN-sv_1 mit den Host-LUN-Kennungen 8 und 9 erhalten und der Zugriff auf die LUN von Host_1 entfernt wird.

```
uemcli /stor/prov/luns/lun -id sv_1 set -addHosts Host_2,Host_3 -hplus 8,9 -removeHosts Host_1
```

Beispiel 4

Der folgende Befehl zeigt, wie Host_2 und Host_3 Zugriff auf LUN-res_2 erhalten und der Zugriff von Host_1 entfernt wird:

```
uemcli -u admin -p Password123! /stor/prov/luns/group -id res_2 set -addHosts Host_2,Host_3  
-removeHosts Host_1
```

Löschen von LUNs

Löschen Sie eine LUN.

ANMERKUNG: Durch das Löschen einer LUN werden sämtliche damit verbundenen Daten aus dem System entfernt. Nachdem eine LUN gelöscht wurde, können die enthaltenen Daten nicht mehr aus Snapshots wiederhergestellt werden. Sichern Sie die Daten einer LUN auf einem anderen Host, bevor Sie sie aus dem System löschen.

Format

```
/stor/prov/luns/lun {-id <value> | -name <value>} delete [-deleteSnapshots {yes | no}] [-async]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID der zu löschenden LUN ein.
-name	Geben Sie den Namen der zu löschenden LUN ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-deleteSnapshots	Geben Sie an, dass Snapshots der LUN zusammen mit der LUN selbst gelöscht werden können. Gültige Werte: <ul style="list-style-type: none">• yes• no(Standard)
-async	Führen Sie den Vorgang im asynchronen Modus aus.

Beispiel

Mit dem folgenden Befehl wird die LUN lun_1 gelöscht:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/luns/lun -id lun_1 delete
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection
```

```
Operation completed successfully.
```

Aktualisieren von Thin Clones einer LUN

(Gilt nur für Thin Clones) Aktualisieren Sie den Thin Clone einer LUN. Dies aktualisiert die Daten des Thin Clone mit Daten von dem angegebenen Quell-Snapshot und ordnet den Thin Clone diesem Snapshot wieder über.

Format

```
/stor/prov/luns/lun {-id <value> | -name <value>} refresh [-async] {-source <value> | -sourceName <value>} [-copyName <value>] [-force]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des zu aktualisierenden Thin Clone ein.
-name	Geben Sie den Namen des zu aktualisierenden Thin Clone ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.
-source	Geben Sie die ID des Snapshot ein, der für die Aktualisierung des Thin Clone verwendet werden soll. Der Snapshot muss der Basis-LUN-Produktreihe angehören.
-sourceName	Geben Sie den Namen des Snapshot ein, der für die Aktualisierung des Thin Clone verwendet werden soll. Der Snapshot muss der Basis-LUN-Produktreihe angehören.
-copyName	Geben Sie den Namen der Kopie an, die vor der Aktualisierung des Thin Clone erstellt werden soll.
-force	Geben Sie dies an, um die LUN bedingungslos zu aktualisieren, auch wenn sie für Hostzugriff konfiguriert ist.

Beispiel

Der folgende Befehl aktualisiert den Thin Clone namens lun_5_tc mit Daten von dem Snapshot SNAP_2.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/luns/lun -id lun_5_tc refresh -source SNAP_2 -copyName Backup1
```

```
[Response]
Storage system address: 10.64.75.201
Storage system port: 443
HTTPS connection

ID = 38654705846
Operation completed successfully.
```

Managen von Consistency Groups

Consistency Groups sind eine Möglichkeit zum Organisieren und Gruppieren von LUNs, um das Speicher-Tiering und Snapshots zu vereinfachen, wenn eine Anwendung mehrere LUNs umfasst.

In der folgenden Tabelle sind die Attribute für Consistency Groups aufgeführt:

Tabelle 115. Attribute für Consistency Groups

Attribut	Beschreibung
ID	ID der Consistency Group
Name	Name der Consistency Group
Description	Kurze Beschreibung der Consistency Group
Type	Typ der Consistency Group Wert ist einer der folgenden (nicht unterschieden nach Groß- und Kleinschreibung):

Tabelle 115. Attribute für Consistency Groups (fortgesetzt)

Attribut	Beschreibung
	<ul style="list-style-type: none"> • Primary • Thin clone (tc bei Verwendung mit <code>-create</code> -Befehl.)
Base storage resource	(Gilt nur für Thin Clones) ID der Basis-Consistency-Group für den Thin Clone.
Source	(Gilt nur für Thin Clones) ID des Quell-Snapshot für den Thin Clone.
Original parent	(Gilt nur für Thin Clones) ID der übergeordneten Consistency Group für den Thin Clone.
Health state	<p>Integritätsstatus der Consistency Group Der Integritätsstatuscode wird in Klammern angezeigt. Folgende Werte sind möglich:</p> <ul style="list-style-type: none"> • OK (5): Die Ressource funktioniert normal. • Degraded/Warning (10): Funktioniert, aber es ist mindestens eines der folgenden Probleme aufgetreten: <ul style="list-style-type: none"> ○ Mindestens ein Speicherpool funktioniert nur eingeschränkt. ○ Die Ressource ist heruntergestuft. ○ Die Ressource hat zu wenig Speicherplatz und muss vergrößert werden. • Minor failure (15): Es ist mindestens eines der folgenden Ereignisse eingetreten: <ul style="list-style-type: none"> ○ Mindestens ein Speicherpool ist ausgefallen. ○ Die Ressource ist nicht verfügbar. • Major failure (20): Es ist mindestens eines der folgenden Ereignisse eingetreten: <ul style="list-style-type: none"> ○ Mindestens ein Speicherpool ist ausgefallen. ○ Die Ressource ist nicht verfügbar. • Critical failure (25): Es ist mindestens eines der folgenden Ereignisse eingetreten: <ul style="list-style-type: none"> ○ Mindestens ein Speicherpool ist nicht verfügbar. ○ Die Ressource ist nicht verfügbar. ○ Die Ressource hat keinen Speicherplatz mehr und muss vergrößert werden. • Non-recoverable error (30): Es ist mindestens eines der folgenden Ereignisse eingetreten: <ul style="list-style-type: none"> ○ Mindestens ein Speicherpool ist nicht verfügbar. ○ Die Ressource ist nicht verfügbar.
Health details	Zusätzliche Integritätsinformationen. Weitere Informationen zur Integrität finden Sie im Anhang A, Referenz.
Total capacity	Gesamtkapazität aller zugeordneten LUNs.
Total current allocation	Gesamte aktuelle Zuweisung aller zugeordneten LUNs.
Total pool space preallocated	Der Speicherplatz, der für zukünftige Zwecke im Pool für alle zugeordnete LUNs reserviert ist, um Schreibvorgänge effizienter zu gestalten. Gleich der Summe aller <code>sizePreallocated</code> -Werte jeder LUN in der Gruppe. Der Pool kann möglicherweise einen Teil dieses Speicherplatzes zurückgewinnen, wenn nur noch wenig Poolspeicherplatz frei ist.
Total pool space used	Gesamter Poolspeicherplatz, der im Pool für alle zugeordneten LUNs, ihre Snapshots oder Thin Clones sowie Overhead verwendet wird.
Thin provisioning enabled	<p>Gibt an, ob Thin Provisioning aktiviert ist. Gültige Werte sind „yes“ und „no“. Der Standardwert ist „no“. Von allen Speicherpools werden mit herkömmlichen und mit Thin Provisioning bereitgestellte Speicherressourcen unterstützt. Bei Standard-Speicherressourcen wird bei der Erstellung der Ressource die gesamte angeforderte Kapazität aus dem Pool zugewiesen. Bei Thin-Provisioning-Speicherressourcen werden immer nur Teile der Kapazität je nach tatsächlicher Nutzung zugewiesen. Da Thin-Provisioning-Speicherressourcen eine höhere Belegung aufweisen können, als ihnen tatsächlich an Speicher zugewiesen ist, ist es möglich, für Speicherpools ein Über-Provisioning festzulegen, damit die Pools eine höhere Speicherkapazität unterstützen können, als sie aufweisen.</p> <p> ANMERKUNG: In der Unisphere-Onlinehilfe erfahren Sie mehr zu Thin Provisioning.</p>
Data Reduction enabled	<p>Gibt an, ob die Datenreduzierung für die Thin-LUN aktiviert ist. Gültige Werte:</p> <ul style="list-style-type: none"> • yes

Tabelle 115. Attribute für Consistency Groups (fortgesetzt)

Attribut	Beschreibung
	<ul style="list-style-type: none"> no mixed: Gibt an, dass bei einigen LUNs in der Consistency Group die Datenreduzierung aktiviert ist, während bei anderen LUNs keine Datenreduzierung aktiviert ist.
Advanced deduplication enabled	<p>Gibt an, ob die erweiterte Deduplizierung aktiviert ist. Diese Option ist erst verfügbar, wenn die Datenreduzierung aktiviert wurde. Ein leerer Wert weist darauf hin, dass die erweiterte Deduplizierung für LUNs in der Consistency Group nicht unterstützt wird. Gültige Werte:</p> <ul style="list-style-type: none"> yes no (Standard) <p>i ANMERKUNG: Erweiterte Deduplizierung ist nur verfügbar auf:</p> <ul style="list-style-type: none"> Dynamischen oder herkömmlichen Pools in Unity 380F-, 480F-, 680F- und 880F-Systemen Dynamische Pools in Unity-All-Flash 450F-, 550F- und 650F-Systemen All-Flash-Pools und Hybrid-Flash-Pools in Unity Hybrid-Systemen 380, 480, 680 und 880
Total non-base size used	(Gilt nur für Standard-Consistency Groups) Menge des Speichers, der für die dieser Consistency Group zugeordneten Snapshots und Thin Clones verwendet wird.
Total family size used	(Gilt nur für Standard-Consistency Groups) Menge des Speichers, der für die ganze Consistency Group-Produktreihe verwendet wird.
Snapshot count	Anzahl der auf der Ressource erstellten Snapshots.
Family snapshot count	(Gilt nur für Standard-Consistency Groups) Anzahl der in der Consistency Group-Produktreihe erstellten Snapshots, einschließlich aller abgeleiteten Snapshots.
Family thin clone count	(Gilt nur für Standard-Consistency Groups) Anzahl der in der Consistency Group-Produktreihe erstellten Thin Clones, einschließlich aller abgeleiteten Thin Clones.
Protection schedule	ID eines Schutzzeitplans, der auf die Konsistenzgruppe angewendet wird. Anzeigen von Schutzplänen erläutert, wie Sie die IDs der Pläne im System anzeigen können.
Protection schedule paused	Gibt an, ob ein angewendeter Schutzplan zurzeit ausgesetzt ist.
LUN access hosts	Liste der Hosts, die über Berechtigungen zum Zugriff auf die zugeordneten LUNs verfügen. i ANMERKUNG: Hosts mit Zugriff auf die Snapshots einiger, aber nicht aller zugeordneten LUNs sind als <code>Mixed</code> markiert.
Snapshots access hosts	Liste der Hosts, die über Zugriff auf die Snapshots der zugeordneten LUNs verfügen. i ANMERKUNG: Hosts mit Zugriff auf die Snapshots einiger, aber nicht aller zugeordneten LUNs sind als Mixed markiert
Replication destination	Gibt an, ob die Speicherressource ein Ziel für eine Replikationssitzung (lokal oder remote) ist. Gültige Werte: <ul style="list-style-type: none"> yes no
Creation time	Zeitpunkt der Erstellung der Consistency Group
Last modified time	Zeitpunkt der letzten Änderung der Consistency Group
FAST VP policy	FAST VP-Tiering Policy der Consistency Group. Diese Policy definiert sowohl die anfängliche Tier-Positionierung als auch das laufende automatisierte Tiering von Daten während den Datenverlagerungsvorgängen für jede LUN in der Consistency Group. Gültige Werte (nicht unterschieden nach Groß- und Kleinschreibung): <ul style="list-style-type: none"> <code>startHighThenAuto</code> (Standardeinstellung): Legt die anfängliche Datenplatzierung auf die Laufwerke mit der höchsten Performance und freiem Speicherplatz fest und verlagert dann Teile der Daten der Storage-Ressource basierend auf der I/O-Aktivität. <code>auto</code>: Legt die anfängliche Datenplatzierung auf eine optimale, vom System bestimmte Einstellung fest und verlagert dann Teile der Daten der Speicherressource basierend auf

Tabelle 115. Attribute für Consistency Groups (fortgesetzt)

Attribut	Beschreibung
	<p>Performancestatistiken der Speicherressource, sodass die Daten entsprechend der I/O-Aktivität auf die Tiers verlagert werden.</p> <ul style="list-style-type: none"> • highest: Legt die anfängliche Datenplatzierung und nachfolgende Datenverlagerung (falls zutreffend) auf die Laufwerke mit der höchsten Performance und freiem Speicherplatz fest. • lowest: legt die anfängliche Datenplatzierung und nachfolgende Datenverlagerung (falls zutreffend) auf die kosteneffizientesten Laufwerke mit freiem Speicherplatz fest. • Mixed: Wert, wenn die LUNs in der Consistency Group verschiedene FAST VP-Policies verwenden.
FAST VP distribution	<p>Jedem Tier zugewiesener Prozentsatz der Ressource Das Format lautet wie folgt: <code><tier_name>:<value>%</code></p> <p>Hierbei gilt:</p> <ul style="list-style-type: none"> • <code><tier_name></code> ist der Name des Storage Tier. • <code><value></code> ist der Prozentsatz des Storage in diesem Tier.

Erstellen einer Consistency Group

Erstellen Sie eine Consistency Group.

Format

```
/stor/prov/luns/group create [-async] -name <value> [-descr <value>] [-type {primary | tc { -source <value> | -sourceName <value> } }] [-sched <value> [-schedPaused {yes | no}]] [-replDest {yes | no}]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.
-name	<p>Geben Sie den Namen der Consistency Group ein.</p> <p>ANMERKUNG: Entscheiden Sie sich für einen Namen, aus dem der Typ und die Version der dafür vorgesehenen Anwendung hervorgehen. Dies erleichtert das Management und die Überwachung der Speicherressource über Unisphere.</p>
-descr	Geben Sie eine kurze Beschreibung der Consistency Group ein.
-type	<p>Geben Sie den Typ der Consistency Group an. Gültige Werte sind folgende (keine Unterscheidung zwischen Groß- und Kleinschreibung):</p> <ul style="list-style-type: none"> • primary (Standard) • tc
-source	(Gilt nur für Thin Clones) Geben Sie die ID des Quell-Snapshot ein, der zur Erstellung von Thin Clones verwendet werden soll.
-sourceName	(Gilt nur für Thin Clones) Geben Sie den Namen des Quell-Snapshot ein, der zur Erstellung von Thin Clones verwendet werden soll.
-sched	Geben Sie die ID eines Schutzplans ein, der auf die Konsistenzgruppe angewendet werden soll. Anzeigen von Schutzplänen erläutert, wie Sie die IDs der Pläne im System anzeigen können.
-schedPaused	<p>Geben Sie an, ob der für -sched angegebene Schutzplan ausgesetzt werden soll. Gültige Werte:</p> <ul style="list-style-type: none"> • yes • no (Standard)

Qualifizierer	Beschreibung
-replDest	(Gilt nicht bei der Erstellung eines Thin Clone) Gibt an, ob die Ressource ein Replikationsziel ist. Gültige Werte: <ul style="list-style-type: none"> • yes • no (Standard)

Beispiel

Mit dem folgenden Befehl wird eine Consistency Group mit den folgenden Einstellungen erstellt:

- Name: GenericStorage01.
- Beschreibung: „MyStorage“.
- Schutzplan SCHED_1

Die Konsistenzgruppe erhält die ID res_1:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/luns/group create -name GenericStorage01 -descr "MyStorage" -sched SCHED_1
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = res_1
Operation completed successfully.
```

Beispiel 2

Mit dem folgenden Befehl wird ein Thin Clone mit den folgenden Einstellungen erstellt:

- Name: MyFC
- Quelle: SNAP_1

Der Thin Clone der Konsistenzgruppe erhält die ID res_2:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/luns/group create name "MyFC" -descr "My FC" -type tc -sourceName SNAP_1
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = res_2
Operation completed successfully.
```

Anzeigen von Consistency Groups

Zeigen Sie die Liste der vorhandenen Consistency Groups an.

Format

```
/stor/prov/luns/group [{"-id <value> | -name <value> | -type {primary | tc [{"-originalParent <value> | -originalParentName <value> | -source <value> | -sourceName <value> | -baseRes <value> | -baseResName <value>}]}]}] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID einer Consistency Group ein.

Qualifizierer	Beschreibung
-name	Geben Sie den Namen einer Consistency Group ein.
-type	Identifiziert den Typ der anzuzeigenden Ressourcen. Gültige Werte sind folgende (keine Unterscheidung zwischen Groß- und Kleinschreibung): <ul style="list-style-type: none"> • primary • tc
-originalParent	(Gilt nur für Thin Clones) Geben Sie die ID einer übergeordneten Consistency Group ein, nach der Thin Clones gefiltert werden sollen.
-originalParentName	(Gilt nur für Thin Clones) Geben Sie den Namen einer übergeordneten Consistency Group ein, nach der Thin Clones gefiltert werden sollen.
-source	(Gilt nur für Thin Clones) Geben Sie die ID eines Quell-Snapshot ein, nach dem Thin Clones gefiltert werden sollen.
-sourceName	(Gilt nur für Thin Clones) Geben Sie den Namen eines Quell-Snapshot ein, nach dem Thin Clones gefiltert werden sollen.
-baseRes	(Gilt nur für Thin Clones) Geben Sie die ID einer Basis-Consistency-Group ein, nach der Thin Clones gefiltert werden sollen.
-baseResName	(Gilt nur für Thin Clones) Geben Sie den Namen einer Basis-Consistency-Group ein, nach der Thin Clones gefiltert werden sollen.

Beispiel

Mit dem folgenden Befehl werden Details zu Consistency Groups und Thin Clones im System angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/luns/group show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      ID                = res_1
      Name                = MyLUNGroup
      Description          = My Consistency group
      Type                 = Primary
      Base storage resource =
      Source               =
      Original parent      =
      Health state         = OK (5)
      Health details       = "The component is operating normally. No action is
required."
      Total capacity       = 107374182400 (100G)
      Thin provisioning enabled = no
      Total current allocation = 107374182400 (100G)
      Total pool space preallocated = 4292853760 (3.9G)
      Total Pool Space Used = 9128919040 (8.5G)
      Total protection size used = 0
      Snapshot count       = 0
      Family snapshot count = 0
      Family thin clone count = 0
      Data Reduction enabled = yes
      Advanced deduplication enabled = yes
      Total current allocation = 10737418240 (10G)
      Protection schedule = SCHD_1
      Protection schedule paused = no
      LUNs access hosts = 1014, 1015
      Snapshots access hosts = 1016 (mixed)
      Replication destination = no
      Creation time         = 2019-08-10 12:55:32
      Last modified time    = 2019-09-10 10:31:56
      FAST VP policy        = mixed
      FAST VP distribution  = Extreme Performance: 55%, Performance: 10%,
Capacity: 35%
```

```

2:      ID = res_1
      Name = MyLUNGroup
      Description = My Consistency group
      Type = Primary
      Base storage resource =
      Source =
      Original parent =
      Health state = OK (5)
      Health details = "The component is operating normally. No
action  is required."
      Total capacity = 107374182400 (100G)
      Thin provisioning enabled = no
      Total current allocation = 107374182400 (100G)
      Total pool space preallocated = 4292853760 (3.9G)
      Total Pool Space Used = 9128919040 (8.5G)
      Total protection size used = 0
      Snapshot count = 0
      Family snapshot count = 0
      Family thin clone count = 0
      Data Reduction enabled = yes
      Advanced deduplication enabled = yes
      Total current allocation = 10737418240 (10G)
      Protection schedule = SCHED_1
      Protection schedule paused = no
      LUNs access hosts = 1014, 1015
      Snapshots access hosts = 1016(mixed)
      Replication destination = no
      Creation time = 2012-12-21 12:55:32
      Last modified time = 2013-01-15 10:31:56
      FAST VP policy = mixed
      FAST VP distribution = Extreme Performance: 55%, Performance: 10%,
Capacity: 35%

```

Ändern von Consistency Groups

Ändern Sie die Einstellungen für eine Consistency Group.

Format

```

/stor/prov/luns/group {-id <value> | -name <value>} set [-async] [-name <value>] [-descr
<value>] [{"-sched <value> | -noSched}] [{"-schedPaused {yes | no}} [{"-lunHosts <value>} [-
snapHosts <value>] | [-addHosts <value>] [-removeHosts <value>] [-addSnapHosts <value>] [-
removeSnapHosts <value>}]] [{"-replDest {yes | no}} [{"-fastvpPolicy {startHighThenAuto | auto |
highest | lowest}}] [{"-dataReduction {yes [-advancedDedup {yes | no}}] | no}}]

```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID der zu ändernden Consistency Group ein.
-name	Geben Sie den Namen der zu ändernden Consistency Group ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.
-name	Geben Sie den Namen der Consistency Group ein.
-descr	Geben Sie eine kurze Beschreibung der Consistency Group ein.

Qualifizierer	Beschreibung
-sched	Geben Sie die ID des Plans ein, der auf die Konsistenzgruppe angewendet werden soll. Anzeigen von Schutzplänen erläutert, wie Sie die IDs der Pläne im System anzeigen können.
-schedPaused	Setzen Sie den Plan für den Qualifizierer -sched aus. Gültige Werte: <ul style="list-style-type: none"> • yes • no (Standard)
-noSched	Heben Sie die Schutzplanzuweisung auf.
-lunHosts	Gibt die kommagetrennte Liste von Hosts mit Zugriff auf LUNs an. Mit diesem Qualifizierer wird der vorhandene Hostzugriff auf die LUNs überschrieben.
-snapHosts	Gibt die durch Kommas getrennte Liste von Hosts mit Zugriff auf Snapshots an. Mit diesem Qualifizierer wird der vorhandene Hostzugriff auf die LUN-Snapshots überschrieben.
-addHosts	Gibt die kommagetrennte Liste der hinzuzufügenden Hosts mit Zugriff auf LUNs an. Mit dieser Option können Sie inkrementell Hosts hinzufügen, die auf die LUNs zugreifen können. Dadurch werden nicht alle vorhandenen Hosts überschrieben, die Zugriff auf die LUNs haben.
-removeHosts	Gibt die kommagetrennte Liste von Hosts an, deren Zugriff auf die LUNs entfernt werden soll. Mit dieser Option können Sie inkrementell den Zugriff von Hosts auf die LUNs entfernen.
-addSnapHosts	Gibt die kommagetrennte Liste der hinzuzufügenden Hosts mit Zugriff auf die LUN-Snapshots an. Mit dieser Option können Sie inkrementell Hosts hinzufügen, die auf die LUN-Snapshots zugreifen können. Dadurch werden nicht alle vorhandenen Hosts überschrieben, die Zugriff auf die LUNs haben.
-removeSnapHosts	Gibt die kommagetrennte Liste von Hosts an, deren Zugriff auf die LUN-Snapshots entfernt werden soll. Mit dieser Option können Sie inkrementell den Zugriff von Hosts auf die LUN-Snapshots entfernen.
-replDest	Geben Sie an, ob die Ressource ein Replikationsziel ist. Gültige Werte: <ul style="list-style-type: none"> • yes • no (Standard)  ANMERKUNG: Dieser Wert muss no für einen Thin Clone sein.
-fastvpPolicy	(Kann für Thin Clones nicht geändert werden) Geben Sie die FAST VP-Tiering Policy der Consistency Group an. Diese Policy definiert sowohl die anfängliche Tier-Positionierung als auch das laufende automatisierte Tiering von Daten während den Datenverlagerungsvorgängen. Gültige Werte (nicht unterschieden nach Groß- und Kleinschreibung): <ul style="list-style-type: none"> • startHighThenAuto (Standardeinstellung): Legt die anfängliche Datenplatzierung auf die Laufwerke mit der höchsten Performance und freiem Speicherplatz fest und verlagert dann Teile der Daten der Storage-Ressource basierend auf der I/O-Aktivität. • auto: Legt die anfängliche Datenplatzierung auf eine optimale, vom System bestimmte Einstellung fest und verlagert dann Teile der Daten der Storage-Ressource basierend auf Performancestatistiken der Storage-Ressource, sodass die Daten entsprechend der I/O-Aktivität auf die Tiers verlagert werden. • highest: Legt die anfängliche Datenplatzierung und nachfolgende Datenverlagerung (falls zutreffend) auf die Laufwerke mit der höchsten Performance und freiem Speicherplatz fest. • lowest: legt die anfängliche Datenplatzierung und nachfolgende Datenverlagerung (falls zutreffend) auf die kosteneffizientesten Laufwerke mit freiem Speicherplatz fest.
-dataReduction	(Kann für Thin Clones nicht geändert werden) Gibt an, ob die Datenreduzierung für Thin-LUNs in dieser Konsistenzgruppe aktiviert ist. Gültige Werte: <ul style="list-style-type: none"> • yes • no
-advancedDedup	Gibt an, ob die erweiterte Deduplizierung für LUNs in dieser Consistency Group aktiviert ist. Diese Option ist erst verfügbar, wenn die Datenreduzierung aktiviert wurde. Ein leerer Wert weist darauf hin, dass die erweiterte Deduplizierung für LUNs in dieser Consistency Group nicht unterstützt wird. Gültige Werte: <ul style="list-style-type: none"> • yes • no (Standard)  ANMERKUNG: Erweiterte Deduplizierung ist nur verfügbar auf: <ul style="list-style-type: none"> • Dynamischen oder herkömmlichen Pools in Unity 380F-, 480F-, 680F- und 880F-Systemen • Dynamische Pools in Unity-All-Flash 450F-, 550F- und 650F-Systemen

Qualifizierer	Beschreibung
	<ul style="list-style-type: none"> All-Flash-Pools und Hybrid-Flash-Pools in Unity Hybrid-Systemen 380, 480, 680 und 880

Beispiel 1

Mit dem folgenden Befehl wird die Konsistenzgruppe res_1 mit den folgenden Einstellungen aktualisiert:

- Name: NewName
- Beschreibung: „New description“
- Schutzplan: SCHED_2
- Der ausgewählte Plan ist zurzeit ausgesetzt
- Die FAST VP Policy ist „start high then auto-tier“

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/luns/group -id res_1 set -name NewName -descr "New description" -sched SCHED_2 -schedPaused yes -fastvpPolicy startHighThenAuto
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = res_1
Operation completed successfully.
```

Beispiel 2

Mit dem folgenden Befehl wird der Snapshot-Zugriff für die neuen Hosts Host_1 und Host_21 auf die Snapshots der Konsistenzgruppe res_23 hinzugefügt.

ANMERKUNG: Obwohl Host_3 und Host_18 bereits über Snapshot-Zugriff für die CG verfügen, muss die vollständige Liste der Hosts, die über Snapshot-Zugriff verfügen sollten, immer wieder angegeben werden, wenn neue Hosts hinzugefügt werden.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/luns/group -id res_23 set -name NewName -snapHosts Host_1, Host_3, Host_18, Host_21
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = res_23
Operation completed successfully.
```

Löschen von Consistency Groups

Löschen Sie eine Consistency Group.

ANMERKUNG: Beim Löschen einer Consistency Group werden alle ihr zugeordneten LUNs und Daten mit der Consistency Group aus dem System gelöscht. Nach dem Löschen einer Consistency Group können die Daten nicht aus Snapshots wiederhergestellt werden. Sichern Sie die Daten der Konsistenzgruppe, bevor Sie sie löschen.

Format

```
/stor/prov/luns/group {-id <value> | -name <value> } delete -id <value> [-async]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID der zu löschenden Consistency Group ein.

Qualifizierer	Beschreibung
-name	Geben Sie den Namen der zu löschenden Consistency Group ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-deleteSnapshots	Geben Sie an, dass Snapshots der LUN zusammen mit der LUN selbst gelöscht werden können. Gültige Werte: <ul style="list-style-type: none"> • yes • no (Standard)
-async	Führen Sie den Vorgang im asynchronen Modus aus.

Beispiel

Mit dem folgenden Befehl wird LUN-Konsistenzgruppe res_1 gelöscht:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/luns/group -id res_1 delete
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Aktualisieren von Thin Clones einer Consistency Group

(Gilt nur für Thin Clones) Aktualisieren Sie den Thin Clone einer Consistency Group. Dies aktualisiert die Daten des Thin Clone mit Daten von dem angegebenen Quell-Snapshot und ordnet den Thin Clone diesem Snapshot wieder über.

Format

```
/stor/prov/luns/group {-id <value> | -name <value>} refresh [-async] {-source <value> |
-sourceName <value>} [-copyName <value>] [-force]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID der zu aktualisierenden Consistency Group ein.
-name	Geben Sie den Namen der zu aktualisierenden Consistency Group ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.
-source	Geben Sie die ID des Snapshot ein, der für die Aktualisierung des Thin Clone verwendet werden soll. Der Snapshot muss der Produktreihe der Basis-Consistency-Group angehören.
-sourceName	Geben Sie den Namen des Snapshot ein, der für die Aktualisierung des Thin Clone verwendet werden soll. Der Snapshot muss der Produktreihe der Basis-Consistency-Group angehören.
-copyName	Geben Sie den Namen der Kopie an, die vor der Aktualisierung des Thin Clone erstellt werden soll.

Qualifizierer	Beschreibung
-force	Die Consistency Group wird bedingungslos aktualisiert, auch wenn auf der Speicherressource Hostzugriff konfiguriert wurde.

Beispiel

Der folgende Befehl aktualisiert den Thin Clone namens res_2_tc mit Daten des Snapshot SNAP_10.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/luns/group -id res_2_tc refresh
-source SNAP_10 -copyName Backup1
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = 38654705846
Operation completed successfully.
```

Managen von VMware NFS-Datenspeichern

VMware NFS-Datenspeichern bieten einen dateibasierten Speicher für VMware ESX-Server zum Hosten virtueller Maschinen (VM). Sie können NFS-Datstores bereitstellen und managen und Details zu jedem NFS-Datstore im System anzeigen, z. B. deren Speicherkapazität und Integrität.

Die einzelnen NFS-Datenspeicher verfügen über eine eindeutige ID.

ANMERKUNG: Sie können keinen NFS-Datenspeicher auf einem NAS-Server erstellen, der IP-Mehrmandantenfähigkeit verwendet.

In der folgenden Tabelle werden die Attribute für NFS-Datenspeicher aufgeführt:

Tabelle 116. Attribute für NFS-Datstores

Attribut	Beschreibung
ID	ID des NFS-Datstore
Name	Name des NFS-Datstore
Description	Beschreibung des NFS-Datstore
Health state	<p>Integritätsstatus des NFS-Datenspeichers Der Integritätsstatuscode wird in Klammern angezeigt. Folgende Werte sind möglich:</p> <ul style="list-style-type: none"> • OK (5): Der NFS-Datenspeicher funktioniert normal. • OK_BUT (7): Der NFS-Datenspeicher funktioniert, aber mindestens eines der beiden folgenden Probleme ist aufgetreten: <ul style="list-style-type: none"> ○ Die Speicherressource wird initialisiert oder gelöscht. ○ Das Dateisystem für diese Speicherressource reicht in Kürze nicht mehr aus. Weisen Sie der Speicherressource mehr Speicherplatz zu. • Degraded/Warning (10): Funktioniert, aber es ist mindestens eines der folgenden Probleme aufgetreten: <ul style="list-style-type: none"> ○ Mindestens ein Speicherpool funktioniert nur eingeschränkt. ○ Eine Replikationssitzung für die Speicherressource wird heruntergestuft. ○ Die Kapazitätshöchstgrenze ist nahezu erreicht. Zur Vermeidung von Datenverlusten müssen Sie die Primärspeichergröße erhöhen oder zusätzliche NFS-Datenspeicher für die Speicherung der Daten anlegen. • Minor failure (15): Es ist mindestens eines der folgenden Ereignisse eingetreten: <ul style="list-style-type: none"> ○ Mindestens ein Speicherpool ist ausgefallen. ○ Der zugehörige NAS-Server ist ausgefallen. • Major failure (20): Es ist mindestens eines der folgenden Ereignisse eingetreten: <ul style="list-style-type: none"> ○ Mindestens ein Speicherpool ist ausgefallen.

Tabelle 116. Attribute für NFS-Datstores (fortgesetzt)

Attribut	Beschreibung
	<ul style="list-style-type: none"> ○ NFS-Datenspeicher ist nicht verfügbar. ● <code>Critical failure (25)</code>: Es ist mindestens eines der folgenden Ereignisse eingetreten: <ul style="list-style-type: none"> ○ Mindestens ein Speicherpool ist nicht verfügbar. ○ NFS-Datenspeicher ist nicht verfügbar. ○ Die volle Kapazität des NFS-Datenspeicher ist erreicht. Zur Vermeidung von Datenverlusten sollten Sie die Primärspeichergröße erhöhen oder zusätzliche NFS-Datstores für die Speicherung der Daten anlegen. ● <code>Non-recoverable error (30)</code>: Es ist mindestens eines der folgenden Ereignisse eingetreten: <ul style="list-style-type: none"> ○ Mindestens ein Speicherpool ist nicht verfügbar. ○ NFS-Datenspeicher ist nicht verfügbar.
Health details	Zusätzliche Integritätsinformationen. Weitere Informationen zur Integrität finden Sie im Anhang A, Referenz.
File system	Kennung des Dateisystems. Die Dateisystem-ID wird für einige Kennzahlbefehle angezeigt. Verwenden Sie diese ID, um die Kennzahlausgabe mit dem zugehörigen NFS-Datenspeicher zu korrelieren.
Server	Name des primären NAS-Servers, der vom NFS-Datenspeicher verwendet wird.
Storage pool ID	Kennung des vom NFS-Datenspeicher verwendeten Speicherpools.
Storage pool	Name des vom NFS-Datenspeicher verwendeten Speicherpools
Size	Für primäre Daten reservierter Speicher
Size used	Die zurzeit für primäre Daten verwendete Speichermenge.
Maximum size	Maximale Größe, auf die die Kapazität des primären Speichers erweitert werden kann.
Host I/O size	<p>Typische Schreib-I/O-Größe vom Host zu VMware-Datenspeicher. Diese Einstellung wird verwendet, um die Speicherblockgröße der I/O der primären Anwendung mithilfe des VMware-Datenspeichers zuzuordnen, der I/O-Performance optimieren kann. Die Host-I/O-Größe kann nur bei der Erstellung konfiguriert werden. Gültige Werte:</p> <ul style="list-style-type: none"> ● 8K ● 16K ● 32K ● 64K ● Exchange 2007 (8K) ● Exchange 2010 (32K) ● Exchange 2013 (32K) ● Oracle (8K) ● SQL Server (8K) ● VMware Horizon VDI (8K) ● SharePoint (32K) ● SAP (8K)
Thin provisioning enabled	<p>Gibt an, ob Thin Provisioning aktiviert ist. Gültige Werte sind „yes“ und „no“. Der Standardwert ist „no“. Von allen Speicherpools werden mit herkömmlichen und mit Thin Provisioning bereitgestellte Speicherressourcen unterstützt. Bei Standard-Speicherressourcen wird bei der Erstellung der Ressource die gesamte angeforderte Kapazität aus dem Pool zugewiesen. Bei Thin-Provisioning-Speicherressourcen werden immer nur Teile der Kapazität je nach tatsächlicher Nutzung zugewiesen. Da Thin-Provisioning-Speicherressourcen eine höhere Belegung aufweisen können, als ihnen tatsächlich an Speicher zugewiesen ist, ist es möglich, für Speicherpools ein Über-Provisioning festzulegen, damit die Pools eine höhere Speicherkapazität unterstützen können, als sie aufweisen.</p> <p> ANMERKUNG: In der Unisphere-Onlinehilfe erfahren Sie mehr zu Thin Provisioning.</p>
Data Reduction enabled	Gibt an, ob Datenreduzierung für diese Ressource aktiviert ist. Gültige Werte:

Tabelle 116. Attribute für NFS-Datstores (fortgesetzt)

Attribut	Beschreibung
	<ul style="list-style-type: none"> • yes • no (Standard) <p>i ANMERKUNG: Die Datenreduzierung ist für Thin-Dateisysteme verfügbar. Die Thin-Dateisysteme müssen auf Unity-Systemen erstellt worden sein, auf denen Version 4.2.x oder höher ausgeführt wird.</p>
Data Reduction space saved	<p>Eingesparter Gesamtspeicherplatz (in GB) für diese Ressource durch Datenreduzierung.</p> <p>i ANMERKUNG: Die Datenreduzierung ist für Thin-Dateisysteme verfügbar. Die Thin-Dateisysteme müssen auf Unity-Systemen erstellt worden sein, auf denen Version 4.2.x oder höher ausgeführt wird.</p>
Data Reduction percent	<p>Eingesparter Gesamtspeicher für die Ressource durch Datenreduzierung (in Prozent).</p> <p>i ANMERKUNG: Die Datenreduzierung ist für Thin-Dateisysteme verfügbar. Die Thin-Dateisysteme müssen auf Unity-Systemen erstellt worden sein, auf denen Version 4.2.x oder höher ausgeführt wird.</p>
Data Reduction ratio	<p>Verhältnis zwischen dem gesamten belegten Speicher vor der Datenreduzierung und nach der Datenreduzierung für diese Ressource.</p> <p>i ANMERKUNG: Die Datenreduzierung ist für Thin-Dateisysteme verfügbar. Die Thin-Dateisysteme müssen auf Unity-Systemen erstellt worden sein, auf denen Version 4.2.x oder höher ausgeführt wird.</p>
Advanced deduplication enabled	<p>Gibt an, ob für diese Ressource die erweiterte Deduplizierung aktiviert ist. Diese Option ist erst verfügbar, wenn die Datenreduzierung aktiviert wurde. Ein leerer Wert zeigt an, dass die erweiterte Deduplizierung auf der Ressource nicht unterstützt wird. Gültige Werte:</p> <ul style="list-style-type: none"> • yes • no (Standard) <p>i ANMERKUNG: Erweiterte Deduplizierung ist nur verfügbar auf:</p> <ul style="list-style-type: none"> • Dynamischen oder herkömmlichen Pools in Unity 380F-, 480F-, 680F- und 880F-Systemen • Dynamische Pools in Unity-All-Flash 450F-, 550F- und 650F-Systemen • All-Flash-Pools und Hybrid-Flash-Pools in Unity Hybrid-Systemen 380, 480, 680 und 880
Current allocation	<p>Wenn diese Option aktiviert ist, wird hier angezeigt, wie viel primärer Speicher zurzeit über Thin Provisioning bereitgestellt wird.</p>
Total pool space preallocated	<p>Der Speicherplatz, der für zukünftige Zwecke im Pool für den NFS-Datenspeicher reserviert ist, um Schreibvorgänge effizienter zu gestalten. Der Pool kann möglicherweise einen Teil dieses Speicherplatzes zurückgewinnen, wenn er vom NFS-Datenspeicher ungenutzt bleibt und der Pool wenig Platz hat.</p>
Total pool space used	<p>Gesamtspeicherplatz im Pool, der vom NFS-Datenspeicher verwendet wird.</p>
Minimum size allocated	<p>(Wird angezeigt für Dateisysteme, die auf einem Unity-System mit OE-Version 4.1 erstellt wurden.) Gibt die Mindestmenge des primären Speichers an, der dem NFS-Datenspeicher über Thin Provisioning bereitgestellt wird. Dateiverkleinerungsvorgänge können die Dateisystemgröße nicht unter diesen Wert reduzieren.</p>
Protection size used	<p>Aktuell mit Schutzdaten belegter Speicher.</p>
Snapshot count	<p>Die Speichergröße des Datenschutzespeichers, der zurzeit über Thin Provisioning bereitgestellt wird.</p>
Protection schedule	<p>ID eines angewendeten Schutzplans.</p>
Protection schedule paused	<p>Gibt an, ob ein angewendeter Schutzplan zurzeit ausgesetzt ist. Gültige Werte sind „yes“ und „no“.</p>
FAST VP policy	<p>FAST VP-Tiering Policy für den NFS-Datenspeicher. Diese Policy definiert sowohl die anfängliche Tier-Positionierung als auch das laufende automatisierte Tiering von Daten</p>

Tabelle 116. Attribute für NFS-Datstores (fortgesetzt)

Attribut	Beschreibung
	während den Datenverlagerungsvorgängen. Gültige Werte (nicht unterschieden nach Groß- und Kleinschreibung): <ul style="list-style-type: none"> • <code>startHighThenAuto</code> (Standardeinstellung): Legt die anfängliche Datenplatzierung auf die Laufwerke mit der höchsten Performance und freiem Speicherplatz fest und verlagert dann Teile der Daten der Storage-Ressource basierend auf der I/O-Aktivität. • <code>auto</code>: Legt die anfängliche Datenplatzierung auf eine optimale, vom System bestimmte Einstellung fest und verlagert dann Teile der Daten der Speicherressource basierend auf Performancestatistiken der Speicherressource, sodass die Daten entsprechend der I/O-Aktivität auf die Tiers verlagert werden. • <code>highest</code>: Legt die anfängliche Datenplatzierung und nachfolgende Datenverlagerung (falls zutreffend) auf die Laufwerke mit der höchsten Performance und freiem Speicherplatz fest. • <code>lowest</code>: legt die anfängliche Datenplatzierung und nachfolgende Datenverlagerung (falls zutreffend) auf die kosteneffizientesten Laufwerke mit freiem Speicherplatz fest.
<code>FAST VP distribution</code>	Prozentsatz des Datenspeichers, der jedem Tier zugewiesen ist. Das Format lautet wie folgt: <code><tier_name>:<value>%</code> Hierbei gilt: <ul style="list-style-type: none"> • <code><tier_name></code> ist der Name des Storage Tier. • <code><value></code> ist der Prozentsatz des Storage in diesem Tier.
<code>Local path</code>	Zu exportierender lokaler Pfad
<code>Export path</code>	Exportpfad zum Datenspeicher.
<code>Default access</code>	Die Standardzugriffseinstellungen für Hostkonfigurationen und nicht konfigurierte Hosts, die auf den NFS-Datstore zugreifen können. Folgende Werte sind möglich: <ul style="list-style-type: none"> • <code>ro</code>: Nur Lesezugriff auf primären Speicher und mit dem NFS-Datenspeicher verbundene Snapshots • <code>rw</code>: Lese- und Schreibzugriff auf primären Speicher und mit dem NFS-Datenspeicher verbundene Snapshots • <code>root</code>: Lese- und Schreib-Root-Zugriff auf primären Speicher und mit dem NFS-Datenspeicher verbundene Snapshots Dies beinhaltet die Möglichkeit zur Einrichtung von Zugriffskontrollen, mit denen die Berechtigungen für andere Anmeldekonto eingeschränkt werden. • <code>na</code>: Kein Zugriff auf den NFS-Datenspeicher oder seine Snapshots
<code>Advanced hostmgmt</code>	Gibt an, ob die in den Hostlisten aufgeführten Hosts mithilfe der <code>/remote/host</code> -Objekte definiert werden, z. B. mit ihrer Kennung. Folgende Werte sind gültig (keine Unterscheidung zwischen Groß- und Kleinschreibung): <ul style="list-style-type: none"> • <code>yes</code> (Standard) • <code>no</code>
<code>Read-only hosts</code>	ID der Hosts mit Nur-Lese-Berechtigung für den NFS-Datenspeicher und die zugehörigen Snapshots
<code>Read/write hosts</code>	ID der Hosts mit Lese- und Schreibberechtigung für den NFS-Datenspeicher und die zugehörigen Snapshots
<code>Root hosts</code>	ID der Hosts mit Root-Berechtigung für den NFS-Datstore und die zugehörigen Snapshots
<code>No access hosts</code>	ID der Hosts, die keinen Zugriff auf den NFS-Datenspeicher bzw. die zugehörigen Snapshots haben
<code>ESX mount protocol</code>	Legt fest, welches NFS-Protokoll zu verwenden ist, um den Datenspeicher auf dem ESXi-Host zu registrieren. Gültige Werte: <ul style="list-style-type: none"> • <code>NFSv3</code> (Standard) • <code>NFSv4</code>
<code>Minimum security</code>	Die minimale Sicherheitsoption, die von einem Client für einen erfolgreichen NFS-Mount-Vorgang bereitgestellt werden muss. Gültige Werte:

Tabelle 116. Attribute für NFS-Datstores (fortgesetzt)

Attribut	Beschreibung
	<ul style="list-style-type: none"> • <code>sys</code>: Keine serverseitige Authentifizierung (Server verlässt sich auf NFS-Clientauthentifizierung) Dies ist die Standardeinstellung, wenn für den NAS-Server kein sicheres NFS konfiguriert ist. Es ist auch die Standardeinstellung, wenn NFS Secure ohne NFSv4 für den NAS-Server aktiviert ist. Auch bekannt als AUTH_SYS-Sicherheit. • <code>krb5</code>: Kerberos V5-Authentifizierung. Dies ist der Standardwert, wenn sicheres NFSv4 für den NAS-Server konfiguriert ist.
<code>NFS owner username</code>	Standardeigentümer der NFS-Share, die dem Datenspeicher zugeordnet ist. Für NFSv3- oder NFSv4-Protokolle ohne konfiguriertes Kerberos ist der Standardeigentümer <code>root</code> .
<code>Replication type</code>	Zeigt an, an welcher asynchronen Replikation dieses Dateisystem teilnimmt. Gültige Werte: <ul style="list-style-type: none"> • <code>none</code> • <code>local</code> • <code>remote</code>
<code>Synchronous replication type</code>	Zeigt an, an welcher synchronen Replikation dieses Dateisystem teilnimmt. Gültige Werte: <ul style="list-style-type: none"> • <code>none</code> • <code>remote</code>
<code>Replication destination</code>	Gibt an, ob die Speicherressource ein Ziel für eine Replikationssitzung (lokal oder remote) ist. Gültige Werte: <ul style="list-style-type: none"> • <code>yes</code> • <code>no</code>
<code>Error Threshold</code>	Gibt den Schwellenwert des belegten Speicherplatzes in der Speicherressource als Prozentsatz an. Bei Überschreitung werden Fehlerwarnmeldungen erzeugt. Der Standardwert ist 95 %. Wenn der Schwellenwert auf 0 festgelegt ist, wird diese Warnmeldung deaktiviert. Diese Option muss auf einen Wert festgelegt werden, der größer ist als der Schwellenwert für Warnmeldung und Info.
<code>Warning Threshold</code>	Gibt den Schwellenwert des belegten Speicherplatzes in der Speicherressource als Prozentsatz an. Bei Überschreitung werden Warnmeldungen erzeugt. Der Standardwert ist 75 %. Wenn der Schwellenwert auf 0 festgelegt ist, wird diese Warnmeldung deaktiviert. Diese Option muss auf einen Wert festgelegt werden, der kleiner ist als der Fehlerschwellenwert und größer als oder gleich dem Info-Schwellenwert.
<code>Info Threshold</code>	Gibt den Schwellenwert des belegten Speicherplatzes in der Speicherressource als Prozentsatz an. Bei Überschreitung werden Informationswarnmeldungen erzeugt. Der Standardwert ist 0 (deaktiviert). Diese Option muss auf einen Wert festgelegt werden, der kleiner ist als der Schwellenwert für die Warnmeldung.
<code>Creation time</code>	Der Zeitpunkt der Erstellung der Ressource.
<code>Last modified time</code>	Der Zeitpunkt der letzten Änderung der Ressource.
<code>Pool full policy</code>	Zu befolgende Policy, wenn der Pool voll ist und es versucht wird, in den NFS-Datenspeicher zu schreiben. Dieses Attribut ermöglicht es Ihnen, Snapshots auf dem NFS-Datenspeicher beizubehalten, wenn ein Pool voll ist. Mögliche Werte sind: <ul style="list-style-type: none"> • <code>Delete All Snaps</code> (Standardeinstellung für Thick-Dateisysteme): Snapshots, die mit dem NFS-Datenspeicher verknüpft sind, werden gelöscht, wenn der Pool die volle Kapazität erreicht. • <code>Fail Writes</code> (Standardeinstellung für Thin-Dateisysteme): Schreibvorgänge auf den NFS-Datenspeicher schlagen fehl, wenn der Pool die volle Kapazität erreicht. <p>ANMERKUNG: Dieses Attribut ist nur für vorhandene NFS-Datenspeicher verfügbar. Sie können dieses Attribut nicht festlegen, wenn Sie einen NFS-Datenspeicher erstellen.</p>
<code>Minimum size</code>	Die geschätzte Mindestgröße, auf die das Dateisystem verkleinert werden kann.
<code>Reclaimable size</code>	Die geschätzte Größe, die vom Pool zurückgewonnen wird, wenn das Dateisystem auf eine bestimmte Größe verkleinert wird.

Tabelle 116. Attribute für NFS-Datstores (fortgesetzt)

Attribut	Beschreibung
Event publishing protocols	Liste der Dateisystem-Zugriffsprotokolle, die für die Ereignisveröffentlichung aktiviert sind. Standardmäßig ist die Liste leer. Gültiger Wert ist <code>nfs</code> (Aktivierung der Ereignisveröffentlichung für NFS).

Erstellen von NFS-Datstores

Erstellen Sie einen NFS-Datstore.

Voraussetzungen

- Konfigurieren Sie mindestens einen Speicherpool für den NFS-Datenspeicher, und weisen Sie dem Pool mindestens ein Laufwerk zu.
- Konfigurieren Sie mindestens einen NAS-Server, dem der NFS-Datstore zugewiesen wird.

ANMERKUNG: Freigabenzugriffseinstellungen für bestimmte Hosts werden nur wirksam, wenn die hostspezifische Einstellung weniger restriktiv ist als die Standardzugriffseinstellung für die Freigaben. Zudem hat die Zugriffseinstellung „Kein Zugriff“ für einen bestimmten Host immer Vorrang vor der Standardzugriffseinstellung.

- Beispiel 1: Wenn die Standardzugriffseinstellung für eine Freigabe „Schreibgeschützt“ und die Zugriffseinstellung für eine bestimmte Hostkonfiguration „Lesen/Schreiben“ lautet, so wird Letztere wirksam.
- Beispiel 2: Wenn die Standardzugriffseinstellung für eine Freigabe „Schreibgeschützt“ und die Zugriffseinstellung für eine bestimmte Hostkonfiguration „Kein Zugriff“ lautet, so kann der Host nicht auf die Freigabe zugreifen.
- Beispiel 3: Wenn die Standardzugriffseinstellung für eine Freigabe „Lesen/Schreiben“ und die Zugriffseinstellung für eine bestimmte Hostkonfiguration „Schreibgeschützt“ lautet, so erhält der Host Lese-/Schreibzugriff.

Format

```
/stor/prov/vmware/nfs create [-async] -name <value> [-descr <value>] {-server <value> |
-serverName <value>} {pool <value> | -poolName <value>} -size <value> [-hostIOSize {8K | 16K
| 32K | 64K | exchange2007 | exchange2010 | exchange2013 | oracle | sqlServer | vmwareHorizon
| sharePoint | sap}] [-thin {yes [-dataReduction {yes [-advancedDedup {yes | no}} | no}}
| no}} [-minSizeAllocated <value>] [-sched <value> [schedPaused {yes | no}]] [-fastvpPolicy
{startHighThenAuto | auto | highest | lowest}] [-defAccess {ro | rw | roroot | root | na}}
[-advHostMgmtEnabled {yes | no}] [-roHosts <value>] [-rwHosts <value>] [-roRootHosts <value>]
[-rootHosts <value>] [ naHosts <value>] [-esxMountProtocol {NFSv4 | NFSv3}] [-minSecurity {sys
| krb5 [-nfsOwner <value>}}] [-allowSuid {yes | no}] [-anonUid <value>] [-anonGid <value>] [-
replDest {yes | no}] [-eventProtocols <value>]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.
-name	Geben Sie einen Namen für den NFS-Datenspeicher ein.
-descr	Geben Sie eine kurze Beschreibung des NFS-Datenspeichers ein.
-server	Geben Sie die ID des NAS-Servers ein, der als primärer NAS-Server für den NFS-Datenspeicher dient. ANMERKUNG: NFS-Datenspeicher können nicht auf einem NAS-Server erstellt werden, der IP-Mehrmandantenfähigkeit verwendet.
-serverName	Geben Sie den Namen des NAS-Servers ein, der als primärer NAS-Server für den NFS-Datenspeicher dient. ANMERKUNG: NFS-Datenspeicher können nicht auf einem NAS-Server erstellt werden, der IP-Mehrmandantenfähigkeit verwendet.

Qualifizierer	Beschreibung
-pool	Geben Sie die ID des Speicherpools ein, den der NFS-Datenspeicher verwendet. Dieser Wert hat Vorrang vor dem Wert für -poolName.  ANMERKUNG: Beim Wert wird zwischen Groß- und Kleinschreibung unterschieden.
-poolName	Geben Sie den Namen des Speicherpools ein, den der NFS-Datastore nutzt.
-size	Geben Sie ein, wie viel Speicher für den NFS-Datenspeicher reserviert werden soll.
-hostIOsize	Geben Sie die typische Schreib-I/O-Größe vom Host zum NFS-Datenspeicher ein. Gültige Werte: <ul style="list-style-type: none"> • 8K (Standard) — Allzweck 8K • 16K: Allgemeiner Speicher 16 K • 32K: Allgemeiner Speicher 32 K • 64K: Allgemeiner Speicher 64 K • exchange2007: 8 K für Microsoft Exchange 2007 Anwendungen • exchange2010: 32 K für Microsoft Exchange 2010 Anwendungen • exchange2013: 32 K für Microsoft Exchange 2013 Anwendungen • oracle: 8 K für Oracle Datenbankanwendungen • sqlserver: 8 K für Microsoft SQL Server-Anwendungen • vmwareHorizon: 8 K für VMware Horizon-VDI-Anwendungen • sharepoint: 32 K für Microsoft SharePoint-Anwendungen • sap: 8 K für SAP-Anwendungen
-thin	Hiermit wird Thin Provisioning auf dem NFS-Datenspeicher aktiviert. Gültige Werte: <ul style="list-style-type: none"> • yes • no (Standard)
-dataReduction	Geben Sie an, ob eine Datenreduzierung für diesen Thin-NFS-Datenspeicher aktiviert werden soll. Gültige Werte: <ul style="list-style-type: none"> • yes • no (Standard)  ANMERKUNG: Die Datenreduzierung ist für Thin-Dateisysteme verfügbar. Die Thin-Dateisysteme müssen auf Unity-Systemen erstellt worden sein, auf denen Version 4.2.x oder höher ausgeführt wird.
-advancedDedup	Gibt an, ob die erweiterte Deduplizierung für diesen Thin-NFS-Datenspeicher aktiviert ist. Gültige Werte: <ul style="list-style-type: none"> • yes • no (Standard)  ANMERKUNG: Thin-Dateisysteme müssen auf einem Unity-System erstellt werden, auf dem Version 4.2.x oder höher ausgeführt wird. Erweiterte Deduplizierung ist nur verfügbar auf: <ul style="list-style-type: none"> • Dynamischen oder herkömmlichen Pools in Unity 380F-, 480F-, 680F- und 880F-Systemen • Dynamische Pools in Unity-All-Flash 450F-, 550F- und 650F-Systemen • All-Flash-Pools und Hybrid-Flash-Pools in Unity Hybrid-Systemen 380, 480, 680 und 880
-minSizeAllocated	(Option verfügbar auf einem Unity-System mit OE-Version 4.1.) Geben Sie die minimale Größe an, die dem Thin-NFS-Datenspeicher zugewiesen werden soll. Automatische und manuelle Dateiverkleinerungsvorgänge können die Dateisystemgröße nicht unter diesen Wert reduzieren. Der Standardwert ist 3 GB, die minimale Größe des Thin-Dateisystems.
-sched	Geben Sie die ID eines Schutzplans ein, der auf die Speicherressource angewendet werden soll.
-schedPaused	Geben Sie an, ob der für -sched angegebene Schutzplan ausgesetzt werden soll. Gültige Werte: <ul style="list-style-type: none"> • yes • no (Standard)
-fastvpPolicy	Geben Sie die FAST VP-Tiering Policy des NFS-Datenspeichers an. Diese Policy definiert sowohl die anfängliche Tier-Positionierung als auch das laufende automatisierte Tiering von Daten während den Datenverlagerungsvorgängen. Folgende Werte sind gültig (keine Unterscheidung zwischen Groß- und Kleinschreibung):

Qualifizierer	Beschreibung
	<ul style="list-style-type: none"> • <code>startHighThenAuto</code> (Standardeinstellung): Legt die anfängliche Datenplatzierung auf die Laufwerke mit der höchsten Performance und freiem Speicherplatz fest und verlagert dann Teile der Daten der Storage-Ressource basierend auf der I/O-Aktivität. • <code>auto</code>: Legt die anfängliche Datenplatzierung auf eine optimale, vom System bestimmte Einstellung fest und verlagert dann Teile der Daten der Storage-Ressource basierend auf Performancestatistiken der Storage-Ressource, sodass die Daten entsprechend der I/O-Aktivität auf die Tiers verlagert werden. • <code>highest</code>: Legt die anfängliche Datenplatzierung und nachfolgende Datenverlagerung (falls zutreffend) auf die Laufwerke mit der höchsten Performance und freiem Speicherplatz fest. • <code>lowest</code>: legt die anfängliche Datenplatzierung und nachfolgende Datenverlagerung (falls zutreffend) auf die kosteneffizientesten Laufwerke mit freiem Speicherplatz fest.
<code>-defAccess</code>	<p>Geben Sie die Standardeinstellung des gleichzeitigen Zugriffs für Hostkonfigurationen und nicht konfigurierte Hosts an, die auf den NFS-Datenspeicher zugreifen können. Gültige Werte:</p> <ul style="list-style-type: none"> • <code>ro</code>: Nur Lesezugriff auf primären Speicher und mit dem NFS-Datenspeicher verbundene Snapshots. • <code>root</code>: Rootzugriff mit Lese-/Schreibrechten auf den primären Speicher und mit dem NFS-Datenspeicher verbundene Snapshots. Dies beinhaltet die Möglichkeit zur Einrichtung von Zugriffskontrollen, mit denen die Berechtigungen für andere Anmeldekonto eingeschränkt werden. • <code>na</code> (Standard) – Kein Zugriff auf den NFS-Datenspeicher oder seine Snapshots.
<code>-advHostMgmtEnabled</code>	<p>Gibt an, ob die in den Hostlisten aufgeführten Hosts mithilfe der <code>/remote/host</code>-Objekte definiert werden, z. B. mit ihrer Kennung (erweitertes Hostmanagement). Folgende Werte sind gültig (keine Unterscheidung zwischen Groß- und Kleinschreibung):</p> <ul style="list-style-type: none"> • <code>yes</code> (Standard) • <code>no</code>
<code>-roHosts</code>	<p>Geben Sie die IDs der einzelnen Hostkonfigurationen ein, denen Sie eine Nur-Lese-Berechtigung für den NFS-Datenspeicher und die zugehörigen Snapshots erteilen möchten. Trennen Sie die einzelnen IDs mit Kommas voneinander ab. Bei Hostkonfigurationen des Typs „Host“ können standardmäßig alle IP-Adressen des Hosts auf den NFS-Datenspeicher und die zugehörigen Snapshots zugreifen. Um nur bestimmten IPs den Zugriff zu erlauben, geben Sie diese in eckigen Klammern hinter der Host-ID ein. Beispiel: ID[IP,IP], wobei „ID“ eine Hostkonfigurations-ID und „IP“ eine IP-Adresse ist.</p>
<code>-rwHosts</code>	<p>Geben Sie die IDs der einzelnen Hosts ein, denen Sie Lese-/Schreibzugriff auf den Datenspeicher erteilen möchten. Dies ist nur zulässig, wenn das NFSv4 ESXi-Mountprotokoll aktiviert und der NFS-Eigentümer festgelegt ist.</p>
<code>-roRootHosts</code>	<p>Geben Sie die IDs der einzelnen Hosts ein, denen Sie schreibgeschützten Root-Zugriff auf den Datenspeicher erteilen möchten.</p>
<code>-rootHosts</code>	<p>Geben Sie die IDs der einzelnen Hostkonfigurationen ein, denen Sie eine Root-Berechtigung für den NFS-Datenspeicher und die zugehörigen Snapshots erteilen möchten. Trennen Sie die einzelnen IDs mit Kommas voneinander ab. Bei Hostkonfigurationen des Typs „Host“ können standardmäßig alle IP-Adressen des Hosts auf den NFS-Datenspeicher und die zugehörigen Snapshots zugreifen. Um nur bestimmten IPs den Zugriff zu erlauben, geben Sie diese in eckigen Klammern hinter der Host-ID ein. Beispiel: ID[IP,IP], wobei „ID“ eine Hostkonfigurations-ID und „IP“ eine IP-Adresse ist.</p>
<code>-naHosts</code>	<p>Geben Sie die IDs der einzelnen Hostkonfigurationen ein, deren Zugriff auf den NFS-Datenspeicher und die zugehörigen Snapshots Sie sperren möchten. Trennen Sie die einzelnen IDs mit Kommas voneinander ab. Bei Hostkonfigurationen des Typs „Host“ können standardmäßig alle IP-Adressen des Hosts nicht auf den NFS-Datenspeicher und die zugehörigen Snapshots zugreifen. Um den Zugriff auf bestimmte IPs zu beschränken, geben Sie die IPs in eckigen Klammern hinter der Host-ID ein. Beispiel: ID[IP,IP], wobei „ID“ eine Hostkonfigurations-ID und „IP“ eine IP-Adresse ist.</p>
<code>-esxMountProtocol</code>	<p>Geben Sie ein, welche NFS-Protokollversion verwendet wird, um den NFS-Datenspeicher auf dem Host zu registrieren. Gültige Werte:</p> <ul style="list-style-type: none"> • <code>NFSv3</code> (Standard) • <code>NFSv4</code>
<code>-nfsOwner</code>	<p>Geben Sie den Standardeigentümer der NFS-Share ein, die dem Datenspeicher zugeordnet ist. Dies muss angegeben werden, wenn die Mindestsicherheit auf <code>krb5</code> eingestellt ist und alle an die Hostzugriffsliste übergebenen Hosts manuell verwaltet werden. Wenn die übergebenen Hosts ESXi-Hosts sind, wird dieser Wert automatisch auf den NFS-Benutzer festgelegt, der auf dem ESXi-Host konfiguriert ist.</p>

Qualifizierer	Beschreibung
	 ANMERKUNG: Für NFSv3- oder NFSv4-Protokolle, die ohne Kerberos konfiguriert sind, ist der Standardbesitzer <code>root</code> .
<code>-minSecurity</code>	Geben Sie die minimale Sicherheitsoption ein, die vom Client für einen erfolgreichen NFS-Mount-Vorgang bereitgestellt werden muss. Gültige Werte sind (vom niedrigsten bis zum höchsten Sicherheitslevel): <ul style="list-style-type: none"> • <code>sys</code>: Keine serverseitige Authentifizierung (Server verlässt sich auf NFS-Clientauthentifizierung) Dies ist die Standardeinstellung, wenn für den NAS-Server kein sicheres NFS konfiguriert ist. Es ist auch die Standardeinstellung, wenn NFS Secure ohne NFSv4 für den NAS-Server aktiviert ist. Auch bekannt als AUTH_SYS-Sicherheit. • <code>krb5</code>: Kerberos V5-Authentifizierung. Dies ist der Standardwert, wenn sicheres NFSv4 für den NAS-Server konfiguriert ist.
<code>-allowSuid</code>	Gibt an, ob die Festlegung der Nutzer-ID (<code>suid</code>) zugelassen werden soll. Gültige Werte: <ul style="list-style-type: none"> • <code>yes</code> • <code>no</code>
<code>-anonUid</code>	Gibt die UID des anonymen Kontos an.
<code>-anonGid</code>	Gibt die GID des anonymen Kontos an.
<code>-replDest</code>	Gibt an, ob die Ressource ein Replikationsziel ist. Gültige Werte: <ul style="list-style-type: none"> • <code>yes</code> • <code>no</code> (Standard)
<code>-eventProtocols</code>	Gibt die durch Kommas getrennte Liste der Dateisystem-Zugriffsprotokolle an, die für die Ereignisveröffentlichung aktiviert sind. Standardmäßig ist die Liste leer. Gültiger Wert ist <code>nfs</code> (Aktivierung der Ereignisveröffentlichung für NFS).

Beispiel

Mit dem folgenden Befehl wird ein NFS-Datenspeicher mit den folgenden Einstellungen erstellt:

- Name: Accounting.
- Beschreibung: Accounting VMs
- Verwendet NAS-Server `nas_1` als primärer NAS-Server.
- Nutzt den Speicherpool „capacity“.
- Größe des primären Speichers: 100 GB.
- Lese-/Schreibzugriff auf `host1`
- Mindestsicherheitsstufe von `krb5`.
- Ein NFS-Eigentümer „John“
- Standardhostzugriff als „-“

Das Dateisystem erhält die ID `NFSDS_1`:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/vmware/nfs create -name Accounting
-descr "Accounting VMs" -server nas_1 -pool capacity -size 100G -rwHosts host1 -esxMountProtocol
NFSv4 -minSecurity krb5 -nfsOwner john -defAccess na
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = NFSDS_1
Operation completed successfully.
```

Anzeigen von NFS-Datenspeichern

Zeigen Sie die Details zu einem NFS-Datenspeicher an. Sie können nach der ID oder dem Namen des NFS-Datenspeichers filtern.

Format

```
/stor/prov/vmware/nfs [ {-id <value> | -name <value>} [-shrinkToSize <value>]} show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	ID des VMware NFS-Dateisystems.
-name	Name des VMware NFS-Dateisystems.
-shrinkToSize	Geben Sie die angestrebte Verkleinerungsgröße an, um eine Schätzung der Mindestgröße und der wiederverwendbaren Größe anzuzeigen. i ANMERKUNG: Mindestgröße und wiederverwendbare Größe werden nur ausgefüllt, wenn dieser Qualifizierer angegeben ist.

Beispiel 1

Mit dem folgenden Befehl werden Details zu sämtlichen NFS-Datstores im System aufgeführt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/vmware/nfs show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:   ID           = vmware_1
     Name        = MyVMware
     Description = My VMware
     Health state = OK (5)
     File system = fs_1
     Server      = SFServer00
     Storage pool ID = pool_1
     Storage pool = capacity
     Size        = 536870912000 (500G)
     Size used   = 128849018880 (120G)
     Protection size used = 0
     Local path  = /
     Export path = 10.64.75.10/MyVMware
     Minimum size =
     Reclaimable size =
```

Beispiel 2

Mit dem folgenden Befehl werden Details zu den vmware_1-NFS-Datenspeichern mit einer Verkleinerungsschätzung aufgeführt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/vmware/nfs -id vmware_1 -shrinkToSize 200G show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:   ID           = vmware_1
     Name        = MyVMware
     Description = My VMware
     Health state = OK (5)
     File system = fs_1
     Server      = SFServer00
     Storage pool ID = pool_1
```

```

Storage pool      = capacity
Format           = UFS64
Size             = 536870912000 (500G)
Size used       = 128849018880 (120G)
Protection size used = 0
Local path       = /
Export path      = 10.64.75.10/MyVMware
Minimum size     = 134217728000 (125G)
Reclaimable size = 322122547200 (300G)

```

Ändern der Einstellungen für NFS-Datenspeicher

Ändern Sie die Einstellungen für einen NFS-Datastore.

Format

```

/stor/prov/vmware/nfs {-id <value> | -name <value>} set [-async] [-descr <value>] [-size
<value>] [-minSizeAllocated <value>] [-dataReduction {yes [-advancedDedup {yes | no}] | no}] [{"-
sched <value> | -noSched}] [-schedPaused {yes | no}] [-fastvpPolicy { startHighThenAuto | auto |
highest | lowest }] [ defAccess {ro | rw | roroot | root | na}] [-advHostMgmtEnabled {yes | no}]
[{"-roHosts <value>"} [-rwHosts <value>] [-roRootHosts <value>] [-rootHosts <value>] [-naHosts
<value>] [-addRoHosts <value>] [-addRwHosts <value>] [-addRoRootHosts <value>] [-addRootHosts
<value>] [-addNaHosts <value>] [-removeHosts <value> }]} [-esxMountProtocol {NFSv4 | NFSv3}]
[-minSecurity {sys | krb5}] [-allowSuid {yes | no}] [-anonUid <value>] [-anonGid <value>] [-
replDest {yes | no}] [-poolFullPolicy {deleteAllSnaps | failWrites}] [-eventProtocols <value>]
[-errorThreshold <value>] [-warningThreshold <value>] [-infoThreshold <value>]

```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des zu ändernden NFS-Datenspeichers ein.
-name	Geben Sie den Namen des zu ändernden NFS-Datenspeichers ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.
-descr	Geben Sie eine kurze Beschreibung des NFS-Datenspeichers ein.
-size	Geben Sie ein, wie viel Poolspeicher für den NFS-Datastore reserviert werden soll.
-minSizeAllocated	(Option verfügbar auf einem Unity-System mit OE-Version 4.1.) Geben Sie die minimale Größe an, die dem Thin-NFS-Datenspeicher zugewiesen werden soll. Automatische und manuelle Dateiverkleinerungsvorgänge können die Dateisystemgröße nicht unter diesen Wert reduzieren. Der Standardwert ist 3 GB, die minimale Größe des Thin-Dateisystems.
-dataReduction	Geben Sie an, ob eine Datenreduzierung für den Thin-NFS-Datenspeicher aktiviert werden soll. Gültige Werte: <ul style="list-style-type: none"> • yes • no  ANMERKUNG: Die Datenreduzierung ist für Thin-Dateisysteme verfügbar. Die Thin-Dateisysteme müssen auf Unity-Systemen erstellt worden sein, auf denen Version 4.2.x oder höher ausgeführt wird.
-advancedDedup	Gibt an, ob die erweiterte Deduplizierung auf dem Thin-NFS-Datenspeicher aktiviert ist. Gültige Werte: <ul style="list-style-type: none"> • yes • no

Qualifizierer	Beschreibung
	<p>i ANMERKUNG: Thin-Dateisysteme müssen auf einem Unity-System erstellt werden, auf dem Version 4.2.x oder höher ausgeführt wird. Erweiterte Deduplizierung ist nur verfügbar auf:</p> <ul style="list-style-type: none"> • Dynamischen oder herkömmlichen Pools in Unity 380F-, 480F-, 680F- und 880F-Systemen • Dynamische Pools in Unity-All-Flash 450F-, 550F- und 650F-Systemen • All-Flash-Pools und Hybrid-Flash-Pools in Unity Hybrid-Systemen 380, 480, 680 und 880
-sched	Geben Sie die ID des Plans ein, der auf den Datenspeicher angewendet werden soll.
-noSched	Hebt die Schutzplanzuweisung auf.
-fastvpPolicy	<p>Geben Sie die FAST VP-Tiering Policy des NFS-Datenspeichers an. Diese Policy definiert sowohl die anfängliche Tier-Positionierung als auch das laufende automatisierte Tiering von Daten während den Datenverlagerungsvorgängen. Gültige Werte (nicht unterschieden nach Groß- und Kleinschreibung):</p> <ul style="list-style-type: none"> • <code>startHighThenAuto</code> (Standardeinstellung): Legt die anfängliche Datenplatzierung auf die Laufwerke mit der höchsten Performance und freiem Speicherplatz fest und verlagert dann Teile der Daten der Storage-Ressource basierend auf der I/O-Aktivität. • <code>auto</code>: Legt die anfängliche Datenplatzierung auf eine optimale, vom System bestimmte Einstellung fest und verlagert dann Teile der Daten der Speicherressource basierend auf Performancestatistiken der Speicherressource, sodass die Daten entsprechend der I/O-Aktivität auf die Tiers verlagert werden. • <code>highest</code>: Legt die anfängliche Datenplatzierung und nachfolgende Datenverlagerung (falls zutreffend) auf die Laufwerke mit der höchsten Performance und freiem Speicherplatz fest. • <code>lowest</code>: legt die anfängliche Datenplatzierung und nachfolgende Datenverlagerung (falls zutreffend) auf die kosteneffizientesten Laufwerke mit freiem Speicherplatz fest.
-schedPaused	<p>Setzen Sie den Plan für den Qualifizierer -sched aus. Gültige Werte:</p> <ul style="list-style-type: none"> • <code>yes</code> • <code>no</code>
-defAccess	<p>Geben Sie die Standardeinstellung des gleichzeitigen Zugriffs für Hostkonfigurationen und nicht konfigurierte Hosts an, die auf den Datenspeicher zugreifen können. Gültige Werte:</p> <ul style="list-style-type: none"> • <code>ro</code>: Nur Lesezugriff auf primären Speicher und mit dem Datenspeicher verbundene Snapshots • <code>root</code>: Schreib-Root-Zugriff auf primären Speicher und mit dem Datenspeicher verbundene Snapshots Dies beinhaltet die Möglichkeit zur Einrichtung von Zugriffskontrollen, mit denen die Berechtigungen für andere Anmeldekonto eingeschränkt werden. • <code>na</code>: Kein Zugriff auf den Datenspeicher oder seine Snapshots
-advHostMgmtEnabled	<p>Gibt an, ob die in den Hostlisten aufgeführten Hosts mithilfe der <code>/remote/host</code>-Objekte und ihrer Kennung definiert werden (erweitertes Hostmanagement). Gültige Werte (nicht unterschieden nach Groß- und Kleinschreibung):</p> <ul style="list-style-type: none"> • <code>Yes</code> (Standard) • <code>No</code> <p>Diese Einstellung kann nur aktualisiert werden, wenn die Liste der fünf Hosts unten leer ist.</p>
-roHosts	Gibt die kommagetrennte Liste von Hosts mit Leseberechtigung für den NFS-Datenspeicher an. Mit diesem Qualifizierer werden die vorhandenen schreibgeschützten Hosts überschrieben.
-rwHosts	Gibt die kommagetrennte Liste von Hosts mit Schreibberechtigung für den NFS-Datenspeicher an. Diese Option ist nur zulässig, wenn das NFSv4 ESXi-Mountprotokoll aktiviert und der NFS-Eigentümer festgelegt ist. Mit diesem Qualifizierer werden die vorhandenen Hosts mit Schreibzugriff überschrieben.
-roRootHosts	Gibt die kommagetrennte Liste von Hosts mit schreibgeschütztem Root-Zugriff auf den NFS-Datenspeicher an. Mit diesem Qualifizierer werden die vorhandenen schreibgeschützten Root-Hosts überschrieben.
-rootHosts	Gibt die kommagetrennte Liste von Hosts mit Root-Zugriff auf den NFS-Datenspeicher an. Dadurch werden die vorhandenen Root-Hosts mit Schreibberechtigung überschrieben.
-naHosts	Gibt die kommagetrennte Liste von Hosts ohne Zugriff auf den NFS-Datenspeicher an. Mit diesem Qualifizierer werden die vorhandenen Hosts ohne Zugriffsberechtigung überschrieben.
-addRoHosts	Gibt die kommagetrennte Liste der hinzuzufügenden Hosts mit schreibgeschütztem Zugriff auf den NFS-Datenstore an. Mit dieser Option können Sie inkrementell Hosts mit schreibgeschütztem Zugriff

Qualifizierer	Beschreibung
	auf den NFS-Datenstore hinzufügen. Dadurch werden nicht alle vorhandenen schreibgeschützten Hosts überschrieben.
<code>-addRwHosts</code>	Gibt die kommagetrennte Liste der hinzuzufügenden Hosts mit Schreibzugriff auf den NFS-Datenspeicher an. Mit dieser Option können Sie inkrementell Hosts mit Schreibzugriff auf den NFS-Datenspeicher hinzufügen. Dadurch werden nicht alle vorhandenen Hosts mit Schreibzugriff überschrieben.
<code>-addRoRootHosts</code>	Gibt die kommagetrennte Liste der hinzuzufügenden Hosts mit schreibgeschütztem Root-Zugriff auf den NFS-Datenspeicher an. Mit dieser Option können Sie inkrementell Hosts mit schreibgeschütztem Root-Zugriff auf den NFS-Datenspeicher hinzufügen. Dadurch werden nicht alle vorhandenen schreibgeschützten Root-Hosts überschrieben.
<code>-addRootHosts</code>	Gibt die kommagetrennte Liste von Hosts an, die Schreib-Root-Zugriff auf den NFS-Datenspeicher erhalten. Mit dieser Option können Sie inkrementell Hosts mit Schreib-Root-Zugriff auf den NFS-Datenspeicher hinzufügen. Dadurch werden nicht alle vorhandenen Hosts mit Schreib-Root-Zugriff überschrieben.
<code>-addNaHosts</code>	Gibt die kommagetrennte Liste von Hosts an, die keinen Zugriff auf den NFS-Datenspeicher haben werden. Mit dieser Option können Sie inkrementell Hosts angeben, die keinen Zugriff auf den NFS-Datenspeicher haben. Dadurch werden nicht alle vorhandenen Hosts ohne Zugriffsberechtigung überschrieben.
<code>-removeHosts</code>	Gibt die kommagetrennte Liste von Hosts an, denen der Zugriff auf den NFS-Datenspeicher entzogen wird. Mit dieser Option können Sie den Hostzugriff auf den NFS-Datenspeicher inkrementell entfernen.
<code>-exMountProtocol</code>	Geben Sie ein, welche NFS-Protokollversion verwendet wird, um den NFS-Datenspeicher auf dem Host zu registrieren. Gültige Werte: <ul style="list-style-type: none"> • NFSv3 (Standard) • NFSv4
<code>-minSecurity</code>	Geben Sie die minimale Sicherheitsoption ein, die vom Client für einen erfolgreichen NFS-Mount-Vorgang bereitgestellt werden muss. Gültige Werte sind (vom niedrigsten bis zum höchsten Sicherheitslevel): <ul style="list-style-type: none"> • <code>sys</code>: Keine serverseitige Authentifizierung (Server verlässt sich auf NFS-Clientauthentifizierung) Dies ist die Standardeinstellung, wenn für den NAS-Server kein sicheres NFS konfiguriert ist. Es ist auch die Standardeinstellung, wenn NFS Secure ohne NFSv4 für den NAS-Server aktiviert ist. Auch bekannt als AUTH_SYS-Sicherheit. • <code>krb5</code>: Kerberos V5-Authentifizierung.
<code>-replDest</code>	Gibt an, ob die Ressource ein Replikationsziel ist. Gültige Werte: <ul style="list-style-type: none"> • <code>yes</code> • <code>no</code>
<code>-errorThreshold</code>	Gibt den Schwellenwert in Prozent an, bei dem überschritten Fehlerwarnmeldungen erzeugt werden. Der Bereich liegt zwischen 0 und 99. Der Standardwert ist 95 %. Wenn der Schwellenwert auf 0 festgelegt ist, wird diese Warnmeldung deaktiviert. Diese Option muss auf einen Wert größer als der <code>-warningThreshold</code> festgelegt werden.
<code>-warningThreshold</code>	Gibt den Schwellenwert in Prozent an, bei dessen Überschreitung Warnmeldungen generiert werden. Der Bereich liegt zwischen 0 und 99. Der Standardwert ist 75 %. Wenn der Schwellenwert auf 0 festgelegt ist, wird diese Warnmeldung deaktiviert. Diese Option muss auf einen Wert festgelegt werden, der kleiner ist als der <code>-errorThreshold</code> -Wert und größer als oder gleich dem <code>-infoThreshold</code> -Wert.
<code>-infoThreshold</code>	Gibt den Schwellenwert in Prozent an, bei dessen Überschreitung Warnmeldungen zur Information generiert werden. Der Bereich liegt zwischen 0 und 99. Der Standardwert ist 0 (deaktiviert). Diese Option muss auf einen Wert festgelegt werden, der kleiner ist als der <code>-warningThreshold</code> -Wert.
<code>-poolFullPolicy</code>	Gibt die zu befolgende Policy an, wenn der Pool voll ist und es versucht wird, in den NFS-Datenspeicher zu schreiben. Dieses Attribut ermöglicht es Ihnen, Snapshots auf dem NFS-Datenspeicher beizubehalten, wenn ein Pool voll ist. Mögliche Werte sind: <ul style="list-style-type: none"> • <code>deleteAllSnaps</code>: Snapshots, die mit dem NFS-Datenspeicher verbunden sind, werden gelöscht, wenn der Speicherpool die volle Kapazität erreicht. • <code>failWrites</code>: Schreibvorgänge auf den NFS-Datenspeicher schlagen fehl, wenn der Pool die volle Kapazität erreicht.

Qualifizierer	Beschreibung
-eventProtocols	Gibt die kommasetrennte Liste der Dateisystem-Zugriffsprotokolle an, die für die Ereignisveröffentlichung aktiviert sind. Standardmäßig ist die Liste leer. Gültiger Wert ist <code>nfs</code> (Aktivierung der Ereignisveröffentlichung für NFS).

Beispiel

Durch den folgenden Befehl wird der NFS-Datenspeicher `NFSDS_1` so geändert, dass die Hostkonfigurationen `HOST_1` und `HOST_2` schreibgeschützten Zugriff erhalten und der Zugriff für `HOST_3` gesperrt wird.

ANMERKUNG: Obwohl `HOST_4` und `HOST_12` bereits schreibgeschützten Zugriff auf den Datenspeicher haben, müssen Sie in der Liste zusammen mit den neuen Hosts, die mit schreibgeschütztem Zugriff hinzugefügt werden, enthalten sein.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/vmware/nfs -id NFSDS_1 set -roHosts "HOST_1,HOST_2, HOST_4, HOST_12" -naHosts "HOST_3"
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = NFSDS_1
Operation completed successfully.
```

Beispiel 3

Im folgenden Beispiel wird `Host_2` schreibgeschützter Zugriff auf `NFSShare_2` zugewiesen, `Host_3` wird Schreibzugriff auf die Freigabe zugewiesen und `Host_1` wird der Zugriff auf die Freigabe entzogen:

```
uemcli /stor/prov/fs/nfs -id NFSShare_2 set -addRoHosts Host_2 -addRwHosts Host_3 -removeHosts Host_1
```

```
ID = NFSShare_2
Operation completed successfully.
```

Löschen von NFS-Datenspeichern

Löschen Sie einen NFS-Datastore.

ANMERKUNG: Beim Löschen eines VMware NFS-Datenspeichers werden sämtliche mit dem Datenspeicher verknüpften Dateien und Ordner aus dem System entfernt. In diesem Fall kann der Inhalt des Datastore nicht mehr über Snapshots wiederhergestellt werden. Sichern Sie die Daten des Datenspeichers, bevor Sie ihn aus dem System löschen.

Format

```
/stor/prov/vmware/nfs {-id <value> | -name <value>} delete [-deleteSnapshots {yes | no}] [-async]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des zu löschenden VMware NFS-Datenspeichers ein.
-name	Geben Sie den Namen des zu löschenden VMware NFS-Datenspeichers ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-deleteSnapshots	Gibt an, dass auch die zugehörigen Snapshots gelöscht werden sollen. Gültige Werte: <ul style="list-style-type: none"> • yes • no (Standard)
-async	Führen Sie den Vorgang im asynchronen Modus aus.

Beispiel

Mit dem folgenden Befehl wird der NFS-Datstore NFSDS_1 gelöscht:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/vmware/nfs -id NFSDS_1 delete
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
Operation completed successfully.
```

Managen von VMware-VMFS-Datenspeichern

VMFS-Datenspeicher (Virtual Machine File System) bieten Blockspeicherung für ESXi-Hosts. VMFS-Datenspeicher werden den ESXi-Hosts gegenüber als LUNs angezeigt, mit denen sich die Hosts über das Fibre Channel(FC)- oder das iSCSI-Protokoll verbinden. Sie können VMFS-Datenspeicher bereitstellen und managen und Details zu jedem VMFS-Datenspeicher im System anzeigen, z. B. deren Speicherkapazität und Integrität.

Tabelle 117. Attribute für VMFS-Datenspeicher

Attribut	Beschreibung
ID	ID des VMFS-Datstore.
LUN	Logical Unit Number (LUN)-ID des VMFS-Datenspeichers.
Name	Name des VMFS-Datenspeichers.
Description	Kurze Beschreibung des VMFS-Datstore.
Type	Gibt den Typ des VMFS-Datenspeichers an. Wert ist einer der folgenden (nicht unterschieden nach Groß- und Kleinschreibung): <ul style="list-style-type: none"> • Primary • Thin clone (tc bei Verwendung mit dem <code>-create</code>-Befehl.)
Base storage resource	(Gilt nur für Thin Clones) ID des Basis-VMFS-Datenspeichers für den Thin Clone.
Source	(Gilt nur für Thin Clones) ID des Quell-Snapshot des Thin Clone.
Original parent	(Gilt nur für Thin Clones) ID des übergeordneten VMFS-Datenspeichers für den Thin Clone.
Health state	Integritätsstatus des VMFS-Datstore. Der Integritätsstatuscode wird in Klammern angezeigt. Folgende Werte sind möglich: <ul style="list-style-type: none"> • OK (5): Der Datenspeicher funktioniert normal. • Degraded/Warning (10): Funktioniert, aber es ist mindestens eines der folgenden Probleme aufgetreten: <ul style="list-style-type: none"> ○ Sein Speicherpool wird heruntergestuft. ○ Die Replikationssitzung ist heruntergestuft. ○ Die Replikationssitzung ist fehlgeschlagen.

Tabelle 117. Attribute für VMFS-Datenspeicher (fortgesetzt)

Attribut	Beschreibung
	<ul style="list-style-type: none"> ○ Die Kapazitätshöchstgrenze ist nahezu erreicht. Zur Vermeidung von Datenverlusten sollten Sie die Größe des primären Speichers erhöhen oder zusätzliche Datenspeicher für die Speicherung der Daten anlegen. ● Minor failure (15): Es ist mindestens eines der folgenden Ereignisse eingetreten: <ul style="list-style-type: none"> ○ Sein Speicherpool ist ausgefallen. ○ Der zugehörige iSCSI-Node ist ausgefallen. ● Major failure (20): Es ist mindestens eines der folgenden Ereignisse eingetreten: <ul style="list-style-type: none"> ○ Datenspeicher ist nicht verfügbar. ○ Sein zugeordneter Speicherpool ist ausgefallen. ● Critical failure (25): Es ist mindestens eines der folgenden Ereignisse eingetreten: <ul style="list-style-type: none"> ○ Der Speicherpool ist nicht verfügbar. ○ Datenspeicher ist nicht verfügbar. ○ Die volle Kapazität des Datastore ist erreicht. Zur Vermeidung von Datenverlusten sollten Sie die Primärspeichergröße erhöhen oder zusätzliche Dateisysteme für die Speicherung der Daten anlegen. ● Non-recoverable error (30): Es ist mindestens eines der folgenden Ereignisse eingetreten: <ul style="list-style-type: none"> ○ Der Speicherpool ist nicht verfügbar. ○ Datenspeicher ist nicht verfügbar.
Health details	Zusätzliche Integritätsinformationen. Weitere Informationen zur Integrität finden Sie im Anhang A, Referenz.
Storage pool ID	ID des vom Datastore verwendeten Speicherpools.
Storage pool	Name des vom Datenspeicher verwendeten Speicherpools
Size	Für primäre Daten reservierter Speicher
Maximum size	Maximale Größe, auf die die Kapazität des primären Speichers erweitert werden kann.
AU size	<p>Die Größe der Zuweisungseinheit in Kilobyte. Gültige Werte:</p> <ul style="list-style-type: none"> ● 8 ● 16 ● 32 ● 64
Thin provisioning enabled	<p>Gibt an, ob Thin Provisioning aktiviert ist. Gültige Werte:</p> <ul style="list-style-type: none"> ● yes ● no (Standard) <p>Von allen Speicherpools werden mit herkömmlichen und mit Thin Provisioning bereitgestellte Speicherressourcen unterstützt. Bei Standard-Speicherressourcen wird bei der Erstellung der Ressource die gesamte angeforderte Kapazität aus dem Pool zugewiesen. Bei Thin-Provisioning-Speicherressourcen werden immer nur Teile der Kapazität je nach tatsächlicher Nutzung zugewiesen. Da Thin-Provisioning-Speicherressourcen eine höhere Belegung aufweisen können, als ihnen tatsächlich an Speicher zugewiesen ist, ist es möglich, für Speicherpools ein Über-Provisioning festzulegen, damit die Pools eine höhere Speicherkapazität unterstützen können, als sie aufweisen.</p> <p> ANMERKUNG: In der Unisphere-Onlinehilfe erfahren Sie mehr zu Thin Provisioning.</p>
Data Reduction enabled	<p>Gibt an, ob die Datenreduzierung für die Thin-LUN aktiviert ist. Gültige Werte:</p> <ul style="list-style-type: none"> ● yes ● no
Data Reduction space saved	Eingesparter Gesamtspeicherplatz für die Thin-LUN (in Gigabyte) durch Datenreduzierung.
Data Reduction percent	Eingesparter Gesamt-Storage für die Thin-LUN (in Prozent) durch Datenreduzierung.
Data Reduction ratio	Verhältnis der Einsparungen zwischen Daten ohne Datenreduzierung und Daten nach der Datenreduzierung.

Tabelle 117. Attribute für VMFS-Datenspeicher (fortgesetzt)

Attribut	Beschreibung
	 ANMERKUNG: Die Datenreduzierung ist für Thin-LUNs verfügbar.
Advanced deduplication enabled	Gibt an, ob die erweiterte Deduplizierung aktiviert ist. Diese Option ist erst verfügbar, wenn die Datenreduzierung aktiviert wurde. Ein leerer Wert weist darauf hin, dass die erweiterte Deduplizierung auf der Speicherressource nicht unterstützt wird. Gültige Werte: <ul style="list-style-type: none"> • yes • no (Standard)  ANMERKUNG: Erweiterte Deduplizierung ist nur verfügbar auf: <ul style="list-style-type: none"> • Dynamischen oder herkömmlichen Pools in Unity 380F-, 480F-, 680F- und 880F-Systemen • Dynamische Pools in Unity-All-Flash 450F-, 550F- und 650F-Systemen • All-Flash-Pools und Hybrid-Flash-Pools in Unity Hybrid-Systemen 380, 480, 680 und 880
Current allocation	Bei aktiviertem Thin Provisioning die Menge an Primärspeicher, die zurzeit über Thin Provisioning bereitgestellt wird.
Total pool space preallocated	Der Speicherplatz, der für zukünftige Zwecke im Pool für den VMFS-Datenspeicher reserviert ist, um Schreibvorgänge effizienter zu gestalten. Der Pool kann einen Teil dieses Speicherplatzes zurückgewinnen, wenn er vom Datenspeicher nicht genutzt wird und der Pool wenig Platz hat.
Total pool space used	Gesamtspeicherplatz des Pools, der vom VMFS-Datenspeicher verwendet wird.
Non-base size used	(Gilt nur für Standard-VMFS-Datenspeicher.) Menge des Speichers, der für die diesem Datenspeicher zugeordneten Snapshots und Thin Clones verwendet wird.
Family size used	(Gilt nur für Standard-VMFS-Datenspeicher.) Menge des Speichers, der für die ganze Datenspeicherproduktreihe verwendet wird.
Snapshot count	Gesamtzahl der Snapshots im VMFS-Datenspeicher.
Family snapshot count	(Gilt nur für Standard-VMFS-Datenspeicher.) Anzahl der Snapshots im Datenspeicher, einschließlich aller abgeleiteten Snapshots.
Family thin clone count	Anzahl der in der VMFS-Datenspeicherproduktreihe erstellten Thin Clones, einschließlich aller abgeleiteten Thin Clones.
Protection schedule	ID eines auf den VMFS-Datenspeicher angewendeten Schutzplans.
Protection schedule paused	Hier wird angegeben, ob ein angewendeter Schutzplan zurzeit ausgesetzt ist.
SP owner	Gibt den Standardeigentümer der LUN an. Gültige Werte: <ul style="list-style-type: none"> • SPA • SPB
Trespassed	Gibt an, ob die LUN an den Peer-SP umgeleitet wird. Gültige Werte: <ul style="list-style-type: none"> • yes • no
LUN access hosts	Liste der Hosts, die über Berechtigungen zum Zugriff auf den VMFS-Datenspeicher verfügen, der den Hosts gegenüber als LUN dargestellt wird
Virtual disk access hosts	Durch Komma getrennte Liste der Hosts, die über Zugriff auf die verbundenen Laufwerke verfügen.
Virtual disk host LUN IDs	Durch Komma getrennte Liste von HLUs (Host LUN Identifiers), die die entsprechenden Hosts verwenden, um auf die virtuellen Laufwerke zuzugreifen.
Snapshots access hosts	Liste der Hosts, die über Berechtigungen zum Zugriff auf die Snapshots des VMFS-Datenspeichers verfügen.
WWN	World Wide Name der VMware-Ressource.
Replication destination	Hier ist angegeben, ob die Speicherressource ein Ziel für eine Replikationssitzung (lokal oder remote) ist. Gültige Werte:

Tabelle 117. Attribute für VMFS-Datenspeicher (fortgesetzt)

Attribut	Beschreibung
	<ul style="list-style-type: none"> • yes • no
Creation time	Der Zeitpunkt der Erstellung der Ressource.
Last modified time	Der Zeitpunkt der letzten Änderung der Ressource.
FAST VP policy	<p>FAST VP-Tiering Policy für den VMFS-Datenspeicher. Diese Policy definiert sowohl die anfängliche Tier-Positionierung als auch das laufende automatisierte Tiering von Daten während den Datenverlagerungsvorgängen. Gültige Werte (nicht unterschieden nach Groß- und Kleinschreibung):</p> <ul style="list-style-type: none"> • <code>startHighThenAuto</code> (Standardeinstellung): Legt die anfängliche Datenplatzierung auf die Laufwerke mit der höchsten Performance und freiem Speicherplatz fest und verlagert dann Teile der Daten der Storage-Ressource basierend auf der I/O-Aktivität. • <code>auto</code>: Legt die anfängliche Datenplatzierung auf eine optimale, vom System bestimmte Einstellung fest und verlagert dann Teile der Daten der Speicherressource basierend auf Performancestatistiken der Speicherressource, sodass die Daten entsprechend der I/O-Aktivität auf die Tiers verlagert werden. • <code>highest</code>: Legt die anfängliche Datenplatzierung und nachfolgende Datenverlagerung (falls zutreffend) auf die Laufwerke mit der höchsten Performance und freiem Speicherplatz fest. • <code>lowest</code>: legt die anfängliche Datenplatzierung und nachfolgende Datenverlagerung (falls zutreffend) auf die kosteneffizientesten Laufwerke mit freiem Speicherplatz fest.
FAST VP distribution	<p>Prozentsatz des Datenspeichers, der jedem Tier zugewiesen ist. Das Format lautet wie folgt:</p> <pre><tier_name>:<value>%</pre> <p>Hierbei gilt:</p> <ul style="list-style-type: none"> • <code><tier_name></code> ist der Name des Storage Tier. • <code><value></code> ist der Prozentsatz des Storage in diesem Tier.
Version	<p>Gibt die VMFS-Version des Datastore an. Gültige Werte:</p> <ul style="list-style-type: none"> • 3 • 5 • 6
Block size	<p>Gibt die Blockgröße in Megabyte an. Gültige Werte:</p> <ul style="list-style-type: none"> • 1 • 2 • 4 • 8
IO limit	Gibt die Kennung des angewendeten I/O-Limits an.
Effective maximum IOPS	Der effektive maximale I/O pro Sekunde für den VMFS-Datenspeicher. Bei VMFS-Datenspeichern mit einer dichte-basierten E/A-Limit-Richtlinie entspricht dieser Wert dem Produkt von <code>Maximum IOPS</code> und <code>Size</code> des angehängten VMFS-Datenspeichers.
Effective maximum KBPS	Die effektiven maximalen KB pro Sekunde für den VMFS-Datenspeicher. Bei VMFS-Datenspeichern mit einer dichte-basierten E/A-Limit-Richtlinie entspricht dieser Wert dem Produkt von <code>Maximum KBPS</code> und <code>Size</code> des angehängten VMFS-Datenspeichers.

Erstellen von VMware VMFS-Datenspeichern

Erstellen Sie einen VMFS-Datstore.

Voraussetzungen

- Konfigurieren Sie mindestens einen Speicherpool für den VMFS-Datenspeicher, und weisen Sie dem Pool mindestens ein Laufwerk zu. Informationen darüber, wie Pools automatisch auf dem System erstellt werden und wie benutzerdefinierte Pools erstellt werden, finden Sie unter den Befehlen für Speicherpools.
- Konfigurieren Sie für iSCSI-Verbindungen mindestens eine iSCSI-Schnittstelle für die Verwendung durch den VMFS-Datenspeicher. In Unisphere ist für Fibre Channel-Verbindungen zu VMFS-Datenspeichern keine zusätzliche Konfiguration erforderlich.

Format

```
/stor/prov/vmware/vmfs create [-async] -name <value> [-descr <value>] [-type {primary | tc {-source <value> | -sourceName <value>}}] [{-pool <value> | -poolName <value>}] [-size <value>] [-thin {yes | no}] [-sched <value> [-schedPaused {yes | no}]] [-spOwner {spa | spb}] [-replDest {yes | no}] [-dataReduction {yes [-advancedDedup {yes | no}] | no}] [-fastvpPolicy {startHighThenAuto | auto | highest | lowest}] [-vdiskHosts <value>] [-hplus <value>] [-snapHosts <value>] [-version {3 -blockSize {1 | 2 | 4 | 8} | 5 | 6}] [-ioLimit <value>]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.
-name	Geben Sie einen Namen für den VMFS-Datenspeicher ein.  ANMERKUNG: Entscheiden Sie sich für einen Namen, aus dem der Typ und die Version der dafür vorgesehenen Anwendung hervorgehen. Dies erleichtert das Management und die Überwachung des VMFS-Datastore über Unisphere.
-descr	Geben Sie eine kurze Beschreibung des VMFS-Datenspeichers ein.
-type	Geben Sie den Typ des VMFS-Datenspeichers an. Gültige Werte sind folgende (keine Unterscheidung zwischen Groß- und Kleinschreibung): <ul style="list-style-type: none"> • primary (Standard) • tc
-source	(Gilt nur für Thin Clones) Geben Sie die ID des Quell-Snapshot ein, der zur Erstellung von Thin Clones verwendet werden soll.
-sourceName	(Gilt nur für Thin Clones) Geben Sie den Namen des Quell-Snapshot ein, der zur Erstellung von Thin Clones verwendet werden soll.
-pool	(Gilt nicht bei der Erstellung eines Thin Clone) Geben Sie die ID des Speicherpools ein, den der VMFS-Datenspeicher verwenden soll.  ANMERKUNG: Beim Wert wird zwischen Groß- und Kleinschreibung unterschieden.
-poolName	(Gilt nicht bei der Erstellung eines Thin Clone) Geben Sie den Namen des Speicherpools ein, den der VMFS-Datenspeicher verwenden wird.
-size	(Gilt nicht bei der Erstellung eines Thin Clone) Geben Sie die Menge des Speichers ein, der für den VMFS-Datenspeicher zu reservieren ist.
-thin	(Gilt nicht bei der Erstellung eines Thin Clone) Aktivieren Sie Thin Provisioning auf dem VMFS-Datenspeicher. Gültige Werte: <ul style="list-style-type: none"> • yes • no (Standard)
-sched	Geben Sie die ID eines Schutzplans ein, der auf die Speicherressource angewendet werden soll.
-schedPaused	Geben Sie an, ob der für den Parameter -sched angegebene Schutzplan ausgesetzt werden soll. Gültige Werte: <ul style="list-style-type: none"> • yes • no

Qualifizierer	Beschreibung
-spOwner	(Gilt nicht bei der Erstellung eines Thin Clone) Geben Sie den Standard-SP an, dem die VMware-Ressource angehören wird. Das Speichersystem bestimmt den Standardwert. Gültige Werte: <ul style="list-style-type: none"> • spa • spb
-replDest	(Gilt nicht bei der Erstellung eines Thin Clone) Gibt an, ob die Ressource ein Replikationsziel ist. Gültige Werte: <ul style="list-style-type: none"> • yes • no (Standard)
-dataReduction	(Gilt nicht bei der Erstellung eines Thin Clone) Geben Sie an, ob für den VMFS-Datenspeicher eine Datenreduzierung aktiviert oder deaktiviert werden soll. Gültige Werte: <ul style="list-style-type: none"> • yes • no (Standard)
-advancedDedup	Geben Sie an, ob die erweiterte Deduplizierung für den VMFS-Datenspeicher aktiviert oder deaktiviert werden soll. Diese Option ist erst verfügbar, wenn die Datenreduzierung aktiviert wurde. Gültige Werte: <ul style="list-style-type: none"> • yes • no (Standard) <p>i ANMERKUNG: Erweiterte Deduplizierung ist nur verfügbar auf:</p> <ul style="list-style-type: none"> • Dynamischen oder herkömmlichen Pools in Unity 380F-, 480F-, 680F- und 880F-Systemen • Dynamische Pools in Unity-All-Flash 450F-, 550F- und 650F-Systemen • All-Flash-Pools in Unity Hybrid 380-, 480-, 680- und 880-Systemen
-fastvpPolicy	(Gilt nicht bei der Erstellung eines Thin Clone) Geben Sie die FAST VP-Tiering Policy für den VMFS-Datenspeicher an. Diese Policy definiert sowohl die anfängliche Tier-Positionierung als auch das laufende automatisierte Tiering von Daten während den Datenverlagerungsvorgängen. Gültige Werte (nicht unterschieden nach Groß- und Kleinschreibung): <ul style="list-style-type: none"> • startHighThenAuto (Standardeinstellung): Legt die anfängliche Datenplatzierung auf die Laufwerke mit der höchsten Performance und freiem Speicherplatz fest und verlagert dann Teile der Daten der Storage-Ressource basierend auf der I/O-Aktivität. • auto: Legt die anfängliche Datenplatzierung auf eine optimale, vom System bestimmte Einstellung fest und verlagert dann Teile der Daten der Speicherressource basierend auf Performancestatistiken der Speicherressource, sodass die Daten entsprechend der I/O-Aktivität auf die Tiers verlagert werden. • highest: Legt die anfängliche Datenplatzierung und nachfolgende Datenverlagerung (falls zutreffend) auf die Laufwerke mit der höchsten Performance und freiem Speicherplatz fest. • lowest: legt die anfängliche Datenplatzierung und nachfolgende Datenverlagerung (falls zutreffend) auf die kosteneffizientesten Laufwerke mit freiem Speicherplatz fest.
-vdiskHosts	Geben Sie die ID jeder Hostkonfiguration ein, um Zugriff auf den VMFS-Datenspeicher zu ermöglichen. Trennen Sie die einzelnen IDs mit Kommas voneinander ab. Standardmäßig können alle iSCSI-Initiatoren auf dem Host auf den VMFS-Datenspeicher zugreifen. Um den Zugriff nur bestimmten Initiatoren zu erlauben, geben Sie die IQN des jeweiligen Initiators in eckigen Klammern hinter der Host-ID ein. Beispiel: ID[IQN,IQN], wobei „ID“ eine Hostkonfigurations-ID und „IQN“ die IQN eines Initiators ist.
-hlus	Geben Sie die kommagetrennte Liste der Host-LUN-Kennungen an, die von den entsprechenden Hosts verwendet werden sollen, die in der Option -vdiskHosts angegeben wurden. Die Anzahl der Positionen in den beiden Listen muss übereinstimmen. Eine leere Zeichenfolge ist jedoch ein gültiger Wert für jedes Element der Liste der Host-LUN-Identifikatoren, sofern die Listenelemente durch Kommata getrennt sind. Ein solches leeres Element bedeutet, dass das System automatisch den Host-LUN-Identifikatorwert zuweisen sollte, mit dem der entsprechende Host auf das virtuelle Laufwerk zugreift. Wenn diese Option nicht angegeben ist, weist das System automatisch den Host-LUN-Kennungswert jedem Host zu, der in der Argumentliste -vdiskHosts angegeben ist.
-snapHosts	Geben Sie die ID der einzelnen Hostkonfigurationen ein, um Zugriff auf die Snapshots des VMFS-Datenspeichers zu ermöglichen. Trennen Sie die einzelnen IDs mit Kommas voneinander ab. Standardmäßig können alle iSCSI-Initiatoren auf dem Host auf alle Snapshots des VMFS-Datenspeichers zugreifen. Um den Zugriff nur bestimmten Initiatoren zu erlauben, geben Sie die IQN des jeweiligen Initiators in eckigen Klammern hinter der Host-ID ein. Beispiel: ID[IQN,IQN], wobei „ID“ eine Hostkonfigurations-ID und „IQN“ die IQN eines Initiators ist.
-version	Geben Sie die VMFS-Version des Datastore ein. Gültige Werte:

Qualifizierer	Beschreibung
	<ul style="list-style-type: none"> • 3 • 5 (Standard) • 6
-blockSize	Geben Sie die Blockgröße des Datastore in Megabyte ein. Gültige Werte: <ul style="list-style-type: none"> • 1 • 2 • 4 • 8 (Standard)
-ioLimit	Geben Sie die Größe des I/O-Limits an, das für die VMFS-Datenspeicher angewendet werden soll.

Beispiel

Mit dem folgenden Befehl wird ein VMFS-Datstore mit den folgenden Einstellungen erstellt:

- Name: Accounting3
- Beschreibung: Accounting Group 3.
- Nutzt den Kapazitätsspeicherpool.
- Stellt Hostzugriffsrechte auf den VMFS-Datstore (dargestellt als ein LUN) für zwei der IQNs für Hostkonfiguration 1014 und für Hostkonfiguration 1015 bereit.
- Kein Schutzplan.

Der VMFS-Datstore erhält die ID VMFS_1:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/vmware/vmfs create -
name "Accounting3" -descr "Accounting Group 3" -pool capacity -size 100G -thin yes -
vdiskHosts "1014,1015"
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = VMFS_1
Operation completed successfully.
```

Anzeigen von VMware VMFS-Datenspeichern

Zeigen Sie die Liste der vorhandenen VMFS-Datenspeicher an. Sie können nach der ID für VMFS-Datenspeicher filtern.

Format

```
/stor/prov/vmware/vmfs [{"-id <value> | -name <value> | -type {primary | tc {-baseRes <value> |
-baseResName <value> | -originalParent <value> | -originalParentName <value> | -source <value> |
-sourceName <value>}}}] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID eines VMFS-Datstore ein.
-name	Geben Sie den Namen eines VMFS-Datenspeichers ein.
-standalone	Zeigt nur VMFS-Datenspeicher an, die nicht zu einer Consistency Group gehören.
-type	Identifiziert den Typ der anzuzeigenden Ressourcen. Gültige Werte sind folgende (keine Unterscheidung zwischen Groß- und Kleinschreibung):

Qualifizierer	Beschreibung
	<ul style="list-style-type: none"> • primary • tc
-baseRes	(Gilt nur für Thin Clones) ID des Basis-VMFS-Datenspeichers, nach dem die Thin Clones gefiltert werden sollen.
-baseResName	(Gilt nur für Thin Clones) Name des Basis-VMFS-Datenspeichers, nach dem die Thin Clones gefiltert werden sollen.
-originalParent	(Gilt nur für Thin Clones) ID des übergeordneten VMFS-Datenspeichers, nach dem die Thin Clones gefiltert werden sollen.
-originalParentName	(Gilt nur für Thin Clones) Name des übergeordneten VMFS-Datenspeichers, nach dem die Thin Clones gefiltert werden sollen.
-source	(Gilt nur für Thin Clones) ID des Quell-Snapshot, nach dem Thin Clones gefiltert werden sollen.
-sourceName	(Gilt nur für Thin Clones) Name des Quell-Snapshot, nach dem die Thin Clones gefiltert werden sollen.

Beispiel 1

Mit dem folgenden Befehl werden Details zu VMFS-Datenspeichern und ihren Thin Clones angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/vmware/vmfs show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:  ID                = res_6
    LUN              = sv_25
    Name             = VMFS Datastore 1
    Description      =
    Type            = Primary
    Base storage resource = res_6
    Source          =
    Original parent  =
    Health state     = OK (5)
    Health details   = "The component is operating normally. No action is
required."
    Storage pool ID  = pool_1
    Storage pool     = Pool_1
    Size            = 1099511627776 (1.0T)
    Maximum size     = 70368744177664 (64.0T)
    Thin provisioning enabled = yes
    Data Reduction enabled = yes
    Data Reduction space saved = 267361714176 (249.0G)
    Data Reduction percent = 57%
    Data Reduction ratio = 2.3:1
    Advanced deduplication enabled = no
    Current allocation = 172823429120 (160.9G)
    Preallocated     = 82576048128 (76.9G)
    Total Pool Space Used = 203844583424 (189.8G)
    Protection size used = 20820606976 (19.3G)
    Non-base size used = 20820606976 (19.3G)
    Family size used = 203844583424 (189.8G)
    Snapshot count   = 2
    Family snapshot count = 2
    Family thin clone count = 0
    Protection schedule = snapSch_1
    Protection schedule paused = no
    SP owner         = SPB
    Trespassed      = no
    Version         = 5
    Block size      = 1
    Virtual disk access hosts = Host_2
    Host LUN IDs    = 12
    Snapshots access hosts =
    WWN            = 60:06:01:60:09:00:43:00:CB:38:88:5B:BB:10:5B:09
```

```

Replication destination      = no
Creation time                = 2018-08-30 18:34:46
Last modified time          = 2018-08-30 18:34:46
IO limit                     =
Effective maximum IOPS       = N/A
Effective maximum KBPS      = N/A

```

Beispiel 2

Der folgende Befehl zeigt Details über Thin Clones an, die von der LUN namens sv_2 abgeleitet sind:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/vmware/vmfs -id vmware_2 show
```

```

Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID                = vmware_2
LUN               = sv_2
Name              = MyFC
Description       = My description
Type              = Thin clone
Base storage resource = vmware_1
Source            = snap_1
Original parent   = vmware_1
Health state      = OK (5)
Storage pool ID   = pool_2
Storage pool      = capacity
Size              = 107374182400 (100G)
Protection size used =
Non-base size used = 0
SP owner          = SPA
Trespassed        = no

```

Ändern der Einstellungen für VMware-VMFS-Datenspeicher

Ändern Sie die Einstellungen für einen VMFS-Datenspeicher.

Format

```

/stor/prov/vmware/vmfs {-id <value> | -name <value>} set [-async] [-name <value>] [-descr <value>] [-size <value>] [{-sched <value> | -noSched}] [-schedPaused {yes | no}] [{[-vdiskHosts <value> [-hplus <value>]] [-snapHosts <value>] | [-addHosts <value> [-hplus <value>]] [-removeHosts <value>] [-addSnapHosts <value>] [-removeSnapHosts <value>]]] [-spOwner {spa | spb}] [-fastvpPolicy {startHighThenAuto | auto | highest | lowest}] [-replDest {yes | no}] [{-ioLimit <value> | -noIoLimit}] [-dataReduction {yes [-advancedDedup {yes | no}] | no}]

```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des zu ändernden VMFS-Datenspeichers ein.
-name	Geben Sie den Namen des zu ändernden VMFS-Datenspeichers ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.

Qualifizierer	Beschreibung
-name	Geben Sie einen Namen für den VMFS-Datenspeicher ein.  ANMERKUNG: Verwenden Sie einen Namen, der den Typ und die Version der Anwendung widerspiegelt, die Sie verwenden möchten. Dieser Name erleichtert das Management und die Überwachung des VMFS-Datenspeichers über Unisphere.
-descr	Geben Sie eine kurze Beschreibung des VMFS-Datenspeichers ein.
-size	(Gilt nicht für Thin Clones) Geben Sie an, wie viel Speicher dem VMFS-Datenspeicher zugewiesen wird.
-sched	Geben Sie die ID eines Schutzplans ein, der auf den VMFS-Datenspeicher angewendet werden soll.
-noSched	Heben Sie die Schutzplanzuweisung auf.
-schedPaused	Geben Sie an, ob der für -sched angegebene Schutzplan ausgesetzt werden soll. Gültige Werte: <ul style="list-style-type: none"> • yes • no
-spOwner	(Gilt nicht für Thin Clones) Geben Sie den Standard SP ab, der den Datenspeicher besitzt. Gültige Werte: <ul style="list-style-type: none"> • spa • spb
-replDest	Gibt an, ob die Ressource ein Replikationsziel ist. Gültige Werte: <ul style="list-style-type: none"> • yes • no  ANMERKUNG: Dieser Wert muss no für einen Thin Clone sein.
-dataReduction	(Gilt nicht für Thin Clones) Geben Sie an, ob für den VMFS-Datenspeicher eine Datenreduzierung aktiviert oder deaktiviert werden soll. Gültige Werte: <ul style="list-style-type: none"> • yes • no
-advancedDedup	Geben Sie an, ob die erweiterte Deduplizierung für den VMFS-Datenspeicher aktiviert oder deaktiviert werden soll. Gültige Werte: <ul style="list-style-type: none"> • yes • no (Standard)  ANMERKUNG: Erweiterte Deduplizierung ist nur verfügbar auf: <ul style="list-style-type: none"> • Dynamischen oder herkömmlichen Pools in Unity 380F-, 480F-, 680F- und 880F-Systemen • Dynamische Pools in Unity-All-Flash 450F-, 550F- und 650F-Systemen • All-Flash-Pools und Hybrid-Flash-Pools in Unity Hybrid-Systemen 380, 480, 680 und 880
-fastvpPolicy	(Gilt nicht für Thin Clones) Geben Sie die FAST VP-Tiering Policy für den VMFS-Datenspeicher an. Diese Policy definiert sowohl die anfängliche Tier-Positionierung als auch das laufende automatisierte Tiering von Daten während den Datenverlagerungsvorgängen. Gültige Werte (nicht unterschieden nach Groß- und Kleinschreibung): <ul style="list-style-type: none"> • startHighThenAuto (Standardeinstellung): Legt die anfängliche Datenplatzierung auf die Laufwerke mit der höchsten Performance und freiem Speicherplatz fest und verlagert dann Teile der Daten der Storage-Ressource basierend auf der I/O-Aktivität. • auto : Legt die anfängliche Datenplatzierung auf eine optimale, vom System bestimmte Einstellung fest und verlagert dann Teile der Daten der Storage-Ressource basierend auf Performancestatistiken der Storage-Ressource, sodass die Daten entsprechend der I/O-Aktivität auf die Tiers verlagert werden. • highest : Legt die anfängliche Datenplatzierung und nachfolgende Datenverlagerung (falls zutreffend) auf die Laufwerke mit der höchsten Performance und freiem Speicherplatz fest. • lowest : legt die anfängliche Datenplatzierung und nachfolgende Datenverlagerung (falls zutreffend) auf die kosteneffizientesten Laufwerke mit freiem Speicherplatz fest.
-vdiskHosts	Gibt die durch Kommas getrennte Liste von Hosts mit Zugriff auf virtuelle Laufwerke an. Mit diesem Qualifizierer wird der vorhandene Hostzugriff auf den VMware VMFS-Datenspeicher überschrieben.

Qualifizierer	Beschreibung
-hlus	Gibt die kommagetrennte Liste der Host-LUN-Kennungen an, die von den entsprechenden Hosts verwendet werden, die in der Option <code>-vdiskHosts</code> oder <code>-addHosts</code> festgelegt wurden. Die Anzahl der Positionen in den beiden Listen muss übereinstimmen. Eine leere Zeichenfolge ist jedoch ein gültiger Wert für jedes Element der Liste der Host-LUN-Identifikatoren, sofern die Listenelemente durch Kommata getrennt sind. Ein solches leeres Zeichenfolgeelement bedeutet, dass das System den Host-LUN-Kennungswert automatisch zuweisen sollte, mit dem der entsprechende Host auf das virtuelle Laufwerk zugreift. Wenn die Option <code>-hlus</code> nicht in der Befehlszeile enthalten ist, weist das System automatisch die Host-LUN-Kennungswerte für jeden Host zu, der in der Argumentliste <code>-vdiskHosts</code> oder <code>-addHosts</code> angegeben ist.
-snapHosts	Gibt die durch Kommas getrennte Liste von Hosts mit Zugriff auf Snapshots an. Mit dieser Option wird der vorhandene Hostzugriff auf die Snapshots des VMFS-Datenspeichers überschrieben.
-addHosts	Gibt die kommagetrennte Liste der hinzuzufügenden Hosts mit Zugriff auf den VMFS-Datenspeicher an. Mit dieser Option können Sie inkrementell Hosts hinzufügen, die auf den VMFS-Datenspeicher zugreifen können. Dadurch werden nicht alle vorhandenen Hosts mit Zugriff überschrieben.
-removeHosts	Gibt die kommagetrennte Liste von Hosts an, deren Zugriff auf den VMFS-Datenspeicher entfernt werden soll. Mit dieser Option können Sie inkrementell den Zugriff von Hosts auf den VMFS-Datenspeicher entfernen. Dadurch werden nicht alle vorhandenen Hosts mit Zugriff überschrieben.
-addSnapHosts	Gibt die kommagetrennte Liste der hinzuzufügenden Hosts mit Zugriff auf die Snapshots an. Mit dieser Option können Sie inkrementell Hosts hinzufügen, die auf die Snapshots zugreifen können. Dadurch werden nicht alle vorhandenen Hosts mit Zugriff überschrieben.
-removeSnapHosts	Gibt die kommagetrennte Liste von Hosts an, deren Zugriff auf die Snapshots entfernt werden soll. Mit dieser Option können Sie inkrementell den Zugriff von Hosts auf die Snapshots entfernen. Dadurch werden nicht alle vorhandenen Hosts mit Zugriff überschrieben.
-ioLimit	Geben Sie die Größe des anzuwendenden I/O-Limits ein.
-noIoLimit	Gibt an, dass ein vorhandenes, auf den VMFS-Datenspeicher angewendetes I/O-Limit entfernt wird.

Beispiel 1

Mit dem folgenden Befehl wird der VMFS-Datstore VMFS_1 mit den folgenden Einstellungen aktualisiert:

- Name: Accounting4
- Beschreibung: Accounting Group 4

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/vmware/vmfs -id VMFS_1 set -name Accounting4 -descr "Accounting Group 4"
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = VMFS_1
Operation completed successfully.
```

Beispiel 2

Mit dem folgenden Befehl wird VMFS-Datenspeicher VMFS_1 aktualisiert, um Zugriff für HOST_22 und HOST_18 hinzuzufügen.

 **ANMERKUNG:** HOST_1 und HOST_2 haben bereits Zugriff auf den Datenspeicher. Sie müssen sie jedoch in der Liste der vDisk-Hosts zusätzlich zu den neuen Hosts angeben, die Sie hinzufügen möchten.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/vmware/vmfs -id VMFS_1 set -vdiskHosts HOST_1, HOST_2, HOST_18, HOST_22
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = VMFS_1
Operation completed successfully.
```

Beispiel 3

Über den folgenden Befehl erhält Host_2 Zugriff auf Datenspeicher res_1 und der Zugriff für Host_1 wird entfernt:

```
uemcli /stor/prov/vmware/vmfs -id res_1 set -addHosts Host_2 -removeHosts Host_1
```

```
ID = res_1
Operation completed successfully.
```

Löschen von VMware VMFS-Datenspeichern

Löschen Sie einen VMFS-Datstore.

i ANMERKUNG: Wenn Sie einen VMFS-Datenspeicher löschen, werden dadurch alle zugehörigen Daten und Snapshots aus dem System entfernt. Nach dem Löschen eines VMFS-Datstore können die Daten nicht aus Snapshots wiederhergestellt werden. Sichern Sie die Daten des VMFS-Datenspeichers, bevor Sie ihn löschen.

Format

```
/stor/prov/vmware/vmfs {-id <value> | -name <value>} delete [-deleteSnapshots {yes | no}] [-async] delete [-deleteSnapshots {yes | no}] [-async]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des zu löschenden VMFS-Datstore ein.
-name	Geben Sie den Namen des zu löschenden VMFS-Datenspeichers ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.
-deleteSnapshots	Geben Sie an, ob der Datstore zusammen mit den Snapshots gelöscht werden kann. Gültige Werte sind „yes“ und „no“ (Standard).

Beispiel

Mit dem folgenden Befehl wird der VMFS-Datstore VMFS_1 gelöscht:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/vmware/vmfs -id VMFS_1 delete
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
Operation completed successfully.
```

Aktualisieren von Thin Clones eines VMFS-Datenspeichers

(Gilt nur für Thin Clones) Aktualisieren Sie den Thin Clone eines VMFS-Datenspeichers. Dies aktualisiert die Daten des Thin Clone mit Daten von dem angegebenen Quell-Snapshot.

Format

```
/stor/prov/vmware/vmfs {-id <value> | -name <value>} refresh [-async] {-source <value> | -sourceName <value>} -copyName <value> [-force]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des VMFS-Datenspeichers ein.
-name	Geben Sie den Namen des VMFS-Datenspeichers ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.
-source	Geben Sie die ID des Snapshot ein, der für die Aktualisierung des Thin Clone verwendet werden soll. Der Snapshot muss der Produktreihe des Basis-VMFS-Datenspeichers angehören.
-sourceName	Geben Sie den Namen des Snapshot ein, der für die Aktualisierung des Thin Clone verwendet werden soll. Der Snapshot muss der Produktreihe des Basis-VMFS-Datenspeichers angehören.
-copyName	Geben Sie den Namen der Kopie an, die vor der Aktualisierung des Thin Clone erstellt werden soll.
-force	Die VMFS-Ressource wird bedingungslos aktualisiert, auch wenn auf der Speicherressource Hostzugriff konfiguriert wurde.

Beispiel

Der folgende Befehl aktualisiert den Thin Clone namens vmware_2_tc mit Daten von dem Snapshot SNAP_2.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/vmware/vmfs -id vmware_2_tc refresh -source SNAP_2 -copyName Backup1
```

```
[Response]
Storage system address: 10.64.75.201
Storage system port: 443
HTTPS connection

ID = 38654705846
Operation completed successfully.
```

Managen von VMware-Protokollendpunkten

Protokollendpunkte (PEs) sind Zugriffspunkte für die ESX-/ESXi-Host-Kommunikation mit dem Speichersystem. Diese Endpunkte stellen nach Bedarf einen Datenpfad für virtuelle Maschinen und ihre jeweiligen vVol-Datenspeicher her. I/O-Vorgänge von VMs werden über den PE an den vVol-Datenspeicher auf dem Storage-System kommuniziert. Ein einziger Protokollendpunkt kann I/O-Anforderungen von einer großen Anzahl von VM-Clients auf ihren virtuellen Volumes bündeln.

NAS-Protokollendpunkte werden auf dem Speichersystem erstellt und verwaltet und entsprechen einem bestimmten NFS-basierten NAS-Server. Es wird empfohlen, für eine hohe Verfügbarkeit mindestens zwei NAS-Server für vVols zu aktivieren, jeweils einen für jeden

SP. Ein Datei-vVol wird jedes Mal an den zugeordneten NAS-PE gebunden, wenn die jeweilige virtuelle Maschine eingeschaltet wird. Wenn die virtuelle Maschine ausgeschaltet wird, wird die Bindung der vVols mit dem PE aufgehoben.

SCSI-Protokollendpunkte entsprechen einer bestimmten iSCSI-Schnittstelle oder Fibre Channel-Verbindung. Das Block-vVol wird jedes Mal an den zugeordneten SCSI-PE gebunden, wenn die jeweilige virtuelle Maschine eingeschaltet wird. Wenn die virtuelle Maschine ausgeschaltet wird, wird die Bindung des PE aufgehoben. SCSI-Protokollendpunkte sind wie LUN-Einhängepunkte, die den I/O-Zugriff auf vVols vom ESXi-Host aus zum Storage-System ermöglichen.

Tabelle 118. Protokollendpunkt-Attribute

Attribut	Beschreibung
ID	Kennung des VMware-Protokollendpunkts
Name	Name des Protokollendpunkts
Type	Typ des Protokollendpunkts Gültige Werte: <ul style="list-style-type: none"> • SCSI • NAS
VMware UUID	VMware-UUID des Protokollendpunkts
Export path (Nur NAS-PEs)	Exportpfad zum PE
IP address	IP-Adresse des NAS-Servers für Datei-PEs
WWN	Der WWN (World Wide Name) für Block-PEs.
Default SP	Kennung für den bevorzugten SP. Gültige Werte: <ul style="list-style-type: none"> • SPA • SPB
Current SP	Kennung für den aktuellen SP. Gültige Werte: <ul style="list-style-type: none"> • SPA • SPB
NAS server	Kennung des zugehörigen NAS-Servers für NAS-PEs
VMware NAS PE server (Nur NAS-PEs)	ID des entsprechenden VMware NAS PE-Servers.
vVol datastore (Nur NAS-PEs)	ID des vVol-Datenspeichers, der den PE verwendet
Host (Nur SCSI-PEs)	Durch Komma getrennte Liste von Kennungen für Hosts, die den PE verwenden.
LUN ID	Logical Unit Number für den Protokollendpunkt auf dem Host.
Health state	Integritätsstatus
Health details	Zusätzliche Integritätsinformationen.

Anzeigen von Protokollendpunkten

Zeigt eine Liste der vorhandenen Protokollendpunkte und deren Merkmale an.

Format

```
/stor/prov/vmware/pe [-id <value>] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des Protokollendpunkts ein.

Beispiel

Das folgende Beispiel zeigt die Details für alle Protokollendpunkte auf dem System an.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/vmware/pe show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      ID                = rfc4122.60060160-ca30-3c00-962b-87806445241a
      Name                = scsi_pe_1
      Type                = SCSI
      VMware UUID         = rfc4122.60060160-ca30-3c00-962b-87806445241a
      Export path         =
      IP address          =
      WWN                 = 60:06:01:60:CA:30:3C:00:96:2B:87:80:64:45:24:1A
      Default SP          = SPA
      Current SP          = SPA
      NAS Server          =
      VMware NAS PE server =
      VVol datastore      =
      Host                = Host_1
      LUN ID              =
      Health state        = OK (5)
      Health details      = "The protocol endpoint is operating normally. No action is
required."
```

Ändern des VMware-Protokollendpunkts

Ändert die Einstellungen für einen VMware-Protokollendpunkt. Dieser Befehl gilt nur für SCSI-Protokollendpunkte.

Format

```
/stor/prov/vmware/pe -id <value> set [-async] -lunid <value>
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des Protokollendpunkts ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.  ANMERKUNG: Gleichzeitige Befehle, unabhängig ob sie asynchron sind, können fehlschlagen, wenn sie beim Versuch, dieselben Systemelemente zu managen, in Konflikt stehen.
-lunid	Geben Sie die neue SCSI-LUN-ID für diesen Protokollendpunkt auf dem Host an.

Beispiel

Der folgende Befehl ändert die LUN, die vom SCSI-Protokollendpunkt verwendet wird.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/vmware/pe set -id
rfc4122.d54a64e3-9511-4832-90c3-b2cdfb622a2c set -lunid 5
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = rfc4122.d54a64e3-9511-4832-90c3-b2cdfb622a2c
Operation completed successfully.
```

vVol-Datenspeicher managen

vVols befinden sich in vVol-Datenspeichern, auch Speichercontainer genannt, die aus Speicherzuweisungen von einem oder mehreren Funktionsprofilen bestehen. Funktionsprofile werden auf einem oder mehreren zugrunde liegenden Speicherpools aufgebaut. Sie können vVol-Datenspeicher basierend auf einem oder mehreren Funktionsprofilen erstellen und ihnen dann eine bestimmte Menge Speicherplatz aus dem Funktionsprofil zuweisen.

Jeder vVol-Datenspeicher verfügt über ein oder mehrere Funktionsprofile, die seine Performance- und Kapazitätsmerkmale beschreiben, wie etwa Laufwerkstyp, FAST VP Tiering-Policy und Speicherplatzeffizienz-Policy (Thick oder Thin). Diese Merkmale werden aus dem zugrunde liegenden Speicherpool abgeleitet. Wenn in vSphere ein Virtual Volume erstellt wird, wird ihm ein Speicher-Policy-Profil zugewiesen. vSphere filtert die kompatiblen und inkompatiblen verfügbaren vVol-Datenspeicher (von einem oder mehreren Speichersystemen), wenn das vVol basierend auf diesen Profilen erstellt wird. Nur vVol-Datenspeicher, die das Speicher-Policy-Profil unterstützen, gelten als kompatible Speichercontainer für die Bereitstellung des vVol.

Tabelle 119. Attribute für vVol-Datenspeicher

Attribut	Beschreibung
ID	Kennung des vVol-Datenspeichers
Name	Name des vVol-Datenspeichers
Description	Beschreibung des vVol-Datenspeichers
VMware UUID	VMware UUID des vVol-Datenspeichers
Type	Typ des vVol-Datenspeichers Gültige Werte: <ul style="list-style-type: none"> • File • Block
Health state	Integritätsstatus des vVol-Datenspeichers Folgende Werte sind möglich: <ul style="list-style-type: none"> • Unknown (0) : Status ist unbekannt. • OK (5) : Läuft normal. • OK BUT (7) <ul style="list-style-type: none"> ○ Die Speicherressourcenzuweisung von einem oder mehreren Pools hat den Schwellenwert von 85 % überschritten. ○ Die Speicherressourcenzuweisung von einem oder mehreren Pools hat den Schwellenwert von 95 % überschritten. • Degraded/Warning (10) <ul style="list-style-type: none"> ○ Die Performance des Pools hat sich auf einem oder mehreren der zugrunde liegenden Speicherpools für das virtuelle Volume verschlechtert. ○ Die Speicherressourcenzuweisung von einem oder mehreren Pools hat den Schwellenwert von 95 % überschritten und die Speicherressource ist überbelegt. • Major failure (20) <ul style="list-style-type: none"> ○ Die Speicherressource ist aufgrund mindestens eines ausgefallenen Speicherpools ausgefallen. ○ Die Speicherressource ist aufgrund mindestens eines nicht verfügbaren Servers nicht verfügbar. ○ Die Speicherressource ist nicht verfügbar und erfordert eine Speicherintegritätsprüfung. • Critical failure (25) : Mindestens ein zugrunde liegender Storage-Pool für ein virtual Volume ist offline. • Non-recoverable error (30) : Ressource ist aufgrund mindestens eines nicht verfügbaren Storage-Pools nicht verfügbar.

Tabelle 119. Attribute für vVol-Datenspeicher (fortgesetzt)

Attribut	Beschreibung
Health details	Detaillierter Integritätsstatus des vVol-Datenspeichers.
Capability profile	Durch Komma getrennte Liste von Kennungen von Funktionsprofilen, die vom vVol-Datenspeicher unterstützt werden. Jede Kennung mit einem „(Not used)“-Suffix gibt an, dass dieses Profil vom vVol-Datenspeicher entfernt werden kann.
Storage pool ID	Durch Komma getrennte Liste von Kennungen von Storage-Pools, die für den vVol-Datenspeicher verwendet werden.
Total capacity	Gesamtkapazität des vVol-Datenspeichers
Total current allocation	Gesamte aktuelle Zuweisung des vVol-Datenspeichers in allen zugehörigen Storage-Pools
Total used capacity	Gesamte beanspruchte Kapazität des vVol-Datenspeichers
Creation time	Uhrzeit der Erstellung des vVol-Datenspeichers
Hosts	Hosts, die Zugriff auf den Datenspeicher haben
Last modified time	Uhrzeit der letzten Änderung des vVol-Datenspeichers

vVol-Datenspeicher erstellen

Erstellen Sie einen Datenspeicher für VMware-vVols.

Format

```
/stor/prov/vmware/vvolds create [-async] -name <value> [-descr <value>] -cp <value> -size <value> -type { block | file } [-hosts <value>]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.
-name	Geben Sie einen Namen für den vVol-Datenspeicher ein.  ANMERKUNG: Der Name kann alphanumerische Werte, einen Bindestrich, einen Unterstrich und einen Punkt enthalten. Er darf nicht mit Bindestrich oder Punkt beginnen und darf nicht nur aus Ziffern bestehen.
-descr	Geben Sie eine kurze Beschreibung des vVol-Datenspeichers ein.
-cp	Geben Sie die Liste von Kennungen von Funktionsprofilen an, die vom vVol-Datenspeicher unterstützt werden.
-size	Geben Sie die Liste der Zuweisungsgrößen an. Geben Sie eine Zuweisung für die Menge des insgesamt verfügbaren Speicherplatzes für die vVol-Bereitstellung auf dem vVol-Datenspeicher für das angegebene Funktionsprofil an. Wenn es mehrere Funktionsprofile gibt, sollte die Liste die Zuweisungsgröße in Bezug auf jedes Funktionsprofil umfassen.
-type	Geben Sie den Typ des vVol-Datenspeichers an. Gültige Werte: <ul style="list-style-type: none"> • block • file
-hosts	Geben Sie die kommasetrennte Liste von Hosts an, die auf den vVol-Datenspeicher werden zugreifen können. Eine Liste der berechtigten Hosts finden Sie unter Anzeigen von Hostkonfigurationen .

Beispiel

Mit dem folgenden Befehl wird ein vVol-Datenspeicher mit den folgenden Einstellungen erstellt:

- Der Name des vVol-Datenspeichers lautet „Engineering department“.
- Ordnet die Funktionsprofile „cp_1“ und „cp_2“ diesem vVol-Datenspeicher zu.
- Weist 10 GB und 12 GB von den Funktionsprofilen „cp_1“ bzw. „cp_2“ dem vVol-Datenspeicher zu.
- Gibt „Host_1“ und „Host_2“ Zugriffsberechtigung auf den Datenspeicher.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/vmware/vvolds create -
name "Engineering department" -cp cp_1,cp_2 -size 10G,12G -type file -hosts "Host_1,Host_2"
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = res_1
Operation completed successfully.
```

vVol-Datenspeicher anzeigen

Zeigen Sie eine Liste der vorhandenen vVol-Datenspeicher und deren Merkmale an.

Format

```
/stor/prov/vmware/vvolds [-id <value>] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des vVol-Datenspeichers ein.

Beispiel

Der folgende Befehl zeigt eine Liste der vVol-Datenspeicher und deren Merkmale an.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/vmware/vvolds show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
1:      ID              = res_1
      Name              = Performance
      Description       =
      VMware UUID      = 550e8400-e29b-41d4-a716-446655440000
      Type              = Block
      Health state      = OK (5)
      Health details    = "The component is operating normally. No action is
required."
      Capability profile = cp_1, cp_2 (Not used)
      Storage pool      = pool_1,pool_3
      Total capacity    = 128849018880 (120G)
      Total current allocation = 12884901888 (12G)
      Total used capacity = 1073741824 (1G)
      Hosts             = Host_1
      Creation time     = 2015-12-21 12:55:32
      Last modified time = 2016-01-15 10:31:56

2:      ID              = res_2
      Name              = engineering
      Description       =
      VMware UUID      = rfc4122.534e0655-f5a3-41d7-8124-9d53be5d0c0d
      Type              = file
      Health state      = OK (5)
      Health details    = "The component is operating normally. No action is
required."
```

```

Capability profile      = cp_1, cp_2
Storage pool          = pool_1, pool_2
Total capacity        = 644245094400 (600.0G)
Total current allocation = 0
Total used capacity   = 0
Creation time         = 2015-06-20 01:48:54
Last modified time    = 2015-06-20 01:48:54

```

vVol-Datenspeicher ändern

Ändern Sie einen vorhandenen vVol-Datenspeicher.

Format

```

/stor/prov/vmware/vvolds -id <value> set [-async] [-name <value>] [-descr <value>] [{-addCp
<value> -size <value> | -modifyCp <value> -size <value> | -removeCp <value>}] [{-hosts <value>|
[-addHosts <value>] [-removeHosts <value>]}] [-force]]

```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des zu ändernden vVol-Datenspeichers ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.
-name	Geben Sie einen Namen für den vVol-Datenspeicher ein.  ANMERKUNG: Der Name kann alphanumerische Werte, einen Bindestrich, einen Unterstrich und einen Punkt enthalten. Er darf nicht mit Bindestrich oder Punkt beginnen und darf nicht nur aus Ziffern bestehen.
-descr	Geben Sie eine neue Beschreibung für den vVol-Datenspeicher ein.
-addCp	Geben Sie die Liste der Kennungen neuer Funktionsprofile ein, die der vVol-Datenspeicher unterstützt.
-modifyCp	Geben Sie die Liste der Kennungen von Funktionsprofilen ein, die bereits von dem vVol-Datenspeicher unterstützt werden, und geben Sie für jeden die neue zugewiesene Größe an.
-size	Geben Sie die Liste der Zuweisungsgrößen an. Geben Sie eine Zuweisung für die Menge des insgesamt verfügbaren Speicherplatzes für die vVol-Bereitstellung auf dem vVol-Datenspeicher für das angegebene Funktionsprofil an. Wenn es mehrere Funktionsprofile gibt, sollte die Liste die Zuweisungsgröße in Bezug auf jedes Funktionsprofil umfassen.
-removeCp	Geben Sie die Liste der Kennungen von Funktionsprofilen ein, die Sie aus dem vVol-Datenspeicher entfernen möchten.  ANMERKUNG: Dieser Befehl kann nur auf Funktionsprofilen verwendet werden, die derzeit nicht von vorhandenen virtuellen Volumes verwendet werden.
-hosts	Gibt die kommagetrennte Liste von Hosts mit Zugriff auf den vVol-Datenspeicher an. Mit diesem Qualifizierer werden die vorhandenen Hostzugriffseinstellungen überschrieben.
-addHosts	Gibt die kommagetrennte Liste der hinzuzufügenden Hosts mit Zugriff auf die vVol-Datenspeicher an. Mit dieser Option können Sie inkrementell Hosts hinzufügen, die auf den vVol-Datenspeicher zugreifen können. Die vorhandenen Hosts werden dadurch nicht überschrieben.
-removeHosts	Gibt die kommagetrennte Liste von Hosts an, deren Zugriff auf den vVol-Datenspeicher entfernt werden soll. Mit dieser Option können Sie inkrementell den Zugriff von Hosts auf den vVol-Datenspeicher entfernen. Die vorhandenen Hosts werden dadurch nicht überschrieben.

Qualifizierer	Beschreibung
-force	Geben Sie diesen Befehl ein, um bedingungslos alle virtuellen Volumes zu trennen, die derzeit an einen Protokollendpunkt gebunden sind, der einem bestimmten Host zugeordnet ist.  ANMERKUNG: Wenn der Hostzugriff für einen vVol-Datenspeicher geändert oder entfernt wird, werden die zugehörigen Protokollendpunkte automatisch getrennt.

Beispiel 1

Mit dem folgenden Befehl werden die folgenden Einstellungen für einen vVol-Datenspeicher geändert:

- Ändert die Beschreibung des vVol-Datenspeichers zu „My new Description“.
- Ändert den Namen des vVol-Datenspeichers zu „My new Name“.
- Ordnet das Funktionsprofil „cp_1“ dem vVol-Datenspeicher „res_1“ zu.
- Weist dem Kapazitätsprofil „cp_1“ 10 GB Speicherplatz aus dem Pool zu.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/vmware/vvolds -id res_1 set -name MyNewName -descr "My new description" -addCp cp_1 -size 10G
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = res_1
Operation completed successfully.
```

Beispiel 2

Mit dem folgenden Befehl wird dem vVol-Datenspeicher Zugriff auf Host_11 hinzugefügt.

 **ANMERKUNG:** Obwohl Host_2, Host_3 und Host_14 bereits Zugriff auf den vVol-Datenspeicher haben, müssen Sie die vollständige Liste der Hosts, die Zugriff auf den vVol-Datenspeicher haben sollen, angeben, da der neue Host Host_11 hinzugefügt wird.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/vmware/vvolds -id res_1 set -hosts Host_2, Host_3, Host_11, Host_14
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = res_1
Operation completed successfully.
```

Beispiel 3

Das folgende Beispiel gewährt Host_2 Zugriff auf den vVol-Datenspeicher res_2 und entzieht Host_1 den Zugriff auf res_2:

```
uemcli /stor/prov/vmware/vvolds -id res_2 set -addHosts Host_2 -removeHosts Host_1
ID = res_2
Operation completed successfully.
```

vVol-Datenspeicher löschen

Löscht angegebene vVol-Datenspeicher und ihre zugeordneten virtuellen Volumes.

Format

```
/stor/prov/vmware/vvolds [-id <value>] delete [-async] [-force { yes | no}]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des vVol-Datenspeichers ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-force	Löschen Sie den vVol-Datenspeicher und alle ihm zugeordneten vVols. Gültige Werte: <ul style="list-style-type: none">• yes• no
-async	Führen Sie den Vorgang im asynchronen Modus aus.

Beispiel

Mit dem folgenden Befehl wird der vVol-Datenspeicher „res_1“ sowie seine virtual Volumes gelöscht.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/vmware/vvolds -id res_1 delete -force yes
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
Operation completed successfully.
```

vVol-Datenspeicherzuweisung managen

Managen Sie die Zuweisung von Storage für vVol-Datenspeicher.

Tabelle 120. Attribute für die vVol-Datenspeicherzuweisung

Attribut	Beschreibung
ID	Kennung der vVol-Datenspeicherzuweisung
vVol datastore	Kennung des vVol-Datenspeichers
Capability profile	Kennung des zugeordneten Funktionsprofils
Storage pool	Durch Komma getrennte Liste von Kennungen von Speicherpools, die dem Funktionsprofil zugeordnet sind
Size	Menge des insgesamt verfügbaren Speicherplatzes für die vVol-Bereitstellung für ein bestimmtes Funktionsprofil auf dem vVol-Datenspeicher
Current allocation	Die Menge des primären Storage, der aktuell für den vVol-Datenspeicher für vVols zugewiesen ist, bereitgestellt mit einem bestimmten Funktionsprofil auf dem vVol-Datenspeicher
Size used	Menge des Speicherplatzes, der von virtual Volumes verwendet wird, die mit einem bestimmten Funktionsprofil auf dem vVol-Datenspeicher bereitgestellt sind

Tabelle 120. Attribute für die vVol-Datenspeicherzuweisung (fortgesetzt)

Attribut	Beschreibung
Health state	Integritätsstatus der vVol-Datenspeicherzuweisung
Health details	Zusätzliche Integritätsinformationen.

Details der vVol-Datenspeicherzuweisung anzeigen

Zeigt vorhandene vVol-Datenspeicherzuweisungen an.

Format

```
/stor/prov/vmware/vvolds/alloc {-id <value> | -vvolds <value> [{-pool <value> | -cp <value>}]}
show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die Zuweisungskennung des vVol-Datenspeichers ein.
-vvolds	Geben Sie die ID des vVol-Datenspeichers ein.
-pool	Geben Sie die ID des Speicherpools ein.
-cp	Geben Sie die ID des Funktionsprofils ein.

ANMERKUNG: Informationen dazu, wie Sie die ID des vVol-Datenspeichers und des zugehörigen Pools und Funktionsprofils erhalten, finden Sie unter [vVol-Datenspeicher anzeigen](#).

Beispiel

Mit dem folgenden Befehl werden die Zuweisungsdetails für den vVol-Datenspeicher „vvol_1“ aus dem Pool „pool_1“ angezeigt, einschließlich der IDs der zugeordneten Funktionsprofile, der aktuellen Größe des Storage-Pools und der aktuellen Größe, die dem vVol-Datenspeicher vom Storage-Pool zugewiesen ist.

```
uemcli /stor/prov/vmware/vvolds/alloc -vvolds vvolds_1 -pool pool_1 show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:   ID                = cpa_1
     VVol datastore   = res_1
     Capability profile = cp_1
     Storage pool     = pool_1
     Size              = 128849018880 (120G)
     Current allocation = 12884901888 (12G)
     Size used         = 1073741824 (1G)
     Health state      = OK (5)
     Health details    = "The component is operating normally. No action is required."
```

vVol-Objekte managen

Virtuelle Volumes sind Kapselungen von Dateien virtueller Maschinen, virtueller Laufwerke und ihrer Ableitungen. Es gibt mehrere vVol-Objekttypen, die einem einzelnen Virtual Volume entsprechen, einschließlich VMDK-vVol (Daten-vVol), Konfig-vVol, Arbeitsspeicher-vVol und Swap-vVol.

Tabelle 121. vVol-Typen

VMDK (Daten)-vVol	Das VMDK-vVol, in Unisphere als Daten -vVol angezeigt, enthält die vDisk-Datei oder das Festplattenlaufwerk für die VM.
Konfig-vVol	Das Konfig -vVol enthält Informationen über Einstellungen, Konfiguration und Status zur VM. Dies umfasst .vmx-, .nvram- und Protokolldateien.
Arbeitsspeicher-vVol	Das Arbeitsspeicher -vVol enthält eine vollständige Kopie des VM-Arbeitsspeichers als Teil eines In-Memory VM-Snapshot.
Swap-vVol	Das Swap -vVol wird erstellt, wenn VMs eingeschaltet werden und Kopien der VM-Arbeitsspeicherseiten enthalten, die nicht im Arbeitsspeicher beibehalten werden.

Tabelle 122. vVol-Attribute

Attribut	Beschreibung
ID	Kennung des virtuellen Volume
Name	Name des virtuellen Volumes.
Type	Typ des virtuellen Volume. Gültige Werte: <ul style="list-style-type: none"> ● Data ● Config ● Memory ● Swap ● Other
Replica type	Replikattyp des virtuellen Volume. Gültige Werte: <ul style="list-style-type: none"> ● Base ● Prepared Snap ● Ready Snap ● Fast-Clone
Parent	Kennung des virtuellen Basis-/übergeordneten Volume für den Snapshot, vorbereiteten Snapshot oder Fast Clone.
Health state	Integritätsstatus des virtuellen Volume
Health details	Zusätzliche Integritätsinformationen für das virtuelle Volume
Datastore	Kennung des mit dem virtuellen Volume verknüpften Datenspeichers
Storage pool	Kennung des Speicherpools, der das virtuelle Volume enthält
Capability profile	Kennung des mit dem virtuellen Volume verknüpften Funktionsprofils
Policy profile	Name des VMware vSphere-Policy-Profiles
Compliant	Gibt an, ob das virtuelle Volume mit dem VMware vSphere-Policy-Profil vorgabekonform ist.
Size	Größe des virtuellen Volume.
Current allocation	Gesamte derzeitige Zuweisung des virtuellen Volume
Bound to	Durch Komma getrennte Liste der Protokollendpunkt-Kennungen, an die das virtuelle Volume gebunden ist. Ein leerer Wert zeigt ein ungebundenes virtuelles Volume an.
Binding details	Bindungsdetails des Protokollendpunkts, an das das virtuelle Volume gebunden ist <ul style="list-style-type: none"> ● Für virtuelle Volumes, die an NFS-Protokollendpunkte gebunden sind, werden die vollständigen NFS-Pfade angezeigt. ● Für virtuelle Volumes, die an iSCSI-Protokollendpunkte gebunden sind, wird die sekundäre ID des virtuellen Volume-iSCSI angezeigt. ● Für ungebundene virtuelle Volumes ist dieser Wert leer.

Tabelle 122. vVol-Attribute (fortgesetzt)

Attribut	Beschreibung
Virtual machine	Kennung der virtuellen Maschine
VM hard disk	Name der zugehörigen VM-Festplatte
SP owner	Name des Storage-Prozessors, auf dem die vVol platziert ist.
Creation time	Zeitpunkt und Uhrzeit der Erstellung des virtual Volume.

vVol-Objekte anzeigen

Zeigen Sie eine Liste der vorhandenen vVol-Datenspeicher und deren Merkmale an.

Format

```
/stor/prov/vmware/vvol {[-id <value> | [-vm <value>] [-cp <value>] [-pool <value>] [-datastore <value>] [-pe <value>] [-parent <value>] [-bound] [-noncompliant] } show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des virtuellen Volumes ein.
-name	Geben Sie den Namen des virtual Volumes ein.
-vm	Geben Sie die ID der zugehörigen VM für das virtuelle Volume ein.
-cp	Geben Sie die ID des mit dem virtuellen Volume verknüpften Funktionsprofils ein.
-pool	Geben Sie die ID des Speicherpools ein, der das virtuelle Volume enthält.
-datastore	Geben Sie die ID des zugehörigen vVol-Datenspeichers ein.
-pe	Geben Sie die ID des Protokollendpunkts ein, für die Sie gebundene virtuelle Volumes anzeigen möchten.
-parent	Geben Sie die ID des übergeordneten virtuellen Volumes ein.
-bound	Spezifizieren Sie, um eine Liste von nur gebundenen virtuelle Volumes anzuzeigen.
-noncompliant	Spezifizieren Sie, um eine Liste nur von virtuellen Volumes anzuzeigen, die nicht vorgabenkonform mit ihren jeweiligen VMware-Policy-Profilen sind.

Beispiel

Das folgende Beispiel zeigt die Details aller vVols für die VM mit der ID „VM_1“ an.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/vmware/vvol -vm VM_1 show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      ID                = rfc4122.de305d54-75b4-431b-adb2-eb6b9e546014
      Name                = Hard disk 1
      Type                = Data
      Replica type        = Base
      Parent              =
      Health state        = OK (5)
      Health details      = "The component is operating normally. No action is required."
      Datastore           = res_1
      Storage pool        = pool_1
      Capability profile   = cp_1
```

```

Policy profile      = VMware policy profile
Compliant          = yes
Size              = 1073741824 (1G)
Thin              = yes
Current allocation = 107374182 (100M)
Bound to          = NASPE_1
Binding details   = 192.168.3.3:/vvol1
Virtual machine    = VM_1
VM hard disk      = VM_Hard Disk 1
SP owner          = SPA
Creation Time     = 2020-04-03 17:14:56

```

vVol-Objekte löschen

Löscht die angegebenen vorhandenen vVol-Objekte.

ANMERKUNG: Das Löschen von vVol-Objekten muss ausdrücklich vom Nutzer bestätigt werden. Die folgende Bestätigungsmeldung wird angezeigt:

```

Virtual volume deletion will also unbind and delete associated snapshots and fast-clones.
Do you want to delete the virtual volume?
yes / no:

```

Der Standardwert im unbeaufsichtigten Modus ist `yes`.

Format

```
/stor/prov/vmware/vvol -id <value> delete [-async]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des virtuellen Volumes ein.
-name	Geben Sie den Namen des virtual Volumes ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.

Beispiel

Mit dem folgenden Befehl wird das virtuelle Volume mit der Kennung `naa.6006016005603c009370093e194fca3f` gelöscht.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/vmware/vvol -id
naa.6006016005603c009370093e194fca3f delete
```

```

Virtual volume deletion will also unbind and delete associated snapshots and fast-clones. Do
you want to delete the virtual volume?
yes / no:
yes

```

```

Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

```

Operation completed successfully.

vVol-Snapshots erstellen

Erfahren Sie, wie Sie native Snapshots eines VMDK (Daten)-vVol-Objekts erstellen.

Erstellen Sie Snapshots eines VMDK, von Daten oder virtual Volumes.

- ANMERKUNG:** Ein vVol-Snapshot, der in Unity erstellt wurde, kann nicht mit vSphere wiederhergestellt werden. Allerdings kann ein vVol-Snapshot, der mit der mit VASA verbundenen vSphere erstellt wurde, entweder mit Unity oder vSphere wiederhergestellt werden.
- ANMERKUNG:** Daten-vVol-Snapshots, die auf Unity erstellt wurden, sind für vSphere nicht sichtbar. Einige vSphere-Workflows, z. B. die Datenmigration mit vMotion, entfernen alle Daten-vVol-Snapshots für die entsprechenden VMDKs. Die entfernten Daten für diese vVol-Snapshots können nach dem Löschen nicht wiederhergestellt werden.

Format

```
/stor/prov/vmware/vvol {-id <value> | -name <value>} createSnap [-snapName <value>] [-async]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des virtual Volumes an.
-name	Geben Sie den Namen des virtual Volumes an.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-snapName	Geben Sie optional den bevorzugten Namen des neuen Snapshots an. Wenn nicht angegeben, weist das System einen Namen mit der vorgegebenen Namenskonventionen <i>UTC_date_time</i> zu.
-async	Geben Sie ihn an, um den Vorgang im asynchronen Modus auszuführen.

Beispiel

Im folgenden Beispiel wird ein Snapshot für das virtual Volume „naa.600601606ab04d003ba396e2c2db4fe3“ mit dem Snapshot-Namen „Backup-Snap“ erstellt.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/vmware/vvol -id  
naa.600601606ab04d003ba396e2c2db4fe3 createSnap -snapName backup-snap
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection
```

```
ID=naa.600601606ab04d00a27149d01a8a4f15  
Operation completed successfully.
```

vVol-Snapshots wiederherstellen

Erfahren Sie, wie Sie einen vorhandenen Snapshot eines VMDK (Daten)-vVol-Objekts wiederherstellen.

Stellen Sie vorhandene Snapshots eines VMDK, von Daten oder virtual Volumes, die in Unisphere oder vSphere erstellt wurden, wieder her.

- ANMERKUNG:** Die zugeordnete VM für den vVol muss in vSphere ausgeschaltet werden, bevor Snapshots wiederhergestellt werden.
- ANMERKUNG:** Ein vVol-Snapshot, der in Unity erstellt wurde, kann nicht mit vSphere wiederhergestellt werden. Allerdings kann ein vVol-Snapshot, der mit der mit VASA verbundenen vSphere erstellt wurde, entweder mit Unity oder vSphere wiederhergestellt werden.

Format

```
/stor/prov/vmware/vvol {-id <value> | -name <value>} restore {-snap <value> | -snapName <value>} [-async]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des virtual Volumes an.
-name	Geben Sie den Namen des virtual Volumes an. Wenn der vVol-Name nicht eindeutig ist, verwenden Sie den Qualifizierer -id.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-snap	Geben Sie die ID des vVol-Snapshots an, von dem aus Sie die VMDK (Daten)-vVol wiederherstellen möchten.
-snapName	Geben Sie den Namen des vVol-Snapshots an, von dem aus Sie die VMDK (Daten)-vVol wiederherstellen möchten.
-async	Geben Sie ihn an, um den Vorgang im asynchronen Modus auszuführen.

Beispiel

Im folgenden Beispiel wird die Snapshot-ID "naa.600601606ab04d00a27149d01a8a4f15" für das virtual Volume "naa.600601606ab04d003ba396e2c2db4fe3" wiederhergestellt.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/vmware/vvol -id naa.600601606ab04d003ba396e2c2db4fe3 restore -snap naa.600601606ab04d00a27149d01a8a4f15
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
Operation completed successfully.
```

Managen von Funktionsprofilen

Ein Funktionsprofil ist eine Gruppe von Storage-Funktionen, die für vVol-Datenspeicher anwendbar sind. Sie müssen mindestens ein Funktionsprofil erstellen, bevor Sie vVol-Datenspeicher erstellen können.

Funktionen werden automatisch von dem zugrunde liegenden Speicherpool abgeleitet und werden durch die Eigenschaften des Pools festgelegt. Nutzungstags werden vom Speicheradministrator zugewiesen.

Es gibt drei Möglichkeiten für das Profil von Speicherfunktionen für einen Pool:

Tabelle 123. Speicherfunktionen

Name der Funktion	Beschreibung
Servicelevelbasiertes Provisioning (physische Bereitstellungen)	<p>Erwartetes Servicelevel für den Pool:</p> <ul style="list-style-type: none"> ● Platinum <ul style="list-style-type: none"> ○ Flash-Pool mit einem Tier ● Gold <ul style="list-style-type: none"> ○ Multi-Tier-Pool mit einer Kombination aus Flash- und SAS-Laufwerken ○ Pool mit einem Tier und SAS RAID 10 ● Silver <ul style="list-style-type: none"> ○ Pool mit mehreren Tiers und einer Kombination aus SAS und NL-SAS ○ Pool mit einem Tier und SAS RAID 5 oder RAID 6 ● Bronze <ul style="list-style-type: none"> ○ Pool mit mehreren Tiers und einer Kombination aus Flash und NL-SAS ○ Pool mit einem Tier und NL-SAS
Servicelevelbasiertes Provisioning (virtuelle Bereitstellungen)	<p>Erwartetes Servicelevel für einen virtuellen Pool:</p> <ul style="list-style-type: none"> ● Gold <ul style="list-style-type: none"> ○ Multi-Tier-Pool mit einer Kombination aus Tiers für extreme Performance und Performance-Tiers ○ Single-Tier-Pool für extreme Performance ● Silver <ul style="list-style-type: none"> ○ Multi-Tier-Pool mit einer Kombination aus Tiers für extreme Performance, Performance-Tiers und Kapazitäts-Tiers ○ Multi-Tier-Pool mit einer Kombination aus Performance- und Kapazitäts-Tiers ○ Single-Tier-Pool für Performance ● Bronze <ul style="list-style-type: none"> ○ Multi-Tier-Pool mit einer Kombination aus Tiers für extreme Performance und Kapazitäts-Tiers ○ Single-Tier-Pool für Kapazität
Nutzungstags	<p>Nutzungstags können auf Funktionsprofile angewendet werden, um diese und die zugeordneten vVol-Datenspeicher einer bestimmten Verwendung zuzuweisen. Beispiel: Ein vVol-Datenspeicher kann für VVols und VMs gekennzeichnet werden, die eine bestimmte Anwendung unterstützen. Die Virtualisierungs- und Speicheradministratoren sollten zusammenarbeiten, um diese Nutzungstags zu definieren.</p>
Speichereigenschaften	<p>Die unterstützten Speichereigenschaften umfassen:</p> <ul style="list-style-type: none"> ● Laufwerkstyp: <ul style="list-style-type: none"> ○ Extreme Performance (Flash) ○ Performance (SAS) ○ Kapazität (NL-SAS) ○ Multi-Tier [gemischt] ○ Extrem-Multi-Tier [gemischt mit Flash] ● RAID-Typ(nur physische Bereitstellungen): <ul style="list-style-type: none"> ○ RAID5 ○ RAID6 ○ RAID10 ○ Heterogene ● FAST Cache (nur physische Bereitstellungen): <ul style="list-style-type: none"> ○ Enabled ○ Disabled ● FAST VP-Tiering Policy: <ul style="list-style-type: none"> ○ Tier mit hoher Verfügbarkeit ○ Hoch starten, dann automatisches Tiering ○ Auto-Tier ○ Tier mit geringer Verfügbarkeit

Tabelle 123. Speicherfunktionen (fortgesetzt)

Name der Funktion	Beschreibung
	<ul style="list-style-type: none"> ● Speicherplatzeffizienz: <ul style="list-style-type: none"> ○ Thick ○ Thin

Tabelle 124. Attribute für Funktionsprofile

Attribut	Beschreibung
ID	Kennung von Funktionsprofil
Name	Name von Funktionsprofil
Description	Beschreibung von Funktionsprofil
VMware UUID	VMware-UUID des Funktionsprofils
Storage pool	Zugehörige Speicherpoolkennung.
Service level	Servicelevel des zugrunde liegenden Speicherpools Gültige Werte: <ul style="list-style-type: none"> ● Platinum ● Gold ● Silver ● Bronze
Usage tag	Durch Komma getrennte Liste benutzerdefinierter Tags. Jeder Tag ist ein Wert, bestehend aus einer alphanumerischen Zeichenfolge.
Drive type	Gibt den Laufwerkstyp des zugrunde liegenden Storage an, der durch den Storage-Pool bestimmt wird. Gültige Werte: <ul style="list-style-type: none"> ● CapacityTier ● PerformanceTier ● ExtremePerformanceTier ● MultiTier ● ExtremeMultiTier
RAID level(nur physische Bereitstellungen)	Gibt das RAID-Level des zugrunde liegenden Speicherpools an. Gültige Werte: <ul style="list-style-type: none"> ● RAID5 ● RAID10 ● RAID6 ● Mixed
FAST Cache(nur physische Bereitstellungen)	Gibt an, ob FAST Cache im zugrunde liegenden Speicherpool aktiviert ist oder nicht. Gültige Werte: <ul style="list-style-type: none"> ● On ● Off
FAST VP policy	Durch Komma getrennte Liste von FAST VP-Speicher-Policies für den zugrunde liegenden Speicherpool Gültige Werte: <ul style="list-style-type: none"> ● Start high then auto-tier ● Auto-tier ● Highest available tier ● Lowest available tier
Space efficiency	Durch Komma getrennte Liste der verfügbaren Speicherplatzeffizienz-Policies für den zugrunde liegenden Speicherpool Gültige Werte: <ul style="list-style-type: none"> ● Thick ● Thin
Health state	Integritätsstatus
Health details	Zusätzliche Integritätsinformationen.

Erstellen eines Funktionsprofils

Erstellen Sie ein Funktionsprofil für vVol-Datenspeicher.

Format

```
/stor/config/cp create [-async] -name <value> [-descr <value>] -pool <value> [-usageTag <value>]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.
-name	Geben Sie einen Namen für das Funktionsprofil ein.  ANMERKUNG: Der Name kann alphanumerische Werte, einen Bindestrich, einen Unterstrich und einen Punkt enthalten. Er darf nicht mit Bindestrich oder Punkt beginnen und darf nicht nur aus Ziffern bestehen.
-descr	Geben Sie eine Beschreibung für das Funktionsprofil ein.
-pool	Geben Sie die Kennung des Speicherpools an, auf dem das Funktionsprofil basiert.
-usageTag	Geben Sie eine durch Komma getrennte Liste der benutzerdefinierten Nutzungs-Tags ein. Jeder Tag ist ein Wert, bestehend aus einer alphanumerischen Zeichenfolge.

Beispiel

Mit dem folgenden Befehl wird ein Funktionsprofil mit den folgenden Einstellungen erstellt:

- Gibt den Funktionsprofilnamen „CapabilityProfile1“ an.
- Gibt an, dass das Funktionsprofil auf „pool_1“ basiert.
- Gibt den Nutzungs-Tag als „Produktion“ an.
- Es wird nicht angegeben, dass es im asynchronen Modus erstellt wird.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/cp create -name  
"CapabilityProfile1" -pool pool_1 -usageTag "Production"
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection
```

```
ID = cp_1  
Operation completed successfully.
```

Anzeigen von Funktionsprofilen

Zeigt eine Liste der vorhandenen Funktionsprofile und deren Merkmale an.

Format

```
/stor/config/cp [-id <value>] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des Funktionsprofils ein.

Beispiel

Der folgende Befehl zeigt eine Liste der vorhandenen Funktionsprofile und deren Merkmale an.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/cp show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID                = cp_1
Name              = CapabilityProfile1
Description       =
VMware UUID       = 550e8400-e29b-41d4-a716-446655440000
Storage pool      = pool_1
Service level     = Gold
Usage tag         = Exchange, OLTP
Drive type        = ExtremeMultiTier
RAID level        = Mixed
FAST Cache        = Off
FAST VP policy    = Start high then auto-tier, Auto-tier, Highest available tier,
Lowest available tier
Space efficiency  = Thin, Thick
Health state      = OK (5)
Health details    = "The component is operating normally. No action is required."
```

Ändern von Funktionsprofilen

Ändern Sie ein vorhandenes Funktionsprofil.

Format

```
/stor/config/cp -id <value> set [-async] [-name <value>] [-descr <value>] [{"-addUsageTag <value>"}
| -removeUsageTag <value>}]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des zu ändernden Funktionsprofils ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.
-name	Geben Sie einen Namen für das Funktionsprofil ein.  ANMERKUNG: Der Name kann alphanumerische Werte, einen Bindestrich, einen Unterstrich und einen Punkt enthalten. Er darf nicht mit Bindestrich oder Punkt beginnen und darf nicht nur aus Ziffern bestehen.
-descr	Geben Sie eine Beschreibung für das Funktionsprofil ein.
-addUsageTag	Durch Komma getrennte Liste benutzerdefinierter Nutzungs-Tags, die dem angegebenen Funktionsprofil hinzugefügt werden sollen. Jeder Tag ist ein Wert, bestehend aus einer alphanumerischen Zeichenfolge.
-removeUsageTag	Durch Komma getrennte Liste benutzerdefinierter Nutzungs-Tags, die aus dem angegebenen Funktionsprofil entfernt werden sollen. Jeder Tag ist ein Wert, bestehend aus einer alphanumerischen Zeichenfolge.

Beispiel

Mit dem folgenden Befehl wird der Name des Funktionsprofils „cp_1“ geändert.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/cp -id cp_1 set -name "CapabilityProfile2"
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection
```

```
ID = cp_1  
Operation completed successfully.
```

Löschen von Funktionsprofilen

Löscht angegebene Funktionsprofile.

Format

```
/stor/config/cp [-id <value>] delete [-async]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des Funktionsprofils ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.

Beispiel

Mit dem folgenden Befehl wird das Funktionsprofil „cp_1“ gelöscht.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/cp -id cp_1 delete
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection
```

```
Operation completed successfully.
```

Managen von I/O-Limits

Eine I/O-Policy ermöglicht es, den Durchsatz und die Bandbreite zu begrenzen, wodurch die Performance in System-Workloads, also zwischen Hosts und Anwendungen und Speicherressourcen, zuverlässiger vorhergesehen werden kann.

In der folgenden Tabelle sind die Attribute für I/O-Limits aufgeführt.

Tabelle 125. Attribute für I/O-Limits

Attribut	Beschreibung
ID	ID des I/O-Limits
Name	Name des I/O-Limits
Description	Kurze Beschreibung des I/O-Limits
Shared	Gibt an, ob es ein gemeinsames I/O-Limit ist, d. h. ob die Einstellungen durchgesetzt werden in Bezug auf die Summe aller Speicherressourcen, die diese Policy haben, oder in Bezug auf jede einzelne Speicherressource. Folgende Werte sind möglich: <ul style="list-style-type: none"> • yes • no (Standardeinstellung)
Paused	Gibt an, ob die definierte I/O-Limit-Policy angehalten wurde. Folgende Werte sind möglich: <ul style="list-style-type: none"> • yes • no
Type	Ob das I/O-Limit absolut oder dichte basiert ist. Folgende Werte sind möglich: <ul style="list-style-type: none"> • absolute (Standardeinstellung) • density
Maximum IOPS	Maximale I/O-Vorgänge pro Sekunde für eine absolute Limit-Policy.
Maximum KBPS	Maximale KB pro Sekunde für eine absolute Limit-Policy.
Maximum IOPS per GB	Maximale IOPS pro GB Größe für das angebundene Objekt. Dies gilt nur, wenn der Policy-Typ dichte basiert ist. Das effektive Limit ist das Produkt der maximalen IOPS und der Größe in GB des ange bundenen Objekts.
Maximum KBPS per GB	Maximale KB/s pro GB Größe für das angebundene Objekt. Dies gilt nur, wenn der Policy-Typ dichte basiert ist. Das effektive Limit ist das Produkt der maximalen KB/s und der Größe in GB des ange bundenen Objekts.
Burst rate	Die Menge des Datenverkehrs über dem Basis-I/O-Limit, der während der Burst-Zeit auftreten kann, ausgedrückt als Prozentsatz des Basislimits. Burst-Zeit und -Häufigkeit müssen ebenfalls angegeben werden. Der Wert ist 1 bis 100.
Burst time	Anzahl der Minuten, während der der Datenverkehr das Basislimit überschreiten kann. Die angegebene Burst-Rate überschreitet den zulässigen Bereich. Verwenden Sie das folgende Format: <Wert><Qualifizierer>. Hierbei gilt: <ul style="list-style-type: none"> • Wert <ul style="list-style-type: none"> ◦ minutes: Anzahl der Minuten im Bereich von 1 bis 60. • Qualifizierer <ul style="list-style-type: none"> ◦ m: Gibt die Minuten an. <p>i ANMERKUNG: Diese Einstellung ist kein festes Limit und wird nur verwendet, um die zusätzlichen I/O-Vorgänge zu berechnen, die für Bursting zugewiesen werden. Die tatsächliche Burst-Zeit hängt von der I/O-Aktivität ab und kann länger als definiert sein, wenn die Aktivität niedriger ist als die zulässige Burst-Rate.</p>
Burst frequency	Anzahl der Stunden zwischen dem Beginn eines Bursts und des folgenden Bursts. Burst-Rate und -Zeit müssen ebenfalls angegeben werden. Verwenden Sie das folgende Format:<Wert><Qualifizierer>. Hierbei gilt: <ul style="list-style-type: none"> • Wert <ul style="list-style-type: none"> ◦ hours: Anzahl der Stunden im Bereich von 1 bis 24. • Qualifizierer <ul style="list-style-type: none"> ◦ h: Gibt die Stunden an. <p>i ANMERKUNG: Wenn eine Burst-Policy-Einstellung anfänglich angewendet oder geändert wird, beginnt das Intervall der Burst-Häufigkeit und der Speicher, der der Policy zugeordnet ist, kann sofort einen Burst verarbeiten, unabhängig davon, wann der letzte Burst aufgetreten ist.</p>
Effective IOPS limit	Dies ist ein schreibgeschützter Wert, der nur für eine gemeinsam verwendete Policy gilt. Es handelt sich um die gesamten effektiven IOPS für alle kombinierten ange bundenen Objekte.

Tabelle 125. Attribute für I/O-Limits (fortgesetzt)

Attribut	Beschreibung
Effective KBPS limit	Dies ist ein schreibgeschützter Wert, der nur für eine gemeinsam verwendete Policy gilt. Es handelt sich um die gesamten effektiven KB/s für alle kombinierten angebotenen Objekte.

Erstellen einer I/O-Begrenzungs-Policy

Erstellen Sie eine I/O-Limit-Policy, die auf eine Speicherressource angewendet werden kann.

Format

```
/stor/config/iolimit create [-async] -name <value> [-descr <value>] [-shared {yes | no}] [-type {absolute | density}] [-maxIOPS <value>] [-maxKBPS <value>] [-maxIOPSDensity <value>] [-maxKBPSDensity <value>] [-burstRate <value> -burstTime <value> -burstFrequency <value>]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.
-name	Geben Sie den Namen des I/O-Limits ein.
-descr	Geben Sie eine kurze Beschreibung des I/O-Limits ein.
-shared	Geben Sie an, ob das I/O-Limit gemeinsam genutzt wird. Folgende Werte sind möglich: <ul style="list-style-type: none"> • yes • no (Standardeinstellung)
-type	Geben Sie an, ob eine absolute oder dichte basierte Policy erstellt wird. Folgende Werte sind möglich: <ul style="list-style-type: none"> • absolute (Standardeinstellung) • density
-maxIOPS	Geben Sie die maximalen IOPS an. Kann nicht festgelegt werden, wenn -type density ist.
-maxKBPS	Geben Sie die maximalen KB/s an. Kann nicht festgelegt werden, wenn -type density ist.
-maxIOPSDensity	Geben Sie die maximalen IOPS pro GB Größe für das angebundene Objekt an. Kann nicht festgelegt werden, wenn -type absolute ist.
-maxKBPSDensity	Geben Sie die maximalen KB/s pro GB Größe für das angebundene Objekt an. Kann nicht festgelegt werden, wenn -type absolute ist.
-burstRate	Geben Sie die Burst-Rate als Prozentsatz über dem Basislimit an. Erfordert die Verwendung von -burstTime und -burstFrequency. Wert ist 1 bis 100.
-burstTime	Geben Sie das Zeitintervall in Minuten an, während dem die Burst-Rate in Kraft ist. Erfordert die Verwendung von -burstRate und -burstFrequency. Verwenden Sie das folgende Format: <Wert>m. Hierbei gilt: <ul style="list-style-type: none"> • <Wert>: Anzahl der Minuten im Bereich von 1 bis 60 • m: Qualifizierer zur Erkennung der Minuten
-burstFrequency	Geben Sie an, wie oft Bursting erlaubt ist (in Stunden). Erfordert die Verwendung von -burstRate und -burstTime. Verwenden Sie das folgende Format: <Wert>h. Hierbei gilt: <ul style="list-style-type: none"> • <Wert>: Anzahl der Stunden im Bereich von 1 bis 24 • h: Qualifizierer zur Erkennung der Stunden

Beispiel 1

Mit dem folgenden Befehl wird eine I/O-Limit-Policy mit den folgenden Einstellungen erstellt:

- Name: finance.
- Beschreibung: for finance department.
- Gemeinsam genutzt.
- Typ: absolut.
- Maximale IOPS: 500.
- Maximale KB/s: 1000.

Die I/O-Limit-Policy erhält die ID IOL_1:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/iolimit create -name "finance" -descr "for finance department" -shared yes -type absolute -maxIOPS 500 -maxKBPS 1000
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection
```

```
ID = IOL_1  
Operation completed successfully.
```

Beispiel 2

Mit dem folgenden Befehl wird eine I/O-Limit-Policy mit den folgenden Einstellungen erstellt:

- Name: engineering.
- Beschreibung: for engineering department.
- Nicht freigegeben.
- Typ: dichte basiert.
- Maximale IOPS pro GB: 600.
- Maximale KB/s pro GB: 2000.
- Burst-Rate: 30 Prozent.
- Burst-Zeit: 5 Minuten.
- Burst-Häufigkeit: 2 Stunden.

Die I/O-Limit-Policy erhält die ID IOL_2:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/iolimit create -name "engineering" -descr "for engineering department" -shared yes -type density -maxIOPSDensity 600 -maxKBPSDensity 2000 -burstRate 30 -burstTime 5m -burstFrequency 2h
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection
```

```
ID = IOL_2  
Operation completed successfully.
```

Beispiel 3

Der folgende Befehl ist fehlgeschlagen, weil `-type` auf `absolute` festgelegt war, aber nur für `-type = density` anwendbare Optionen angegeben wurden.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/iolimit create -name "HR2" -type absolute -maxIOPSDensity 2000 -maxKBPSDensity 3000
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection
```

```
Operation failed. Error code: 0x900912a  
Mismatch between policy type and limit values. Absolute policy requires Maximum IOPS and/or
```

```
Maximum KBPS while Density-based policy requires Maximum IOPS per GB and/or Maximum KBPS per GB. (Error Code:0x900912a)
```

Beispiel 4

Der folgende Befehl ist fehlgeschlagen, weil `-type` auf `density` festgelegt war, aber nur für `-type = absolute` anwendbare Optionen angegeben wurden.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/iolimit create -name "HR3" -type density -maxIOPS 2000 -maxKBPS 3000
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
Operation failed. Error code: 0x900912a
Mismatch between policy type and limit values. Absolute policy requires Maximum IOPS and/or Maximum KBPS while Density-based policy requires Maximum IOPS per GB and/or Maximum KBPS per GB. (Error Code:0x900912a)
```

Löschen einer I/O-Limit-Policy

Löschen Sie eine I/O-Limit-Policy.

Format

```
/stor/config/iolimit -id <value> delete [-async] [-force]
```

Objektqualifizierer

Qualifizierer	Beschreibung
<code>-id</code>	Geben Sie den Namen der I/O-Limit-Policy ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
<code>-async</code>	Führen Sie den Vorgang im asynchronen Modus aus.
<code>-force</code>	Legen Sie fest, ob eine I/O-Limit-Policy gelöscht werden kann, wenn sie von Speicherressourcen oder Snapshots noch verwendet wird. Wenn das nicht festgelegt ist, wird eine Fehlermeldung ausgegeben. Andernfalls wird die I/O-Limit-Policy von allen Speicherressourcen und/oder Snapshots entfernt, bevor sie gelöscht wird.

Beispiel

Mit dem folgenden Befehl wird die I/O-Limit-Policy „IOL_1“ gelöscht:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/iolimit -id IOL_1 delete
```

```
Storage system address: 10.64.75.201
Storage system port: 443
HTTPS connection
```

```
Operation completed successfully.
```

Ändern einer I/O-Limit-Policy

Ändern Sie die Einstellungen einer vorhandenen I/O-Limit-Policy.

Format

```
/stor/config/iolimit -id <value> set [-async] [-name <value>] [-descr <value>] [-paused {yes | no}] [-type {absolute | density}] [{{-maxIOPS <value> | -noMaxIOPS}}] [{{-maxKBPS <value> | -noMaxKBPS}}] [{{-maxIOPSDensity <value> | -noMaxIOPSDensity}}] [{{-maxKBPSDensity <value> | -noMaxKBPSDensity}}] [{{-noBurst | [-burstRate <value> -burstTime <value> -burstFrequency <value>}}]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie den Namen der zu ändernden I/O-Limit-Policy ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.
-name	Geben Sie den Namen des I/O-Limits ein.
-descr	Geben Sie eine kurze Beschreibung des I/O-Limits ein.
-paused	Gibt an, ob die definierte I/O-Limit-Policy angehalten oder wiederaufgenommen wurde. Folgende Werte sind möglich: <ul style="list-style-type: none"> • yes • no (Standardeinstellung)
-type	Geben Sie an, ob eine absolute oder dichte basierte Policy erstellt wird. Folgende Werte sind möglich: <ul style="list-style-type: none"> • absolute (Standardeinstellung) • density
-maxIOPS	Geben Sie die maximalen IOPS an.
-maxKBPS	Geben Sie die maximalen KB/s an.
-noMaxIOPS	Geben Sie dies zum Löschen der Einstellung -maxIOPS an.
-noMaxKBPS	Geben Sie dies zum Löschen der Einstellung -maxKBPS an.
-maxIOPSDensity	Geben Sie die maximalen IOPS pro GB Größe für das angebundene Objekt an.
-maxKBPSDensity	Geben Sie die maximalen KB/s pro GB Größe für das angebundene Objekt an.
-nomaxIOPSDensity	Geben Sie dies zum Löschen der Einstellung -maxIOPSDensity an.
-nomaxKBPSDensity	Geben Sie dies zum Löschen der Einstellung -maxKBPSDensity an.
-noBurst	Geben Sie dies zum Deaktivieren des Bursting für die aktuelle I/O-Limit-Policy und Löschen der Werte für -burstRate, -burstTime und -burstFrequency an.
-burstRate	Geben Sie die Burst-Rate als Prozentsatz über dem Basislimit an. Erfordert die Verwendung von -burstTime und -burstFrequency. Wert ist 1 bis 100.
-burstTime	Geben Sie das Zeitintervall in Minuten an, während dem die Burst-Rate in Kraft ist. Erfordert die Verwendung von -burstRate und -burstFrequency. Verwenden Sie das folgende Format: <Wert>m. Hierbei gilt:

Qualifizierer	Beschreibung
	<ul style="list-style-type: none"> • <Wert>: Anzahl der Minuten im Bereich von 1 bis 60 • m: Qualifizierer zur Erkennung der Minuten
-burstFrequency	<p>Geben Sie an, wie oft Bursting erlaubt ist (in Stunden). Erfordert die Verwendung von -burstRate und -burstTime. Verwenden Sie das folgende Format:</p> <p><Wert>h. Hierbei gilt:</p> <ul style="list-style-type: none"> • <Wert>: Anzahl der Stunden im Bereich von 1 bis 24 • h: Qualifizierer zur Erkennung der Stunden

Beispiel 1

Mit dem folgenden Befehl wird die I/O-Limit-Policy „IOL_1“ mit diesen Einstellungen aktualisiert:

- Name: engineering.
- Maximale IOPS: 1000.
- Löscht die maximale KB/s-Einstellung.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/iolimit -id IOL_1 set -name "engineering" -maxIOPS 1000 -noKBPS
```

```
Storage system address: 10.64.75.201
Storage system port: 443
HTTPS connection
```

```
Operation completed successfully.
```

Beispiel 2

Mit dem folgenden Befehl wird die I/O-Limit-Policy IOL_1 angehalten:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/iolimit -id IOL_1 set -paused yes
```

```
Storage system address: 10.64.75.201
Storage system port: 443
HTTPS connection
```

```
Operation completed successfully.
```

Anzeigen von I/O-Limit-Policies

Zeigen Sie die Einstellungen für die angegebene I/O-Limit-Policy oder für alle vorhandenen I/O-Limit-Policies an.

Format

```
/stor/config/iolimit [-id <value>] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie den Namen der I/O-Limit-Policy ein, die angezeigt werden soll.

Beispiel

Mit dem folgenden Befehl werden Details zu allen I/O-Limit-Policies im System angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/iolimit show -detail
```

```
Storage system address: 10.64.75.201
Storage system port: 443
HTTPS connection

1:      ID              = IOL_1
      Name              = Finance
      Description       = for finance department
      Shared            = yes
      Paused            = yes
      Type              = absolute
      Maximum IOPS      = 500
      Maximum KBPS      = 1000
      Maximum IOPS per GB =
      Maximum KBPS per GB =
      Burst rate        =
      Burst time        =
      Burst frequency   =
      Effective IOPS limit = 500
      Effective KBPS limit = 1000

2:      ID              = IOL_2
      Name              = Engineering
      Description       = for engineering department
      Shared            = no
      Paused            = no
      Type              = density
      Maximum IOPS      =
      Maximum KBPS      =
      Maximum IOPS per GB = 600
      Maximum KBPS per GB = 2000
      Burst rate        = 30%
      Burst time        = 5m
      Burst frequency   = 2h
      Effective IOPS limit = 1800
      Effective KBPS limit = 6000
```

 **ANMERKUNG:** Das an IOL_2 angehängte Objekt in diesem Beispiel verfügt über 3 GB Speicher.

Managen der I/O-Limitkonfiguration

Eine I/O-Policy ermöglicht es, den Durchsatz und die Bandbreite zu begrenzen, wodurch die Performance in System-Workloads, also zwischen Hosts und Anwendungen und Speicherressourcen, zuverlässiger vorhergesehen werden kann.

Eine I/O-Begrenzungs-Policy kann auf eine einzelne LUN oder eine Gruppe von LUNs angewendet werden. Es kann nur eine I/O-Begrenzungs-Policy auf eine einzelne LUN oder eine LUN angewendet werden, die Teil einer Consistency Group ist.

In der folgenden Tabelle sind die Attribute für I/O-Limitkonfigurationen aufgeführt.

Tabelle 126. Attribute für die I/O-Limitkonfiguration

Attribut	Beschreibung
IO limits paused	Ob die auf dem System definierten I/O-Limit-Policies durchgesetzt werden.
Maximum controllable storage objects	Maximale Anzahl von Speicherobjekten, die erzwungene I/O-Limits haben können; dazu gehören Speicherressourcen und angebundene Snapshots.
Actively controlled storage objects	Anzahl von Speicherobjekten, die derzeit erzwungene I/O-Limits haben; dazu gehören Speicherressourcen und angebundene Snapshots.

Anzeigen der I/O-Limit-Konfigurationseinstellung

Zeigen Sie die Einstellungen für die vorhandene I/O-Limit-Konfigurationseinstellung an.

Format

```
/stor/config/iolimit/config show
```

Beispiel

Mit dem folgenden Befehl werden im System definierten I/O-Limits angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/iolimit/config show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
1:      IO limits paused                = yes
        Max controllable storage objects = 512
        Actively controlled storage objects = 200
```

Durchsetzen der Verwendung der I/O-Limit-Konfigurationseinstellung

Setzen Sie die Verwendung der vorhandenen I/O-Limit-Konfigurationseinstellung im gesamten System durch.

ANMERKUNG: Die Durchsetzung von Host-I/O-Limits wird global in Ihrem gesamten System gesteuert. Sie können die Verwendung einer bestimmten Policy nicht deaktivieren oder aktivieren.

Format

```
/stor/config/iolimit/config set -paused {yes|no}
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-paused	Geben Sie an, ob die auf dem System definierten I/O-Limit-Policies durchgesetzt werden. Gültige Werte sind „yes“ und „no“.

Beispiel

Mit dem folgenden Befehl wird die Verwendung von I/O-Limits auf dem System durchgesetzt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/iolimit/config set -paused no
```

```
Storage system address: 10.64.75.201
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Schützen von Daten

Themen:

- Management von Snapshots
- Managen von Snapshot-NFS-Shares
- Managen von Snapshot-CIFS-Freigaben
- Managen von Replikationssitzungen
- Managen von virtuellen RecoverPoint-Appliances-CHAP-Konten
- Managen der Data-at-Rest-Verschlüsselung (nur physische Bereitstellungen)
- Managen von KMIP-Support (nur physische Bereitstellungen)

Management von Snapshots

Ein Snapshot ist ein virtuelles Point-In-Time Image der Daten in einer Speicherressource, die seit dem letzten Snapshot geändert wurden. Mit Snapshots wird der Inhalt einer festgelegten Speicherressource an einem bestimmten Datum und zu einer bestimmten Uhrzeit aufgezeichnet. Es handelt sich jedoch nicht um eine gespiegelte Kopie der Daten. Durch die regelmäßige Erstellung von Snapshots von Dateisystemen und LUNs können Sie auf effektive Weise die Anforderungen an den Schutz der Daten und an die Recovery erfüllen. Auf der Grundlage der Bedeutung und der Flüchtigkeit von Daten in einer Speicherressource können Sie Pläne festlegen, in denen die Zeitpunkte und die Intervalle für die Snapshot-Erstellung definiert sind.

Setzen Sie Snapshots wie folgt ein:

- Wiederherstellung des Zustands einer Speicherressource zu einem früheren Zeitpunkt.
- Zugriff auf den Inhalt eines Snapshot zur Wiederherstellung beschädigter oder versehentlich gelöschter Dateien und Daten.

Um Snapshots regelmäßig automatisch zu erstellen, verknüpfen Sie die Snapshots mit Zeitplänen. [Managen von Snapshot-Schutzplänen](#) erläutert, wie Zeitpläne im System konfiguriert werden. Die einzelnen Snapshots verfügen über eigene IDs.

i ANMERKUNG: Snapshots sind kein Ersatz für Speicherbackups. Snapshots sind nicht für die Wiederherstellung nach Ausfällen oder bei Verlust der physischen Geräte vorgesehen.

In der folgenden Tabelle sind die Attribute für Snapshots aufgeführt.

Tabelle 127. Snapshot-Attribute

Attribut	Beschreibung
ID	ID des Snapshot.
Name	Name des Snapshot.
State	Status des Snapshot. Gültige Werte: <ul style="list-style-type: none"> • initializing • ready • faulted • offline • destroying
Attached	Gibt an, ob der Snapshot an einen Host angebunden ist. i ANMERKUNG: Bei Dateisystem-Snapshots ist das Feld leer.
Source	ID der Speicherressource, von der der Snapshot erstellt wurde.
Source type	Der Typ der Speicherressource, von der der Snapshot erstellt wurde.
Attach details	Eine kommagetrennte Liste von Exportpfaden oder WWNs für angebundene Snapshots.
Members	Eine kommagetrennte Liste der zum Snapshot gehörigen LUNs.

Tabelle 127. Snapshot-Attribute (fortgesetzt)

Attribut	Beschreibung
	 ANMERKUNG: Bei Dateisystem-Snapshots ist das Feld leer.
Source snapshot	Für einen Snapshot eines Snapshot die ID des übergeordneten Snapshot.
Description	Snapshot-Beschreibung.
Creation time	Datum und Uhrzeit der Snapshot-Erstellung.
Expiration time	Datum und Uhrzeit, an dem der Snapshot aus dem System gelöscht wird. Der Standardwert ist 7 Tage.
Last writable time	Zeitpunkt, zu dem der Snapshot oder dessen übergeordneter Snapshot zuletzt getrennt wurde.
Last refresh time	Gibt den letzten Zeitpunkt an, zu dem der Snapshot aktualisiert wurde.
Created by	Name des Benutzers, Schutzplans oder Backup-Vorgangs, der für die Erstellung des Snapshot verantwortlich ist. Gültige Werte: <ul style="list-style-type: none"> • Der Name des Benutzerkontos (bei manuell von einem Benutzer erstellten Snapshots). • Bei geplanten Snapshots wird der Name des Schutzplans verwendet. • Bei Snapshots, die durch die Backupsoftware des Hosts erstellt werden, werden folgende Werte verwendet: <ul style="list-style-type: none"> ◦ NDMP: Der Snapshot wurde unter Verwendung des Network Data Management Protocol (NDMP) erstellt. ◦ VSS: Der Snapshot wurde vom Microsoft Volume Snapshot Service (VSS), auch als Schattenkopie bzw. „Vorherige Version“ bezeichnet, erstellt. • Snapshot Restore: Gibt einen Snapshot an, der beim Wiederherstellen eines Dateisystems oder eines VMware NFS-Datenspeichers vom System automatisch erstellt wurde. Mithilfe des Snapshot können Sie den Zustand der Speicherressource vor der letzten Wiederherstellung wiederherstellen.
Modified	Gibt an, ob der Snapshot an einen Mount-Punkt für Snapshot angebunden war oder ist oder Shares aufweist. Gültige Werte: <ul style="list-style-type: none"> • yes • no
Allow auto-delete	Gibt an, ob das System den Snapshot automatisch löschen kann. Gültige Werte: <ul style="list-style-type: none"> • yes • no Der Standardwert ist yes.
Size	Vom Snapshot verbrauchte Pool-Kapazität.  ANMERKUNG: Dieses Feld ist bei Snapshots von Consistency Groups und VMware-Blockanwendungen leer.
Access	Gibt an, ob ein Dateisystem-Snapshot ein schreibgeschützter Kontrollpunkt ist oder der Benutzerzugriffstyp „Lesen/Schreiben“ lautet.
IO limit	Durch Komma getrennte I/O-Limit-Policy-IDs für die angebenen Snapshots blockbasierter Speicherressourcen. Mitglieder einer Snapshotgruppe können andere I/O-Limit-Policy-IDs haben.
Effective maximum IOPS	Abhängig vom Policy-Typ. Für eine dichte-basierte Policy ist dieser Wert das Produkt der maximalen IOPS und der Größe des angehängten Snapshot. Dies ist ein schreibgeschütztes Attribut.
Effective maximum KBPS	Abhängig vom Policy-Typ. Für eine dichte-basierte Policy ist dieser Wert das Produkt der maximalen KB/s und der Größe des angehängten Snapshot. Dies ist ein schreibgeschütztes Attribut.
Remote system	Eine durch Kommas getrennte Liste von Remote-Systemen, deren Snapshot repliziert wird oder zu dem repliziert wird. Es gibt höchstens 4 Remote-Systeme.
Read/write hosts	Durch Kommas getrennte Liste von Hostkennungen mit Schreibberechtigung Gilt nur, wenn der Snapshot an einen dynamischen Mount-Punkt für Snapshot angebunden ist.
Read-only hosts	Durch Kommas getrennte Liste von Hostkennungen mit Leseberechtigung Gilt nur, wenn der Snapshot an einen dynamischen Mount-Punkt für Snapshot angebunden ist.

Tabelle 127. Snapshot-Attribute (fortgesetzt)

Attribut	Beschreibung
Replicated	Gibt an, ob der Snapshot asynchron repliziert wird. Gültige Werte: <ul style="list-style-type: none"> • no: Nicht für die Replikation markiert. • pending: Für die Replikation markiert, wartet aber auf Synchronisation. • yes: Erfolgreich auf dem Ziel repliziert. • failed to replicate, check System Alerts for details: Replikation ist fehlgeschlagen. • in progress: Snapshot wird übertragen
Sync replicated	Gibt an, ob der Schnappschuss an einer synchronen Replikationssitzung teilnimmt. Gültige Werte: <ul style="list-style-type: none"> • no: Der Snapshot wurde entweder auf dem Zielstandort erstellt und wird nicht auf dem Quellsystem repliziert oder der Snapshot wurde vor der Einrichtung der synchronen Replikationssitzung erstellt. • yes: Erfolgreich repliziert • failed to replicate: Der Snapshot wurde auf dem Quellstandort erstellt, während sich eine Replikationssitzung in einem aufgeteilten Zustand befand. Der Schnappschuss wurde nicht auf dem Zielstandort repliziert.
Remote expiration time	Eine durch Kommas getrennte Liste der Ablaufzeit, die jedem Remote-System entspricht, wenn der Snapshot von jedem Ziel entfernt wird.
Remote allow auto-delete	Gibt an, ob die automatische Löschung auf dem Ziel auch für diesen Snapshot gilt. Gültige Werte: <ul style="list-style-type: none"> • yes • no Der Standardwert ist no.
Clone count	Zeigt die Anzahl der Thin Clones an, die dem Snapshot zugeordnet sind.
Replication Origin	Array, von dem der replizierte Snapshot erstellt wurde. Gültige Werte: <ul style="list-style-type: none"> • N/A : Gibt an, dass der Snapshot nicht auf dem Remote-System repliziert wurde, oder synchron vom System repliziert wurde, dessen OE-Version älter als 5.1.0 ist. • [System serial number] – Gibt das System an, von dem der Snapshot stammt.

Erstellen von Snapshots

Erstellen Sie einen Snapshot einer Speicherressource.

ANMERKUNG: Snapshots von LUNs sind nicht für die Verwendung als Spiegel, für die Disaster Recovery oder als Hochverfügbarkeitstools vorgesehen. Da LUN-Snapshots teilweise aus Echtzeitdaten auf den LUNs abgeleitet sind, kann es vorkommen, dass kein Zugriff mehr auf die Snapshots besteht, diese also nicht mehr gelesen werden können, wenn kein Zugriff auf die primäre LUN mehr besteht.

Voraussetzungen

Snapshots werden im Schutzspeicher der Speicherressource gespeichert. Vergewissern Sie sich, dass die Kapazität des Schutzspeichers für Snapshots ausreicht. [Anzeigen von Dateisystemen](#) erläutert, wie die Größe des aktuellen Schutzspeichers für Dateisysteme angezeigt wird. [Anzeigen von LUNs](#) erläutert, wie die aktuelle Schutzgröße für LUNs angezeigt wird.

Format

```
/prot/snap create [-async] -source <value> [-name <value>] [-descr <value>] [{"-keepFor <value>"} | -allowAutoDelete {yes | no}] [-access {ckpt | share}] [-replicateSnap [-dstSys <value>]] [{"-keepSameAsSource | -keepRemotelyFor <value> | -allowRemoteAutoDelete {yes | no}}]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.
-name	Geben Sie einen Namen für den Snapshot ein.
-descr	Geben Sie eine Beschreibung für den Snapshot ein.
-source	Geben Sie die ID der Speicherressource ein, von der Sie einen Snapshot erstellen möchten. Anzeigen von Dateisystemen erläutert, wie die Einstellungen für Dateisysteme angezeigt werden. Anzeigen von Consistency Groups erläutert, wie die Einstellungen für die iSCSI-Speicherressourcen angezeigt werden.
-keepFor	<p>Geben Sie ein, wie lange ein Snapshot aufbewahrt werden soll. Das Intervall kann in Tagen oder Stunden definiert werden. Vom System werden abgelaufene Snapshots automatisch gelöscht. Das Format lautet wie folgt:</p> <pre><value><qualifier></pre> <p>Hierbei gilt:</p> <ul style="list-style-type: none"> • value : Geben Sie die Zahl der Stunden bzw. Tage ein: <ul style="list-style-type: none"> ○ Bei Stunden können Zahlen im Bereich von 1 bis 8.760 eingegeben werden. ○ Bei Tagen können Zahlen im Bereich von 1 bis 365 eingegeben werden. • qualifier : Geben Sie den Qualifizierer für den Wert ein. Folgende Werte sind möglich: <ul style="list-style-type: none"> ○ h : Gibt die Stunden an. ○ d : Gibt die Tage an. <p> ANMERKUNG: Bei geplanten Snapshots, die mit einem Plan verknüpft sind, wird über den Qualifizierer <code>-keepFor</code> in den Planregeln die Aufbewahrungsfrist festgelegt. Managen von Aufgabenregeln bietet Einzelheiten zu Planregeln.</p>
-allowAutoDelete	<p>Geben Sie an, ob das System automatisch den Snapshot oder Snapshot-Satz löschen kann. Gültige Werte:</p> <ul style="list-style-type: none"> • <code>yes</code> (Standard) • <code>no</code>
-access	<p>Geben Sie an, ob der Snapshot ein schreibgeschützter Kontrollpunkt ist oder „Lesen/Schreiben“ für CIFS (SMB)-Freigaben oder NFS-Exporte eingestellt ist. Gültige Werte:</p> <ul style="list-style-type: none"> • <code>ckpt</code> (Standard) • <code>share</code>
-replicateSnap	<p>Geben Sie an, ob dieser Snapshot für die Replikation markiert werden soll. Gültige Werte:</p> <ul style="list-style-type: none"> • <code>yes</code> • <code>no</code> (Standard)
-keepSameAsSource	Gibt an, ob die gleiche Aufbewahrungs-Policy (Ablaufzeit und automatisches Löschen) der Quelle für das Ziel verwendet werden soll. Dies ist eine einmalige Kopie der Aufbewahrungs-Policy des Quell-Snapshot und die Remoteaufbewahrungs-Policy wird nicht aktualisiert, wenn die Quellaufbewahrungs-Policy geändert wird. Keine Werte sind zulässig.
-keepRemotelyFor	<p>Gibt die Aufbewahrungsdauer an, nach der der Snapshot auf dem Ziel gelöscht wird. Das Intervall kann in Tagen oder Stunden definiert werden. Der Wert hat das folgende Format:</p> <pre><value><qualifier></pre> <p>Hierbei gilt:</p> <ul style="list-style-type: none"> • Wert: ein ganzzahliger Wert. Wenn der Qualifizierer <code>h</code> (Stunden) ist, ist der zulässige Bereich von 1 bis 43800. Wenn der Qualifizierer <code>d</code> (Tage) ist, ist der zulässige Bereich von 1 bis 1825. • Qualifizierer: ein Qualifizierer des Werts. Gültige Werte sind <code>h</code> (Stunden) und <code>d</code> (Tage).
-allowRemoteAutoDelete	<p>Gibt an, ob automatisches Löschen auf der replizierten Kopie dieses Snapshot oder Snapshot-Satzes erlaubt ist. Gültige Werte:</p> <ul style="list-style-type: none"> • <code>yes</code> • <code>no</code>

Qualifizierer	Beschreibung
-dstSys	Identifiziert das Zielsystem, auf das der Nutzer-Snapshot repliziert wird. Sie müssen diesen Qualifizierer angeben, wenn mehrere Replikationssitzungen einer Quellressource vorhanden sind, die die asynchrone Replikation unterstützt. <ul style="list-style-type: none"> • Wenn nur eine asynchrone Sitzung für die Snapshot-Replikation verfügbar ist, ist dieser Qualifizierer optional. • Wenn mehr als eine asynchrone Sitzung für die Snapshot-Replikation verfügbar ist, muss -dstSys einen Wert haben.

Beispiel

Mit dem folgenden Befehl wird ein Snapshot eines Dateisystems mit den folgenden Einstellungen erstellt:

- Name: accounting
- Speicherressource: Dateisystem FS_1.
- Aufbewahrungsfrist: 1 Tag

Dem Snapshot wird die ID SNAP_1 zugewiesen:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/snap create -name accounting -source FS_1 -keepFor 1d
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = SNAP_1
Operation completed successfully.
```

Anzeigen von Snapshots

Anzeigen von Details zu den Snapshots im System. Sie können nach der Snapshot-ID, dem Snapshotnamen oder der Speicherressourcen-ID filtern.

 **ANMERKUNG:** Aktionsbefehl „show“ erläutert, wie das Ausgabeformat geändert wird.

Format

```
/prot/snap [{"-id <value> | -name <value>} [-members] | -source <value>}] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Identifiziert die ID eines Snapshots.
-name	Identifiziert den Namen des Snapshot.
-members	Flag zeigt an, dass nur Mitglied-Snapshots gezeigt werden.  ANMERKUNG: Dies gilt nur für Snapshots von Consistency Groups und VMware VMFS-Speicherressourcen.
-source	Identifiziert die ID einer Speicherressource, um nur die damit verbundenen Snapshots anzuzeigen.

Beispiel 1

Mit dem folgenden Befehl werden Details zu sämtlichen Snapshots im System angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/snap show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      ID                = 38654705680
      Name                = Snapshot1
      State               = Ready
      Attached            = no
      Resource            = app_1
      Resource type       = LUN_group
      Source              = app_1
      Source type         = LUN_group
      Members             = sv_1,sv_2
      Attach details      = 60:06:01:60:D2:04:00:00:78:4F:09:51:22:EB:34:E3,
60:06:01:60:D2:04:00:00:78:4F:09:51:22:EB:34:E4

2:      ID                = 38654705681
      Name                = Snapshot2
      State               = Ready
      Attached            = no
      Resource            = app_1
      Resource type       = LUN_group
      Source              = app_2
      Source type         = LUN_group
      Members             = sv_3,sv_4
      Attach details      = 60:06:01:60:D2:04:00:00:78:4F:09:51:22:EB:34:E3,
60:06:01:60:D2:04:00:00:78:4F:09:51:22:EB:34:E4
```

Beispiel 2

Mit dem folgenden Befehl werden Details zu sämtlichen Snapshots im System angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/snap show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      ID                = 171798691871
      Name                = snap_test2
      State               = Ready
      Attached            = no
      Source              = res_3
      Source Type         = File system
      Members             =
      Attach details      =
      Source Snapshot     =
      Description         =
      Creation time       = 2019-07-23 17:14:56
      Expiration time     = Never
      Last writable time  = Never
      Last refresh time   = Never
      Created by          = admin
      Modified            = no
      Allow auto-delete   = yes
      Size                = 3221225472 (3.0G)
      Access              = Checkpoint
      IO limit            =
      Effective maximum IOPS =
      Effective maximum KBPS =
      Read/write hosts    =
      Read-only hosts     =
      Sync replicated     = no
      Remote system       = FCNCH197158598, FCNCH097574970
```

```

Remote expiration time = 2019-07-24 08:23:57, Never
Remote Allow auto-delete = no, yes
Replicated = pending, pending
Clone count =
Replication Origin = FCNCH197158598

```

Anhängen von Snapshots an Hosts

Binden Sie für Snapshots von Speicherressourcen einen Snapshot an, um ihn für Hosts verfügbar zu machen.

ANMERKUNG: Wenn der standardmäßige Anhangstyp verwendet wird, bevor ein Host auf einen angebotenen Snapshot zugreifen kann, muss er die entsprechenden Snapshot-Berechtigungen für die jeweilige Speicherressource besitzen. [Managen von LUNs](#) erläutert, wie Sie die Berechtigungen für den Hostzugriff bei LUN-Speicherressourcen konfigurieren.

Format

```

/prot/snap {-id <value> | -name <value>} attach [-async] [-copyName <value>] [-type {default |
dynamic [-roHosts <value>] [-rwHosts <value>]} [-force {yes | no}]]

```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des anzuhängenden Snapshot ein.
-name	Geben Sie den Namen des anzuhängenden Snapshot ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.
-copyName	Geben Sie den Namen der Kopie an, die das System vor dem Anhängen des ausgewählten Snapshot erstellt. Wird diese Befehlszeilenoption festgelegt und kein Name angegeben, weist das System der Kopie einen Namen zu. ANMERKUNG: Ist diese Befehlszeilenoption nicht festgelegt, wird keine Kopie erstellt.
-type	Anhangstyp. Gültige Werte sind folgende (keine Unterscheidung zwischen Groß- und Kleinschreibung): <ul style="list-style-type: none"> default (Standardeinstellung): Ermöglicht die Hochstufung jeweils nur eines Snapshot der übergeordneten Speicherressource. dynamic: ermöglicht die Hochstufung mehrerer Snapshots derselben übergeordneten Speicherressource gleichzeitig.
-roHosts	Geben Sie die kommagetrennte Liste von Hosts an, die Lesezugriff auf den Snapshot haben.
-rwHosts	Geben Sie die kommagetrennte Liste von Hosts an, die Lese-/Schreibzugriff auf den Snapshot haben.
-force	Geben Sie an, dass Lese-/Schreibzugriff für den Snapshot konfiguriert werden kann, obwohl das Objekt unabhängige Thin Clones hat. Gültige Werte: <ul style="list-style-type: none"> yes no (Standardeinstellung)

Beispiel

Mit dem folgenden Befehl wird der Snapshot SNAP_1 angehängt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/snap -id SNAP_1 attach -type dynamic -roHosts Host_1,Host_2 -rwHosts Host_3,Host_4
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection  
  
Operation completed successfully.
```

Aktualisieren von Snapshots

 **ANMERKUNG:** Der Befehl zum Aktualisieren von Snapshots gilt für Block- und Datei-Snapshots.

Format

```
/prot/snap {-id <value> | -name <value>} refresh [-async] [-copyName <value>]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	ID des zu aktualisierenden Snapshot.
-name	Name des zu aktualisierenden Snapshot.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.
-copyName	Geben Sie den Namen der Kopie an, die das System vor der Aktualisierung erstellt. Wenn kein Name angegeben wird („ "), wird eine Kopie mit einem Datum/Zeitstempelnamen erstellt.  ANMERKUNG: Ist diese Befehlszeilenoption nicht festgelegt, wird keine Kopie erstellt.

Beispiel

Mit dem folgenden Befehl wird ein Snapshot aktualisiert:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/snap -id 38654705680 refresh -copyName copy1
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection  
  
ID = 38654705680  
Operation completed successfully
```

Replizieren von Snapshots

 **ANMERKUNG:** Damit können Sie Snapshots replizieren, nachdem sie erstellt wurden.

Format

```
/prot/snap {-id <value> | -name <value>} replicate [ -dstSys <value> ] [ {-keepSameAsSource | -keepRemotelyFor <value> | -allowRemoteAutoDelete {yes | no}} ] [-force]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Identifiziert den Snapshot.
-name	Identifiziert den Snapshot anhand seines Namens.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-dstSys	Identifiziert das Remote-System, auf das der Nutzer-Snapshot repliziert wird. Dieser Qualifizierer muss angegeben werden, wenn mehrere Replikationssitzungen der Quellressource vorhanden sind, die die asynchrone Snapshot-Replikation unterstützt.
-keepSameAsSource	Gibt an, ob die gleiche Aufbewahrungs-Policy (Ablaufzeit und automatisches Löschen) der Quelle für das Ziel verwendet werden soll oder nicht. Dies ist eine einmalige Kopie der Aufbewahrungs-Policy des Quell-Snapshot und die Remoteaufbewahrungs-Policy wird nicht aktualisiert, wenn die Quellaufbewahrungs-Policy geändert wird.
-keepRemotelyFor	Gibt die Aufbewahrungsfrist an, nach der der Snapshot auf dem Ziel gelöscht wird. Das Intervall kann in Tagen oder Stunden definiert werden. Der Wert hat das folgende Format: <value><qualifier> Hierbei gilt: <ul style="list-style-type: none">• value: Geben Sie die Zahl der Stunden bzw. Tage ein:<ul style="list-style-type: none">○ Bei Stunden können Zahlen im Bereich von 1 bis 43.800 eingegeben werden.○ Bei Tagen können Zahlen im Bereich von 1 bis 1825 eingegeben werden.• qualifier: Geben Sie den Qualifizierer für den Wert ein. Folgende Werte sind möglich:<ul style="list-style-type: none">○ h: Gibt die Stunden an.○ d: Gibt die Tage an.
-allowRemoteAutoDelete	Gibt an, ob automatisches Löschen auf der replizierten Kopie dieses Snapshot oder Snapshot-Satzes erlaubt ist. Gültige Werte: <ul style="list-style-type: none">• yes• no
-force	Gilt nur für Dateisystem-Snapshots. Replizieren Sie den Snapshot asynchron, unabhängig davon, ob der Replikationsstatus des Snapshots auf einem Zielsystem der synchronen Replikation nicht aktualisiert werden konnte, wenn die entsprechende synchrone Replikationssitzung nicht aktiv ist.

Beispiel

Mit dem folgenden Befehl wird ein Snapshot repliziert:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/snap -id 38654705680 replicate -keepRemotelyFor 1d
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
Operation completed successfully.
```

Trennen von Snapshots

Bei Snapshots von Speicherressourcen können angehängte Snapshots getrennt werden, damit die Hosts nicht mehr darauf zugreifen können.

i ANMERKUNG: Damit ein Host auf einen angehängten Snapshot zugreifen kann, muss er die entsprechenden Snapshot-Berechtigungen für die jeweilige Speicherressource besitzen. [Managen von LUNs](#) erläutert, wie Sie die Berechtigungen für den Hostzugriff für LUN-Speicher konfigurieren.

Format

```
/prot/snap {-id <value> | -name <value> } detach [-async]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des zu trennenden Snapshot ein.
-name	Geben Sie den Namen des zu trennenden Snapshot ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.

Beispiel

Mit dem folgenden Befehl wird der Snapshot SNAP_1 getrennt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/snap -id SNAP_1 detach
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Wiederherstellen einer Speicherressource mithilfe eines Snapshot

Beim Wiederherstellen einer Speicherressource mithilfe eines Snapshot wird ein früherer Zustand der Speicherressource wiederhergestellt; es wird also ein Rollback ausgeführt. Während der Wiederherstellung wird die gesamte Speicherressource, einschließlich aller darauf gespeicherter Dateien und Daten, durch den Inhalt des ausgewählten Snapshot ersetzt.

Bei der Wiederherstellung einer Speicherressource an einen Snapshot, erstellt das System vor Beginn der Wiederherstellung automatisch einen Snapshot des aktuellen Status der Speicherressource. Dadurch wird sichergestellt, dass der Wiederherstellungsvorgang nicht zu einem unbeabsichtigten Datenverlust führt. Sie können diesen neuen Snapshot später verwenden, um bei Bedarf den vorherigen Zustand der Speicherressource wiederherzustellen.

Voraussetzungen

- Zur Vermeidung von Datenverlusten vergewissern Sie sich, dass auf allen Hosts alle Lese- und Schreibvorgänge auf die wiederherzustellende Speicherressource beendet wurden.
- Bei LUN-Speicher:
 - Wenn der Snapshot angehängt wird, müssen Sie ihn zunächst trennen, da andernfalls bei der Wiederherstellung ein Fehler angezeigt wird.

- Wenn ein Host mit der (vom Host als Laufwerk erkannten) LUN verbunden ist, die Sie wiederherstellen möchten, führen Sie eine der folgenden Optionen aus, um die LUN vom Host trennen:
 - Deaktivieren Sie in Windows im Geräte-Manager die LUN, bei der eventuell ein Hostneustart erforderlich wäre.
 - Führen Sie in Linux/UNIX den Befehl „unmount“ für das virtuelle Laufwerk aus.
 Sobald die Verbindung zur LUN getrennt ist, können Sie mit der Wiederherstellung fortfahren und anschließend die wiederhergestellte LUN auf dem Host aktivieren bzw. mounten.

Format

```
/prot/snap {-id <value> | -name <value> } restore [-backupName <value>] [-async]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des Snapshot ein, auf dessen Zustand Sie die zugehörige Speicherressource wiederherstellen möchten.
-name	Geben Sie den Namen des Snapshot ein, auf dessen Zustand Sie die zugehörigen Speicherressourcen wiederherstellen möchten.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.
-backupName	Gibt den Namen des Snapshot an, den das System automatisch im ersten Schritt des Wiederherstellungsvorgangs erstellt. Das System weist diesem Snapshot einen Namen zu, sofern der Benutzer keinen Namen angibt.

Beispiel

Mit dem folgenden Befehl wird Snapshot SNAP_1, ein Snapshot für iSCSI-Speicher, wiederhergestellt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/snap -id SNAP_1 restore
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
Operation completed successfully.
```

Löschen eines Snapshot

Löschen Sie einen Snapshot einer Speicherressource.

i ANMERKUNG: Nach dem Löschen eines Snapshot ist es nicht mehr möglich, Daten aus dem Snapshot oder eine Speicherressource auf den Stand des Snapshot wiederherzustellen.

Format

```
/prot/snap {-id <value> | -name <value>} delete [-async] [-overrideLock] [-force]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des zu löschenden Snapshots ein.
-name	Geben Sie den Namen des Snapshot ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.
-overrideLock	Setzen Sie die Einschränkung außer Kraft, die das Löschen eines Snapshot verhindert, der von einer Anwendung gesperrt ist. Der Versuch, einen gesperrten Snapshot zu löschen, ohne dass diese Option aktiviert wurde, erzeugt eine Fehlermeldung mit den Details der Anwendung, die den Snapshot gesperrt hat. i ANMERKUNG: Verwenden Sie diese Option nicht, wenn Anwendungen derzeit auf den Snapshot verweisen, um Auswirkungen auf die Leistung dieser Anwendungen zu vermeiden. Diese Option wird nicht alle Einschränkungen umgehen, nur die Sperre, die bestimmte Anwendungen möglicherweise in Bezug auf den Snapshot haben.
-force	Entfernt den Snapshot am Zielstandort bedingungslos, auch wenn er von der synchronen Replikationssitzung als repliziert markiert wird. i ANMERKUNG: Diese Option ist nur für Snapshots an synchronen Zielstandorten anwendbar.

Beispiel

Mit dem folgenden Befehl wird der Snapshot SNAP_1 gelöscht:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/snap -id SNAP_1 delete
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
Operation completed successfully.
```

Kopieren von Snapshots

Kopieren eines Snapshot.

Format

```
/prot/snap { -id <value> | -name <value> } copy [-async] [-copyName <value>]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des Snapshot ein, auf dessen Zustand Sie die zugehörige Speicherressource wiederherstellen möchten.
-name	Geben Sie den Namen des Snapshot ein, auf dessen Zustand Sie die zugehörigen Speicherressourcen wiederherstellen möchten.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.
-copyName	Geben Sie den Namen der Kopie ein, die das System vor dem Anhängen des ausgewählten Snapshot erstellt. Wird dieser Switch festgelegt und kein Name angegeben, weist das System der Kopie einen Namen zu.  ANMERKUNG: Ist dieser Switch nicht festgelegt, wird keine Kopie erstellt.

Beispiel

Mit dem folgenden Befehl wird eine Kopie von SNAP_1 namens „SNAP_Copy“ erstellt:

- Name: accounting

Dem Snapshot wird die ID SNAP_1 zugewiesen:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/snap -id SNAP_1 copy -copyName SNAP_Copy
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = SNAP_1
Operation completed successfully.
```

Ändern von Snapshots

Ändern Sie die Einstellungen eines Snapshot.

Format

```
/prot/snap {-id <value> | -name <value>} set [-async] [-newName <value>] [-descr <value>]
[[-keepFor <value> | -allowAutoDelete {yes | no}]] [[-roHosts <value> -rwHosts <value>] [-
addRoHosts <value>] [-addRwHosts <value>] [-removeHosts <value>]] [-force]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des Snapshot ein, auf dessen Zustand Sie die zugehörige Speicherressource wiederherstellen möchten.
-name	Geben Sie den Namen des Snapshot ein, auf dessen Zustand Sie die zugehörigen Speicherressourcen wiederherstellen möchten.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.
-newName	Geben Sie einen neuen Namen für den Snapshot ein.
-descr	Geben Sie eine Beschreibung für den Snapshot ein.
-keepFor	Geben Sie ein, wie lange ein Snapshot aufbewahrt werden soll. Das Intervall kann in Tagen oder Stunden definiert werden. Vom System werden abgelaufene Snapshots automatisch gelöscht. Das Format lautet wie folgt:

Qualifizierer	Beschreibung
	<p><value><qualifier></p> <p>Dabei gilt Folgendes:</p> <ul style="list-style-type: none"> • <value>: Geben Sie die Zahl der Stunden bzw. Tage ein: <ul style="list-style-type: none"> ○ Bei Stunden können Zahlen im Bereich von 1 bis 8.760 eingegeben werden. ○ Bei Tagen können Zahlen im Bereich von 1 bis 365 eingegeben werden. • <qualifier>: Geben Sie den Qualifizierer für den Wert ein. Folgende Werte sind möglich: <ul style="list-style-type: none"> ○ h: Gibt die Stunden an. ○ d: Gibt die Tage an. <p>i ANMERKUNG: Bei geplanten Snapshots, die mit einem Plan verknüpft sind, wird über den Qualifizierer <code>-keepFor</code> in den Planregeln die Aufbewahrungsfrist festgelegt. Managen von Aufgabenregeln bietet Einzelheiten zu Planregeln.</p>
<code>-allowAutoDelete</code>	<p>Geben Sie an, ob das System automatisch den Snapshot oder Snapshot-Satz löschen kann. Gültige Werte:</p> <ul style="list-style-type: none"> • yes • no
<code>-roHosts</code>	<p>Gibt eine kommasetrennte Liste von Hosts mit schreibgeschütztem Zugriff auf den Snapshot an. Diese Option gilt nur, wenn der Snapshot an einen dynamischen Mount-Punkt für Snapshot angebunden ist. Mit diesem Qualifizierer werden die vorhandenen schreibgeschützten Hosts überschrieben.</p>
<code>-rwHosts</code>	<p>Gibt eine kommasetrennte Liste von Hosts mit Schreibzugriff auf den Snapshot an. Diese Option gilt nur, wenn der Snapshot an einen dynamischen Mount-Punkt für Snapshot angebunden ist. Mit diesem Qualifizierer werden die vorhandenen Hosts mit Schreibzugriff überschrieben.</p>
<code>-force</code>	<p>Modifiziert den Snapshot am Zielstandort bedingungslos, auch wenn er von der synchronen Replikationssitzung als repliziert markiert wird.</p> <p>i ANMERKUNG: Diese Option ist nur für Snapshots an synchronen Zielstandorten anwendbar.</p>
<code>-addRoHosts</code>	<p>Gibt eine kommasetrennte Liste von Hosts mit schreibgeschütztem Zugriff auf den Snapshot an. Mit dieser Option können Sie inkrementell Hosts mit schreibgeschütztem Zugriff hinzufügen. Die vorhandenen schreibgeschützten Hosts werden dabei nicht überschrieben.</p>
<code>-addRwHosts</code>	<p>Gibt eine kommasetrennte Liste von Hosts mit Schreibzugriff auf den Snapshot an. Mit dieser Option können Sie inkrementell Hosts mit Schreibzugriff hinzufügen. Die vorhandenen Hosts mit Schreibzugriff werden dabei nicht überschrieben.</p>
<code>-removeHosts</code>	<p>Gibt eine kommasetrennte Liste von Hosts an, deren Snapshot-Zugriff Sie entfernen möchten.</p>

Beispiel 1

Mit dem folgenden Befehl wird der Name des Snapshot SNAP_1 in MySnap geändert:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/snap -id SNAP_1 set -newName MySnap
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = SNAP_1
Operation completed successfully.
```

Beispiel 2

Im folgenden Beispiel wird Host_6 Schreibzugriff auf Snapshot 38654705670 zugewiesen, Host_5 schreibgeschützten Zugriff auf Snapshot 38654705670 und der Zugriff von Host_1 auf den Snapshot wird entfernt:

```
uemcli /prot/snap -id 38654705670 set -addRwHosts Host_6 -addRoHosts Host_5 -removeHosts Host_1
```

```
Operation completed successfully.
```

Managen von Snapshot-NFS-Shares

In der folgenden Tabelle werden die Attribute des Snapshot-NFS-Share aufgeführt:

Tabelle 128. Attribute des Snapshot-NFS-Share

Attribut	Beschreibung
ID	ID der Snapshot-NFS-Freigabe
Name	Name des Snapshot-NFS-Share.
Description	Beschreibung der Snapshot-NFS-Freigabe
Snapshot	Übergeordneter Snapshot (siehe Management von Snapshots).
Local path	Zu exportierender lokaler Pfad
Export path	Exportpfad zur Freigabe
Default access	Gibt die Standardzugriffsebene an. Gültige Werte: <ul style="list-style-type: none"> • ro: Nur Lesezugriff • rw: Schreibzugriff • roroot: Schreibgeschützter Root-Zugriff • root: Root-Zugriff • na: Kein Zugriff
Advanced host mgmt	Gibt an, ob die in den Hostlisten aufgeführten Hosts mithilfe der /remote/host-Objekte definiert werden, z. B. mit ihrer Kennung. Folgende Werte sind gültig (keine Unterscheidung zwischen Groß- und Kleinschreibung): <ul style="list-style-type: none"> • yes (Standard) • no
Read-only hosts	Durch Kommas getrennte Liste von Hostkennungen mit Leseberechtigung
Read/write hosts	Durch Kommas getrennte Liste von Hostkennungen mit Schreib- und Leseberechtigung
Root hosts	Durch Kommas getrennte Liste von Hostkennungen mit Root-Berechtigung
No access hosts	Durch Kommas getrennte Liste von Hostkennungen ohne Zugriffsberechtigung
Creation time	Der Zeitpunkt der Erstellung der Freigabe
Last modified time	Der Zeitpunkt der letzten Änderung der Freigabe
Role	Rolle des Snapshot-NFS-Share Gültige Werte: <ul style="list-style-type: none"> • backup: Gibt an, dass die Snapshot-Share in einer Backuprolle ausgeführt wird. Gilt für Snapshot Shares, die zum Zweck von Backup und Disaster Recovery auf einem NAS-Server erstellt wurden, der in einem Replikationszielmodus ausgeführt wird. <p>ANMERKUNG: Wenn ein NAS-Server ein Failover durchführt und zum Quellsystem in einer Replikation wird, gibt die Rolle von Snapshot Shares auf dem NAS-Server immer noch die Backuprolle wieder.</p> • production: Gibt an, dass die Snapshot-Share in einer Produktionsrolle ausgeführt wird. Auf NAS-Servern, die nicht als Replikationsziel fungieren, werden alle Snapshot Shares in einem Produktionsmodus betrieben.
Minimum security	Die minimale Sicherheitsoption, die von einem Client für den NFS-Mount-Vorgang bereitgestellt werden muss. Gültige Werte sind (von am wenigsten sicher bis am sichersten): <ul style="list-style-type: none"> • sys: Auch bekannt als AUTH_SYS-Sicherheit Dies zeigt an, dass keine serverseitige Authentifizierung vorhanden ist. Wenn sicheres NFS auf einem NAS-Server nicht konfiguriert ist, ist dies der Standardwert. • krb5: Kerberos V5-Authentifizierung. Dies ist der Standardwert, wenn sicheres NFS auf dem NAS-Server konfiguriert ist. • krb5i: Kerberos V5-Authentifizierung und Integrität • krb5p: Kerberos V5-Authentifizierung und Integrität, Verschlüsselung ist aktiviert

ANMERKUNG: `Read-only hosts` Die Attribute `Read/write hosts`, `Root hosts` und `No access hosts` werden als eine durch Komma getrennte Liste von Paaren von Hostkennungen und Tokens angezeigt, die in eckigen Klammern stehen. Das Token-Format hängt vom Hosttyp ab:

- `host`: kommagetrennte Liste von IP-Adressen
- `subnet`: durch Schrägstrich getrenntes Paar von IP-Adresse und Netzmaske
- `netgroup`: Netzwerkadresse der Netzwerkgruppe

Erstellen von NFS-Snapshots

Erstellen Sie eine Snapshot-NFS-Freigabe.

Format

```
/prot/snap/nfs create [-async] -name <value> [-descr <value>] -snap <value> -path <value> [-advHostMgmtEnabled {yes | no}] [-defAccess {ro | rw | roroot | root | na}] [-roHosts <value>] [-rwHosts <value>] [-roRootHosts <value>] [-rootHosts <value>] [-naHosts <value>] [-minSecurity {sys | krb5 | krb5i | krb5p}]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
<code>-async</code>	Führen Sie den Vorgang im asynchronen Modus aus.
<code>-name</code>	Geben Sie den Benutzernamen der Freigabe ein.
<code>-descr</code>	Geben Sie die Beschreibung der Freigabe ein.
<code>-snap</code>	Geben Sie den Snapshot ein, dem die Share zugeordnet werden soll.
<code>-path</code>	Geben Sie den Pfad ein, unter dem das Dateisystem gemountet werden soll. Der Standardwert ist <code>/</code> .
<code>-defAccess</code>	Gibt den Standardzugriffs-Level der Freigabe an. Gültige Werte: <ul style="list-style-type: none"> • <code>ro</code>: Nur Lesezugriff • <code>rw</code>: Schreibzugriff • <code>roroot</code>: Schreibgeschützter Root-Zugriff • <code>root</code>: Root-Zugriff • <code>na</code>: Kein Zugriff (Standardeinstellung)
<code>-advHostMgmtEnabled</code>	Gibt an, ob die in den Hostlisten aufgeführten Hosts mithilfe der <code>/remote/host</code> -Objekte definiert werden, z. B. mit ihrer Kennung (erweitertes Hostmanagement). Folgende Werte sind gültig (keine Unterscheidung zwischen Groß- und Kleinschreibung): <ul style="list-style-type: none"> • <code>yes</code> • <code>no</code>
<code>-roHosts</code>	Gibt die durch Kommas getrennte Liste von Hostkennungen mit Leseberechtigung an. Optional können damit die Host-IP-Adressen des Typs „Host“ ausgewählt werden. Sie werden definiert als eine durch Kommas getrennte Liste von IP-Adressen in eckigen Klammern und folgen der Hostkennung.
<code>-rwHosts</code>	Gibt die durch Kommas getrennte Liste von Hostkennungen mit Schreib- und Leseberechtigung an. Optional können damit die Host-IP-Adressen des Typs „Host“ ausgewählt werden. Sie werden definiert als eine durch Kommas getrennte Liste von IP-Adressen in eckigen Klammern und folgen der Hostkennung.
<code>-roRootHosts</code>	Gibt die kommagetrennte Liste von Hostkennungen mit schreibgeschützter Root-Berechtigung an.
<code>-rootHosts</code>	Gibt die durch Kommas getrennte Liste von Hostkennungen mit Root-Berechtigung an. Optional können damit die Host-IP-Adressen des Typs „Host“ ausgewählt werden. Sie werden definiert als eine durch Kommas getrennte Liste von IP-Adressen in eckigen Klammern und folgen der Hostkennung.

Qualifizierer	Beschreibung
-naHosts	Gibt die durch Kommas getrennte Liste von Hostkennungen ohne Zugriffsberechtigung an. Optional können damit die Host-IP-Adressen des Typs „Host“ ausgewählt werden. Sie werden definiert als eine durch Kommas getrennte Liste von IP-Adressen in eckigen Klammern und folgen der Hostkennung.
-minSecurity	Gibt die minimale Sicherheitsoption an, die von einem Client für den NFS-Mount-Vorgang bereitgestellt werden muss. Gültige Werte sind (von am wenigsten sicher bis am sichersten): <ul style="list-style-type: none"> • <code>sys</code>: Auch bekannt als AUTH_SYS-Sicherheit. Dies zeigt an, dass keine serverseitige Authentifizierung vorhanden ist. Wenn sicheres NFS auf einem NAS-Server nicht konfiguriert ist, ist dies der Standardwert. • <code>krb5</code>: Kerberos V5-Authentifizierung. Dies ist der Standardwert, wenn sicheres NFS auf dem NAS-Server konfiguriert ist. • <code>krb5i</code>: Kerberos V5-Authentifizierung und Integrität • <code>krb5p</code>: Kerberos V5-Authentifizierung und Integrität, Verschlüsselung ist aktiviert

Beispiel

Mit dem folgenden Befehl wird ein Snapshot eines Dateisystems mit den folgenden Einstellungen erstellt:

- Name: NFSshare
- Beschreibung: My Share
- Snapshot-ID lautet SNAP_1.
- Pfad ist /.
- Hosts mit Lesezugriff sind Host_1 und Host_2.
- Host mit Einstellung Lesen/Schreiben ist Host_3.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/snap/nfs create -name NFSshare
-descr "My share" -snap SNAP_1 -path / -roHosts "Host_1,Host_2" -rwHosts "Host_3" -defAccess na
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = NFS_1
Operation completed successfully.
```

Anzeigen von Snapshot-NFS-Freigaben

Führt die vorhandenen Snapshot-NFS-Shares auf.

Format

```
/prot/snap/nfs [{"-id <value> | -name <value> | -snap <value> | -snapName <value>}] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Die ID des NFS-Share.
-name	Der Name des NFS-Share.
-snap	Die ID des übergeordneten Snapshot. Die Liste von Shares, die mit dem angegebenen Snapshot verbunden sind, wird angezeigt.
-snapName	Der Name des übergeordneten Snapshot. Die Liste von Shares, die mit dem angegebenen Snapshot verbunden sind, wird angezeigt.

Beispiel

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/snap/nfs show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:   ID                = nfs_2
     Name              = Share_2012-08-24 16:05_00
     Description       =
     Snapshot          = app_1_sg_1
     Local path        = /fs_1_wckpapp/group.app_1_sg_1.fs.fs_1_wckp
     Export path       = 10.0.0.1:/Share_2012-08-24 16:05_00
     Default access    = na
     Advanced host mgmt. = yes
     No access hosts   =
     Read-only hosts   = Host_1, Host_2
     Read/write hosts  = Host_3
     Read-only Root hosts =
     Root hosts        =
     Creation time     = 2012-08-24 12:18:22
     Last modified time = 2012-08-24 12:18:22
     Role              = production
     Minimum security  = krb5
```

Einrichten von Snapshot-NFS-Freigaben

Verändert eine vorhandene Snapshot-NFS-Freigabe.

Format

```
/prot/snap/nfs {-id <value> | -name <value>} set [-async] [-descr <value>] [-defAccess { ro | rw | roroot | root | na }] [-advHostMgmtEnabled { yes | no }] [{"[-roHosts <value>] [-rwHosts <value>] [-roRootHosts <value>] [-rootHosts <value>] [-naHosts <value>] [-addRoHosts <value>] [-addRwHosts <value>] [-addRoRootHosts <value>] [-addRootHosts <value>] [-addNaHosts <value>] [-removeHosts <value>]]} [-minSecurity {sys | krb5 | krb5i | krb5p}]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	ID der Snapshot-NFS-Freigabe
-name	Name des Snapshot-NFS-Share.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.
-descr	Geben Sie die Beschreibung der Freigabe ein.
-defAccess	Gibt die neue Benutzerbeschreibung der Share an. Gültige Werte: <ul style="list-style-type: none">• ro: Nur Lesezugriff• rw: Schreibzugriff• roRoot: Schreibgeschützter Root-Zugriff• root: Root-Zugriff• na: Kein Zugriff

Qualifizierer	Beschreibung
-advHostMgmtEnabled	Gibt an, ob die in den Hostlisten aufgeführten Hosts mithilfe der /remote/host-Objekte und ihrer Kennung definiert werden (erweitertes Hostmanagement). Gültige Werte (keine Unterscheidung zwischen Groß- und Kleinschreibung): ja oder nein. Diese Einstellung kann nur aktualisiert werden, wenn die Liste der vier Hosts unten leer ist.
-roHosts	Gibt die kommasetrennte Liste von Kennungen der Hosts mit Leseberechtigung für die Snapshot-NFS-Freigabe an. Dadurch werden die vorhandenen schreibgeschützten Hosts überschrieben.
-rwHosts	Gibt die kommasetrennte Liste von Kennungen der Hosts mit Schreibberechtigung für die Snapshot-NFS-Freigabe an. Mit diesem Qualifizierer werden die vorhandenen Hosts mit Schreibzugriff überschrieben.
-roRootHosts	Gibt die kommasetrennte Liste von Kennungen der Hosts mit schreibgeschütztem Root-Zugriff auf die Snapshot-NFS-Freigabe an. Mit diesem Qualifizierer werden die vorhandenen schreibgeschützten Root-Hosts überschrieben.
-rootHosts	Gibt die kommasetrennte Liste von Kennungen der Hosts mit Root-Zugriff auf die Snapshot-NFS-Freigabe an. Mit diesem Qualifizierer werden die vorhandenen Root-Hosts überschrieben.
-naHosts	Gibt die kommasetrennte Liste von Kennungen der Hosts ohne Zugriff auf die Snapshot-NFS-Freigabe an. Mit diesem Qualifizierer werden die vorhandenen Hosts ohne Zugriffsberechtigung überschrieben.
-addRoHosts	Gibt die kommasetrennte Liste der hinzuzufügenden Hosts mit schreibgeschütztem Zugriff auf die Snapshot-NFS-Freigabe an. Mit dieser Option können Sie inkrementell Hosts mit schreibgeschütztem Zugriff auf die VMware NFS-Snapshot-Freigabe hinzufügen. Dadurch werden nicht alle vorhandenen schreibgeschützten Hosts überschrieben.
-addRwHosts	Gibt die kommasetrennte Liste der hinzuzufügenden Hosts mit Schreibzugriff auf die Snapshot-NFS-Freigabe an. Mit dieser Option können Sie inkrementell Hosts mit Schreibzugriff auf die Snapshot-NFS-Freigabe hinzufügen. Dadurch werden nicht alle vorhandenen Hosts mit Schreibzugriff überschrieben.
-addRoRootHosts	Gibt die kommasetrennte Liste der hinzuzufügenden Hosts mit schreibgeschütztem Root-Zugriff auf die Snapshot-NFS-Freigabe an. Mit dieser Option können Sie inkrementell Hosts mit schreibgeschütztem Root-Zugriff auf die Snapshot-NFS-Freigabe hinzufügen. Dadurch werden nicht alle vorhandenen schreibgeschützten Root-Hosts überschrieben.
-addRootHosts	Gibt die kommasetrennte Liste von Hosts an, die Schreib-Root-Zugriff auf die Snapshot-NFS-Freigabe erhalten. Mit dieser Option können Sie inkrementell Hosts mit Schreib-Root-Zugriff auf die Snapshot-NFS-Freigabe hinzufügen. Dadurch werden nicht alle vorhandenen Hosts mit Schreib-Root-Zugriff überschrieben.
-addNaHosts	Gibt die kommasetrennte Liste von Hosts ohne Zugriff auf die Snapshot-NFS-Freigabe an. Mit dieser Option können Sie inkrementell Hosts angeben, die keinen Zugriff auf die Snapshot-NFS-Freigabe haben. Dadurch werden nicht alle vorhandenen Hosts ohne Zugriffsberechtigung überschrieben.
-removeHosts	Gibt die kommasetrennte Liste von Hosts an, für die der Zugriff auf die Snapshot-NFS-Freigabe entfernt wird. Mit dieser Option können Sie den Hostzugriff auf die Snapshot-NFS-Freigabe inkrementell entfernen.
-minSecurity	Gibt die minimale Sicherheitsoption an, die von einem Client für den NFS-Mount-Vorgang bereitgestellt werden muss. Gültige Werte sind (von am wenigsten sicher bis am sichersten): <ul style="list-style-type: none"> • <code>sys</code>: Auch bekannt als AUTH_SYS-Sicherheit. Dies zeigt an, dass keine serverseitige Authentifizierung vorhanden ist. Wenn sicheres NFS auf einem NAS-Server nicht konfiguriert ist, ist dies der Standardwert. • <code>krb5</code>: Kerberos V5-Authentifizierung. Dies ist der Standardwert, wenn sicheres NFS auf dem NAS-Server konfiguriert ist. • <code>krb5i</code>: Kerberos V5-Authentifizierung und Integrität • <code>krb5p</code>: Kerberos V5-Authentifizierung und Integrität, Verschlüsselung ist aktiviert

Beispiel 1

Das folgende Beispiel fügt eine Beschreibung von Snapshot NFS_1 hinzu.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/snap/nfs -id NFS_1 set -descr "My share"
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection
```

```
ID = NFS_1  
Operation completed successfully.
```

Beispiel 2

Im folgenden Beispiel wird Host_2 mit schreibgeschütztem Root-Zugriff hinzugefügt, Host_3 wird mit Schreib-Root-Zugriff hinzugefügt und Host_1 wird der Zugriff auf NFSShare_1 entzogen.

```
uemcli /prot/snap/nfs -id NFSShare_1 set -addRoHosts Host_2 -addRoRootHosts Host_3 -removeHosts Host_1
```

```
D = NFSShare_1  
Operation completed successfully.
```

Löschen von Snapshot-NFS-Shares

Löschen Sie einen Snapshot-NFS-Share.

 **ANMERKUNG:** Nach dem Löschen eines Snapshot-Share ist es nicht mehr möglich, Daten daraus oder eine Speicherressource darauf wiederherzustellen.

Format

```
/prot/snap/nfs {-id <value> | -name <value>} delete [-async]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des zu löschenden Snapshots ein.
-name	Geben Sie den Namen des zu löschenden Snapshot ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.

Beispiel

Mit dem folgenden Befehl wird der Snapshot nfs_1 gelöscht:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/snap/nfs -id nfs_1 delete
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection
```

```
Operation completed successfully.
```

Managen von Snapshot-CIFS-Freigaben

In der folgenden Tabelle sind die Attribute für Snapshot-CIFS (SMB)-Freigaben aufgeführt:

Tabelle 129. Attribute der Snapshot-CIFS-Freigaben

Attribut	Beschreibung
ID	ID der Snapshot-CIFS-Freigabe.
Name	Name der Snapshot-CIFS-Freigabe.
Description	Beschreibung der Snapshot-CIFS-Freigabe.
Snapshot	Übergeordneter Snapshot (siehe Management von Snapshots.)
Local path	Zu exportierender lokaler Pfad
Export path	Exportpfad zur Freigabe
Creation time	Der Zeitpunkt der Erstellung der Freigabe
Last modified time	Der Zeitpunkt der letzten Änderung der Freigabe
Availability enabled	Kontinuierlicher Verfügbarkeitsstatus.
Encryption enabled	CIFS-Verschlüsselungsstatus.
Umask	Gibt die Standard-Unix-Umask für neue Dateien an, die auf der Freigabe erstellt werden. Wenn nicht angegeben, wird die Umask standardmäßig auf 022 festgelegt.
ABE enabled	Gibt an, ob ein ABE-Filter (Access-Based Enumeration) aktiviert ist. Folgende Werte sind möglich: <ul style="list-style-type: none"> • <code>yes</code>: Filtert die Liste der verfügbaren Dateien und Ordner auf der Freigabe, sodass nur diejenigen angezeigt werden, auf die der anfragende Benutzer Zugriff hat. • <code>no</code>(Standard)
DFS enabled	Gibt an, ob DFS (Distributed File System) aktiviert ist. Folgende Werte sind möglich: <ul style="list-style-type: none"> • <code>yes</code>: Hiermit können Administratoren freigegebene Ordner gruppieren, die sich auf verschiedenen Freigaben befinden, indem sie sie transparent mit einem oder mehreren DFS-Namespaces verbinden. • <code>no</code>
BranchCache enabled	Gibt an, ob BranchCache aktiviert ist. Folgende Werte sind möglich: <ul style="list-style-type: none"> • <code>yes</code>: Kopiert Inhalte von den Contentservern im Hauptgebäude oder der gehosteten Cloud und legt die Inhalte in Zwischenspeichern in Zweigstellen ab. Dadurch können Clientcomputer in Zweigstellen lokal auf Inhalte zugreifen anstatt über das WAN. • <code>no</code>(Standard)
Offline availability	Gibt an, ob Offlineverfügbarkeit aktiviert ist. Wenn diese Option aktiviert ist, können Benutzer mithilfe dieser Funktion auf ihren Computern mit freigegebenen Ordnern arbeiten, die auf einem Server gespeichert sind, auch wenn sie nicht mit dem Netzwerk verbunden sind. Folgende Werte sind möglich: <ul style="list-style-type: none"> • <code>none</code>: Verhindert, dass Clients Dokumente und Programme im Offline-Cache speichern (Standard) • <code>documents</code>: Alle Dateien, die Clients öffnen, sind offline verfügbar. • <code>programs</code>: Alle Programme und Dateien, die Clients öffnen, sind offline verfügbar. Programme und Dateien werden

Tabelle 129. Attribute der Snapshot-CIFS-Freigaben (fortgesetzt)

Attribut	Beschreibung
	<p>vorzugsweise aus dem Offline-Cache geöffnet, auch wenn eine Verbindung zum Netzwerk besteht.</p> <ul style="list-style-type: none"> • <code>manual</code>: Nur bestimmte Dateien sind offline verfügbar.

Erstellen eines CIFS-Snapshot

Erstellen Sie eine Snapshot-CIFS (SMB)-Freigabe.

Format

```
/prot/snap/cifs create [-async] -name <value> [-descr <value>] -snap <value> -path <value> [-enableContinuousAvailability {yes | no} ] [-enableCIFSEncryption {yes | no} ] [-umask <value> ] [-enableABE {yes | no} ] [-enableBranchCache {yes | no} ] [-offlineAvailability {none | documents | programs | manual} ]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
<code>-async</code>	Führen Sie den Vorgang im asynchronen Modus aus.
<code>-name</code>	Geben Sie den Benutzernamen der Freigabe ein.
<code>-descr</code>	Geben Sie die Beschreibung der Freigabe ein.
<code>-snap</code>	Geben Sie den Snapshot ein, dem die Share zugeordnet werden soll.
<code>-path</code>	Geben Sie den Pfad ein, auf dem das Dateisystem gemountet werden soll.
<code>-enableContinuousAvailability</code>	Geben Sie an, ob die kontinuierliche Verfügbarkeit aktiviert ist.
<code>-enableCIFSEncryption</code>	Geben Sie an, ob die CIFS-Verschlüsselung aktiviert ist.
<code>-umask</code>	Geben Sie die Standard-Unix-Umask für neue Dateien ein, die auf der Freigabe erstellt werden.
<code>-enableABE</code>	Geben Sie an, ob Access-Based Enumeration aktiviert ist. Gültige Werte: <ul style="list-style-type: none"> • <code>yes</code> • <code>no</code> (Standard)
<code>-enableBranchCache</code>	Geben Sie an, wenn <code>BranchCache</code> aktiviert ist. Gültige Werte: <ul style="list-style-type: none"> • <code>yes</code> • <code>no</code> (Standard)
<code>-offlineAvailability</code>	Geben Sie die Art der Offline-Verfügbarkeit an. Gültige Werte: <ul style="list-style-type: none"> • <code>none</code> (Standard): Verhindert, dass Clients Dokumente und Programme im Offline-Cache speichern. • <code>documents</code> : Erlaubt, dass alle Dateien, die Clients öffnen, offline verfügbar sind. • <code>programs</code> : Erlaubt, dass alle Programme und Dateien, die Clients öffnen, offline verfügbar sind. Programme und Dateien werden aus dem Offline-Cache geöffnet, auch wenn eine Verbindung zum Netzwerk besteht. • <code>manual</code> : Erlaubt nur bestimmten Dateien, offline verfügbar zu sein.

Beispiel

Mit dem folgenden Befehl wird ein Snapshot eines Dateisystems mit den folgenden Einstellungen erstellt:

- Name: CIFSshare

- Beschreibung: My Share
- Snapshot ist „cifssnap1“
- Pfad ist /.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/snap/cifs create -name CIFSshare
-descr "My share" -path /
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = cifs_1
Operation completed successfully.
```

Anzeigen von Snapshot-CIFS-Freigaben

Führt die vorhandenen Snapshot-CIFS (SMB)-Freigaben auf.

Format

```
/prot/snap/cifs [{-id <value> | -name <value> | -snap <value> | -snapName <value>}] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Die ID des CIFS-Share.
-name	Der Name des CIFS-Share.
-snap	Die ID des übergeordneten Snapshot. Die Liste von Shares, die mit dem angegebenen Snapshot verbunden sind, wird angezeigt.
-snapName	Der Name des übergeordneten Snapshot. Die Liste von Shares, die mit dem angegebenen Snapshot verbunden sind, wird angezeigt.

Beispiel

```
uemcli /prot/snap/cifs show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
1:  ID                = cifs_2
    Name              = Share_2012-08-24 16:05_00
    Description       =
    Snapshot          = app_1_sg_1
    Local path        = /group.app_1_sg_1.fs.fs_1_wckp
    Export path       = 10.64.76.120:/Share_2012-08-24 16:05_00
    Default access    = na
    No access hosts   =
    Read-only hosts   = 1014[10.192.168.5,10.192.168.6], 1015[10.192.168.9]
    Read/write hosts  = 1016[10.244.245.0/255.255.255.0]
    Root hosts        =
    Creation time     = 2012-08-24 12:18:22
    Last modified time = 2012-08-24 12:18:22
```

Einrichten von Snapshot-CIFS-Shares

Verändert eine vorhandene Snapshot-CIFS (SMB)-Freigabe.

Format

```
/prot/snap/cifs {-id <value> | -name <value>} set [-async] [-descr <value>] [-enableContinuousAvailability {yes | no} ] [-enableCIFSEncryption {yes | no} ] [-umask <value> ] [-enableABE {yes | no} ] [-enableBranchCache {yes | no}] [-offlineAvailability {none | documents | programs | manual}] [-defAccess { na | rw }] [-naHosts <value>] [-rwHosts <value>]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	ID der Snapshot-CIFS-Freigabe.
-name	Name der Snapshot-CIFS-Freigabe.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.
-desc	Gibt die neue Benutzerbeschreibung der Share an.
-enableContinuousAvailability	Geben Sie an, ob die kontinuierliche Verfügbarkeit aktiviert ist.
-enableCIFSEncryption	Geben Sie an, ob die CIFS-Verschlüsselung aktiviert ist.
-umask	Geben Sie die Standard-UNIX-Umask für neue Dateien ein, die auf der Freigabe erstellt werden.
-enableABE	Geben Sie an, ob Access-Based Enumeration (ABE) aktiviert ist. Gültige Werte: <ul style="list-style-type: none"> • yes • no
-enableBranchCache	Geben Sie an, ob BranchCache aktiviert ist. Gültige Werte: <ul style="list-style-type: none"> • yes • no
-offlineAvailability	Geben Sie die Art der Offline-Verfügbarkeit an. Gültige Werte: <ul style="list-style-type: none"> • none: Verhindert, dass Clients Dokumente und Programme in einem Offline-Cache speichern. • documents: Erlaubt, dass alle Dateien, die Clients öffnen, offline verfügbar sind. • programs: Erlaubt, dass alle Programme und Dateien, die Clients öffnen, offline verfügbar sind. Programme und Dateien werden aus dem Offline-Cache geöffnet, auch wenn eine Verbindung zum Netzwerk besteht. • manual: Erlaubt nur bestimmten Dateien, offline verfügbar zu sein.
-defAccess	Gibt die Standardzugriffsebene an. Gültige Werte sind folgende (keine Unterscheidung zwischen Groß- und Kleinschreibung): <ul style="list-style-type: none"> • rw • na
-rwHosts	Gibt die kommagetrennte Liste von Kennungen der Hosts mit Schreibberechtigung an. Mit dieser Option werden die vorhandenen Hosts mit Schreibzugriff überschrieben.
-naHosts	Gibt die durch Kommas getrennte Liste von Hostkennungen ohne Zugriffsberechtigung an. Mit dieser Option werden die vorhandenen Hosts ohne Zugriffsberechtigung überschrieben.

Beispiel

```
uemcli /prot/snap/cifs -id cifs_1 set -descr "My share"
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection
```

```
ID = cifs_1  
Operation completed successfully.
```

Löschen von Snapshot-CIFS-Freigaben

Löschen (zerstören) Sie eine Snapshot-CIFS (SMB)-Freigabe.

ANMERKUNG: Nach dem Löschen einer Snapshot-Freigabe ist es nicht mehr möglich, Daten daraus oder eine Speicherressource darauf wiederherzustellen.

Format

```
/prot/snap/cifs {-id <value> | -name <value>} delete [-async]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des zu löschenden Snapshots ein.
-name	Geben Sie den Namen des zu löschenden Snapshot ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.

Beispiel

Mit dem folgenden Befehl wird der Snapshot cif_1 gelöscht:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/snap/cifs -id smb_1 delete
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection
```

```
Operation completed successfully.
```

Managen von Replikationssitzungen

Bei der Speicherreplikation werden Speicherdaten entweder lokal oder auf einem Remotenetzwerkgerät repliziert. Bei der Replikation wird eine schreibgeschützte Point-in-Time-Kopie der Speicher-Quelldaten erstellt. Diese Kopie wird regelmäßig aktualisiert, um sie jeweils auf dem aktuellen Stand zu halten. Die Speicherreplikation bietet eine höhere Redundanz für den Fall, dass das Hauptbackupsystem des Speichers ausfällt. Dies bietet folgende Vorteile:

- Die mit einem Systemausfall verbundenen Kosten werden minimiert.
- Die Wiederherstellung nach einer Naturkatastrophe oder einem von Menschen verursachten Ausfall wird deutlich erleichtert.

Die einzelnen Replikationssitzungen verfügen über eigene IDs. In der Unisphere-Onlinehilfe finden Sie weitere Informationen zur Speicherreplikation.

Es ist wichtig zu beachten, dass bei der Replikation von einem Unity-System, auf dem eine neuere OE-Version ausgeführt wird (zum Beispiel OE 4.1.x), zu einem Unity-System, auf dem eine ältere OE-Version ausgeführt wird (zum Beispiel OE 4.0.x), keine Funktionen der neueren OE-Version auf der Quelle aktiviert sein können.

ANMERKUNG: Es wird immer nur ein Befehl in einer Replikationssitzung unterstützt. Bevor Sie einen neuen Befehl ausführen, warten Sie, bis die derzeitige Aktion in der Replikationssitzung beendet ist.

In der folgenden Tabelle sind die Attribute für Replikationssitzungen aufgeführt:

Tabelle 130. Attribute für Replikationssitzungen

Attribut	Beschreibung
ID	Die ID der Sitzung.
Name	Name der Replikationssitzung.
Session type	Der Speichertyp der Sitzung. Gültige Werte: <ul style="list-style-type: none"> • lun • block • file • nas server
Synchronization type	Art der Synchronisierung. Gültige Werte: <ul style="list-style-type: none"> • auto: Daten werden im Hinblick auf die Einhaltung des gewünschten Recovery Point Objective (RPO) automatisch repliziert. • manual: Die Daten werden nur bei manueller Initiierung repliziert. • sync: Die Daten werden mit RPO = 0 synchron repliziert. <p>ANMERKUNG: Bei asynchronen Replikationen steigt mit einem höheren RPO auch das Risiko eines potenziellen Datenverlusts und ebenso der erforderliche Schutzspeicherplatz. Durch Senken des RPO kann auch das Risiko des Datenverlusts gesenkt werden, aber gleichzeitig wird der Netzwerkverkehr zunehmen, was sich negativ auf die Performance auswirken kann. Das Standard-RPO liegt bei einer Stunde.</p>
RPO	Recovery Point Objective (RPO)-Intervall für die automatische Synchronisierung. Für die synchrone Replikation wird das RPO automatisch auf 0 festgelegt.
Resource type	Der Typ der Speicherressource, auf den die Replikationssitzung angewendet wird. Gültige Werte: <ul style="list-style-type: none"> • LUN • LUN group • File System • VMware VMFS • VMware NFS • NAS Server
Sync State	Zusätzlicher Status der Replikationssitzung, speziell für den Replikationsmodus. <ul style="list-style-type: none"> • Bei der asynchronen Replikation sind gültige Werte: <ul style="list-style-type: none"> ◦ idle: Kein aktives Synchronisieren. Ab OE 5.x können Sie die Attribute der Replikationssitzung ändern, während die Sitzung inaktiv ist. ◦ manual: Vom Nutzer initiierte Synchronisation. ◦ auto syncing: Vom System initiierte Synchronisierung. • Bei der synchronen Replikation sind gültige Werte: <ul style="list-style-type: none"> ◦ unknown: Unbekannter Synchronisierungsstatus. ◦ out of sync: Ziel ist nicht mit der Quelle synchronisiert. ◦ in sync: Das Ziel ist eine identische Kopie der Quelle. ◦ consistent: Das Ziel ist eine Point-in-Time-Kopie der Quelle. ◦ syncing: Vom System initiierte Synchronisierung. ◦ inconsistent: Das Ziel ist keine Point-in-Time-Kopie der Quelle.
Health state	Der Integritätsstatus der Sitzung. Gültige Werte:

Tabelle 130. Attribute für Replikationssitzungen (fortgesetzt)

Attribut	Beschreibung
	<ul style="list-style-type: none"> ● Unknown: Die Integrität der Sitzung ist nicht bestimmbar. ● OK: Die Sitzung funktioniert normal. ● Degraded/warning: Durch einen Fehler ist mindestens eines der folgenden Ereignisse eingetreten: <ul style="list-style-type: none"> ○ Die Sitzung wurde angehalten. ○ Es ist zu einem Sitzungs-Failover gekommen – wahrscheinlich, weil die Quell-Speicherressource nicht mehr verfügbar ist. Die Ziel-Speicherressource befindet sich nun im Zustand „Lesen/Schreiben“. Prüfen Sie den Status der Quelle, und prüfen Sie, ob es Probleme mit der Netzwerkverbindung gibt. Sobald die Sitzung wieder online ist, können Sie per Failback zum normalen Betrieb zurückkehren. ○ Die Sitzung wird synchronisiert. ● Minor failure: Die Kommunikation mit dem Replikationshost wurde unterbrochen. Das System ist wahrscheinlich heruntergefahren, oder es besteht ein Problem mit der Netzwerkverbindung zwischen den Systemen. Möglicherweise ist auch eine Änderung an der Netzwerkkonfiguration auf einer der beiden Seiten Ursache der Unterbrechung der Kommunikation. ● Critical failure: Bei der Sitzung ist ein Fehler aufgetreten, durch den die Sitzung angehalten wurde. <p>i ANMERKUNG: Wenn die Replikationssitzung fehlerhaft ist, versuchen Sie zusätzlich zum Lösen des Problems (z. B. kein Speicherplatz mehr im Zielpool), die Replikationssitzung anzuhalten und anschließend fortzusetzen. Falls das Problem weiterhin besteht, löschen Sie die Replikationssitzung und erstellen Sie sie dann erneut.</p>
Health details	Zusätzliche Integritätsinformationen.
Operational status	<p>Betriebsstatus der Sitzung. Der Code des Betriebsstatus wird in Klammern angegeben.</p> <ul style="list-style-type: none"> ● Unknown (0x0) ● Non Recoverable Error (0x7) ● Lost Communication (0xd) ● Failed Over with Sync (0x8400) ● Failed Over (0x8401) ● Manual Syncing (0x8402) ● Paused (0x8403) ● Idle (0x8404) ● Auto Sync Configured (0x8405) ● Destination Extend Failed Not Syncing (0x840B) ● Destination Extend In Progress (0x840C) ● Active (0x840D) ● Lost Sync Communication (0x840E) ● Syncing (0x8411)
Source status	<p>Der Status der Quell-Speicherressource in der Sitzung. Gültige Werte:</p> <ul style="list-style-type: none"> ● Unknown: Der Status der Quelle ist unbekannt. ● OK: Die Quelle funktioniert normal. ● Paused: Die Replikationssitzung für die Quelle ist zurzeit angehalten. ● Fatal replication issue: Die Quelle hat einen kritischen Fehler festgestellt, die Replikationssitzung wurde gestoppt. Löschen Sie die Replikationssitzung, und erstellen Sie sie erneut. ● Lost communication: Die Kommunikation mit dem Replikationshost wurde unterbrochen. Das System ist wahrscheinlich heruntergefahren, oder es besteht ein Problem mit der Netzwerkverbindung zwischen den Systemen. Möglicherweise ist auch eine Änderung an der Netzwerkkonfiguration auf einer der beiden Seiten Ursache der Unterbrechung der Kommunikation. ● Failed over: Bei der Replikationssitzung ist es zu einem Failover auf den Zielstandort gekommen. Im Failover-Status bestehen für das Zielobjekt Lese-/Schreibrechte. Wenn die Kommunikation zwischen Quelle und Ziel wieder möglich ist, wird für die Quelle „Restricted

Tabelle 130. Attribute für Replikationssitzungen (fortgesetzt)

Attribut	Beschreibung
	<p>Replication Access = Yes“ angezeigt. Damit die Vorgänge am Quellstandort fortgesetzt werden, muss ein Failback der Replikationssitzung stattfinden.</p> <ul style="list-style-type: none"> • Switched over: Die Replikationssitzung findet am Quellstandort statt. Hat ein solcher Switchover stattgefunden, bestehen für das Quellobjekt Lese-/Schreibrechte. Wenn die Kommunikation zwischen Quelle und Ziel wieder möglich ist, wird für das Ziel „Restricted Replication Access = Yes“ angezeigt. Damit die Vorgänge am Zielstandort fortgesetzt werden, muss ein Failover der Replikationssitzung stattfinden.
Destination status	<p>Der Status der Ziel-Speicherressource in der Sitzung. Gültige Werte:</p> <ul style="list-style-type: none"> • Unknown: Der Status der Zielressource ist unbekannt. • OK: Die Zielressource funktioniert normal. • Paused: Die Replikationssitzung für die Zielressource ist zurzeit angehalten. • Fatal replication issue: Das Ziel hat einen kritischen Fehler festgestellt, die Replikationssitzung wurde gestoppt. Löschen Sie die Replikationssitzung, und erstellen Sie sie erneut. • Lost communication: Die Kommunikation mit dem Replikationshost wurde unterbrochen. Das System ist wahrscheinlich heruntergefahren, oder es besteht ein Problem mit der Netzwerkverbindung zwischen den Systemen. Möglicherweise ist auch eine Änderung an der Netzwerkkonfiguration auf einer der beiden Seiten Ursache der Unterbrechung der Kommunikation. • Failed over: Bei der Replikationssitzung ist es zu einem Failover auf den Zielstandort gekommen. Im Failover-Status bestehen für das Zielobjekt Lese-/Schreibrechte. Wenn die Kommunikation zwischen Quelle und Ziel wieder möglich ist, wird für die Quelle „Restricted Replication Access = Yes“ angezeigt. Damit die Vorgänge am Quellstandort fortgesetzt werden, muss ein Failback der Replikationssitzung stattfinden. • Switched over: Die Replikationssitzung findet am Quellstandort statt. Hat ein solcher Switchover stattgefunden, bestehen für das Quellobjekt Lese-/Schreibrechte. Wenn die Kommunikation zwischen Quelle und Ziel wieder möglich ist, wird für das Ziel „Restricted Replication Access = Yes“ angezeigt. Damit die Vorgänge am Zielstandort fortgesetzt werden, muss ein Failover der Replikationssitzung stattfinden.
Network status	<p>Status der Netzwerkverbindung. Gültige Werte:</p> <ul style="list-style-type: none"> • Unknown: Der Netzwerkstatus ist zurzeit unbekannt. Wenn dieser Wert weiterhin angezeigt wird, prüfen Sie die Netzwerkverbindungen. • OK: Die Netzwerkverbindung funktioniert normal. • Lost Communication: Die Kommunikation mit dem Replikationshost wurde unterbrochen. Das System ist wahrscheinlich heruntergefahren oder es besteht ein Problem mit der Netzwerkverbindung zwischen den Systemen (verlorene IP-Pakete). Möglicherweise ist auch eine Änderung an der Netzwerkkonfiguration auf einer der beiden Seiten Ursache der Unterbrechung der Kommunikation. • Lost Sync Communication: Die Fibre-Channel-Kommunikation zum Remotesystem für die synchrone Replikation wurde unterbrochen. Wahrscheinlich sind bei der Fibre-Channel-Verbindung Probleme aufgetreten.
Destination type	<p>Die Art des in der Sitzung verwendeten Ziels. Gültige Werte:</p> <ul style="list-style-type: none"> • local: Es verbleibt eine vollständige Kopie der Speicherressource auf dem lokalen System. Gegenüber Snapshots hat dies den Vorteil, dass nicht nur Kopien der einzelnen Änderungen gespeichert werden. • remote: Es wird eine vollständige Kopie der Speicherressource auf einem Remotesystem gespeichert. Dafür müssen die Daten über das Netzwerk übertragen werden. Die Remotereplikation wird häufig verwendet, damit an einem Remotestandort eine Kopie verfügbar ist, falls am lokalen Ort die Daten aufgrund einer Naturkatastrophe oder aus ähnlichen Gründen verloren gehen.
Destination system	<p>Bei Remotesitzungen die ID des Remotesystems, auf dem die Daten repliziert werden.</p>
Local role	<p>Die lokale Systemrolle. Gültige Werte:</p> <ul style="list-style-type: none"> • Unknown: Der Status des lokalen Systems ist unbekannt. • Source: Die Ressource auf lokalem System wird auf das Remotesystem repliziert.

Tabelle 130. Attribute für Replikationssitzungen (fortgesetzt)

Attribut	Beschreibung
	<ul style="list-style-type: none"> • Destination: Die Ressource auf lokalem System ist das Replikationsziel der Ressource auf dem Remotesystem. • Loopback: Die an der Replikationssitzung beteiligten Ressourcen befinden sich auf demselben Speichersystem. • Local: Die an der Replikationssitzung beteiligten Ressourcen befinden sich auf verschiedenen Speicherprozessoren des lokalen Systems.
Source resource	ID der Quell-Speicherressource in der Sitzung. Hierbei kann es sich um eine lokale Quelle oder eine Remoteressource handeln.
Source SP A interface	ID der Schnittstelle auf dem SPA des Quellsystems für die Replikation.
Source SP B interface	ID der Schnittstelle auf dem SPB des Quellsystems für die Replikation.
Destination resource	ID der Speicherressource, auf der die Daten repliziert werden.
Destination SP A interface	ID der Schnittstelle auf dem SPA des Zielsystems für die Replikation.
Destination SP B interface	ID der Schnittstelle auf dem SPB des Zielsystems für die Replikation.
Time of last sync	Datum und Uhrzeit der letzten Replikationssynchronisierung.
Sync status	Der Prozentsatz, zu dem die Replikationssynchronisierung bereits abgeschlossen ist, sowie die noch verbleibende Zeit. <i>i</i> ANMERKUNG: Bei synchroner Replikation wird der Prozentsatz gemeldet, wenn die Replikation im Synchronisierungszustand ist.
Sync transfer rate	Synchronisationsübertragungsrate, wenn sich die Sitzung im Synchronisieren-Status befindet. Bei Multi-LUN-Anwendungen gibt es eine Liste mit durch Kommata getrennten Werten. <i>i</i> ANMERKUNG: Dieses Attribut gilt nur für asynchrone Replikationen.
Sync transfer size remaining	Verbleibende noch zu übertragende Größe während der Synchronisation. Bei Multi-LUN-Anwendungen gibt es eine Liste mit durch Kommata getrennten Werten. <i>i</i> ANMERKUNG: Dieses Attribut gilt nur für asynchrone Replikationen.
Previous transfer rate	Vorherige durchschnittliche Übertragungsrate für die Replikationssitzung <i>i</i> ANMERKUNG: Dieses Attribut gilt nur für asynchrone Replikationen.
Average transfer rate	Durchschnittliche Datenübertragungsrate für die Replikationssitzung. <i>i</i> ANMERKUNG: Dieses Attribut gilt nur für asynchrone Replikationen.
Element pairs	Für Consistency-Group- und VMware VMFS-Datenspeicherreplikationen sind dies die LUN-Elementpaare innerhalb der Replikation.
Hourly snapshot keep for	Zeitraum, für den replizierte stündliche Snapshots auf dem Ziel gehalten werden. Ausgabe kann Folgendes sein: <ul style="list-style-type: none"> • Leer, wenn geplante Snapshots nicht repliziert werden. • <code><Wert><Qualifizierer></code> – wenn eine Aufbewahrungsdauer angegeben wird, wobei gilt: <ul style="list-style-type: none"> ◦ Wert: ein ganzzahliger Wert. Wenn der Qualifizierer h (Stunden) ist, ist der zulässige Bereich von 1 bis 42840. Wenn der Qualifizierer d (Tage) ist, ist der zulässige Bereich von 1 bis 1785. ◦ Qualifizierer: ein Qualifizierer des Werts. Die gültigen Werte sind folgende: <ul style="list-style-type: none"> ▪ h (Stunden) ▪ d (Tage) • Forever: Wenn kein Wert für <code>-keepFor</code> angegeben ist und „allow auto-delete“ gelten soll. • Same as source: Die Aufbewahrungs-Policy für das Ziel soll mit der Aufbewahrungs-Policy für die Quelle identisch sein. <i>i</i> ANMERKUNG: Dieses Attribut gilt nur für asynchrone Replikationen.

Tabelle 130. Attribute für Replikationssitzungen (fortgesetzt)

Attribut	Beschreibung
Hourly snapshot allow auto-delete	<p>Gibt an, ob die „auto-delete“-Policy des Zielspeicherpools zulässt, dass die replizierten stündlichen Snapshots auf dem Ziel gelöscht werden. Ausgabe kann Folgendes sein:</p> <ul style="list-style-type: none"> • Leer, wenn geplante Snapshots nicht repliziert werden. • <code>same as source</code>: Die Aufbewahrungs-Policy für das Ziel soll mit der Aufbewahrungs-Policy für die Quelle identisch sein. • <code>yes</code>: Wenn <code>-allowAutoDelete</code> festgelegt ist. • <code>no</code>: Wenn <code>-keepFor</code> festgelegt ist. <p>ANMERKUNG: Dieses Attribut gilt nur für asynchrone Replikationen.</p>
Daily snapshot keep for	<p>Zeitraum, für den replizierte tägliche Snapshots auf dem Ziel gehalten werden. Ausgabe kann Folgendes sein:</p> <ul style="list-style-type: none"> • Leer, wenn geplante Snapshots nicht repliziert werden. • <i>Wert</i>: ein ganzzahliger Wert. Wenn der <i>Qualifizierer</i> <code>h</code> (Stunden) ist, ist der zulässige Bereich von 1 bis 42840. Wenn der <i>Qualifizierer</i> <code>d</code> (Tage) ist, ist der zulässige Bereich von 1 bis 1785. • <i>Qualifizierer</i>: ein Qualifizierer des Werts. Die gültigen Werte sind folgende: <ul style="list-style-type: none"> ◦ <code>h</code> (Stunden) ◦ <code>d</code> (Tage) • <code>same as source</code>: Die Aufbewahrungs-Policy für das Ziel soll mit der Aufbewahrungs-Policy für die Quelle identisch sein. <p>ANMERKUNG: Dieses Attribut gilt nur für asynchrone Replikationen.</p>
Daily snapshot allow auto-delete	<p>Gibt an, ob die „auto-delete“-Policy des Zielspeicherpools zulässt, dass die replizierten täglichen Snapshots auf dem Ziel gelöscht werden. Ausgabe kann Folgendes sein:</p> <ul style="list-style-type: none"> • Leer, wenn geplante Snapshots nicht repliziert werden. • <code>same as source</code>: Die Aufbewahrungs-Policy für das Ziel soll mit der Aufbewahrungs-Policy für die Quelle identisch sein. • <code>yes</code>: Wenn <code>-allowAutoDelete</code> festgelegt ist. • <code>no</code>: Wenn <code>-keepFor</code> festgelegt ist. <p>ANMERKUNG: Dieses Attribut gilt nur für asynchrone Replikationen.</p>
Allow Async Snap Replication (nur asynchrone Replikationssitzungen des Dateisystems)	<p>Gibt an, ob die Snapshot-Replikation in asynchronen Replikationssitzungen zugelassen werden soll oder nicht. Mögliche Werte sind:</p> <ul style="list-style-type: none"> • <code>yes</code>: Snapshot-Replikation in asynchronen Sitzungen zulassen. • <code>no</code>: Snapshot-Replikation in asynchronen Sitzungen nicht zulassen.
Cascade Replicated Snap	<p>Ob „Repl Cate Snap“ in der Kaskaden-Replikationssitzung ist oder nicht.</p> <ul style="list-style-type: none"> • <code>yes</code>: Wenn Snap aus der eingehenden Sitzung repliziert wird, wird es automatisch in dieser Replikationssitzung repliziert. • <code>no</code>: Wenn Snap aus der eingehenden Sitzung repliziert wird, wird es nicht automatisch in dieser Replikationssitzung repliziert. <p>ANMERKUNG: Dieser Qualifizierer wird nur für asynchrone Dateisystemreplikationen verwendet.</p>

Erstellen von Replikationssitzungen

Stellen Sie sicher, dass Sie die erforderlichen Konfigurationsaufgaben abgeschlossen haben, bevor Sie eine Replikationssitzung erstellen.

Bei der asynchronen Replikation können Sie vorhandene Snapshots und im Rahmen von Snapshot-Zeitplänen erstellte Snapshots replizieren.

Bei der synchronen Dateireplikation können Sie vorhandene Snapshots oder im Rahmen von Snapshot-Zeitplänen erstellte Snapshots replizieren.

ANMERKUNG: Snapshots, die erstellt und angehängt wurden, sowie Snapshots mit Lese-/Schreibzugriff (Share-Snapshots, im Gegensatz zu schreibgeschützten Prüfpunkt-Snapshots) sind nicht für die Replikation qualifiziert. Nur nicht angehängte (schreibgeschützte) Snapshots sind für die Replikation qualifiziert.

Es gelten folgende Bedingungen für die Snapshot-Replikation:

- Asynchrone Replikation: Sie können vorhandene Snapshots und im Rahmen von Snapshot-Zeitplänen erstellte Snapshots replizieren.
- Synchrone Dateireplikation: Sie können vorhandene Snapshots oder im Rahmen von Snapshot-Zeitplänen erstellte Snapshots nicht replizieren. Sie können diese Snapshots und von Snapshot-Zeitplänen erstellte Snapshots erst replizieren, nachdem Sie die synchrone Replikationssitzung eingerichtet haben und sie aktiv ist.

ANMERKUNG: Auf einem durch Replikation geschützten NAS-Server müssen Sie für jedes darauf vorhandene Dateisystem eine Replikationssitzung erstellen. Andernfalls gehen Konfigurationen in Bezug auf das Dateisystem, wie Shares und Exporte, nach einem Failover für die Replikationssitzung des NAS-Servers möglicherweise verloren.

Für eine Snapshot-Replikation von einem Quellsystem mit OE-Version 4.0, 4.1, 4.2, 4.3 oder 4.4 auf ein Zielsystem, auf dem OE-Version 5.x ausgeführt wird, muss zuerst ein Upgrade des Quellsystems auf OE-Version 4.5 durchgeführt werden. Ein Upgrade auf OE-Version 4.5 ist nicht erforderlich, wird jedoch empfohlen, wenn Sie eine LUN- oder Dateisystemreplikation von OE-Version 4.0, 4.1, 4.2, 4.3 oder 4.4 auf OE-Version 5.0 ohne Snapshot-Replikation durchführen möchten.

Voraussetzungen

Erledigen Sie vor der Erstellung einer Replikationssitzung die folgenden Konfigurationsaufgaben:

- Erstellen Sie die Speicherressource, die die Replikationsquelle bereitstellt.
- Erstellen Sie für die lokale Replikation ein Replikationsziel in einem lokalen -System.
- Erstellen Sie für die Remotereplikation eine Replikationsverbindung zu einem Remotesystem und erstellen Sie ein Replikationsziel in diesem Remotesystem.
- Erstellen Sie für asynchrone Replikation in einer Topologie mit gleichzeitig bestehender asynchroner und synchroner Replikation den NAS-Zielservers für die asynchrone Replikation so, dass die Attribute `-replDest` und `-backupOnly` auf **Ja** festgelegt sind. Diese Attribute müssen auf dem NAS-Zielservers für die asynchrone Replikation auf **Ja** festgelegt sein, wenn der NAS-Quellservers synchron repliziert wird. Andernfalls kann die asynchrone Replikationssitzung nicht erstellt werden.

Format

```
/prot/rep/session create [-async] -srcRes <value> [-srcSPAInterface <value>] [-srcSPBInterface <value>] -dstType {local | remote -dstSys <value>} -dstRes <value> [-dstSPAInterface <value>] [-dstSPBInterface <value>] [-name <value>] [-elementPairs <value>] -syncType {manual [-autoInitiate {yes | no}] | auto [-rpo <value>]} [-replicateHourlySnaps {yes [{-keepSameAsSource | -keepFor <value> | -allowAutoDelete}] | no}] [-replicateDailySnaps {yes [{-keepSameAsSource | -keepFor <value> | -allowAutoDelete}] | no}] [-replicateExistingSnaps [-allowAsyncSnapReplication {yes | no}] [enableUserSnapCommonBase {-autosearch | -srcCommonBaseSnap <value> -dstCommonBaseSnap <value> [-skipSnapSignatureCheck]}]]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
<code>-async</code>	Ausführen einer Aktion im asynchronen Modus
<code>-srcRes</code>	Geben Sie die ID der als Quelle zu verwendenden Speicherressource ein.
<code>-srcSPAInterface</code>	Geben Sie die ID der Schnittstelle ein, die auf dem SPA des Quellsystems für die Replikation verwendet wird. ANMERKUNG: Dieser Qualifizierer wird nur für asynchrone Replikationen auf Remotesystemen verwendet. Wenn der Qualifizierer nicht angegeben ist, wird die Schnittstelle vom System automatisch erkannt.
<code>-srcSPBInterface</code>	Geben Sie die ID der Schnittstelle auf dem SPB des Quellsystems für die Replikation ein.

Qualifizierer	Beschreibung
	<p>i ANMERKUNG: Dieser Qualifizierer wird nur für asynchrone Replikationen auf Remotesystemen verwendet. Wenn der Qualifizierer nicht angegeben ist, wird die Schnittstelle vom System automatisch erkannt.</p>
-dstType	<p>Geben Sie den Ziel-Typ an. Gültige Werte:</p> <ul style="list-style-type: none"> • local: Es verbleibt eine vollständige Kopie der Speicherressource auf dem lokalen System. Gegenüber Snapshots hat dies den Vorteil, dass nicht nur Kopien der einzelnen Änderungen gespeichert werden. • remote: Es wird eine vollständige Kopie der Speicherressource auf einem Remotesystem gespeichert. Dafür müssen die Daten über das Netzwerk übertragen werden. <p>Die Remotereplikation wird häufig verwendet, damit an einem Remotestandort eine Kopie verfügbar ist, falls am lokalen Ort die Daten aufgrund einer Naturkatastrophe oder aus ähnlichen Gründen verloren gehen.</p>
-dstSys	<p>Geben Sie zur Remotereplikation die ID des Zielsystems ein. Anzeigen von Einstellungen für Remotespeichersysteme erläutert, wie Sie die IDs der Remotesystemkonfiguration im lokalen System anzeigen.</p>
-dstRes	<p>Geben Sie die ID der Ziel-Speicherressource ein.</p>
-dstSPAInterface	<p>Geben Sie die ID der Schnittstelle auf dem SPA des Zielsystems für die Replikation ein.</p> <p>i ANMERKUNG: Dieser Qualifizierer wird nur für asynchrone Replikationen auf Remotesystemen verwendet. Wenn der Qualifizierer nicht angegeben ist, wird die Schnittstelle vom System automatisch erkannt.</p>
-dstSPBInterface	<p>Geben Sie die ID der Schnittstelle auf dem SPB des Zielsystems für die Replikation ein.</p> <p>i ANMERKUNG: Dieser Qualifizierer wird nur für asynchrone Replikationen auf Remotesystemen verwendet. Wenn der Qualifizierer nicht angegeben ist, wird die Schnittstelle vom System automatisch erkannt.</p>
-syncType	<p>Dieser Parameter gibt an, ob die erste Replikationssynchronisation (eine vollständige Synchronisation) automatisch durchgeführt werden soll. Das folgende Beispiel zeigt die Option manuell, die für die erste Replikationssynchronisation verwendet wird: <code>-syncType {manual [-autoInitiate {yes no}] auto [-rpo <value>]}</code></p> <p>Gültige Werte:</p> <ul style="list-style-type: none"> • manual: Die Daten werden bei manueller Initiierung repliziert. • -autoInitiate- Die Werte für -autoInitiate lauten wie folgt: <ul style="list-style-type: none"> ◦ yes aktiviert die automatische Synchronisation. ◦ no deaktiviert die automatische Synchronisation. • auto [-rpo <value>]: Daten werden im Hinblick auf die Einhaltung des gewünschten Recovery Point Objective (RPO) automatisch repliziert. <p>i ANMERKUNG: Dieser Qualifizierer wird nur für asynchrone Replikationen verwendet.</p> <p>Mit einem höheren RPO steigt auch das Risiko eines potenziellen Datenverlusts und der erforderliche Schutzspeicherplatz. Durch Senken des RPO wird das Risiko des Datenverlusts reduziert, aber gleichzeitig nimmt der Netzwerkverkehr zu, was sich negativ auf die Performance auswirken kann. Das Standard-RPO liegt bei einer Stunde.</p>
-autoInitiate	<p>Geben Sie an, ob die erste Replikationssynchronisierung automatisch durchgeführt wird. Gültige Werte:</p> <ul style="list-style-type: none"> • yes • no <p>i ANMERKUNG: Dieser Qualifizierer wird nur für asynchrone Replikationen verwendet.</p>
-rpo	<p>Geben Sie das Zeitintervall für die Synchronisation ein. Das Format lautet wie folgt:</p> <p><code><HH> [:MM]</code></p> <p>Dabei gilt Folgendes:</p>

Qualifizierer	Beschreibung
	<ul style="list-style-type: none"> • HH: Geben Sie die Zahl der Stunden ein. Der zulässige Bereich liegt zwischen 00 und 24 Stunden (1 Tag). • MM: Geben Sie die Zahl der Minuten in 5-Minuten-Schritten ein. Es können Werte im Bereich zwischen 05 und 55 eingegeben werden. <p>Für eine synchrone Replikation geben Sie den Wert 0 ein. Anschließend kann der Wert nicht von Null auf ungleich Null oder von ungleich Null auf Null zurückgesetzt werden.</p>
-replicateHourlySnaps	<p>Geben Sie an, ob stündlich geplante Snapshots zur Replikation markiert werden sollen. Gültige Werte:</p> <ul style="list-style-type: none"> • yes • no <p> ANMERKUNG: Dieser Qualifizierer wird nur für asynchrone Replikationen verwendet.</p>
-replicateDailySnaps	<p>Geben Sie an, ob täglich geplante Snapshots zur Replikation markiert werden sollen. Gültige Werte:</p> <ul style="list-style-type: none"> • yes • no <p> ANMERKUNG: Dieser Qualifizierer wird nur für asynchrone Replikationen verwendet.</p>
-keepSameAsSource	<p>Geben Sie an, ob die gleiche Aufbewahrungs-Policy (Ablaufzeit und automatisches Löschen) der Quelle für das Ziel verwendet werden soll. Diese Option gibt Änderungen an der Quellaufbewahrungs-Policy an die Ziel-Aufbewahrungs-Policy weiter (ab diesem Zeitpunkt für neu erstellte geplante Snapshots, alte Snapshots bleiben unverändert). Keine Werte sind zulässig.</p> <p>Diese Option ist standardmäßig aktiviert, wenn -keepFor oder -allowAutoDelete nicht festgelegt ist.</p> <p> ANMERKUNG: Dieser Qualifizierer wird nur für asynchrone Replikationen verwendet.</p>
-keepFor	<p>Gibt die Aufbewahrungsdauer an, nach der der Snapshot auf dem Ziel gelöscht wird. Das Intervall kann in Tagen oder Stunden definiert werden. Das Format lautet wie folgt:</p> <p><code><value><qualifier></code></p> <p>Dabei gilt Folgendes:</p> <ul style="list-style-type: none"> • Wert: ein ganzzahliger Wert. Wenn der Qualifizierer h (Stunden) ist, ist der zulässige Bereich von 1 bis 42840. Wenn der Qualifizierer d (Tage) ist, ist der zulässige Bereich von 1 bis 1785. • Qualifizierer: ein Qualifizierer des Werts. Die gültigen Werte sind folgende: <ul style="list-style-type: none"> ○ h (Stunden) ○ d (Tage) <p> ANMERKUNG: Dieser Qualifizierer wird nur für asynchrone Replikationen verwendet.</p>
-allowAutoDelete	<p>Geben Sie an, ob automatisches Löschen auf der replizierten Kopie dieses Snapshot oder dieses Snapshot-Set zulässig ist.</p> <p> ANMERKUNG: Dieser Qualifizierer wird nur für asynchrone Replikationen verwendet.</p>
-replicateExistingSnaps	<p>Gibt an, ob Snapshots auf der Quellressource repliziert werden sollen. Dieser Qualifizierer ist eine einmalige Option, die während der Erstellung der Sitzung verfügbar ist und durch die Snapshots, die zu diesem Zeitpunkt auf der Quelle vorhanden sind, repliziert werden.</p> <p> ANMERKUNG: Dieser Qualifizierer wird nur für asynchrone Replikationen verwendet.</p> <p>Es werden nur Nutzer-Snapshots repliziert, die nach der Erstellung der Common-Base-Snapshots erstellt wurden und den Status „Inaktiv“ oder „Ausstehend“ haben.</p> <p>Es werden alle in Betracht kommenden Snapshots repliziert und die Quellaufbewahrungs-Policy wird als Zielaufbewahrungs-Policy auf sie angewendet. Damit ein Snapshot für diese Option in Betracht kommt, muss er diese 3 Kriterien erfüllen:</p> <ul style="list-style-type: none"> • Der Snapshot wird entweder durch den Benutzer oder einen Snapshot-Plan erstellt.

Qualifizierer	Beschreibung
	<ul style="list-style-type: none"> Der Snapshot ist schreibgeschützt (der Dateiressourcen-Snapshot muss ein Checkpoint-Snapshot sein; es darf kein Blockressourcen-Snapshot verbunden sein). Es findet gerade keine Löschung des Snapshot statt.
<code>-allowAsyncSnapReplication</code>	<p>Geben Sie an, ob eine Snapshot-Replikation in einer asynchronen Sitzung zulässig ist. Gültige Werte:</p> <ul style="list-style-type: none"> <code>yes</code> <code>no</code> <p> ANMERKUNG: Dieser Qualifizierer wird nur für asynchrone Dateisystemreplikationen verwendet.</p>
<code>-enableUserSnapCommonBase</code>	<p>Legen Sie den Nutzer-Snapshot als gemeinsame Basis für Unity-Systeme mit OE-Version 5.1 fest.</p> <p>Wenn dieser Qualifizierer nicht vorhanden ist, behandelt das System den Nutzer-Snapshot nicht als gemeinsame Basis.</p> <p> ANMERKUNG: Dieser Qualifizierer muss festgelegt werden, wenn die Replikationssitzung konfiguriert ist.</p>
<code>-srcCommonBaseSnap</code>	<p>Geben Sie die Nutzer-Snapshot-Kennung an, die als gemeinsame Basis auf der Quellressource für Unity-Systeme mit OE-Version 5.1 verwendet wird.</p>
<code>-dstCommonBaseSnap</code>	<p>Geben Sie die Nutzer-Snapshot-Kennung an, die als gemeinsame Basis auf der Zielressource für Unity-Systeme mit OE-Version 5.1 verwendet wird.</p>
<code>-autosearch</code>	<p>Aktivieren Sie das System, um eine automatische Suche durchzuführen, um einen Nutzer-Snapshot zu finden, der als eine gemeinsame Basis für Unity-Systeme mit OE-Version 5.1 verwendet werden kann.</p> <p>Wenn dieser Qualifizierer nicht enthalten ist, wird die Funktion <code>-autosearch</code> deaktiviert.</p> <p> ANMERKUNG: Dieser Qualifizierer muss festgelegt werden, wenn die Replikationssitzung konfiguriert ist und Sie eine vollständige Kopie nach einem Failover vermeiden möchten.</p>
<code>-skipSnapSignatureCheck</code>	<p>Geben Sie an, ob Sie die Prüfung der Nutzer-Snapshot-Signatur überspringen möchten, wenn Sie den Nutzer-Snapshot als gemeinsame Basis für Unity-Systeme mit OE-Version 5.1 verwenden. Dieser Qualifizierer ist nur gültig, wenn die Quell- und Zielnutzer-Snapshots als gemeinsame Basis angegeben werden.</p> <p> ANMERKUNG: Überprüfen Sie, ob die Nutzer-Snapshots als eine gemeinsame Basis qualifiziert sind.</p>
<code>-cascadeReplicatedSnap</code>	<p>Gibt an, ob Sie Snapshots automatisch downstream replizieren möchten, wenn der Snapshot aus der eingehenden Replikationssitzung repliziert wird.</p> <p>Die folgenden Werte sind gültig:</p> <ul style="list-style-type: none"> <code>yes</code> <code>no</code> (Standard)
<code>-overwriteDestination</code>	<p>Geben Sie an, ob die schmutzigen Daten auf dem Ziel überschrieben werden sollen. Die vollständige Datenübertragung nimmt mehr Zeit in Anspruch. Wenn dieser Qualifizierer nicht angegeben ist, kann das Ziel unterschiedliche Daten enthalten als die Quelle, wenn das Ziel beschädigte Daten enthält.</p>

Beispiel

Mit dem folgenden Befehl wird eine Replikationssitzung mit den folgenden Einstellungen erstellt:

- Quellspeicherressource: Dateisystem RS_1
- Es ist ein Remotezielsystem angegeben.
- Remotezielsystem: RS_2
- Remotespeicherressource: Dateisystem LUN_2

- Die Synchronisierung findet automatisch statt.
- RPO beträgt 2 Stunden und 30 Minuten

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/rep/session create -name REPl -srcRes RS_1 -dstType remote -dstSys RS_2 -dstRes LUN_2 -syncType auto -rpo 02h30m
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = 81604378625_FCNC097274B3A_0000_81604378627_FCNC097274B37_0000
Operation completed successfully.
```

Anzeigen von Replikationssitzungen

Zeigen Sie Details zu Replikationssitzungen an. Sie können nach der Sitzungs-ID filtern.

 **ANMERKUNG:** Der Befehl show action erläutert, wie das Ausgabeformat geändert wird.

Format

```
/prot/rep/session [{-id <value> | -name <value> | -res <value>}] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID der Replikationssitzung ein.
-name	Geben Sie den Namen der Replikationssitzung ein.
-res	Geben Sie die ID einer lokalen Speicherressource im System ein, um die damit verbundenen Sitzungen anzuzeigen.

Beispiel 1

Mit dem folgenden Befehl werden sämtliche Replikationssitzungen im System angezeigt.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/rep/session show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
1:      ID              = 81604378625_FCNC097274B3A_0000_81604378627_FCNC097274B37_0000
      Name              = MyRep1
      Session type      = block
      Synchronization type = manual
      RPO                =
      Sync State        = idle
      Health state      = OK (5)
      Operational status = Idle (0x8404)
      Time of last sync  =
      Sync status       =
      Element pairs     = sv_4 => sv_4
```

Beispiel 2

Mit dem folgenden Befehl werden sämtliche Replikationssitzungen im System und ihre Details angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/rep/session show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      ID              =
42949672965_FCNC0972DDD67_0000_42949672967_FCNC0972DDD67_0000
      Name              = rep_sess_sv_1_sv_2_local
      Session type      = lun
      Synchronization type = manual
      RPO                =
      Resource type     = LUN
      Sync State        = idle
      Health state      = OK (5)
      Health details    = "This replication session is operating normally. No
action is required."
      Operational status = Idle (0x8404)
      Source status     = OK
      Destination status = OK
      Network status    = OK
      Destination type  = local
      Destination system = local
      Local role        = Local
      Source resource   = sv_1
      Source SP-A interface = N/A
      Source SP-B interface = N/A
      Destination resource = sv_2
      Destination SP-A interface = N/A
      Destination SP-B interface = N/A
      Time of last sync = N/A
      Sync status       =
      Sync transfer rate = N/A
      Sync transfer size remaining = 0
      Previous transfer rate = N/A
      Average transfer rate = N/A
      Element pairs     = N/A
      Hourly snapshot keep for = 3h
      Hourly snapshot allow auto-delete = no
      Daily snapshot keep for = not replicated
      Daily snapshot allow auto-delete = not replicated
      Allow Async Snap Replication = N/A
      Cascade Replicated Snap = no
```

Ändern der Einstellungen für Replikationssitzungen

Ändern Sie die Einstellungen für eine Replikationssitzung.

Format

```
/prot/rep/session {-id <value> | -name <value>} set [-async] [-newName <value>] [-srcSPAInterface <value>] [-dstSPAInterface <value>] [-srcSPBInterface <value>] [-dstSPBInterface <value>] [-syncType {manual | auto [-rpo <value>]}] [-replicateHourlySnaps {yes [{-keepSameAsSource | -keepFor <value> | -allowAutoDelete}] | no}] [-replicateDailySnaps {yes [{-keepSameAsSource | -keepFor <value> | -allowAutoDelete}] | no}] [-allowAsyncSnapReplication {yes [-cascadeReplicatedSnap {yes | no}] | no}]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID der zu ändernden Replikationssitzung ein.
-name	Geben Sie den Namen der zu ändernden Replikationssitzung ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Ausführen einer Aktion im asynchronen Modus
-newName	Geben Sie den neuen Namen der Replikationssitzung ein.
-srcSPAInterface	Geben Sie die ID der Schnittstelle ein, die auf dem SPA des Quellsystems für die Replikation verwendet wird.  ANMERKUNG: Dieser Qualifizierer wird nur für asynchrone Replikationen auf Remotesystemen verwendet. Wenn der Qualifizierer nicht angegeben ist, wird die Schnittstelle vom System automatisch erkannt.
-srcSPBInterface	Geben Sie die ID der Schnittstelle auf dem SPB des Quellsystems für die Replikation ein.  ANMERKUNG: Dieser Qualifizierer wird nur für asynchrone Replikationen auf Remotesystemen verwendet. Wenn der Qualifizierer nicht angegeben ist, wird die Schnittstelle vom System automatisch erkannt.
-dstSPAInterface	Geben Sie die ID der Schnittstelle auf dem SPA des Zielsystems für die Replikation ein.  ANMERKUNG: Dieser Qualifizierer wird nur für asynchrone Replikationen auf Remotesystemen verwendet. Wenn der Qualifizierer nicht angegeben ist, wird die Schnittstelle vom System automatisch erkannt.
-dstSPBInterface	Geben Sie die ID der Schnittstelle auf dem SPB des Zielsystems für die Replikation ein.  ANMERKUNG: Dieser Qualifizierer wird nur für asynchrone Replikationen auf Remotesystemen verwendet. Wenn der Qualifizierer nicht angegeben ist, wird die Schnittstelle vom System automatisch erkannt.
-syncType	Dieser Parameter gibt an, ob die erste Replikationssynchronisation (eine vollständige Synchronisation) automatisch durchgeführt werden soll. Das folgende Beispiel zeigt die Option manuel11 , die für die erste Replikationssynchronisation verwendet wird: <code>-syncType {manual auto [-rpo <value>]}</code> Gültige Werte: <ul style="list-style-type: none"> • manual: Die Daten werden bei manueller Initiierung repliziert. • auto [-rpo <value>]: Daten werden im Hinblick auf die Einhaltung des gewünschten Recovery Point Objective (RPO) automatisch repliziert.  ANMERKUNG: Dieser Qualifizierer wird nur für asynchrone Replikationen verwendet. Mit einem höheren RPO steigt auch das Risiko eines potenziellen Datenverlusts und der erforderliche Schutzspeicherplatz. Durch Senken des RPO wird das Risiko des Datenverlusts reduziert, aber gleichzeitig nimmt der Netzwerkverkehr zu, was sich negativ auf die Performance auswirken kann. Das Standard-RPO liegt bei einer Stunde.
-rpo	Geben Sie bei der automatischen Synchronisierung das Zeitintervall für die Durchführung an. Das Format lautet wie folgt: <HH> [:MM] Dabei gilt Folgendes: <ul style="list-style-type: none"> • HH: Geben Sie die Zahl der Stunden ein. Der zulässige Bereich liegt zwischen 00 und 24 Stunden (1 Tag). • MM: Geben Sie die Zahl der Minuten in 5-Minuten-Schritten ein. Es können Werte im Bereich zwischen 05 und 55 eingegeben werden.  ANMERKUNG: Für eine synchrone Replikation geben Sie den Wert 0 ein. Der Wert kann nicht von Null auf ungleich Null oder von ungleich Null auf Null zurückgesetzt werden.
-replicateHourlySnaps	Geben Sie an, ob stündlich geplante Snapshots zur Replikation markiert werden sollen. Gültige Werte: <ul style="list-style-type: none"> • yes

Qualifizierer	Beschreibung
	<ul style="list-style-type: none"> no <p>ANMERKUNG: Dieser Qualifizierer wird nur für asynchrone Replikationen verwendet.</p>
-replicateDailySnaps	<p>Geben Sie an, ob täglich geplante Snapshots zur Replikation markiert werden sollen. Gültige Werte:</p> <ul style="list-style-type: none"> yes no <p>ANMERKUNG: Dieser Qualifizierer wird nur für asynchrone Replikationen verwendet.</p>
-keepSameAsSource	<p>Geben Sie an, ob die gleiche Aufbewahrungs-Policy (Ablaufzeit und automatisches Löschen) der Quelle für das Ziel verwendet werden soll. Diese Option gibt Änderungen an der Quellaufbewahrungs-Policy an die Ziel-Aufbewahrungs-Policy weiter (ab diesem Zeitpunkt für neu erstellte geplante Snapshots, alte Snapshots bleiben unverändert). Keine Werte sind zulässig.</p> <p>ANMERKUNG: Dieser Qualifizierer wird nur für asynchrone Replikationen verwendet.</p>
-keepFor	<p>Geben Sie die Aufbewahrungszeit an, nach der der Snapshot auf dem Ziel gelöscht wird. Das Intervall kann in Tagen oder Stunden definiert werden. Das Format lautet wie folgt:</p> <p><value><qualifier></p> <p>Dabei gilt Folgendes:</p> <ul style="list-style-type: none"> Wert: ein ganzzahliger Wert. Wenn der Qualifizierer h (Stunden) ist, ist der zulässige Bereich von 1 bis 42840. Wenn der Qualifizierer d (Tage) ist, ist der zulässige Bereich von 1 bis 1785. Qualifizierer: ein Qualifizierer des Werts. Die gültigen Werte sind folgende: <ul style="list-style-type: none"> h (Stunden) d (Tage) <p>ANMERKUNG: Dieser Qualifizierer wird nur für asynchrone Replikationen verwendet.</p>
-allowAutoDelete	<p>ANMERKUNG: Nur gültig, wenn -replicateHourlySnaps yes oder -replicateDailySnaps yes.</p> <p>Geben Sie an, ob automatisches Löschen auf der replizierten Kopie dieses Snapshot oder dieses Snapshot-Set zulässig ist. Gültige Werte:</p> <ul style="list-style-type: none"> yes no <p>ANMERKUNG: Dieser Qualifizierer wird nur für asynchrone Replikationen verwendet.</p>
-allowAsyncSnapReplication	<p>Gibt an, ob die Snapshot-Replikation in asynchronen Sitzungen zugelassen werden soll. Gültige Werte:</p> <ul style="list-style-type: none"> yes no
-cascadeReplicatedSnap	<p>Gibt an, ob Snapshots in der Kaskaden-Replikationssitzung repliziert werden sollen. Dieser Qualifizierer kann nur geändert werden, wenn die Sitzung aktiv ist. Gültige Werte:</p> <ul style="list-style-type: none"> yes no (default)

Beispiel

Der folgende Befehl ändert die Quell- und die Zielschnittstelle für die Replikationssitzung 81604378625_FCNC097274B3A_0000_81604378627_FCNC097274B37_0000:

```
uemcli /prot/rep/session -id 81604378625_FCNC097274B3A_0000_81604378627_FCNC097274B37_0000 set -srcSPAInterface if_1 -srcSPBInterface if_2 -dstSPAInterface if_3 -dstSPBInterface if_4
```

```
Storage system address: 10.0.0.1
Storage system port: 443
```

```
HTTPS connection
```

```
ID = 81604378625_FCNC097274B3A_0000_81604378627_FCNC097274B37_0000  
Operation completed successfully.
```

Anhalten von Replikationssitzungen

Halten Sie eine oder mehrere Replikationssitzungen auf Remotesystemebene an.

Format

```
/prot/rep/session {-id <value> | -name <value>} pause [-async]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID der anzuhaltenden Replikationssitzung ein.
-name	Geben Sie den Namen jeder anzuhaltenden Replikationssitzung ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Ausführen einer Aktion im asynchronen Modus

Beispiel

Mit dem folgenden Befehl wird die Replikationssitzung
81604378625_FCNC097274B3A_0000_81604378627_FCNC097274B37_0000 angehalten:

```
uemcli /prot/rep/session -id 81604378625_FCNC097274B3A_0000_81604378627_FCNC097274B37_0000  
pause
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection
```

```
Operation completed successfully.
```

Fortsetzen von Replikationssitzungen

Setzt eine oder mehrere vorhandene Replikationssitzungen auf Remoteebene fort.

Format

```
/prot/rep/session {-id <value> | -name <value>} resume [-async] [-forceFullCopy] [-  
allowFullCopy] [-srcSPAInterface <value>] [-dstSPAInterface <value>] [-srcSPBInterface <value>]  
[-dstSPBInterface <value>] [-forceSyncData]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID der Replikationssitzung ein, die Sie wieder aufnehmen möchten.
-name	Geben Sie den Namen jeder Replikationssitzung ein, die Sie fortsetzen möchten.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Ausführen einer Aktion im asynchronen Modus
-allowFullCopy	<p>Dieser Qualifizierer gibt an, dass eine vollständige Synchronisation durchgeführt werden kann, wenn kein Common-Base-Snapshot vorhanden ist, wenn eine asynchrone Replikationssitzung fortgesetzt wird.</p> <p>Die Option -allowFullCopy wird nicht unterstützt, wenn eine synchrone Replikationssitzung nach einer Pause wieder aufgenommen wird. Die vollständige Kopie wird mit dem gleichen Verhalten mit -allowFullCopy durchgeführt, das für die synchrone Dateireplikation festgelegt wurde, wenn die Sitzung über keine Common-Base-Snapshots verfügt und weder -allowFullCopy noch -forceFullCopy angegeben ist.</p> <p>Wenn das Quellsystem über Snapshots verfügt, die vor dem Upgrade des Systems auf Unity 5.1.2 erstellt wurden, und diese Snapshots als Common-Base-Snapshots verwendet werden, lösen diese Snapshots eine vollständige Synchronisation aus. Seit Unity 5.1.2 verfügen Common-Base-Snapshots über Signaturen, die eine Delta-Synchronisation erlauben.</p> <p> ANMERKUNG: Dieser Qualifizierer unterstützt keine synchronen Block-Replikationen.</p>
-forceFullCopy	<p>Dieser Qualifizierer gibt an, dass eine vollständige Synchronisation durchgeführt wird, wenn eine asynchrone Replikationssitzung fortgesetzt wird.</p> <p>Die Option -forceFullCopy wird nicht unterstützt, wenn eine synchrone Replikationssitzung nach einer Pause wieder aufgenommen wird.</p> <p> ANMERKUNG: Dieser Qualifizierer unterstützt keine synchronen Block-Replikationen.</p>
-srcSPAInterface	<p>Geben Sie die ID der Schnittstelle ein, die auf dem SPA des Quellsystems für die Replikation verwendet wird.</p> <p> ANMERKUNG: Dieser Qualifizierer wird nur für asynchrone Replikationen auf Remotesystemen verwendet. Wenn der Qualifizierer nicht angegeben ist, wird die Schnittstelle vom System automatisch erkannt.</p>
-dstSPAInterface	<p>Geben Sie die ID der Schnittstelle auf dem SPA des Zielsystems für die Replikation ein.</p> <p> ANMERKUNG: Dieser Qualifizierer wird nur für asynchrone Replikationen auf Remotesystemen verwendet. Wenn der Qualifizierer nicht angegeben ist, wird die Schnittstelle vom System automatisch erkannt.</p>
-srcSPBInterface	<p>Geben Sie die ID der Schnittstelle auf dem SPB des Quellsystems für die Replikation ein.</p> <p> ANMERKUNG: Dieser Qualifizierer wird nur für asynchrone Replikationen auf Remotesystemen verwendet. Wenn der Qualifizierer nicht angegeben ist, wird die Schnittstelle vom System automatisch erkannt.</p>
-dstSPBInterface	<p>Geben Sie die ID der Schnittstelle auf dem SPB des Zielsystems für die Replikation ein.</p> <p> ANMERKUNG: Dieser Qualifizierer wird nur für asynchrone Replikationen auf Remotesystemen verwendet. Wenn der Qualifizierer nicht angegeben ist, wird die Schnittstelle vom System automatisch erkannt.</p>
-forceSyncData	<p>Dieser Qualifizierer erzwingt eine Datenübertragung vom Quellsystem zum Remote-System. Diese Übertragung erfolgt, selbst wenn das Remote-System über Daten verfügt, die nicht vom Quellsystem repliziert werden.</p> <p> ANMERKUNG: Dieser Qualifizierer wird nur für asynchrone Replikationen verwendet.</p>

Beispiel

Mit dem folgenden Befehl wird die Replikationssitzung 81604378625_FCNCHE097274B3A_0000_81604378627_FCNCHE097274B37_0000 fortgesetzt:

```
uemcli /prot/rep/session -id 81604378625_FCNCHE097274B3A_0000_81604378627_FCNCHE097274B37_0000 resume
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = 81604378625_FCNCHE097274B3A_0000_81604378627_FCNCHE097274B37_0000
Operation completed successfully.
```

Manuelles Synchronisieren von Replikationssitzungen

Synchronisieren Sie eine Replikationssitzung manuell.

Format

```
/prot/rep/session{-id <value> | -name <value>} sync [-async]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID der zu synchronisierenden Replikationssitzung ein.
-name	Geben Sie die ID der zu synchronisierenden Replikationssitzung ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Ausführen einer Aktion im asynchronen Modus

Beispiel

Mit dem folgenden Befehl wird eine erneute manuelle Synchronisierung der Replikationssitzung REPS_1 durchgeführt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/rep/session -id REPS_1 sync
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Löschen einer Replikationssitzung

Löschen Sie eine Replikationssitzung. Beim Löschen wird automatisch die Quell-Speicherressource mit der Ziel-Speicherressource synchronisiert. Anschließend wird für beide Lese- und Schreibzugriff festgelegt, und danach wird die Sitzung gelöscht. Sie können einen Host mit einer beliebigen der beiden Speicherressourcen verbinden. Das Löschen der Sitzung vom Quellsystem entfernt automatisch die Ziel- und Quell-Replikationssitzungen. Dadurch wird sichergestellt, dass Sie die verknüpften Speicherressourcen oder NAS-Server nicht manuell vom Zielsystem löschen müssen.

ANMERKUNG: Sobald Sie eine Replikationssitzung löschen, werden Daten der Quellspeicherressource nicht mehr auf dem Ziel repliziert. Damit sind die Daten nicht mehr geschützt. Beim Löschen einer synchronen Replikationssitzung des Dateisystems wird die Sitzung zwar gelöscht, aber wenn die anfängliche Synchronisation nicht abgeschlossen ist, läuft das Zielsystem in einen nicht behebbaren Fehler. Löschen Sie in diesem Fall das Zielsystem.

Format

```
/prot/rep/session {-id <value> | -name <value>} delete [-async]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID der zu löschenden Replikationssitzung ein.
-name	Geben Sie den Namen der zu löschenden Replikationssitzung ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Ausführen einer Aktion im asynchronen Modus

Beispiel

Der folgende Befehl löscht die Replikationssitzung 81604378625_FCNCHE097274B3A_0000_81604378627_FCNCHE097274B37_0000:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/rep/session -id  
81604378625_FCNCHE097274B3A_0000_81604378627_FCNCHE097274B37_0000 delete
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection  
  
Operation completed successfully.
```

Failover von Replikationssitzungen

Führen Sie diesen Befehl auf dem Zielsystem als Failover einer Replikationssitzung als Reaktion auf eine Notfallsituation aus, in der die Quelle nicht mehr verfügbar ist. Dabei können Daten verloren gehen.

Nach dem Failover hat das Zielsystem den Status „Lesen/Schreiben“. Zur Wiederherstellung der Kommunikation zwischen der Quelle und dem Ziel können Sie für die Sitzung einen Failback durchführen. [Failback von Replikationssitzungen](#) erläutert das Failback einer Replikationssitzung nach einem Failover.

ANMERKUNG: Bei Failover-Vorgängen werden aktive Datenübertragungen beendet, wodurch es zu einem Datenverlust kommen kann. Wenn der Quellstandort bei der Durchführung eines Failovers noch verfügbar ist, versucht das System, die Quellspeicherressource vom Status „Lesen/Schreiben“ in „Schreibgeschützt“ zu ändern.

Initiieren Sie eine geplante Nicht-Verfügbarkeit

Um eine geplante Nicht-Verfügbarkeit einzuleiten, führen Sie diesen Befehl auf dem Quellsystem mit der Option -sync und dem Wert yes aus. Wenn Sie vom Quellsystem ein Failover einer Replikationssitzung ausführen, wird das Zielsystem vollständig mit der Quelle synchronisiert. Dadurch wird sichergestellt, dass keine Daten verloren gehen. Die Zielspeicherressource kann für den Zugriff auf den Host verwendet werden.

Format

```
/prot/rep/session {-id <value> | -name <value>} failover [-async] [-sync {yes | no}] [-force]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID der Replikationssitzung für das Failover ein.
-name	Geben Sie den Namen der Replikationssitzung für das Failover ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Ausführen einer Aktion im asynchronen Modus
-sync	Gibt bei einer asynchronen Replikationssitzung an, ob vor dem Failover der Replikationssitzung eine Synchronisation durchgeführt werden muss. Gibt bei einer synchronen Replikationssitzung an, ob nach dem Failover der Sitzung eine Synchronisation in der umgekehrten Richtung beibehalten werden soll. Gültige Werte: <ul style="list-style-type: none">• yes: Für ein geplantes Failover. Kann nur über das Quellsystem ausgeführt werden. Wenn für <code>-sync</code> nichts angegeben ist, ist dies der Standardwert für eine lokale Replikationssitzung oder eine Sitzung, bei der <code>role=source</code> gilt.• no: Für ein ungeplantes Failover. Kann nur über das Zielsystem ausgeführt werden. Wenn für <code>-sync</code> nichts angegeben ist, ist dies der Standardwert für eine Remotereplikationssitzung oder eine Sitzung, bei der <code>role=destination</code> gilt. <p> ANMERKUNG: Ist der Netzwerkstatus=OK, ist das Quellsystem wahrscheinlich fehlerfrei. Wird der Befehl über das Zielsystem ohne diese Option ausgeführt, schlägt er fehl. Es wird empfohlen, den Befehl mit der Option <code>yes</code> erneut auf dem Quellsystem auszuführen. Jedoch ist es nach wie vor zulässig, den Befehl mit der Option <code>no</code> über das Zielsystem auszuführen.</p>
-force	Gibt an, ob eine vorgeschaltete Prüfung in Dateisystemen eines NAS-Servers übersprungen werden soll, wenn ein Replikations-Failover über den NAS-Quellserver ausgeführt wird. Keine Werte sind zulässig.

Beispiel

Der folgende Befehl führt ein Failback auf Replikationssitzung 81604378625_FCNC097274B3A_0000_81604378627_FCNC097274B37_0000 durch:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/rep/session -id 81604378625_FCNC097274B3A_0000_81604378627_FCNC097274B37_0000 failover
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
Operation completed successfully.
```

Failback von Replikationssitzungen

Führen Sie ein Failback einer Replikationssitzung durch, bei der es zum Failover gekommen war. Ein Failback führt zu folgendem Ergebnis:

- Die Ziel- und Quell-Storage-Ressourcen werden miteinander synchronisiert.
- Die Ziel-Storage-Ressource ist nun schreibgeschützt.
- Die Quell-Storage-Ressource hat den Status „Lesen/Schreiben“.

Wenn die Failback-Operation abgeschlossen ist, wird die Replikationssitzung fortgesetzt, und Sie können Ihre Hosts mit der Quell-Storage-Ressource verbinden.

 **ANMERKUNG:** Achten Sie darauf, dass die Hosts nicht auf die Ziel-Storage-Ressource schreiben, da diese schreibgeschützt ist.

Format

```
/prot/rep/session {-id <value> | -name <value>} failback [-async] [-forceFullCopy] [-allowFullCopy] [-force] [-syncData {force | ignore}]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID der Replikationssitzung für das Failback ein.
-name	Geben Sie den Namen der Replikationssitzung für das Failback ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Ausführen einer Aktion im asynchronen Modus
-allowFullCopy	<p>Dieser Qualifizierer gibt an, dass nach einem Failback eine vollständige Synchronisation durchgeführt werden kann, wenn kein Common-Base-Snapshot vorhanden ist, wenn eine asynchrone Replikationssitzung fortgesetzt wird.</p> <p>Die Option -allowFullCopy wird nicht unterstützt, wenn eine synchrone Replikationssitzung nach einer Pause wieder aufgenommen wird. Die vollständige Kopie wird mit dem gleichen Verhalten mit -allowFullCopy durchgeführt, das für die synchrone Dateireplikation festgelegt wurde, wenn die Sitzung über keine Common-Base-Snapshots verfügt und weder -allowFullCopy noch -forceFullCopy angegeben ist.</p> <p>Wenn das Quellsystem über Snapshots verfügt, die vor dem Upgrade des Systems auf Unity 5.1.2 erstellt wurden, und diese Snapshots als Common-Base-Snapshots verwendet werden, lösen diese Snapshots eine vollständige Synchronisation aus. Seit Unity 5.1.2 verfügen Common-Base-Snapshots über Signaturen, die Delta-Synchronisationen erlauben.</p> <p> ANMERKUNG: Dieser Qualifizierer unterstützt keine synchronen Block-Replikationen.</p>
-forceFullCopy	<p>Dieser Qualifizierer gibt an, dass eine vollständige Synchronisation durchgeführt wird, wenn eine asynchrone Replikationssitzung fortgesetzt wird.</p> <p>Die Option -forceFullCopy wird nicht unterstützt, wenn eine synchrone Replikationssitzung nach einer Pause wieder aufgenommen wird.</p> <p> ANMERKUNG: Dieser Qualifizierer unterstützt keine synchronen Block-Replikationen.</p>
-force	Vor einem Failback einer synchronen NAS-Server-Replikationssitzung wird geprüft, ob die zugehörigen asynchronen Dateisystemreplikationssitzungen erhalten bleiben, wenn sie gleichzeitig bestehen. Wenn dieser Qualifizierer angegeben ist, wird diese Prüfung übersprungen.
-syncData	<p>Bestimmt das Verhalten der Übertragung von Daten vom Quellsystem auf das Remotesystem. Wenn der Qualifizierer nicht angegeben wird, schlägt der Befehl fehl, wenn auf dem Remote-System Daten vom Quellsystem nicht repliziert wurden. Gültige Werte:</p> <ul style="list-style-type: none"> • force: Erzwingen der Datenübertragung vom Quellsystem auf das Remotesystem, auch wenn das Remotesystem nicht synchronisierte Daten hat. • ignore: Überspringen Sie die Datenübertragung vom Quellsystem zum Remote-System und lösen Sie die Replikationssitzung umgekehrt vom Remote-System zum Quellsystem aus. <p> ANMERKUNG: Dieser Qualifizierer wird nur für asynchrone Replikationen verwendet.</p>

Beispiel

Der folgende Befehl führt ein Failback auf Replikationssitzung 81604378625_FCNCHE097274B3A_0000_81604378627_FCNCHE097274B37_0000 durch:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/rep/session -id 81604378625_FCNCHE097274B3A_0000_81604378627_FCNCHE097274B37_0000 failback
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection
```

```
Operation completed successfully.
```

Beibehalten von asynchronen Replikationssitzungen

Initiiert einen Vorgang zum Beibehalten asynchroner Replikationssitzungen auf einer synchronen Replikationssitzung des NAS-Servers. Nach dem Failover oder Failback einer synchronen Replikationssitzung des NAS-Servers mit ihren synchronen Replikationssitzungen des Dateisystems werden die asynchronen Replikationssitzungen durch den Vorgang des Beibehaltens der asynchronen Replikationssitzungen auf den neuen Produktionsstandort umgestellt.

Format

```
/prot/rep/session {-id <value> | -name <value>} preserveAsync [-dstSys <value>]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Identifiziert die synchrone Replikationssitzung des NAS-Servers.
-name	Identifiziert die synchrone Replikationssitzung des NAS-Servers nach Name.
-dstSys	Identifiziert das Remotesystem, das als NAS-Zielsystem zur Beibehaltung der asynchronen Replikationssitzung ausgewählt wird. Wenn dieser Qualifizierer nicht angegeben ist, werden alle asynchronen Remotesysteme überprüft. Das erste System mit einer übereinstimmenden asynchronen Replikationssitzung (das dieselben NAS-Server-ID wie die synchrone Replikationssitzung hat) wird zur Beibehaltung der Sitzung ausgewählt.

Beispiel

Mit dem folgenden Befehl werden asynchrone Replikationssitzungen für 81604378625_FCNCHE097274B3A_0000_81604378627_FCNCHE097274B37_0000 beibehalten:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/rep/session -id 81604378625_FCNCHE097274B3A_0000_81604378627_FCNCHE097274B37_0000 preserveAsync
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection
```

```
Operation completed successfully.
```

Erneutes Erstellen einer Replikationssitzung

Wenn die Quell- und Zielsysteme einen Common-Base-Snapshot gemeinsam nutzen, können Sie eine Replikationssitzung erneut erstellen.

Synchrone und asynchrone Replikationssitzungen können neu erstellt werden. Die folgenden Sitzungen für jeden Typ können erneut erstellt werden:

- Synchrone Dateisystemsitzungen

- Asynchrone Dateisystemsitzungen
- Asynchrone Block-Sitzungen

Die folgenden Typen von synchronen und asynchronen Replikationssitzungen können nicht wiederhergestellt werden:

- Synchroner Block-Sitzungen
- Synchroner NAS-Server-Sitzungen
- Asynchrone NAS-Server-Sitzungen

Format

```
/prot/rep/session create [-async] -srcRes <value> -dstType remote -dstSys <value>
-dstRes <value> -syncType {manual [-autoInitiate {yes | no}] | auto [-rpo <value>]}
-enableUserSnapCommonBase -autoSearch -srcCommonBaseSnap <value> -dstCommonBaseSnap <value>
-skipSnapSignatureCheck
```

Objektqualifizierer

Qualifizierer	Beschreibung
-async	Ausführen einer Aktion im asynchronen Modus
-srcRes	Geben Sie die ID der als Quelle zu verwendenden Speicherressource ein.
-dstType	Geben Sie den Ziel-Typ an. Gültige Werte: <ul style="list-style-type: none"> • local: Es verbleibt eine vollständige Kopie der Speicherressource auf dem lokalen System. Gegenüber Snapshots hat diese Option den Vorteil, dass nicht nur Kopien der einzelnen Änderungen gespeichert werden. • remote: Es wird eine vollständige Kopie der Speicherressource auf einem Remotesystem gespeichert. Dafür müssen die Daten über das Netzwerk übertragen werden. Die Remotereplikation wird häufig verwendet, damit an einem Remotestandort eine Kopie verfügbar ist, falls die Daten aufgrund von Notfallsituationen verloren gehen. Beispielsweise kann ein Verlust durch eine Naturkatastrophe am lokalen Standort verursacht werden.
-dstSys	Geben Sie zur Remotereplikation die ID des Zielsystems ein. Anzeigen von Einstellungen für Remotespeichersysteme erläutert, wie Sie die IDs der Remotesystemkonfiguration im lokalen System anzeigen.
-dstRes	Geben Sie die ID der Ziel-Speicherressource ein.
-syncType	Dieser Parameter gibt an, ob die erste Replikationssynchronisation (eine vollständige Synchronisation) automatisch durchgeführt werden soll. Das folgende Beispiel zeigt die Option manuell , die für die erste Replikationssynchronisation verwendet wird: <code>-syncType {manual [-autoInitiate {yes no}] auto [-rpo <value>]}</code> Gültige Werte: <ul style="list-style-type: none"> • manual: Die Daten werden bei manueller Initiierung repliziert. • -autoInitiate– Die Werte für -autoInitiate lauten wie folgt: <ul style="list-style-type: none"> ◦ ja aktiviert die automatische Synchronisation. ◦ nein deaktiviert die automatische Synchronisation. • auto [-rpo <value>]: Daten werden im Hinblick auf die Einhaltung des gewünschten Recovery Point Objective (RPO) automatisch repliziert. <p> ANMERKUNG: Dieser Qualifizierer wird nur für asynchrone Replikationen verwendet.</p> <p>Mit einem höheren RPO steigt auch das Risiko eines potenziellen Datenverlusts und der erforderliche Schutzspeicherplatz. Durch Senken des RPO wird das Risiko des Datenverlusts reduziert, aber gleichzeitig nimmt der Netzwerkverkehr zu, was sich negativ auf die Performance auswirken kann. Das Standard-RPO liegt bei einer Stunde.</p>
-rpo	Geben Sie das Zeitintervall für die Synchronisation ein. Das Format lautet wie folgt: <HH>[:MM] Hierbei gilt:

Qualifizierer	Beschreibung
	<ul style="list-style-type: none"> • HH: Geben Sie die Zahl der Stunden ein. Der zulässige Bereich liegt zwischen 00 und 24 Stunden (1 Tag). • MM: Geben Sie die Zahl der Minuten in 5-Minuten-Schritten ein. Der Bereich ist 05–55. <p>Für eine synchrone Replikation geben Sie den Wert 0 ein. Wenn der Wert festgelegt ist, kann er nicht von Null auf ungleich Null oder von ungleich Null auf Null zurückgesetzt werden.</p>
-enableUserSnapCommonBase	<p>Legen Sie den Nutzer-Snapshot als gemeinsame Basis für Unity-Systeme mit OE-Version 5.1 fest.</p> <p>Wenn dieser Qualifizierer vorhanden ist, behandelt das System den Nutzer-Snapshot nicht als gemeinsame Basis.</p> <p>i ANMERKUNG: Wenn Sie beim erneuten Erstellen der Sitzung eine vollständige Kopie vermeiden möchten, muss dieser Qualifizierer festgelegt werden, wenn die Replikationssitzung konfiguriert ist.</p>
-autosearch	<p>Aktivieren Sie das System für die Suche nach dem Nutzer-Snapshot, der als Common-Base-Snapshot für Unity-Systeme mit OE-Version 5.1 festgelegt wurde.</p> <p>Wenn dieser Qualifizierer nicht enthalten ist, wird die Funktion <code>-autosearch</code> deaktiviert.</p> <p>i ANMERKUNG: Wenn Sie beim erneuten Erstellen der Sitzung eine vollständige Kopie vermeiden möchten, muss dieser Qualifizierer festgelegt werden, wenn die Replikationssitzung konfiguriert ist.</p>
-srcCommonBaseSnap	<p>Geben Sie die Nutzer-Snapshot-Kennung an, die als gemeinsame Basis auf der Quellressource für Unity-Systeme mit OE-Version 5.1 verwendet wird.</p> <p>i ANMERKUNG: Wenn Sie beim erneuten Erstellen der Sitzung eine vollständige Kopie vermeiden möchten, muss dieser Qualifizierer festgelegt werden, wenn die Replikationssitzung konfiguriert ist.</p>
-dstCommonBaseSnap	<p>Geben Sie die Nutzer-Snapshot-Kennung an, die als gemeinsame Basis auf der Zielressource für Unity-Systeme mit OE-Version 5.1 verwendet wird.</p> <p>i ANMERKUNG: Wenn Sie beim erneuten Erstellen der Sitzung eine vollständige Kopie vermeiden möchten, muss dieser Qualifizierer festgelegt werden, wenn die Replikationssitzung konfiguriert ist.</p>
-skipSnapSignatureCheck	<p>Geben Sie an, ob Sie die Prüfung der Nutzer-Snapshot-Signatur überspringen möchten, wenn Sie den Nutzer-Snapshot als gemeinsame Basis für Unity-Systeme mit OE-Version 5.1 verwenden. Dieser Qualifizierer ist nur gültig, wenn die Quell- und Zielnutzer-Snapshots als gemeinsame Basis angegeben werden.</p> <p>i ANMERKUNG: Bestätigen Sie, dass die Nutzer-Snapshots zur Verwendung als eine gemeinsame Basis qualifiziert sind.</p>

Managen von virtuellen RecoverPoint-Appliances-CHAP-Konten

Wenn Sie eine RecoverPoint Appliance (RPA) konfigurieren, um mit dem Speichersystem zu arbeiten, können Sie optional mithilfe des Challenge Handshake Authentication Protocol (CHAP) die iSCSI-Schnittstellenauthentifizierung installieren. Zwei Typen von CHAP werden unterstützt:

- RPA Incoming Forward CHAP: Dies wird vom Speichersystem verwendet, um den RPA zu authentifizieren. Dieses CHAP ist dem iSCSI-CHAP-Konto ähnlich. Weitere Informationen zum Konfigurieren dieses CHAP finden Sie unter [Managen von iSCSI-CHAP-Konten für die einseitige CHAP-Authentifizierung](#).
- RPA Outgoing Forward CHAP: Dies wird vom RPA verwendet, um das Speichersystem zu authentifizieren.

In diesem Abschnitt werden die Attribute und Befehle beschrieben, die es Ihnen ermöglichen, RPA-CHAP-Konten zu managen.

In der folgenden Tabelle sind die Attribute fü

Tabelle 131. RPA-CHAP-Attribute

Attribut	Beschreibung
Out username	Der ausgehende CHAP-Benutzername.
Out secret	Der ausgehende CHAP-Schlüssel (Passwort).
Out secret format	Das Eingabeformat des ausgehenden CHAP-Schlüssels. Gültige Werte: <ul style="list-style-type: none"> • <code>ascii</code>: Schlüssel im ASCII-Format (Standard) • <code>hex</code>: Schlüssel im hexadezimalen Format

Zeigen Sie das RPA-CHAP-Konto an.

Zeigen Sie das RPA-CHAP-Konto an.

Format

```
/remote/rpa/chap show
```

Beispiel

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/rpa/chap show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      Out username = admin
```

Ändern eines RPA-CHAP-Kontos

Ändern Sie das RPA-CHAP-Konto.

Format

```
/remote/rpa/chap set [ -outUsername <value>] [ { -outSecret <value> | -outSecretSecure } [-outSecretFormat {ascii|hex}]]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
<code>-outUsername</code>	Geben Sie den ausgehenden CHAP-Benutzernamen ein.
<code>-outSecret</code>	Geben Sie den ausgehenden CHAP-Schlüssel (Passwort) ein. Standardmäßig handelt es sich beim CHAP-Schlüssel um eine ASCII-Zeichenfolge aus 12 bis 16 Zeichen. Hexadezimale Schlüssel bestehen aus 12 bis 16 Datenpaaren (24 bis 32 Zeichen).
<code>-outSecretSecure</code>	Geben Sie den ausgehenden CHAP-Schlüssel im sicheren Modus ein. Sie werden separat aufgefordert, das Passwort einzugeben.
<code>-outSecretFormat</code>	Das Eingabeformat des ausgehenden CHAP-Schlüssels. Gültige Werte: <ul style="list-style-type: none"> • <code>ascii</code>: Schlüssel im ASCII-Format • <code>hex</code>: Schlüssel im hexadezimalen Format

Beispiel

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/rpa/chap set -outUsername admin
-outSecret abcdef123456
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
Operation completed successfully.
```

Managen der Data-at-Rest-Verschlüsselung (nur physische Bereitstellungen)

 **ANMERKUNG:** Diese Funktion ist in Ihrer Implementierung möglicherweise nicht verfügbar.

Tabelle 132. Attribute der Data-at-Rest-Verschlüsselung

Attribut	Beschreibung
Encryption mode	Encryption-Mode Gültige Werte: <ul style="list-style-type: none"> • Unencrypted • Controller Based Encryption
Encryption status	Status des Verschlüsselungsprozesses Gültige Werte: <ul style="list-style-type: none"> • Not encrypting • In progress • Encrypted • Scrubbing  ANMERKUNG: Dieses Attribut ist nicht anwendbar und ist leer, wenn die Lizenz für die Funktion nicht installiert ist.
Percent encrypted	Prozentsatz der Benutzerdaten, die verschlüsselt sind
Backup keystore status	Status des Keystore-Backups Gültige Werte: <ul style="list-style-type: none"> • No operation required • Keystore is inaccessible • Backup keystore operation required • Backup keystore operation in progress • Backup keystore operation complete Der Keystore muss mithilfe des Befehls „uemcli“ -download gesichert und außerhalb des Speichersystems gespeichert werden.  ANMERKUNG: Dieses Attribut ist nicht anwendbar und ist leer, wenn die Lizenz für die Funktion nicht installiert ist.
KMIP status	Status des KMIP-Supports. Gültige Werte: <ul style="list-style-type: none"> • Enabled: KMIP-Funktion ist aktiviert. • Disabled: KMIP-Funktion ist deaktiviert. • Unsupported: KMIP-Funktion wird nicht unterstützt. • Unknown: Status der KMIP-Funktion kann nicht bestimmt werden.  ANMERKUNG: Sobald es aktiviert ist, kann das Speichersystem mit externen Key-Management-Servern interagieren, die KMIP-konform für Key-Management im Zusammenhang mit Data-at-Rest-Verschlüsselung sind.
SED status	Status der selbstverschlüsselnden Festplatte. <ul style="list-style-type: none"> • Locking Enabled– Die selbstverschlüsselnde Festplatte ist aktiviert.

Tabelle 132. Attribute der Data-at-Rest-Verschlüsselung (fortgesetzt)

Attribut	Beschreibung
	<ul style="list-style-type: none"> • Locking Disabled– Die selbstverschlüsselnde Festplatte ist nicht aktiviert. • Unsupported– Die selbstverschlüsselnde Festplatte wird vom Storage-System nicht unterstützt. <p>i ANMERKUNG: Sobald diese Option aktiviert ist, kann das Storage-System mit externen Key-Managementservern interagieren, die für das Key-Management im Zusammenhang mit Data-at-Rest-Verschlüsselung KMIP-konform sind.</p>

Anzeigen der Einstellungen der Data-at-Rest-Verschlüsselung (nur physische Bereitstellungen)

Zeigen Sie die Einstellungen der Data-at-Rest-Verschlüsselung an.

Format

```
/prot/encrypt show
```

Beispiel

Mit dem folgenden Befehl werden die Einstellungen der Data-at-Rest-Verschlüsselung im System aufgelistet:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/encrypt show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1: Encryption mode           = Controller Based Encryption
   Encryption status         = Encrypted
   Percent encrypted         = 100.00%
   Backup keystore status    = Backup keystore operation complete
   KMIP status               = Enabled
   SED status                = Locking enabled
```

Ändern der Verschlüsselungseinstellung für KMIP-Support (nur physische Bereitstellungen)

Wenn Verschlüsselung und KMIP-Support aktiviert sind, interagiert das Speichersystem mit externen Key-Managementservern, die KMIP-konform für das Key-Management im Zusammenhang mit der Funktion Data-at-Rest-Verschlüsselung sind. Wenn Verschlüsselung aktiviert und KMIP-Support deaktiviert ist, interagiert das Speichersystem mit einem internen Key-Management-Server für das Key-Management.

Format

```
/prot/encrypt set -kmipEnabled {yes | no}
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-kmipEnabled	Gibt an, ob KMIP-Support aktiviert oder deaktiviert werden soll. Gültige Werte:

Qualifizierer	Beschreibung
	<ul style="list-style-type: none"> • yes • no

Beispiel

Der folgende Befehl ändert die Verschlüsselungseinstellung so, dass KMIP-Support aktiviert ist:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/encrypt set -kmipEnabled yes
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
Operation completed successfully.
```

Managen von KMIP-Support (nur physische Bereitstellungen)

KMIP-Serverkonfiguration des Speichersystems

Tabelle 133. KMIP-Attribute

Attribut	Beschreibung
ID	Kennung des KMIP-Servers
Username	Benutzername für den Zugriff auf den KMIP-Server
Password	Passwort für den Zugriff auf den KMIP-Server
Port	Portnummer für den Aufbau einer Verbindung zu einem KMIP-Server
Timeout	Zeitdauer für den Aufbau einer Verbindung zu einem KMIP-Server. Falls das System vor der angegebenen Zeitüberschreitung keine Antwort vom KMIP-Server empfängt, werden keine weiteren Anforderungen gesendet.
Address	Eine Liste der KMIP-Serveradressen, die durch ein Komma getrennt werden. IP-Adressen und FQDN-Hostnamen werden unterstützt. Das System verwendet die Adressen in der Reihenfolge von links nach rechts. ANMERKUNG: Wenn eine der KMIP-Serveradressen als FQDN-Hostname konfiguriert oder geändert wurde, muss ein DNS-Server auf dem Storage-System konfiguriert werden.
State	Eine kommagetrennte Liste von KMIP-Serverzuständen (oben, unten, unbekannt).

Anzeigen von KMIP-Einstellungen (nur physische Bereitstellungen)

Zeigen Sie Einstellungen für KMIP-Support an.

Format

```
/prot/encrypt/kmip show
```

Beispiel

Mit dem folgenden Befehl werden die Einstellungen der Data-at-Rest-Verschlüsselung im System aufgelistet:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/encrypt/kmip show
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection
```

```
1:   ID           = kmip_0  
    Username    = admin  
    Address     = 10.245.95.125  
    Port        = 5696  
    Timeout     = 300  
    State       = Up
```

Ändern der Einstellungen für KMIP-Support (nur physische Bereitstellungen)

Ändern Sie die Parameter des Key-Management-Servers in Bezug auf den KMIP-Support.

Format

```
/prot/encrypt/kmip set [-username <value>] [{-passwd <value> | -passwdSecure}] [-port <value>]  
[-timeout <value>] [-addr <value>]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-username	Geben Sie den für den Zugriff auf den KMIP-Server zu verwendenden Benutzernamen an.
-passwd	Geben Sie das für den Zugriff auf den KMIP-Server zu verwendende Passwort an.
-passwdSecure	Geben Sie das Passwort im sicheren Modus an – der Benutzer wird aufgefordert, das Passwort und die Passwortbestätigung einzugeben.
-port	Geben Sie die vom KMIP-Server für die KMIP-Kommunikation verwendete Portnummer an. Der Standardwert ist 5.696.
-timeout	Geben Sie das Timeout für den KMIP-Server in Sekunden an. Falls das System nach der angegebenen Zeitüberschreitung keine Antwort vom KMIP-Server empfängt, werden keine weiteren Anforderungen gesendet. Der Standardwert ist 30 Sekunden.
-addr	Geben Sie eine Liste der KMIP-Serveradressen an, die als Standardadressen festgelegt werden sollen. Trennen Sie die Adressen mit Komma voneinander ab. IP-Adressen und FQDN-Hostnamen werden unterstützt. Die Adressen werden vom System in der eingegebenen Reihenfolge verwendet.

ANMERKUNG: Jeder Anbieter von Key-Management-Servern kann unterschiedliche Authentifizierungsanforderungen verwenden, die möglicherweise einen Nutzernamen oder ein Kennwort oder beides benötigen. Beispiele:

- Für Gemalto sind Nutzernamen und Kennwort optional und in der Regel für die Client-Authentifizierung erforderlich.
- Für Unbound sind Nutzernamen und Kennwort optional und in der Regel für die Client-Authentifizierung erforderlich.
- Für Thales CipherTrust oder Vormetric sollte kein Nutzernamen oder Kennwort angegeben werden. Die Clientauthentifizierung verwendet das Client-Zertifikat des Unity-Systems.
- Für IBM SKLM ist der Nutzernamen die KMIP-Geräte-ID. Es sollte kein Kennwort angegeben werden.
- Für CloudLink werden ein Nutzernamen und ein Kennwort benötigt.

Nutzernamen- und Kennwort-Einträge sind immer noch bei der Erstellung erforderlich, aber der entsprechende Eintrag sollte leer ("") sein, wenn kein Wert für ihn angegeben werden soll.

Beispiel

Mit dem folgenden Befehl werden die KMIP-Transporteinstellungen geändert:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/encrypt/kmip set -username skoobee  
-passwd doobee -port 5696 -timeout 20 -addr 10.245.95.125
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection  
  
Operation completed successfully.
```

Überprüfen von KMIP-Einstellungen (nur physische Bereitstellungen)

Prüfen Sie die aktuelle Verbindung mit dem KMIP-Server.

Format

```
/prot/encrypt/kmip verify
```

Beispiel

Der folgende Befehl prüft die Verbindung zum KMIP-Server:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/encrypt/kmip verify
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection  
  
Operation completed successfully.
```

Datenmobilität

Themen:

- Managen von VNX-Importsitzungen
- Managen von VNX-Importsitzungen für Block
- Managen von VNX-Importsitzungen für File
- Anzeigen von Importsitzungselementen
- Verwalten generischer Blockressourcen-Importsitzungen
- Common-Base-Snapshots
- Managen von LUN-Verschiebungssitzungen

Managen von VNX-Importsitzungen

Eine VNX-Importsitzung (Migrationssitzung) wird verwendet, um Daten aus einem VNX1- oder VNX2-Speichersystem (Quelle) zu einem Unity-Remotespeichersystem (Ziel) zu importieren. Zwei Typen von VNX-Importen sind verfügbar:

- Virtual Data Mover (VDM) und der zugehörige Dateisystemimport
- Block-LUN-Import oder Import von Consistency Group (CG) mit LUNs

Die einzelnen Importsitzungen verfügen über eigene IDs. In der Unisphere-Onlinehilfe finden Sie weitere Informationen zum Speicherimport.

i ANMERKUNG: Es wird immer nur ein Befehl in einer Importsitzung unterstützt. Bevor Sie einen neuen Befehl ausführen, warten Sie, bis die derzeitige Aktion in der Importsitzung beendet ist.

In der folgenden Tabelle sind die Attribute für Importsitzungen aufgeführt:

Tabelle 134. Attribute für Importsitzung

Attribut	Beschreibung
ID	ID der Importsitzung.
Name	Name der Importsitzung.
Session type	Typ der Importsitzung. Gültige Werte: <ul style="list-style-type: none"> • nas • block
Health state	Integritätsstatus der Importsitzung. Gültige Werte: <ul style="list-style-type: none"> • Unknown (0): Die Remotesystemintegrität kann nicht bestimmt werden. • OK (5): Die Sitzung funktioniert normal. • OK BUT (7): Die Sitzung hat einen der folgenden Status: <ul style="list-style-type: none"> ○ Sitzung initialisiert, aber angehalten. ○ Sitzung angehalten, um Daten in ursprüngliche Kopie zu migrieren. ○ Sitzung angehalten, um Daten in inkrementelle Kopie zu synchronisieren. • Degraded/Warning (10): Die Sitzung ist aus einem der folgenden Gründe fehlgeschlagen: <ul style="list-style-type: none"> ○ Sitzung konnte einige Quelldateien nicht lesen. ○ Sitzung konnte Datei nicht von der Quelle zum Ziel kopieren. • Minor failure (15): Die Sitzung ist aus einem der unter Gründe für geringfügige Fehler in Importsitzung aufgeführten Gründe fehlgeschlagen. • Non-recoverable failure (30): Durch einen Fehler ist mindestens eines der folgenden Ereignisse eingetreten: <ul style="list-style-type: none"> ○ Die Sitzung ist fehlgeschlagen.

Tabelle 134. Attribute für Importsitzung (fortgesetzt)

Attribut	Beschreibung
	<ul style="list-style-type: none"> ○ Die Sitzung ist aufgrund eines nicht behebbaren Fehlers in der ursprünglichen Kopie fehlgeschlagen. ○ Die Sitzung ist aufgrund eines nicht behebbaren Fehlers in der inkrementellen Kopie fehlgeschlagen.
Health details	Zusätzliche Integritätsinformationen. Weitere Einzelheiten finden Sie in Anhang A, Referenz.
State	Status der Importsitzung. Gültige Werte: <ul style="list-style-type: none"> ● Initialized ● Initial copy ● Ready to cutover ● Paused ● Cutting over ● Incremental copy ● Ready to commit ● Committing ● Completed ● Cancelling ● Cancelled ● Pending ● Syncing
Progress	Fortschritt der Importsitzung. Nur unterstützt für NAS-Import.
Source system	Kennung des Remotesystems für Quellsystem.
Source resource	Kennung der Quellressource.
Target resource	Kennung der Zielressource. Initialisierter Status: leer. Andere Statusangaben: Kennung der Zielressource.

Tabelle 135. Gründe für geringfügige Fehler in Importsitzung

Gründe
Sitzung konnte keine Zielressource bereitstellen.
Sitzung konnte keine Daten in die ursprüngliche Kopie migrieren.
Sitzung konnte keine Daten in die ursprüngliche Kopie migrieren und wurde angehalten.
Sitzung konnte aufgrund von Verbindungsfehler keine Daten in die ursprüngliche Kopie migrieren.
Sitzung konnte aufgrund von Verbindungsfehler keine Daten in die ursprüngliche Kopie migrieren und wurde angehalten.
Sitzung konnte aufgrund von I/O-Quellfehler keine Daten in die ursprüngliche Kopie migrieren.
Sitzung konnte aufgrund von I/O-Quellfehler keine Daten in die ursprüngliche Kopie migrieren und wurde angehalten.
Sitzung konnte aufgrund von I/O-Zielfehler keine Daten in die ursprüngliche Kopie migrieren.
Sitzung konnte aufgrund von I/O-Zielfehler keine Daten in die ursprüngliche Kopie migrieren und wurde angehalten.
Sitzung konnte keine Daten in inkrementelle Kopie synchronisieren.
Sitzung konnte keine Daten in inkrementelle Kopie synchronisieren und wurde angehalten.
Sitzung konnte aufgrund von Verbindungsfehler keine Daten in die inkrementelle Kopie synchronisieren.
Sitzung konnte aufgrund von Verbindungsfehler keine Daten in die inkrementelle Kopie synchronisieren und wurde angehalten.
Sitzung konnte aufgrund von I/O-Quellfehler keine Daten in die inkrementelle Kopie synchronisieren.
Sitzung konnte aufgrund von I/O-Quellfehler keine Daten in die inkrementelle Kopie synchronisieren und wurde angehalten.
Sitzung konnte aufgrund von I/O-Zielfehler keine Daten in die inkrementelle Kopie synchronisieren.

Tabelle 135. Gründe für geringfügige Fehler in Importsitzung (fortgesetzt)

Gründe
Sitzung konnte aufgrund von I/O-Zielfehler keine Daten in die inkrementelle Kopie synchronisieren und wurde angehalten.
Sitzung konnte Commit-Vorgang nicht ausführen.
Sitzung konnte Abbruchvorgang nicht ausführen.
Sitzungssynchronisierung fehlgeschlagen.
Sitzungssynchronisierung aufgrund des Kopiervorgangs von Quelle zu Ziel fehlgeschlagen.
Sitzung konnte Umstellung nicht ausführen.
Sitzung konnte Konfiguration nicht ausführen.
Sitzung ist aufgrund eines Datenfehlers fehlgeschlagen.
Sitzung ist aufgrund eines Verbindungsfehlers fehlgeschlagen.
Sitzung konnte Startvorgang nicht ausführen.

Anzeigen von Importsitzungen

Zeigen Sie Details zu vorhandenen Importsitzungen für File und Block an. Sie können nach der Sitzungs-ID filtern.

Format

```
/import/session [-id <value> | -active | -completed | -cancelled] [-type {block | nas}] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID der Importsitzung ein.
-active	Zeigen Sie nur aktive Sitzungen (Sitzungen, die nicht abgeschlossen oder abgebrochen wurden) an.
-completed	Zeigen Sie nur abgeschlossene Sitzungen an.
-cancelled	Zeigen Sie nur abgebrochene Sitzungen an.
-type	Gibt an, welche Art von Sitzungen angezeigt werden soll. Gültige Werte: <ul style="list-style-type: none"> • block • nas

Beispiel

Mit dem folgenden Befehl werden alle vorhandenen Dateiimportsitzungen auf dem System angezeigt.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /import/session show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      ID                = import_1
      Name                = import_sess_vdm1_BB0050562C7D2A_FCNC0972C330D
      Session type        = nas
      Health state        = OK (5)
      Health details      = "The component is
operating normally. No action is required."
      State                = Initialized
      Progress            = empty
```

```

Source system          = RS_65535
Source resource       = vdm1
Target resource       = nas_1

2: ID                  = import_2
   Name                = VNX LUN Group 1 import
   Session type       = block
   Health state       = OK (5)
   Health details     = "The component is
operating normally. No action is required."
   State              = Initial copy
   Progress           =
   Source system      = RS_65535
   Source resource    = LUNGroup1
   Target resource    = res_1

```

Managen von VNX-Importsitzungen für Block

Ein Block-VNX-Import ist der Prozess, bei dem Block-LUNs oder LUN-Gruppen aus einem VNX1/VNX2-Speichersystem (Quelle) in ein Unity-Remotespeichersystem (Ziel) importiert werden. Beim Block-VNX-Import wird die SAN Copy-Funktion genutzt, die aktiviert und auf dem Quellsystem konfiguriert sein muss.

Die einzelnen Blockimportsitzungen verfügen über eigene IDs. In der Unisphere-Onlinehilfe finden Sie weitere Informationen zum Import von Blockspeicher.

ANMERKUNG: Es wird immer nur ein Befehl in einer Blockimportsitzung unterstützt. Bevor Sie einen neuen Befehl ausführen, warten Sie, bis die derzeitige Aktion in der Blockimportsitzung beendet ist.

In der folgenden Tabelle werden die Attribute in Bezug auf Blockimportsitzungen aufgelistet:

Tabelle 136. Attribute für Blockimportsitzung

Attribut	Beschreibung
ID	ID der Blockimportsitzung.
Name	Name der Blockimportsitzung.
Health state	<p>Integritätsstatus der Blockimportsitzung. Gültige Werte:</p> <ul style="list-style-type: none"> • Unknown (0): Die Remotesystemintegrität kann nicht bestimmt werden. • OK (5): Die Sitzung funktioniert normal. • OK BUT (7): Die Sitzung hat einen der folgenden Status: <ul style="list-style-type: none"> ○ Sitzung initialisiert, aber angehalten. ○ Sitzung angehalten, um Daten in ursprüngliche Kopie zu migrieren. ○ Sitzung angehalten, um Daten in inkrementelle Kopie zu synchronisieren. • Degraded/warning (10): Die Sitzung ist aus einem der folgenden Gründe fehlgeschlagen: <ul style="list-style-type: none"> ○ Sitzung konnte einige Quelldateien nicht lesen. ○ Sitzung konnte Datei nicht von der Quelle zum Ziel kopieren. • Minor failure (15): Die Sitzung ist aus einem der unter Gründe für geringfügige Fehler in Importsitzung aufgeführten Gründe fehlgeschlagen. • Non-recoverable error (30): Durch einen Fehler ist mindestens eines der folgenden Ereignisse eingetreten: <ul style="list-style-type: none"> ○ Die Sitzung ist fehlgeschlagen. ○ Die Sitzung ist aufgrund eines nicht behebbaren Fehlers in der ursprünglichen Kopie fehlgeschlagen. ○ Die Sitzung ist aufgrund eines nicht behebbaren Fehlers in der inkrementellen Kopie fehlgeschlagen. <p>ANMERKUNG: Wenn die Migrationssitzung fehlerhaft ist, kann sie nicht wiederhergestellt werden. Sie müssen die Sitzung löschen und anschließend neu erstellen.</p>
Health details	Zusätzliche Integritätsinformationen. Weitere Einzelheiten finden Sie in Anhang A, Referenz.
State	Status der Blockimportsitzung. Gültige Werte:

Tabelle 136. Attribute für Blockimportsitzung (fortgesetzt)

Attribut	Beschreibung
	<ul style="list-style-type: none"> • Pending • Syncing • Paused • Ready to cutover • Cancelling • Cancelled
Progress	Fortschritt der Blockimportsitzung.
Source system	Kennung des Remotesystems für Quellsystem.
Source resource	Kennung der Quellressource.
Target resource	Kennung der Zielressource.
Estimated remaining bytes	Gibt die aktuell geschätzten verbleibenden Byte an, die für die aktuelle Importphase übertragen werden. Nur unterstützt für Blockimport.
Percent remaining for import	Gibt den Prozentsatz der verbleibenden zu importierenden Byte im Vergleich zur Gesamtgröße der Importressource an.
Cutover threshold percentage	Wenn Percent remaining for import unter diesem Schwellenwert liegt, ändert sich der Status der Importsitzung in Ready to cutover.
Throttle	Gibt an, ob die Importübertragung gedrosselt werden soll. Wenn die Drosselung angewendet wird, wird die Datenübertragungsrate der Importsitzung gedrosselt, um Auswirkungen auf I/O-Hostvorgänge zu minimieren. Wenn die Drosselung deaktiviert ist, funktioniert die Importsitzung in voller Geschwindigkeit, was die I/O-Hostlatenz beeinträchtigen könnte. Gültige Werte: <ul style="list-style-type: none"> • yes • no

Erstellen einer Blockimportsitzung

Voraussetzungen

Erledigen Sie vor der Erstellung einer Blockimportsitzung die folgenden Konfigurationsaufgaben:

- Erstellen Sie Schnittstellen auf Quelle und Ziel für die Datenübertragung.
- Erstellen Sie eine Importverbindung zu einem Unity-basierten Zielsystem.
- Erstellen Sie ein Blockimportziel (LUN oder LUN-Gruppe) auf dem Zielsystem.

Format

```
/import/session/block create [-async] [-name <value>] [-throttle {yes | no}] -srcSys
<value> -srcRes <value> -lunPoolPairs <value> [-cutoverThreshold <value>] [-hosts <value>] [-
importAsVMwareDatastore {yes | no}]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie die Aktion im asynchronen Modus aus.
-name	Gibt den Namen der Importsitzung an.  ANMERKUNG: Wenn kein Name angegeben wird, wird er nach folgendem Muster erzeugt:

Qualifizierer	Beschreibung
	<code>import_sess_<srcRes>_<srcSysSerialNumber>_<targetSysSerialNumber>[_<index>]</code>
<code>-throttle</code>	Gibt an, ob die Importübertragung gedrosselt werden soll. Eine Drosselung wirkt sich auf die Importgeschwindigkeit und die Hostlatenz für die zugehörigen LUNs und Dateisysteme aus, die auf den Quell- und Zielspeichersystemen verwendet werden. Gültige Werte: <ul style="list-style-type: none"> • yes • no <p>i ANMERKUNG: Standardmäßig wird die Importübertragung gedrosselt, was bedeutet, dass sie auf einen Wert gedrosselt wird, der unter der vollen Geschwindigkeit liegt.</p>
<code>-srcSys</code>	Gibt das Quellsystem an.
<code>-srcRes</code>	Gibt die Quellressource an.
<code>-lunPoolPairs</code>	Gibt die LUN-Poolpaare an. Eine kommasetrennte Liste von Zuordnungen zwischen der Quell-LUN und der Zielspeicherkonfiguration. <p>i ANMERKUNG: Verwenden Sie das Format srcLUN1: tgtPool1, ..., Ziel-LUNs haben dieselben Eigenschaften wie die Quell-LUNs, z. B. Name, IsThin, SP und Größe.</p>
<code>-cutoverThreshold</code>	Der Schwellenwertprozentsatz, unter dem die Importsitzung für die Umstellung bereit ist.
<code>-hosts</code>	Gibt die Hosts an. Eine kommasetrennte Liste geeigneter Host-IDs für Zugriff auf Zielelemente.
<code>-importAsVMwareDatastore</code>	Gibt an, ob die Quell-LUN als ein VMware-Datenspeicher (VMFS) importiert werden soll. Diese Option gilt nur für eine LUN-Sitzung und nicht für eine CG-Sitzung. Gültige Werte: <ul style="list-style-type: none"> • yes • no

Beispiel

Mit dem folgenden Befehl wird eine Importsitzung mit den folgenden Einstellungen erstellt:

- Der Name der Importsitzung lautet `lun_17_import`.
- Das Quellspeichersystem ist `RS_1`.
- Die Quellspeicherressource ist `17`.
- Das LUN-Poolpaar ist `17:pool_1`.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! import/session/block create -name
lun_17_import -srcSys RS_65596 -srcRes 17 -lunPoolPairs 17:pool_1 -importAsVMwareDatastore yes
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = import_1
Operation completed successfully.
```

Änderung der Importsitzungseinstellungen für Block

Ändern Sie die Einstellungen für Blockimportsitzungen.

Format

```
/import/session/block -id <value> set [-async] [-name <value>] [-paused {yes | no}] [-throttle
{yes | no}] [-cutoverThreshold <value>]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID der Importsitzung ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie die Aktion im asynchronen Modus aus.
-name	Gibt den neuen Namen der Importsitzung an.
-throttle	Gibt an, ob die Importübertragung gedrosselt werden soll. Eine Drosselung wirkt sich auf die Importgeschwindigkeit und die Hostlatenz für die zugehörigen LUNs und Dateisysteme aus, die auf den Quell- und Zielspeichersystemen verwendet werden. Gültige Werte: <ul style="list-style-type: none">• yes• no  ANMERKUNG: Standardmäßig wird die Importübertragung gedrosselt, was bedeutet, dass sie auf einen Wert gedrosselt wird, der unter der vollen Geschwindigkeit liegt.
-paused	Gibt an, ob die Importsitzung angehalten werden soll. Gültige Werte: <ul style="list-style-type: none">• yes• no  ANMERKUNG: no Startet oder setzt die Importsitzung fort.
-cutoverThreshold	Gibt den Schwellenwertprozentsatz an, unter dem die Importsitzung für die Umstellung bereit ist.

Beispiel

Mit dem folgenden Befehl werden die Einstellungen für die Blockimportsitzung von „name“ auf „newName“ festgelegt, das Level für „cutoverThreshold“ wird auf 5 festgelegt und es wird keine Drosselung angewendet:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /import/session/block -id import_1 set -name newName -throttle no -cutoverThreshold 5
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
Operation completed successfully.
```

Umstellung von Importsitzungen für Block

Stellen Sie eine vorhandene Blockimportsitzung um und schließen Sie sie ab. Die Umstellung einer Blockimportsitzung kann lange dauern und zu einer Betriebsunterbrechung führen. Um den Zeitraum der Unterbrechung zu reduzieren, legen Sie den Schwellenwert für die Umstellung so niedrig wie möglich fest. Durch die Reduzierung des Schwellenwerts für die Umstellung auf einen niedrigen Wert muss eine kleinere Anzahl von Änderungen übertragen werden, nachdem die Anwendung in den Ruhezustand versetzt wurde. Der Schwellenwert für die Umstellung ist ein Prozentsatz der LUN-Größe. Daher wird für größere LUNs empfohlen, dass der Schwellenwert für die Umstellung auf einen Wert festgelegt wird, der kleiner als der Standardwert von 5 % ist. Die Umstellung einer Importsitzung sollte zudem nur durchgeführt werden, wenn die Sitzung sich im Status „Bereit für Umstellung“ befindet. Dadurch wird sichergestellt, dass die Umstellung durchgeführt wird, wenn die geringste Anzahl von Änderungen übertragen werden muss.

Nach erfolgreicher Umstellung werden Host-I/Os auf die Zielseite umgestellt und der Importvorgang wird automatisch abgeschlossen.

Format

```
/import/session/block -id <value> cutover [-async]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID der Importsitzung ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie die Aktion im asynchronen Modus aus.

Beispiel

Mit dem folgenden Befehl wird die Importsitzung import_1 auf das Zielsystem umgestellt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /import/session/block -id import_1 cutover
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection
```

```
Operation completed successfully.
```

Abbrechen einer Blockimportsitzung

Brechen Sie eine vorhandene Blockimportsitzung ab.

Format

```
/import/session/block -id <value> cancel [-async]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID der Importsitzung ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie die Aktion im asynchronen Modus aus.

Beispiel

Mit dem folgenden Befehl wird die Blockimportsitzung import_1 abgebrochen.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /import/session/block -id import_1 cancel
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection  
  
Operation completed successfully.
```

Anzeigen von Importsitzungen für Block

Zeigen Sie Details zu Importsitzungen für Block an. Sie können nach der Sitzungs-ID filtern.

Format

```
/import/session/block [{-id <value> | -active | -completed | -cancelled}] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID der Importsitzung ein.
-active	Zeigen Sie nur aktive Sitzungen (Sitzungen, die nicht abgeschlossen oder abgebrochen wurden) an.
-completed	Zeigen Sie nur abgeschlossene Sitzungen an.
-cancelled	Zeigen Sie nur abgebrochene Sitzungen an.

Beispiel

Mit dem folgenden Befehl werden Blockimportsitzungen auf dem System angezeigt.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /import/session/block show -detail
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection  
  
1:      ID                = import_2  
      Name                = VNX LUN Group 1 import  
      Session type        = block  
      Health state         = OK (5)  
      Health details       = "This import session  
is operating normally. No action is required."  
      State                = Syncing  
      Progress             = 0%  
      Source system        = RS_65535  
      Source resource       = LUNGroup1  
      Target resource       = res_1  
      Estimated remaining bytes = 47185920 (45 M)  
      Percent remaining for import = 6  
      Cutover threshold percent = 5  
      Throttle             = no
```

Managen von VNX-Importsitzungen für File

Ein Virtual Data Mover (VDM)-Dateiimport ist der Prozess, bei dem ein VDM auf einem VNX1- oder VNX2-Speichersystem (Quelle) auf ein Unity-Remotespeichersystem (Ziel) importiert wird. Die Dateisysteme (gemeinsames oder geteiltes Protokoll) des VDM werden in UFS64-Dateisysteme auf dem Zielspeichersystem importiert.

Die einzelnen Dateiimportsitzungen verfügen über eigene IDs. In der Unisphere-Onlinehilfe finden Sie weitere Informationen zum Import von VDM-Dateispeicher.

ANMERKUNG: Es wird immer nur ein Befehl in einer Dateiimportsitzung unterstützt. Bevor Sie einen neuen Befehl ausführen, warten Sie, bis die derzeitige Aktion in der Dateiimportsitzung beendet ist.

In der folgenden Tabelle sind die Attribute für Dateiimportsitzungen aufgeführt:

Tabelle 137. Attribute für Dateiimportsitzung

Attribut	Beschreibung
ID	ID der Dateiimportsitzung.
Name	Name der Dateiimportsitzung.
Health state	<p>Integritätsstatus der Importsitzung. Gültige Werte:</p> <ul style="list-style-type: none"> ● Unknown (0): Die Remotesystemintegrität kann nicht bestimmt werden. ● OK (5): Die Sitzung funktioniert normal. ● OK BUT (7): Die Sitzung hat einen der folgenden Status: <ul style="list-style-type: none"> ○ Sitzung initialisiert, aber angehalten. ○ Sitzung angehalten, um Daten in ursprüngliche Kopie zu migrieren. ○ Sitzung angehalten, um Daten in inkrementelle Kopie zu synchronisieren. ● Degraded/Warning (10): Die Sitzung ist aus einem der folgenden Gründe fehlgeschlagen: <ul style="list-style-type: none"> ○ Sitzung konnte einige Quelldateien nicht lesen. ○ Sitzung konnte Datei nicht von der Quelle zum Ziel kopieren. ● Minor failure (15): Die Sitzung ist aus einem der Gründe fehlgeschlagen, die in Gründe für geringfügige Fehler in Importsitzung aufgelistet sind. ● Non-recoverable error (30): Durch einen Fehler ist mindestens eines der folgenden Ereignisse eingetreten: <ul style="list-style-type: none"> ○ Die Sitzung ist fehlgeschlagen. ○ Die Sitzung ist aufgrund eines nicht behebbaren Fehlers in der ursprünglichen Kopie fehlgeschlagen. ○ Die Sitzung ist aufgrund eines nicht behebbaren Fehlers in der inkrementellen Kopie fehlgeschlagen. <p>ANMERKUNG: Wenn die Migrationssitzung fehlerhaft ist, kann sie nicht wiederhergestellt werden. Sie müssen die Migrationssitzung löschen und anschließend neu erstellen.</p>
Health details	Zusätzliche Integritätsinformationen. Weitere Einzelheiten finden Sie in Anhang A, Referenz.
State	<p>Status der Importsitzung des NAS-Servers. Gültige Werte:</p> <ul style="list-style-type: none"> ● Initialized ● Initial Copy ● Ready to Cutover ● Cutting Over ● Incremental Copy ● Ready to commit ● Committing ● Completed ● Cancelling ● Cancelled
Progress	Fortschritt der Importsitzung.
Source system	Kennung des Remotesystems für Quellsystem.
Source resource	Kennung der Quellressource.
Source import interface	Quellimport-Schnittstellenkennung für Datenübertragung.

Tabelle 137. Attribute für Dateimportsitzung (fortgesetzt)

Attribut	Beschreibung
Source file systems imported as VMWare datastore	Quelldateisysteme, die als VMware-Datenspeicher importiert werden. Der Wert ist eine Liste der Quelldateisystem-IDs, im Format eines Bereichs (für kontinuierliche Dateisystem-IDs) oder eines durch Kommas getrennten Werts (für Dateisysteme, die verteilt sind) der Quelldateisystem-IDs. Beispiel: 13,20~25,30.
Source file systems imported with Data Reduction enabled	Quelldateisysteme, die mit aktivierter Datenreduzierung importiert werden. Der Wert ist eine Liste der Quelldateisystem-IDs, im Format eines Bereichs (für kontinuierliche Dateisystem-IDs) oder eines durch Kommas getrennten Werts (für Dateisysteme, die verteilt sind) der Quelldateisystem-IDs. Beispiel: 13,20~25,30.
Source file systems imported with advanced deduplication enabled	Quelldateisysteme, die mit aktivierter erweiterter Deduplizierung importiert werden.
Target resource	Kennung der Zielressource.
Target resource pool	Zielressource, die die Poolkennung enthält.
Target file system to pool mapping	Zielressourcen werden erst nach dem Start der Importsitzung bereitgestellt (durch Wiederaufnahme). Bevor die Zieldateisysteme bereitgestellt werden (das heißt, nach der Erstellung, aber vor dem Start), erfolgt die Zuordnung von einem Bereich (für kontinuierliche Dateisystem-IDs) oder einem durch Kommas getrennten Wert (für Dateisystem-IDs, die verteilt sind) der Quelldateisystem-IDs zu einem Zielpool. Beispiel: 24~26;pool_1; 28,33~36,40;pool_2;50,55;pool_3;78;pool_4. Nachdem alle Zieldateisysteme bereitgestellt wurden (das heißt, nach dem Start der Sitzung), erfolgt die Zuordnung von einem Bereich (für kontinuierliche Dateisystem-IDs) oder einem durch Kommas getrennten Wert (für Dateisystem-IDs, die verteilt sind) der Zieldateisystem-IDs zu einem Zielpool. Beispiel: res_1~res_3;pool_1; res_4~res_9; pool_2;res_10~res_11;pool_3;res_12;pool_4.
Target file system access policy mapping	Zeigt die Zugriffs-Policy für das Dateisystemziel an. Nur die Multiprotokoll-Sitzung zeigt den Wert, nur CIFS an und die Nur-NFS-Sitzung wird leer gelassen. Es ist eine durch Semikolons getrennte Liste von Quelldateisystem-IDs und Zugriffs-Policy-Paaren. Beispiel: "24~26: WINDOWS; 28,33~36,40: NATIVE; 50,55: UNIX"
Target import interface	Zielimport-Schnittstellenkennung für Datenübertragung.
Target default production port	Kennung des Zielproduktionsports. Standardport, auf dem Produktionsschnittstellen erstellt werden.
Target production interface to port mapping	Zielressourcen werden erst nach dem Start der Importsitzung bereitgestellt (durch Wiederaufnahme). Bevor die Zielproduktionsschnittstellen bereitgestellt werden, erfolgt die Zuordnung von einer Liste mit Quellproduktionsschnittstellen zu einem Zielport. Beispiel: if_6;if_7: spa_iom_0_eth0; if_9:spa_iom_0_eth1. Nachdem die Zielproduktionsschnittstellen bereitgestellt wurden, erfolgt die Zuordnung von einer Liste mit Zielproduktionsschnittstellen zu einem Zielport. Beispiel: if_4;if_5:spa_iom_0_eth0; if_7:port spa_iom_0_eth1.
Target production interface to VLAN mapping	Zielressourcen werden erst nach dem Start der Importsitzung bereitgestellt (durch Wiederaufnahme). Bevor die Zielproduktionsschnittstellen bereitgestellt werden, erfolgt die Zuordnung von einer Liste mit Quellproduktionsschnittstellen zu einem Ziel-VLAN. Zum Beispiel if_6: 6; if_9:9. Nachdem die Zielproduktionsschnittstellen bereitgestellt wurden, erfolgt die Zuordnung von einer Liste mit Zielproduktionsschnittstellen zu einem Ziel-VLAN. Zum Beispiel if_4:4; if_7:7.
CIFS domain username	Benutzername für die Authentifizierung an Windows-Domain
CIFS domain password	Passwort für die Authentifizierung an Windows-Domain
CIFS local administrator username	Benutzername für die Authentifizierung an SMB-Server auf dem Quell-VDM (bevor die Importsitzung gestartet wird). Dieses Benutzerkonto wird auf den Ziel-NAS-Server importiert.
CIFS local administrator password	Passwort für die Authentifizierung an SMB-Server auf dem Quell-VDM (bevor die Importsitzung gestartet wird). Dieses Benutzerkonto wird auf den Ziel-NAS-Server importiert.

Erstellen einer NAS-Importsitzung

Erstellen Sie eine NAS-Importsitzung.

i ANMERKUNG: Mit diesem Befehl wird nur der Importsitzung erstellt. Um die Importsitzung über die UEMCLI zu starten, führen Sie den Befehl `/import/session/nas set` aus und geben Sie **Nein** für den Aktionsqualifizierer `-paused` an.

Voraussetzungen

Erledigen Sie vor der Erstellung einer NAS-Importsitzung die folgenden Konfigurationsaufgaben:

- Erstellen Sie Schnittstellen auf den Quell- und Zielsystemen für die Datenübertragung.
- Erstellen Sie eine Importverbindung von dem VNX-Quellsystem zu dem aktuellen Unity-basierten Zielsystem.
- Erstellen Sie einen Zielpool.
- Wenn das VNX-Quellsystem mit der Codeseite 8859-1 oder 8859-15 für die NFSv3-Clients konfiguriert wurde, vergewissern Sie sich, dass die Codeseite für das Unity-System mit der auf dem VNX-System verwendeten Codeseite übereinstimmt. Ab Unity OE 4.3 kann die Codeseite des Unity-Systems über den Servicebefehl `svc_nas {<NAS_server_name> | all} -param -facility vdm -modify codepage -value <value>` geändert werden.

Format

```
/import/session/nas create [-async] [-name <value>] -srcSys <value> -srcRes <value>
-targetResPool <value> [-targetImportIf <value>] [-productionIfPortPairs <value>] [-
productionIfVlanPairs <value>] -fsPoolPairs <value>] -defaultProductionPort <value>
[-srcDhsmUsername <value>] [-srcDhsmPasswd <value>] [-srcDhsmPasswdSecure <value>] [-
unixDirectoryService {directMatch | local | nis | ldap |localThenNis |
localThenLdap | none}] [-srcLocalCifsAdminUsername <value> {-srcLocalCifsAdminPasswd
<value>|-srcLocalCifsAdminPasswdSecure}] [-srcFsImportedAsVMWareDatastore <value>] [-
srcFsImportedWithDataReductionEnabled <value>] [-srcFsImportedWithAdvancedDedupEnabled <value>]
[-skipServerParamCheck]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	(Optional) Führen Sie den Vorgang im asynchronen Modus aus.
-name	(Optional) Gibt den neuen Namen der Importsitzung an. i ANMERKUNG: Wenn kein Name angegeben wird, wird er nach folgendem Muster erzeugt. <code>import_sess_<srcRes>_<srcSysSerialNumber>_<targetSysSerialNumber>[_<index>]</code>
-srcSys	Gibt das Quellsystem (remote) an.
-srcRes	Gibt die Quellressource an.
-targetResPool	Gibt den Standardspeicherpool an, um die Konfigurationsinformationen und Dateisysteme des NAS-Zielservers zu speichern.
-targetImportIf	(Optional) Gibt die Zielreplikationsschnittstelle für die Importsitzung an.
-productionIfPortPairs	(Optional) Gibt die Quell-VDM-Produktionsschnittstellen und die Zielportpaare an. Werte sind kommagetrennte Listen von Zuordnungen zwischen Quell-VDM-Produktionsschnittstellen und Zielports. i ANMERKUNG: Verwenden Sie das folgende Format: <code>source_interface_1:dest_port_1</code> <code>source_interface_2:dest_port_2</code>

Qualifizierer	Beschreibung
-productionIfVlanPairs	(Optional) Gibt die Quell-VDM-Produktionsschnittstellen und die Ziel-VLAN-Paare an. Werte sind durch Kommas getrennte Listen von Zuordnungen zwischen Quell-VDM-Produktionsschnittstellen und Ziel-VLAN-Paaren. <i>i</i> ANMERKUNG: Verwenden Sie das folgende Format: source_interface_1:1,source_interface_2:2
-fsPoolPairs	(Optional) Gibt die Quelldateisystem-IDs und die Zielpoolpaare an. Werte sind kommagetrennte Listen von Zuordnungen zwischen Dateisystem-IDs und Zielpoolpaaren. <i>i</i> ANMERKUNG: Verwenden Sie das Format sourceFsId1: destination_pool_friendlyId (sourceFsId muss eine vorhandene unterstützte Quelldateisystem-ID sein, andernfalls schlägt die Validierung fehl) oder sourceFsId2 ~ sourceFsId3: destination_pool_friendlyId (sourceFsId2 und sourceFsId3 müssen bestehende unterstützte Quelldateisystem-IDs sein. Die anderen Dateisystem-IDs zwischen sourceFsId2 und sourceFsId3 müssen nicht unbedingt vorhanden sein. Beim Erstellen werden nur vorhandene Quelldateisystem-IDs verwendet. Nicht vorhandene Dateisystem-IDs im Bereich werden übersprungen. Bei der Eingabe 12:pool_1,15~20:pool_2 müssen Quelldateisystem-IDs mit 12, 15 und 20 beispielsweise vorhanden sein, aber Quelldateisysteme, die mit 16 bis 19 beginnen, müssen nicht vorhanden sind.
-defaultProductionPort	Gibt den Zielport an, auf dem NAS-Serverproduktionsschnittstellen standardmäßig erstellt werden.
-srcDhsmUsername	Gibt den Nutzernamen für die Authentifizierung beim DHSM-Service auf dem Quell-Data Mover an. <i>i</i> ANMERKUNG: Wenn der Quell-VDM über FLR-E/C-Dateisysteme verfügt, muss der Dateimport eine Verbindung mit dem DHSM-Service auf dem Quell-Data Mover herstellen. Wenn der DHSM-Service mit Basic- oder Digest-Authentifizierung konfiguriert ist, muss der Nutzernamen angegeben werden.
-srcDhsmPasswd	Gibt das Passwort für die Authentifizierung beim DHSM-Service auf dem Quell-Data Mover an.
-srcDhsmPasswdSecure	Gibt das Passwort für die Authentifizierung beim DHSM-Service auf dem Quell-Data Mover im sicheren Modus an. <i>i</i> ANMERKUNG: Der Benutzer wird aufgefordert, das Passwort einzugeben und zu bestätigen.
-unixDirectoryService	(Optional) Gibt an, welcher UNIX-Verzeichnisdienst importiert werden soll. Verzeichnisdienst wird für die Abfrage von Identitätsinformationen für UNIX verwendet (wie etwa UIDs, GIDs, Netzgruppen). Gültige Werte: <ul style="list-style-type: none"> • directMatch : Importiert Quell-UnixDirectoryService zum Ziel ohne jegliche Änderung. • local : Verwendet lokale Dateien (passwd, group, hosts, netgroup) zum Abfragen von Identitätsinformationen für UNIX. • nis : Verwendet NIS zum Abfragen von Identitätsinformationen für UNIX. • ldap : Verwendet LDAP zum Abfragen von Identitätsinformationen für UNIX. • localThinNis : Verwendet lokale Dateien und dann NIS zum Abfragen von Identitätsinformationen für UNIX. • localThinLdap : Verwendet lokale Dateien und dann LDAP zum Abfragen von Identitätsinformationen für UNIX. • none : Verwendet keinen der UNIX-Verzeichnisservices.
-srcLocalCifsAdminUsername	(Optional) Gibt den Nutzernamen für die Authentifizierung auf dem CIFS-Server auf dem Quell-VDM an.
-srcLocalCifsAdminPasswd	(Optional) Gibt das Passwort für die Authentifizierung auf dem CIFS-Server auf dem Quell-VDM an.
-srcLocalCifsAdminPasswd Secure	(Optional) Gibt ein Passwort im sicheren Modus an.

Qualifizierer	Beschreibung
	<p> ANMERKUNG: Der Benutzer wird aufgefordert, das Passwort einzugeben und zu bestätigen.</p>
-srcFsImportedAsVMWareDatastore	<p>(Optional) Gibt an, welche Quelldateisysteme als VMware-Datenspeicherdateisysteme importiert werden. Werte sind eine durch Kommas getrennte Liste von Quelldateisystem-IDs mit durch Komma getrenntem Wert einer einzelnen Dateisystem-ID oder eines Bereichs von Dateisystem-IDs, beispielsweise sourceFsId1 , sourceFsId2~sourceFsId3. sourceFsId1, sourceFsId2 und sourceFsId3 müssen vorhandene, unterstützte Quelldateisystem-IDs sein. Die Quelldateisysteme mit IDs zwischen sourceFsId2 und sourceFsId3 müssen nicht unbedingt vorhanden sein. Beim Erstellen werden nur vorhandene Quelldateisystem-IDs verwendet. Nicht vorhandene Dateisysteme im Bereich werden übersprungen. Wenn beispielsweise 13,15~20,25 eingegeben wird, müssen Quelldateisysteme mit IDs 13,15,20 und 25 vorhanden sein. Quelldateisysteme mit IDs von 16 bis 19 müssen jedoch nicht vorhanden sein.</p> <p> ANMERKUNG: Wenn ein VNX-Dateisystem durch diese Option angegeben wird, sollte es keine Struktur-Quotas oder Benutzer-Quotas enthalten.</p>
-srcFsImportedWithDataReductionEnabled	<p>(Optional) Gibt an, welche Quelldateisysteme mit aktivierter Datenreduzierung importiert werden. Werte sind eine durch Kommas getrennte Liste von Quelldateisystem-IDs mit durch Komma getrenntem Wert einer einzelnen Dateisystem-ID oder eines Bereichs von Dateisystem-IDs, beispielsweise sourceFsId1 , sourceFsId2~sourceFsId3. sourceFsId1, sourceFsId2 und sourceFsId3 müssen vorhandene, unterstützte Quelldateisystem-IDs sein. Die Quelldateisysteme mit IDs zwischen sourceFsId2 und sourceFsId3 müssen nicht unbedingt vorhanden sein. Beim Erstellen werden nur vorhandene Quelldateisystem-IDs verwendet. Nicht vorhandene Dateisysteme im Bereich werden übersprungen. Wenn beispielsweise 13,15~20,25 eingegeben wird, müssen Quelldateisysteme mit IDs 13,15,20 und 25 vorhanden sein. Quelldateisysteme mit IDs von 16 bis 19 müssen jedoch nicht vorhanden sein.</p>
-srcFsImportedWithAdvancedDedupEnabled	<p>(Optional) Gibt an, welche Quelldateisysteme mit aktivierter erweiterter Deduplizierung importiert werden. Werte sind eine durch Kommas getrennte Liste von Quelldateisystem-IDs mit durch Komma getrenntem Wert einer einzelnen Dateisystem-ID oder eines Bereichs von Dateisystem-IDs, beispielsweise sourceFsId1 , sourceFsId2~sourceFsId3. sourceFsId1, sourceFsId2 und sourceFsId3 müssen vorhandene, unterstützte Quelldateisystem-IDs sein. Die Quelldateisysteme mit IDs zwischen sourceFsId2 und sourceFsId3 müssen nicht unbedingt vorhanden sein. Beim Erstellen werden nur vorhandene Quelldateisystem-IDs verwendet. Nicht vorhandene Dateisysteme im Bereich werden übersprungen. Wenn beispielsweise 13, 15~20, 25 eingegeben wird, müssen Quelldateisysteme mit IDs 13,15, 20 und 25 vorhanden sein. Quelldateisysteme mit IDs von 16 bis 19 müssen jedoch nicht vorhanden sein.</p>
-skipServerParamCheck	<p>(Optional) Gibt an, ob die Serverparameterprüfung übersprungen werden soll (Vergleich). Bei Auswahl dieser Option wird die Prüfung der Serverparameter übersprungen. Im unbeaufsichtigten Modus wird die Prüfung nicht übersprungen. Bei der Erstellung einer Importsitzung werden Serverparameter zwischen VNX und Unity verglichen. Wenn die Erstellung der Importsitzung mit einem Serverparameterfehler fehlschlägt, kann die Erstellung durch diese Option fortgesetzt werden.</p> <p> VORSICHT: Durch das Überspringen der Serverparameterprüfung kann es zu Unterbrechungen bei der Umstellung während des Imports kommen.</p>

Beispiel für eine Importsitzung

Mit dem folgenden Befehl wird eine Importsitzung mit den folgenden Einstellungen erstellt:

 **ANMERKUNG:** Der Quell-VDM ist ein Nur-NFS-VDM.

- Der Name der Importsitzung lautet newName.
- Das Quellspeichersystem ist RS_1.
- Die Quellspeicherressource (VDM) ist src_vdm_to_migrate.

- Der Zielressourcenpool ist pool_1.
- Die Zielimportschnittstelle ist if_3.
- Die Quell-VDM-Produktionsschnittstelle und die Zielportpaare sind source_interface_1:spa_iom_0_eth1 und source_interface_2:spa_iom_0_eth0.
- Das Quelldateisystem und die Zielpoolpaare sind 100~200:pool_2 und 255:pool_3.
- Der Zielport, auf dem die Produktionsschnittstellen des NAS-Servers erstellt werden, ist spa_iom_0_eth0.
- Migrieren Sie den UNIX-Verzeichnisdienst mit direkter Übereinstimmung.
- Dateisysteme 13, 20 bis 25 und 30 müssen als VMware-Datenspeicher-Dateisysteme importiert werden.
- Überspringen Sie die Prüfung der Serverparameter.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! import/session/nas create -name
newName -srcSys RS_1 -srcRes src_vdm_to_migrate -targetResPool pool_1 -targetImportIf
if_3 -productionIfPortPairs source_interface_1:spa_iom_0_eth1,source_interface_2:spa_iom_0_eth0
-fsPoolPairs 100~200:pool_2,255:pool_3 -defaultProductionPort spa_iom_0_eth0
-unixDirectoryService directMatch -srcFsImportedAsVMwareDatastore 13,20~25,30
-skipServerParamCheck
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

Using '-skipServerParamCheck' option could lead to disruptive cutover during migration. Do you want to continue?

```
yes / no: yes
ID = import_1
```

Operation completed successfully.

Mit dem folgenden Befehl wird eine Importsitzung mit den folgenden Einstellungen erstellt:

 **ANMERKUNG:** Der Quell-VDM ist ein Nur-NFS-VDM.

- Der Name der Importsitzung lautet newName.
- Das Quellspeichersystem ist RS_1.
- Die Quellspeicherressource (VDM) ist src_vdm_to_migrate.
- Der Zielressourcenpool ist pool_1.
- Die Zielimportschnittstelle ist if_3.
- Die Quell-VDM-Produktionsschnittstelle und die Zielportpaare sind source_interface_1:spa_iom_0_eth1 und source_interface_2:spa_iom_0_eth0.
- Das Quelldateisystem und die Zielpoolpaare sind 100~200:pool_2 und 255:pool_3.
- Der Zielport, auf dem die Produktionsschnittstellen des NAS-Servers erstellt werden, ist spa_iom_0_eth0.
- Migrieren Sie den UNIX-Verzeichnisdienst mit direkter Übereinstimmung.
- Dateisysteme 13, 20 bis 25 und 30 müssen als VMware-Datenspeicherdateisysteme importiert werden.
- Dateisysteme 14, 22, 25 bis 30 werden als Thin importiert.
- Dateisysteme 31 und 40 bis 45 werden importiert und es wird eine Datenreduzierung auf diese angewendet.
- Überspringen Sie die Prüfung der Serverparameter.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! / import/session/nas create -name
newName -srcSys RS_1 -srcRes src_vdm_to_migrate -targetResPool pool_1 -targetImportIf
if_3 -productionIfPortPairs source_interface_1:spa_iom_0_eth1,source_interface_2:spa_iom_0_eth0
-fsPoolPairs 100~200:pool_2,255:pool_3 -defaultProductionPort spa_iom_0_eth0
-unixDirectoryService directMatch -srcFsImportedAsVMwareDatastore 13,20~25,30
-srcFsImportedAsThin 14,22,25~30 -srcFsImportedWithDataReductionEnabled 31,40~45
-skipServerParamCheck
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = import_1
```

Operation completed successfully.

Mit dem folgenden Befehl wird eine Importsitzung mit den folgenden Einstellungen erstellt:

 **ANMERKUNG:** Der Quell-VDM ist ein Nur-CIFS-VDM.

- Der Name der Importsitzung lautet newName.

- Das Quellspeichersystem ist RS_1.
- Die Quellspeicherressource (VDM) ist src_vdm_to_migrate.
- Der Zielressourcenpool ist pool_1.
- Die Zielimportschnittstelle ist if_3.
- Die Quell-VDM-Produktionsschnittstelle und die Zielportpaare sind source_interface_1:spa_iom_0_eth1 und source_interface_2:spa_iom_0_eth0.
- Das Quelldateisystem und die Zielpoolpaare sind 100~200:pool_2 und 255:pool_3.
- Der Zielport, auf dem die Produktionsschnittstellen des NAS-Servers erstellt werden, ist spa_iom_0_eth0.
- Der Nutzername für die Authentifizierung auf dem CIFS-Server auf dem Quell-VDM ist cifsadmin1.
- Das Passwort für die Authentifizierung auf dem CIFS-Server auf dem Quell-VDM ist cifspasswort1.
- Dateisysteme 13, 20 bis 25 und 30 müssen als VMware-Datenspeicherdateisysteme importiert werden.
- Dateisysteme 14, 22, 25 bis 30 werden als Thin importiert.
- Dateisysteme 31 und 40 bis 45 werden importiert und es wird eine Datenreduzierung auf diese angewendet.
- Überspringen Sie die Prüfung der Serverparameter.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! import/session/nas create -name
newName -srcSys RS_1 -srcRes src_vdm_to_migrate -targetResPool pool_1 -targetImportIf
if_3 -productionIfPortPairs source_interface_1:spa_iom_0_eth1,source_interface_2:spa_iom_0_eth0
-fsPoolPairs 100~200:pool_2,255:pool_3 -defaultProductionPort spa_iom_0_eth0
-srcFsImportedAsVMwareDatastore 13,20~25,30 -srcLocalCifsAdminUsername cifsadmin1
-srcLocalCifsAdminPasswd cifspasswort1 -skipServerParamCheck
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
Using '-skipServerParamCheck' option could lead to disruptive cutover during migration. Do
you want to continue?
yes / no: yes
ID = import_1
Operation completed successfully.
```

Änderung der Importsitzungseinstellungen für File

Ändern Sie die Einstellungen für eine NAS-Importsitzung.

Format

```
/import/session/nas -id <value> set [-async] [-paused {yes | no}] -name <value>] [-targetResPool
<value>] [-fsPoolPairs <value>] [-targetImportIf <value>] [-productionIfPortPairs <value>] [-
productionIfVlanPairs <value>] [-srcLocalCifsAdminUsername <value> {-srcLocalCifsAdminPasswd
<value> | srcLocalCifsAdminPasswdSecure}] [-srcFsImportedAsVMwareDatastore <value>] [-
srcFsImportedWithDataReductionEnabled <value>] [-srcFsImportedWithAdvancedDedupEnabled <value>]]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID der Importsitzung ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie die Aktion im asynchronen Modus aus.
-name	Gibt den neuen Namen der Importsitzung an.
-paused	Gibt an, ob die Sitzung angehalten werden soll. Gültige Werte:

Qualifizierer	Beschreibung
	<ul style="list-style-type: none"> • yes • no <p> ANMERKUNG: no Startet oder setzt die Importsitzung fort.</p>
-targetResPool	Gibt den neuen Pool für die Zielressource an. Nur zutreffend, wenn der Status der Sitzung „Initialisiert“ lautet oder das Provisioning des NAS-Zielservers fehlschlägt.
-fsPoolPairs	Gibt die IDs des Quelldateisystems und die Zielpoolpaare an. Nur zutreffend, wenn der Status der Sitzung „Initialisiert“ lautet oder das Provisioning des Zieldateisystems fehlschlägt.
-targetImportIf	Gibt die neue Zielmigrationsschnittstelle an. Nur zutreffend, wenn der Status der Sitzung „Initialisiert“ lautet oder das Provisioning des NAS-Zielservers fehlschlägt.
-productionIfPortPairs	Gibt die Quell-VDM-Produktionsschnittstelle und die Zielportpaare an. Nur zutreffend, wenn der Status der Sitzung „Initialisiert“ lautet oder die Erstellung der Zielproduktionsschnittstelle fehlschlägt.
-productionIfVlanPairs	Gibt die Quell-VDM-Produktionsschnittstelle und die Ziel-VLAN-Paare an. Nur zutreffend, wenn der Status der Sitzung „Initialisiert“ lautet oder die Erstellung der Zielproduktionsschnittstelle fehlschlägt.
-srcLocalCifsAdminUsername	Gibt den Benutzernamen für die Authentifizierung auf dem CIFS-Server auf dem Quell-VDM an.
-srcLocalCifsAdminPasswd	Gibt das Passwort für die Authentifizierung auf dem CIFS-Server auf dem Quell-VDM an.
-srcLocalCifsAdminPasswdSecure	Gibt ein Passwort im sicheren Modus an.  ANMERKUNG: Der Benutzer wird aufgefordert, das Passwort einzugeben und zu bestätigen.
-srcFsImportedAsVMWareDatastore	Gibt an, welche Quelldateisysteme als VMware-Datenspeicher-Dateisysteme importiert werden. Gilt nur für den Dateimport, wenn die Sitzung initialisiert wird.  ANMERKUNG: Wenn ein VNX-Dateisystem durch diese Option angegeben wird, sollte es keine Struktur-Quotas oder Benutzer-Quotas enthalten.
-srcFsImportedWithDataReductionEnabled	Gibt an, welche Quelldateisysteme mit aktivierter Datenreduzierung importiert werden. Gilt nur für den Dateimport, wenn die Sitzung initialisiert wird.
-srcFsImportedWithAdvancedDedupEnabled	Gibt an, welche Quelldateisysteme mit aktivierter erweiterter Deduplizierung importiert werden. Gilt nur für den Dateimport, wenn die Sitzung initialisiert wird.

Beispiel

Mit dem folgenden Befehl werden die NAS-Importsitzungseinstellungen geändert:

 **ANMERKUNG:** Mit diesem Befehl wird nur die Konfiguration der Importsitzung geändert. Zur Wiederaufnahme (zum Start) der Importsitzung über die UEMCLI müssen Sie den Befehl `/import/session/nas set` ausführen und **Nein** für den Aktionsqualifizierer `-paused` angeben.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /import/session/nas -id
import_1 set -name newName -targetResPool pool_2 -targetImportIf if_3
-productionIfPortPairs source_interface_1:spa_iom_0_eth1,source_interface_2:spa_iom_0_eth0
```

```
-fsPoolPairs 100~200:pool_2,255:pool_3 -srcFsImportedAsVMWareDatastore 17~20
-srcFsImportedWithDataReductionEnabled 31,40~45
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Starten oder Wiederaufnehmen einer Importsitzung

Sobald eine Importsitzung erstellt und gegebenenfalls modifiziert wird, bleibt sie im initialisierten Zustand, bis sie gestartet (oder wiederaufgenommen) wird. Mit dem folgenden Befehl wird die Beispiel-NAS-Importsitzung gestartet (oder wiederaufgenommen):

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /import/session/nas -id import_1 set -paused
no
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Umstellen von Importsitzungen für File

Stellen Sie eine vorhandene NAS-Importsitzung um. Durch das Umstellen einer Sitzung werden die aktiven Host-I/Os auf die Zielseite umgestellt und es wird eine inkrementelle Synchronisation von der Quelle zum Ziel initiiert.

Format

```
/import/session/nas -id <value> cutover [-async] [-netbiosName <value>] [-cifsServerName <value>]
-domainUsername <value> {-domainPasswd <value> | -domainPasswdSecure} [-ou] <AD organizational
unit tree>
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Gibt die ID der Importsitzung an.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie die Aktion im asynchronen Modus aus.
-netbiosName	Gibt den neuen NetBIOS-Namen für die Quelle des CIFS-Servers an.
-cifsServerName	Gibt den neuen Namen für den CIFS-Quellserver nach der Umstellung an. SMB (CIFS)-Servername muss auf dem Netzwerk eindeutig sein.  ANMERKUNG: Wenn nicht angegeben, ist der Standardname für das Umbenennen des CIFS-Quellservers der ursprüngliche CIFS-Servername mit einem vorangestellten Unterstrich (_).
-domainUsername	Gibt den Domainadministratorknamen an. Dieser Name ist erforderlich, um den CIFS-Quellserver umzubenennen und ihn mit Active Directory zu verbinden. (Nur für AD-verbundene CIFS-Server-Migration verwendet)
-domainPasswd	Gibt das Passwort des Domainbenutzers an.

Qualifizierer	Beschreibung
-domainPasswdSecure	Gibt ein Passwort im sicheren Modus an.  ANMERKUNG: Der Benutzer wird aufgefordert, das Passwort einzugeben und zu bestätigen.
-ou	Gibt die vollständige Active Directory-Organisationseinheit für den CIFS-Quellserver an.  ANMERKUNG: Dieser Parameter ist optional. Falls angegeben, wird die LDAP Suche des CIFS-Servers in AD in der angegebenen OU-Struktur angezeigt.

Beispiel 1

Mit dem folgenden Befehl wird die NFS-Importsitzung import_1 auf das Zielsystem umgestellt:

```
uemcli -d 10.0.0.1 -u Local/joe -p <value> /import/session/nas -id import_1 cutover
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Beispiel 2

Der folgende Befehl zeigt, wie die KMU-Importsitzung import_1 auf das Zielsystem umgestellt wird:

```
uemcli -d 10.0.0.1 -u Local/joe -p <value> /import/session/nas -id import_1 cutover
-cifsServerName <value> -domainUsername <value> -domainPasswd <value>
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Beispiel 3

Der folgende Befehl zeigt, wie die CIFS-Importsitzung import_1 auf das Zielsystem umgestellt wird, während Sie die AD-Organisationseinheit angeben:

```
uemcli -u admin -p <password> -sslPolicy accept /import/session/nas -id import_1 cutover
-netbiosName <value> -cifsServerName <value> -domainUsername <value> -domainPasswd <value> -ou
<value>
```

Der folgende Befehl zeigt, wie die CIFS-Importsitzung import_2 auf das Zielsystem umgestellt wird, nachdem import_1 umgeschaltet wurde:

```
uemcli -u admin -p <value> -sslPolicy accept /import/session/nas -id import_2 cutover
-netbiosName <value> -cifsServerName <value> -domainUsername <value> -domainPasswd <value>
```

Commit von Importsitzungen für File

Führen Sie Commit für eine vorhandene NAS-Importsitzung durch. Durch die Durchführung von Commit für eine Sitzung wird der Importvorgang abgeschlossen.

Format

```
/import/session/nas -id <value> commit [-async]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID der Importsitzung ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie die Aktion im asynchronen Modus aus.

Beispiel

Mit dem folgenden Befehl wird die Importsitzung import_1 committed.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /import/session/nas -id import_1 commit
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection
```

```
Operation completed successfully.
```

Abbrechen einer NAS-Importsitzung

Brechen Sie eine vorhandene NAS-Importsitzung ab.

Format

```
/import/session/nas -id <value> cancel [-async] [-domainUsername <value> {-domainPasswd <value>  
| -domainPasswdSecure}] [-ou <value>]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID der Importsitzung ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie die Aktion im asynchronen Modus aus.
-domainUsername	Gibt den Domainbenutzer mit Administratorrechten zur Aktualisierung von Active Directory an (nicht erforderlich für eigenständige CIFS-Server).
-domainPasswd	Gibt das Benutzerpasswort der Domain an (nicht erforderlich für eigenständige CIFS-Server).
-domainPasswdSecure	Gibt das Passwort im sicheren Modus an (nicht erforderlich für eigenständige CIFS-Server).  ANMERKUNG: Der Benutzer wird aufgefordert, das Passwort einzugeben und zu bestätigen.
-ou	Gibt die vollständige AD-Organisationseinheit für den CIFS-Quellserver an.  ANMERKUNG: Dies ist ein optionaler Parameter, wenn Sie angegeben haben, dass die sich LDAP-Suche des CIFS-Servers in AD in der angegebenen OU-Struktur befindet.

Qualifizierer	Beschreibung
	Gibt eine durch Doppelpunkte (:) getrennte Liste der OU an Berücksichtigen Sie, dass es zwei OUs, OU1 und OU2, für den CIFS-Server gibt. Lassen Sie OU2 unter OU1. Dann wird der <Wert> wie 'ou=ou2:ou=ou1' aussehen.

Beispiel 1

Mit dem folgenden Befehl wird die NAS-Importsitzung import_1 abgebrochen.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /import/session/nas -id import_1 cancel -skipSourceRestore
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
Operation completed successfully.
```

Beispiel 2

Mit dem folgenden Befehl wird die NAS-Importsitzung import_1 abgebrochen.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /import/session/nas -id import_1 cancel -domainUsername user1 -domainPasswd password1 -ou 'ou=Computers:ou=EMC Celerra'
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
Operation completed successfully.
```

Anzeigen von Importsitzungen für File

Zeigen Sie Details zu Importsitzungen für File an. Sie können nach der Sitzungs-ID filtern.

Format

```
/import/session/nas [{-id <value> | -active | -completed | -cancelled}] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID der Importsitzung ein.
-active	Zeigen Sie nur aktive Sitzungen (Sitzungen, die nicht abgeschlossen oder abgebrochen wurden) an.
-completed	Zeigen Sie nur abgeschlossene Sitzungen an.
-cancelled	Zeigen Sie nur abgebrochene Sitzungen an.

Beispiel

Mit dem folgenden Befehl werden File-Importsitzungen auf dem System angezeigt.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /import/session/nas show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      ID                               = import_1
      Type                               = cifs
      Name                               = test1
      Health state                       = OK (5)
      Health details                     = "The import session
is operating normally."
      State                               = Cancelled
      Progress                            =
      Source system                       = RS_65536
      Source resource                     = vdm_cifs_frank
      Source import interface             = nas_migration_frank
      Source file systems imported as VMware datastore =
      Source file systems imported with compression enabled =
      Source file systems imported with data reduction enabled =
      Source file systems imported with advanced deduplication enabled =
      Target resource                     = nas_1
      Target resource pool                 = pool_1
      Target file system to pool mapping   = res_10~res_11:pool_1
      Target file system access policy mapping =
      Target import interface              = if_5
      Target default production port       = spa_iom_0_eth0
      Target production interface to port mapping = if_6:spa_iom_0_eth0
      Target production interface to vlan mapping = if_6:0
      CIFS local user                     = Administrator
      Source DHSM user                    =

2:      ID                               = import_3
      Type                               = Multiprotocol
      Name                               = test2
      Health state                       = OK (5)
      Health details                     = "The import session
is operating normally."
      State                               = Cancelled
      Progress                            =
      Source system                       = RS_65536
      Source resource                     = vdm_test
      Source import interface             = nas_migration_test1
      Source file systems imported as VMware datastore =
      Source file systems imported with compression enabled =
      Source file systems imported with data reduction enabled =
      Source file systems imported with advanced deduplication enabled =
      Target resource                     = nas_2
      Target resource pool                 = pool_1
      Target file system to pool mapping   = res_12~res_13:pool_1
      Target file system access policy mapping = 1400:UNIX;

174:WINDOWS
      Target import interface              = if_5
      Target default production port       = spa_iom_0_eth0
      Target production interface to port mapping = if_7:spa_iom_0_eth0
      Target production interface to vlan mapping = if_7:0
      CIFS local user                     = Administrator
      Source DHSM user                    =
```

Anzeigen von Importsitzungselementen

Zeigen Sie Details zum Status des Imports für jedes Element in der aktiven Importsitzung an, z. B. jede LUN in einer Consistency Group (CG).

In der folgenden Tabelle sind die Attribute für Importsitzungselemente aufgeführt:

Tabelle 138. Attribute von Importsitzungselementen

Attribut	Beschreibung
Source system	Identifiziert das Quellsystem.
Source resource	Identifiziert die Quellressource.
Target resource	Identifiziert die Zielressource.
Health state	Integritätsstatus des Importelementes.
Health details	Zusätzliche Integritätsinformationen.
Stage	Importphase der Datenübertragung. Gültige Werte: <ul style="list-style-type: none"> • Initial sync • Incremental sync • Final sync
Iteration	Iterationsnummer in dieser Phase der Importdatenübertragung. Diese Eigenschaft gilt nur für die inkrementelle Kopierphase des LUN-Imports.
Progress	Importfortschritt der aktuellen Synchronisationsiteration.

Format

```
/import/session/element -importId <value> show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-importId	Geben Sie die ID der Importsitzung ein.

Beispiel

Der folgende Befehl zeigt den Status des Imports für jedes Element in der angegebenen Importsitzung an:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /import/session/element -importId import_2 show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:   Source system   = RS_1
     Source resource = lun1
     Target resource = sv_1
     Health state   = OK (5)
     Health details  = "The component is operating normally. No action is required."
     Stage          = Incremental Sync
     Iteration       = 4
     Progress        = 10%
     Source system   = RS_1
     Source resource = lun4
     Target Resource = sv_2
     Health state   = OK (5)
     Health details  = "The component is operating normally. No action is required."
     Stage          = Incremental sync
     Iteration       = 4
     Progress        = 0%
```

Verwalten generischer Blockressourcen-Importsitzungen

Dieser Befehl importiert generische Blockressourcen (wie LUNs, Volumes oder virtuelle Festplatten) aus einem Drittanbieter-Blockspeichersystem, das seinen Blockgeräten (LUNs) einen Fibre Channel (FC)- oder eine iSCSI-Schnittstelle zur Verfügung stellt. Es verwendet die SAN Copy Pull-Funktion, die auf dem lokalen Speichersystem ausgeführt wird.

Wenn das iSCSI-Protokoll verwendet wird, müssen iSCSI-Verbindungen und Verbindungspfade erstellt und konfiguriert worden sein, bevor Sie generische Importsitzungen verwalten können. Weitere Informationen über die Konfiguration von iSCSI-Verbindungen und Verbindungspfaden finden Sie in den Abschnitten „Verwalten von iSCSI-Verbindungen“ und „Verwalten von iSCSI-Verbindungspfaden“ in diesem Kapitel.

In der folgenden Tabelle sind die Attribute für Importsitzungen aufgeführt:

Tabelle 139. Attribute für Importsitzung

Attribut	Beschreibung
ID	ID der Importsitzung.
Name	Name der Importsitzung.
Description	Beschreibung der Importsitzung.
Health state	Integritätsstatus der Importsitzung. Gültige Werte: <ul style="list-style-type: none"> • Unknown (0) – Die Remotesystemintegrität kann nicht bestimmt werden. • OK (5) – Die Sitzung hat einen der folgenden Status: <ul style="list-style-type: none"> ○ Sitzung funktioniert normal. ○ Sitzung ist abgeschlossen. ○ Sitzung wurde abgebrochen. • OK_BUT (7) – Die Sitzung hat einen der folgenden Status: <ul style="list-style-type: none"> ○ Sitzung wurde bei Neustart des Speicherprozessors wiederhergestellt. ○ Sitzung wurde in Warteschlange gestellt. ○ Die Sitzung wurde angehalten. • Degraded/Warning (10) – Die Sitzung hat einen der folgenden Status: <ul style="list-style-type: none"> ○ Automatische Recovery wird ausgeführt. ○ Recovery erfolgt bei Neustart des Speicherprozessors. ○ Warten auf LUN-Überschreitung. • Minor failure (15) – Die Sitzung ist fehlgeschlagen, entweder weil ein SP ausgefallen ist oder weil die Sitzung abgebrochen wurde. • Major failure – Die Sitzung ist aus einem der folgenden Gründe fehlgeschlagen: <ul style="list-style-type: none"> ○ Auf der Quellblockressource wurde ein beschädigter Block gefunden. ○ Ein Neustart bei automatischer Recovery ist fehlgeschlagen. ○ Die Sitzung wurde bei einem Neustart des Speicherprozessors gestoppt. ○ Die Ziel-LUN und die Importsitzung befinden sich auf verschiedenen Speicherprozessoren. ○ Die Ziel-LUN wurde überschritten. • Critical failure – Die Sitzung ist aus einem der folgenden Gründe fehlgeschlagen: <ul style="list-style-type: none"> ○ Entweder die Quellblockressource oder die Ziel-LUN wurde nicht gefunden. ○ Es konnte entweder auf die Quellblockressource oder auf die Ziel-LUN nicht zugegriffen werden. ○ Die Quellblockressource hat einen ungültigen Verbindungstyp. ○ Die Quellblockressource ist fehlgeschlagen. ○ Die Ziel-LUN ist inkonsistent. • Non-recoverable failure (30) – Die Sitzung ist aufgrund eines nicht behebbaren Fehlers fehlgeschlagen.
Health details	Zusätzliche Integritätsinformationen. Weitere Einzelheiten finden Sie in Anhang A, Referenz.
State	Status der Importsitzung. Gültige Werte: <ul style="list-style-type: none"> • Initialized • Pending

Tabelle 139. Attribute für Importsitzung (fortgesetzt)

Attribut	Beschreibung
	<ul style="list-style-type: none"> • Running • Paused • Failed • Completed • Cancelled
SP owner	Eigentümer des Standardziel-LUN-Speicherprozessors. Gültige Werte: <ul style="list-style-type: none"> • SPA • SPB
Source system name	Vom Benutzer bei Erstellung der Sitzung angegebener Name des Remotesystems.
Source LUN WWN	<p>Weltweiter Name (WWN) der Quellblockressource. Der WWN kann mit den folgenden vier Präfixen übergeben werden:</p> <ul style="list-style-type: none"> • wwn. • nna. • wwn-0x. • 0x. <p>Es ist möglich, den WWN ohne Präfixe zu übergeben. Zum Beispiel können folgende WWN-Notationen verwendet werden:</p> <ul style="list-style-type: none"> • 50060485c5edaa5d – 16 hexadezimale Zeichen • 50:06:04:85:c5:ed:aa:5d – Byte getrennt durch Doppelpunkte • 50:6:4:85:c5:ed:aa:5d – Führende Ziffer des Bytes entfällt, wenn sie Null ist • 50-06-04-85-c5-ed-aa-5d – Byte getrennt durch Bindestriche <p> ANMERKUNG: Wenn das System den WWN als nicht erkennbar ablehnt, können Sie den WWN manuell in das Format des Dell Unity-Systems umwandeln, zum Beispiel 60:00:01:6F.</p>
Target resource	Die CLI-ID der Ziel-Speicherressource.
Target resource name	Der Name der Ziel-Speicherressource
Target resource type	Typ der Zielspeicherressource. Gültige Werte: <ul style="list-style-type: none"> • -LUN • VMware-VMFS
Size of source	Größe der Daten, die von der Quellblockressource auf die Ziel-LUN zu übertragen sind.
Size copied	Gesamtzahl der Byte, die von der Quellblockressource auf die Ziel-LUN übertragen wurden.
Size remaining	Aktuell verbleibende Größe in Byte, die von der Quellblockressource auf die Ziel-LUN zu übertragen sind.
Percent completed	Prozentsatz der Byte, die von der Quellblockressource auf die Ziel-LUN übertragen wurden.
Start time	Startzeit des Kopiervorgangs.
Estimated time to complete	Aktuell geschätzte Zeit für das Kopieren der Quellblockressource auf die Ziel-LUN.
Throttle	<p>Reduziert die CPU-Last und die I/O-Latenz auf dem Zielsystem. Je geringer der Drosselungswert ist, desto geringer sind die Auswirkungen auf die Hostlatenz und desto länger wird der Import dauern. Gültige Werte:</p> <ul style="list-style-type: none"> • Low • Medium • High (Standard)

Erstellen einer generischen Importsitzung

Erstellen Sie eine Importsitzung für Drittanbietersysteme.

Format

```
/import/session/generic create [-name <value>] [-descr <value>] [-srcSystemName <value>]
-srcLUNWWN <value> {-targetRes <value> | -targetResName <value>} [-throttle {Low | Medium |
High}] [-async]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-name	Identifiziert die Importsitzung durch einen eindeutigen Namen. Wenn dieser Name nicht angegeben wird, wird er nach folgendem Muster erzeugt: <target LUN CLI ID>-<target LUN name>-<timestamp>. Zum Beispiel könnte der Name als sv_1-LUN01-20180601T160654 erzeugt werden.
-descr	Gibt die Beschreibung der Importsitzung an.
-srcSystemName	Name des Remote-Drittanbietersystems. Wenn dieser Name nicht angegeben ist, bleibt die Option leer und die Sitzung kann durch den Remotesystemnamen nicht nachverfolgt werden.
-srcLUNWWN	Gibt den WWN der Quell-LUN an. Der WWN kann mit den folgenden vier Präfixen übergeben werden: <ul style="list-style-type: none"> • wwn. • nna. • wwn-0x. • 0x. Es ist möglich, den WWN ohne Präfixe zu übergeben. Zum Beispiel können folgende WWN-Notationen verwendet werden: <ul style="list-style-type: none"> • 50060485c5edaa5d – 16 hexadezimale Zeichen • 50:06:04:85:c5:ed:aa:5d – Byte getrennt durch Doppelpunkte • 50:6:4:85:c5:ed:aa:5d – Führende Ziffer des Bytes entfällt, wenn sie Null ist • 50-06-04-85-c5-ed-aa-5d – Byte getrennt durch Bindestriche <i>ANMERKUNG:</i> Wenn das System den WWN als nicht erkennbar ablehnt, können Sie den WWN manuell in das Format des Dell Unity-Systems umwandeln, zum Beispiel 60:00:01:6F.
-targetRes	Die CLI-ID der Ziel-Speicherressource.
-targetResName	Der Name der Ziel-Speicherressource
-throttle	Gibt den Drosselungswert der Importsitzung an. Gültige Werte: <ul style="list-style-type: none"> • Low • Medium • High (Standard) <i>ANMERKUNG:</i> Sie können die Drosselungseinstellung ändern, wenn eine Sitzung ausgeführt wird oder pausiert. Nur die CLI-Befehlsausgabe <code>/import/session/generic show -detail</code> gibt diese Änderung wieder, wenn die Sitzung ausgeführt wird. Nachdem die Sitzung abgeschlossen wurde, gibt die Ausgabe dieses Befehls jedoch den Drosselungswert wieder, der bei der Erstellung der Sitzung eingestellt wurde, und nicht den geänderten Wert.
-async	Führen Sie den Vorgang im asynchronen Modus aus.

Beispiel

Mit dem folgenden Befehl wird eine Importsitzung erstellt.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /import/session/generic
create -name lun_17_import -srcSystemName MyOldGranSystem -srcLUNWWN
06:00:00:00:05:00:00:00:01:00:00:00:00:00:00:00:03 -targetRes sv_1 -throttle High
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = glimp_1
Operation Completed successfully.
```

Anzeigen der Einstellungen der generischen Importsitzung

Zeigen Sie Details zu bestehenden Importsitzungen für Drittanbietersysteme an.

Format

```
/import/session/generic [{-id <value> | -name <value> | -srcSystemName <value> | -active |
-running | -paused | -failed | -pending | -completed | -cancelled}] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID der Importsitzung ein.
-name	Geben Sie den eindeutigen Namen für die Importsitzung ein.
-srcSystemName	Name des Drittanbietersystems, der vom Benutzer bei der Erstellung der Importsitzung angegeben wurde.
-active	Es werden nur aktive Sitzungen angezeigt (Sitzungen, die ausgeführt werden, angehalten wurden, fehlgeschlagen sind oder ausstehen).
-running	Nur Sitzungen zeigen, die ausgeführt werden.
-paused	Nur pausierte Sitzungen zeigen.
-failed	Nur fehlgeschlagene Sitzungen zeigen.
-pending	Nur anhängige Sitzungen zeigen.
-completed	Zeigen Sie nur abgeschlossene Sitzungen an.
-cancelled	Zeigen Sie nur abgebrochene Sitzungen an.

Beispiel

Mit dem folgenden Befehl werden alle Importsitzungen auf dem System angezeigt.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /import/session/generic show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:   ID                = gen_import_1
     Name             = Session_for1527875375
     Description      =
     Health state     = OK (5)
     Health details   = "The generic LUN import session is running normally."
     State            = Running
     SP owner         = SPB
     Trespassed       = no
     Source system name =
     Source LUN WWN   = 60:06:01:60:0B:10:3D:00:80:84:11:5B:3A:20:8E:6A
     Target resource  = sv_23
     Target resource name = destLun_Compression_Disabled_TLU_1_Standalone
     Target resource type = LUN
     Size of source   = 21474836480 (20.0G)
     Size copied      = 408944640 (390.0M)
     Size remaining   = 21065891840 (19.6G)
     Percent completed = 1%
```

```

Start time = 2018-06-01 17:50:03
Estimated time to complete = 2018-06-02 01:32:58
Throttle = Low

2: ID = gen_import_2
Name = Session_for1527875405
Description =
Health state = OK (5)
Health details = "The generic LUN import session is running normally."
State = Running
SP owner = SPA
Trespassed = no
Source system name =
Source LUN WWN = 60:06:01:60:0B:10:3D:00:8A:84:11:5B:55:AD:35:5D
Target resource = sv_24
Target resource name = destLun_DLU_1_Ds
Target resource type = VMware_VMFS
Size of source = 21474836480 (20.0G)
Size copied = 81264640 (77.5M)
Size remaining = 21393571840 (19.9G)
Percent completed = 0%
Start time = 2018-06-01 17:50:39
Estimated time to complete = 2018-06-01 19:14:35
Throttle = Low

```

Ändern der Einstellungen der generischen Importsitzung

Ändert die bestehenden Einstellungen der Importsitzungen für Drittanbietersysteme.

Format

```

/import/session/generic {-id <value> | -name <value>} set [-newName <value>] [-descr <value>]
[-srcSystemName <value>] [-throttle <value>] [-async]

```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID der Importsitzung ein.
-name	Geben Sie den eindeutigen Namen für die Importsitzung ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-newName	Gibt den neuen Namen der Importsitzung an.
-descr	Gibt die Beschreibung der Importsitzung an.
-srcSystemName	Name des Remote-Drittanbietersystems. Wenn dieser Name nicht angegeben ist, bleibt die Option leer und die Sitzung kann durch den Remotesystemnamen nicht nachverfolgt werden.
-throttle	Gibt den Drosselungswert der Importsitzung an. Gültige Werte: <ul style="list-style-type: none"> • Low • Medium • High <p>i ANMERKUNG: Sie können die Drosselungseinstellung ändern, wenn eine Sitzung ausgeführt wird oder pausiert. Nur die CLI-Befehlsausgabe <code>/import/session/generic show -detail</code> gibt diese Änderung wieder, wenn die Sitzung ausgeführt wird. Nachdem die Sitzung abgeschlossen wurde, gibt die Ausgabe dieses Befehls</p>

Qualifizierer	Beschreibung
	jedoch den Drosselungswert wieder, der bei der Erstellung der Sitzung eingestellt wurde, und nicht den geänderten Wert.
-async	Führen Sie den Vorgang im asynchronen Modus aus.

Beispiel

Mit dem folgenden Befehl werden die Einstellungen der Importsitzung von „name“ auf „newName“ geändert:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /import/session/generic -id gen_import_1 set -name newName
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Anhalten einer generischen Importsitzung

Hält eine laufende Importsitzung eines Drittanbietersystems an.

Format

```
/import/session/generic {-id <value> | -name <value>} pause [-async]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID der Importsitzung ein.
-name	Geben Sie den eindeutigen Namen für die Importsitzung ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.

Beispiel

Mit dem folgenden Befehl wird die Importsitzung „gen_import_1“ angehalten.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /import/session/generic -id gen_import_1 pause
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Wiederaufnehmen einer generischen Importsitzung

Nimmt die Ausführung einer Importsitzung eines Drittanbietersystems wieder auf.

Format

```
/import/session/generic {-id <value> | -name <value>} resume [-async]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID der Importsitzung ein.
-name	Geben Sie den eindeutigen Namen für die Importsitzung ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.

Beispiel

Mit dem folgenden Befehl wird die Importsitzung „gen_import_1“ wiederaufgenommen.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /import/session/generic -id gen_import_1 resume
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection
```

```
Operation completed successfully.
```

Abbrechen einer generischen Importsitzung

Bricht eine bestehende aktive oder gescheiterte Importsitzung eines Drittanbietersystems ab.

 **ANMERKUNG:** Sobald eine Importsitzung abgebrochen wurde, kann sie nicht mehr erneut gestartet werden.

Format

```
/import/session/generic {-id <value> | -name <value>} cancel [-async]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID der Importsitzung ein.
-name	Geben Sie den eindeutigen Namen für die Importsitzung ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.

Beispiel

Mit dem folgenden Befehl wird die NAS-Importsitzung „gen_import_1“ abgebrochen.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /import/session/generic -id gen_import_1 cancel
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection
```

```
Operation completed successfully.
```

Neustarten einer generischen Importsitzung

Startet eine fehlgeschlagene Importsitzung eines Drittanbietersystems neu, sobald die Ursache des Fehlers behoben wurde. Die Sitzung wird neu gestartet und kopiert Daten aus der letzten in einem Prüfpunkt gespeicherten Blockadresse. Wenn jedoch der Drosselungswert während der Ausführung der Sitzung geändert wurde, wird der Drosselungswert verwendet, der bei der Erstellung der ersten Sitzung eingestellt wurde, und nicht der geänderte Wert.

Format

```
/import/session/generic {-id <value> | -name <value>} restart [-async]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID der Importsitzung ein.
-name	Geben Sie den eindeutigen Namen für die Importsitzung ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.

Beispiel

Mit dem folgenden Befehl wird die Importsitzung „gen_import_1“ neu gestartet.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /import/session/generic -id gen_import_1 restart
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection
```

```
Operation completed successfully.
```

Löschen einer generischen Importsitzung

Löscht eine angegebene abgebrochene oder abgeschlossene Importsitzung eines Drittanbietersystems. Die Löschoption löscht alle historischen Daten für die angegebene Importsitzung.

Format

```
/import/session/generic {-id <value> | -name <value>} delete [-async]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID der Importsitzung ein.
-name	Geben Sie den eindeutigen Namen für die Importsitzung ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.

Beispiel

Mit dem folgenden Befehl wird die Importsitzung „gen_import_1“ gelöscht.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /import/session/generic -id gen_import_1 delete
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection
```

```
Operation completed successfully.
```

Common-Base-Snapshots

Durch die Referenzierung eines Common-Base-Snapshots können Sie eine vollständige Kopie vermeiden, wenn Sie nach einem ungeplanten Failover einen Failback-Vorgang auf die ursprüngliche Quelle durchführen.

Wenn bei einem ungeplanten Failover eine Dateisystem-Replikationssitzung unterbrochen wird, können Sie diese Sitzung mit dem Common-Base-Snapshot erneut erstellen.

Attribute der Snapshot-Vorabprüfung

Attribut	Beschreibung
Session ID	Die ID der synchronen Dateireplikationssitzung.
Session name	Der Name der synchronen Dateireplikationssitzung.
Source common base snapshot ID	Die ID des Common-Base-Snapshot am Quellstandort.
Source common base snapshot name	Der Name des Common-Base-Snapshot am Quellstandort.
Destination common base snapshot ID	Die ID des Common-Base-Snapshot am Zielstandort.

Attribut	Beschreibung
Destination common base snapshot name	Der Name des Common-Base-Snapshot am Zielstandort.

Eine Vorabprüfung für vorhandene Common-Base-Snapshots durchführen

Suchen Sie nach Common-Basis-Snapshots auf einem NAS-Server oder in einer Dateireplikationssitzung, bevor Sie einen Failback-Vorgang durchführen. Durch die Verwendung vorhandener Common-Base-Snapshots können Sie die Funktion „Vollständige Kopie vermeiden“ verwenden und eine Delta-Synchronisation durchführen. Diese Art der Synchronisation sendet nur Daten, die nach dem Failover zurück auf das Quellsystem geändert wurden.

ANMERKUNG: Dieser Befehl gilt nur für die synchrone Dateireplikation.

Common-Base-Snapshots können Snapshots sein, die nach einem festgelegten Zeitplan erstellt und auf das Ziel repliziert wurden. Common-Base-Snapshots können auch manuell auf der Quelle erstellt und auf das Zielsystem repliziert werden.

ANMERKUNG: Die Vorabprüfung kann nur mit der CLI durchgeführt werden. Sie kann nicht in der Unisphere-Benutzeroberfläche durchgeführt werden.

Format

```
/prot/rep/session/commonbase {-session <value> | -sessionName <value>} show -detail
```

Objektqualifizierer

Qualifizierer	Beschreibung
-session	Identifiziert die Replikationssitzung nach ID-Nummer.
-sessionName	Identifiziert die Replikationssitzung nach einem zugewiesenen Namen.
-detail	Zeigen Sie die Snapshot-Details an.

Beispiel

Im folgenden Beispiel sehen Sie eine Überprüfung auf Common-Base-Snapshots in einer synchronen Dateireplikationssitzung.

```
uemcli /prot/rep/session/commonbase -session
171798691845_FCNC097274B3A_0000_171798691846_FCNC097274B37_0000 show -detail

[Response]
Storage system address: 10.64.75.201
Storage system port: 443
HTTPS connection

1:   Session ID           =
171798691845_FCNC097274B3A_0000_171798691846_FCNC097274B37_0000
    Session name        = Repl
    Source common base snapshot ID      = 171798691846
    Source common base snapshot name    = Snap1
    Destination common base snapshot ID = 171798691848
    Destination common base snapshot name = Snap1

ID = 171798691845_FCNC097274B3A_0000_171798691846_FCNC097274B37_0000
Operation completed successfully.
```

Managen von LUN-Verschiebungssitzungen

Verwenden Sie die Funktion „LUN verschieben“, wenn Sie vorhandene LUNs im System verschieben müssen, wie zwischen Pools zum Lastenausgleich, zur Nutzung neu erworbener Spindeln oder zur Aktivierung der Datenreduzierung (entweder für neu geschriebene Daten oder für sowohl neu geschriebene als auch vorhandene Daten) auf einer Thin-LUN in einem All-Flash-Pool. Beachten Sie, dass bei einer Anwendung von Datenreduzierung auf vorhandene Daten die LUN-Daten innerhalb desselben Pools verschoben werden.

Wenn Sie eine LUN verschieben, die:

- keine Datenreduzierung vorsieht, wird sie als nicht komprimiert verschoben.
- eine Datenreduzierung vorsieht und in einen All-Flash-Pool verschoben werden soll, wird sie als komprimiert verschoben. Wenn Sie sie nicht in einen All-Flash-Pool verschieben, wird sie als nicht komprimiert verschoben.
- keine Thin-LUN ist, wird sie als Nicht-Thin-LUN as verschoben.
- eine Thin-LUN ist, wird sie als Thin-LUN verschoben.

In der folgenden Tabelle sind die Attribute für das Verschieben von LUNs aufgeführt:

Tabelle 140. Attribute zum Verschieben von LUNs

Attribut	Beschreibung
ID	ID der Verschiebungssitzung.
Source resource	Speicherressource für die Quelle.
Source member LUN	Quellmitglied-LUN, wenn die Speicherressource eine LUN-Gruppe ist.
Destination pool	Pool für das Ziel.
State	Aktueller Status, der den Lebenszyklus einer Verschiebungssitzung darstellt. Folgende Werte sind möglich: <ul style="list-style-type: none"> • Initializing: Verschiebungssitzung wird gerade initialisiert. • Queued: Verschiebungssitzung ist in die Warteschlange eingereiht. Das System beginnt die Datenübertragung, wenn genügend Ressourcen zur Verfügung stehen. • Running: gibt an, dass die Verschiebungssitzung Daten überträgt. • Failed: Bei der Verschiebungssitzung ist ein Fehler aufgetreten. Sehen Sie sich die Integrität der Verschiebungssitzung an, um weitere Informationen zu erhalten. • Cancelling: gibt an, dass die Verschiebungssitzung gerade abgebrochen wird. • Cancelled: gibt an, dass die Verschiebungssitzung abgebrochen wurde. • Completed: Die Datenübertragung für die Verschiebungssitzung wurde abgeschlossen.
Progress	Der Fortschritt der Verschiebungssitzung wird in Prozent ausgedrückt.
Health state	Integritätsstatus der Verschiebungssitzung. Folgende Werte sind möglich: <ul style="list-style-type: none"> • Unknown: Die Integrität der Verschiebungssitzung ist nicht bestimmbar. • OK: Die Verschiebungssitzung funktioniert normal. • Major failure: Wählen Sie eine der folgenden Optionen aus: <ul style="list-style-type: none"> ○ Der Pool ist offline gegangen und das Verschieben kann nicht fortgesetzt werden. Bitte entfernen Sie die Verschiebungssitzung, beheben Sie das Problem und erstellen Sie die Verschiebungssitzung neu. ○ Der Pool hat den verfügbaren Speicherplatz überschritten und das Verschieben kann nicht fortgesetzt werden. Bitte entfernen Sie die Verschiebungssitzung, beheben Sie das Problem und erstellen Sie die Verschiebungssitzung neu. ○ Bei der Verschiebungssitzung ist ein interner Fehler aufgetreten. Wenden Sie sich an Ihren Serviceprovider.
Health details	Zusätzliche Integritätsinformationen. Weitere Informationen zur Integrität finden Sie im Anhang A, Referenz.
Priority	Priorität für die Verschiebungssitzung. Folgende Werte sind möglich: <ul style="list-style-type: none"> • Idle: kein Kopie-I/O generiert. Die Verschiebungssitzung spiegelt den Host-I/O weiterhin. • Low: für Verschiebungssitzungen, die die geringste Priorität gegenüber anderen Verschiebungssitzungen haben. • Below normal: für Verschiebungssitzungen, die etwas weniger kritisch als die durchschnittliche oder normale Verschiebungssitzung sind.

Tabelle 140. Attribute zum Verschieben von LUNs (fortgesetzt)

Attribut	Beschreibung
	<ul style="list-style-type: none"> • Normal: für Verschiebungssitzungen, die für die meisten Anwendungsbeispiele geeignet sind. Dies ist der Standardwert. • Above normal: für Verschiebungssitzungen, die ein wenig kritischer als die durchschnittliche oder normale Verschiebungssitzung sind. • High: für Verschiebungssitzungen, die die höchste Priorität gegenüber anderen Verschiebungssitzungen haben.
Average transfer rate	Durchschnittliche Datenübertragungsrate der Verschiebungssitzung in MB/s.
Current transfer rate	Aktuelle Übertragungsrate der Verschiebungssitzung in MB/s.
Estimated time left	Geschätzte Zeit in Sekunden, die basierend auf der aktuellen Übertragungsrate verbleibt.

Erstellen einer Sitzung zum Verschieben einer LUN

Format

```
/move/session create -srcRes <value> [-srcMemberLun <value>] -targetPool <value> [-priority {idle | low | below | normal | above | high} ] [-thin {yes | no}] [-dataReductionEnabled {yes [-advancedDedupEnabled {yes | no}] | no}] [-async]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-srcRes	LUN-Kennung für eine eigenständige Quell-LUN oder eine Consistency-Group-Kennung bei Verschieben einer LUN, die Mitglied der Consistency Group ist.
-srcMemberLun	Quell-LUN-Kennung, wenn die LUN Mitglied einer Consistency Group ist.
-targetPool	Kennung des Zielspeicherpools, in dem die verschobenen Ressourcen erstellt werden.
-priority	Priorität der Verschiebungssitzung. Gültige Werte: <ul style="list-style-type: none"> • idle: für Verschiebungssitzungen, die den Host-I/O weiterhin spiegeln. • low: für Verschiebungssitzungen, die die geringste Priorität gegenüber anderen Verschiebungssitzungen haben. • below: für Verschiebungssitzungen, die etwas weniger kritisch als die durchschnittliche oder normale Verschiebungssitzung sind. • normal (Standardeinstellung): für Verschiebungssitzungen, die für die meisten Anwendungsbeispiele geeignet sind. • above: für Verschiebungssitzungen, die ein wenig kritischer als die durchschnittliche oder normale Verschiebungssitzung sind. • high: für Verschiebungssitzungen, die die höchste Priorität gegenüber anderen Verschiebungssitzungen haben.
-thin	Gibt an, ob ein Thin-Ziel erstellt werden soll. Gültige Werte: <ul style="list-style-type: none"> • yes (Standard) • no
-dataReductionEnabled	Gibt an, ob ein Ziel mit aktivierter Datenreduzierung erstellt werden soll. Gültige Werte: <ul style="list-style-type: none"> • yes • no (Standard)
-advancedDedupEnabled	Gibt an, ob ein Ziel erstellt werden soll, auf das die erweiterte Deduplizierung angewendet wird. Diese Option gilt nur, wenn die Datenreduktion aktiviert ist. Gültige Werte: <ul style="list-style-type: none"> • yes • no (Standard)

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.

Beispiel 1

Mit dem folgenden Befehl wird eine Verschiebungssitzung erstellt.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /move/session create -srcRes sv_1 -targetPool pool_1 -priority above -thin yes -dataReductionEnabled no
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = move_1
Operation completed successfully.
```

Beispiel 2

Der folgende Befehl erstellt eine Verschiebungssitzung, einschließlich der Quellmitglieds-LUN-ID.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /move/session create -srcRes res_1 -srcMemberLun sv_2 -targetPool pool_2 -priority above -thin yes -dataReductionEnabled yes -advancedDedupEnabled yes
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = move_2
Operation completed successfully.
```

Anzeigen einer LUN-Verschiebungssitzung

Format

```
/move/session [-id <value>] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID der Verschiebungssitzung ein.

Beispiel

Mit dem folgenden Befehl werden Details für eine LUN-Verschiebungssitzung angezeigt.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /move/session show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
1: ID = movesession_1
   Source resource = sv_1
   Source member LUN =
   Destination pool = pool_1
```

```

State = Initializing
Progress = 0%
Health state = OK
Health details = "The component is operating normally. No action is required."
Priority = Normal
Average transfer rate = 0 MB/s
Current transfer rate = 0 MB/s
Estimated time left = N/A

2: ID = movesession_2
Source resource = res_1
Source member LUN = lun_2
Destination pool = pool_2
State = Running
Progress = 17%
Health state = OK
Health details = "The component is operating normally. No action is required."
Priority = Above Normal
Average transfer rate = 147 MB/s
Current transfer rate = 232 MB/s
Estimated time left = 7m

```

Ändern der Einstellungen für die LUN-Verschiebungssitzung

Format

```
/move/session -id <value> set [-priority {idle | low | below | normal | above | high}] [-async]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID der Verschiebungssitzung ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-priority	Geben Sie die Priorität der Verschiebungssitzung an. Gültige Werte: <ul style="list-style-type: none"> idle: für Verschiebungssitzungen, die den Host-I/O weiterhin spiegeln. low: für Verschiebungssitzungen, die die geringste Priorität gegenüber anderen Verschiebungssitzungen haben. below: für Verschiebungssitzungen, die etwas weniger kritisch als die durchschnittliche oder normale Verschiebungssitzung sind. normal (Standardeinstellung): für Verschiebungssitzungen, die für die meisten Anwendungsbeispiele geeignet sind. above: für Verschiebungssitzungen, die ein wenig kritischer als die durchschnittliche oder normale Verschiebungssitzung sind. high: für Verschiebungssitzungen, die die höchste Priorität gegenüber anderen Verschiebungssitzungen haben.
-async	Führen Sie den Vorgang im asynchronen Modus aus.

Beispiel

Mit dem folgenden Befehl werden die Einstellungen einer Verschiebungssitzung geändert.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /move/session -id MoveSession_1 set -priority below
```

```

Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

```

```
ID = MoveSession_1
Operation completed successfully.
```

Löschen einer LUN-Verschiebungssitzung

Löscht eine LUN-Verschiebungssitzung, die abgeschlossen/abgebrochen wurde oder fehlgeschlagen ist. Sie können keine Verschiebungssitzung löschen, die ausgeführt wird.

Format

```
/move/session -id <value> delete [-async]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID der Verschiebungssitzung ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.

Beispiel

Mit dem folgenden Befehl wird eine Verschiebungssitzung gelöscht.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /move/session -id movesession_1 delete
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully
```

Abbrechen einer Sitzung zum Verschieben einer LUN

Bricht eine LUN-Verschiebungssitzung ab, die ausgeführt wird.

Format

```
/move/session -id <value> cancel [-async]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID der Verschiebungssitzung ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-async	Führen Sie den Vorgang im asynchronen Modus aus.

Beispiel

Mit dem folgenden Befehl wird eine Verschiebungssitzung abgebrochen.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /move/session -id movesession_1 cancel
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection  
  
Operation completed successfully.
```

Management von Ereignissen und Warnmeldungen

Themen:

- Anzeigen von Ereignisprotokollen und Warnmeldungen
- Konfigurieren von Warnmeldungseinstellungen
- Konfigurieren von SNMP-Zielen für Warnmeldungen

Anzeigen von Ereignisprotokollen und Warnmeldungen

Im System werden verschiedene Systemereignisse überwacht und Berichte erstellt. Die Ereignisse werden in einem Benutzerprotokoll festgehalten. Jedes Ereignis wird mit einem eigenen Eintrag protokolliert. Bei einigen Protokolleinträgen werden Warnmeldungen erzeugt. Warnmeldungen sind in der Regel Ereignisse, die auf Fehler hinweisen und denen der Systemadministrator seine Aufmerksamkeit widmen muss. So kann zum Beispiel eine Warnmeldung darauf hinweisen, dass es zu einem Laufwerkfehler gekommen ist oder dass das System nur noch über eine geringe Speicherkapazität verfügt.

In Unisphere werden Ereignisse als Meldungen und Warnmeldungen angezeigt. In der Unisphere-CLI werden zusätzliche Ereignisattribute mit ausführlicheren Ereignisberichten als in Unisphere angezeigt. [Konfigurieren von Warnmeldungseinstellungen](#) erläutert die Befehle für die Konfiguration von Warnmeldungen. Weitere Informationen zu Protokollen und Warnmeldungen finden Sie in der Unisphere-Onlinehilfe.

Die einzelnen Ereignisdatensätze und Warnmeldungen sind mit einer ID gekennzeichnet.

In der folgenden Tabelle sind die Attribute für Ereignisdatensätze aufgeführt.

Tabelle 141. Attribute für Ereignisdatensätze

Attribut	Beschreibung
Message ID	Die ID des Ereignisdatensatzes.
Description	Kurze Beschreibung des Ereignisses.
Severity	Schweregrad des Ereignisses. Gültige Werte: <ul style="list-style-type: none"> • <code>info</code> : Es ist ein Ereignis eingetreten, das keine Auswirkungen auf die Funktionsweise des Systems hat. • <code>notice</code> : Es ist ein wichtiges Ereignis eingetreten, das keine Auswirkungen auf die Funktionsweise des Systems hat. • <code>warning</code> : Es ist ein Fehler aufgetreten, der beachtet werden sollte, aber keine bedeutenden Auswirkungen auf das System hat. • <code>error</code> : Es ist ein Fehler aufgetreten, der geringe Auswirkungen auf das System hat. Das Problem sollte in der näheren Zukunft angegangen werden, aber eine unmittelbare Lösung ist nicht erforderlich. • <code>critical</code> : Es ist ein Fehler aufgetreten, der schwerwiegende Auswirkungen auf das System hat und umgehend behoben werden sollte.
Time	Datum und Uhrzeit des Ereignisses in Greenwich Mean Time (GMT).
Node	Name des SP, der das Ereignis ausgelöst hat. Gültige Werte: <ul style="list-style-type: none"> • <code>spa</code> • <code>spb</code>
Process	ID des Systemprozesses, der das Ereignis ausgelöst hat.
Category	Die Ereigniskategorie.

Tabelle 141. Attribute für Ereignisdatensätze (fortgesetzt)

Attribut	Beschreibung
	 ANMERKUNG: Wenn Sie sich beim System angemeldet haben und einen Befehl über die CLI ausführen, werden Ereignisse mit dem Kategorie-Attributwert <i>authentication</i> doppelt aufgeführt, weil Anmeldung und Authentifizierung separate Ereignisse sind.
Account	Das Konto des Benutzers, der das Ereignis ausgelöst hat. Wenn ein Ereignis nicht von einem Benutzer ausgelöst wurde oder das Konto nicht verfügbar ist, wird <i>N/A</i> angezeigt.
Component	Die Systemkomponente, die das Ereignis ausgelöst hat. Diese Informationen richten sich an das Servicepersonal.
Product	Das Produkt, das das Ereignis ausgelöst hat. Diese Informationen richten sich an das Servicepersonal.

Tabelle 142. Attribute für Warnmeldungen

Attribut	Beschreibung
ID	ID der Warnmeldung.
Time	Datum und Uhrzeit (in GMT), an dem die Warnmeldung aufgetreten ist.
Message ID	Warnmeldungs-ID.
Message	Die Warnmeldung.
Description	Die Beschreibung eines Problems.
Severity	Der Schweregrad der Warnmeldung. Gültige Werte: <ul style="list-style-type: none"> info: Es ist ein Ereignis eingetreten, das keine Auswirkungen auf die Funktionsweise des Systems hat. notice: Es ist ein wichtiges Ereignis eingetreten, das keine Auswirkungen auf die Funktionsweise des Systems hat. warning: Es ist ein Fehler aufgetreten, der beachtet werden sollte, aber keine bedeutenden Auswirkungen auf das System hat. error: Es ist ein Fehler aufgetreten, der geringe Auswirkungen auf das System hat. Das Problem sollte in der näheren Zukunft angegangen werden, aber eine unmittelbare Lösung ist nicht erforderlich. critical: Es ist ein Fehler aufgetreten, der schwerwiegende Auswirkungen auf das System hat und umgehend behoben werden sollte.
Acknowledged	Gibt an, ob die Warnmeldung bestätigt wurde oder nicht. Gültige Werte: <ul style="list-style-type: none"> yes no
State	Zeigt den Status der Warnmeldung für jede Warnmeldung an. Mögliche Werte sind: <ul style="list-style-type: none"> Active_Auto: Aktive Warnmeldungen, die nach der Auflösung automatisch gelöscht werden. Active_Manual: Aktive Warnmeldungen, die mit dem Befehl <code>/event/alert/hist deactivate</code> nach der Auflösung manuell gelöscht werden müssen. Inactive: Bereits behobene Warnmeldungen. Updating: Warnmeldungen, die zwischen den anderen Status wechseln.
Duplications	Gibt an, wie viele doppelte Warnmeldungen innerhalb von drei Minuten nach der anfänglichen Warnmeldung aufgetreten sind. Zeigt 0 an, wenn keine doppelten Warnmeldungen vorhanden sind.

Anzeigen von Ereignisdatensätzen

Zeigen Sie ein detailliertes Protokoll der Systemereignisse an. Jedes Ereignis ist ein Datensatz im Protokoll, und jeder Datensatz hat eine eigene ID. Sie können 100 Ereignisdatensätze gleichzeitig anzeigen und nach den Protokollierungszeiträumen sowie dem Schweregrad filtern.

 **ANMERKUNG:** Aktionsbefehl „show“ erläutert, wie das Ausgabeformat geändert wird.

Format

```
/event/log show [-messageID <value>] [-fromTime <value>] [-toTime <value>] [-limit <value>] [-severity {critical | error | warning | notice | info}]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-messageID	Geben Sie die Meldungskennung des Protokoll Datensatzes ein.
-fromTime	Geben Sie ein, ab wann die Ereignisdatensätze angezeigt werden sollen. Das Format für den Zeitpunkt lautet JJJJ-MM-TT HH:MM:SS.  ANMERKUNG: Wenn Sie diesen Qualifizierer weglassen, beginnt die angezeigte Protokollliste mit dem ersten Protokoll.
-toTime	Geben Sie ein, bis wann die Ereignisdatensätze angezeigt werden sollen. Das Format für den Zeitpunkt lautet JJJJ-MM-TT HH:MM:SS.  ANMERKUNG: Wenn Sie diesen Qualifizierer weglassen, wird die aktuelle Systemzeit als Wert verwendet.
-limit	Geben Sie an, wie viele Datensätze maximal angezeigt werden sollen. Der Standardwert von 100 kann nicht überschritten werden.
-severity	Geben Sie ein, ab welchem Schweregrad Ereignisse angezeigt werden. Wenn Sie beispielsweise critical eingeben, werden die Datensätze mit dem Schweregrad „alert“ und „emergency“ ebenfalls angezeigt.

Beispiel

```
uemcli uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /event/log show -messageId "14:70001" -fromTime "2009-11-09 00:00:00.000" -toTime "2009-11-09 23:59:59.999"
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:   Message ID   = 14:70001
     Description = User admin authenticated in authority LocalDirectory/Local
     Severity    = info
     Time        = 2009-11-09 19:43:08.577
     Node        = spa
     Account     = unix/spa/root
     Component   = Server

2:   Message ID   = 14:70001
     Description = User user1 authenticated in authority LocalDirectory/Local
     Severity    = info
     Time        = 2009-11-09 19:41:32.654
     Node        = spa
     Account     = unix/spa/root
     Component   = Server
```

Anzeigen von Warnmeldungs-Verlaufsinformationen

Zeigen Sie eine detaillierte Liste sämtlicher Systemwarnmeldungen an. Wenn eine neue Warnmeldung eingeht, werden Warnmeldungen, die älter als sieben Tage sind, gelöscht.

Format

```
/event/alert/hist show [-state {Active_Manual | Active_Auto | Inactive | Active_Updating | All}]
[-fromTime <value>] [-toTime <value>] [-limit <value>] [-acknowledged {yes | no}] [-severity
{critical | error | warning | notice | info}] [-messageID <value>]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-fromTime	Geben Sie ein, ab wann die Ereignisdatensätze angezeigt werden sollen. Das Format für den Zeitpunkt lautet JJJJ-MM-TT HH:MM:SS.  ANMERKUNG: Wenn Sie diesen Qualifizierer weglassen, beginnt die angezeigte Protokollliste mit dem ersten Protokoll.
-toTime	Geben Sie ein, bis wann die Ereignisdatensätze angezeigt werden sollen. Das Format für den Zeitpunkt lautet JJJJ-MM-TT HH:MM:SS.  ANMERKUNG: Wenn Sie diesen Qualifizierer weglassen, wird die aktuelle Systemzeit als Wert verwendet.
-limit	Geben Sie an, wie viele Datensätze maximal angezeigt werden sollen. Der Standardwert von 100 kann nicht überschritten werden.
-acknowledged	Geben Sie eine Liste der Warnmeldungen an, die bestätigt wurden oder nicht bestätigt wurden. Gültige Werte: <ul style="list-style-type: none"> • yes • no
-severity	Geben Sie ein, ab welchem Schweregrad Ereignisse angezeigt werden. Wenn Sie beispielsweise critical eingeben, werden die Datensätze mit dem Schweregrad „alert“ und „emergency“ ebenfalls angezeigt.
-state	Geben Sie den Status der Warnmeldungen an, die Sie anzeigen möchten. Wenn diese Option nicht angegeben wird, werden nur aktive Warnmeldungen angezeigt. Gültige Werte: <ul style="list-style-type: none"> • Active_Auto : Zeigt alle aktiven Warnmeldungen an, die nach der Auflösung automatisch gelöscht werden. • Active_Manual : Zeigt alle aktiven Warnmeldungen an, die mit dem Befehl /event/alert/hist deactivate nach der Auflösung manuell gelöscht werden müssen. • Inactive : Zeigt alle aufgelösten oder deaktivierten Warnmeldungen an. • Active_Updating : Zeigt alle Warnmeldungen an, die zwischen den Status wechseln. • All : Zeigt alle aktiven und inaktiven Warnmeldungen an.
-messageID	Geben Sie die ID der Warnmeldung an, die Sie anzeigen möchten. Wenn diese Option nicht angegeben wird, werden alle Warnmeldungen angezeigt.

Beispiel

```
uemcli uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /event/alert/hist show -state
Active_Manual -limit 2 -fromTime "2009-11-09 19:43:08" -severity info -messageID 14:38000c
```

```
1: ID = alert_6
   Time = 2019-06-26 07:09:42.100
   Message ID = 14:38000c
   Message = Invalid messaged ID supplied.
   Description = "There are one or more new technical advisories available for viewing on
the Technical Advisories page."
   Severity = error
   Acknowledged = no
   State = Active_Manual(unsolved and need manually marked as inactive after been
solved)
   Duplications = 0

2: ID = alert_3
   Time = 2019-06-26 06:40:15.837
   Message ID = 14:38000c
   Message = There are new advisories available for viewing on the Technical
```

```
Advisories page.  
  Description = "There are one or more new technical advisories available for viewing on  
the Technical Advisories page."  
  Severity    = notice  
  Acknowledged = no  
  State       = Active_Manual(unsolved and need manually marked as inactive after been  
solved)  
  Duplications = 2
```

Bestätigen von Warnmeldungen

Bestätigen Sie spezifische Warnmeldungen.

Format

```
/event/alert/hist -id <value> ack
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die Kennung der Warnmeldung ein, die Sie bestätigen möchten.

Beispiel

Der folgende Befehl bestätigt „alert_2“.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /event/alert/hist -id alert_2 ack
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection  
  
Operation completed successfully.
```

Löschen von Warnmeldungen

Löschen Sie bestimmte Warnmeldungen.

Format

```
/event/alert/hist -id <value> delete
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die Kennung der Warnmeldung ein, die Sie löschen möchten.

Beispiel

Mit dem folgenden Befehl wird die Warnmeldung „alert_3“ gelöscht:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /event/alert/hist -id alert_3 delete
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection  
  
Operation completed successfully.
```

Warnmeldungen deaktivieren

Manuelles Deaktivieren einer Warnmeldung, die sich im Status *Active_Manual* befindet, nachdem sie aufgelöst wurde.

Format

```
/event/alert/hist -id <value> deactivate
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die Kennung der Warnmeldung ein.

Beispiel

Das folgende Beispiel zeigt, wie Sie *alert_1* deaktivieren, das sich im Status *Active_Manual* befindet, nachdem es aufgelöst wurde. Es wird empfohlen, dass Sie keine Warnmeldungen deaktivieren, bei denen das Problem noch nicht behoben wurde. Deaktivierte Warnmeldungen können nicht erneut aktiviert werden. Deaktivieren Sie die Warnmeldung daher nicht, wenn Sie nicht sicher sind, ob Sie aufgelöst wurde oder nicht.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /event/alert/hist -id alert_1 deactivate
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection  
  
You should only deactivate an alert when the issue has been solved. Once the alert has been  
deactivated, it can't be activated again. Do you want to proceed?  
yes / no: yes  
  
Operation completed successfully.
```

Konfigurieren von Warnmeldungseinstellungen

Geben Sie an, wie im System Warnmeldungen, d. h. Benachrichtigungen zu System- und Benutzerereignissen, verarbeitet werden. Sie können festlegen, dass die Warnmeldungen direkt an Ihren Serviceanbieter gesendet und per E-Mail an bestimmte Adressen weitergeleitet werden. Sie können auch festlegen, dass Warnmeldungen als Traps an SNMP-Ziele gesendet werden. Weitere Einzelheiten zum Einrichten eines Ziels im Hinblick auf den Empfang von Warnmeldungen via SNMP finden Sie unter [Konfigurieren von SNMP-Zielen für Warnmeldungen](#). Unter [Anzeigen von Ereignisprotokollen und Warnmeldungen](#) finden Sie Details zur Anzeige der aktuellen Protokolle und Alarmmeldungen.

 **ANMERKUNG:** Um E-Mail-Warnmeldungen versenden zu können, müssen Sie einen SMTP-Server wie unter [Managen von SMTP-Servereinstellungen](#) erläutert im System konfigurieren.

In der folgenden Tabelle sind die Attribute für Warnmeldungen aufgeführt:

Tabelle 143. Attribute für Warnmeldungen

Attribut	Beschreibung
Language	Sprache, in der E-Mail-Warnmeldungen versendet werden.

Tabelle 143. Attribute für Warnmeldungen (fortgesetzt)

Attribut	Beschreibung
E-mail from address	E-Mail-Adresse, von der Warnmeldungs-E-Mails gesendet werden.
SNMP severity threshold	Der Schweregrad, ab dem Warnmeldungen als SNMP-Traps versendet werden. Gültige Werte: <ul style="list-style-type: none"> • critical: Es ist ein Fehler aufgetreten, der schwerwiegende Auswirkungen auf das System hat und umgehend behoben werden sollte. • error: Es ist ein Fehler aufgetreten, der geringe Auswirkungen auf das System hat. Das Problem sollte in der näheren Zukunft angegangen werden, aber eine unmittelbare Lösung ist nicht erforderlich. • warning: Es ist ein Fehler aufgetreten, der beachtet werden sollte, aber keine bedeutenden Auswirkungen auf das System hat. • notice: Es ist ein wichtiges Ereignis eingetreten, das keine Auswirkungen auf die Funktionsweise des Systems hat. • info: Es ist ein Ereignis eingetreten, das keine Auswirkungen auf die Funktionsweise des Systems hat.
SNMP version	Die SNMP-Version, die am Ziel ausgeführt wird.
SNMP engine ID	Die ID der SNMP-Engine für das SNMP-Ziel.
Show all pool threshold alerts	Gibt an, ob Schwellenwertwarnmeldungen für den Prozentsatz der Poolspeicherplatz-Nutzung aktiviert sind. Mögliche Werte sind: <ul style="list-style-type: none"> • yes • no <p>ANMERKUNG: Unabhängig davon, ob dies aktiviert ist, werden Warnmeldungen immer für Thin-Provisioning-Pools gesendet, die überbelegt sind.</p>
Call home suppression start time	Datum und Uhrzeit, zu der die Call-Home-Unterdrückung gestartet werden soll.
Call home suppression end time	Datum und Uhrzeit, zu der die Call-Home-Unterdrückung beendet werden soll.

Anzeigen von Warnmeldungseinstellungen

Zeigen Sie die Einstellungen zum Umgang mit den Warnmeldungen im System an.

Format

```
/event/alert/conf show
```

Beispiel

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /event/alert/conf show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:   Language                = en-US
     SNMP severity threshold = Info
     SNMP version           = 3.0
     SNMP engine ID        =
     Show all pool threshold alerts = no
     Call home suppression start time= 2017-04-10 00:00:00
     Call home suppression end time  = 2017-04-12 00:00:00
```

Warnmeldungseinstellungen ändern

Konfigurieren Sie die Einstellungen zum Umgang mit den Warnmeldungen im System.

i ANMERKUNG: Damit die E-Mail-Warnmeldungen funktionieren, müssen Sie einen SMTP-Server im System konfigurieren. Hinweise dazu finden Sie unter [Managen von SMTP-Servereinstellungen](#).

Format

```
/event/alert/conf set [-emailFromAddr <value>] [-snmpSeverity {critical|error|warning|notice|info}] [-showAllPoolThresholdAlerts {yes | no}] [{"-callHomeSuppressionEndTime <value> | -stopCallHomeSuppression}]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-emailFromAddr	Geben Sie eine E-Mail-Adresse an, von der Warnmeldungen gesendet werden.
-snmpSeverity	Hier geben Sie den Schweregrad der Warnmeldungen an, ab dem SNMP-Traps versendet werden. Mögliche Werte sind: <ul style="list-style-type: none">• critical• error• warning• notice• info
-showAllPoolThresholdAlerts	Geben Sie an, ob die Warnmeldung aufgrund eines überschrittenen Poolschwellenwerts erzeugt wurde. Gültige Werte: <ul style="list-style-type: none">• yes• no
-callHomeSuppressionEndTime	Geben Sie Datum und Uhrzeit an, zu der die Call-Home-Unterdrückung beendet werden soll. Das Gesamtzeitfenster für die Unterdrückung ist die Zeit zwischen der aktuellen Uhrzeit und der Unterdrückungs-Endzeit bzw. bei laufenden Unterdrückungs-Zeitfenstern die Zeit zwischen der Startzeit und der Unterdrückungs-Endzeit. Das Zeitfenster für die Unterdrückung kann zwischen 1 und 48 Stunden betragen (in 1-Minuten-Schritten). i ANMERKUNG: Verwenden Sie diese Option, um die Call-Home-Warnmeldungen temporär zu unterdrücken, wenn Sie bestimmte Serviceaktionen auf Ihrem System ausführen müssen.
-stopCallHomeSuppression	Geben Sie dies an, um die Call-Home-Unterdrückung zu deaktivieren.

Beispiel 1

Mit dem folgenden Befehl werden die folgenden Warnmeldungseinstellungen geändert:

- Absenderadresse: from@email.com.
- Mindest-Schweregrad für den Versand von SNMP-Traps: error

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /event/alert/conf set -emailFromAddr "from@mail.com" -snmpSeverity error
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Beispiel 2

Mit dem folgenden Befehl wird die Endzeit für die Unterdrückung von Call-Home-Warnmeldungen festgelegt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /event/alert/conf set --stopCallHomeSuppression
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Konfigurieren der Einstellungen für Warnmeldungen per E-Mail

Legen Sie Einstellungen für Warnmeldungen per E-Mail fest.

Tabelle 144. Attribute für Warnmeldungen per E-Mail

Attribut	Beschreibung
ID	ID der Konfiguration für die Warnmeldungs-E-Mails
Address	E-Mail-Adresse, von der Warnmeldungs-E-Mails gesendet werden.
Severity threshold	Mindestschweregrad, ab dem Warnmeldungen per E-Mail versendet werden. Gültige Werte: <ul style="list-style-type: none">• critical: Es ist ein Fehler aufgetreten, der schwerwiegende Auswirkungen auf das System hat und umgehend behoben werden sollte.• error: Es ist ein Fehler aufgetreten, der geringe Auswirkungen auf das System hat. Das Problem sollte in der näheren Zukunft angegangen werden, aber eine unmittelbare Lösung ist nicht erforderlich.• warning: Es ist ein Fehler aufgetreten, der beachtet werden sollte, aber keine bedeutenden Auswirkungen auf das System hat.• notice: Es ist ein wichtiges Ereignis eingetreten, das keine Auswirkungen auf die Funktionsweise des Systems hat.• info: Es ist ein Ereignis eingetreten, das keine Auswirkungen auf die Funktionsweise des Systems hat.

Konfigurieren der Einstellungen für Warnmeldungen per E-Mail

Sie können die Einstellungen für Warnmeldungen vom Typ „E-Mail an“ konfigurieren.

Format

```
/event/alert/conf/emailto create -addr <value> [ -severity {critical | error | warning | notice | info} ]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-addr	Geben Sie eine E-Mail-Adresse zum Empfangen der Warnmeldungen an.
-severity	Geben Sie einen Mindestschweregrad an, ab dem der E-Mail-Versand ausgelöst wird. Gültige Werte: <ul style="list-style-type: none">• critical• error• warning• notice (Standardeinstellung)• info

Beispiel

Dieses Beispiel zeigt die Konfiguration von „stuff1@mail.com“ als „E-Mail an“-Adresse und des Schweregrads „info“ als Mindestschweregrad.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /event/alert/conf/emailto create -addr stuff1@mail.com -severity info
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = alertEmailConfig_1
Operation completed successfully.
```

Ändern der Einstellungen für Warnmeldungen per E-Mail

Sie können die aktuelle Konfiguration für die Warnmeldung „E-Mail an“ ändern.

Format

```
/event/alert/conf/emailto { -id <value> | -addr <value> } set [ -newAddr <value> ] [ -severity { info | notice | warning | error | critical } ]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID der Warnmeldungsconfiguration an, die Sie ändern möchten.
-addr	Geben Sie die Adresse für den Warnmeldungstyp „E-Mail an“ ein, bei der Sie Einstellungen ändern möchten.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-newAddr	Geben Sie eine neue E-Mail-Adresse zum Empfangen der Warnmeldungen an.
-severity	Geben Sie den neuen Mindestschweregrad an, ab dem der E-Mail-Versand ausgelöst wird. Gültige Werte: <ul style="list-style-type: none">• critical• error• warning• notice• info

Beispiel

Der folgende Befehl ändert die Adresse für „E-Mail an“ in „stuff1@newmail.com“ und gibt an, dass der Mindestschweregrad zum Auslösen des E-Mail-Versands „info“ ist.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /event/alert/conf/emailto -addr stuff1@mail.com set -newAddr stuff1@newmail.com -severity info
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = alertEmailConfig_1
Operation completed successfully.
```

Anzeigen der Einstellungen für Warnmeldungen per E-Mail

Sie können die Einstellungen für Warnmeldungen vom Typ „E-Mail an“ anzeigen.

Format

```
/event/alert/conf/emailto [{ -id <value> | -addr <value>}] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID der Warnmeldungskonfiguration ein, die Sie anzeigen möchten.
-addr	Geben Sie die Adresse für den Warnmeldungstyp „E-Mail an“ ein, deren Einstellungen Sie anzeigen möchten.

Beispiel

Mit diesem Befehl wird die Konfiguration aller E-Mail-Adressen für Warnmeldungen auf dem System angezeigt.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /event/alert/conf/emailto show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      ID          = alertEmailConfig_1
      Address      = stuff1@mail.com
      Severity threshold = Info

2:      ID          = alertEmailConfig_2
      Address      = stuff2@mail.com
      Severity threshold = Notice

3:      ID          = alertEmailConfig_3
      Address      = stuff3@mail.com
      Severity threshold = Notice
```

Testen der Einstellungen für E-Mail-Warnmeldungen

Senden Sie eine Test-E-Mail an alle E-Mail-Adressen, die zum Erhalt von Warnmeldungsbenachrichtigungen konfiguriert wurden.

Format

```
/event/alert/conf testEmailAlert
```

Beispiel

Das folgende Beispiel zeigt, wie Einstellungen für Warnmeldungen per E-Mail getestet werden.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /event/alert/conf testEmailAlert
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

Operation completed successfully.

Löschen von Einstellungen für Warnmeldungen per E-Mail

Sie können die Konfigurationen für Warnmeldungen per E-Mail löschen.

Format

```
/event/alert/conf/emailto -id <value> delete
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID der Warnmeldungskonfiguration ein, die Sie löschen möchten.

Beispiel

Der folgende Befehl ändert die Adresse für „E-Mail an“ in „stuff1@newmail.com“ und gibt an, dass der Mindestschweregrad zum Auslösen des E-Mail-Versands „info“ ist.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /event/alert/conf/emailto -id alertEmailConfig_1 delete
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection
```

Operation completed successfully.

Konfigurieren von SNMP-Zielen für Warnmeldungen

Im System wird das Simple Network Management Protocol (SNMP) zur Übertragung von Systemwarnmeldungen als Traps auf einen SNMP-Zielhost verwendet. Bei Traps handelt es sich um asynchrone Meldungen, mit denen das SNMP-Ziel bei System- und Benutzerereignissen benachrichtigt wird. Die drei Trap-Typen sind:

- Informationen: Routinestatusinformationen zu Systemvorgängen.
- Warnungen: Es ist ein Problem aufgetreten oder es wird ein Problem auftreten.
- Fehler: Systemprobleme, die aufgetreten sind oder gerade auftreten.

Sie können konfigurieren, zu welchen Arten von Warnmeldungen (Informationen, Fehler, Notfälle) Berichte ausgegeben werden.

Die einzelnen SNMP-Ziele verfügen über eigene IDs.

In der folgenden Tabelle sind die Attribute für SNMP-Ziele aufgeführt:

Tabelle 145. Attribute für SNMP-Ziele

Attribut	Beschreibung
ID	Die ID des SNMP-Ziels.
Host	Der Hostname bzw. die IP-Adresse des SNMP-Ziels.
Port	Der Hostport am SNMP-Ziel, an dem die Traps eingehen.
User name	Der Benutzername für den Zugriff auf das SNMP-Ziel.
Auth protocol	Das für die Authentifizierung des Zugriffs auf das SNMP-Ziel verwendete Protokoll. Folgende Werte sind möglich: <ul style="list-style-type: none">• none: Keine Authentifizierung

Tabelle 145. Attribute für SNMP-Ziele (fortgesetzt)

Attribut	Beschreibung
	<ul style="list-style-type: none"> ● md5: Message-Digest-Algorithmus 5 ● sha: Secure Hash-Algorithmus
Auth password	Authentifizierungspasswort für den Zugriff auf das SNMP-Ziel.
Privacy protocol	Das Protokoll, das zur Aktivierung des Datenschutzes auf dem SNMP-Ziel verwendet wird. Mit dem Protokoll werden die SNMP-Pakete verschlüsselt. Folgende Werte sind möglich: <ul style="list-style-type: none"> ● none: Keine Verschlüsselung ● aes: Advanced Encryption Standard ● des: Data Encryption Standard
Privacy password	Das Datenschutzpasswort für das Datenschutzprotokoll.

Erstellen von SNMP-Zielen

Erstellen Sie ein SNMP-Trap-Ziel für Systemwarnmeldungen.

Format

```
/event/alert/snmp create -host <value> -port <value> -userName <value> [ -authProto { none | md5 { -authPassword <value> | -authPasswordSecure } [ -privProto { none | aes { -privPassword <value> | -privPasswordSecure } | des { -privPassword <value> | -privPasswordSecure } } ] | sha { -authPassword <value> | -authPasswordSecure } [ -privProto { none | aes { -privPassword <value> | -privPasswordSecure } } ] ] | -v2c -community <value> }
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-host	Geben Sie den Hostnamen oder die IP-Adresse des SNMP-Ziels ein.
-port	Geben Sie den Hostport am SNMP-Ziel an, an dem die Traps eingehen.
-userName	Geben Sie den Benutzernamen an, der für den Zugriff auf das SNMP-Ziel verwendet wird.
-authProto	Geben Sie das Protokoll an, das zur Authentifizierung des Zugriffs auf das SNMP-Ziel verwendet wird. Folgende Werte sind möglich: <ul style="list-style-type: none"> ● none: Keine Authentifizierung ● md5: Message-Digest-Algorithmus 5 ● sha: Secure Hash-Algorithmus
-authPassword	Geben Sie das Authentifizierungspasswort ein.
-authPasswordSecure	Geben Sie das Passwort im sicheren Modus an. Der Benutzer wird aufgefordert, das Passwort einzugeben.
-privProto	Geben Sie das Protokoll an, das zur Aktivierung des Datenschutzes auf dem SNMP-Ziel verwendet wird. Folgende Werte sind möglich: <ul style="list-style-type: none"> ● none: Keine Verschlüsselung ● aes: Advanced Encryption Standard ● des: Data Encryption Standard
-privPassword	Geben Sie das Datenschutzpasswort ein.
-privPasswordSecure	Geben Sie das Passwort im sicheren Modus an. Der Benutzer wird aufgefordert, das Passwort einzugeben.
-v2c	Geben Sie an, dass ein SNMP v2c-Ziel erstellt werden soll.

Qualifizierer	Beschreibung
-community	Geben Sie die SNMP v2c-Ziel-Community-Zeichenfolge an.

Beispiel

Mit dem folgenden Befehl wird ein SNMP-Ziel mit den folgenden Einstellungen erstellt:

- Host-IP: 10.64.75.1
- Hostport: 333
- Benutzername: user1
- Autorisierungsprotokoll: md5
- Autorisierungspasswort: authpassword1234
- Datenschutzprotokoll: des
- Datenschutzpasswort: privpassword321

Das SNMP-Ziel erhält die ID „Host1_333“:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /event/alert/snmp create -host 10.64.75.1
-port 333 -userName user1 authProto md5 -authPassword authpassword1234 -privProto des -
privPassword privpassword321
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = Host1_333
Operation completed successfully.
```

Anzeigen von SNMP-Zielen

Anzeigen von Details zu SNMP-Zielen Sie können nach der ID des SNMP-Ziels filtern.

 **ANMERKUNG:** Aktionsbefehl „show“ erläutert, wie das Ausgabeformat geändert wird.

Format

```
/event/alert/snmp [-id <value>] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID eines SNMP-Ziels ein.

Beispiel

Mit dem folgenden Befehl werden sämtliche SNMP-Ziele aufgeführt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /event/alert/snmp show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
1:   ID           = snmp_target_1
     Version      = v3
     Host         = 10.0.1.3
     Port        = 123
     User name    = v3User
```

```

Auth protocol      = None
Privacy protocol   = None
Community          =

2:  ID              = snmp_target_2
    Version         = v2c
    Host            = 10.0.1.3
    Port           = 879
    User name       =
    Auth protocol   =
    Privacy protocol =
    Community       = v2CommunityStr

```

Ändern der Einstellungen für das SNMP-Ziel

Ändern Sie die Einstellungen für ein SNMP-Ziel.

Format

```

/event/alert/snmp -id <value> set [ -host <value> ] [ -port <value> ] [ -userName <value> ]
[ -authProto { none | md5 { -authPassword <value> | -authPasswordSecure } [ -privProto { none
| aes { -privPassword <value> | -privPasswordSecure } | des { -privPassword <value> |
-privPasswordSecure } } ] | sha { -authPassword <value> | -authPasswordSecure } [ -privProto
{ none | aes { -privPassword <value> | -privPasswordSecure } | des { -privPassword <value> |
-privPasswordSecure } } ] ] ] | [ -community <value> ] }

```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des zu ändernden SNMP-Ziels ein.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-host	Geben Sie den Hostnamen oder die IP-Adresse des SNMP-Ziels ein.
-port	Geben Sie den Hostport am SNMP-Ziel an, an dem die Traps eingehen.
-userName	Geben Sie den Benutzernamen an, der für den Zugriff auf das SNMP-Ziel verwendet wird.
-authProto	Geben Sie das Protokoll an, das zur Authentifizierung des Zugriffs auf das SNMP-Ziel verwendet wird. Folgende Werte sind möglich: <ul style="list-style-type: none"> • none: Keine Authentifizierung • md5: Message-Digest-Algorithmus 5 • sha: Secure Hash-Algorithmus
-authPassword	Geben Sie das Authentifizierungspasswort ein.
-authPasswordSecure	Geben Sie das Passwort im sicheren Modus an. Der Benutzer wird aufgefordert, das Passwort einzugeben.
-privProto	Geben Sie das Protokoll an, das zur Aktivierung des Datenschutzes auf dem SNMP-Ziel verwendet wird. Folgende Werte sind möglich: <ul style="list-style-type: none"> • none: Keine Verschlüsselung • aes: Advanced Encryption Standard • des: Data Encryption Standard
-privPassword	Geben Sie das Datenschutzpasswort ein.
-privPasswordSecure	Geben Sie das Passwort im sicheren Modus an. Der Benutzer wird aufgefordert, das Passwort einzugeben.

Qualifizierer	Beschreibung
-community	Geben Sie die SNMP v2c-Ziel-Community-Zeichenfolge an.

Beispiel

Mit dem folgenden Befehl ändern Sie das Autorisierungsprotokoll, das Datenschutzprotokoll, das Autorisierungspasswort und das Datenschutzpasswort für SNMP-Ziel Host1_323:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /event/alert/snmp -id Host1_323 set -authProto md5 -authPassword newauthpassword -privProto des -privPassword newprivpassword
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = Host1_323
Operation completed successfully.
```

Löschen von SNMP-Zielen

Löschen Sie ein SNMP-Ziel.

 **ANMERKUNG:** Wenn Sie ein SNMP-Ziel löschen, werden keine Warnmeldungen mehr als Traps an das System gesendet.

Format

```
/event/alert/snmp -id <value> delete
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die ID des zu löschenden SNMP-Ziels ein.

Beispiel

Mit dem folgenden Befehl wird SNMP-Ziel Host1_323 gelöscht:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /event/alert/snmp -id Host1_323 delete
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
Operation completed successfully.
```

Warten des Systems

Themen:

- Ändern des Servicepassworts
- Wartung des Systems
- Managen von Core-Speicherauszugsdateien
- Managen von Serviceinformationen
- Managen des SSH-Zugriffs
- Warten des Speicherprozessors (SP)

Ändern des Servicepassworts

Das System wird mit einem Standardservicepasswort ausgeliefert, mit dem Wartungsarbeiten am System durchgeführt werden können. Das alte Servicekennwort kann nach dem Ändern des Passworts nicht mehr verwendet werden.

Voraussetzungen

Beide Speicherprozessoren (SPs) müssen sich im System befinden und als Startmodus den Normalmodus aufweisen. Wenn Sie einen SP entfernt haben oder bei einem SP ein Fehler aufgetreten ist, müssen Sie den SP ersetzen, um das Servicepasswort ändern zu können.

Format

```
/service/user set { -passwd <value> | -passwdSecure } { { -oldpasswd <value> |
-oldpasswdSecure } | -force }
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-passwd	Geben Sie ein neues Servicepasswort ein. Die Anforderungen an das Passwort lauten wie folgt: <ul style="list-style-type: none"> • Kennwörter müssen 8 bis 64 Zeichen lang sein und mindestens einen Groß- und Kleinbuchstaben sowie eine Zahl enthalten. • Kennwörter dürfen kein einfaches Anführungszeichen ('), kaufmännisches Und-Zeichen (&) oder Leerzeichen enthalten. • Beim Wechsel des Kennworts darf nicht auf die drei unmittelbar zuvor verwendeten Kennwörter zurückgegriffen werden.
-passwdSecure	Geben Sie das Kennwort im sicheren Modus an – der Nutzer wird aufgefordert, das Kennwort und die Kennwortbestätigung einzugeben.
-oldpasswd	Geben Sie das alte Passwort ein, damit Sie das neue Passwort festlegen können.
-oldpasswdSecure	Gibt das Kennwort im sicheren Modus an – der Nutzer wird aufgefordert, das Kennwort einzugeben.
-force	Geben Sie an, ob dies eine Anfrage zur Passwortänderung oder zur Passwortzurücksetzung ist. Dieser Qualifizierer ist nur für Servicenutzer vorgesehen.

Beispiel

Mit dem folgenden Befehl ändern Sie das Servicepasswort: Der Befehl kann nur im Normalmodus ausgeführt werden.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /service/user set -passwd NewPassword456! -oldpasswd OldPassword456!
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection  
  
Operation completed successfully.
```

Wartung des Systems

Wenden Sie Serviceaktionen auf das System an. Dieser Befehl muss mit Servicebenutzer-Anmeldedaten ausgeführt werden.

Neustarten der Managementsoftware

Startet die Managementsoftware auf dem System neu. Der Befehl kann nur im Normalmodus ausgeführt werden.

Format

```
/service/system restart
```

Beispiel

Mit dem folgenden Befehl wird die Managementsoftware des Systems neu gestartet:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /service/system restart
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection  
  
Operation completed successfully.
```

Herunterfahren des Systems

Schaltet das System aus.

 **ANMERKUNG:** Der Befehl kann nur im Normalmodus ausgeführt werden.

Format

```
/service/system shutdown
```

Beispiel

Mit dem folgenden Befehl wird das System heruntergefahren (nur im Normalmodus):

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /service/system shutdown
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection  
  
Operation completed successfully.
```

Erneutes Initialisieren des Systems

Initialisieren Sie das Speichersystem erneut. Zur Ausführung dieser Aktion sollte sich das System im Servicemodus befinden.

Format

```
/service/system reinit
```

Beispiel

Mit dem folgenden Befehl wird das Speichersystem erneut initialisiert:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /service/system reinit
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Sammeln von Serviceinformationen

Sammeln Sie Informationen zu Ihrem System, und speichern Sie sie in einer Datei. Die Datei kann dann mithilfe des Befehls `uemcli -download` heruntergeladen werden. (Siehe [Anzeigen der Befehlszeilenoptionen](#)).

Format

```
/service/system collect {-serviceInfo [-type {full | perfAssessment | perfTrace}] | -config [-showPrivateData]}
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
<code>-serviceInfo</code>	Sammeln Sie Informationen zu Ihrem System und speichern Sie sie in einer <code>.tar</code> -Datei. Ihr Serviceprovider kann die gesammelten Informationen zur Analyse Ihres Systems nutzen.
<code>-type</code>	Geben Sie den Typ der zu sammelnden Serviceinformation an. Gültige Werte: <ul style="list-style-type: none">• <code>full</code> (Standardeinstellung): Vollständigen Satz Serviceinformationen sammeln• <code>perfAssessment</code>: Sammeln Sie Serviceinformationen für die Durchführung einer Leistungskontrolle.• <code>perfTrace</code>: Sammeln Sie Serviceinformationen für die Durchführung einer Nachverfolgung.• <code>minimum</code>: Sammeln Sie einen Mindestsatz von Serviceinformationen (nur Protokolldateien).
<code>-config</code>	Erstellen Sie einen Snapshot der aktuellen Systemkonfiguration und speichern Sie ihn in einer Datei. Er erfasst alle Daten, die erforderlich sind, um die aktuelle Konfiguration auf einem neuen oder erneut initialisierten System neu zu erstellen. Er erfasst keine Protokolldateien oder andere Arten von Diagnosedaten.
<code>-showPrivateData</code>	Einschließen vertraulicher Informationen (wie etwa IP-Adressen) in die gesammelten Daten.

Beispiel 1

Mit dem folgenden Befehl werden Informationen über das System gesammelt und in einer Datei gespeichert:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /service/system collect -serviceInfo
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
Operation completed successfully.
```

Beispiel 2

Mit dem folgenden Befehl werden Serviceinformationen über die Systemleistung gesammelt und in einer Datei gespeichert.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /service/system collect -serviceInfo -type perfAssessment
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection
```

```
Operation completed successfully.
```

Managen von Core-Speicherauszugsdateien

Managen Sie die Liste der Core-Speicherauszugsdateien, die Systeminformationen enthalten, die der Support zur Fehlerbehebung verwendet.

Core-Speicherauszugsdateien werden vom System immer dann erzeugt, wenn ein SP-Fehler vorliegt. Core-Speicherauszugsdateien werden vom Support zur Fehlerbehebung und Problemlösung verwendet.

Tabelle 146. Core-Speicherauszugsattribute

Attribut	Beschreibung
ID	Gibt die eindeutige Kennung der Core-Speicherauszugsdatei an.
Name	Name der Core-Speicherauszugsdatei
Creation time	Datum und Uhrzeit der Erzeugung der Core-Speicherauszugsdatei
File size	Die Gesamtgröße aller Core-Speicherauszugsdateien im Ordner „dump“.

Anzeigen von Core-Speicherauszügen

Zeigen Sie eine Liste der vom System für beide Speicherprozessoren erzeugten Core-Speicherauszugsdateien an. Die Datei können mithilfe des Befehls `uemcli -download` heruntergeladen werden. (Siehe [Anzeigen der Befehlszeilenoptionen](#)).

Format

```
/service/system/dump [-id <value>] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Gibt die eindeutige Kennung der Core-Speicherauszugsdatei an.

Beispiel

Der folgende Befehl zeigt eine Liste der System-Core-Speicherauszüge.

```
uemcli -d 10.0.0.1 -u local/serviceuser -p Password /service/system/dump -id
"mspb:logDaemon_:2017-03-15_07_34_54_878_logDaemon.x" show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      ID              = mspb:logDaemon_:2017-03-15_07_34_54_878_logDaemon.x
      Name              =
logDaemon_dump_spb_FCNCH097052190_2017-03-15_07_34_54_878_logDaemon.x_dir
      Creation time     = 2017-03-15 07:34:54.000
      File size         = 126MB
```

Löschen von Core-Speicherauszügen

Löschen Sie eine Core-Speicherauszugsdatei aus der vom System generierten Liste der Core-Speicherauszüge.

Format

```
/service/system/dump {-id <value>} delete
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie die eindeutige Kennung der Core-Speicherauszugsdatei an, die gelöscht werden soll.

Beispiel

Der folgende Befehl löscht einen Core-Speicherauszug durch Angabe seines Namens.

```
uemcli -d 10.0.0.1 -u local/serviceuser -p Password /service/system/dump -id
mspa:CP_:2016-06-22_15_13_20_19151_ECOM delete
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Managen von Serviceinformationen

Managen und listen Sie die Serviceinformationsdateien auf, die auf Ihrem System erzeugt wurden.

Tabelle 147. Attribute der Serviceinformationsdatei

Attribut	Beschreibung
ID	Gibt die eindeutige Kennung der Serviceinformationsdatei an.
Name	Name der Serviceinformationsdatei.
Creation time	Datum und Uhrzeit der Erzeugung der Serviceinformationsdatei.
File size	Gesamtgröße aller Serviceinformationsdateien im System

Anzeigen der Liste „Serviceinformationsdatei“

Zeigen Sie die Liste der Serviceinformationsdateien an, die auf Ihrem System erzeugt werden.

Verwenden Sie den Befehl `uemcli -download`, um die Serviceinformationsdateien herunterzuladen. Detaillierte Informationen zur Verwendung finden Sie im Abschnitt [Switches anzeigen](#).

Format

```
/service/system/serviceInfo [-id <value>] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Geben Sie optional die ID der Serviceinformationsdatei an, die Sie anzeigen möchten.

Beispiel

Das folgende Beispiel zeigt die Liste der Serviceinformationsdateien.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /service/system/serviceInfo show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:   ID           = m2018-12-31_20_19_02:spa__VNxe3200
     Name        = spa__VNxe3200_service_data_FCnCH097274951_2018-12-31_20_19_02.tar
     Creation time = 2018-12-31T20:23:35.000Z
     File size    = 100MB
```

Managen des SSH-Zugriffs

Verwalten Sie den SSH-Zugriff (Secure Shell) auf das System. Dieser Befehl muss mit Servicebenutzer-Anmeldedaten ausgeführt werden.

Einrichten von SSH-Zugriff

Managen Sie den SSH-Zugriff auf das System.

Format

```
/service/ssh set -enabled {yes | no}
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-enabled	Flag, die anzeigt, ob der SSH-Zugriff aktiviert ist. Die Anforderungen an das Passwort lauten wie folgt: Folgende Werte sind möglich: <ul style="list-style-type: none">• yes• no

Beispiel

Mit dem folgenden Befehl wird der SSH-Zugriff auf das System aktiviert:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /service/ssh set -enabled yes
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection  
  
Operation completed successfully.
```

Anzeigen von SSH-Einstellungen

Zeigt die SSH-Einstellungen an.

Format

```
/service/ssh show
```

Beispiel

Mit dem folgenden Befehl werden die SSH-Einstellungen angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /service/ssh show
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection  
  
1:      SSH enabled      = yes
```

Warten des Speicherprozessors (SP)

Ermöglicht Benutzern das Anwenden von Serviceaktionen auf den Speicherprozessor. Dieser Befehl muss mit Servicebenutzer-Anmeldedaten ausgeführt werden.

Starten des Servicemodus

Schalten Sie den Speicherprozessor in den Servicemodus um. Dieser Befehl kann nur im Normalmodus ausgeführt werden.

Format

```
/service/sp -id <value> service
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Identifiziert den Speicherprozessor.

Beispiel

Mit dem folgenden Befehl wird in den Servicemodus umgeschaltet:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /service/sp -id spa service
```

```
Storage system address: 10.0.0.1  
Storage system port: 443
```

```
HTTPS connection
```

```
Operation completed successfully.
```

Reboot

Starten Sie den Speicherprozessor neu.

Format

```
/service/sp -id <value> reboot
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Identifiziert den Speicherprozessor.

Beispiel

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /service/sp -id spa reboot
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection  
  
Operation completed successfully.
```

Neues Image erstellen

Erstellen Sie ein neues Image des Speicherprozessors.

Format

```
/service/sp -id <value> reimage
```

Objektqualifizierer

Qualifizierer	Beschreibung
-id	Identifiziert den Speicherprozessor.

Beispiel

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /service/sp -id spa reimage
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection  
  
Operation completed successfully.
```

Messwerte managen

Themen:

- Service zum Managen von Messwerten
- Managen von Messwerteinstellungen
- Werte von Verlaufsmesswerten managen
- Echtzeitmesswerte managen

Service zum Managen von Messwerten

Speichersystemmesswerte erfassen Informationen über die Systemperformance und die Speicherauslastung und sammeln diese Informationen zur Überprüfung durch den Benutzer. Durch die Analyse der Systemmesswerte kann das zukünftige Wachstum des Systems geplant werden.

Verlaufs- und Echtzeitmesswerte sind in vordefinierten Intervallen verfügbar. Hochfrequente Messwerte (kurzes Intervall) werden nicht so lange wie niederfrequente Messwerte (langes Intervall) aufbewahrt.

In der folgenden Tabelle sind die Messwertserviceattribute aufgeführt:

Tabelle 148. Messwertserviceattribute

Attribut	Beschreibung
History enabled	Gibt an, ob die Erfassung von Verlaufsmesswerten aktiviert ist. Folgende Werte sind möglich: <ul style="list-style-type: none"> • yes • no Der Standardwert beträgt yes.
History retention	Identifiziert den Zeitstempel des frühesten verfügbaren Werts für jedes Frequenzintervall. Die Formate sind: <ul style="list-style-type: none"> • YYYY-MM-DD HH:MM:SS (60 Sek.) • YYYY-MM-DD HH:MM:SS (300 Sek.) • YYYY-MM-DD HH:MM:SS (3600 Sek.) • YYYY-MM-DD HH:MM:SS (14400 Sek.) Wenn die Daten für ein bestimmtes Intervall nicht verfügbar sind, zeigt das System „not available“ anstatt eines Zeitstempels an. <p>i ANMERKUNG: Die Zeitstempel weisen standardmäßig die UTC-Zeit auf. Wenn Sie mit <code>-gmt.off</code> eine andere Zeitzone angeben, werden die Zeitstempel entsprechend angepasst.</p>

Messwertserviceeinstellungen anzeigen

Zeigen Sie die aktuellen Messwertserviceeinstellungen an.

i **ANMERKUNG:** Verwenden Sie den Befehl „show action“, um das Ausgabeformat zu ändern.

Format

```
/metrics/service show
```

Beispiel

Mit dem folgenden Befehl werden die Messwertserviceeinstellungen für das System angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /metrics/service show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1: History enabled = yes
   History retention= 2012-9-20 12:00:00 (60 sec), 2012-9-14 12:00:00 (300 sec), not
   available (3600 sec), not available (14400 sec)
```

Messwertservice konfigurieren

Verlaufsmesswernerfassung aktivieren.

Format

```
/metrics/service set -historyEnabled { yes | no }
```

 **ANMERKUNG:** Nur Administratoren dürfen diesen Befehl ausführen.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-historyEnabled	Gibt an, ob die Erfassung von Verlaufsmesswerten aktiviert oder deaktiviert ist. Folgende Werte sind möglich: <ul style="list-style-type: none">• yes• no <p> ANMERKUNG: Das System fordert eine Bestätigung an, wenn Sie no angeben.</p>

Beispiel

Der folgende Befehl aktiviert die Messwernerfassung:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /metrics/service set -historyEnabled yes
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
Operation completed successfully.
```

Managen von Messwerteinstellungen

Speichersystemmesswerte erfassen Informationen über die Systemperformance und die Speicherauslastung und sammeln diese Informationen zur Überprüfung durch den Benutzer. Durch die Analyse der Systemmesswerte kann das zukünftige Wachstum des Systems geplant werden.

In der folgenden Tabelle sind die Messwertattribute aufgeführt:

Tabelle 149. Messwertattribute

Attribut	Beschreibung
Path	Eindeutige ID für den Messwert.  ANMERKUNG: Messwerte sind normalerweise Objekten zugeordnet. Diese Zuordnung wird durch das Zeichen "*" im Messwertpfad dargestellt, zum Beispiel sp.*.net.device.*.bytes , der zwei Objekten zugeordnet ist, SP und dem Netzwerkgerät. Die Messwertbefehle akzeptieren einen Messwertpfad, bei dem das * durch ein Objekt ersetzt ist, und geben nur das Ergebnis für das angegebene Objekt zurück. Das System erzeugt einen Fehler, wenn das angegebene Objekt ungültig ist.
Description	Beschreibung des Messwerts.
Type	Messwerttyp. Gültige Werte: <ul style="list-style-type: none"> • <code>rate</code>: Ein Zählerunterschied in Bezug auf eine Zeiteinheit. • <code>counter</code>: Eine monoton zunehmende, nicht signierte Menge. • <code>fact</code>: Stellt Point-in-Time-Informationen dar. Tatsachenwerte gehen voraussichtlich auf und ab. • <code>64 bits counter</code>: Ein Zähler von 64 Bit. • <code>text</code>: Literal
Unit	Maßeinheit für den Messwert.
Availability	Verfügbarkeit des Messwerts. Folgende Werte sind möglich: <ul style="list-style-type: none"> • <code>historical</code>: Der Messwert ist in der Verlaufsmesswernerfassung enthalten. • <code>real-time</code>: Der Messwert unterstützt Echtzeitabonnements. • <code>historical, real-time</code>: Der Messwert unterstützt die Verlaufs- und die Echtzeiterfassung. Dieses Attribut gilt nicht für Familien-, Satz- und zusammengesetzte Messwerte.

Anzeigen von Messwerteinstellungen

Zeigen Sie Informationen zu unterstützten Messwerten an.

 **ANMERKUNG:** Verwenden Sie den Befehl „show action“, um das Ausgabeformat zu ändern.

Format

```
/metrics/metric [-path <value>] [-availability { historical | real-time } ] show
```

Objektqualifizierer

Qualifizierer	Beschreibung
-path	Geben Sie eine durch Kommata getrennte Liste von Messwertpfaden an.  ANMERKUNG: Ersetzen Sie bei der Eingabe von Messwertpfaden in den Objektnamen „.“ durch „\.“, „.“ durch „\“,“ und „\“ durch „\\“. Wenn Sie diesen Switch auslassen, werden alle verfügbaren Messwerte angegeben.
-availability	Geben Sie einen anzuzeigenden Messwerttyp an. Folgende Werte sind möglich: <ul style="list-style-type: none"> • <code>historical</code> • <code>real-time</code>

Qualifizierer	Beschreibung
	Wenn Sie diesen Switch auslassen, werden alle Messwerte angezeigt.

Beispiel 1

Mit dem folgenden Befehl werden alle verfügbaren Messwertserviceeinstellungen für das System angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /metrics/metric show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1: Path      = sp.*.cifs.global.basic.readsRate
2: Path      = sp.*.cifs.global.basic.totalCallsRate
3: Path      = sp.*.cifs.global.basic.writeAvgSize
```

Beispiel 2

Mit dem folgenden Befehl werden alle verfügbaren Messwertserviceeinstellungen für das System mit zusätzlichen Details angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /metrics/metric show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1: Path      = sp.*.blockCache.global.summary.cleanPages
   Description = Number of Clean Pages on SP, based on a logical
                        64 KB page size
   Type       = fact
   Unit       = Count
   Availability = real-time

2: Path      = sp.*.blockCache.global.summary.dirtyBytes
   Description = Amount of Dirty Data (MB) on SP
   Type       = fact
   Unit       = MB
   Availability = historical, real-time

3: Path      = sp.*.blockCache.global.summary.dirtyPages
   Description = Number of Dirty Pages on SP, based on a logical
                        64 KB page size
   Type       = fact
   Unit       = Count
   Availability = real-time
```

Beispiel 3

Mit dem folgenden Befehl werden alle verfügbaren Messwertserviceeinstellungen in Echtzeit für das System angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /metrics/metric -availability real-time show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

439: Path = sp.*.storage.pool.*.sizeTotal
440: Path = sp.*.storage.pool.*.sizeUsed
```

```

441: Path = sp.*.storage.pool.*.sizeUsedBlocks
442: Path = sp.*.storage.pool.*.snapshotSizeSubscribed
443: Path = sp.*.storage.pool.*.snapshotSizeUsed
444: Path = sp.*.storage.summary.readBlocksRate
445: Path = sp.*.storage.summary.readBytesRate
446: Path = sp.*.storage.summary.readsRate
447: Path = sp.*.storage.summary.totalBytesRate

```

Beispiel 4

Mit dem folgenden Befehl werden die Messwertserviceeinstellungen für die Messwerte mit den angegebenen Pfaden angezeigt:

```

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /metrics/metric
- path sp.*.storage.lun.*.avgReadSize, sp.*.storage.filesystem.*.writesRate,
sp.*.cifs.smb2.basic.readsRate-Show - detail

```

```

Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1: Path          = sp.*.storage.lun.*.avgReadSize
   Description   = Average read size on this LUN
   Type          = fact
   Unit          = KB
   Availability  = historical, real-time

2: Path          = sp.*.storage.filesystem.*.writesRate
   Description   = Rate of sp.*.storage.filesystem.*.writes
   Type          = rate
   Unit          = Requests/s
   Availability  = historical, real-time

3: Path          = sp.*.cifs.smb2.basic.readsRate
   Description   = Rate of sp.*.cifs.smb2.basic.reads
   Type          = rate
   Unit          = Ops/s
   Availability  = real-time

```

Werte von Verlaufsmesswerten managen

Speichersystemmesswerte erfassen Informationen über die Systemperformance und die Speicherauslastung und sammeln diese Informationen zur Überprüfung durch den Benutzer. Durch die Analyse der Systemmesswerte kann das zukünftige Wachstum des Systems geplant werden.

Verlaufsmesswerte sind in vordefinierten Intervallen verfügbar. Hochfrequente Messwerte (kurzes Intervall) werden nicht so lange wie niederfrequente Messwerte (langes Intervall) aufbewahrt.

In der folgenden Tabelle sind die Verlaufsmesswertattribute aufgeführt:

Tabelle 150. Verlaufsmesswertattribute

Attribut	Beschreibung
Timestamp	Zeit der Erfassung des Messwerts. Das Format ist wie folgt: YYYY-MM-DD HH:MM:SS Hierbei gilt: <ul style="list-style-type: none"> • YYYY: Jahr • MM: Monat • DD: Tag

Tabelle 150. Verlaufsmesswertattribute (fortgesetzt)

Attribut	Beschreibung
	<ul style="list-style-type: none"> • HH: Stunde • MM: Minute • SS: Sekunde
Dynamic attributes	Identifiziert den Objektnamen oder Messwert.

Anzeigen von Verlaufsmesswerteinstellungen

Zeigen Sie die Verlaufsmesswerteinstellungen an. Die Standardausgabe wird in Tabellenform angezeigt.

 **ANMERKUNG:** Verwenden Sie den Befehl „show action“, um das Ausgabeformat zu ändern.

Format

```
/metrics/value/hist -path <value> show -interval { 60 | 300 | 3600 | 14400 }[ -from <value> ]
[ -to <value>] [ -count <value> ] [ -flat ] [ -summary ]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-path	<p>Geben Sie eine durch Komma getrennte Liste von Messwertpfaden an.</p> <p> ANMERKUNG: Ersetzen Sie bei der Eingabe von Messwertpfaden in den Objektnamen „.“ durch „\.“, „.“ durch „\\.“, und „\“ durch „\\“.</p>
-interval	Geben Sie ein Intervall für die Messwerte an. Das Standardintervall ist Sekunden.
-from	<p>Geben Sie den Anfang des Abfragezeitraums an. Das Format ist wie folgt: YYYY-MM-DD HH:MM:SS oder YYYY-MM-DDTHH:MM:SS, wobei:</p> <ul style="list-style-type: none"> • YYYY: Jahr • MM: Monat • DD: Tag • T: Zeittrennzeichen • HH: Stunde • MM: Minute • SS: Sekunde <p> ANMERKUNG: Vergewissern Sie sich, dass der Wert eine Uhrzeit in der Vergangenheit ist. Optional können Sie auch nur das Datum (im Format YYYY-MM-DD) oder die Zeit (im Format HH:MM:SS) angeben. Wenn Sie die Zeit nicht angeben, verwendet das System automatisch 00:00:00. Wenn Sie das Datum nicht angeben, wird das aktuelle Systemdatum verwendet.</p>
-to	<p>Geben Sie das Ende des Abfragezeitraums an. Das Format ist wie folgt: YYYY-MM-DD HH:MM:SS oder YYYY-MM-DDTHH:MM:SS, wobei:</p> <ul style="list-style-type: none"> • YYYY: Jahr • MM: Monat • DD: Tag • T: Zeittrennzeichen • HH: Stunde • MM: Minute • SS: Sekunde <p> ANMERKUNG: Vergewissern Sie sich, dass der Wert eine Uhrzeit in der Vergangenheit ist. Optional können Sie auch nur das Datum (im Format YYYY-MM-DD) oder die Zeit (im Format HH:MM:SS) angeben. Wenn Sie die Zeit</p>

Qualifizierer	Beschreibung
	nicht angeben, verwendet das System automatisch 00:00:00. Wenn Sie das Datum nicht angeben, wird das aktuelle Systemdatum verwendet.
-count	Geben Sie die Anzahl der anzuzeigenden Beispiele an. Ein Beispiel entspricht einer Gruppe aus Messwerten, die mit einem einzelnen Zeitstempel verknüpft sind. Gültige Werte sind Zahlen, die größer oder gleich eins sind.
-flat	Zeigt die Elementwerte für gruppierte Messwerte an.
-summary	Zeigt den maximalen, den minimalen und den durchschnittlichen Wert für jeden Messwert an.

i ANMERKUNG: Die Qualifizierer `-from` und `-to` haben Vorrang gegenüber dem Qualifizierer `-count`. Im Beispiel unten bestehen nur 7 Muster zwischen den `from`- und `to`-Daten. Obwohl der Wert für den Qualifizierer `-count` auf 10 eingestellt ist, werden nur 7 Werte angezeigt. Wenn die Qualifizierer `-from` und `-to` nicht angegeben sind, umfasst die Ausgabe 10 Muster.

Beispiele für Ausgaben verschiedener Kombinationen der Qualifizierer `-from`, `-to` und `-count`

Die folgende Tabelle illustriert die Ausgabe bei Kombinationen der Qualifizierer `-from`, `-to` und `-count`. Es wird als aktuelle Zeit 2012-09-21 12:30:00 angenommen.

Qualifizierer-Kombination	Ausgabe
<code>-from <future date/time></code>	Beispiel: <code>-from „2012-09-21 12:31:00“</code> Resultat: Dies führt zu einem Fehler, da der Zeitpunkt für den Qualifizierer <code>-from</code> in der Zukunft liegt.
<code>-from <current date/time or date/time in the past></code> <code>-to <future date/time></code>	Beispiel: <code>-from „2012-09-01 00:00:00“ -to „2012-09-21 12:31:00“</code> Resultat: Dies führt zu einem Fehler, da der Zeitpunkt für den Qualifizierer <code>-to</code> in der Zukunft liegt.
<code>-from <date/time in the past></code> <code>-count <value></code>	Beispiel: <code>-from „2012-09-20 01:02:00“ -count 100</code> Resultat: Das Resultat enthält 100 Muster von „2012-09-20 01:02:00“. Wenn weniger als 100 Muster verfügbar sind, listet das Resultat alle Muster von der angegebenen Zeit bis zum derzeitigen Zeitpunkt auf.
<code>-from <date/time in the past></code> <code>-to <current date/time or date/time in the past></code> <code>-count <value></code>	Beispiel: <code>-from „2012-09-20 01:02:00“ -to „20-09-20 12:00:00“ -count 100</code> Resultat: Das Resultat enthält 100 Muster innerhalb des angegebenen Zeitraums. Wenn weniger als 100 Muster verfügbar sind, listet das Resultat alle Muster innerhalb des Zeitraums auf.
<code>-to <current date/time or date/time in the past></code> <code>-count <value></code>	Beispiel: <code>-to „20-09-20 12:00:00“ -count 100</code> Resultat: Das Resultat enthält die letzten 100 Muster vor dem angegebenen Zeitpunkt. Wenn weniger als 100 Muster verfügbar sind, listet das Resultat alle Muster auf.
<code>-count <value></code>	Beispiel: <code>-count 100</code> Resultat: Das Resultat enthält die letzten 100 Muster, oder wenn weniger als 100 Muster verfügbar sind, listet das Resultat alle Muster auf.
<code>-to <current date/time or date/time in the past></code>	Beispiel: <code>-to „20-09-20 12:00:00“</code> Resultat: Das Resultat enthält alle Muster vom Zeitstempel des frühesten Musters bis zum angegebenen Zeitpunkt.
<code>-from, -to, and -count are not specified.</code>	Resultat: Das Resultat enthält die letzten 100 Muster, oder wenn weniger als 100 Muster verfügbar sind, listet das Resultat alle Muster auf. Dies ist äquivalent mit „ <code>-count 100</code> “.

Beispiel 1

Mit dem folgenden Befehl wird die angegebene einzelne Kennzahl „SPA LUN sv_1“ alle 60 Sekunden während des Abfragezeitraums angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /metrics/value/hist -path
sp.spa.storage.lun.sv_1.readsRate show -interval 60 -from "2014-06-24 02:12:00" -to "2014-06-24
02:14:00"
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

Timestamp	SP	LUN	Read Counts/s
2014-06-24 02:12:00	spa	sv_1	4.001
2014-06-24 02:13:00	spa	sv_1	2.400
2014-06-24 02:14:00	spa	sv_1	9.602

Beispiel 2

Mit dem folgenden Befehl wird die angegebene Kennzahl, zugeordnet einem einzigen Objekttyp, SPs, alle 60 Sekunden während des Abfragezeitraums angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /metrics/value/hist -path
sp.*.cpu.summary.utilization show -interval 60 -from "2014-06-24 02:57:00" -to "2014-06-24
02:59:10"
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

Timestamp	SP	summary CPU Util %
2014-06-24 02:57:00	spa	12.62
	spb	32.46
2014-06-24 02:58:00	spa	13.06
	spb	19.75
2014-06-24 02:59:00	spa	13.44
	spb	32.47

Beispiel 3

Mit dem folgenden Befehl wird die angegebene Kennzahl, zwei Objekttypen zugeordnet, SPs und LUNs, alle 60 Sekunden während des Abfragezeitraums angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /metrics/value/hist -path
sp.*.storage.lun.*.readsRate show -interval 60 -from "2014-06-24 02:59:00" -to "2014-06-24
03:01:00"
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

Timestamp	SP	LUN	Read Counts/s
2014-06-24 02:59:00	spa	sv_1	0.050
	spa	sv_2	0
	spb	sv_1	0
	spb	sv_2	0.033
2014-06-24 03:00:00	spa	sv_1	0.467

```

|spa      |sv_2      |          | 0
|spb      |sv_1      |          | 0
|spb      |sv_2      |          | 0.117
2014-06-24 03:01:00 |spa      |sv_1      |          | 0.833
|spa      |sv_2      |          | 0
|spb      |sv_1      |          | 0
|spb      |sv_2      |          | 0.467

```

Beispiel 4

Mit dem folgenden Befehl wird die angegebene Kennzahl, drei Objekttypen zugeordnet, SPs, Pools und LUNs, alle 60 Sekunden während des Abfragezeitraums angezeigt:

```

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /metrics/value/hist -path
sp.*.storage.pool.*.lun.*.dataSizeAllocated show -interval 60 -from "2014-06-24 03:04:00" -to
"2014-06-24 03:06:00"

```

```

Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

```

Timestamp	SP	Pool Statistics	LUN	Data Size Allocated Bytes
2014-06-24 03:04:00	spa	pool_1	sv_1	6442450944
	spa	pool_1	sv_2	8589934592
	spb	pool_1	sv_1	6442450944
2014-06-24 03:05:00	spb	pool_1	sv_2	8589934592
	spa	pool_1	sv_1	6442450944
	spa	pool_1	sv_2	8589934592
2014-06-24 03:06:00	spb	pool_1	sv_1	6442450944
	spb	pool_1	sv_2	8589934592
	spa	pool_1	sv_1	6442450944
	spa	pool_1	sv_2	8589934592

Beispiel 5

Mit dem folgenden Befehl werden Kennzahlen, zwei Objekttypen zugeordnet, SPs und LUNs, und eine einzelne Kennzahl, SPA zugeordnet, alle 60 Sekunden während des Abfragezeitraums angezeigt:

```

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /metrics/value/hist -path
sp.*.storage.lun.*.readsRate, sp.*.storage.lun.*.writesRate, sp. spa.cpu.summary.utilization
show -interval 60 -from "2014-06-24 03:04:00" -to "2014-06-24 03:06:00"

```

```

Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

```

Timestamp	SP	LUN	Read Counts/s	Write Counts/s	SP	summary CPU Util %
2014-06-24 03:10:00	spa	sv_1	0	0	spa	12.63
	spa	sv_2	1.050	9.066		
	spb	sv_1	0.067	9.350		
2014-06-24 03:11:00	spb	sv_2	0.100	14.95		12.56
	spa	sv_1	0	0	spa	
	spa	sv_2	0.700	26.62		
2014-06-24 03:12:00	spb	sv_1	0.167	12.28		12.12
	spb	sv_2	2.883	25.65		
	spa	sv_1	0.667	19.53	spa	
	spa	sv_2	0.333	26.87		
	spb	sv_1	7.066	3.700		

```
| spb      | sv_2    | 7.066 | 3.383 |
```

Beispiel 6

Der folgende Befehl zeigt die Mitgliedswerte für angegebene Kennzahlen alle 60 Sekunden während des Abfragezeitraums an:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /metrics/value/hist -path  
sp.*.cpu.summary.utilization show -interval 60 -from "2014-06-24 03:14:00" -to "2014-06-24  
03:16:00" -flat
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection
```

Timestamp	spa	spb
	summary	summary
	CPU	CPU
	Util %	Util %
2014-06-24 03:14:00	15.06	26.78
2014-06-24 03:15:00	15.82	29.39
2014-06-24 03:16:00	15.94	23.59

Beispiel 7

Der folgende Befehl zeigt den maximalen, minimalen und durchschnittlichen Wert für jede Kennzahl alle 60 Sekunden während des Abfragezeitraums an:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /metrics/value/hist -path  
sp.*.cpu.summary.utilization show -interval 60 -from "2014-06-24 03:19:00" -to "2014-06-24  
03:21:00" -summary
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection
```

Timestamp	SP	summary
		CPU
		Util %
2014-06-24 03:19:00	spa	17.72
	spb	43.52
2014-06-24 03:20:00	spa	15.35
	spb	37.82
2014-06-24 03:21:00	spa	15.08
	spb	36.32
Summary	SP	summary
		CPU
		Util %
Minimum	spa	15.08
	spb	36.32
Average	spa	16.05
	spb	39.22
Maximum	spa	17.72
	spb	43.52

Echtzeitmesswerte managen

Speichersystemmesswerte erfassen Informationen über die Systemperformance und die Speicherauslastung und sammeln diese Informationen zur Überprüfung durch den Benutzer. Durch die Analyse der Systemmesswerte kann das zukünftige Wachstum des Systems geplant werden.

In der folgenden Tabelle sind die Echtzeitmesswertattribute aufgeführt.

Tabelle 151. Echtzeitmesswertattribute

Attribut	Beschreibung
Timestamp	Zeit der Erfassung des Messwerts. Das Format lautet wie folgt: YYYY-MM-DD HH:MM:SSHierbei gilt: <ul style="list-style-type: none"> • YYYY: Jahr • MM: Monat • DD: Tag • HH: Stunde • MM: Minute • SS: Sekunde
Dynamic attributes	Identifiziert den Objektnamen oder Messwert.

Anzeigen von Echtzeitmesswerteinstellungen

Zeigen Sie die Echtzeitmesswerteinstellungen an. Die Standardausgabe wird in Tabellenform angezeigt.

 **ANMERKUNG:** Verwenden Sie den Befehl „show action“, um das Ausgabeformat zu ändern.

Format

```
/metrics/value/rt -path <value> show -interval <value> [ -to <value>] [ -count <value> ] [ -flat ] [ -summary ]
```

Objektqualifizierer

Qualifizierer	Beschreibung
-path	Geben Sie eine durch Komma getrennte Liste von Messwertpfaden an.  ANMERKUNG: Ersetzen Sie bei der Eingabe von Messwertpfaden in den Objektnamen „.“ durch „\.“, „.“ durch „.\" und „\“ durch „\\“.

Aktionsqualifizierer

Qualifizierer	Beschreibung
-interval	Geben Sie ein Intervall für die Messwerte an. Das Standardintervall ist Sekunden.
-to	Geben Sie das Ende des Abfragezeitraums an. Das Format lautet wie folgt: YYYY-MM-DD HH:MM:SS oder YYYY-MM-DDTHH:MM:SS, wobei: <ul style="list-style-type: none"> • YYYY: Jahr • MM: Monat • DD: Tag • T: Zeittrennzeichen • HH: Stunde • MM: Minute

Qualifizierer	Beschreibung
	<ul style="list-style-type: none"> ss: Sekunde <p>i ANMERKUNG: Vergewissern Sie sich, dass der Wert eine Uhrzeit in der Vergangenheit ist. Optional können Sie auch nur das Datum (im Format YYYY-MM-DD) oder die Zeit (im Format HH:MM:SS) angeben. Wenn Sie die Zeit nicht angeben, verwendet das System automatisch 00:00:00. Wenn Sie das Datum nicht angeben, wird das aktuelle Systemdatum verwendet.</p>
-count	Geben Sie die Anzahl der anzuzeigenden Beispiele an. Ein Beispiel entspricht einer Gruppe aus Messwerten, die mit einem einzelnen Zeitstempel verknüpft sind. Gültige Werte sind Zahlen, die größer oder gleich eins sind.
-flat	Zeigt die Elementwerte für gruppierte Messwerte an.
-summary	Zeigt den maximalen, den minimalen und den durchschnittlichen Wert für jeden Messwert an.

i ANMERKUNG: Objekte können zu jedem Zeitpunkt kommen und gehen, vor allem durch Erstellen und Löschen von Objekten. Im nicht hierarchischen Format wird jedes Mal, wenn ein neues Objekt hinzukommt, der Titel in tabellarischem oder CSV-Format oder die Attribute im NVP-Format entsprechend angepasst und nach Bedarf auf dem Bildschirm neu ausgegeben. Wenn ein Objekt nicht mehr gültig ist, aber bereits eine Spalte in tabellarischem oder CSV-Format hat, wird die Spalte nur dann beibehalten, wenn der Wert leer ist. Andernfalls wird das Objekt nicht mehr angezeigt.

Beispiel 1

Mit dem folgenden Befehl wird der angegebene Echtzeitmesswert alle 10 Sekunden angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! uemcli /metrics/value/rt -path sp.*.storage.lun.*.readsRate show -interval 10
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Timestamp          | SP      | LUN      | Read
-----+-----+-----+-----
2014-06-24 03:26:10 | spb     | sv_1     | 0.225
2014-06-24 03:26:20 | spb     | sv_1     | 0.200
                   | spb     | sv_2     | 0.100
2014-06-24 03:26:30 | spb     | sv_2     | 0.200
```

Beispiel 2

Mit dem folgenden Befehl werden die Elementwerte für den angegebenen gruppierten Echtzeitmesswert alle 10 Sekunden im CSV-Format angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! uemcli /metrics/value/rt -path sp.*.storage.lun.*.readsRate show -interval 10 -flat -output csv
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Timestamp,spb sv_1 Read Counts/s
2014-06-24 03:26:10,0.225
Timestamp,spb sv_1 Read Counts/s,spb sv_2 Read Counts/s
2014-06-24 03:26:20,0.200,0.100
2014-06-24 03:26:30,,0.200
```

Beispiel 3

Mit dem folgenden Befehl wird der angegebene Echtzeitmesswert alle 10 Sekunden im NVP-Format angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! uemcli /metrics/value/rt -path  
sp.*.storage.lun.*.readsRate show -interval 10 -output nvp
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection  
  
1: Timestamp = 2014-06-24 03:26:10  
  SP         = spb  
  Client     = sv_1  
  CIFS Read  = 0.225  
  
2: Timestamp = 2014-06-24 03:26:20  
  SP         = spb  
  Client     = sv_1  
  CIFS Read  = 0.200  
  
3: Timestamp = 2014-06-24 03:26:20  
  SP         = spb  
  Client     = sv_2  
  CIFS Read  = 0.100  
  
4: Timestamp = 2014-06-24 03:26:30  
  SP         = spb  
  Client     = sv_2  
  CIFS Read  = 0.200
```

Anwendungsbeispiele

Themen:

- Pool-Anwendungsbeispiele
- Anwendungsbeispiele für die Dateifreigabe
- Anwendungsbeispiele für Ressourcenkonfiguration
- Anwendungsbeispiel für Replikationskonfiguration

Pool-Anwendungsbeispiele

In diesem Abschnitt werden verschiedene CLI-Anwendungsbeispiele für Pools beschrieben.

Automatisches Konfigurieren von Pools

Die folgenden Kriterien müssen erfüllt sein, um Pools automatisch zu erstellen.

- Eine FAST VP/FAST Cache-Lizenz ist nicht installiert.
- Keine andere Pools wurden erstellt.
- Bei virtuellen Bereitstellungen wurde allen virtuellen Laufwerken ein Tier-Typ zugewiesen.

Abrufen der Standardkonfiguration für Pools

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/auto show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      Target          = Pool
      Name              = Performance
      Drives (current) =
      Drives (new)     = 6 x 600GB SAS; 6 x 300GB SAS
      RAID level       = 5
      Stripe length    = 5,9

2:      Target          = Pool
      Name              = Capacity
      Drives (current) =
      Drives (new)     = 12 x 2TB NL SAS
      RAID level       = 5
      Stripe length    = 5,9

3:      Target          = Pool
      Name              = Extreme Performance
      Drives (current) =
      Drives (new)     = 10 x 100GB EFD
      RAID level       = 1
      Stripe length    = 2

4:      Target          = Spares
      Name              = Unused / Hot Spare Candidates
      Drives (current) =
      Drives (new)     = 1 x 600GB SAS; 1 x 300GB SAS; 1 x 1TB NL-SAS; 1 x 100GB EFD
```

```
RAID level      =
Stripe length   =
```

Initiieren der automatischen Konfiguration

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/auto set
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
All disks in the system will be used to configure pools. Do you want to proceed?
yes / no: yes
```

```
Operation completed successfully.
```

Abrufen der Liste der konfigurierten Pools

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/pool show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
1:      ID              = SPL_1
        Name            = Performance
        Description      =
        Total space      = 4947802324992 (4.5T)
        Current allocation = 0
        Remaining space   = 4947802324992 (4.5T)
        Subscription      = 0
        Subscription percent = 0%
        Alert threshold   = 70%
        Drives            = 6 x 600GB SAS; 6 x 300GB SAS
        Number of drives   = 12
        RAID level        = 5
        Stripe length     = 5,9
        Health state      = OK (5)
        Recommended resource =
        FAST Cache enabled = no
        Data relocation    =
        Data to move up    =
        Data to move down  =
        Data to move within =
        Estimated relocation time =

2:      ID              = SPL_2
        Name            = Capacity
        Description      =
        Total space      = 24947802324992 (19.5T)
        Current allocation = 0
        Remaining space   = 24947802324992 (19.5T)
        Subscription      = 0
        Subscription percent = 0%
        Alert threshold   = 70%
        Drives            = 12 x 2TB NL-SAS
        Number of drives   = 12
        RAID level        = 5
        Stripe length     = 5,9
        Health state      = OK (5)
        Recommended resource =
        FAST Cache enabled = no
        Data relocation    =
        Data to move up    =
        Data to move down  =
        Data to move within =
        Estimated relocation time =
```

```

3:   ID                = SPL_3
     Name              = Extreme performance
     Description       =
     Total space       = 517802324992 (487.1G)
     Current allocation = 0
     Remaining space   = 517802324992 (487.1G)
     Subscription      = 0
     Subscription percent = 0%
     Alert threshold   = 70%
     Drives            = 10 x 100GB EFD
     Number of drives  = 10
     RAID level        = 1
     Stripe length     = 2
     Health state      = OK (5)
     Recommended resource =
     FAST Cache enabled = no
     Data relocation   =
     Data to move up   =
     Data to move down =
     Data to move within =
     Estimated relocation time =

```

Erstellen eines Pools mithilfe von Laufwerken mit spezifischen Merkmalen

Dieses Beispiel gilt für Hybrid-Flash-Arrays, die nur traditionelle Speicherpools unterstützen.

Abrufen der Liste der Speicherprofile

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/profile -configurable show
```

```

Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:   ID                = profile_22
     Description       = SAS RAID5
     Drive type        = SAS
     RAID level        = 5
     Maximum capacity  = 4611148087296 (4.1T)
     Stripe length     = Maximum capacity
     Disk group        = dg_16
     Maximum drives to configure = 5
     Maximum capacity to configure = 1884243623936 (1.7T)

2:   ID                = profile_30
     Description       = SAS RAID10 (1+1)
     Drive type        = SAS
     RAID level        = 10
     Maximum capacity  = 9749818597376 (8.8T)
     Stripe length     = 2
     Disk group        = dg_13, dg_15
     Maximum drives to configure = 10, 10
     Maximum capacity to configure = 1247522127872 (1.1T), 2954304921600 (2.6T)

3:   ID                = profile_31
     Description       = SAS RAID10 (2+2)
     Drive type        = SAS
     RAID level        = 10
     Maximum capacity  = 9749818597376 (8.8T)
     Stripe length     = 4
     Disk group        = dg_13, dg_15
     Maximum drives to configure = 8, 8
     Maximum capacity to configure = 2363443937280 (2.1T), 952103075840 (886.7G)

```

Konfigurieren eines neuen Pools

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/pool create -name MyPool -description "My custom pool" -storProfile profile_22 -diskGroup dg_16 -drivesNumber 5
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = GP_4
Operation completed successfully.
```

Konfigurieren eines dynamischen Speicherpools

Sie können dynamische Speicherpools für All-Flash-Modelle von Unity mit OE-Version 4.2.x oder höher konfigurieren. Neue Speicherpools, die für diese Modelle erstellt werden, sind standardmäßig dynamische Speicherpools. Dynamische Speicherpools implementieren erweiterte RAID-Technologie. In dynamischen Speicherpools wird eine RAID-Gruppe über Laufwerk-Extents in mehreren Laufwerken verteilt. Der erforderliche freie Speicherplatz wird auch über Laufwerk-Extents in mehreren Laufwerken verteilt. Wenn ein Laufwerk ausfällt, werden die Extents auf dem ausgefallenen Laufwerk neu erstellt, um Speicherplatz-Extents innerhalb des Pools frei zu halten.

Wenn Sie dynamische Speicherpools konfigurieren, können Sie Laufwerke unterschiedlicher Kapazität von verschiedenen Laufwerksgruppen mit den gleichen Flash-Laufwerkstypen auswählen, um einen Pool zu erstellen. Die Gesamtanzahl der Laufwerke des Laufwerkstyps muss mindestens die Stripe-Breite plus 1 sein. Zum Beispiel muss die Gesamtanzahl der Laufwerke für eine RAID-4+1-Gruppe mindestens 6 sein.

Schritt 1: Liste der verfügbaren Laufwerksgruppen anzeigen

Zeigen Sie die Liste der verfügbaren Laufwerksgruppen an, wie im folgenden Beispiel gezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/dg show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:  ID                = dg_2
    Drive type        = SAS Flash 2
    FAST Cache        = yes
    Drive size        = 196971960832 (183.4G)
    Vendor size       = 200.0G
    Rotational speed  = 0 rpm
    Number of drives  = 12
    Unconfigured drives = 12
    Capacity          = 2363663529984 (2.1T)
    Recommended number of spares = 0

2:  ID                = dg_3
    Drive type        = SAS Flash 2
    FAST Cache        = yes
    Drive size        = 393846128640 (366.7G)
    Vendor size       = 400.0G
    Rotational speed  = 0 rpm
    Number of drives  = 12
    Unconfigured drives = 6
    Capacity          = 4726153543680 (4.2T)
    Recommended number of spares = 0
```

Schritt 2: Liste der Storage-Profile anzeigen

Zeigen Sie die Liste der Speicherprofile an, wie im folgenden Beispiel gezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/profile show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:   ID                = profile_1
     Type              = Dynamic
     Description       = SAS Flash 2 RAID5 (4+1)
     Drive type        = SAS Flash 2
     RAID level        = 5
     Maximum capacity  = 97373737844736 (88.5T)
     Stripe length     = 5
     Disk group        =
     Maximum drives to configure =
     Maximum capacity to configure =
```

Schritt 3: Dynamischen Pool konfigurieren

Konfigurieren Sie den dynamischen Speicherpool mit den angegebenen Laufwerksgruppen und Profilen. Legen Sie **-type** optional auf **dynamisch** fest und stellen Sie sicher, dass der Wert **-drivesNumber** für jeden Laufwerkstyp nicht kleiner ist als die Breite der RAID-Gruppe der Laufwerksgruppe plus 1:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/pool create -name mypool
-diskGroup dg_2,dg_3 -drivesNumber 4,2 -storProfile profile_1 -type dynamic
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = pool_13
Operation completed successfully.
```

Konfigurieren eines herkömmlichen Speicherpools für ein All-Flash-Modell

Sie können herkömmliche Pools für all-Flash-Modelle von Unity mit OE-Version 4.2. x und höher konfigurieren, indem Sie explizit das Attribut `Type` auf `traditional` festlegen. Wenn Sie `Type` nicht auf `traditional` festlegen, wenn Sie einen Pool in der Unisphere-CLI erstellen, wird ein dynamischer Pool erstellt.

Schritt 1: Liste der Storage-Profile anzeigen

Zeigen Sie die Liste der Speicherprofile an, wie im folgenden Beispiel gezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/profile -traditional
-configurable show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:   ID                = tprofile_2
     Type              = Traditional
     Description       = SAS Flash 2 RAID5 (8+1)
     Drive type        = SAS Flash 2
     RAID level        = 5
     Maximum capacity  = 95010661072896 (86.4T)
     Stripe length     = 9
     Disk group        = dg_34, dg_26
     Maximum drives to configure = 9, 9
     Maximum capacity to configure = 60189403250688 (54.7T), 2232208064512 (2.0T)

2:   ID                = tprofile_4
     Type              = Traditional
```

```

Description          = SAS Flash 2 RAID5
Drive type           = SAS Flash 2
RAID level           = 5
Maximum capacity     = 95010661072896 (86.4T)
Stripe length       = Maximum capacity
Disk group           = dg_34, dg_26
Maximum drives to configure = 9, 10
Maximum capacity to configure = 60189403250688 (54.7T), 2691354329088 (2.4T)

```

Schritt 2: Herkömmlichen Pools konfigurieren

Konfigurieren Sie einen herkömmlichen Speicherpool mit dem angegebenen Profil. Stellen Sie sicher, dass Sie `-type` auf **herkömmlich** einstellen und dass `-drivesNumber` ein Vielfaches der Breite der RAID-Gruppe ist.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/pool create -name test -diskGroup dg_34 -drivesNumber 9 -storProfile tprofile_2 -type traditional
```

```

Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

```

```

ID = pool_6
Operation completed successfully.

```

Hinzufügen von Festplatten zu einem vorhandenen Pool

Abrufen der Liste der vorhandenen Pools

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /store/config/pool show
```

```

Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:   ID           = SPL_1
     Name        = Performance
     Description  =
     Free space   = 408944640 (390G)
     Capacity    = 1099511627776 (1T)
     Drives      = 6 x 250GB SAS
     Number of drives = 6
     Unused drives = 1
     RAID level   = 5
     System pool  = yes

2:   ID           = SPL_2
     Name        = Capacity
     Description  =
     Free space   = 1319413953331 (1.2T)
     Capacity    = 13194139533312 (12T)
     Drives      = 8 x 2GB NL-SAS
     Number of drives = 8
     Unused drives = 0
     RAID level   = 6
     System pool  = yes

3:   ID           = SPL_3
     Name        = Extreme Performance
     Description  =
     Free space   = 209715200 (200M)
     Capacity    = 322122547200 (300G)
     Drive type   = EFD
     Number of drives = 4
     Unused drives = 0

```

```
RAID level      = 5
System pool     = yes
```

Abrufen der Liste der empfohlenen Festplattengruppen für den ausgewählten Pool

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/dg recom -pool SPL_3
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      ID              = DG_4
      Drive type       = EFD
      Drive size      = 107374182400 (100G)
      Number of drives = 4
      Allowed numbers of drives = 4
      Capacity        = 419430400 (400G)
```

Erweitern des vorhandenen Pools

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/pool -id SPL_3 extend -diskGroup DG_4 -drivesNumber 4
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = SPL_3
Operation completed successfully.
```

Anwendungsbeispiele für die Dateifreigabe

In diesem Abschnitt werden verschiedene Anwendungsbeispiele für die NAS-Server-Dateifreigabe beschrieben.

Erstellen eines NAS-Servers mit Multiprotokoll-Dateifreigabe

Erstellen des NAS-Servers

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/server create -name MyFS1 -sp spa -pool pool_0 -mpSharingEnabled yes -unixDirectoryService ldap -defaultUnixUser fred2 -defaultWindowsUser "fred2"
```

```
ID = nas_1
Operation completed successfully.
```

Anzeigen der NAS-Serverdetails

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/server show -detail
```

```
1:      ID              = nas_1
      Name             = MyFS1
      NetBIOS name     =
      SP              = spa
      Storage pool     = pool_0
      Tenant          =
      Interface       =
      NFS enabled     = yes
      NFSv4 enabled   = no
```

```

CIFS enabled = no
Workgroup =
Windows domain =
Organization unit =
Multiprotocol sharing enabled = yes
Unix directory service = ldap
Default Unix username = fred2
Default Windows username = fred2
Extended Unix credentials enabled = no
Credentials cache retention = 15
Health state = OK_But (7)
Health details = "The component cannot
operate normally - additional configuration steps are
required. Please ensure configuration of Unix directory
service. Please ensure configuration of CIFS server."

```

Konfigurieren von LDAP und Hochladen des Zertifikats der Zertifizierungsstelle

Konfigurieren von LDAP

```

uemcli /net/nas/ldap -server nas_1 set -ip 10.0.0.1,10.0.0.1 -port 636 -protocol ldaps
authType simple -bindDn "cn=administrator,cn=User,dc=emc,dc=com" -bindPasswd "Ldap123!" -baseDn
"dc=emc,dc=com"

```

Operation completed successfully.

Hochladen des Zertifikats der Zertifizierungsstelle:

```

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! -upload -f "MyCert.pem" /net/nas/ldap -server
nas_1 -type CACertificate

```

Operation completed successfully.

Anzeigen der LDAP-Konfiguration:

```

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/ldap show -detail

```

```

[Response]
1:   NAS server = nas_1
     Servers   = 10.0.0.1, 10.0.0.1
     Port      = 636
     Protocol  = ldaps
     Verify certificate = yes
     Authentication type = simple
     Bind DN   = cn=administrator,cn=User,dc=emc,dc=com
     Use CIFS account =
     Principal =
     Realm     =
     Base DN   = dc=emc,dc=com
     Profile DN =

```

Konfigurieren von SMB für den NAS-Server

Erstellen der Schnittstelle für den NAS-Server

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/if create -server nas_1 -port eth0_SPA -addr 10.0.0.1 -netmask 255.255.255.0
```

```
ID = if_0  
Operation completed successfully
```

Konfigurieren des NAS-Servers als SMB-Server

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/cifs create -server nas_1 -domain spb.sspg.lab.emc.com -username Administrator -passwd password1
```

```
ID = cifs_1  
Operation completed successfully.
```

Anzeigen des Integritätsstatus des NAS-Servers

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/server show -detail
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection  
  
1: ID = nas_1  
Name = auto_mig_vdm_6380  
SP = spa  
Storage pool = pool_24  
Tenant =  
Interface = if_24  
CIFS enabled = yes  
Multiprotocol sharing enabled = no  
Unix directory service = none  
Default Unix username =  
Default Windows username =  
Username translation =  
Health state = OK (5)  
Health details = "The component is operating normally. No  
action is required."  
Type = 64  
Migration Destination = yes  
Preferred production interfaces overridden =  
Preferred production IPv4 interface = auto  
Preferred production IPv6 interface = auto  
Preferred backup and DR test IPv4 interface = auto  
Preferred backup and DR test IPv6 interface = auto  
Source preferred production IPv4 interface =  
Source preferred production IPv6 interface =
```

Gemeinsames Nutzen des Dateisystems von NFS und SMB

Erstellen des Multiprotokolldateisystems

```
/stor/prov/fs create -name MyFS -server nas_1 -pool pool_0 -size 1000M -type multiprotocol  
-accessPolicy native
```

```
ID = res_1  
Operation completed successfully.
```

Erstellen eines NFS-Share für das Multiprotokolldateisystem

```
/stor/prov/fs/nfs create -name NFSshare -fs res_1 -path / -defAccess rw
```

```
ID = NFSshare_1  
Operation completed successfully.
```

Erstellen einer SMB-Freigabe für das Multiprotokolldateisystem

```
/stor/prov/fs/cifs create -name CIFSshare -fs res_1 -path / -comment "cifsshare"
```

```
ID = SMBshare_1  
Operation completed successfully
```

Erzeugen und Überprüfen des Benutzerzuordnungsberichts

Erzeugen des Benutzerzuordnungsberichts

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/server -id nas_1 update -userMapping  
-dryRun
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection  
  
Operation completed successfully.
```

Abrufen des Benutzerzuordnungsberichts

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! uemcli -download /net/nas/server -id nas_1  
-type mappingReport
```

```
Operation completed successfully.  
  
>ls mappingReport_2014-11-18_18-08-00.txt
```

Anwendungsbeispiele für Ressourcenkonfiguration

In diesem Abschnitt werden Anwendungsbeispiele für die Konfiguration verschiedener Speicherressourcen beschrieben.

Identifizieren der Poolkapazität und Konfigurieren einer Ressource

Identifizieren des Speichersystems, auf dem sich der zu verwendende Server standardmäßig befindet

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/nas/server -id nas_1 show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
1: ID           = nas_1
   Name         = MySFS1
   CIFS enabled = yes
   NFS enabled  = no
   SP           = spa
   Interface    = if_1
```

Überprüfen der maximalen Kapazität des entsprechenden Pools auf dem identifizierten Speichersystem

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/config/pool show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
1: ID           = pool_1
   Name         = TestPool
   Description  =
   Total space  = 6266625720320 (5.6T)
   Current allocation = 2684354560 (2.5G)
   Remaining space = 6263941365760 (5.6T)
   Subscription = 111967084544 (104.2G)
   Subscription percent = 1%
   Alert threshold = 70%
   Drives        = 4 x 3.1T SAS Flash 3
   Number of drives = 4
   RAID level    = 10
   Stripe length = 2
   Rebalancing   = no
   Rebalancing progress =
   Health state  = OK (5)
   Health details = "The component is operating normally.
No action is required."
   FAST Cache enabled = no
   Protection size used = 32768 (32.0K)
   Auto-delete state = Idle
   Auto-delete paused = no
   Auto-delete pool full threshold enabled = yes
   Auto-delete pool full high water mark = 95%
   Auto-delete pool full low water mark = 85%
   Auto-delete snapshot space used threshold enabled = no
   Auto-delete snapshot space used high water mark = 25%
   Auto-delete snapshot space used low water mark = 20%

2: ID           = pool_2
   Name         = Test1
   Description  =
   Total space  = 43403328880640 (39.4T)
   Current allocation = 57982058496 (54.0G)
   Remaining space = 43345346822144 (39.4T)
   Subscription = 1627792605184 (1.4T)
   Subscription percent = 3%
   Alert threshold = 70%
```

```

Drives = 15 x 600.0G SAS;
        2 x 200.0G SAS Flash 2;
        8 x 6.0T NL-SAS;
        2 x 800.0G SAS Flash 2

Number of drives = 27
RAID level = Mixed
Stripe length = Mixed
Rebalancing = no
Rebalancing progress =
Health state = OK (5)
Health details = "The component is operating normally.
No action is required."
FAST Cache enabled = yes
Protection size used = 2147483648 (2.0G)
Auto-delete state = Idle
Auto-delete paused = no
Auto-delete pool full threshold enabled = no
Auto-delete pool full high water mark = 95%
Auto-delete pool full low water mark = 85%
Auto-delete snapshot space used threshold enabled = no
Auto-delete snapshot space used high water mark = 25%
Auto-delete snapshot space used low water mark = 20%

```

Konfigurieren einer Ressource

```

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /stor/prov/fs create -name FileSystem01
-descr "NFS shares" -pool capacity -server nas_1 -size 1TB -type nfs

```

```

Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

```

```

ID = res_1
Operation completed successfully.

```

Anwendungsbeispiel für Replikationskonfiguration

Dieser Abschnitt beschreibt die Anwendungsbeispiele für die Konfiguration der Replikation für Block- oder Dateispeicherressourcen.

Bevor Sie beginnen

Bevor Sie mit der Konfiguration der Replikation fortfahren, stellen Sie sicher, dass Sie folgende Schritte ausführen:

- Erstellen Sie identische Speicherressourcen auf Quell- und Zielsystemen.
- Konfigurieren Sie Replikationsschnittstellen für jeden SP auf den Quell- und Zielsystemen.
- Auf dem Zielsystem werden die entsprechenden Speicherressourcen und NAS-Server einzeln erstellt, wobei das `-replDest`-Attribut auf `yes` festgelegt wird.
- Stellen Sie für die Dateireplikation Folgendes sicher:
 - Beginnen Sie damit, identische NAS-Server auf beiden Systemen zu erstellen, und erstellen Sie dann identische Dateisysteme.
 - Konfigurieren Sie den NAS-Server auf dem Zielsystem mit einem Namen, der sich von dem Namen des NAS-Servers auf dem Quellsystem unterscheidet.
 - Konfigurieren Sie Dateisysteme auf dem Zielsystem und Dateisysteme auf dem Quellsystem mit dem gleichen Namen.

Lokale Replikation konfigurieren

Replikationsschnittstellen und Verbindungen gelten nicht für lokale Replikation. Wenn Sie die CLI oder die REST API verwenden, können Sie nach der Erstellung der identischen Quell- und Zielspeicherressourcen oder NAS-Server auf dem Speichersystem damit fortfahren, eine Replikationssitzung zu konfigurieren.

i ANMERKUNG: Lokale Replikation ist nur auf asynchrone Replikation anwendbar. Lokale Replikation ist nicht auf synchrone Replikation anwendbar.

Wenn Sie Unisphere verwenden, müssen Sie nur die Quellspeicherressourcen oder NAS-Server auf dem Speichersystem erstellen. Unisphere lässt nicht zu, dass Sie eine Sitzung mit einem bestehenden Ziel erstellen. Eine DR_ wird auf den Ressourcennamen für lokale Ziele verkettet, um sicherzustellen, dass die Quell- und Zielnamen im selben System eindeutig sind (d. h. LUN-Namen müssen eindeutig sein).

Beachten Sie Folgendes:

- Für ein Disaster-Recovery-Szenario wird empfohlen, dass die Ziel-Speicherressource und der Ziel-NAS-Server auf einem anderen Speicherpool konfiguriert wird als der Pool, auf dem die Quell-Speicherressource und der Quell-NAS-Server konfiguriert sind.
- Für ein Migrationsszenario, also die Migration von Quell-Speicherressource und Quell-NAS-Server auf eine Ziel-Speicherressource und einen Ziel-NAS-Server im selben Pool, verwenden Sie die Befehlszeilenoberfläche, um die lokale Replikation zu konfigurieren. Die Unisphere-GUI lässt keine lokale Replikation zwischen Speicherressourcen und NAS-Servern auf demselben Pool zu.

Konfigurieren der asynchronen Replikation

Voraussetzungen

Wenn Sie eine asynchrone Replikation für einen Mandanten konfigurieren, erstellen Sie einen Speicherpool für den Mandanten auf dem Zielsystem, der mit dem entsprechenden Speicherpool auf dem Quellsystem übereinstimmt (sofern vorhanden). Wenn Sie den Mandanten hinzufügen, verwenden Sie dieselbe UUID und dieselben VLANs wie der Mandant auf der Quelle.

Wenn ein NAS-Server repliziert wird, muss der Ziel-NAS-Server über eine entsprechende Mandantenkonfiguration verfügen. Sie können beispielsweise einen NAS-Server ohne Mandanten nicht zu einem NAS-Server mit Mandanten replizieren. Mandanten müssen auf dem Zielsystem unter Verwendung derselben UUID wie auf dem Quellsystem erstellt werden.

Wenn Sie eine asynchrone Replikation in einer Topologie mit gleichzeitig bestehender synchroner und asynchroner Replikation konfigurieren, erstellen Sie den NAS-Zielserver für die asynchrone Replikation so, dass die Attribute `-rep1Dest` und `-backupOnly` auf **Ja** festgelegt sind. Diese Attribute müssen auf dem NAS-Zielserver für die asynchrone Replikation auf **Ja** festgelegt sein, wenn der NAS-Quellserver synchron repliziert wird. Andernfalls kann die asynchrone Replikationssitzung nicht erstellt werden.

Schritte

1. Konfigurieren Sie die Replikationsschnittstellen auf jedem Speicherprozessor der Quell- und Zielsysteme.
2. Konfigurieren Sie eine Replikationsverbindung mithilfe des Verbindungsmodus **Asynchron**.
3. Erstellen Sie für Dateispeicher eine Replikationssitzung für den dem Dateispeicher zugeordneten NAS-Server.

i ANMERKUNG: In einem NAS-Server enthaltene Speicherressourcen werden automatisch repliziert, wenn eine Replikationssitzung erstmals für den NAS-Server konfiguriert wird. Die Replikationssitzung für die Speicherressourcen erben dieselben Attribute wie die zugeordnete Replikationssitzung des zugehörigen NAS-Servers. Für die Speicherressourcen, die nicht an der Replikation teilnehmen sollen, können Sie die zugeordneten Replikationssitzungen manuell entfernen.

4. Erstellen Sie eine Remotereplikationssitzung für die Speicherressource.

i ANMERKUNG: Sie müssen nur Replikationsschnittstellen und -verbindungen für die erste Replikationssitzung zwischen zwei Systemen konfigurieren. Für nachfolgende Replikationssitzungen zwischen denselben Systemen kann dieselbe Verbindung erneut verwendet werden.

5. (Optional) Erstellen Sie einen oder mehrere Zeitpläne für die Bandbreite, um zu steuern, wann die Replikation stattfindet und wie viel Bandbreite während der Replikation verwendet werden soll.

Zeitpläne für die Bandbreite sind für Replikationsverbindungen zum Remotesystem konfiguriert. Alle asynchronen Replikationssitzungen mit aktiver Datenübertragung auf Ihren Replikationsverbindungen geben die Bandbreite, die für die angegebenen Tage und Stunden zugewiesen wird, gleichmäßig frei.

i ANMERKUNG: Wenn kein Zeitplan festgelegt ist, wird während der Replikation die gesamte verfügbare Bandbreite verwendet.

Konfigurieren der synchronen Replikation

Info über diese Aufgabe

Nur Remotereplikation wird für synchrone Replikation unterstützt.

Wenn ein NAS-Server repliziert wird, muss der Ziel-NAS-Server über eine entsprechende Mandantenkonfiguration verfügen. Sie können beispielsweise einen NAS-Server ohne Mandanten nicht zu einem NAS-Server mit Mandanten replizieren. Mandanten müssen auf dem Zielsystem unter Verwendung derselben UUID wie auf dem Quellsystem erstellt werden.

Schritte

1. Identifizieren Sie die FC-Ports (Fibre Channel) für die synchrone Replikation auf jedem System.

Führen Sie zum Ermitteln des FC-Ports, der für die synchrone Replikation verwendet wird, in der CLI-Konsole den Befehl `/remote/sys show -detail` aus. In der Ausgabe werden ähnliche Portinformationen wie im folgenden Beispiel angezeigt:

```
Synchronous FC ports = spb_fc4, spa_fc4
```

Weitere Informationen finden Sie im *Benutzerhandbuch zur Unisphere CLI*:

2. Erstellen Sie Zonen für die FC-Ports für die synchrone Replikation zwischen den Systemen.
Wenn sich die Quell- und Zielsysteme an einem gemeinsamen Standort befinden, können Sie anstelle von Zoning auswählen, direkt verbundene FC-Kabel zwischen den Speicherprozessoren zu verwenden.
3. Konfigurieren Sie die Replikationsschnittstellen auf jedem Speicherprozessor der Quell- und Zielsysteme basierend auf dem gewünschten Verbindungsmodus:
 - Verwenden Sie zur Unterstützung der synchronen Replikation (Verbindungsmodus **Synchron**) die Managementports für die synchrone Replikation auf jedem Speicherprozessor beider Systeme.
 - Konfigurieren Sie zur Unterstützung der asynchronen und synchronen Replikation (Verbindungsmodus **Beide**) zusätzlich zu den Replikationsschnittstellen für Managementports für die synchrone Replikation weitere Schnittstellen mithilfe der Ethernetports auf jedem Speicherprozessor der Quell- und Zielsysteme.
4. Konfigurieren Sie die Replikationsverbindung zwischen Quell- und Zielsystemen nur vom Quellsystem.
 - Geben Sie zur Unterstützung der synchronen Replikation den Verbindungsmodus **Synchron** an.
 - Geben Sie zur Unterstützung der asynchronen und synchronen Replikation den Verbindungsmodus **Beide** an.
5. Erstellen Sie die synchrone Replikationssitzung.

ANMERKUNG: Sie müssen nur Replikationsschnittstellen und -verbindungen für die erste Replikationssitzung zwischen zwei Systemen konfigurieren. Für nachfolgende Replikationssitzungen zwischen denselben Systemen kann dieselbe Verbindung erneut verwendet werden.

Erstellen einer Replikationsschnittstelle

Voraussetzungen

Schutz- und Mobilitätsschnittstellen (Import) können von Replikation und Import gemeinsam genutzt werden. Für den Import benötigen nur VDM-Importe Schnittstellen. Blockimporte erfordern keine Schnittstellen.

Schutz- und Mobilitätsschnittstellen (Import) werden zur Unterstützung von VDM-Importen konfiguriert und müssen vor der Herstellung einer Importverbindung erstellt werden. SPA und SPB auf dem Zielsystem wird eine Mobilitätsschnittstellen-IP-Adresse zugewiesen. Sobald die Mobilitätsschnittstelle konfiguriert wurde, können Sie die Importverbindung zwischen dem Unity-System und dem VNX-System herstellen. Mobilitätsschnittstellen werden nicht für Blockimportsitzungen verwendet.

Sorgen Sie für Folgendes:

- Der Schnittstellenport ist verkabelt und mit einem Netzwerkschwitch verbunden.
- Beide Speichersysteme sind betriebsbereit.

Rufen Sie die folgenden Informationen für jeden Speicherprozessor (SP) ab:

- Die mit der Schnittstelle (Replikation oder Import) verknüpfte IP-Adresse Vergewissern Sie sich trotz der Tatsache, dass Sie eine IPv4- oder IPv6-basierte Adresse angeben können, dass Sie für beide Speicherprozessoren den gleichen Adresstyp angeben.
- Die IP-Adressmaske oder Präfixlänge, anhand der das zugeordnete Subnetz identifiziert wird.
- Die der Schnittstelle zugeordnete Gateway-IP-Adresse.
- Falls zutreffend, die VLAN-ID (zwischen 1 und 4095), die Sie der Schnittstelle zuweisen möchten.

ANMERKUNG: Damit das Netzwerk weiterhin ordnungsgemäß funktioniert, dürfen Sie die VLAN-ID erst festlegen, nachdem Sie den Netzwerk-Switchport für die Unterstützung des VLAN-Tagging für mehrere VLAN-IDs konfiguriert haben.

Info über diese Aufgabe

Stellen Sie sicher, dass Sie auf jedem Speichersystem Replikationsschnittstellen erstellen.

Schritte

1. Führen Sie folgenden Befehl aus, um die Schnittstelle auf SP A zu erstellen:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/if create -type replication -port eth1_spa -addr 10.0.1.1 -netmask 255.255.255.0 -gateway 10.0.1.0
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = IF_1
Operation completed successfully.
```

2. Führen Sie folgenden Befehl aus, um die Schnittstelle auf SP B zu erstellen:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/if create -type replication -port eth1_spb -addr 10.0.1.2 -netmask 255.255.255.0 -gateway 10.0.1.0
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

ID = IF_2
Operation completed successfully.
```

Anzeigen von Schnittstellen

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /net/if show
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:      ID              = IF_0
      Type            = iscsi
      Port            = eth0_spa
      VLAN ID         = 0
      IP address       = 3ffe:80c0:22c:4e:a:0:2:7f/64
      Subnet mask      =
      Gateway         = fe80::20a8bff:fe5a:967c
      SP              = spa

2:      ID              = IF_1
      Type            = replication
      Port            = eth1_spa
      VLAN ID         = 1
      IP address       = 10.0.1.1
      Subnet mask      = 255.255.255.0
      Gateway         = 10.0.1.0
      SP              = spa

3:      ID              = IF_2
      Type            = replication
      Port            = eth1_spb
      VLAN ID         =
      IP address       = 10.0.1.2
      Subnet mask      = 255.255.248.0
      Gateway         = 10.0.1.0
      SP              = spb
```

Erstellen einer Replikationsverbindung

Voraussetzungen

Stellen Sie sicher, dass Sie relevante Replikationsschnittstellenpaare eingerichtet haben, eines auf jedem Speichersystem, auf dem Quell- und Zielsystem. Ermitteln Sie die folgenden Informationen:

- Für die Remotereplikation die IP-Adresse und die zugeordneten Benutzerauthentifizierungsinformationen für die Verbindung zum Remotesystem.
- Für die lokale Replikation das Ihrem Benutzerkonto zugeordnete Passwort.
- Der Verbindungsmodus, den Sie für die Replikation verwenden möchten: **Asynchron**, **Synchron** oder **Beides**.

ANMERKUNG: Wenn bereits eine Replikationsverbindung vorhanden ist und Sie einen anderen Modus für die Replikation hinzufügen möchten, müssen Sie keine neue Verbindung erstellen. Ändern Sie den Modus der vorhandenen Replikationsverbindung in „Beide“.

Info über diese Aufgabe

Beachten Sie, dass Sie eine asynchrone Replikationsverbindung mit dem Remote-System mit der IP-Adresse 10.1.1.1 erstellen möchten.

Schritte

Führen Sie den folgenden Befehl aus:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/sys create -addr 10.1.1.1 -srcUsername admin1 -srcPassword Password456! -dstUsername admin2 -dstPassword Password986! -connectionType async
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = RS_1
Operation completed successfully.
```

Anzeigen von Einstellungen für Remotespeichersysteme

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /remote/sys show -detail
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
1:      ID                = RS_1
      Name                = MyTargetSystem
      Address             = 10.1.1.1
      Model               = Unity 300
      Serial number       = FCNCH01234567A90
      Connection type     = async
      Source interfaces   = N/A
      Local interfaces    = N/A
      Remote interfaces   = N/A
      Operational status  = OK (0x2)
      Health state        = OK (5)
      Health details      = "Communication with the replication
                           host is established. No action is
                           required."
      Synchronous FC ports = spb_fc4, spa_fc4
```

Erstellen einer Replikationssitzung für Blockspeicher

Voraussetzungen

Füllen Sie folgende Felder aus:

- Für Remotereplikation:
 - Identifizieren Sie das Remotesystem, das als Replikationsziel fungiert.
 - Erstellen Sie relevante Replikationsschnittstellen, eine Replikationsverbindung und eine Speicherressource auf dem Remotesystem, das als Replikationsziel fungiert.
- Erstellen Sie für die lokale Replikation eine Speicherressource, die als Ziel fungiert.
- Legen Sie den gewünschten Modus der Replikationssynchronisation fest. Sie können asynchrone (async), synchrone (sync) oder manuelle Synchronisation (manuell) festlegen.
- Bestimmen Sie für asynchrone Replikation die RPO (Recovery Point Objective) für die Replikationssitzung.

Schritte

Führen Sie den folgenden Befehl aus, um eine synchrone Replikationssitzung zwischen der LUN „LUN_1“ auf dem Quellsystem und der LUN „LUN_2“ auf dem Remotesystem „RS_2“ zu erstellen:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/rep/session create -name REPl -srcRes LUN_1 -dstType remote -dstSys RS_2 -dstRes LUN_2 -syncType auto -rpo 0
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
```

```
ID = 81604378625_FCNCH097274B3A_0000_81604378627_FCNCH097274B37_0000
Operation completed successfully.
```

Erstellen einer asynchronen Replikationssitzung für Dateispeicherung

Voraussetzungen

Füllen Sie folgende Felder aus:

- Für Remotereplikation:
 - Identifizieren Sie das Remotesystem, das als Replikationsziel fungiert.
 - Erstellen Sie relevante Replikationsschnittstellen, eine Replikationsverbindung und eine Speicherressource auf dem Remotesystem, das als Replikationsziel fungiert. Die Speicherressource auf dem Zielsystem muss dieselbe Größe haben.
- Erstellen Sie für die lokale Replikation eine Speicherressource, die als Ziel fungiert.
- Erstellen Sie für die Dateireplikation eine Replikationssitzung auf dem NAS-Server, der der Dateispeicherung zugeordnet ist.
- Bestimmen Sie für asynchrone Replikation die RPO (Recovery Point Objective) für die Replikationssitzung.

ANMERKUNG: Wenn Sie asynchrone Replikation in einer Topologie mit gleichzeitig bestehender synchroner und asynchroner Replikation mit einer Quellressource konfigurieren, erstellen Sie den NAS-Zielserver für die asynchrone Replikation so, dass die Attribute `-replDest` und `-backupOnly` auf **Ja** festgelegt sind. Diese Attribute müssen auf dem NAS-Zielserver für die asynchrone Replikation auf **Ja** festgelegt sein, wenn der NAS-Quellserver synchron repliziert wird. Andernfalls kann die asynchrone Replikationssitzung nicht erstellt werden.

Info über diese Aufgabe

Konfigurieren Sie eine asynchrone Replikationssitzung zwischen den NAS-Servern, die der Dateispeicherung zugeordnet sind, mit einem RPO, das auf 2 Stunden und 30 Minuten eingestellt ist, und automatischer Synchronisierung. Auf dem Quellsystem ist das Dateisystem „res_7“ dem NAS-Server „nas_1“ zugeordnet. Und das Dateisystem „res_8“ ist dem NAS-Server „nas_2“ auf dem Remotesystem zugeordnet.

Schritte

1. Führen Sie den folgenden Befehl aus, um eine asynchrone Replikationssitzung zwischen den NAS-Servern zu erstellen:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/rep/session create -async -srcRes nas_1 -dstType remote -dstSys RS_2 -dstRes nas_2 auto -rpo 02h30m
```

```
Job ID = N-86
Operation completed successfully.
```

2. Führen Sie den folgenden Befehl aus, um eine asynchrone Replikationssitzung zwischen dem Dateisystem „res_7“ auf dem Quellsystem und dem Dateisystem „res_8“ zu erstellen, das sich auf dem Remotesystem „RS_2“ befindet, mit einem RPO, das auf 2 Stunden und 30 Minuten eingestellt ist, und automatischer Synchronisation:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/rep/session create -async -srcRes res_7 -dstType remote -dstSys RS_2 -dstRes res_8 -syncType auto -rpo 02h30m
```

```
Job ID = N-89  
Operation completed successfully.
```

Erstellen einer synchronen Replikationssitzung für Dateispeicherung

Voraussetzungen

Füllen Sie folgende Felder aus:

- Für Remotereplikation:
 - Identifizieren Sie das Remotesystem, das als Replikationsziel fungiert.
 - Erstellen Sie relevante Replikationsschnittstellen, eine Replikationsverbindung und eine Speicherressource auf dem Remotesystem, das als Replikationsziel fungiert. Die Speicherressource auf dem Zielsystem muss dieselbe Größe haben.
- Erstellen Sie für die lokale Replikation eine Speicherressource, die als Ziel fungiert.
- Erstellen Sie für die Dateireplikation eine Replikationssitzung auf dem NAS-Server, der der Dateispeicherung zugeordnet ist.

Info über diese Aufgabe

Konfigurieren Sie eine synchrone Replikationssitzung zwischen den NAS-Servern, die der Dateispeicherung zugeordnet sind.

Schritte

1. Führen Sie den folgenden Befehl aus, um eine synchrone Replikationssitzung zwischen den NAS-Servern zu erstellen:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/rep/session create -name MyNSRep1 -srcRes nas_1 -dstType remote -dstSys RS_1 -dstRes nas_1
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection
```

```
ID = 103079215106_FCNCH097274999_0000_103079215106_FCNCH0972749A9_0000  
Operation completed successfully.
```

2. Führen Sie den folgenden Befehl aus, um eine synchrone Replikationssitzung zwischen den Dateisystemen auf dem Quellsystem und auf dem Remotesystem zu erstellen:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/rep/session create -name MyFSRep1 -srcRes res_1 -dstType remote -dstSys RS_1 -dstRes res_1
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection
```

```
ID = 171798691844_FCNCH097274999_0000_171798691844_FCNCH0972749A9_0000  
Operation completed successfully.
```

Anzeigen von Replikationssitzungen

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /prot/rep/session show
```

```
Storage system address: 10.0.0.1  
Storage system port: 443  
HTTPS connection
```

```
1: ID = 81604378635_FCNCH097274B3A_0000_81604378637_FCNCH097274B37_0000  
Name = REP2
```

```
Session type      = nas server
Synchronization type = auto
Resource type     = NAS Server
Destination type  = remote
```

Themen:

- [Health details](#)

Health details

Das Attribut Health details enthält eine benutzerfreundliche Beschreibung des Integritätsstatus der Komponente. Wenn zutreffend, enthält es auch eine URL zur Onlinehilfe oder Supportseite, die Schritte zur Lösung eines Problems bietet. Eine Komponente kann mehrere Zeichenfolgen zur Beschreibung aufweisen, die den Integritätsstatus der relevanten Unterkomponenten anzeigen. Beispiel:

```
Health details = "The storage resource has failed because it uses a storage pool  
that includes one or more disks with problems. Remedy the problem with the disks.  
(http://10.0.0.1/alerts/context_sensitive/dpe_invalid_disk.htm)", "An I/O module in your disk-  
processor enclosure (DPE) may have faulted. Reboot the storage processor (SP). If the problem  
persists after the reboot, replace the I/O module. (http://10.0.0.1/alerts/context_sensitive/  
replace_failed_part.htm) "
```