Dell EMC Unity™-Produktreihe

Dell EMC Unity All Flash, Unity Hybrid, UnityVSA

Version 5.x

Sicherheitskonfigurationsleitfaden

P/N 302-002-564 REV 09

DELL EMC

Stand Juni 2019

EMC Deutschland GmbH
Am Kronberger Hang 2a 65824 Schwalbach/Taunus
Tel.: +49 6196 4728-0
www.DellEMC.com/de-de/index.htm

INHALT

Weitere Ressourcen

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
Produkt- und Funktionsdokumentation sowie Versionshinweise finden Sie in der technischen Dokumentation zu Unity unter: www.emc.com/de-de/documentation/unity-family.htm.

Fehlerbehebung
Informationen über Produkte, Softwareupdates, Lizenzierung und Service finden Sie auf der Online Support-Website (Registrierung erforderlich) unter https://Support.EMC.com. Melden Sie sich an, und suchen Sie die gewünschte Seite für **Support nach Produkt**.

Technischer Support
Für technischen Support und Serviceanfragen besuchen Sie die Online Support-Website unter: https://Support.EMC.com. Suchen Sie nach der Anmeldung **Service-Request erstellen**. Um eine Serviceanfrage stellen zu können, müssen Sie über einen gültigen Supportvertrag verfügen. Wenden Sie sich an Ihren Vertriebsmitarbeiter, wenn Sie einen gültigen Supportvertrag benötigen oder Fragen zu Ihrem Konto haben.

In diesem Dokument verwendete Konventionen für spezielle Hinweise

⚠ GEFAHR

Weist auf gefährliche Situationen hin, die zum Tod oder zu schweren Verletzungen führen.

⚠ WARNUNG

Weist auf gefährliche Situationen hin, die zum Tod oder zu schweren Verletzungen führen können.

⚠ ACHTUNG

Weist auf gefährliche Situationen hin, die zu leichten oder mittelschweren Verletzungen führen können.

HINWEIS

Bezieht sich auf Praktiken, die nicht zu Verletzungen führen.

Hinweis

Enthält Informationen, die wichtig, aber nicht sicherheitsrelevant sind.

KAPITEL 1

Einleitung

In diesem Kapitel werden verschiedene in das Speichersystem implementierte Sicherheitsfunktionen beschrieben.

Folgende Themen werden behandelt:

Überblick

Das Speichersystem nutzt verschiedene Sicherheitsfunktionen zum Steuern des Benutzer- und Netzwerkzugriffs, zum Monitoring des Systemzugriffs und der Systemverwendung und zum Support der Übertragung von Speicherdaten. Dieses Dokument beschreibt die verfügbaren Sicherheitsfunktionen.

Dieses Dokument ist für Administratoren gedacht, die für die Konfiguration und den Betrieb des Speichersystems verantwortlich sind.

Der Leitfaden behandelt Sicherheitseinstellungen in den Kategorien in Tabelle 1 auf Seite 10:

Tabelle 1 Kategorien für Sicherheitseinstellungen

Sicherheitskategorie	Beschreibung
Zugriffskontrolle	Einschränkung des Zugriffs nach Endbenutzer oder anderen Einheiten, um Hardware, Software oder spezielle Produktfunktionen zu schützen
Protokolle	Managen der Ereignisprotokollierung
Kommunikationssicherheit	Schutz der Produktnetzwerkkommunikation
Datensicherheit	Schutz der Produktdaten
Wartung	Kontrolle der Produktservicevorgänge durch den Hersteller oder Servicepartner
Warnmeldungssystem	Managen von Warnmeldungen und Benachrichtigungen für sicherheitsbezogene Ereignisse
Weitere Sicherheitseinstellungen	Sicherheitseinstellungen, die nicht in eine der vorherigen Kategorien fallen, wie die physische Sicherheit

Verwandte Funktionen und Informationen zur Funktion

Spezifische Informationen in Bezug auf die in diesem Dokument beschriebenen Merkmale und Funktionen erhalten Sie in Folgendem für Unity:

- *Unisphere® Befehlszeilenoberflächen-Benutzerhandbuch*
- Unisphere-Onlinehilfe
- *SMI-S-Provider-Programmierhandbuch*
- *Servicebefehle – Technische Hinweise*
- *Secure Remote Support Services – Anforderungen und Konfiguration*

Der vollständige Satz EMC Kundenpublikationen ist auf der EMC Online Support-Website unter http://Support.EMC.com verfügbar. Klicken Sie nach der Anmeldung auf der Website auf die Seite **Support nach Produkt**, um nach Informationen für die spezifische erforderliche Funktion zu suchen.

KAPITEL 2

Zugriffskontrolle

In diesem Kapitel werden verschiedene in das Speichersystem implementierte Zugriffskontrollfunktionen beschrieben.

Folgende Themen werden behandelt:

Standardmäßige werkseitige Management- und Servicekonten für Speichersysteme

Das Speichersystem weist standardmäßige werkseitige Benutzerkontoeinstellungen für den Erstzugriff und die Erstkonfiguration des Speichersystems auf. Siehe Tabelle 2 auf Seite 12.

Tabelle 2 Standardmäßige werkseitige Benutzerkontoeinstellungen

Kontotyp	Benutzername	Password	Rechte
Management (Unisphere)	admin	Password123#	Administratorrechte für das Zurücksetzen von Standardpasswörtern, das Konfigurieren der Systemeinstellungen, das Erstellen von Benutzerkonten und das Zuweisen von Speicher.
Service	service	Service	Servicevorgänge durchführen

Hinweis

Während der Erstkonfiguration müssen Sie das Standardpasswort für die Management- und Servicekonten ändern.

Kontomanagement für Speichersysteme

In Tabelle 3 auf Seite 12 wird gezeigt, wie Sie Speichersystemkonten managen können.

Tabelle 3 Kontomanagementmethoden

Kontorollen	Beschreibung
Management: • Administrator • Speicheradministrator • Sicherheitsadministrator • Operator • VM-Administrator	Nach Abschluss der Erstkonfiguration des Speichersystems können Sie Benutzer und Gruppen des Speichersystems (entweder lokale Konten, LDAP-Konten oder beide) über Unisphere oder die Unisphere-CLI managen. • Bei lokalen Konten können Sie einen neuen Benutzer hinzufügen, einen ausgewählten Benutzer löschen, die Rolle des Benutzers ändern und das Benutzerpasswort zurücksetzen (ändern). • Bei LDAP-Benutzern können Sie einen LDAP-Benutzer hinzufügen, einen ausgewählten Benutzer löschen und die Rolle des Benutzers ändern. • Bei LDAP-Gruppen können Sie eine LDAP-Gruppe hinzufügen, eine

Tabelle 3 Kontomanagementmethoden (Fortsetzung)

Kontorollen	Beschreibung
	ausgewählte Gruppe löschen und die Rolle der Gruppe ändern.
Service	Sie können keine Servicekonten für Speichersysteme erstellen oder löschen. Sie können das Servicekontopasswort in Unisphere zurücksetzen. Wählen Sie unter System die Funktion **Service** > **Serviceaufgaben** > **Servicepasswort ändern** aus.

Hinweis

Sie können die standardmäßigen werkseitigen Kontopasswörter für Speichersysteme durch Drücken der Taste zum Reset des Passworts auf dem Speichersystemgehäuse zurücksetzen. Weitere Informationen erhalten Sie in der *Unisphere-Onlinehilfe* und im *Hardwareinformationshandbuch* für das System.

Unisphere

Die Authentifizierung des Zugriffs auf Unisphere wird über die Anmeldeinformationen des Benutzerkontos (lokal oder LDAP) durchgeführt. Benutzerkonten werden erstellt und anschließend verwaltet durch die Auswahl **Benutzerverwaltung** unter **Einstellungen** > **Benutzer und Gruppen** in Unisphere. Die Autorisierungen, die für Unisphere gültig sind, hängen von der dem Benutzerkonto zugewiesenen Rolle ab.

Bevor ein Benutzer den Unisphere-UI-Inhalt auf eine Managementworkstation herunterladen kann, muss er Anmeldeinformationen für die Authentifizierung angeben und eine Sitzung auf dem Speichersystem einrichten. Wenn der Benutzer die Netzwerkadresse des Speichersystems als URL in einen Webbrowser eingibt, wird ihm eine Anmeldeseite angezeigt, auf der er sich entweder als lokaler Benutzer oder über einen LDAP-Verzeichnisserver authentifizieren kann. Die vom Benutzer eingegebenen Anmeldeinformationen werden geprüft und bei einer erfolgreichen Authentifizierung wird auf dem Speichersystem eine UI-Managementsitzung erstellt. Danach wird die Unisphere-UI heruntergeladen und auf der Managementworkstation des Benutzers instanziiert. Der Benutzer kann das Speichersystem dann im Rahmen der ihm zugewiesenen Rolle überwachen und managen.

LDAP

Das Lightweight Directory Access Protocol (LDAP) ist ein Anwendungsprotokoll zur Durchführung von Abfragen in Verzeichnisdiensten in TCP/IP-Netzwerken. LDAP ermöglicht ein zentrales Management der Authentifizierung, Identität und Gruppeninformationen, verwendet für die Autorisierung auf dem Speichersystem. 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. Beispielsweise können Sie Zugriffsrollen (Administrator, Speicheradministrator, Sicherheitsadministrator, Operator, VM-Administrator) zu

LDAP-Benutzern oder -Gruppen zuweisen. Durch die angewendete Rolle wird die Ebene der Autorisierung festgelegt, die Benutzer oder eine Gruppe beim Verwalten des Speichersystems haben. Die LDAP-Einstellungen werden nur zur einfacheren Steuerung der Unisphere-CLI und von Unisphere, nicht jedoch für den Zugriff auf Speicherressourcen verwendet.

Sitzungsregeln

Unisphere-Sitzungen zeichnen sich durch Folgendes aus:

- Ablaufzeit = 1 Stunde
- Überschreitung des Zeitlimits für die Sitzung ist nicht konfigurierbar
- Sitzungs-IDs werden während der Authentifizierung generiert und sind für eine Sitzung gültig.

Verwendung von Nutzername und Passwort

Nutzernamen und Passwörter für Unisphere-Konten müssen diese Anforderungen erfüllen, wie in der folgenden Tabelle gezeigt.

Tabelle 4 Anforderungen für den Nutzernamen des Unisphere Kontos

Einschränkung	Anforderung an Nutzernamen
Mindestanzahl an alphanumerischen Zeichen	1
Maximale Anzahl alphanumerischer Zeichen	64
Unterstützte Sonderzeichen	. (dot)

Passwörter für Unisphere-Konten müssen diese Anforderungen erfüllen, wie in der folgenden Tabelle gezeigt.

Tabelle 5 Anforderungen an Passwörter für Unisphere-Konten

Einschränkung	Passwortanforderungen
Mindestanzahl an Zeichen	8
Mindestanzahl an großgeschriebenen Zeichen	1
Mindestanzahl an kleingeschriebenen Zeichen	1
Mindestanzahl an numerischen Zeichen	1
Mindestanzahl an Sonderzeichen • Zu den unterstützten Sonderzeichen zählen: ▪ !,@#$%^*_~?	1
Maximale Anzahl an Zeichen	40

Hinweis

Sie können Kontopasswörter in Unisphere ändern, indem Sie **Einstellungen** und anschließend unter **Benutzer und Gruppen** die Optionen **Benutzerverwaltung** > **Mehr Aktionen** > **Passwort zurücksetzen** auswählen. Beim Wechsel des Passworts dürfen die drei unmittelbar zuvor verwendeten Passwörter nicht erneut verwendet werden. Die *Unisphere-Onlinehilfe* bietet weitere Informationen.

HINWEIS

Im STIG-Modus muss das Passwort mindestens 15 Zeichen enthalten. Im STIG-Modus werden außerdem zusätzliche Anforderungen für die Anzahl, den Zeitraum und den Ablaufstatus von Passwörtern festgelegt. Benutzerkonten, die vor der Aktivierung des STIG-Modus erstellt wurden, sind hiervon nicht betroffen, es sei denn, das Passwort wurde geändert. Weitere Informationen zum STIG-Modus finden Sie unter Managen des STIG-Modus (nur physische Bereitstellungen) auf Seite 88.

Autorisierung

In Tabelle 6 auf Seite 15 werden die Rollen gezeigt, die Sie lokalen Speichersystembenutzern zuweisen können, sowie die mit diesen Rollen verknüpften Rechte. Darüber hinaus können Sie diese Rollen LDAP-Benutzern und -Gruppen zuweisen.

Tabelle 6 Lokale Benutzerrollen und -rechte

Aufgabe	Operator	Speicheradministrator	Sicherheitsadministrator	Administrator	VM-Administrator
Ändern des eigenen lokalen Anmeldepassworts	x	x	x	x	
Hinzufügen, Löschen oder Ändern von Hosts				x	
Erstellen von Speicher		x		x	
Löschen von Speicher		x		x	
Hinzufügen von Speicherobjekten, wie LUNs, Freigaben und Speichergruppen, zu Speicherressourcen		x		x	
Anzeigen von Speicherkonfiguration und -status	x	x	x	x	
Anzeigen von Unisphere-Benutzerkonten		x	x	x	
Hinzufügen, Löschen, Ändern, Sperren oder Entsperren von Unisphere-Benutzerkonten			x	x	
Anzeigen des aktuellen Software- oder Lizenzstatus	x	x	x	x	
Durchführen von Software- oder Lizenzupgrades				x	
Durchführen der Erstkonfiguration				x	
Ändern der NAS-Serverkonfiguration				x	
Ändern der Systemeinstellungen				x	
Netzwerkeinstellungen ändern				x	
Ändern der Sprache der Managementoberfläche	x	x	x	x	

Tabelle 6 Lokale Benutzerrollen und -rechte (Fortsetzung)

Aufgabe	Operator	Speicheradministrator	Sicherheitsadministrator	Administrator	VM-Administrator
Anzeigen von Protokoll- und Warnmeldungsinformationen	x	x	x	x	
Anzeigen des Verschlüsselungsstatus	x	x	x	x	
Durchführen von Backups für Verschlüsselungs-Keystore, Auditprotokoll und Prüfsumme			x	x	
Ändern des FIPS 140-2-Modus			x	x	
Ändern des STIG-Modus			x	x	
Herstellen von VASA-Verbindungen zwischen vCenter und Speichersystem				x	x

Nachdem eine Verbindung zwischen vCenter und dem Speichersystem hergestellt wurde, können vCenter-Benutzer mit der VM-Administratorrolle eine Teilmenge der Informationen zu Speicherkonfigurationen und Status sehen, die für dieses vCenter und die ESXi-Server relevant sind. vCenter-Benutzer können nur die Informationen sehen, die im Rahmen der vCenter-Zugriffskontrolle für sie zur Verfügung stehen.

Hinweis

Sie können Kontorollen in Unisphere ändern, indem Sie **Einstellungen** und anschließend unter **Benutzer und Gruppen** die Optionen **Benutzerverwaltung** > **Mehr Aktionen** > **Rolle ändern** auswählen. Die *Unisphere-Onlinehilfe* bietet weitere Informationen.

NAT
Für die lokale Anmeldung am Speichersystem über Unisphere wird kein NAT unterstützt.

Befehlszeilenoberfläche (CLI)

Die Unisphere-CLI bietet eine Befehlszeilenoberfläche für die Unisphere-Funktionen.

Zum Ausführen der Unisphere-CLI ist eine spezielle Befehlszeilensoftware für Speichersysteme erforderlich. Sie können diese Software auf der Produktseite für Ihr Speichersystem der Website des EMC Online Support herunterladen (https://support.emc.com).

Sitzungsregeln
Der Unisphere-CLI-Client unterstützt keine Sitzungen. Geben Sie mit der Befehlszeilensyntax den Benutzernamen und das Passwort für das Konto bei jedem ausgegebenen Befehl an.

Sie können den Unisphere-CLI-Befehl `-saveuser` zum Speichern der Zugangsdaten (Benutzername und Passwort) für ein spezifisches Konto in einer Datei in der sicheren LockBox verwenden, 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. Nach dem Speichern der Zugangsdaten wendet die CLI sie automatisch

auf das angegebene Speichersystemziel und den angegebenen Speichersystemport an, wenn Sie einen Befehl ausführen.

Passwortverwendung
Die Authentifizierung bei der Unisphere-CLI erfolgt gemäß den in Unisphere erstellten und gemanagten Managementkonten. Für Unisphere und spezielle Befehle gelten je nach Rolle des aktuellen Anmeldekontos dieselben Berechtigungen.

Gespeicherte 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.
- Aus dem System importierte SSL-Zertifikate.
- Informationen zum Standardsystem, auf das über die Unisphere-CLI zugegriffen wird, einschließlich des Systemnamens bzw. der IP-Adresse und der Portnummer des Systems.

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:

- Windows Server 2003 (XP): `C:\Documents and Settings\$<user_name>\Local Settings\ApplicationData\.emc\uemcli\cert`
- Unter Windows 7, Windows 8 und Windows 10: `C:\Users\${user_name}\AppData\Local\.emc\uemcli\cert`
- Unter UNIX/Linux: `<home_directory>/.emc/uemcli/cert`

Suchen Sie die Dateien config.xml und config.key. Bei der Deinstallation der Unisphere-CLI werden diese Verzeichnisse und Dateien nicht gelöscht und können optional aufbewahrt werden. Werden diese Dateien nicht mehr gebraucht, sollten Sie sie löschen.

SSH-Serviceoberfläche des Speichersystems

Die SSH-Serviceschnittstelle des Speichersystems bietet bei Aktivierung eine Befehlszeilenoberfläche für die Durchführung von Funktionen, die denen ähneln oder mit diesen zusammenhängen, die auf der Unisphere-Serviceseite verfügbar sind (wählen Sie unter **System** die Optionen **Service** > **Serviceaufgaben** > **SSH aktivieren** aus).

Über das Servicekonto können Benutzer folgende Funktionen durchführen:

- Ausführung spezieller Speichersystem-Servicebefehle für das Monitoring und Troubleshooting von VNXe-Systemeinstellungen und -Vorgängen
- Es kann nur ein begrenzter Satz von Befehlen ausgeführt werden, die als Mitglied eines nicht privilegierten Linux-Nutzerkontos im eingeschränkten Shell-Modus zugewiesen sind. Dieses Konto hat keinen Zugriff auf proprietäre Systemdateien, Konfigurationsdateien oder Benutzer- oder Kundendaten.

Weitere Informationen zur Verwendung von Servicebefehlen finden Sie im Dokument mit technischen Hinweisen zu *Servicebefehlen*.

Die Einstellung der SSH-Serviceschnittstelle des Speichersystems bleibt auch nach Systemneustarts, Failover-Vorgängen sowie im Service- und Normalmodus bestehen. Aus diesem Grund bleibt die SSH-Serviceschnittstelle des Speichersystems nach der

Aktivierung so lange aktiviert, bis sie über die Seite Unisphere-Service wieder deaktiviert wird (wählen Sie unter **System Service** > **Serviceaufgaben** > **SSH deaktivieren** aus).

Für maximale Systemsicherheit wird empfohlen, die SSH-Serviceschnittstelle des Speichersystems jederzeit deaktiviert zu lassen, es sei denn, sie ist für die Durchführung von Servicevorgängen auf dem Speichersystem erforderlich. Deaktivieren Sie die SSH-Schnittstelle nach der Durchführung der erforderlichen Servicevorgänge wieder, um dafür zu sorgen, dass das System sicher bleibt.

Sitzungen
Die SSH-Serviceoberflächensitzungen des Speichersystems werden gemäß den SSH-Clienteinstellungen verwaltet. Die Sitzungsmerkmale sind durch die SSH-Clientkonfigurationseinstellungen festgelegt.

Passwortverwendung
Das Servicekonto ist ein Konto, über das Servicemitarbeiter einfache Linux-Befehle ausführen können.

Das Standardpasswort für die Speichersystem-Serviceoberfläche ist service. Bei der Erstkonfiguration für das Speichersystem müssen Sie das Standardservicepasswort ändern. Es gelten dieselben Passworteinschränkungen wie für Unisphere-Managementkonten (siehe Verwendung von Nutzername und Passwort auf Seite 14). Informationen zum Speichersystem-Servicebefehl `svc_service_password`, der für das Management der Passworteinstellungen für das Speichersystem-Servicekonto verwendet wird, finden Sie im Dokument mit den technischen Hinweisen, *Service Commands*.

Autorisierung
Wie in Tabelle 7 auf Seite 18 gezeigt, wird die Autorisierung für das Servicekonto auf zwei Arten definiert.

Tabelle 7 Servicekontoautorisierung – Definitionen

Autorisierungstyp	Beschreibung
Berechtigungen für Linux-Dateisystem	Dateisystemberechtigungen definieren die meisten Aufgaben, die über das Servicekonto für das Speichersystem durchgeführt werden können. Beispiel: Für die meisten Linux-Tools und -Dienstprogramme, die den Systembetrieb verändern, sind Superuser-Kontorechte erforderlich. Da das Servicekonto nicht über diese Zugriffsrechte verfügt, kann es keine Linux-Tools und -Dienstprogramme verwenden, für das es keine Ausführungsberechtigungen hat, und kann keine Konfigurationsdateien bearbeiten, die Root-Zugriff zum Lesen oder Bearbeiten benötigen.
Zugriffskontrolllisten (Access control lists, ACLs)	Der ACL-Mechanismus auf dem Speichersystem verwendet eine Liste sehr spezieller Regeln, um den Zugriff durch das Servicekonto auf Systemressourcen explizit zu gewähren oder zu verweigern. Diese Regeln geben Servicekontoberechtigungen für andere Bereiche des Speichersystems an, die ansonsten nicht durch standardmäßige Linux-Dateisystemberechtigungen definiert werden.

Speichersystem-Servicebefehle
Eine Reihe von Befehlen für Problemdiagnose, Systemkonfiguration und System-Recovery sind in der Betriebsumgebung der OE des Speichersystems installiert. Diese Befehle stellen ausführliche Informationen und eine geringere Systemkontrolle bereit,

als über Unisphere verfügbar ist. Im Dokument mit technischen Hinweisen, *Service Commands*, werden diese Befehle und ihr häufigster Verwendungszweck beschrieben.

SP-Ethernetserviceport und IPMItool für Speichersysteme

Das Speichersystem ermöglicht den Konsolenzugriff über einen Ethernetserviceport, der sich in jedem Speicherprozessor befindet. Dieser Zugriff erfordert die Verwendung des IPMItool. Das IPMItool ist ein Netzwerktool, das ssh oder telnet ähnelt und über eine Ethernetverbindung und unter Verwendung des IPMI-Protokolls eine Verknüpfung zu jedem Speicherprozessor herstellt. Das IPMItool ist ein Windows-Dienstprogramm, das einen sicheren Kommunikationskanal zum Zugriff auf die SP-Konsole eines Speichersystems aushandelt. Dieses Dienstprogramm erfordert Anmeldedaten und eine IP-Adresse zum Aktivieren der Konsole. Weitere Informationen über das IPMItool finden Sie in den *IPMItool User Guide Technical Notes*.

Die SP-Ethernet-Serviceportschnittstelle bietet dieselben Funktionen wie die SSH-Serviceschnittstelle und unterliegt auch denselben Einschränkungen. Der Unterschied ist, dass Benutzer über eine Ethernetportverbindung und nicht über einen SSH-Client auf die Schnittstelle zugreifen.

Eine Liste der Servicebefehle finden Sie in den *Service Commands Technical Notes*.

SMI-S-Provider

Durch den SMI-S-Provider kommt es zu keinen Änderungen in punkto Sicherheit. Ein SMI-S-Client verbindet sich über den HTTPS-Port 5989 mit dem Speichersystem. Die Anmeldeinformationen sind dieselben wie diejenigen der Unisphere-UI- oder CLI-Benutzer. Alle Sicherheitsregeln, die für UI- und CLI-Benutzer gelten, gelten auch für SMI-S-Verbindungen. Unisphere-UI- und -CLI-Benutzer können sich über die SMI-S-Schnittstelle authentifizieren. Für die SMI-S-Schnittstelle werden keine separaten Benutzer definiert. Nach der Authentifizierung hat der SMI-S-Client die gleichen Rechte wie Unisphere-UI- und -CLI-Benutzer. Das *SMI-S-Provider-Programmierhandbuch* für das Speichersystem enthält weitere Informationen zur Konfiguration dieses Services.

Unterstützung für die vSphere Storage API for Storage Awareness

Die vSphere Storage API for Storage Awareness (VASA) ist eine von VMware definierte anbieterneutrale API für die Speichererkennung. Ein VASA Provider (VP) ist eine speicherseitige Softwarekomponente, die als Speichererkennungsservice für vSphere fungiert. ESXi-Hosts und vCenter Server verbinden sich mit dem VP und erhalten Informationen über verfügbare Speichertopologie, Funktionen und Status. vCenter Server stellt diese Informationen später vSphere-Clients bereit. VASA wird von VMware-Clients statt der Unisphere-Clients verwendet.

Der VP wird auf dem aktiven Speicherprozessor (SP) des Speichersystems ausgeführt. Der vSphere-Benutzer muss diese VP-Instanz für jedes Speichersystem als Anbieter von VASA-Informationen konfigurieren. Wenn ein SP ausfällt, wird der zugehörige Prozess auf dem Peer-SP zusammen mit dem VASA-VP neu gestartet. Für die IP-Adresse wird ein automatisches Failover durchgeführt. Intern ist im Protokoll ein Fehler zu sehen, wenn Konfigurationsänderungsereignisse vom neu aktivierten VP abgerufen werden. Daraufhin wird jedoch automatisch eine Neusynchronisierung der VASA-Objekte ohne Benutzereingriff durchgeführt.

Das Speichersystem stellt VASA 3.0- und VASA 2.0-Schnittstellen für vSphere 6 und VASA 1.0-Schnittstellen für vSphere 5.x bereit.

VASA 1.0 wird ausschließlich für die Überwachung verwendet und von VMware-Clients (und nicht von Unisphere-Clients) genutzt. VASA 1.0 ist eine reine Reportingschnittstelle und wird für die Erfassung grundlegender Informationen zum Speichersystem und den zugehörigen Speichergeräten, die sie der virtuellen Umgebung bereitstellt, verwendet. Sie vereinfacht die täglichen Provisioning-, Monitoring- und Troubleshooting-Aufgaben über vSphere:

- Speichersichtbarkeit: Erkennt Eigenschaftsänderungen intern und sendet die aktualisierten Informationen an vCenter
- Integritäts- und Kapazitätswarnmeldungen: Überwacht intern auf Änderungen des Integritätszustands und auf überschrittene Kapazitätsschwellenwerte; löst entsprechende Warnungen für vCenter aus:
  - Integritätszustand für das Array, SPs, I/O-Ports, LUNs und Dateisysteme
  - Änderungshinweise auf Klassenebene bei Änderungen des Integritätsstatus dieser Objekte
  - Warnungen in Bezug auf Speicherplatzkapazität für LUNs und Dateisysteme
- VASA-Speicherfunktionen: Überwacht intern auf Änderungen der Speicherfunktionen; meldet die geänderten Funktionen an vCenter
- Speicher-DRS-Integration: vSphere nutzt intern erhaltene Informationen vom VP für die Geschäftslogik verschiedener Speicher-DRS-Workflows.

VASA 3.0 und 2.0 unterstützen virtuelle Volumes (VVols). VASA 3.0 und VASA 2.0 unterstützen Schnittstellen zur Abfrage von Speicherabstraktionen wie VVols und Speichercontainer. Diese Informationen helfen Speicher-Policy-basiertem Management (SPBM) bei Entscheidungen zur Platzierung des virtuellen Laufwerks und zur Compliance. VASA 3.0 und VASA 2.0 unterstützen außerdem Schnittstellen für das Provisioning und Management des Lebenszyklus von virtuellen Volumes zur Sicherung virtueller Laufwerke. Diese Schnittstellen werden direkt von ESXi-Hosts aufgerufen.

Weitere Informationen im Zusammenhang mit VASA, vSphere und VVols finden Sie in der VMware-Dokumentation und der Unisphere-Onlinehilfe.

Authentifizierung im Zusammenhang mit VASA
Um eine Verbindung zwischen vCenter und dem Unisphere-VP zu initiieren, müssen Sie im vSphere-Client 3 wichtige Angaben eingeben:

- Die URL des VP im folgenden Format:
  - Für VASA 3.0 und VASA 2.0 https://<Management -IP-Adresse>:8443/vasa/version.xml
  - Für VASA 1.0 https://<Management-IP-Adresse>:8444/vasa/version.xml oder https://<Management-IP-Adresse>:8444/vasa/services/vasaService
- Den Benutzernamen eines Unisphere-Benutzers (die Rolle muss entweder VM-Administrator oder Administrator sein):

  Hinweis

  Die VM-Administratorrolle dient ausschließlich als Mittel zur Registrierung von Zertifikaten.

  - für lokale Benutzer verwenden Sie die Syntax local/<Benutzername>
  - Für LDAP-Benutzer verwenden Sie die Syntax:<Domain>/<Benutzername>

- Das diesem Benutzer zugeordnete Passwort

Die hier verwendeten Unisphere-Anmeldedaten werden nur in diesem ersten Verbindungsschritt verwendet. Wenn die Unisphere-Anmeldedaten für das Zielspeichersystem gültig sind, wird das Zertifikat von vCenter Server automatisch beim Speichersystem registriert. Mit diesem Zertifikat werden alle nachfolgenden Anforderungen vom vCenter authentifiziert. Keine manuellen Schritte sind zum Installieren oder Hochladen dieses Zertifikats zum VP erforderlich. Wenn das Zertifikat abgelaufen ist, muss vCenter ein neues Zertifikat registrieren, damit eine neue Sitzung unterstützt werden kann. Wird das Zertifikat vom Benutzer widerrufen, ist die Sitzung nicht mehr gültig und die Verbindung wird getrennt.

vCenter-Sitzung, sichere Verbindung und Anmeldedaten

Eine vCenter-Sitzung beginnt, wenn ein vSphere-Administrator dem vCenter-Server über den vSphere-Client die VP-URL und die Anmeldedaten mitteilt. Der vCenter-Server verwendet die URL, die Anmeldedaten und das SSL-Zertifikat des VP, um eine sichere Verbindung mit dem VP herzustellen. Eine vCenter-Sitzung endet, wenn eines der folgenden Ereignisse eintritt:

- Ein Administrator entfernt den VP über den vSphere-Client aus der vCenter-Konfiguration und der vCenter-Server beendet die Verbindung.
- Der vCenter Server oder ein vCenter Server-Service schlägt fehl, wodurch die Verbindung getrennt wird. Wenn vCenter oder der Service erneut gestartet wird, wird versucht, die SSL-Verbindung wiederherzustellen. Wenn dies nicht möglich ist, wird eine neue SSL-Verbindung gestartet.
- Der VASA Provider schlägt fehl, die Verbindung wird beendet. Wenn der VASA Provider gestartet wird, kann er zur Wiederherstellung der SSL-Verbindung und VASA-Sitzung auf die Kommunikation vom vCenter Server antworten.

Eine vCenter-Sitzung basiert auf einer sicheren HTTPS-Kommunikation zwischen einem vCenter-Server und einem VP. Die VASA-Architektur verwendet SSL-Zertifikate und VASA-Sitzungsbezeichner, um sichere Verbindungen zu unterstützen. Mit VASA 1.0 hat der vCenter Server das VP-Zertifikat während der VP-Installation oder beim Herstellen einer VASA-Sitzung zu seinem Truststore hinzugefügt. Der VP hat das vCenter Server-Zertifikat zu seinem Truststore hinzugefügt, als Storage Monitoring Service (SMS) die Funktion registerVASACertificate aufgerufen hat. In VASA 3.0 und VASA 2.0 fungiert vCenter Server als die VMware-Zertifizierungsstelle (VMware certificate authority, VMCA). Der VP überträgt auf Anforderung ein selbstsigniertes Zertifikat nach Autorisierung der Anfrage. Er fügt das vCenter Server-Zertifikat in seinen Truststore ein, stellt dann eine Anfrage zur Signierung eines Zertifikats aus und ersetzt das selbstsignierte Zertifikat durch das VMCA-signierte Zertifikat. Zukünftige Verbindungen werden vom Server (dem VP) mit dem Client (SMS)-Zertifikat authentifiziert, das gegen das zuvor registrierte Stammsignierungszertifikat validiert wurde. Ein VP generiert eindeutige Bezeichner für Speicherentitätsobjekte und vCenter Server nutzt den Bezeichner zum Anfordern von Daten für eine bestimmte Entität.

Ein VP nutzt SSL-Zertifikate und den VASA-Sitzungsbezeichner zum Validieren von VASA-Sitzungen. Nachdem die Sitzung hergestellt wurde, muss ein VP das SSL-Zertifikat und den VASA-Sitzungsbezeichner validieren, der mit jedem Funktionsaufruf über vCenter Server verknüpft ist. Der VP verwendet das im Truststore gespeicherte vCenter Server-Zertifikat, um das Zertifikat zu validieren, das vCenter SMS-Funktionsaufrufen zugeordnet ist. Eine VASA-Sitzung bleibt über mehrere SSL-Verbindungen bestehen. Wenn eine SSL-Verbindung getrennt wird, führt der vCenter Server einen SSL-Handshake mit dem VP aus, um die SSL-Verbindung innerhalb des Kontexts derselben VASA-Sitzung wiederherzustellen. Wenn ein SSL-Zertifikat abläuft, muss der vSphere-Administrator ein neues Zertifikat erzeugen. Der vCenter

Server stellt eine neue SSL-Verbindung her und registriert das neue Zertifikat beim VP.

Hinweis

Das Aufheben der Registrierung von 3.0 und 2.0-VPs unterscheidet sich von der Aufhebung der Registrierung von 1.0-VPs. SMS ruft bei einem 3.0- oder 2.0-VP nicht die Funktion unregisterVASACertificate auf, also kann der VP auch nach der Aufhebung der Registrierung weiterhin sein VMCA-signiertes, von SMS erhaltenes Zertifikat nutzen und hat weiterhin Zugriff auf das VMCA-Stammzertifikat.

SSO mit Unisphere Central

Die SSO-Funktion, die Unisphere Central hinzugefügt wurde, bietet Authentifizierungsservices für mehrere Speichersysteme, die für die Verwendung dieser Funktion konfiguriert wurden. Diese Funktion bietet eine einfache Möglichkeit für einen Benutzer, sich an jedem System anzumelden, ohne sich bei jedem System erneut authentifizieren zu müssen.

Unisphere Central ist der zentrale Authentifizierungsserver, der SSO vereinfacht. Diese Funktion erlaubt einem Benutzer Folgendes:

- Sich bei Unisphere Central anzumelden und Unisphere auf einem Speichersystem auszuwählen und zu starten, ohne erneut Anmeldedaten einzugeben
- Sich an einem Speichersystem anzumelden und dann andere Speichersysteme auszuwählen, die mit derselben Unisphere Central-Instanz verknüpft sind, und sich bei diesen ohne erneute Eingabe von Anmeldedaten anmelden zu können

Unisphere Central führt regelmäßig eine Abfrage durch, um Statusinformationen von den Speichersystemen abzufragen, die es managt. Die Identität, die mit in diesem Kontext durchgeführten Abfragen verbunden ist, ist das Unisphere Central-Zertifikat SSL/X.509. Dieses Zertifikat ist von der Unisphere Central-Zertifizierungsstelle signiert, der jede Speichersysteminstanz vertraut, die gemäß Konfiguration von Unisphere Central gemanagt wird.

Darüber hinaus bietet diese Funktion die Möglichkeit zur einmaligen Abmeldung. Wenn Sie sich von Unisphere Central abmelden, melden Sie sich dadurch gleichzeitig auch von allen zugehörigen Sitzungen des Speichersystems ab.

Anforderungen

So verwenden Sie die einmalige Anmeldung:

- Auf Unity- und UnityVSA-Speichersystemen muss die OE-Version 4.0 oder höher ausgeführt werden.
- Unisphere Central-Version 4.0 oder höher muss verwendet werden.
- Sowohl der Unisphere Central-Server als auch die Speichersysteme müssen so konfiguriert sein, dass sie sich gegenüber demselben AD/LDAP-Verzeichnis authentifizieren.
- Der LDAP-Benutzer muss einer Unisphere-Rolle direkt zugeordnet sein oder Mitglied einer AD/LDAP-Gruppe sein, die einer Unisphere-Rolle auf dem Speichersystem und in Unisphere Central zugeordnet ist.
- Auf jedem Speichersystem muss die einmalige Anmeldung aktiviert sein.
- Der Benutzer muss sich als LDAP-Benutzer anmelden.

Hinweis

In Fällen, in denen diese Anforderungen nicht erfüllt sind, muss sich der Benutzer an dem individuellen System als lokaler Benutzer anmelden und Anmeldedaten zur Authentifizierung angeben, um auf dieses System zuzugreifen.

Sie benötigen Administratorrechte, um SSO zu aktivieren. Benutzer mit Speicheradministrator-, Operator- oder VM-Administratorrechten können SSO nicht aktivieren. Verwenden Sie den folgenden uemcli-Befehl, um SSO zu aktivieren:

```
uemcli -d <IP address> -u <username> -p <password> /sys/ur set -
ssoEnabled yes
```

Jedes Speichersystem, bei dem diese Funktion aktiviert ist, kann ein Client des zentralen Authentifizierungsservers und Teil der SSO-Umgebung sein. Weitere Informationen über diesen Befehl finden Sie im *Unisphere CLI-Benutzerhandbuch*.

Überlegungen und Beschränkungen

Das Timeout der Benutzersitzung zwischen dem Webclient und dem zentralen Authentifizierungsserver beträgt 45 Minuten.

Das Timeout der Anwendungssitzung zwischen dem Webclient und dem Speichersystem beträgt eine Stunde.

Hinweis

Informationen zu Kompatibilität und Interoperabilität in Bezug auf Webbrowser finden Sie in der Simple Support Matrix für das Speichersystem auf der Supportwebsite.

SSO-Prozessabläufe

Die folgenden Sequenzen stellen die Prozessabläufe bei der Authentifizierung in Bezug auf SSO in Verbindung mit Unisphere Central dar.

Zugriff auf ein Speichersystem über Unisphere Central

1. Der Benutzer startet einen Webbrowser auf einer Management-Workstation und gibt die Netzwerkadresse von Unisphere Central als URL an.
2. Der Browser wird vom Webserver zu einer lokalen Anmelde-URL von Unisphere Central umgeleitet, und dem Benutzer wird ein Anmeldebildschirm angezeigt.
3. Der Benutzer gibt die LDAP-Zugangsdaten ein und sendet sie ab. Der Benutzername ist in der Form <LDAP-DOMAIN>/Benutzername.
4. Ein Sitzungs-Token wird festgelegt und der Browser wird vom System auf die ursprünglich angegebene URL umgeleitet.
5. Der Browser lädt den Unisphere-Content herunter und Unisphere Central wird instanziiert.
6. Der Benutzer navigiert dann über Unisphere zu einem bestimmten zu überwachenden Speichersystem.
7. Der Benutzer klickt auf die Netzwerkadresse für das Speichersystem.
8. Ein neues Browserfenster mit der URL des Speichersystems wird erstellt.
9. Der Browser wird zum Unisphere Central-Authentifizierungsserver umgeleitet, wo der Benutzer bereits authentifiziert wurde.
10. Der Browser wird zu der Unisphere-Downloadseite umgeleitet und eine Sitzung wird erstellt, in der das Speichersystem das neue Serviceticket verwendet.
11. Unisphere wird heruntergeladen und instanziiert.

12. Der Benutzer beginnt mit dem Management/Monitoring des Speichersystems.

Zugriff auf Speichersysteme, die mit Unisphere Central verbunden sind

1. Der Benutzer startet einen Webbrowser auf einer Management-Workstation und gibt die Netzwerkadresse eines Speichersystems als URL an.
2. Der Browser wird zum lokalen Anmeldeservice von Unisphere Central umgeleitet und dem Benutzer wird ein Anmeldebildschirm angezeigt.
3. Der Benutzer gibt die LDAP-Zugangsdaten ein und sendet sie ab. Der Benutzername ist in der Form <LDAP-DOMAIN>/Benutzername.
4. Ein Sitzungs-Token wird als Cookie festgelegt und der Browser wird vom System auf die ursprünglich angegebene URL umgeleitet.
5. Der Browser lädt den Unisphere-Content herunter und Unisphere wird instanziiert.
6. Der Benutzer öffnet dann ein anderes Fenster oder eine andere Registerkarte im Webbrowser und gibt die Netzwerkadresse eines anderen Speichersystems als URL an.
7. Der Browser wird zum Unisphere Central-Authentifizierungsserver umgeleitet, wo der Benutzer bereits authentifiziert wurde. Ein neues Service-Ticket wird erstellt.
8. Der Browser wird zu der Unisphere-Downloadseite umgeleitet und erstellt mit dem neuen Serviceticket eine Sitzung mit dem zweiten Speichersystem.
9. Unisphere wird für das zweite Speichersystem heruntergeladen und instanziiert.
10. Der Benutzer beginnt mit dem Management/Monitoring des zweiten Speichersystems.

Anmelden bei einem lokalen Speichersystem

Wenn Sie ein lokales Konto verwenden oder keine Verbindung zum Unisphere Central-Authentifizierungsserver besteht, können Sie sich an einem lokalen Speichersystem anmelden. Dazu verwenden Sie den Authentifizierungsserver, der sich im System befindet, anstatt sich über Unisphere Central anzumelden. Es gibt zwei Möglichkeiten, sich lokal am Speichersystem anzumelden:

- Wenn der Browser zum Unisphere Central-Authentifizierungsserver umgeleitet wird, ist eine Option verfügbar, mit der der Benutzer zum System zurückwechseln und sich lokal anmelden kann.
- Wenn kein Zugriff auf Unisphere Central möglich ist, kann die folgende URL-Syntax verwendet werden, um das System zu durchsuchen oder darauf zuzugreifen und sich lokal anzumelden: `https://<storagesystemIP>?casHome=LOCAL`

Dabei ist *storagesystemIP* die IP-Adresse des Speichersystems.

SSO- und NAT-Support

SSO unterstützt keine NAT-Konfigurationen. Für die lokale Anmeldung beim Speichersystem über Unisphere wird ebenfalls kein NAT unterstützt.

Sicherheit auf Dateisystemobjekten

In einer Umgebung mit Multiprotokoll wird die Sicherheits-Policy auf Dateisystemebene festgelegt und ist unabhängig für jedes Dateisystem. Jedes Dateisystem verwendet seine Zugriffs-Policy, um die Zusammenführung der unterschiedlichen Semantiken der NFS- und SMB-Zugriffskontrollen zu bestimmen.

Die Auswahl einer Zugriffs-Policy bestimmt, welcher Mechanismus verwendet wird, um Dateisicherheit auf dem jeweiligen Dateisystem durchzusetzen.

HINWEIS

Wenn das ältere SMB1-Protokoll in Ihrer Umgebung nicht unterstützt werden muss, kann es mithilfe des Servicebefehls `svc_nas` deaktiviert werden. Weitere Informationen über diesen Servicebefehl finden Sie unter *Technische Hinweise zu Servicebefehlen*.

Unix-Sicherheitsmodell

Wenn die Unix-Policy ausgewählt ist, werden alle Versuche, die Sicherheit auf Dateiebene vom SMB-Protokoll zu ändern, wie z. B. Änderungen an Zugriffskontrolllisten (ACLs), ignoriert. Als Unix-Zugriffsrechte werden die Modusbits oder NFSv4-ACL eines Dateisystemobjekts bezeichnet. Modusbits werden durch eine Bitfolge dargestellt. Jedes Bit stellt einen Zugriffsmodus oder eine Berechtigung dar, die dem Benutzer, der Eigentümer der Datei ist, der Gruppe, die mit dem Dateisystemobjekt verbunden ist, und allen anderen Benutzern zugeordnet ist. UNIX-Modusbits werden als drei Reihen verketteter rwx-Tripel (für Lesen, Schreiben und Ausführen) für jede Kategorie von Benutzern (Benutzer, Gruppe oder andere) angezeigt. Eine Zugriffskontrollliste (ACL) ist eine Liste von Benutzern und Benutzergruppen, durch die der Zugriff auf und die Ablehnung von Services gesteuert wird.

Windows-Sicherheitsmodell

Das Windows-Sicherheitsmodell basiert in erster Linie auf Objektrechten. Dazu gehört die Verwendung einer SD (Security Descriptor, Sicherheitsbeschreibung) und ihrer ACL (Access Control List, Zugriffskontrollliste). Wenn SMB-Policy ausgewählt ist, werden Änderungen an den Modusbits vom NFS-Protokoll ignoriert.

Der Zugriff auf ein Dateisystemobjekt basiert darauf, ob Berechtigungen durch die Verwendung eines Sicherheitsdeskriptors gesetzt wurden, die den Zugriff erlauben oder verweigern. Der SD beschreibt den Eigentümer des Objekts und Gruppen-SIDs für das Objekt zusammen mit seinen ACLs. Eine ACL ist Teil des Sicherheitsdeskriptors für jedes Objekt. Jede ACL enthält Zugriffskontrolleinträge (ACEs). Jeder ACE wiederum enthält eine einzige SID, die einen Benutzer, eine Gruppe oder Computer identifiziert, sowie eine Liste von Rechten, die für diese SID verweigert oder gewährt werden.

Dateisystemzugriff in einer Multiprotokollumgebung

Der Dateizugriff wird durch NAS-Server bereitgestellt. Ein NAS-Server umfasst eine Reihe von Dateisystemen, in denen Daten gespeichert werden. Der NAS-Server bietet Zugriff auf diese Daten für die NFS- und SMB-Dateiprotokolle durch die Freigabe von Dateisystemen über SMB-Shares und NFS-Shares. Der NAS-Servermodus für Multiprotokollfreigaben ermöglicht die gemeinsame Verwendung derselben Daten von SMB und NFS. Da der Multiprotokollfreigabemodus den gleichzeitigen Zugriff von SMB und NFS auf ein Dateisystem ermöglicht, muss die Zuordnung von Windows-Benutzern zu Unix-Benutzern und die Definition der anzuwendenden Sicherheitsregeln (Modusbits, ACL und Benutzeranmeldedaten) für die Multiprotokollfreigabe ordnungsgemäß berücksichtigt und konfiguriert werden.

Hinweis

Weitere Informationen über das Konfigurieren und Verwalten von NAS-Servern in Bezug auf Multiprotokollfreigabe, Benutzerzuordnung, Zugriffs-Policies und Benutzeranmeldedaten erhalten Sie in der Unisphere-Onlinehilfe und im *Unisphere Command Line Interface-Benutzerhandbuch*.

Benutzerzuordnung

In einem Multiprotokollkontext muss ein Windows-Benutzer einem UNIX-Benutzer zugeordnet werden. Allerdings muss ein UNIX-Benutzer nur dann einem Windows-Benutzer zugeordnet werden, wenn die Zugriffs-Policy Windows ist. Diese Zuordnung ist notwendig, damit Dateisystemsicherheit durchgesetzt werden kann, auch wenn sie für das Protokoll nicht systemeigen ist. Die folgenden Komponenten sind an der Benutzerzuordnung beteiligt:

- Unix-Verzeichnisdienste, lokale Dateien oder beides
- Windows-Resolver
- Sichere Zuordnung (secmap) – ein Cache, der alle Zuordnungen zwischen SIDs und UID oder GIDs enthält, die von einem NAS-Server verwendet werden.
- ntxmap

Hinweis

Die Benutzerzuordnung beeinflusst nicht die Benutzer oder Gruppen, die lokal auf dem SMB-Server sind.

Unix-Verzeichnisdienste und lokale Dateien

UNIX-Verzeichnisdienste (UDS) und lokale Dateien werden für Folgendes verwendet:

- Für eine gegebene UID (Benutzerkennung) wird der entsprechende Unix-Kontoname zurückgegeben.
- Für einen gegebenen Unix-Kontonamen wird die entsprechende UID und die primäre GID (Gruppenkennung) zurückgegeben.

Die unterstützten Services sind:

- LDAP
- NIS
- Lokale Dateien
- Keine (die einzig mögliche Zuordnung ist durch den Standardbenutzer)

Für den NAS-Server muss entweder ein UDS aktiviert sein oder es müssen lokale Dateien oder sowohl lokale Dateien als auch ein UDS aktiviert sein, wenn Multiprotokollfreigabe aktiviert ist. Die Eigenschaft für den Unix-Verzeichnisdienst des NAS-Servers bestimmt, was für die Benutzerzuordnung verwendet wird.

Windows-Resolver

Windows-Resolver werden verwendet, um Folgendes für die Benutzerzuordnung zu tun:

- Für eine gegebene SID (Sicherheitskennung) wird der entsprechende Windows-Kontoname zurückgegeben.
- Für einen gegebenen Windows-Kontonamen wird die entsprechende SID zurückgegeben.

Die Windows-Resolver sind:

- Der Domain-Controller (DC) der Domain
- Die LGDB (Local Group Database, Datenbank der lokalen Gruppe) des SMB-Servers

secmap
Die Funktion secmap dient dazu, alle SID-zu-UID- und Primär-GID- und UID-zu-SID-Zuordnungen zu speichern, um Kohärenz in allen Dateisystemen des NAS-Servers zu ermöglichen.

ntxmap
ntxmap wird verwendet, um ein Windows-Konto mit einem Unix-Konto zu verknüpfen, wenn der Name verschieden ist. Wenn beispielsweise ein Benutzer ein Konto namens „Gerald“ unter Windows hat, aber sein Konto unter Unix „Gerry“ lautet, wird ntxmap verwendet, um die Korrelation zwischen beiden herzustellen.

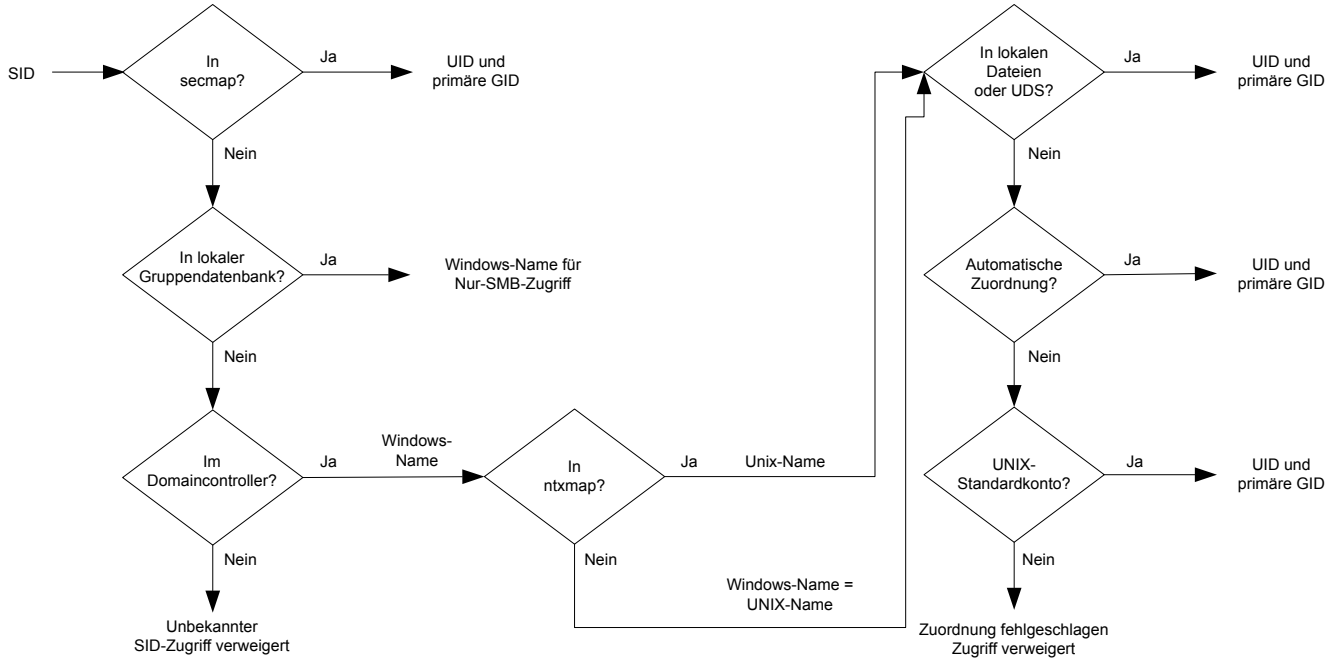
SID-zu-UID, primäre GID-Zuordnung
Die folgende Sequenz ist die Vorgehensweise für die Auflösung einer SID in eine UID, primäre GID-Zuordnung:

1. secmap wird nach der SID durchsucht. Wenn die SID gefunden wird, wird die UID- und GID-Zuordnung aufgelöst.
2. Wenn die SID nicht in secmap gefunden wird, muss der Windows-Name, der der SID entspricht, gefunden werden.
    a. Die lokalen Gruppendatenbanken der SMB-Server des NAS werden nach der SID durchsucht. Wenn die SID gefunden wird, ist der zugehörige Windows-Name der lokale Benutzername zusammen mit dem SMB-Servernamen.
    b. Wenn die SID in der lokalen Gruppendatenbank nicht gefunden wird, wird der DC der Domain durchsucht. Wenn die SID gefunden wird, ist der zugehörige Windows-Name der Benutzername. Ist die SID nicht auflösbar, wird der Zugriff verweigert.
3. Der Windows-Name wird in einen UNIX-Namen übersetzt. Die ntxmap wird für diesen Zweck verwendet.
    a. Wenn der Windows-Name in ntxmap gefunden wird, wird der Eintrag als Unix-Name verwendet.
    b. Wenn der Windows-Name nicht in ntxmap gefunden wird, wird der Windows-Name als Unix-Name verwendet.
4. Der UDS (NIS-Server, LDAP-Server oder lokale Dateien) wird mithilfe des Unix-Namens durchsucht.
    a. Wenn der Unix-Benutzername im UDS gefunden wird, wird die UID- und GID-Zuordnung aufgelöst.
    b. Wenn der UNIX-Name nicht gefunden wird, aber die Funktion zur automatischen Zuordnung für nicht zugeordnete Windows-Konten aktiviert ist, wird die UID automatisch zugeordnet.
    c. Wenn der Unix-Benutzername im UDS nicht gefunden wird, es jedoch ein Unix-Standardkonto gibt, wird die UID- und GID-Zuordnung in die des Unix-Standardkontos aufgelöst.
    d. Ist die SID nicht auflösbar, wird der Zugriff verweigert.

Wenn die Zuordnung gefunden wird, wird sie der dauerhaften secmap-Datenbank hinzugefügt. Wenn die Zuordnung nicht gefunden wird, wird die fehlgeschlagene Zuordnung der dauerhaften secmap-Datenbank hinzugefügt.

Im folgenden Diagramm ist der Prozess für die Auflösung einer SID in eine UID, die primäre GID-Zuordnung, dargestellt:

Abbildung 1 Prozess für die Auflösung einer SID in eine UID, die primäre GID-Zuordnung



UID-zu-SID-Zuordnung

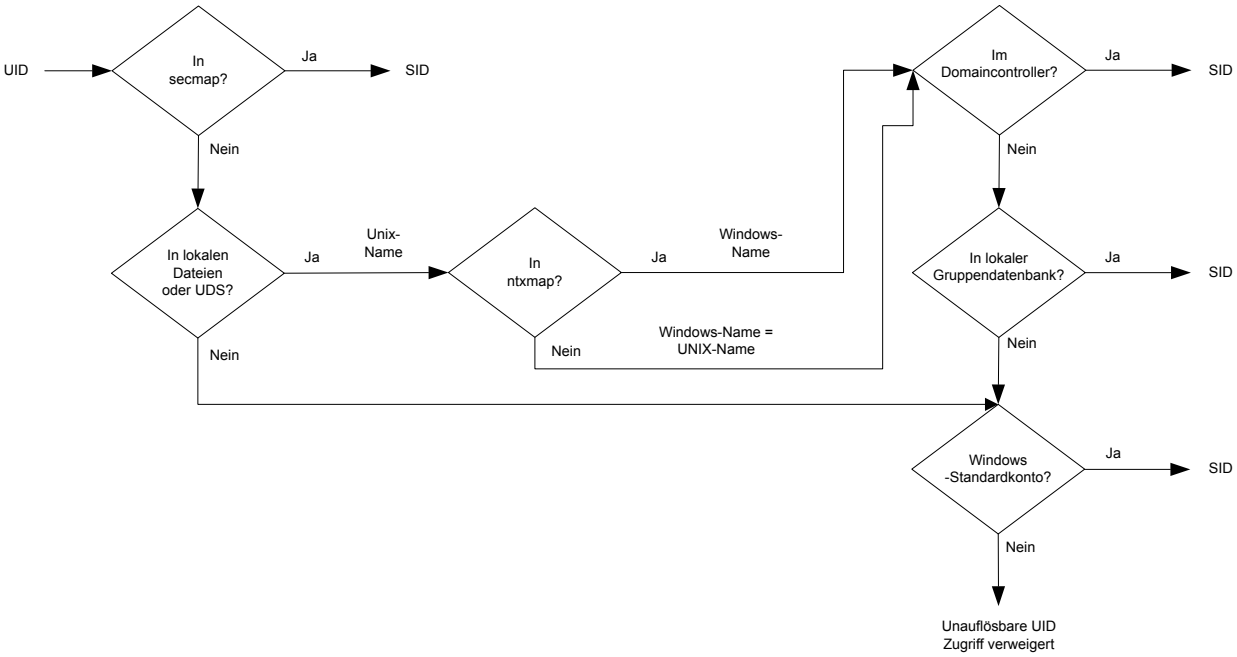
Die folgende Sequenz ist die Vorgehensweise, um eine UID in eine SID-Zuordnung aufzulösen:

1. secmap wird nach der UID durchsucht. Wenn die UID gefunden wird, wird die SID-Zuordnung aufgelöst.
2. Wenn die UID nicht in secmap gefunden wird, muss der Unix-Name, der der UID entspricht, gefunden werden.
   a. Der UDS (NIS-Server, LDAP-Server oder lokale Dateien) wird mithilfe der UID durchsucht. Wenn die UID gefunden wird, ist der zugehörige Unix-Name der Benutzername.
   b. Wenn die UID im UDS nicht gefunden wird, es jedoch ein Windows-Standardkonto gibt, wird die UID der SID des Windows-Standardkontos zugeordnet.
3. Wenn die Windows-Standardkontoinformation nicht verwendet wird, wird der Unix-Name in einen Windows-Namen übersetzt. Die ntxmap wird für diesen Zweck verwendet.
   a. Wenn der Unix-Name in ntxmap gefunden wird, wird der Eintrag als Windows-Name verwendet.
   b. Wenn der Unix-Name nicht in ntxmap gefunden wird, wird der Unix-Name als Windows-Name verwendet.
4. Der Windows-DC oder die Datenbank der lokalen Gruppe wird mithilfe des Windows-Namens durchsucht.
   a. Wenn der Windows-Name gefunden wird, wird die SID-Zuordnung aufgelöst.
   b. Wenn der Windows-Name einen Punkt enthält und der Teil des Namens, der auf den letzten Punkt folgt, dem Namen eines SMB-Servers entspricht, wird die Datenbank der lokalen Gruppe dieses SMB-Servers durchsucht, um die SID-Zuordnung aufzulösen.
   c. Wenn der Windows-Name nicht gefunden wird, es jedoch ein Windows-Standardkonto gibt, wird die SID der des Windows-Standardkontos zugeordnet.
   d. Ist die SID nicht auflösbar, wird der Zugriff verweigert.

Wenn die Zuordnung gefunden wird, wird sie der dauerhaften Secmap-Datenbank hinzugefügt. Wenn die Zuordnung nicht gefunden wird, wird die fehlgeschlagene Zuordnung der dauerhaften secmap-Datenbank hinzugefügt.

Im folgenden Diagramm ist der Prozess für die Auflösung einer UID in eine SID-Zuordnung dargestellt:

Abbildung 2 Prozess für die Auflösung einer UID in eine SID-Zuordnung



Zugriffs-Policies für NFS, SMB und FTP

In einer Multiprotokollumgebung verwendet das Speichersystem Dateisystemzugriffs-Policies, um die Benutzerzugriffskontrolle für die Dateisysteme zu managen. Es gibt zwei Arten von Sicherheit, UNIX und Windows.

Für Unix-Sicherheitsauthentifizierung werden die Anmeldedaten vom UDS (Unix-Directory Services) erstellt, außer für nicht sicheren NFS-Zugang, wo die Anmeldedaten vom Hostclient bereitgestellt werden. Benutzerrechte werden von den Modusbits und NFSv4-ACL bestimmt. Die Benutzer- und Gruppenkennungen (UID bzw. GID) werden zur Identifizierung verwendet. Es sind keine Berechtigungen mit UNIX-Sicherheit verbunden.

Bei der Windows-Sicherheitsauthentifizierung werden die Anmeldedaten aus dem Windows-Domain-Controller (DC) und der Datenbank der lokalen Gruppe (LGDB) des SMB-Servers erstellt. Benutzerrechte werden von den SMB-ACLs festgelegt. Die Sicherheitskennung (SID) wird zur Identifizierung verwendet. Mit der Windows-Sicherheit sind Berechtigungen verknüpft, darunter TakeOwnership, Backup und Wiederherstellung, die von der LGDB oder dem Gruppenrichtlinienobjekt (GPO) des SMB-Servers gewährt werden.

In der folgenden Tabelle werden die Zugriffs-Policies beschrieben, die definieren, welche Sicherheit von welchen Protokollen verwendet wird:

Access policy	Beschreibung
Nativ (Standard einstellung)	• Jedes Protokoll managt den Zugriff gemäß den nativen Sicherheitsmechanismen. • Die Sicherheit für NFS-Shares verwendet die UNIX-Anmeldedaten, die mit der Anforderung zur Prüfung der NFSv3-UNIX-Modusbits oder der NFSv4-ACL verknüpft sind. Der Zugriff wird dann gewährt oder verweigert. • Die Sicherheit für SMB-Shares verwendet die Windows-Anmeldedaten, die mit der Anforderung zur Prüfung der SMB-ACL verknüpft sind. Der Zugriff wird dann gewährt oder verweigert. • Die Änderungen der NFSv3-UNIX-Modusbits und der NFSv4-ACL-Berechtigungen werden miteinander synchronisiert. • Es gibt keine Synchronisation zwischen den UNIX- und Windows-Berechtigungen.
Windows	• Stellt den Zugriff auf Dateiebene für Windows und UNIX mithilfe der Windows-Sicherheit sicher. • Verwendet Windows-Anmeldedaten zur Prüfung der SMB-ACL. • Berechtigungen für neu erstellte Dateien werden durch eine SMB-ACL-Konvertierung bestimmt. Die Änderungen der SMB-ACL-Berechtigungen werden für die NFSv3-UNIX-Modusbits oder die NFSv4-ACL synchronisiert. • Änderungen der NFSv3-Modusbits und der NFSv4-ACL-Berechtigungen werden abgelehnt.
UNIX	• Stellt den Zugriff auf Dateiebene für Windows und UNIX mithilfe der UNIX-Sicherheit sicher.

Access policy	Beschreibung
	• Auf Anforderung des SMB-Zugriffs werden die UNIX-Anmeldedaten aus lokalen Dateien erstellt oder das UDS wird verwendet, um die NFSv3-Modusbits oder die NFSv4-ACL auf Berechtigungen zu prüfen. • Berechtigungen für neu erstellte Dateien werden durch die UMASK bestimmt. • Die Änderungen der NFSv3-UNIX-Modusbits oder der NFSv4-ACL-Berechtigungen werden für die SMB-ACL synchronisiert. • Änderungen der SMB-ACL-Berechtigungen sind zulässig, um Unterbrechungen zu vermeiden, diese Berechtigungen werden jedoch nicht beibehalten.

Bei FTP hängt die Authentifizierung mit Windows oder Unix vom Format des Benutzernamens ab, der für die Authentifizierung am NAS-Server verwendet wird. Bei Verwendung der Windows-Authentifizierung ähnelt die FTP-Zugriffskontrolle der für SMB, andernfalls der für NFS. FTP- und SFTP-Clients werden bei Herstellung der Verbindung mit dem NAS-Server authentifiziert. Dies kann eine SMB-Authentifizierung sein (wenn das Format für den Benutzernamen `domain\user` oder `user@domain` ist) oder eine Unix-Authentifizierung (für die anderen Formate eines einzelnen Benutzernamens). Die SMB-Authentifizierung wird durch den Windows-DC der im NAS-Server definierten Domain sichergestellt. Die Unix-Authentifizierung wird durch den NAS-Server gemäß dem verschlüsselten Passwort ermöglicht, das in einem Remote-LDAP-Server, einem Remote-NIS-Server oder in der lokalen Passwortdatei des NAS-Servers gespeichert wird.

Anmeldedaten für Sicherheit auf Dateiebene

Zur Durchsetzung von Sicherheit auf Dateiebene muss das Speichersystem Anmeldedaten erstellen, die mit der bearbeiteten SMB- oder NFS-Anforderung verknüpft sind. Es gibt zwei Arten von Anmeldedaten, Windows und UNIX. Windows- und Unix-Anmeldedaten werden vom NAS-Server für die folgenden Anwendungsbeispiele erstellt.

- Zur Erstellung von Unix-Anmeldedaten mit mehr als 16 Gruppen für eine NFS-Anforderung. Die Eigenschaft „Erweiterte Anmeldedaten“ des NAS-Servers muss festgelegt werden, um diese Möglichkeit bereitzustellen.
- Zur Erstellung von Unix-Anmeldedaten für eine SMB-Anforderung, wenn die Zugriffs-Policy für das Dateisystem Unix ist.
- Zur Erstellung von Windows-Anmeldedaten für eine SMB-Anforderung.
- Zur Erstellung von Windows-Anmeldedaten für eine NFS-Anforderung, wenn die Zugriffs-Policy für das Dateisystem Windows ist.

Hinweis

Für eine NFS-Anforderung, wenn die Eigenschaft „Erweiterte Anmeldedaten“ nicht festgelegt ist, werden die Unix-Anmeldedaten aus der NFS-Anforderung verwendet. Wenn Kerberos-Authentifizierung für eine SMB-Anforderung verwendet wird, sind die Windows-Anmeldedaten des Domainbenutzers im Kerberos-Ticket der Anforderung zur Sitzungseinrichtung enthalten.

Ein persistenter Anmeldedatencache wird für Folgendes verwendet:

- Windows-Anmeldedaten, die für den Zugriff auf ein Dateisystem mit einer Windows-Zugriffs-Policy erstellt wurden.

- Unix-Anmeldedaten, die für den Zugriff über NFS erstellt wurden, wenn die erweiterte Anmeldedatenoption aktiviert ist.

Es gibt eine Cacheinstanz für jeden NAS-Server.

Gewähren von Zugriff für nicht zugeordnete Benutzer
Multiprotokoll erfordert Folgendes:

- Ein Windows-Benutzer muss einem UNIX-Benutzer zugeordnet sein.
- Ein UNIX-Benutzer muss einem Windows-Benutzer zugeordnet sein, damit die Windows-Anmeldedaten erstellt werden können, wenn der Benutzer auf ein Dateisystem zugreift, das eine Windows-Zugriffs-Policy aufweist.

Zwei Eigenschaften sind dem NAS-Server in Bezug auf nicht zugeordnete Benutzer zugeordnet:

- Der standardmäßige UNIX-Benutzer
- Der standardmäßige Windows-Benutzer

Wenn ein nicht zugeordneter Windows-Benutzer versucht, eine Verbindung zu einem Multiprotokolldateisystem herzustellen, und das Unix-Standardbenutzerkonto für den NAS-Server konfiguriert ist, werden die Benutzerkennung (UID) und primäre Gruppenkennung (GID) für den Unix-Standardbenutzer in den Windows-Anmeldedaten verwendet. Auf ähnliche Weise wird, wenn ein nicht zugeordneter Unix-Benutzer versucht, eine Verbindung zu einem Multiprotokolldateisystem herzustellen, und das Windows-Standardbenutzerkonto für den NAS-Server konfiguriert ist, die Windows-Anmeldedaten des Windows-Standardbenutzers verwendet.

HINWEIS

Wenn der Unix-Standardbenutzer nicht in den Unix-Verzeichnisdiensten (Unix Directory Services, UDS) festgelegt ist, wird der SMB-Zugriff für nicht zugeordnete Benutzer verweigert. Wenn der Windows-Standardbenutzer nicht im Windows-DC oder in der LGDB gefunden wird, wird der NFS-Zugriff auf ein Dateisystem, das einer Windows-Zugriffs-Policy unterliegt, für nicht zugeordnete Benutzer verweigert.

Hinweis

Der UNIX-Standardbenutzer kann ein gültiger vorhandener UNIX-Kontoname sein oder das Format `@uid=`*`xxxx`*`,gid=`*`yyyy`*`@` haben, wobei *xxxx* die numerischen Dezimalwerte der UID sind und *yyyy* für die primäre GID steht. Diese Werte können über Unisphere oder über die Befehlszeilenoberfläche auf dem System konfiguriert werden.

UNIX-Anmeldedaten für NFS-Anforderungen
Zur Verarbeitung von NFS Anforderungen für ein Nur-NFS- oder Multiprotokolldateisystem mit einer Unix- oder nativen Zugriffs-Policy müssen Unix-Anmeldedaten verwendet werden. Die UNIX-Anmeldedaten werden immer in jeder Anforderung integriert; allerdings sind die Anmeldedaten auf 16 Extragruppen beschränkt. Die Eigenschaft `extendedUnixCredEnabled` des NAS-Servers bietet die Möglichkeit, Anmeldedaten mit mehr als 16 Gruppen zu erstellen. Wenn diese Eigenschaft festgelegt ist, werden die aktiven UDS mit der UID abgefragt, um die Primär-GID und alle Gruppen-GIDs zu erhalten, zu denen sie gehört. Wenn die UID in den UDS nicht gefunden wird, werden die in der Anforderung integrierten UNIX-Anmeldedaten verwendet.

Hinweis

Für sicheren NFS-Zugriff werden die Anmeldedaten immer mit dem UDS erstellt.

UNIX-Anmeldedaten für SMB-Anforderungen

Zur Verarbeitung von SMB-Anforderungen für ein Multiprotokolldateisystem mit einer Unix-Zugriffs-Policy müssen zunächst zum Zeitpunkt der Einrichtung der Sitzung Windows-Anmeldedaten für den SMB-Benutzer erstellt werden. Die SID des Windows-Benutzers wird verwendet, um den Namen in Active Directory zu finden. Dieser Name wird dann verwendet (optional über ntxmap), um eine Unix-UID und -GID in dem UDS oder in einer lokalen Datei („passwd“) zu finden. Die Eigentümer-UID des Benutzers ist in den Windows-Anmeldedaten enthalten. Beim Zugriff auf ein Dateisystem mit einer UNIX-Zugriffs-Policy wird die ID des Benutzers zum Abfragen der UDS verwendet, um die UNIX-Anmeldedaten zu erstellen, ähnlich wie bei der Erstellung von erweiterten Anmeldedaten für NFS. Die UID ist für das Quotenmanagement erforderlich.

Windows-Anmeldedaten für SMB-Anforderungen

Zur Verarbeitung von SMB-Anforderungen für ein Nur-SMB- oder Multiprotokolldateisystem mit einer Windows- oder nativen Zugriffs-Policy müssen Windows-Anmeldedaten verwendet werden. Die Windows-Anmeldedaten für SMB müssen nur einmal zum Zeitpunkt der Anforderung einer Sitzungseinrichtung erstellt werden, wenn sich der Benutzer verbindet.

Wenn Kerberos-Authentifizierung verwendet wird, sind die Anmeldedaten des Benutzers im Kerberos-Ticket der Anforderung zur Sitzungseinrichtung enthalten, anders als bei der Verwendung von NTLM (NT LAN Manager). Weitere Informationen werden vom Windows-DC oder der LGDB abgefragt. Für Kerberos wird die Liste der Extragruppen-SIDs dem Kerberos-Ticket und der Liste der lokalen Extragruppen-SIDs entnommen. Die Liste der Rechte werden der LGDB entnommen. Für NTLM wird die Liste der Extragruppen-SIDs dem Windows-DC und der Liste der lokalen Extragruppen-SIDs entnommen. Die Liste der Rechte werden der LGDB entnommen.

Darüber hinaus wird die entsprechende UID und primäre GID auch von der Benutzerzuordnungskomponente abgerufen. Da die Primärgruppen-SID für die Zugriffsprüfung nicht verwendet wird, wird stattdessen die primäre UNIX-GID verwendet.

Hinweis

NTLM ist eine ältere Suite proprietärer Sicherheitsprotokolle, die Authentifizierung, Integrität und Vertraulichkeit für Benutzer bereitstellt. Kerberos ist ein offenes Standardprotokoll, das schnellere Authentifizierung durch den Einsatz eines Ticketing-Systems bietet. Kerberos verleiht Systemen in einem Netzwerk mehr Sicherheit als NTLM.

Windows-Anmeldedaten für NFS-Anforderungen

Die Windows-Anmeldedaten werden nur erstellt oder abgerufen, wenn ein Benutzer über eine NFS-Anforderung versucht, auf ein Dateisystem zuzugreifen, das über eine Windows-Zugriffs-Policy verfügt. Die UID wird aus der NFS-Anforderung extrahiert. Es gibt einen globalen Cache für Windows-Anmeldedaten. Damit wird vermieden, dass die Anmeldedaten bei jeder NFS-Anforderung mit einer zugehörigen Aufbewahrungszeit erstellt werden müssen. Wenn die Windows-Anmeldedaten in diesem Cache gefunden werden, ist keine weitere Aktion erforderlich. Wenn die Windows-Anmeldedaten nicht gefunden werden, wird der UDS oder die lokale Datei abgefragt, um den Namen für die UID zu finden. Der Name wird dann verwendet (optional, durch ntxmap), um einen Windows-Benutzer zu finden, und die

Anmeldedaten werden vom Windows-DC oder LGDB abgerufen. Wenn die Zuordnung nicht gefunden wird, werden stattdessen die Windows-Anmeldedaten des standardmäßigen Windows-Benutzers verwendet oder der Zugriff wird verweigert.

NFS secure

NFS secure bezeichnet die Verwendung von Kerberos für die Authentifizierung von Benutzern mit NFSv3 und NFSv4. Kerberos bietet Integrität (Signierung) und Datenschutz (Verschlüsselung). Integrität und Datenschutz müssen nicht aktiviert werden, es handelt sich um Optionen für den NFS-Export.

Ohne Kerberos verlässt der Server sich vollkommen auf die Authentifizierung der Benutzer durch den Client: der Server vertraut dem Client. Mit Kerberos ist dies nicht der Fall, der Server vertraut dem KDC (Key Distribution Center). Das KDC übernimmt die Authentifizierung und verwaltet Konten (Prinzipale) und Passwort. Darüber hinaus wird keinerlei Passwort über die Verbindung gesendet.

Ohne Kerberos werden die Anmeldedaten des Benutzers unverschlüsselt über das Internet gesendet und können daher einfach manipuliert werden. Mit Kerberos ist die Identität des Benutzers (Prinzipal) in dem verschlüsselten Kerberos-Ticket enthalten, das nur vom Zielserver und dem KDC gelesen werden kann. Diese sind die einzigen, die den Chiffrierschlüssel kennen.

In Kombination mit NFS secure wird die AES128- und AES256-Verschlüsselung in Kerberos unterstützt. Neben NFS secure wirkt sich dies auch auf SMB und LDAP aus. Diese Verschlüsselungen werden jetzt standardmäßig von Windows und Linux unterstützt. Diese neuen Verschlüsselungen sind deutlich sicherer. Es ist jedoch vom Client abhängig, ob diese verwendet werden. Der Server erstellt durch Abfragen des aktiven UDS aus dem Benutzer-Prinzipal die Anmeldedaten für den Benutzer. Da NIS nicht gesichert ist, wird von der Verwendung in Kombination mit NFS secure abgeraten. Es wird empfohlen, Kerberos mit LDAP oder LDAPS zu verwenden.

NFS secure kann entweder über Unisphere oder die UEM-CLI konfiguriert werden.

Dateiprotokollbeziehungen
Für Kerberos ist Folgendes erforderlich:

- DNS: Sie müssen DNS-Namen anstelle von IP-Adressen verwenden.
- NTP: Alle Teilnehmer müssen zeitlich synchronisiert sein.
- UDS: Dieses dient der Erstellung von Anmeldedaten.
- Hostname: Kerberos arbeitet mit Namen, nicht mit IP-Adressen.

NFS secure verwendet abhängig vom Wert des Hostnamens einen oder zwei SPNs. Wenn der Hostname im Format für vollständig qualifizierte Domainnamen „host.domain“ vorliegt:

- Den kurzen SPN: nfs/host@REALM
- Den langen SPN: nfs/host.domainFQDN@REALM

Wenn der Hostname nicht im Format für vollständig qualifizierte Domainnamen vorliegt, wird nur der kurze SPN verwendet.

Ähnlich wie bei SMB, wobei ein SMB-Server einer Domain hinzugefügt werden kann, kann ein NFS-Server einem Bereich (der äquivalente Begriff für Domain in Kerberos) hinzugefügt werden. Dazu gibt es zwei Optionen:

- Verwenden der konfigurierten Windows-Domain, sofern vorhanden
- Vollständiges Konfigurieren eines UNIX-KDC-basierten Kerberos-Bereichs

Wenn sich der Administrator für die Verwendung der konfigurierten Windows-Domain entscheidet, muss er nichts weiter tun. Jeder vom NFS-Service verwendete SPN wird

automatisch dem KDC hinzugefügt/daraus entfernt, wenn der SMB-Server hinzugefügt/entfernt wird. Beachten Sie, dass der SMB-Server nicht gelöscht werden kann, wenn NFS secure für die Verwendung der SMB-Konfiguration konfiguriert ist.

Wenn sich der Administrator für die Verwendung eines UNIX-basierten Kerberos-Bereichs entscheidet, ist weiteres Konfigurieren erforderlich:

- Bereichsname: Der Name des Kerberos-Bereichs, der in der Regel nur Großbuchstaben enthält.
- Vollständiges Konfigurieren eines UNIX-KDC-basierten Kerberos-Bereichs

Um zu erreichen, dass ein Client einen NFS-Export mit einer bestimmten Sicherheit mountet, wird ein Sicherheitsparameter, sec, bereitgestellt, der angibt, welche minimale Sicherheit zulässig ist. Es gibt 4 Arten von Sicherheit:

- AUTH_SYS: Standardmäßige Legacy-Sicherheit, bei der Kerberos nicht verwendet wird. Der Server vertraut den vom Client bereitgestellten Anmeldedaten.
- KRB5: Authentifizierung mithilfe von Kerberos v5
- KRB5i: Kerberos-Authentifizierung plus Integrität (Signatur)
- KRB5p: Kerberos-Authentifizierung sowie Integrität und Datenschutz (Verschlüsselung)

Wenn ein NFS-Client versucht, einen Export mit einer Sicherheit zu mounten, die niedriger als die konfigurierte minimale Sicherheit ist, wird der Zugriff verweigert. Wenn beispielsweise der minimale Zugriff KRB5i ist, werden alle Mounts mit AUTH_SYS oder KRB5 abgelehnt.

Erstellen von Anmeldedaten

Wenn ein Benutzer eine Verbindung zu dem System herstellt, wird nur der Prinzipal user@REALM präsentiert, der aus dem Kerberos-Ticket extrahiert wird. Im Gegensatz zur AUTH_SYS-Sicherheit sind die Anmeldedaten nicht in der NFS-Anforderung enthalten. Aus dem Prinzipal wird der Benutzerteil (vor dem @) extrahiert und zur Suche nach dem UDS für die entsprechende Benutzer-ID verwendet. Aus dieser Benutzer-ID werden vom System mithilfe eines aktiven UDS die Anmeldedaten erstellt, ähnlich wie bei aktiven erweiterten NFS-Anmeldedaten (mit der Ausnahme, dass ohne Kerberos die UID direkt von der Anforderung bereitgestellt wird).

Wenn der Prinzipal in der UDS nicht zugeordnet ist, werden stattdessen die konfigurierten Standard-UNIX-Benutzeranmeldedaten verwendet. Wenn der UNIX-Standardbenutzer nicht festgelegt ist, werden keine Anmeldedaten verwendet.

Replikation

Wenn das Ziel einer Replikation ein NAS-Server ist, besteht die Möglichkeit, für Backup oder Disaster Recovery über NFS auf die Daten zuzugreifen. NFS secure kann in diesen Fällen nicht verwendet werden, da die Nutzung der direkten IP-Adressen nicht mit Kerberos kompatibel ist. Außerdem kann kein vollständig qualifizierter Domainname verwendet werden, da dieser auf die Produktionsschnittstellen auf der Quelle oder die lokalen Schnittstellen auf dem Ziel auflösen könnte.

Dynamic Access Control

Mit Dynamic Access Control (DAC) können Administratoren Zugriffskontrollberechtigungen und -einschränkungen auf Ressourcen anwenden. Dies erfolgt auf Grundlage von festgelegten Regeln, die die Sensitivität der Ressourcen, den Job oder die Rolle des Benutzers sowie die Konfiguration des Geräts, das zum Zugriff auf diese Ressourcen verwendet wird, beinhalten können.

DAC Claims Based Access Control (CBAC) ist eine Funktion von Windows Server 2012, mit der Zugriffskontrolle für den Domaincontroller mit einer Gruppe von Central

Access Policies (CAPs) definiert werden kann. Jeder Central Access Policy (identifiziert durch ihre CAPID) sind eine Reihe zentraler Zugriffsregeln (Central Acces Rules, CARs) zugeordnet. CAPs können Group Policy Objects (GPOs) zugewiesen werden. Dies ist der Mechanismus zum Verteilen von CAPs an einzelne Dateiserver. Die CAP, die für eine bestimmte Ressource (d. h., ein Verzeichnis oder Datei) gilt, wird durch die CAPID bestimmt. Wenn ein NAS-Server mit Windows-Shares (SMB) erstellt wird, ruft er beim Beitritt zur Domain die richtige CAP und CAR ab.

Jede CAR weist folgende Attribute auf:

- Ausdruck für Ressourcenziel
- Zugriffskontrollliste für aktuelle Berechtigungen
- Zugriffskontrollliste für vorgeschlagene Berechtigungen (optional)

Der Ausdruck für das Ressourcenziel (Anwendbarkeitsausdruck) wird ausgewertet, um zu ermitteln, ob die CAR für eine bestimmte Ressource anwendbar ist oder nicht (z. B. @Resource.Department != @User.Department). Wenn dieser Ausdruck als TRUE bewertet wird, wird die Zugriffskontrollliste für aktuelle Berechtigungen während der Überprüfung des Zugriffs verwendet; andernfalls wird die Regel ignoriert. Die Zugriffskontrollliste für vorgeschlagene Berechtigungen erlaubt dem Administrator, die Auswirkung der vorgeschlagenen Änderungen an den aktuellen Berechtigungen anzuzeigen. Wenn die Bewertung der vorgeschlagenen Berechtigungen aktiviert ist, werden die Unterschiede zwischen den aktuellen und vorgeschlagenen Berechtigungen während einer Überprüfung des Zugriffs (im Serverprotokoll) protokolliert.

Ein Windows-Client (Windows Server 2012 oder Windows 8.x) kann verwendet werden, um Ressourcen (d. h., Verzeichnissen oder Dateien) eine CAP zuzuordnen, falls erforderlich (dies ist optional). Wenn dies erfolgt ist, wird die angegebene CAP vom NAS-Server für die entsprechenden Ressourcen durchgesetzt. Ein Windows-Client kann auch zum Ausführen der manuellen Klassifizierung von Ressourcen (z. B. Festlegen des Landes oder der Abteilung) verwendet werden.

DAC CBAC ist standardmäßig auf dem Speichersystem aktiviert; mit einem Servicebefehl, `svc_dac`, können Sie Folgendes ausführen:

- Aktivieren oder Deaktivieren der DAC-Funktion: Wenn deaktiviert, wird die CAP ignoriert, die einer Ressource zugeordnet ist (d. h. nur die DACL bestimmt den Zugriff).
- Aktivieren Sie oder deaktivieren Sie die Bewertung der vorgeschlagenen Berechtigungen. Jede CAR kann vorgeschlagene Berechtigungen haben und diese sind auf den Dateiservern verteilt. Nur diese Berechtigungen werden in der Regel nicht ausgewertet. Der Befehl `svc_dac` kann verwendet werden, um die Bewertung dieser Berechtigungen zu aktivieren. Nach der Aktivierung werden Unterschiede zwischen den effektiven Berechtigungen und den vorgeschlagenen Berechtigungen an das Serverprotokoll gesendet. Mit der Bewertung der vorgeschlagenen Berechtigungen können Sie vorgeschlagene Änderungen an CARs sicher testen.
- Fragen Sie die CAPs oder CARs ab, die einem NAS-Server compname zugeordnet sind (alle, nach eindeutigem Namen oder nach ID).
- Fügen Sie benutzerdefinierte Recovery-Regeln hinzu oder entfernen Sie sie (um die Recovery-Standardregel zu ersetzen).
- Steuern Sie die Ausführlichkeit der Protokollierung, die von DAC für Diagnosezwecke erzeugt wird.

Detaillierte Informationen über den Befehl `svc_dac` finden Sie unter *Servicebefehle EMC Unity Produktreihe – Technische Hinweise*.

KAPITEL 3

Protokollierung

In diesem Kapitel werden verschiedene in das Speichersystem implementierte Protokollierungsfunktionen beschrieben.

Folgende Themen werden behandelt:

Protokollierung

Das Speichersystem speichert die in der folgenden Tabelle aufgeführten Arten von Protokollen für die Nachverfolgung von Systemevents.

Tabelle 8 Protokolle

Protokolltyp	Beschreibung
Systemprotokoll	In Unisphere angezeigte Informationen, um Benutzer über Speichersystemevents zu informieren, für die Maßnahmen ergriffen werden müssen. Diese Datensätze werden gemäß der Standardspracheinstellung für das System lokalisiert. **Hinweis** Ereignisse, für die Maßnahmen ergriffen werden müssen, umfassen Auditereignisse. Es werden jedoch nicht alle protokollierten Ereignisse in der GUI angezeigt. Auditprotokolleinträge, die einen gewissen Schweregradschwellwert nicht erreichen, werden vom System protokolliert, jedoch nicht in der GUI angezeigt.
Systemwarnmeldung	Informationen, mit denen Servicemitarbeiter den Status oder das Verhalten des Speichersystems diagnostizieren oder überwachen. Diese Datensätze werden nur in Englisch aufgezeichnet.

Anzeigen und Managen von Protokollen

Die in der folgenden Tabelle aufgeführten Protokollierungsfunktionen sind für Speichersysteme verfügbar.

Tabelle 9 Protokollierungsfunktionen

Feature	Beschreibung
Löschen von Protokolleinträgen	Wenn das Protokollsystem des Speichersystems zwei Millionen Protokolleinträge umfasst, werden die ältesten 500.000 Einträge gelöscht (wie durch die Protokollaufzeichnungsdauer festgelegt), um 1,5 Millionen Protokolleinträge zu erreichen. Sie können Protokolleinträge archivieren, indem Sie die Remote-Protokollierung aktivieren, sodass Protokolleinträge zu einem Remote-Netzwerk-Node hochgeladen werden, wo sie archiviert oder gesichert werden können. Weitere Informationen finden Sie im Abschnitt Protokollierung auf Seite 40.
Protokollierungsebenen	Protokollierungsebenen können nicht für Speichersysteme konfiguriert werden. Protokollierungsebenen können nur für exportierte Protokolldateien konfiguriert werden, wie im Abschnitt Protokollierung auf Seite 40 beschrieben.
Warnmeldungsintegration	Sie können Warnmeldungsinformationen für Speichersysteme wie folgt anzeigen: • Nur Warnmeldungen anzeigen:

Tabelle 9 Protokollierungsfunktionen (Fortsetzung)

Feature	Beschreibung
	▪ Navigieren Sie in Unisphere zu **Ereignisse** > **Warnmeldungen**. • Protokollereignisse anzeigen: ▪ Geben Sie in der Unisphere-CLI den Befehl `uemcli /event/alert/hist show` ein. ▪ In Unisphere, wechseln Sie zu **System** > **Service** > **Protokolle**.
Externes Protokollmanagement	Sie können Protokolleinträge archivieren, indem Sie die Remote-Protokollierung aktivieren, sodass Protokolleinträge zu einem Remote-Netzwerk-Node hochgeladen werden, wo sie archiviert oder gesichert werden können. Dort können Sie Tools wie syslog verwenden, um Protokollergebnisse zu filtern und zu analysieren. Weitere Informationen finden Sie im Abschnitt Protokollierung auf Seite 40.
Zeitliche Synchronisierung	Die Protokollzeit wird im GMT-Format aufgezeichnet und gemäß der Speichersystemzeit verwaltet (möglicherweise über einen NTP-Server mit der lokalen Netzwerkzeit synchronisiert).

Remote-Protokollierungsoptionen

Das Speichersystem unterstützt die Protokollierung von Nutzermeldungen/Auditmeldungen auf maximal 5 Remotehost. Über das Speichersystem muss ein Zugriff auf den Remotehost möglich sein. Für die Sicherheit der Protokollinformationen muss über die Netzwerkzugriffskontrollen oder die Systemsicherheit auf dem Remotehost gesorgt werden.

Standardmäßig überträgt das Speichersystem Protokollinformationen über Port 514 mit UDP. Die folgenden Remote-Protokollierungseinstellungen sind über Unisphere konfigurierbar. Melden Sie sich bei Unisphere an und klicken Sie auf **Einstellungen** > **Management** > **Remoteprotokollierung**.

- Aktivieren Sie die Protokollierung auf einem Remotehost.
- Netzwerkname oder IP-Adresse, an den/die das Speichersystem Remoteprotokollinformationen sendet.
- Typ der zu sendenden Protokollmeldungen. Legen Sie mithilfe des Felds Gerät den Typ der Protokollmeldung fest. Es empfiehlt sich, die Option „Benutzermeldungen“ auszuwählen.
- Schweregrad der Ereignisse, die an einen Remotehost gesendet werden sollen
- Portnummer und -typ (UDP oder TCP) für die Protokollübertragung

Konfigurieren eines Hosts für den Empfang von Speichersystem-Protokollmeldungen

Vor der Konfiguration der Remoteprotokollierung für ein System müssen Sie jedes Remotesystem konfigurieren, um Protokollierungsmeldungen vom Speichersystem zu erhalten. Eine Root/ein Administrator auf dem empfangenden Computer kann den syslog-Remoteserver oder rsyslog-Server durch die Bearbeitung der syslog server- oder rsyslog server-Konfigurationsdatei (syslogng.conf oder rsyslog.conf) auf dem

Remotesystem für den Empfang von Protokollinformationen entsprechend konfigurieren.

Hinweis

Weitere Informationen zum Einrichten und Ausführen eines syslog-Remote-Servers finden Sie in der Dokumentation für das Betriebssystem, das auf dem Remotesystem ausgeführt wird.

KAPITEL 4

Kommunikationssicherheit

In diesem Kapitel werden verschiedene in das Speichersystem implementierte Funktionen für die Kommunikationssicherheit beschrieben.

Folgende Themen werden behandelt:

Portnutzung

Die Kommunikation mit den Unisphere- und CLI-Oberflächen erfolgt über HTTPS (Port 443). Versuche, auf Unisphere über Port 80 (über HTTP) zuzugreifen, werden automatisch an Port 443 umgeleitet.

Netzwerkports des Speichersystems

In Tabelle 10 auf Seite 44 sind die Netzwerkservices (und entsprechenden Ports) im Speichersystem dargestellt.

Tabelle 10 Netzwerkports des Speichersystems

Service	Protokoll	Port	Beschreibung
FTP	TCP	21	Port 21 ist der Kontrollport, den der FTP-Service auf eingehende FTP-Anforderungen überwacht.
SFTP	TCP/UDP	22	Warnmeldungen über SFTP (FTP über SSH) SFTP ist ein Client-/Serverprotokoll. Benutzer können mithilfe von SFTP Dateiübertragungen auf einem Speichersystem im lokalen Subnetz durchführen. Ermöglicht ausgehende FTP-Kontrollverbindungen. Ist der Port geschlossen, ist FTP nicht verfügbar.
SSH/SSHD, VSI	TCP/UDP	22	Lässt SSH-Zugriff zu (falls aktiviert). Wird auch für das VSI-Plug-in verwendet. Ist der Port geschlossen, sind Managementverbindungen über SSH und das VSI-Plug-in nicht verfügbar.
Dynamisches DNS-Update	TCP/UDP	53	Wird zum Übertragen von DNS-Abfragen an den Server in Kombination mit dem Dynamic Host Control Protocol (DHCP) verwendet. Ist dieser Port geschlossen, funktioniert die DNS-Namensauflösung nicht.
DHCP-Client	UDP	67	Ermöglicht dem Speichersystem, während des anfänglichen Konfigurationsprozesses als DHCP-Client zu agieren. Wird zum Übermitteln von Meldungen vom Client (Speichersystem) zum DHCP-Server verwendet, um Managementoberflächeninformationen automatisch abzurufen. Wird außerdem verwendet, um DHCP für die Managementoberfläche eines Speichersystems zu konfigurieren, das

Tabelle 10 Netzwerkports des Speichersystems (Fortsetzung)

Service	Protokoll	Port	Beschreibung
			bereits bereitgestellt wurde. Ist dieser Port geschlossen, werden dynamische IP-Adressen nicht über DHCP zugewiesen.
DHCP-Client	UDP	68	Ermöglicht dem Speichersystem, während des anfänglichen Konfigurationsprozesses als DHCP-Client zu agieren. Wird zum Empfangen von Meldungen vom DHCP-Server zum Client (Speichersystem) verwendet, um Managementoberflächeninformationen automatisch abzurufen. Wird außerdem verwendet, um DHCP für die Managementoberfläche eines Speichersystems zu konfigurieren, das bereits bereitgestellt wurde. Ist dieser Port geschlossen, werden dynamische IP-Adressen nicht über DHCP zugewiesen.
HTTP	TCP/UDP	80	Umleitung für HTTP-Datenverkehr zu Unisphere und zur Unisphere-CLI. Ist der Port geschlossen, ist Managementdatenverkehr zum Standard-HTTP-Port nicht verfügbar.
NAS, VAAI-NAS	TCP	111	Bietet NAS-Datenspeicher für VMware und wird für VAAI-NAS verwendet. Ist dieser Port geschlossen, sind NAS-Datenspeicher und VAAI-NAS nicht verfügbar.
Portmapper, rpcbind (Netzwerkinfrastruktur)	TCP/UDP	111	Wird vom Standard-Portmapper oder dem rpcbind-Service geöffnet und ist ein zusätzlicher Speichersystem-Netzwerkservice. Er kann nicht beendet werden. Per Definition kann ein Clientsystem bei einer Netzwerkverbindung zum Port diesen abfragen. Es wird keine Authentifizierung durchgeführt.
NTP	UDP	123	NTP-Zeitsynchronisation. Ist der Port geschlossen, wird die Zeit zwischen Arrays nicht synchronisiert.
DCE Remote Procedure Call (DCERPC) und NDMP	UDP	135	Mehrere Zwecke für Microsoft Client. Auch verwendet für NDMP.
NETBIOS Name Service (SMB)	TCP/UDP	137	Der NETBIOS Name Service ist mit den Speichersystem-SMB-Dateifreigabeservices verbunden und eine Kernkomponente dieser Funktion

Tabelle 10 Netzwerkports des Speichersystems (Fortsetzung)

Service	Protokoll	Port	Beschreibung
			(Wins). Wenn dieser Port deaktiviert ist, deaktiviert er alle SMB-bezogenen Services.
NETBIOS Datagram Service (SMB)	UDP	138	Der NETBIOS Datagram Service ist mit den Speichersystem-SMB-Dateifreigabeservices verbunden und eine Kernkomponente dieser Funktion. Nur der Service zum Durchsuchen wird verwendet. Wenn dieser Port deaktiviert ist, deaktiviert er die Funktion zum Durchsuchen.
NETBIOS-Sitzungsservice (SMB)	TCP/UDP	139	Der NETBIOS Session Service ist mit den Speichersystem-SMB-Dateifreigabeservices verbunden und eine Kernkomponente dieser Funktion. Wenn SMB-Services aktiviert sind, ist dieser Port geöffnet. Er ist insbesondere für frühere Versionen von Windows erforderlich (vor Windows 2000). Clients mit befugtem Zugriff auf die Speichersystem-SMB-Services benötigen für den kontinuierlichen Betrieb eine Netzwerkverbindung zum Port.
SNMP Unix Multiplexer	TCP	199	SNMP-Kommunikation. Ist dieser Port geschlossen, werden Speichersystem-Warnmeldungsmechanismen, die auf SNMP basieren, nicht gesendet.
LDAP	TCP/UDP	389	Nicht sichere LDAP-Abfragen. Ist dieser Port geschlossen, sind nicht sichere LDAP-Authentifizierungsabfragen nicht verfügbar. Sicheres LDAP ist als Alternative konfigurierbar.
Service Location Protocol (SLP)	TCP/UDP	427	Ermöglicht es Hosts (oder anderen Ressourcen), verfügbare, von einem Speichersystem bereitgestellte Services zu erkennen.
HTTPS	TCP/UDP	443	Sicherer HTTP-Datenverkehr zu Unisphere und zur Unisphere-CLI. Ist dieser Port geschlossen, ist keine Kommunikation mit dem Array möglich. **Hinweis** Bei SMI-S wird dieser Port für das Arraymanagement verwendet; Port 5989 ist jedoch eigentlich der Standardport für diesen Zweck.

Tabelle 10 Netzwerkports des Speichersystems (Fortsetzung)

Service	Protokoll	Port	Beschreibung
SMB	TCP	445	SMB (auf dem Domain-Controller) und SMB-Verbindungsport für Windows 2000-Clients und höher. Clients mit befugtem Zugriff auf die Speichersystem-SMB-Services benötigen für den kontinuierlichen Betrieb eine Netzwerkverbindung zum Port. Eine Deaktivierung dieses Ports deaktiviert alle SMB-bezogenen Services. Ist Port 139 ebenfalls deaktiviert, wird die SMB-Dateifreigabe deaktiviert.
DHCP (nur IPv6)	UDP	546	DHCP (v6)-Client Ist dieser Port geschlossen, werden dynamische IP-Adressen nicht über DHCP zugewiesen.
DHCP (nur IPv6)	UDP	547	DHCP (v6)-Server. Ist dieser Port geschlossen, werden dynamische IP-Adressen nicht über DHCP zugewiesen.
LDAPS	TCP/UDP	636	Sichere LDAP-Abfragen. Ist dieser Port geschlossen, sind sichere LDAP-Authentifizierungsabfragen nicht verfügbar.
FTP	TCP	1024:65535	Verwendet für FTP (passiv). Port 1024:65535 bezieht sich auf Daten, während Port 1025: 65535 mit dem Management zusammenhängt.
mountd (NFS)	TCP/UDP	1234	Verwendet für den Mountservice, der eine Kernkomponente des NFS-Service (Versionen 2, 3 und 4) und eine wichtige Komponente der Interaktion zwischen SP und NAS-Server ist.
NAS, VAAI-NAS	TCP	2049	Bietet NAS-Datenspeicher für VMware und wird für VAAI-NAS verwendet. Ist dieser Port geschlossen, sind NAS-Datenspeicher und VAAI-NAS nicht verfügbar.
NFS	TCP/UDP	2049	Verwendet für die Bereitstellung von NFS-Services.
UDI-SSH	TCP	2222	Leitet Datenverkehr von Port 22 für das eth*-Gerät um.
iSCSI	TCP	3260	Bietet Zugriff auf iSCSI-Services. Ist dieser Port geschlossen, sind dateibasierte iSCSI-Services nicht verfügbar.
NFS	TCP/UDP	4.000	Wird zum Bereitstellen der statd-Services von NFS verwendet. statd ist

Tabelle 10 Netzwerkports des Speichersystems (Fortsetzung)

Service	Protokoll	Port	Beschreibung
			der Dateisperrmonitor von NFS und arbeitet mit lockd zusammen, um Absturz- und Recovery-Funktionen für NFS zu bieten. Ist dieser Port geschlossen, sind NAS-statd-Services nicht verfügbar.
NFS	TCP/UDP	4001	Wird zum Bereitstellen der lockd-Services von NFS verwendet. lockd ist der Dateisperr-Daemon von NFS. Er verarbeitet Sperranfragen von NFS-Clients und arbeitet mit dem statd-Daemon zusammen. Ist dieser Port geschlossen, sind NAS-lockd-Services nicht verfügbar.
NFS	TCP/UDP	4002	Verwendet für die Bereitstellung von NFS-rquotad-Services. Der rquotad-Daemon bietet Quota-Informationen für NFS-Clients, auf denen ein Dateisystem gemountet ist. Ist dieser Port geschlossen, sind NAS-rquotad-Services nicht verfügbar.
SMB	UDP	4.003	Ermöglicht, dass SMB-ACL von einem Linux-Host aus mit den Tools `emcgetsd` oder `emcsetsd` angezeigt oder geändert werden kann.
Portable Archive Interchange (PAX) (Backupservices)	TCP	4658	• PAX ist ein Speichersystem-Archivprotokoll, das mit Standard-UNIX-Bandformaten arbeitet. • Dieser Service muss an mehrere interne Netzwerkschnittstellen gebunden werden und wird daher auch an die externe Schnittstelle gebunden. Über das externe Netzwerk eingehende Anforderungen werden jedoch abgelehnt. • Hintergrundinformationen zu PAX finden Sie in der entsprechenden EMC Dokumentation zu Backups. Es gibt mehrere technische Module zu diesem Thema für verschiedene Backup-Tools.
VSI	TCP	5080	Dieser Port steht für das VSI-Plug-in zur Verfügung. Ist dieser Port geschlossen, ist das VSI-Plug-in nicht verfügbar.
Replikationsservices	TCP	5085	Verbunden mit Replikationsservices

Tabelle 10 Netzwerkports des Speichersystems (Fortsetzung)

Service	Protokoll	Port	Beschreibung
KMIP (Key Management Interoperability Protocol)	TCP	5696	Für KMIP, unterstützt externe Schlüsselverwaltung mit KMIP. Falls geschlossen, sind KMIP-Services nicht verfügbar.
SMI-S	TCP	5989	Wird bei SMI-S für das Arraymanagement verwendet. Der SMI-S-Client verbindet sich über SMI-S TCP 5989 HTTPS mit dem Array. Das *SMI-S-Provider-Programmierhandbuch* bietet weitere Informationen über die Konfiguration dieses Service.
VASA	TCP	8443	VASA Vendor Provider für VASA 2.0.
VASA	TCP	8444	VASA Vendor Provider für VASA 1.0.
RCP (Replikationsservices)	TCP	8888	Vom Replicator (auf der sekundären Seite) verwendet. Der Port wird vom Replicator offen gelassen, sobald Daten repliziert werden müssen. Nach dem Starten gibt es keine Möglichkeit, den Service zu beenden.
NDMP	TCP	10.000	• Ermöglicht die Kontrolle von Backup und Recovery eines NDMP (Network Data Management Protocol)-Servers über eine Netzwerkbackup-Anwendung ohne Installation von Drittanbietersoftware auf dem Server. In einem Speichersystem fungiert der NAS-Server als NDMP-Server. • Der NDMP-Service kann deaktiviert werden, wenn kein NDMP-Band-Backup verwendet wird. • Der NDMP-Service wird über eine Kombination aus Benutzername und Passwort authentifiziert. Der Benutzername ist konfigurierbar. In der NDMP-Dokumentation wird beschrieben, wie Sie das Passwort für verschiedene Umgebungen konfigurieren.
NDMP	TCP	10500:10531	Verwenden Sie für Drei-Wege-Backup/Restore-Sitzungen die NAS-Server Ports 10500 bis 10531.
IWD	Intern	60260	IWD-Erstkonfigurations-Daemon. Ist dieser Port geschlossen, ist die

Tabelle 10 Netzwerkports des Speichersystems (Fortsetzung)

Service	Protokoll	Port	Beschreibung
			Initialisierung des Array über das Netzwerk nicht möglich.

Ports, zu denen das Speichersystem eine Verbindung herstellen kann

Das Speichersystem dient unter verschiedenen Umständen als Netzwerkclient, zum Beispiel bei der Kommunikation mit einem LDAP-Server. In diesen Fällen initiiert das Speichersystem die Kommunikation, und die Netzwerkinfrastruktur muss diese Verbindungen unterstützen. In Tabelle 11 auf Seite 50 sind die Ports beschrieben, auf die ein Speichersystem zugreifen können muss, damit der entsprechende Service ordnungsgemäß funktionieren kann. Dies schließt die Unisphere-CLI ein.

Tabelle 11 Netzwerkverbindungen, die vom Speichersystem initiiert werden können

Service	Protokoll	Port	Beschreibung
FTP	TCP	20	Für FTP-Datenübertragung verwendeter Port. Dieser Port kann geöffnet werden, indem FTP aktiviert wird, wie in der nächsten Zeile beschrieben. Authentifizierung wird auf Port 21 durchgeführt und vom FTP-Protokoll definiert.
FTP/SFTP	TCP	21	Warnmeldungen über SFTP (FTP über SSH) SFTP ist ein Client-/Serverprotokoll. Benutzer können mithilfe von SFTP Dateiübertragungen auf einem Speichersystem im lokalen Subnetz durchführen. Ermöglicht ausgehende FTP-Kontrollverbindungen. Ist der Port geschlossen, ist FTP nicht verfügbar.
SSH/SSHD, VSI	TCP	22	Lässt SSH-Zugriff zu (falls aktiviert). Wird auch für das VSI-Plug-in verwendet. Ist der Port geschlossen, sind Managementverbindungen über das SSH- und VSI-Plug-in nicht verfügbar.
SMTP	TCP	25	Ermöglicht dem System das Senden von E-Mails. Ist dieser Port geschlossen, sind E-Mail-Benachrichtigungen nicht verfügbar.
DNS	TCP/UDP	53	DNS-Abfragen. Ist dieser Port geschlossen, funktioniert die DNS-Namensauflösung nicht.
DHCP	UDP	67-68	Ermöglicht dem Speichersystem, als DHCP-Client zu fungieren. Ist dieser Port geschlossen, werden dynamische IP-Adressen nicht über DHCP zugewiesen.
HTTP	TCP	80	Umleitung für HTTP-Datenverkehr zu Unisphere und zur Unisphere-CLI. Ist der Port geschlossen, ist Managementdatenverkehr zum Standard-HTTP-Port nicht verfügbar.
Kerberos	TCP/UDP	88	Bietet ausgehende Kerberos-Tickets. Ist der Port geschlossen, sind die Kerberos-Authentifizierung und alle Protokolle, die ihn verwenden (z. B. SMB, LDAP, GPO, secNFS), nicht verfügbar.

Tabelle 11 Netzwerkverbindungen, die vom Speichersystem initiiert werden können (Fortsetzung)

Service	Protokoll	Port	Beschreibung
Portmapper, rpcbind (Netzwerkinfrastruktur)	TCP/UDP	111	Wird vom Standard-Portmapper oder dem rpcbind-Service geöffnet und ist ein zusätzlicher Speichersystem-Netzwerkservice. Er kann nicht beendet werden. Per Definition kann ein Clientsystem bei einer Netzwerkverbindung zum Port diesen abfragen. Es wird keine Authentifizierung durchgeführt.
NTP	UDP	123	NTP-Zeitsynchronisation. Ist der Port geschlossen, wird die Zeit zwischen Arrays nicht synchronisiert.
NETBIOS Name Service (SMB)	TCP/UDP	137	Der NETBIOS Name Service ist mit den Speichersystem-SMB-Dateifreigabeservices verbunden und eine Kernkomponente dieser Funktion (Wins). Wenn dieser Port deaktiviert ist, deaktiviert er alle SMB-bezogenen Services.
NETBIOS Datagram Service (SMB)	UDP	138	Der NETBIOS Datagram Service ist mit den Speichersystem-SMB-Dateifreigabeservices verbunden und eine Kernkomponente dieser Funktion. Nur der Service zum Durchsuchen wird verwendet. Wenn dieser Port deaktiviert ist, deaktiviert er die Funktion zum Durchsuchen.
NETBIOS-Sitzungsservice (SMB)	TCP/UDP	139	Der NETBIOS Session Service ist mit den Speichersystem-SMB-Dateifreigabeservices verbunden und eine Kernkomponente dieser Funktion. Wenn SMB-Services aktiviert sind, ist dieser Port geöffnet. Er ist insbesondere für frühere Versionen von Windows erforderlich (vor Windows 2000). Clients mit befugtem Zugriff auf die Speichersystem-SMB-Services benötigen für den kontinuierlichen Betrieb eine Netzwerkverbindung zum Port.
LDAP	TCP/UDP	389[a]	Nicht sichere LDAP-Abfragen. Ist dieser Port geschlossen, sind nicht sichere LDAP-Authentifizierungsabfragen nicht verfügbar. Sicheres LDAP ist als Alternative konfigurierbar.
Service Location Protocol (SLP)	TCP/UDP	427	Ermöglicht es Hosts (oder anderen Ressourcen), verfügbare, von einem Speichersystem bereitgestellte Services zu erkennen.
HTTPS	TCP	443	HTTPS-Datenverkehr zu Unisphere und zur Unisphere-CLI; und für sichere Remoteservices, wenn ESRS aktiviert und Integrated ESRS auf dem Speichersystem konfiguriert ist. Ist dieser Port geschlossen, ist keine Kommunikation mit dem Array möglich.
Kerberos	TCP/UDP	464	Ermöglicht die Änderung und Festlegung des Kerberos-Passworts. Ist dieser Port geschlossen, hat dies Auswirkungen auf SMB.
Remote Syslog	UDP	514[a]	Syslog – Protokollieren von Systemmeldungen auf einem Remotehost. Der vom System verwendete Hostport kann konfiguriert werden.
LDAPS	TCP/UDP	636[a]	Sichere LDAP-Abfragen. Ist dieser Port geschlossen, sind sichere LDAP-Authentifizierungsabfragen nicht verfügbar.

Tabelle 11 Netzwerkverbindungen, die vom Speichersystem initiiert werden können (Fortsetzung)

Service	Protokoll	Port	Beschreibung
VMware	TCP	843	VMawareness – ermöglicht die VMware SDK-Kommunikation mit vSphere. Ist dieser Port geschlossen, ist die vCenter/ ESX-Erkennung nicht verfügbar.
FTP	TCP	1024:65535	Ermöglicht ausgehende FTP-Kontrollverbindungen. Ist der Port geschlossen, ist FTP nicht verfügbar.
SOCKS	TCP	1080	Port 1080 ist der Standardport, wenn der Port nicht angegeben und ESRS aktiviert und Integrated ESRS auf dem Speichersystem konfiguriert ist und eine Firewall zwischen dem Speichersystem und einem Proxyserver eingesetzt wird. Wenn der Standard- oder personalisierte Port geschlossen ist, ist Kommunikation mit dem Array über den Port nicht verfügbar.
mountd (NFS)	TCP/UDP	1234	Verwendet für den Mountservice, der eine Kernkomponente des NFS-Service (Versionen 2, 3 und 4) und eine wichtige Komponente der Interaktion zwischen SP und NAS-Server ist.
NFS	TCP/UDP	2049	Verwendet für die Bereitstellung von NFS-Services.
HTTP	TCP	3128	Port 3128 ist der Standardport, wenn der Port nicht angegeben und ESRS aktiviert und Integrated ESRS auf dem Speichersystem konfiguriert ist und eine Firewall zwischen dem Speichersystem und einem Proxyserver eingesetzt wird. Wenn der Standard- oder benutzerdefinierte Port geschlossen ist, ist Kommunikation mit dem Array über den Port nicht verfügbar.
iSNS	TCP	3205	Verwendet zum Senden von Internet Storage Naming Service (iSNS)-Registrierungen an den iSNS-Server.
iSCSI	TCP	3260	Bietet Zugriff auf iSCSI-Services. Ist dieser Port geschlossen, sind dateibasierte iSCSI-Services nicht verfügbar.
NFS	TCP/UDP	4.000	Wird zum Bereitstellen der statd-Services von NFS verwendet. statd ist der Dateisperrmonitor von NFS und arbeitet mit lockd zusammen, um Absturz- und Recovery-Funktionen für NFS zu bieten.
NFS	TCP/UDP	4001	Wird zum Bereitstellen der lockd-Services von NFS verwendet. lockd ist der Dateisperr-Daemon von NFS. Er verarbeitet Sperranfragen von NFS-Clients und arbeitet mit dem statd-Daemon zusammen.
NFS	TCP/UDP	4002	Verwendet für die Bereitstellung von NFS-rquotad-Services. Der rquotad-Daemon bietet Quota-Informationen für NFS-Clients, auf denen ein Dateisystem gemountet ist.
VSI	TCP	5080	Dieser Port steht für das VSI-Plug-in zur Verfügung. Ist dieser Port geschlossen, ist das VSI-Plug-in nicht verfügbar.
KMIP	TCP	5696	Für KMIP, unterstützt externe Schlüsselverwaltung mit KMIP. Falls geschlossen, sind KMIP-Services nicht verfügbar.

Tabelle 11 Netzwerkverbindungen, die vom Speichersystem initiiert werden können (Fortsetzung)

Service	Protokoll	Port	Beschreibung
HTTPS	TCP	8443	HTTPS-Datenverkehr für sicheren Remotesupport, wenn ESRS aktiviert und Integrated ESRS auf dem Speichersystem konfiguriert ist. Wenn dieser Port geschlossen ist, sinkt die Remotesupportperformance erheblich. Dies hat direkte Auswirkungen auf die Zeit zur Lösung von Problemen im Hinblick auf das Unity-Speichersystem.
REST	TCP	9443	Wird zum Senden von Servicebenachrichtigungen an einen ESRS-Gatewayserver verwendet, wenn ESRS aktiviert und Centralized ESRS auf dem Speichersystem konfiguriert ist.
CAVA (Common Anti-Virus Agent):	TCP	12228	Wird verwendet, um für Kunden eine CAVA-Virenschutzlösung mithilfe eines NAS-Servers anzubieten. Falls geschlossen, ist die CAVA-Virenschutzlösung nicht verfügbar.
IWD	Intern	60260	IWD-Erstkonfigurations-Daemon. Ist dieser Port geschlossen, ist die Initialisierung des Array über das Netzwerk nicht möglich.

a. Die LDAP- und LDAPS-Portnummern können aus Unisphere überschrieben werden, wenn Sie Verzeichnisdienste konfigurieren. Die Standardportnummer wird in einem Eingabefeld angezeigt, das vom Benutzer überschrieben werden kann. Außerdem kann die Remote Syslog-Portnummer in Unisphere überschrieben werden.

Speichersystemzertifikat

Das Speichersystem generiert automatisch ein selbstsigniertes Zertifikat während der ersten Initialisierung. Das Zertifikat wird sowohl im NVRAM als auch in der Back-end-LUN gespeichert. Später präsentiert das Speichersystem dieses Zertifikat den Clients, die versuchen, eine Verbindung zum Speichersystem über den Managementport herzustellen.

Gemäß Einstellung läuft das Zertifikat nach 3 Jahren ab, jedoch generiert das Speichersystem das Zertifikat einen Monat vor diesem Ablaufdatum erneut. Außerdem können Sie mit dem Servicebefehl `svc_custom_cert` ein neues Zertifikat hochladen. Dieser Befehl installiert ein angegebenes SSL-Zertifikat im PEM-Format für die Verwendung mit der Unisphere-Managementoberfläche. Weitere Informationen über diesen Servicebefehl finden Sie in den *Technischen Hinweisen zu Servicebefehlen*. Sie können Zertifikate nicht über Unisphere oder die Unisphere-CLI anzeigen. Sie können Zertifikate aber über einen Browserclient oder ein Webtool anzeigen, das versucht, eine Verbindung zum Managementport herzustellen.

Hinweis

Wenn sich das Array im FIPS-Modus befindet und ein Zertifikat außerhalb des Arrays generiert wird, muss das Zertifikat nicht nur im PEM-Format vorliegen, sondern der private Schlüssel muss auch das PKCS#1-Format aufweisen. Sie können einen openssl-Befehl für diese Konvertierung verwenden. Nachdem die .cer- und .pk-Dateien generiert wurden, ist dieser zusätzliche Schritt erforderlich, wenn das Zertifikat in einem Array im FIPS-Modus verwendet werden soll.

Zum Erhöhen der Sicherheit verwenden einige Unternehmen CA-Zertifikatsketten. Bei Zertifikatsketten werden zwei oder mehr CA-Zertifikate miteinander verknüpft. Das primäre CA-Zertifikat ist das Stammzertifikat am Ende der CA-Zertifikatskette. Da das System die gesamte Zertifikatskette zum Überprüfen der Authentizität eines empfangenen Zertifikats benötigt, sollten Sie den Verzeichnisserveradministrator fragen, ob Zertifikatsketten verwendet werden. Ist dies der Fall, müssen Sie alle relevanten Zertifikate in einer Datei verketten und diese Version hochladen. Das Zertifikat muss mit PEM/Base64 kodiert sein und das Suffix .cer aufweisen.

Austauschen eines selbstsignierten Speichersystemzertifikats durch Zertifikate, die von einer lokalen Zertifizierungsstelle signiert sind

Bevor Sie neue Zertifikate für das Speichersystem von einer lokalen Zertifizierungsstelle hochladen können, um die vorhandenen selbstsignierten Unisphere SSL-Zertifikate zu ersetzen, müssen Sie Folgendes tun:

1. Erstellen Sie einen privaten Schlüssel auf dem Speicherprozessor (SP).

   Hinweis

   Beispiel:

   ```
   22:59:02 service@unknown spa:~/openssl> openssl genrsa -des3 -out
   unitycert.key -passout pass:emcemc
   Generating RSA private key, 2048 bit long modulus
   ..........................+++
   ..................................................................................
   +++
   e is 65537 (0x10001)
   ```

2. Entfernen Sie die Passphrase aus dem Schlüssel auf dem SP.

   HINWEIS

   Dieser Schritt ist sehr wichtig. Wenn die Passphrase nicht aus dem Schlüssel entfernt wird, führt dies zu einem SP-Fehler.

   Hinweis

   Beispiel:

   ```
   22:59:08 service@unknown spa:~/openssl> openssl rsa -in unitycert.key -
   passin pass:emcemc -out unitycert.pk
   writing RSA key
   ```

3. Fordern Sie eine CSR auf dem SP an.

Hinweis

Beispiel:

```
22:59:12 service@unknown spa:~/openssl> openssl req -new -sha256 -key
unitycert.pk -out unitycert.csr -days 1825
-subj '/C=US/ST=MA/L=Sarasota/O=MyCust/CN=10.0.0.1'
```

Hier ist ein Beispiel: **`-subj '/C=US/ST=MA/L=Sarasota/O=MyCust/CN=10.0.0.1'`**. Sie sollten es so ändern, dass es Ihrer Umgebung entspricht.

4. Lassen Sie die CSR von Ihrer Zertifizierungsstelle signieren (Windows CA-Server, OpenSSL-CA-Server oder einen anderen CA-Server). Im Folgenden finden Sie Beispiele für das Senden einer CSR an einen CA-Server zur Unterzeichnung mit folgenden Mitteln:

   - Drucken Sie die CSR mit dem Befehl `cat`, kopieren oder fügen Sie sie in Ihren lokalen Editor ein und benennen Sie sie als unitycert.csr.

     ```
     23:00:01 service@unknown spa:~/openssl> cat unitycert.csr
      -----BEGIN CERTIFICATE REQUEST-----
     MIICljCCAX4CAQAwUTELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAk1BMREwDwYDVQ
     QH
     DAhTYXJhc290YTEPMA0GA1UECgwGTXlDdXN0MREwDwYDVQQDDAgxMC4wLjAuMT
     CC

     ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOBxqufN1Vpm0hq5K5UU0o
     cd
     teL2hJr5T1WIOmwQreX4nIdHIxVoWmyepmT7IZJIrQZQc8GuFDRx5qZ/
     cwlxoup7
     3aprMKCx8Ka6nQE3ue46tehYxqwA7mCyT1XYIW7c5l1HJmEddj
     +Lqj23OwXTkOjX
     skzubLfI08zDgYyW+KrmMmnAQIpPucHiX8FmjhilNGUXXiN7f/
     jtDq4M1QZcj2Vp
     CVySMB5b1bGs1u10HQcv/
     aBSE5cU7FAxaLyJpIHJnk8fPXJo02hSu6B3NG7RDa1B
     35gW6qqlbFIjXUlWtzi4JKA6GIzCq576YcGeQA5QuIrKqE6feeTjsKD1Ac9tXa
     cC
     AwEAAaAAMA0GCSqGSIb3DQEBCwUAA4IBAQBpJn2Fu9noAMhn
     +IbTJf9EVTAYsZGc
     ddtgZcnVgEpI/dxB0p4ME210hg28UEwKl0wFAypGm8LaMxg0lbtfpUpU31JbaS
     +2
     lJc/79vxTfrWWNnSF95C+wer2LB93VLov8MSQqPZfl0LPb4NRU/
     XaE4l9Vh5DYl4
     /FmwHXsifwV5f1TUkvhC8YTwn5frWQjruz
     +ItZ3z9DetQX0OXYXMcaPX5Qp6aU5m
     dsXFHDDiaVbOofJN9z6OPOsWUhn0ZwEpnW8q/
     +V72MdBIfiwEjoQqZZKh4w1l0/7
     uElP8BfS7vH/i87OCqHJM0g/O3IndF+p5wYzmhrDPg/f3belQVQvKs7Z
     -----END CERTIFICATE REQUEST-----
     ```

   - Laden Sie CSR nach Secure Copy Protocol (SCP) herunter.

     Hinweis

     Um CSR-Dateien mithilfe von SCP herunterzuladen, verwenden Sie ein Drittanbietertool (z. B. WinSCP), um eine Verbindung zur Unity-Management-IP-Schnittstelle (username: service) herzustellen, und kopieren Sie dann die Datei `unitycert.csr` auf den lokalen Computer.

5. Nachdem Sie das signierte Zertifikat vom Zertifizierungsstellenserver erhalten haben, laden Sie es auf den SP hoch und speichern Sie es unter dem Namen `unitycert.crt` (entsprechend `unitycert.pk`).

Hinweis

Beispiel:

```
$ svc_custom_cert unitycert

Example:
service@spa spa:~> svc_custom_cert pod6 Successfully installed custom
certificate files. Restarting web server ...
Unsupported
Sun May 22 05:37:48 2016:7645\0x7f44ba3e27c0:32:Module CIC/1.1.10.6
loaded
```

Speichersystemschnittstellen, -services und -funktionen, die das Internetprotokoll Version 6 unterstützen

Sie können die Schnittstellen auf einem System konfigurieren und IPv6-Adressen (Internetprotokoll Version 6) verwenden, um verschiedene Services und Funktionen zu konfigurieren. Die folgende Liste enthält alle Funktionen, die das IPv6-Protokoll unterstützen:

- Schnittstellen (SF, iSCSI): zum statischen Zuweisen einer IPv4- oder IPv6-Adresse zu einer Schnittstelle
- Hosts: zum Eingeben eines Netzwerknamens, einer IPv4-Adresse oder einer IPv6-Adresse eines Hosts
- Routen: zum Konfigurieren von Routen für das IPv4- oder IPv6-Protokoll
- Diagnose: zum Initiieren eines diagnostischen `ping`-CLI-Befehls mit einer IPv4- oder IPv6-Zieladresse. Wählen Sie in Unisphere **Einstellungen** > **Zugriff** > **Routing** > **Ping/Trace** aus, um auf den Bildschirm Ping/Trace zuzugreifen, der die IPv6-Zieladressen ebenfalls unterstützt.

Alle Speichersystemkomponenten unterstützen IPv4 und die meisten unterstützen IPv6.In Tabelle 12 auf Seite 56 zeigt die Verfügbarkeit des IPv6-Supports nach Einstellungstyp und Komponente:

Tabelle 12 IPv6-Unterstützung nach Einstellungstyp und Komponente

Einstellungstyp	Komponente	Von IPv6 unterstützt
Unisphere-Managementeinstellungen	Managementports	Ja
	Domain Name Server (DNS)	Ja
	NTP (Network Time Protocol)-Server	Ja
	Remote-Protokollierungsserver	Ja
	LDAP-Server	Nein

Tabelle 12 IPv6-Unterstützung nach Einstellungstyp und Komponente (Fortsetzung)

Einstellungstyp	Komponente	Von IPv6 unterstützt
Unisphere-Hostkonfigurationseinstellungen	Microsoft Exchange	Ja
	VMware-Datastore (NFS)	Ja
	VMware-Datastore (VMFS)	Ja
	Hyper-V-Datastore	Ja
Unisphere-Warnmeldungseinstellungen	SNMP-Trap-Ziele	Ja
	SMTP-Server	Ja
	EMC Secure Remote Support Services (ESRS)	Nein
Speicherservereinstellungen	iSCSI-Server	Ja
	Server für freigegebene Ordner	Ja
	Network Information Service (NIS)-Server (für NFS-NAS-Server)	Ja
	Active Directory-Server (für SMB-NAS-Server)	Ja
	Internet Storage Service (iSNS)-Server	Ja
Sonstige	PING-Ziele	Ja
	Remotejournal	Ja
	LDAP	Ja

IPv6-Adressenstandard

Das Internetprotokoll der Version 6 (IPv6) ist ein Internetprotokoll-Adressenstandard, der von der Internet Engineering Task Force (IETF) entwickelt wurde. Er ersetzt den IPv4-Adressenstandard, den die meisten Internetservices heute verwenden.

IPv4 nutzt 32-Bit-IP-Adressen. Es stehen ca. 4,3 Milliarden mögliche Adressen zur Verfügung. Durch die explosionsartige Zunahme an Internetbenutzern und mit dem Internet verbundenen Geräten wird der verfügbare IPv4-Adressraum knapp. IPv6 behebt das Problem des Adressenmangels, da es 128-Bit-Adressen nutzt. Dadurch stehen ca. 340 Billionen Adressen zur Verfügung. IPv6 behebt auch andere IPv4-Probleme, z. B. hinsichtlich der Mobilität, der automatischen Konfiguration und der gesamten Erweiterbarkeit.

Bei einer IPv6-Adresse handelt es sich um einen Hexadezimalwert, der 8 durch Doppelpunkte getrennte 16-Bit-Felder aufweist:

`hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh`

Jedes Zeichen in einer IPv6-Adresse kann eine Zahl von 0 bis 9 oder ein Buchstabe von A bis F sein.

Weitere Informationen zum IPv6-Standard (RFC 2460) finden Sie auf der IETF-Website (http://www.ietf.org).

Zugriff auf die Speichersystem-Managementoberfläche mit IPv6

Wenn Sie Managementverbindungen im Speichersystem einrichten, können Sie das System so konfigurieren, dass es folgende Typen von IP-Adressen akzeptiert:

- statische IPv6-Adressen (Internetprotokoll Version 6), über DHCP abgerufene IPv4-Adressen und statische IPv4-Adressen
- reine IPv4-Adressen

IPv6-Adressen können der Managementoberfläche statisch zugewiesen werden. IPv6-Adressen der Managementoberfläche können auf einen von zwei Modi festgelegt werden: manuell/statisch oder deaktiviert. Wenn Sie IPv6 deaktivieren, wird die Bindung des Protokolls an die Schnittstelle nicht aufgehoben. Mit dem Befehl „disable“ werden alle Unicast-IPv6-Adressen entfernt, die der Managementoberfläche zugewiesen sind, und das Speichersystem antwortet nicht mehr auf Anforderungen über IPv6. IPv6 ist standardmäßig deaktiviert.

Nach dem Installieren, Verkabeln und Hochfahren des Systems muss der Speichersystem-Managementoberfläche eine IP-Adresse zugewiesen werden. Wenn Sie das Speichersystem nicht in einem dynamischen Netzwerk ausführen oder manuell eine statische IP-Adresse zuweisen möchten, müssen Sie das Connection Utility herunterladen, installieren und ausführen. Weitere Informationen zum Connection Utility finden Sie unter Ausführen des Verbindungsdienstprogramms auf Seite 60.

Es werden über die Managementoberfläche unter Verwendung von IPv6 eingehende Anforderungen für das Speichersystem unterstützt. Sie können die Managementoberfläche eines Speichersystems so konfigurieren, dass sie in einer reinen IPv4- oder in einer reinen IPv6-Umgebung oder aber in einer kombinierten IPv4- und IPv6-Umgebung funktioniert, und Sie können das Speichersystem über die Unisphere-UI und die CLI (Command Line Interface, Befehlszeilenoberfläche) managen.

Ausgehende Services wie Network Time Protocol (NTP) und Domain Naming System (DNS) unterstützen die IPv6-Adressierung entweder durch die Verwendung expliziter IPv6-Adressen oder durch die Verwendung von DNS-Namen. Wenn ein DNS-Name sowohl zu IPv6 als auch zu IPv4 aufgelöst werden kann, kommuniziert das Speichersystem über IPv6 mit dem Server.

Die CLI-Befehle „manage network interface set“ und „show“, die zum Managen der Managementoberfläche verwendet werden können, umfassen Attribute für IPv6. Weitere Informationen über diese Befehle zum Managen der Netzwerkschnittstelle und den zugehörigen Attributen finden Sie im *Unisphere Command Line Interface-Benutzerhandbuch*.

Konfigurieren der Managementoberfläche mit DHCP

Nach dem Installieren, Verkabeln und Hochfahren des Systems muss der Speichersystem-Managementoberfläche eine IP-Adresse zugewiesen werden. Wenn Sie das Speichersystem in einem dynamischen Netzwerk mit einem DHCP-Server (Dynamic Host Control Protocol) und einem DNS-Server (Domain Name System) ausführen, kann die Management-IP-Adresse automatisch zugewiesen werden.

Hinweis

Wenn Sie das Speichersystem nicht in einer dynamischen Netzwerkumgebung ausführen oder manuell eine statische IP-Adresse zuweisen möchten, müssen Sie das Connection Utility installieren und ausführen. Weitere Informationen über das Connection Utility finden Sie unter Ausführen des Verbindungsdienstprogramms auf Seite 60.

Bei der Netzwerkkonfiguration müssen Sie die verfügbaren IP-Adressen, die korrekten Subnetzmasken sowie die Gateway- und Namensserveradressen festlegen. Weitere Informationen zum Einrichten von DHCP- und DNS-Servern finden Sie in Ihrer spezifischen Netzwerkdokumentation.

DHCP ist ein Protokoll zum automatischen Zuweisen von dynamischen IP-Adressen (Internet Protocol) zu Geräten in einem Netzwerk. Es ermöglicht Ihnen, IP-Adressen über einen zentralisierten Server zu steuern und automatisch eine neue, eindeutige IP-Adresse zuzuweisen, wenn ein Speichersystem mit dem Netzwerk Ihres Unternehmens verbunden wird. Diese dynamische Adressierung vereinfacht die Netzwerkadministration, da die Software IP-Adressen nachverfolgt. Es ist kein Administrator für die Aufgabe erforderlich.

Der DNS-Server ist ein IP-basierter Server, der Domainnamen in IP-Adressen übersetzt. Im Gegensatz zu numerischen IP-Adressen sind Domainnamen alphabetisch. Ferner kann man sie sich in der Regel einfacher merken. Da ein IP-Netzwerk auf IP-Adressen basiert, muss der DNS-Server Domainnamen in entsprechende IP-Adressen übersetzen. Beispiel: Der Domainname www.Javanet.com wird in die IP-Adresse 209.94.128.8. übersetzt.

Keine administrativen Informationen, wie Benutzernamen, Passwörter oder Ähnliches, werden während der Konfiguration von DHCP/dynamisches DNS ausgetauscht. Für die Konfiguration der Management-IP-Elemente (DHCP-Präferenz, DNS- und NTP-Serverkonfiguration) gilt das bestehende Unisphere-Sicherheits-Framework. DNS- und DHCP-Ereignisse, wie das Abrufen einer neuen IP-Adresse bei Ablaufen der Leasingdauer, werden in Speichersystem-Auditprotokollen aufgezeichnet. Wird DHCP nicht für die Konfiguration der Speichersystem-Management-IP verwendet, werden keine zusätzlichen Netzwerkports geöffnet.

Dynamische IP-Adressen (DHCP) dürfen nicht für Komponenten der ESRS VE-Server (EMC Secure Remote Services Virtual Edition), Policy Manager-Server oder gemanagte Geräte verwendet werden.

Hinweis

Wenn Sie DHCP zum Zuweisen von IP-Adressen zu ESRS-Komponenten (ESRS VE-Server, Policy Manager-Server oder gemanagte Geräte) verwenden, müssen diese statische IP-Adressen aufweisen. Leases für IP-Adressen, die EMC Geräte verwenden, können nicht so festgelegt werden, dass sie ablaufen. EMC empfiehlt, dass Sie den Geräten, die von ESRS gemanagt werden sollen, statische IP-Adressen zuweisen.

Ausführen des Verbindungsdienstprogramms

Hinweis

Wenn Sie das Speichersystem in einer dynamischen Netzwerkumgebung ausführen, die einen DHCP- und einen DNS-Server umfasst, müssen Sie das Connection Utility nicht verwenden und können der Speichersystem-Managementoberfläche stattdessen automatisch eine dynamische IP-Adresse (nur IPv4) zuweisen lassen. Wenn ein Speichersystem eine statische IP-Adresse verwendet, wird die Verwendung einer speziellen IP-Adresse manuell mit dem Connection Utility konfiguriert. Ein Problem bei der statischen Zuweisung, das aus einem Fehler oder Unaufmerksamkeit resultieren kann, tritt auf, wenn zwei Speichersysteme mit derselben Management-IP-Adresse konfiguriert werden. Dies sorgt für einen Konflikt, der zum Verlust der Netzwerkverbindung führen kann. Die Verwendung von DHCP zur dynamischen Zuweisung von IP-Adressen minimiert diese Art von Konflikten. Speichersysteme, die DHCP für die IP-Zuweisung verwenden, müssen keine statisch zugewiesenen IP-Adressen verwenden.

Das Installationsprogramm für das Connection Utility ist auf der EMC Online-Support-Website (https://support.emc.com) unter der Auswahl **Downloads** in der Menüleiste der Produktseite für Ihr Speichersystem verfügbar. Laden Sie die Software herunter, und installieren Sie das Programm auf einem Windows-Host. Wenn Sie das Connection Utility von einem Computer in demselben Subnetz wie das Speichersystem ausführen, erkennt das Connection Utility automatisch alle nicht konfigurierten Speichersysteme. Wenn Sie das Connection Utility in einem anderen Subnetz ausführen, können Sie die Konfiguration auf einem USB-Laufwerk speichern und auf das Speichersystem übertragen. Wenn sich das Speichersystem in einem anderen Subnetz als der Host mit dem Connection Utility befindet, können Sie die Konfiguration manuell vornehmen und IP-Netzwerk und Hostname-Informationen auf einem USB-Laufwerk als Textdatei speichern und das USB-Laufwerk an beide SPs anscchließen, die dann automatisch die IP-Netzwerk und Hostname-Informationen einstellen.

Hinweis

Die Management-IP-Adresse kann nicht geändert werden, wenn sich beide Speicherprozessoren (SPs) im Servicemodus befinden.

Nach der Ausführung des Connection Utility und der Übertragung der Konfiguration auf das Speichersystem können Sie die IP-Adresse, die Sie der Speichersystem-Managementoberfläche zugewiesen haben, in einen Webbrowser eingeben, um eine Verbindung zu dem Speichersystem herzustellen.

Wenn Sie sich das erste Mal bei dem Speichersystem anmelden, wird der Assistent für die Erstkonfiguration gestartet. Mit dem Assistenten für die Erstkonfiguration können Sie das Speichersystem konfigurieren, um Speicherressourcen zu erstellen.

Hinweis

Weitere Informationen über das Connection Utility finden Sie im *Unity Series Installation Guide*.

Protokollverschlüsselung (SMB) und Signaturen

Die SMB 3.0- und Windows 2012-Unterstützung ermöglicht die SMB-Verschlüsselung für SMB-fähige Hosts auf dem Speichersystem. Die SMB-Verschlüsselung ermöglicht sicheren Zugriff auf die Daten von SMB-Datei-Shares. Mit dieser Verschlüsselung wird die Sicherheit des Datenzugriffs in nicht vertrauenswürdigen Netzwerken sichergestellt. Sie bietet End-to-End-Verschlüsselung von gesendeten SMB-Daten zwischen dem Array und dem Host. Die Daten werden vor Abhörangriffen in nicht vertrauenswürdigen Netzwerken geschützt.

Die SMB-Verschlüsselung kann für jede Share einzeln konfiguriert werden. Nachdem eine Share als verschlüsselt definiert wurde, muss jeder SMB3-Client alle Anforderungen an diese Share verschlüsseln. Andernfalls wird der Zugriff auf die Share verweigert.

Zum Aktivieren der SMB-Verschlüsselung legen Sie entweder die Option **Protokollverschlüsselung** in den erweiterten SMB-Share-Eigenschaften in Unisphere fest oder stellen Sie sie über die CLI-Befehle `create` und `set` für SMB-Shares ein. Auf dem SMB-Client muss keine Einstellung vorgenommen werden.

Hinweis

Weitere Informationen über die SMB-Verschlüsselung finden Sie in der Unisphere-Onlinehilfe und im *Unisphere Command Line Interface-Benutzerhandbuch*.

SMB bietet außerdem Datenintegritätsprüfung (Signatur). Dieser Mechanismus sorgt dafür, dass Pakete nicht abgefangen, geändert oder erneut ausgeführt werden. Durch SMB-Signaturen wird eine Signatur zu jedem Paket hinzugefügt und sichergestellt, dass Drittanbieter keine Änderungen an Paketen vorgenommen haben.

Zur Verwendung von SMB-Signaturen müssen für den Client und den Server einer Transaktion SMB-Signaturen aktiviert sein. Standardmäßig müssen bei Windows Server-Domain-Controllern die Clients SMB-Signaturen verwenden. Bei Windows Server-Domains (Windows 2000 und höher) werden SMB-Signaturen mit einer Group Policy Object (GPO)-Policy festgelegt. Für Windows XP sind GPO-Services für SMB-Signaturen nicht verfügbar. Sie müssen die Windows Registry-Einstellungen verwenden.

Hinweis

Das Konfigurieren von SMB-Signaturen über GPOs wirkt sich auf alle Clients und Server in der Domäne aus und einzelne Registry-Einstellungen werden überschrieben. Detaillierte Informationen zum Aktivieren und Konfigurieren von SMB-Signaturen finden Sie in der Microsoft-Sicherheitsdokumentation.

In SMB1 führt das Aktivieren von Signaturen zu deutlichen Performanceeinbußen, vor allem bei der Aktivierung im WAN. Im Vergleich zu SMB1 kommt es bei SMB2- und SMB3-Signaturen nur zu geringen Verschlechterungen der Performance. Die Auswirkungen von Signaturen auf die Performance werden größer, wenn Sie schnellere Netzwerke verwenden.

HINWEIS

Wenn das ältere SMB1-Protokoll in Ihrer Umgebung nicht unterstützt werden muss, kann es mithilfe des Servicebefehls `svc_nas` deaktiviert werden. Weitere Informationen über diesen Servicebefehl finden Sie unter *Technische Hinweise zu Servicebefehlen*.

Konfigurieren von SMB-Signaturen mit GPOs

In Tabelle 13 auf Seite 62 werden die für SMB1-Signaturen verfügbaren GPOs erläutert.

Hinweis

Bei SMB2 und SMB3 verfügt jede Version über ein GPO für beide Seiten (Serverseite und Clientseite) für die Aktivierung der Option „Kommunikation digital signieren (immer)“. Weder die Serverseite noch die Clientseite verfügt über ein GPO zum Aktivieren der Option „Kommunikation digital signieren (wenn Client zustimmt)“.

Tabelle 13 GPOs für SMB1-Signaturen

GPO-Name	Funktion	Standardeinstellung
Microsoft-Netzwerkserver: Kommunikation digital signieren (immer)	Gibt an, ob die serverseitige SMB-Komponente eine Signatur erfordert	Disabled
Microsoft-Netzwerkserver: Kommunikation digital signieren (wenn Client zustimmt)	Gibt an, ob für die serverseitige SMB-Komponente Signaturen aktiviert sind	Disabled
Microsoft-Netzwerkclient: Kommunikation digital signieren (immer)	Gibt an, ob die clientseitige SMB-Komponente eine Signatur erfordert	Disabled
Microsoft-Netzwerkclient: Kommunikation digital signieren (wenn Server zustimmt)	Gibt an, ob für die cleintseitige SMB-Komponente Signaturen aktiviert sind	Aktiviert

Sie können SMB-Signaturen auch über Windows Registry konfigurieren. Wenn kein GPO-Service verfügbar ist, wie z. B. in einer Windows NT-Umgebung, werden die Registry-Einstellungen verwendet.

Konfigurieren von SMB-Signaturen mit Windows Registry

Registry-Einstellungen wirken sich nur auf den einzelnen Server oder Client aus, den Sie konfigurieren. Sie werden auf einzelnen Windows-Workstations und -Servern konfiguriert und haben Auswirkungen auf einzelnen Windows-Workstations und -Server.

Hinweis

Die folgenden Registry-Einstellungen beziehen sich auf Windows NT mit SP 4 oder höher. Diese Registry-Einträge sind in Windows-Server vorhanden, sollten aber über GPOs festgelegt werden.

Die serverseitigen Einstellungen befinden sich unter: `HKEY_LOCAL_MACHINE \System\CurrentControlSet\Services\lanmanserver\parameters\`

Hinweis

Bei SMB2 und SMB3 verfügt jede Version über einen Registry-Schlüssel für jede Seite (Serverseite und Clientseite) zur Aktivierung der Option „requiresecuritysignature“. Weder die Serverseite noch die Clientseite verfügt über einen Registry-Schlüssel zur Aktivierung der Option „enablesecuritysignature“.

Tabelle 14 Registry-Einträge für serverseitige SMB1-Signaturen

Registry-Einträge	Werte	Zweck
`enablesecuritysignature`	• 0 deaktiviert (Standardeinstellung) • 1 aktiviert	Bestimmt, ob SMB-Signaturen aktiviert sind.
`requiresecuritysignature`	• 0 deaktiviert (Standardeinstellung) • 1 aktiviert	Bestimmt, ob SMB-Signaturen erforderlich sind.

Die clientseitigen Einstellungen befinden sich unter: `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\lanmanworkstation\parameters\`

Tabelle 15 Registry-Einträge für clientseitige SMB1-Signaturen

Registry-Einträge	Werte	Zweck
`enablesecuritysignature`	• 0 deaktiviert • 1 aktiviert (Standardeinstellung)	Bestimmt, ob SMB-Signaturen aktiviert sind.
`requiresecuritysignature`	• 0 deaktiviert (Standardeinstellung) • 1 aktiviert	Bestimmt, ob SMB-Signaturen erforderlich sind.

IP Packet Reflect

IP Packet Reflect bietet eine zusätzliche Sicherheitsebene für Ihr Netzwerk. Da der Großteil des Netzwerkdatenverkehrs auf einem NAS-Server (einschließlich aller Dateisystem-I/Os) clientinitiiert ist, verwendet der NAS-Server Packet Reflect, um auf Clientanforderungen zu antworten. Bei Packet Reflect muss die Route für die Antwortpakete nicht bestimmt werden. Da Antwortpakete immer über dieselbe Schnittstelle wie die Anforderungspakete ausgehen, können Anforderungspakete nicht verwendet werden, um andere LANs indirekt zu überschwemmen. In Fällen, in denen zwei Netzwerkgeräte vorhanden sind, von denen eines mit dem Internet und das andere mit dem Intranet verbunden ist, werden Antworten auf Anforderungen im Internet nicht im Intranet angezeigt. Darüber hinaus haben Pakete aus externen Netzwerken keine Auswirkungen auf die internen Netzwerke, die vom Speichersystem verwendet werden.

IP Packet Reflect kann für jeden NAS-Server aktiviert werden. Es ist standardmäßig für alle NAS-Server aktiviert.

IP-Mehrmandantenfähigkeit

IP-Mehrmandantenfähigkeit bietet die Möglichkeit, den NAS-Servern auf einem Speicherprozessor isolierte, dateibasierte Speicherpartitionen zuzuweisen. Mandanten werden verwendet, um das kosteneffiziente Management verfügbarer Ressourcen zu ermöglichen und gleichzeitig sicherzustellen, dass die Sichtbarkeit und das Management des Mandanten nur auf die zugewiesenen Ressourcen beschränkt ist.

Hinweis

Wenn dies die erste Erstellung eines Mandanten in Ihrer Umgebung ist, lassen Sie das System automatisch einen UUID-Wert (Universal Unique Identifier) für den Mandanten erzeugen. Geben Sie für vorhandene Mandanten in Ihrer Umgebung, die über einen vom System erzeugten UUID-Wert verfügen, den UUID-Wert manuell ein.

Mit IP-Mehrmandantenfähigkeit kann jeder Mandant Folgendes haben:

- eigene IP-Adressen und Portnummern
- eigene VLAN-Domain
- eigene Routing-Tabelle
- eigene IP-Firewall
- DNS-Server oder andere administrative Server ermöglichen es dem Mandanten, seine eigene Authentifizierung und Sicherheitsvalidierung zu haben.

IP-Mehrmandantenfähigkeit wird implementiert, indem ein Mandant dem Speichersystem hinzugefügt wird, dem Mandanten eine Reihe von VLANs zugeordnet wird und dann für jeden der VLANs des Mandanten nach Bedarf ein NAS-Server erstellt wird. Es wird empfohlen, dass Sie für den Mandanten einen separaten Pool erstellen und dass Sie diesen Pool allen NAS-Servern des Mandanten zuordnen.

Hinweis

Ein Pool besteht aus einer Reihe von Laufwerken, die bestimmte Speichermerkmale für die Ressourcen bereitstellen, von denen sie genutzt werden.

Beachten Sie folgende Informationen über die Funktion IP-Mehrmandantenfähigkeit:

- Es gibt eine 1:n-Beziehung zwischen Mandanten und NAS-Server. Ein Mandant kann mehreren NAS-Servern zugeordnet sein, aber ein NAS-Server kann nur einem Mandanten zugeordnet sein.
- Sie können einen NAS-Server einem Mandanten zuordnen, wenn Sie den NAS-Server erstellen. Sobald Sie einen NAS-Server, der einem Mandanten zugeordnet ist, erstellen, können Sie seine Eigenschaften nicht mehr ändern.
- Während der Replikation werden Daten für einen Mandanten über das Netzwerk des Serviceanbieters anstatt über das Netzwerk des Mandanten übertragen.
- Da mehrere Mandanten dasselbe Speichersystem gemeinsam nutzen können, kann sich eine Spitze im Datenverkehr für einen Mandanten negativ auf die Reaktionszeit für andere Mandanten auswirken.

Informationen über VLANs

VLANs (Virtual Local Area Networks) sind logische Netzwerke, die unabhängig von einer physischen Netzwerkkonfiguration funktionieren. Z. B. können Sie mithilfe von VLANs alle Computer einer Abteilung in demselben Subnetz verwalten, wodurch die

Sicherheit erhöht und der Broadcast-Datenverkehr des Netzwerks reduziert werden kann.

Wenn einer einzigen Netzwerkschnittstelle mehrere logische Schnittstellen zugewiesen werden, kann jeder der Schnittstellen ein anderes VLAN zugewiesen werden. Besitzt jede Schnittstelle ein anderes VLAN, werden Pakete nur akzeptiert, wenn die Ziel-IP-Adresse mit der IP-Adresse der Schnittstelle und das VLAN-Tag des Pakets mit der VLAN-ID der Schnittstelle übereinstimmt. Ist die VLAN-ID einer Schnittstelle auf 0 festgelegt, werden Pakete ohne VLAN-Tags gesendet.

Es gibt zwei Methoden, mit VLANs zu arbeiten:

- Konfigurieren Sie einen Switchport mit einer VLAN-Kennung und verbinden Sie einen NAS-Serverport oder eine iSCSI-Schnittstelle mit diesem Switchport. Das Unity-System bemerkt nicht, dass es Teil des VLAN ist, und keine besondere Konfiguration des NAS-Servers oder der iSCSI-Schnittstelle ist erforderlich. In diesem Fall wird die VLAN-ID auf 0 (null) festgelegt.
- Implementieren Sie die IP-Mehrmandantenfähigkeit mithilfe von VLANs. In diesem Szenario ist jedem Mandanten ein Satz von einem oder mehreren VLANs zugeordnet und der NAS-Server ist verantwortlich für die Interpretation der VLAN-Tags und die richtige Verarbeitung der Pakete. Dies ermöglicht es dem NAS-Server, eine Verbindung zu mehreren VLANs und ihren entsprechenden Subnetzen über eine einzige physische Verbindung herzustellen. Bei dieser Methode werden die Switchports für Server so konfiguriert, dass sie bei Paketen, die an den Server gesendet werden, VLAN-Tags enthalten.

Unterstützung des Managements für FIPS 140-2

Der Federal Information Processing Standard 140-2 (FIPS 140-2) beschreibt von der US-Bundesregierung festgelegte Anforderungen, die IT-Produkte für die sensitive, aber nicht geheime Verwendung (Sensitive, but Unclassified, SBU) erfüllen sollten. Der Standard definiert die Sicherheitsanforderungen, die ein kryptografisches Modul in einem Sicherheitssystem, das nicht geheime Informationen in IT-Systemen schützt, erfüllen muss. Weitere Informationen über FIPS 140-2 finden Sie in der FIPS 1402-2-Publikation.

Das Speichersystem unterstützt einen FIPS-140-2-Modus für die SSL-Module, die den Clientmanagementverkehr verarbeiten. Die Managementkommunikation zum und vom System wird mit SSL verschlüsselt. Als Teil dieses Prozesses handeln Client und Speichermanagementsoftware eine Chiffre für den Austausch aus. Durch Aktivierung des FIPS-140-2-Modus wird die aushandelbare Gruppe der Cipher-Suites nur auf diejenigen eingeschränkt, die in der Publikation FIPS 140-2 Approved Security Functions aufgeführt sind. Wenn der FIPS-140-2-Modus aktiviert ist, können einige Ihrer vorhandenen Clients nicht mehr mit den Managementports des Systems kommunizieren, wenn sie die von FIPS 140-2 genehmigten Cipher-Suites nicht unterstützen. Der FIPS-140-2-Modus kann auf einem Speichersystem nicht aktiviert werden, wenn sich nicht mit FIPS kompatible Zertifikate im Zertifikatspeicher befinden. Sie müssen alle nicht FIPS-konformen Zertifikate vom Speichersystem entfernen, bevor Sie den FIPS-140-2-Modus aktivieren.

Managen des FIPS-140-2-Modus auf dem Speichersystem

Nur der Administrator und der Sicherheitsadministrator haben die Rechte zum Managen der Einstellung für den FIPS 140-2-Modus. Verwenden Sie den folgenden CLI-Befehl, um die Einstellung für den FIPS-140-2-Modus auf einem Speichersystem festzulegen:

Mit `uemcli /sys/security set -fips140Enabled yes` wird es in den FIPS-140-2-Modus versetzt.

Mit `uemcli /sys/securty set -fips140Enabled no` wird der FIPS-140-2-Modus deaktiviert.

Verwenden Sie den folgenden CLI-Befehl, um den aktuellen FIPS-140-2-Modus für das Speichersystem zu ermitteln:

```
uemcli /sys/security show
```

Wenn Sie die Einstellung für den FIPS 140-2-Modus auf einem Speichersystem ändern, werden beide SPs nacheinander automatisch neu gestartet, um die neue Einstellung zu übernehmen. Wenn der Neustart des ersten SP abgeschlossen ist, wird der andere SP neu gestartet. Das System arbeitet nur dann vollständig im konfigurierten FIPS-140-2-Modus, nachdem beide SPs neu gestartet sind.

Managementsupport für SSL-Kommunikation

Die Managementkommunikation zum und vom Speichersystem wird mit SSL verschlüsselt. Im Rahmen dieses Prozesses handeln der Client und das Speichersystem ein zu verwendendes SSL-Protokoll aus. Das Speichersystem unterstützt standardmäßig TLS 1.0-, TLS 1.1- und TLS 1.2-Protokolle für die SSL-Kommunikation. Das Speichersystem enthält eine administrative Einstellung, mit der TLS 1.0 im System deaktiviert werden kann. Durch die Deaktivierung des TLS 1.0-Protokolls mithilfe dieser Einstellung unterstützt das Speichersystem nur die SSL-Kommunikation mittels der TLS 1.1- und TLS 1.2-Protokolle und TLS 1.0 wird nicht als gültiges Protokoll erachtet.

Hinweis

Die Deaktivierung von TLS 1.0 kann sich auf vorhandene Clientanwendungen auswirken, die mit den TLS 1.1- oder TLS 1.2-Protokollen nicht kompatibel sind. In diesem Fall sollte die Unterstützung für TLS 1.0 aktiviert bleiben. Die folgenden Funktionen können nicht verwendet werden, wenn TLS 1.0 deaktiviert ist:

- Technische Ratgeber
- Benachrichtigungen zu Aktualisierungen von Software, Laufwerksfirmware und Sprachpaketen
- Replikation von OE-Versionen vor 4.3 auf OE-Version 4.3

Managen von TLS 1.0 auf dem Speichersystem

Nur der Administrator oder der Sicherheitsadministrator hat die Rechte zum Managen der Einstellung für die Aktivierung von TLS 1.0. Verwenden Sie den folgenden Befehl, um die Einstellung für die Aktivierung von TLS 1.0 auf einem Speichersystem festzulegen:

`uemcli /sys/security set -tls1Enabled yes` aktiviert die Verwendung des TLS 1.0-Protokolls.

`uemcli /sys/security set -tls1Enabled no` deaktiviert die Verwendung des TLS 1.0-Protokolls.

Weitere Informationen über diesen Befehl finden Sie im *Unisphere CLI-Benutzerhandbuch*.

Managementsupport für eingeschränkten Shell-Modus (rbash)

Die SSH-Serviceschnittstelle des Speichersystems wird mit dem eingeschränktem Shell-Modus (rbash) verstärkt. Diese Funktion ist für das Servicekonto beim Upgrade auf Unity OE Version 4.5 oder höher standardmäßig aktiviert. Obwohl es möglich ist, den eingeschränkten Shell-Modus vorübergehend zu deaktivieren, geschieht das nicht dauerhaft und er wird automatisch wieder aktiviert, wenn eines der folgenden Ereignisse eintritt:

- Der primäre Serviceprozessor wird neu gestartet.
- 24 Stunden vergehen, seit der eingeschränkte Shell-Modus deaktiviert wurde.

Diese Funktion erhöht den Sicherheitsstatus des Unity-Speichersystems, indem sie die Nutzer des Servicekontos auf die folgenden Funktionen beschränkt:

- Es kann nur ein begrenzter Satz von Befehlen ausgeführt werden, die einem Mitglied eines nicht privilegierten Linux-Nutzerkontos im eingeschränkten Shell-Modus zugewiesen sind. Das Servicenutzerkonto hat keinen Zugriff auf proprietäre Systemdateien, Konfigurationsdateien, Nutzer- oder Kundendaten.
- Servicenutzer können keinen Code ausführen, der nicht vertrauenswürdig ist und potenziell dazu genutzt werden könnte, lokale Schwachstellen bei der Berechtigungseskalation auszunutzen.

Neben den Serviceskripten enthält eine Whitelist grundlegende Befehle, die dem Servicepersonal zur Verfügung stehen. Dies sind die sicheren Befehle oder die Befehle mit Sicherheitskontrolle, aus denen Nutzer den eingeschränkten Shell-Modus nicht verlassen können. Diese Befehle sind für das Dell EMC-Servicepersonal unerlässlich, um Wartungsarbeiten durchzuführen, ohne das Recht auf root zu erhöhen. Informationen zu diesen Befehlen finden Sie im Artikel 528422 in der Wissensdatenbank.

HINWEIS

Eine Überprüfung auf Schwachstellen im Netzwerk kann nicht mit standardmäßig eingeschränkter Shell durchgeführt werden. Unisphere-Administratornutzer müssen den eingeschränkten Shell-Modus deaktivieren, um einen Sicherheitsscan zu ermöglichen. Für maximale Systemsicherheit wird dringend empfohlen, den eingeschränkten Shell-Modus jederzeit aktiviert zu lassen, es sei denn, es ist für die Durchführung einer Sicherheitsüberprüfung erforderlich. Um sicherzustellen, dass das System nicht lokalen Schwachstellen bei der Berechtigungseskalation ausgesetzt ist, aktivieren Sie den eingeschränkten Shell-Modus, sobald der Sicherheitsscan abgeschlossen ist.

Managen des eingeschränkten Shell-Modus auf dem Speichersystem

Nur der Administrator hat die Rechte, um die eingeschränkte Shell-Modus-Einstellung zu managen. Verwenden Sie den folgenden CLI-Befehl, um die Einstellung für den eingeschränkten Shell-Modus auf einem Speichersystem festzulegen:

`uemcli /sys/security set -rbashEnabled yes` aktiviert den eingeschränkten Shell-Modus für den Servicenutzermodus.

`uemcli /sys/security set -rbashEnabled no` deaktiviert den eingeschränkten Shell-Modus.

Verwenden Sie den folgenden CLI-Befehl, um den derzeitigen eingeschränkten Shell- für das Speichersystem festzulegen:

```
uemcli /sys/security show
```

KAPITEL 5

Datensicherheitseinstellungen

In diesem Kapitel werden die im Speichersystem für unterstützte Speichertypen verfügbaren Sicherheitsfunktionen beschrieben.

Folgende Themen werden behandelt:

Informationen über Data-at-Rest-Verschlüsselung (nur physische Bereitstellungen)

Data-at-Rest-Verschlüsselung (D@RE) wird über die controllerbasierte Verschlüsselung (Controller-Based Encryption, CBE) auf der physischen Laufwerksebene bereitgestellt. Diese Funktion soll dafür sorgen, dass alle Kundendaten und personenbezogenen Daten mit starker Verschlüsselung verschlüsselt werden, primär um Sicherheit bei Verlust eines Laufwerks zu ermöglichen.

Ein eindeutiger DEK (Data Encryption Key) wird für jedes Laufwerk erstellt und verwendet, um Daten zu verschlüsseln, während sie an das Laufwerk gesendet werden. Der DEK wird zur Ver-/Entschlüsselung von Benutzerdaten verwendet, mithilfe eines 256-Bit-AES-Algorithmus (Advanced Encryption Standard) mit dem Betriebsmodus XOR Encrypt XOR Tweakable Block Cipher mit Ciphertext Stealing (XTS).

Bei dem KEK (Key Encryption Key) handelt es sich um einen von RSA BSAFE erstellten, zufällig generierten 256-Bit-Schlüssel, der verwendet wird, um die DEKs zum Zeitpunkt der DEK-Erzeugung zu verpacken, damit die DEKs geschützt und gesichert sind, während sie sich durch das Speichersystem bewegen. Der für das Ver- und Entpacken der DEKs mithilfe des KEK verwendete Algorithmus ist ein 256-Bit-AES-Key-Wrap-Algorithmus, wie in RFC 3394 angegeben.

Bei dem KWK (Key Encryption Key Wrapping Key) handelt es sich um einen von RSA BSAFE erstellten, zufällig generierten 256-Bit-Schlüssel, der verwendet wird, um den KEK zum Zeitpunkt der Erzeugung zu verpacken, damit der KEK geschützt und gesichert ist, während er sich durch das Array und zum SAS (Serial Attached SCSI)-Controller bewegt. Der für das Ver- und Entpacken des KEK mithilfe des KWK verwendete Algorithmus ist ein 256-Bit-AES-Key-Wrap-Algorithmus, wie in RFC 3394 angegeben.

Unabhängig von CBE wird Systemspeicherplatz auf den Speicherprozessoren (SPs) mithilfe einer in der Linux-Distribution nativen Verschlüsselungsfunktion (dm_crypt) verschlüsselt. Bestimmte Partitionen auf dem Systemlaufwerk werden standardmäßig verschlüsselt, es sei denn, die Verschlüsselung ist zum Fertigungszeitpunkt nicht auf dem System aktiviert. Bei den Systempartitionen, die nicht verschlüsselt sind, könnten unverschlüsselte Daten wie Diagnosespeicherauszüge vorhanden sein. Wenn Diagnosematerial auf die Systempartition geschrieben wurde, können daraus außerdem einige wenige unverschlüsselte Benutzerdaten resultieren. Alle unter Verwendung von regulären I/O-Protokollen (iSCSI, FC) in das Array geschriebenen Daten sind verschlüsselt. Alles, was über den Kontrollpfad in das Array gelangt, wird von dieser Lösung nicht verschlüsselt. Sensible Informationen (z. B. Passwörter) werden jedoch über einen anderen Mechanismus verschlüsselt (wie auf nicht verschlüsselnden Arrays).

Eine als Key Manager bezeichnete Komponente ist für das Erzeugen, Speichern und sonstige Managen der Chiffrierschlüssel für das System verantwortlich. Der Keystore, der erzeugt wird, um die Chiffrierschlüssel zu speichern, befindet sich auf einer gemanagten LUN im privaten Speicherplatz auf dem System. Schlüssel werden in Reaktion auf Benachrichtigungen, dass ein Speicherpool hinzugefügt oder entfernt wurde, erzeugt oder gelöscht. Wichtige Backups werden automatisch vom System durchgeführt. Darüber hinaus werden durch Änderungen an der Konfiguration des Systems, die zu Änderungen an dem Keystore führen, informative Warnmeldungen erzeugt, die wichtige Backups empfehlen. Wenn es zu einem Vorgang kommt, der zu

einer Änderung des Keystore führt, wird eine Warnmeldung angezeigt und bleibt bestehen.

Es wird eine separate Auditingfunktion für allgemeine wichtige Vorgänge zur Verfügung gestellt, die alle wichtigen Einrichtungs-, Löschungs-, Backup- und Wiederherstellungsänderungen sowie das Hinzufügen von SLIC nachverfolgt.

Zusätzliche Informationen über die Funktion für Data-at-Rest-Verschlüsselung finden Sie im *Unity: Whitepaper Data at Rest Encryption*.

Funktionsaktivierung
D@RE ist eine lizenzierte Funktion. Die Lizenz muss bei der Erstkonfiguration des Systems installiert werden. Nach der Aktivierung kann der Verschlüsselungsvorgang nicht zurückgesetzt werden.

Im Rahmen der Verschlüsselung werden Datenchiffrierschlüssel erstellt und alle Benutzerdaten werden verschlüsselt. Die Chiffrierschlüssel werden in einer Keystore-Datei gespeichert. Die Keystore-Datei, die erzeugt wird, befindet sich auf einer gemanagten LUN im privaten Speicherplatz auf dem System.

Es wird dringend empfohlen, ein Backup der erzeugten Keystore-Datei an einem anderen Speicherort außerhalb des Systems zu erstellen, wo der Keystore sicher und geheim aufbewahrt werden kann. Sollte der Keystore auf dem System beschädigt werden, funktioniert das System nicht mehr. Das System geht in den Servicemodus über und es wird nur das Betriebssystem gestartet. In diesem Status wird bei dem Versuch, über Unisphere auf das System zuzugreifen, ein Fehler ausgegeben, dass der Keystore nicht zugänglich ist. In diesem Fall sind zur Behebung die Backup-Keystore-Datei und ein Serviceprojekt erforderlich.

Verschlüsselungsstatus

Der folgende D@RE-Funktionsstatus kann entweder über Unisphere oder einen CLI-Befehl angezeigt werden:

- Verschlüsselungsmodus: verwendete Art der Verschlüsselung, beispielsweise Controller-basierte Verschlüsselung.
- Verschlüsselungsstatus: basierend auf dem tatsächlichen Verschlüsselungsstatus:
  - Nicht unterstützt: Die Verschlüsselung des Systemspeicherplatzes auf den Speicherprozessoren ist deaktiviert.
  - Nicht lizenziert: Die Data-at-Rest-Verschlüsselungslizenz wurde nicht auf dem System installiert.
  - Verschlüsselt: Die Verschlüsselung ist abgeschlossen.
  - Wird nicht verschlüsselt: CBE ist deaktiviert.
  - Scrubbing – Prozess, bei dem zufällig ausgewählte Daten in unbelegten Speicherplatz auf Laufwerken geschrieben werden oder bei dem Nullen auf ungebundene Laufwerke geschrieben werden, um Restdaten aus früherer Verwendung zu löschen.

    Hinweis

    Bei SAS-Flash-2-Laufwerken wird statt Zeroing das Aufheben der Zuordnung für das Scrubbing von Laufwerken verwendet. Weitere Informationen über Data-at-Rest-Verschlüsselung und den Schrubbing-Prozess finden Sie im Whitepaper *EMC Unity: Data-at-Rest-Verschlüsselung* auf Online Support (https://support.emc.com).

  - Wird verschlüsselt: Die Verschlüsselung wird durchgeführt.

- KMIP-Status, ob KMIP aktiviert oder deaktiviert ist.

Um den Status der D@RE-Funktion in Unisphere anzuzeigen, wählen Sie **Einstellungen** > **Management** > **Verschlüsselung** aus. Der Status der Verschlüsselung wird unter **Verschlüsselung managen** angezeigt.

Hinweis

Verwenden Sie alternativ den CLI-Befehl `uemcli -u <username> -p <password> /prot/encrypt show -detail` zum Anzeigen des Status der Funktion (Verschlüsselungsmodus, Verschlüsselungsstatus, Prozent verschlüsselt, Backup-Keystore-Status und KMIP-Status). Sie können diesen CLI-Befehl auch verwenden, um den Status des Keystore anzuzeigen und zu ermitteln, ob Benutzervorgänge erforderlich sind. Detaillierte Informationen über diese CLI-Befehle finden Sie im *Unisphere Command Line Interface Guide*.

Externes Key-Management

Support für externes Key-Management erfolgt durch die Verwendung des KMIP (Key Management Interoperability Protocol). KMIP definiert die Funktionsweise eines Clients mit einem externen Key-Manager.

Hinweis

Das externe Key-Management wird nur mit Key-Management-Servern unterstützt, die das von OASIS entwickelte KMIP-Protokoll implementiert haben. Wenn ein Gemalto KeySecure KMIP-Server verwendet wird, erfordert der Key-Manager auf dem Speichersystem die Konfiguration des Benutzernamens und des Passworts auf dem Server.

Das Aktivieren und Konfigurieren der Unterstützung für KMIP auf dem Speichersystem ist abhängig davon, ob auf dem Speichersystem Verschlüsselung aktiviert ist. Wenn Verschlüsselung und KMIP aktiviert sind, wird der Zündschlüssel aus dem Speichersystem zu einem externen Key-Manager migriert und die lokale Kopie wird gelöscht. Außerdem wird der alte Speicherort der lokal gespeicherten Schlüssel neu programmiert und kann nicht geöffnet werden, sobald die Schlüssel migriert wurden. Es wird empfohlen, ein neues Backup der Keystore-Datei zu erzeugen.

Eine Benutzerrolle als Administrator oder Sicherheitsadministrator ist erforderlich, um externes Key-Management zu konfigurieren. Wählen Sie, um ein externes Key-Management zu konfigurieren, **Einstellungen** > **Management** > **Verschlüsselung** aus und wählen Sie unter **Verschlüsselung managen** > **Externes Key-Management** die Option **Konfigurieren** aus. Geben Sie die erforderlichen Informationen im Dialogfeld ein, das angezeigt wird, um die Eigenschaften des Key-Management-Servers zu konfigurieren und den KMIP-Server dem KMIP-Server-Cluster hinzuzufügen. Das Dialogfeld bietet außerdem die Möglichkeit, die relevanten Zertifikate von Zertifizierungsstelle und Client zu importieren und zu managen und die Konfiguration zu überprüfen. Die Konfiguration erfordert zwei Zertifikate:

- Zertifikat der Zertifizierungsstelle im PEM-Format
- Eine passwortgeschützte PKCS #12-Datei, die das Clientzertifikat enthält

Eine Kopie der Konfiguration für den KMIP-Server, einschließlich der Zertifikate und Konfigurationsdaten des Servers, wird lokal an sicheren Standorten auf dem Speichersystem sowie auf Back-End-Systemlaufwerken gespeichert, um Redundanz zu ermöglichen.

Hinweis

Informationen zu Kompatibilität und Interoperabilität in Bezug auf KMIP-Server finden Sie in der Simple Support Matrix für das Speichersystem auf der Supportwebsite.

Zertifikate werden auf den aktiven SP heruntergeladen. Zur Startzeit stellt das System, immer wenn ein Problem mit Zertifikaten gemeldet wird, die Zertifikate von der lokalen Kopie der Lockbox wieder her und versucht es erneut. Wenn es erneut fehlschlägt, wechselt das System in den Servicemodus. Wenn ein Unterschied gefunden wird, wird der Inhalt der Lockbox im Back-end aktualisiert.

Hinweis

Verwenden Sie alternativ den CLI-Befehl `uemcli -u<username> -p<password> /prot/encrypt/kmip -set -username <value> {-passwd <value> | -passwdSecure} -port <value> [-timeout <value>] -server <value>`, um KMIP zu konfigurieren. Verwenden Sie den CLI-Befehl `uemcli -u<username> -p<password> /sys/cert [ -type { CA | Server | Client | TrustedPeer } ] [ -service {Mgmt_LDAP | Mgmt_KMIP | VASA_HTTP } [ -scope <value> ] ] [ -id <value> ]`, um Zertifikate von Zertifizierungsstelle und Client zu importieren. Verwenden Sie den CLI-Befehl `uemcli -u<username> -p<password> /prot/encrypt/kmip -verify`, um die Konfiguration zu überprüfen. Detaillierte Informationen über diese CLI-Befehle finden Sie im *Unisphere Command Line Interface Guide*.

Im Falle eines Problems mit oder einer unerwarteten Änderung an der KMIP-Konfiguration oder dem Status kann das System die richtige Konfiguration oder den Status nicht verifizieren und startet im Servicemodus. Das System kann nicht in den Normalmodus zurückkehren, bis das Problem gelöst ist. Ein Serviceskript, `svc_kmip`, kann verwendet werden, um die richtige KMIP-Serverkonfiguration und bei Bedarf die Unity-Zertifikate wiederherzustellen, damit das System in den Normalmodus zurückkehren kann.

HINWEIS

Das Serviceskript, `svc_kmip`, dient nur zur Recovery und kann nicht verwendet werden, um die KMIP-Konfiguration einzurichten und sie auf einem neuen System zu aktivieren. Weitere Informationen über dieses Serviceskript finden Sie unter *Technische Hinweise zu Servicebefehlen*.

Sichern der Keystore-Datei

Durch Änderungen an der Konfiguration des Systems, die zu Änderungen am Keystore führen, werden Informationswarnmeldungen erzeugt, die dauerhaft angezeigt werden und Schlüsselbackups empfehlen. Eine neue Warnmeldung wird erzeugt, nachdem der Keystore für ein Backup vom System abgerufen wurde.

Hinweis

Es wird dringend empfohlen, ein Backup der erzeugten Keystore-Datei an einem anderen Speicherort außerhalb des Systems zu erstellen, wo der Keystore sicher und geheim aufbewahrt werden kann. Wenn die Keystore-Dateien auf dem System beschädigt und nicht mehr zugänglich sind, wird das System in den Servicemodus versetzt. In diesem Fall sind zur Behebung die Backup-Keystore-Datei und ein Serviceprojekt erforderlich.

Zum Sichern der Keystore-Datei ist die Benutzerrolle Administrator oder Sicherheitsadministrator erforderlich. Wählen Sie zum Sichern der Keystore-Datei an einem Speicherort außerhalb des Systems, an dem der Keystore sicher und geheim aufbewahrt werden kann, **Einstellungen** > **Management** > **Verschlüsselung** aus und wählen Sie unter **Verschlüsselung verwalten** > **Keystore** die Option **Keystore-Datei sichern** aus. Das angezeigte Dialogfeld führt Sie durch die Schritte für das Backup der erzeugten Keystore-Datei.

Hinweis

Verwenden Sie alternativ den CLI-Befehl `uemcli -u<username> -p<password> -download encryption -type backupKeys`, um die Keystore-Datei an einem Speicherort außerhalb des Systems zu sichern, an dem der Keystore sicher und geheim aufbewahrt werden kann. Detaillierte Informationen über diesen CLI-Befehl finden Sie im *Unisphere Command Line Interface Guide*.

Auditprotokollierung mit Data-at-Rest-Verschlüsselung

Die D@RE-Funktion bietet eine separate Auditingfunktion, die die Protokollierung der folgenden Keystore-Vorgänge unterstützt:

- Funktionsaktivierung
- Schlüsselerstellung
- Schlüssellöschung
- Keystore-Backup
- Abschluss der Festplattenverschlüsselung
- SLIC-Hinzufügung

Das Auditprotokoll für Keystore-Vorgänge wird im privaten Speicherplatz auf dem System gespeichert. Wählen Sie zum Herunterladen des vollständigen Auditprotokolls und der Prüfsummeninformationen oder der Informationen für ein bestimmtes Jahr und einen bestimmten Monat **Einstellungen** > **Management** > **Verschlüsselung** und dann unter **Verschlüsselung managen** > **Auditprotokoll** die Option **Auditprotokoll und Prüfsumme herunterladen** aus. Um eine neu erzeugte Prüfsummendatei für die Auditprotokolldatei herunterzuladen, die zu einem früheren Zeitpunkt abgerufen wurde, wählen Sie **Einstellungen** > **Management** > **Verschlüsselung** und dann unter**Verschlüsselung managen** > **Auditprotokoll** die Option **Prüfsumme herunterladen** aus. Der angegebene Dateiname muss exakt mit der Auditprotokolldatei übereinstimmen, die zuvor abgerufen wurde.

Hinweis

Verwenden Sie alternativ den CLI-Befehl `uemcli -u<username> -p<password> -download encryption -type auditLog -entries <all or YYYY-MM>`, um das vollständige Auditprotokoll und die Prüfsummeninformationen bzw. ein partielles Auditprotokoll herunterzuladen. Detaillierte Informationen über diesen CLI-Befehl finden Sie im *Unisphere Command Line Interface Guide*.

Hot-Spare-Vorgänge

Wenn ein System bereits mit DEKs für alle Festplattenlaufwerke im System konfiguriert ist, die bereitgestellten Pools angehören, werden Laufwerke, die aktuell keinem bereitgestellten Pool zugeordnet sind, als ungebundene Laufwerke angesehen. Das Entfernen ungebundener Laufwerke oder das Auftreten eines Defekts bei ungebundenen Laufwerken hat keine Auswirkung auf den Keystore und macht daher

kein Backup der Keystore-Datei erforderlich. Ebenso hat das Austauschen eines ungebundenen Laufwerks keine Auswirkung auf den Keystore und macht daher kein Backup der Keystore-Datei erforderlich.

Hinweis

Ungebundene Festplattenlaufwerke werden zum Entfernen bereits vorhandener Daten mit Standarddaten überschrieben.

Wenn ein System bereits mit DEKs für alle Laufwerke im System konfiguriert ist, die bereitgestellten Pools angehören, werden diese Laufwerke als gebundene Laufwerke angesehen. Wenn ein gebundenes Laufwerk entfernt wird oder bei dem Laufwerk ein Defekt auftritt und dieses nach einem Zeitraum von 5 Minuten durch ein permanentes Hot Spare ersetzt wird, wird für das Hot Spare ein DEK generiert und die Neuerstellung beginnt. Der DEK des entfernten Laufwerks wird sofort aus dem Keystore entfernt. An diesem Punkt wird vom Key Manager ein geänderter Keystore-Status festgelegt und es wird eine Warnmeldung ausgelöst, dass der Keystore gesichert werden soll, da DEK-Änderungen am Keystore vorgenommen wurden.

Wenn das entfernte Festplattenlaufwerk an beliebiger Stelle wieder in das System eingesetzt wird, bevor die 5 Minuten abgelaufen sind, ist keine Neuerstellung erforderlich und es werden keine Änderungen am Keystore vorgenommen. Der DEK bleibt gleich, da der Schlüssel mit dem Festplattenlaufwerk und nicht mit dem Steckplatz verknüpft ist. Außerdem wird keine Warnmeldung über einen geänderten Keystore-Status erzeugt.

Hinweis

Wenn eine Bereinigung oder Zerstörung des entfernten Laufwerks erforderlich ist, sollte dies unabhängig erfolgen.

Hinzufügen eines Festplattenlaufwerks zu einem Speichersystem mit aktivierter Verschlüsselung

Das Installieren einer oder mehrerer neuer Festplatten in das System löst keine Erzeugung eines neuen DEK für jede Festplatte aus. Dieser Vorgang wird nicht für ein neues Laufwerk auftreten, bis die Festplatte in einem Pool bereitgestellt wird. An diesem Punkt wird vom Key Manager ein geänderter Keystore-Status festgelegt und es wird eine Warnmeldung ausgelöst, dass der Keystore gesichert werden soll, da DEK-Änderungen am Keystore vorgenommen wurden.

Wenn Sie einem Speichersystem ein neues Festplattenlaufwerk hinzufügen, wird das Laufwerk als ungebunden angesehen. Ungebundene Festplattenlaufwerke werden mit Standarddaten überschrieben, um bereits vorhandene Daten zu entfernen. Nur der adressierbare Speicherplatz des Laufwerks wird überschrieben. Alle restlichen Klartextdaten, die sich in verborgenen Positionen auf dem Laufwerk befinden, werden nicht überschrieben.

HINWEIS

Falls ein potenzieller Zugriff auf Datenreste aus der vorherigen Nutzung eines Laufwerks gegen die Sicherheitsrichtlinien verstößt, müssen Sie das Laufwerk gesondert bereinigen, bevor es in das Speichersystem mit aktivierter Verschlüsselung eingesetzt wird.

Entfernen eines Festplattenlaufwerks aus einem Speichersystem mit aktivierter Verschlüsselung

Wenn ein System bereits mit DEKs für alle Laufwerke im System konfiguriert ist, die bereitgestellten Pools angehören, werden diese Laufwerke als gebundene Laufwerke angesehen. Wenn ein gebundenes Laufwerk entfernt und nach Ablauf von fünf Minuten nicht ersetzt wird, wird der DEK für das Laufwerk nicht aus dem Keystore entfernt. Der Schlüssel bleibt gültig, bis der bereitgestellte Pool gelöscht oder ein neues Laufwerk eingesetzt wird. Wenn das entfernte Festplattenlaufwerk an beliebiger Stelle wieder in das System eingesetzt wird, bevor die 5 Minuten abgelaufen sind, ist anders als bei einem Ersatzlaufwerk keine Neuerstellung erforderlich und es werden keine Änderungen am Keystore vorgenommen. Der DEK bleibt gleich, da der Schlüssel mit dem Festplattenlaufwerk und nicht mit dem Steckplatz verknüpft ist. Außerdem wird keine Warnmeldung über einen geänderten Keystore-Status erzeugt.

Hinweis

Wenn eine Bereinigung oder Zerstörung des entfernten Laufwerks erforderlich ist, sollte dies unabhängig erfolgen.

Ersetzen von Gehäuse und Speicherprozessoren bei einem Speichersystem mit aktivierter Verschlüsselung

Der generierte Keystore steht in Verbindung mit der Hardware im Speichersystem. Zum Ersetzen von Gehäuse und SPs aus einem Speichersystem mit aktivierter Verschlüsselung ist ein Serviceprojekt erforderlich.

Datensicherheitseinstellungen

Tabelle 16 auf Seite 76 zeigt die Sicherheitsfunktionen, die für unterstützte Speichersystem-Speichertypen verfügbar sind.

Tabelle 16 Sicherheitsfunktionen

Speichertyp	Port	Protokoll	Sicherheitseinstellungen
iSCSI-Speicher	3260	TCP	• Die Zugriffskontrolle auf der Ebene des iSCSI-Hosts (Initiatoren) ist über Unisphere verfügbar. (Clients können auf primären Speicher, Snapshots oder beides zugreifen.) • Die CHAP-Authentifizierung wird unterstützt, damit Speichersystem-iSCSI-Server (Ziele) iSCSI-Hosts (Initiators) authentifizieren können, die versuchen, auf iSCSI-basierten Speicher zuzugreifen. • Die gegenseitige CHAP-Authentifizierung wird unterstützt, damit iSCSI-Hosts (Initiatoren) Speichersystem-iSCSI-Server authentifizieren können.
SMB-Speicher	445	TCP, UDP	• Die Authentifizierung für Domänen- und Administrationsmaßnahmen wird über Active Directory-Benutzer- und Gruppenkonten bereitgestellt.

Tabelle 16 Sicherheitsfunktionen (Fortsetzung)

Speichertyp	Port	Protokoll	Sicherheitseinstellungen
			• Datei- und Freigabezugriffskontrollen werden über Windows-Verzeichnisdienste bereitgestellt. Die Zugriffskontrollliste (ACL) für die SMB-Share kann auch über eine SMI-S-Schnittstelle konfiguriert werden. • Sicherheitssignaturen werden über SMB-Signaturen unterstützt. • Die SMB-Verschlüsselung wird für SMB-fähige Hosts über SMB 3.0 und Windows 2012 bereitgestellt. • Optionale File-Level Retention-Services werden über Add-On-Software unterstützt.
NFS-Speicher	2049	TCP	• Die freigabebasierte Zugriffskontrolle wird über Unisphere bereitgestellt. • Dieser Speicher bietet Unterstützung für NFS-Authentifizierungs- und Zugriffskontrollmethoden in NFS-Version 3 und 4. • Optionale File-Level Retention-Services werden über Add-On-Software unterstützt.
KDC	88		• Key Distribution Center. Kerberos-Server, der Kerberos-Tickets für die Verbindung mit Kerberos-Services bereitstellt.
Backup und Wiederherstellung			• NDMP-Sicherheit kann basierend auf freigegebenen NDMP-Schlüsseln implementiert werden.

KAPITEL 6

Sicherheitswartung

In diesem Kapitel werden verschiedene in das Speichersystem implementierte Sicherheitswartungsfunktionen beschrieben.

Folgende Themen werden behandelt:

Sichere Wartung

Das Speichersystem bietet folgende sichere Funktionen für die Durchführung der Remotesystemwartung und des Remotesystemupdates:

- Lizenzaktivierung
- Softwareupgrade
- Software-Hotfixes

Lizenzupdate

Über die Funktion für Lizenzupdates können Benutzer Lizenzen für spezielle Speichersystemfunktionen abrufen und installieren. In Tabelle 17 auf Seite 80 sind die Sicherheitsfunktionen der Lizenzupdatefunktion aufgeführt.

Tabelle 17 Sicherheitsfunktionen des Lizenzupdates

Prozess	Sicherheit
Erwerb von Lizenzen auf der EMC Online-Support-Website	Der Lizenzerwerb erfolgt in einer authentifizierten Sitzung auf der EMC Online Support-Website.
Erhalt der Lizenzdateien	Lizenzen werden an die E-Mail-Adresse gesendet, die in einer authentifizierten Transaktion der EMC Online Support-Website angegeben ist.
Hochladen und Installieren von Lizenzen über den Unisphere-Client auf dem Speichersystem	• Lizenzdateien werden über HTTPS-authentifizierte Unisphere-Sitzungen in das Speichersystem hochgeladen. • Das Speichersystem validiert eingehende Lizenzdateien mit digitalen Signaturen. Jede lizenzierte Funktion wird über eine eindeutige Signatur in der Lizenzdatei validiert.

Softwareupgrade

Über die Speichersystemsoftware erhalten Benutzer die Software für Upgrades oder Aktualisierungen der auf dem Speichersystem ausgeführten Software. In Tabelle 18 auf Seite 80 sind die Sicherheitsfunktionen der Speichersystem-Softwareupgradefunktion aufgeführt.

Tabelle 18 Sicherheitsfunktionen für das Softwareupgrade

Prozess	Beschreibung
Herunterladen der Speichersystemsoftware von der EMC Online Support-Website	Der Lizenzerwerb erfolgt in einer authentifizierten Sitzung auf der EMC Online Support-Website.

Tabelle 18 Sicherheitsfunktionen für das Softwareupgrade (Fortsetzung)

Prozess	Beschreibung
Hochladen der Speichersystemsoftware	Die Software wird über eine HTTPS-authentifizierte Unisphere-Sitzung zum Speichersystem hochgeladen.

EMC Secure Remote Support für Ihr Speichersystem

Die ESRS-Funktion (EMC Secure Remote Support) gewährt Ihrem autorisierten EMC Serviceprovider über einen sicheren und verschlüsselten Tunnel Remotezugriff auf Ihr Speichersystem. Für den ausgehenden Zugriff muss das Management-IP-Netzwerk des Speichersystems HTTPS-Datenverkehr in beiden Richtungen zulassen. Über den sicheren Tunnel, den ESRS zwischen dem Speichersystemgerät und autorisierten Systemen im Netzwerk des Supportcenters einrichtet, können auch Dateien aus dem Speichersystem bzw. zurück in das Netzwerk des Supportcenters übertragen werden.

Zwei Remoteserviceoptionen sind verfügbar, mit denen Speichersysteminformationen zwecks Remote-Troubleshooting an den Supportcenter gesendet werden können:

- Centralized ESRS Virtual Edition (VE)
- Integrated ESRS (nur physische Bereitstellungen)

Centralized EMC Secure Remote Services

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 Servern des Supportcenters und einem arrayexternen ESRS Gateway. Das ESRS Gateway ist der einzige Eingangs- und Ausgangspunkt für alle IP-basierten ESRS-Aktivitäten für die Speichersysteme, 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 (optional) und den Proxyservern (optional) sowie dem Supportcenter. 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.

Weitere Informationen zu ESRS Gateway und Policy Manager finden Sie auf der EMC Secure Remote Services-Produktseite auf EMC Online Support (https://support.emc.com).

Intregrated EMC Secure Remote Services (nur physische Bereitstellungen)

Hinweis

Diese Funktion ist in Ihrer Implementierung möglicherweise nicht verfügbar.

Integrated ESRS wird direkt auf Ihrem Speichersystem ausgeführt. Wenn Sie diese Option auswählen, stellt Ihr Speichersystem eine sichere Verbindung zwischen dem Speichersystem und den Servern des Supportcenters her. Die integrierte Remoteserviceoption kann entweder als nur ausgehende Verbindung oder als ausgehende/eingehende Verbindung (dies ist die Standardeinstellung) konfiguriert

werden. Mit der Konfiguration für nur ausgehende Verbindungen werden die Funktionen der Remoteserviceverbindungen für die Remoteübertragung zum Supportcenter aus dem Speichersystem aktiviert. Mit der Konfiguration für ausgehende/eingehende Verbindungen werden die Funktionen der Remoteserviceverbindungen für die Remoteübertragung zum und vom Supportcenter mit dem Speichersystem aktiviert. Wenn die Konfigurationsoption für ausgehende/eingehende Verbindungen ausgewählt ist, muss die Verbindung zwischen dem Speichersystem und einem optionalen Policy Manager sowie allen zugehörigen Proxyservern entweder über Unisphere oder über die Befehlszeilenoberfläche konfiguriert werden.

KAPITEL 7

Einstellungen für Sicherheitswarnmeldungen

In diesem Kapitel werden die verschiedenen Methoden beschrieben, die verfügbar sind, um Administratoren über die im Speichersystem auftretenden Warnmeldungen zu benachrichtigen.

Folgende Themen werden behandelt:

Warnmeldungseinstellungen

Speichersystem-Warnmeldungen informieren Administratoren über Ereignisse im Speichersystem, wenn Maßnahmen ergriffen werden müssen. Speichersystemereignisse können wie in Tabelle 19 auf Seite 84 gezeigt gemeldet werden.

Tabelle 19 Warnmeldungseinstellungen

Warnmeldungstyp	Beschreibung
Visuelle Benachrichtigung	Zeigt informative Pop-up-Meldungen in Echtzeit an, wenn Benutzer sich bei der Oberfläche anmelden, um anzugeben, wann Warnmeldungsbedingungen eintreten. Pop-ups stellen grundlegende Informationen zu Warnmeldungsbedingungen bereit. Weitere Informationen finden Sie unter **Einstellungen** > **Warnmeldungen** > **E-Mail-Warnmeldungen und SMTP-Konfiguration festlegen**. **Hinweis** Visuelle Speichersystem-Warnmeldungsbenachrichtigungen sind nicht konfigurierbar. Darüber hinaus verfügt das Speichersystem nicht über die Option für die Authentifizierung bei einem SMTP-Mailserver. Wenn Ihr Mailserver erfordert, dass alle Clients sich authentifizieren, um E-Mails zu übermitteln, kann das Speichersystem keine E-Mail-Warnmeldungen über diesen Mailserver senden.
EMail-Benachrichtigung	Ermöglicht Ihnen die Angabe einer oder mehrerer E-Mail-Adressen, an die Warnmeldungen gesendet werden sollen. Sie können folgende Einstellungen konfigurieren: • E-Mail-Adressen, an die Systemwarnmeldungen gesendet werden sollen • Schweregrad (kritisch, Fehler, Warnung, Hinweis oder Informationen), der für die E-Mail-Benachrichtigung erforderlich ist **Hinweis** Damit die Benachrichtigung über Speichersystem-Warnmeldungen per E-Mail funktioniert, muss ein SMTP-Zielserver für das Speichersystem konfiguriert werden.
SNMP-Traps	Sie übertragen Warnmeldungsinformationen an angegebene Hosts (Trap-Ziele), die als Repositories für Warnmeldungsinformationen des Speichernetzwerksystems fungieren. Sie können SNMP-Traps über Unisphere konfigurieren. Folgende Einstellungen stehen zur Verfügung: • IP-Adresse eines Netzwerk-SNMP-Trap-Ziels • Optionale Sicherheitseinstellungen für Trap-Datenübertragung ▪ Authentifizierungsprotokoll: Hashing-Algorithmus für SNMP-Traps (SHA oder MD5) ▪ Datenschutzprotokoll: Verschlüsselungsalgorithmus für SNMP-Traps (DES oder AES) ▪ Version: Version wird für SNMP-Traps (v2c oder v3) verwendet. ▪ Community: SNMP-Communityzeichenfolge (gilt nur für SNMP v2c-Ziele) Die Unisphere-Onlinehilfe bietet weitere Informationen.
EMC Secure Remote Support Services (ESRS)	ESRS (EMC Secure Remote Support Services) bietet eine IP-basierte Verbindung, über die der EMC Support Fehlerdateien und Warnmeldungen von Ihrem Speichersystem erhält und ein Remote-Troubleshooting durchführen kann, wodurch eine schnelle und effiziente Behebung möglich ist.

Tabelle 19 Warnmeldungseinstellungen (Fortsetzung)

Warnmeldungstyp	Beschreibung
	Hinweis Verfügbar in OE (Operating Environment, Betriebsumgebung) Version 4.0 oder höher. Damit ESRS funktioniert, muss es auf dem Speichersystem aktiviert werden.

Konfigurieren der Warnmeldungseinstellungen

Sie können Speichersystem-Warnmeldungseinstellungen für E-Mail-Benachrichtigungen und SNMP-Traps über das Speichersystem konfigurieren.

Konfigurieren der Warnmeldungseinstellungen für E-Mail-Benachrichtigungen

Unisphere:

Vorgehensweise

1. Wählen Sie **Einstellungen** > **Warnmeldungen** > **E-Mail und SMTP** aus.
2. Konfigurieren Sie im Bereich **E-Mail-Warnmeldungen und SMTP-Konfiguration festlegen** unter **E-Mail-Warnmeldungen an folgende E-Mail-Liste senden** die E-Mail-Adressen, an die die Warnmeldungsbenachrichtigungen gesendet werden sollen.
3. Konfigurieren Sie unter **Sicherheitsebene der zu sendenden Warnmeldungen:** einen der folgenden Werte für den Schweregrad, bei dem E-Mail-Warnmeldungen generiert werden:
   - Kritisch
   - Fehler und darüber
   - Warnung und darüber
   - Hinweis und darüber
   - Information und darüber

   Hinweis

   Damit der Speichersystem-Warnmeldungsmechanismus per E-Mail funktioniert, muss ein Ziel-SMTP-Server für das Speichersystem konfiguriert werden.
4. Konfigurieren Sie unter **SMTP-Netzwerkeinstellungen festlegen:** den-SMTP-Zielserver.

Konfigurieren von Warnmeldungseinstellungen für SNMP-Traps

Unisphere:

Vorgehensweise

1. Wählen Sie **Einstellungen** > **Warnmeldungen** > **SNMP** aus.

2. Konfigurieren Sie im Bereich **SNMP-Warnmeldungen managen** unter **Warnmeldungen über SNMP-Traps an diese Ziele senden:** die folgenden Informationen für die SNMP-Trap-Ziele:
   - Netzwerkname oder IP-Adresse
   - Zu verwendendes Authentifizierungsprotokoll
   - Zu verwendendes Datenschutzprotokoll
   - Zu verwendende SNMP-Version
   - Communityzeichenfolge (gilt nur für SNMP v2c-Ziele)
3. Konfigurieren Sie unter **Sicherheitsebene der zu sendenden Warnmeldungen:** einen der folgenden Werte für den Schweregrad, bei dem SNMP-Traps erzeugt werden:
   - Kritisch
   - Fehler und darüber
   - Warnungen und darüber
   - Hinweis und darüber
   - Information und darüber

KAPITEL 8

Weitere Sicherheitseinstellungen

Dieses Kapitel enthält weitere Informationen, die für einen sicheren Betrieb des Speichersystems relevant sind.

Folgende Themen werden behandelt:

Informationen über STIG

Ein Security Technical Implementation Guide (STIG) definiert einen Konfigurations- und Wartungsstandard für Computerbereitstellungen, der vom Informationssicherheitsprogramm des US Department of Defense (DoD) vorgeschrieben wird. Diese Richtlinien dienen zur Verbesserung der Sicherheitseinstellungen und Konfigurationsoptionen, bevor die Systeme mit einem Netzwerk verbunden werden. Weitere Informationen zu den verschiedenen STIGs finden Sie auf der Website http://iase.disa.mil/stigs/index.html.

Einige der Schritte für die Sicherheitsverstärkung zum Erfüllen der STIG-Anforderungen werden durch Ausführen der Serviceskripte aktiviert. Mit dem Servicebefehl `svc_stig` werden der STIG-Modus auf einem Unity-System (nur physische Bereitstellungen) aktiviert oder deaktiviert und der Status des STIG-Modus angegeben. Dieser Servicebefehl bietet eine einfache und automatisierte Methode zum Anwenden dieser Änderungen. Diese Änderungen können auch zu einem späteren Zeitpunkt rückgängig gemacht werden, wenn dies erforderlich sein sollte (z. B. zum Troubleshooting eines Betriebsproblems).

Hinweis

Obwohl die an den Konfigurations- und Managementoptionen vorgenommenen Änderungen, die vom STIG-Modus implementiert werden, rückgängig gemacht werden können, werden nicht alle zugehörigen Einstellungen auf ihre Standardwerte zurückgesetzt. Einige Einstellungen, z. B. Berechtigungs- und Rechteänderungen an Dateisystemen auf OE-Ebene, werden beibehalten.

Das Speichersystem behält den STIG-Modus bei, auch während eines Softwareupgrades.

Managen des STIG-Modus (nur physische Bereitstellungen)

Wenn der STIG-Modus über den Servicebefehl `svc_stig` aktiviert wird, wird der Status der jeweils angewendeten STIGs (Kategorie I oder Kategorie II oder beide) angezeigt. Sie können die angewendeten Kategorien jedoch mit `svc_stig -e` festlegen, ohne die Optionen anzugeben, mit denen standardmäßig STIGs sowohl der Kategorie I als auch der Kategorie II angewendet werden. Wenn CAT II aktiviert ist, werden auf der SSH-Serviceoberfläche des Speichersystems und in Unisphere ein DoD-Anmeldebanner für interaktive Sitzungen angezeigt.

Führen Sie zur Sicherheitsverstärkung Ihres Speichersystems diese drei Schritte nacheinander aus:

1. Aktivieren Sie den STIG-Modus. Mit diesem Prozess werden die Änderungen auf den passiven SP angewendet und dieser neu gestartet. Sobald der passive SP vollständig betriebsbereit ist, wird er zum aktiven SP. Die Änderungen werden dann auf den vorherigen aktiven SP angewendet und auf diesem SP wird ein Neustart ausgegeben.
2. Aktivieren Sie den FIPS 140-2-Modus. Dieser Prozess führt dazu, dass die SPs wieder neu gestartet werden. Weitere Informationen zum FIPS 140-2-Modus finden Sie unter Unterstützung des Managements für FIPS 140-2 auf Seite 65.
3. Aktivieren Sie die STIG-konformen Benutzerkontoeinstellungen. Weitere Informationen zu den STIG-konformen Benutzerkontoeinstellungen finden Sie unter Managen von Benutzerkontoeinstellungen im STIG-Modus (nur physische Bereitstellungen) auf Seite 90.

Zum Deaktivieren der Sicherheitsverstärkung Ihres Speichersystems führen Sie diese drei Schritte nacheinander aus:

1. Deaktivieren Sie die STIG-konformen Benutzerkontoeinstellungen.
2. Deaktivieren Sie den FIPS 140-2-Modus.
3. Deaktivieren Sie den STIG-Modus.

Anwendungsbeispiele

```
Usage: svc_stig [<qualifiers>] where the qualifiers are:

  -h|--help             : Display this message
  -d|--disable       [options] : Disable STIGs
  -e|--enable        [options] : Enable STIGs
  -s|--status        [options] : Get status for STIGs

This script enables, disables, and provides current status for each
catgory of STIGs.

See the help text below for more information on options.

Refer to the system documentation for a complete description of
STIGs
supported.

-d|--disable:
  Used to Disable all STIGs (no option specified).
  Options:

    -c|--cat [X]    : disable a specific category of STIGs

-e|--enable:
  Used to Enable all STIGs (no option specified).
  Options:

    -c|--cat [X]    : enable a specific category of STIGs

-s|--status:
  Used to show the current status (enabled or disabled) for all
STIGs
  (no option specified).
  Options:

    -c|--cat [X]    : show status for a specific Category of STIGs
    -b|--boolean-format : show boolean status for a specific
Category of STIGs
```

Beispiel 1 Aktivieren des STIG-Modus

```
12:51:21 service@OB-M1204-spb spb:~> svc_stig -e
################################################################################
###########
WARNING:
WARNING: This action will cause a reboot of the system!!
WARNING:
################################################################################
###########

################################################################################
###########
INFO:
INFO: Both Storage Processors will reboot in sequence, starting
with peer SP.
```

Beispiel 1 Aktivieren des STIG-Modus (Fortsetzung)

```
INFO: When primary SP comes back from reboot, the process will
automatically
INFO: restart to finish applying. Monitor status with 'svc_stig -
s'. If status
INFO: does not change to expected value within 30 minutes, contact
service
INFO: provider.
INFO:
################################################################
###########
Enter "yes" if want to proceed with this action:
```

Beispiel 2 Anzeigen des Status des STIG-Modus

```
13:25:15 service@OB-M1204-spa spa:~> svc_stig -s
STIG CATEGORY 1: ENABLED
STIG CATEGORY 2: ENABLED
```

Managen von Benutzerkontoeinstellungen im STIG-Modus (nur physische Bereitstellungen)

Ein Benutzer mit der Rolle eines Administrators oder Sicherheitsadministrators kann Einstellungen im Zusammenhang mit Benutzerkonten aktivieren, deaktivieren, anzeigen und konfigurieren. Die Einstellungen gelten für alle Benutzerkonten, sofern nicht anders angegeben. Wenn Benutzerkontoeinstellungen aktiviert sind, ohne einen bestimmten Wert für die jeweilige Einstellung anzugeben, wird automatisch der STIG-konforme Standardwert angewendet. Wenn Benutzerkontoeinstellungen deaktiviert sind, wird die jeweilige Einstellung auf ihren Wert vor Aktivierung der Funktion zurückgesetzt. Die folgenden Funktionen für Benutzerkontoeinstellungen gelten nur für Systeme, für die der STIG-Modus aktiviert ist:

- Anforderungen für zusätzliche Passwörter
- Anforderungen für fehlgeschlagene Anmeldungen
- Sperrdauer
- Timeout einer Sitzung im Leerlauf
- Aktivieren der Standardadministratorsperre

Im Folgenden ist eine Zusammenfassung der Beschränkungen für die Funktionen der Benutzerkontoeinstellungen angegeben:

- Die Funktion ist nur über die folgenden UEMCLI-Befehle verfügbar: `/user/account/settings set` und `/user/account/settings show`.
- Dieser Befehl kann nur von einem Benutzer mit der Rolle eines Administrators oder Sicherheitsadministrators ausgeführt werden.
- Das Passwort für das Standardadministratorkonto läuft nie ab.
- Der Befehl gibt einen Fehler zurück, wenn er bei deaktiviertem STIG-Modus verwendet wird.
- Diese Funktion muss nach Aktivierung des STIG-Modus separat aktiviert werden.

- Diese Funktion muss vor Deaktivierung des STIG-Modus separat deaktiviert werden.

Anforderungen für zusätzliche Passwörter

Anforderungen für zusätzliche Passwörter werden für die Benutzerkonten hinzugefügt, die nach Aktivierung des STIG-Modus erstellt oder geändert wurden:

- Mindestgröße des Passworts
- Anzahl der Passwörter
- Passwortdauer

Die Einstellung für die Mindestgröße des Passworts (`-passwdMinSize`) steht für die Mindestgröße, die Passwörter für lokale Benutzerkonten beim Erstellen eines Benutzerkontos oder beim Ändern eines Passworts haben müssen. Die Mindestgröße für das Passwort kann im Bereich von 8 bis 40 Zeichen konfiguriert werden. Wenn Benutzerkontoeinstellungen ohne Festlegung der Mindestgröße des Passworts aktiviert werden, beträgt der Standardwert 15 Zeichen. Wenn Benutzerkontoeinstellungen deaktiviert sind, ist die Mindestgröße des Passworts auf 8 Zeichen festgelegt. Jede Änderung an dieser Einstellung hat keinen Einfluss auf lokale Benutzerkonten, die vor der Änderung erstellt wurden, es sei denn, das Passwort wird geändert.

Die Einstellung für die Anzahl von Passwörtern (`-passwdCount`) steht für die Anzahl von Passwörtern, die für lokale Benutzerkonten nicht erneut verwendet werden können. Die Anzahl der Passwörter kann im Bereich von 3 bis 12 Passwörtern konfiguriert werden. Wenn Benutzerkontoeinstellungen ohne Festlegung der Passwortanzahl aktiviert werden, beträgt der Standardwert 5 Passwörter. Wenn Benutzerkontoeinstellungen deaktiviert sind, ist die Passwortanzahl auf 3 Passwörter festgelegt. Diese Einstellung wirkt sich auf alle bereits vorhandenen und neuen Benutzerkonten aus.

Die Einstellung für die Passwortdauer (`-passwdPeriod`) steht für den Zeitraum in Tagen, nach der das Passwort für lokale Benutzerkonten abläuft. Die Passwortdauer kann im Bereich von 1 bis 180 Tagen konfiguriert werden, wobei der Wert „-noPasswdPeriod“ bedeutet, dass ein Passwort nie abläuft. Wenn Benutzerkontoeinstellungen ohne Festlegung der Passwortdauer aktiviert werden, beträgt der Standardwert 60 Tage. Wenn Benutzerkontoeinstellungen deaktiviert sind, erfolgt für die Passwortdauer keine Angabe. Diese Einstellung wirkt sich auf alle bereits vorhandenen und neuen Benutzerkonten aus. Diese Einstellung gilt jedoch nicht für das Standard-Administratorbenutzerkonto, dessen Passwort nie abläuft.

Passwortablaufstatus

Ein Benutzer mit der Rolle eines Administrators oder Sicherheitsadministrators kann den Parameter des Passwortablaufstatus für alle lokalen Benutzerkonten anzeigen. Dieser Parameter kann nicht festgelegt werden. Er kann nur angezeigt werden, wenn die Option `-detail` im UEMCLI-Befehl `/user/account/settings show` angegeben ist.

Der Passwortablaufstatus für ein Benutzerkonto wird mit einem der folgenden Werte angezeigt:

- –: Wird angezeigt, wenn ein Passwort festgelegt ist, das nie abläuft, wenn das Benutzerkonto vom Typ „LDAP“ ist oder wenn die Benutzerkontoeinstellungen deaktiviert sind.
- Verbleibende Anzahl von Tagen: Wird angezeigt, wenn die Benutzerkontoeinstellungen aktiviert sind und die Passwortdauer auf einen Wert größer als 0 konfiguriert ist.
- Abgelaufen: Wird angezeigt, wenn das Passwort für das Benutzerkonto abgelaufen ist.

Anforderungen für fehlgeschlagene Anmeldungen
Nach Aktivierung des STIG-Modus werden die folgenden Anforderungen fehlgeschlagener Anmeldungen für lokale Benutzerkonten hinzugefügt:

- Maximale Anzahl fehlgeschlagener Anmeldungen
- Zeitraum fehlgeschlagener Anmeldungen

Die maximale Anzahl von aufeinanderfolgenden fehlgeschlagenen Anmeldungen, die für lokale Benutzerkonten zulässig ist, kann im Bereich von 1 bis 10 aufeinanderfolgende fehlgeschlagene Anmeldungen konfiguriert werden. Wenn Benutzerkontoeinstellungen ohne Festlegung der maximalen Anzahl fehlgeschlagener Anmeldungen aktiviert werden, beträgt der Standardwert 3 aufeinanderfolgende fehlgeschlagene Anmeldungen. Wenn Benutzerkontoeinstellungen deaktiviert sind, erfolgt für die maximale Anzahl von aufeinanderfolgenden fehlgeschlagenen Anmeldungen keine Angabe.

Hinweis

Die Einstellungen für den Zeitraum fehlgeschlagener Anmeldungen (`-failedLoginPeriod`) und die Sperrdauer (`-lockoutPeriod`) müssen mit einem Wert angegeben werden, wenn die Einstellung für die maximale Anzahl fehlgeschlagener Anmeldungen (`-maxFailedLogins`) festgelegt ist. Der Wert `-noMaxFailedLogins` bedeutet, dass es keine maximal zulässige Anzahl von aufeinanderfolgenden fehlgeschlagenen Anmeldungen gibt. Darüber hinaus müssen `-noFailedLoginPeriod` und `-noLockoutPeriod` angegeben werden, wenn `-noMaxFailedLogins` festgelegt ist. Weitere Informationen zu diesen Einstellungen erhalten Sie unter Deaktivierung/Reaktivierung der Zählung fehlgeschlagener Anmeldungen auf Seite 93.

Die Einstellung für den Zeitraum fehlgeschlagener Anmeldungen steht für den Zeitraum in Sekunden, in denen die Anzahl der fehlgeschlagenen Anmeldungen für lokale Benutzerkonten aufgezeichnet wird. Der Zeitraum kann im Bereich von 1 bis 3.600 Sekunden konfiguriert werden. Wenn Benutzerkontoeinstellungen ohne Festlegung des Zeitraums fehlgeschlagener Anmeldungen aktiviert werden, beträgt der Standardwert 900 Sekunden. Wenn Benutzerkontoeinstellungen deaktiviert sind, erfolgt für den Zeitraum fehlgeschlagener Anmeldungen keine Angabe.

Hinweis

Die Einstellungen für den Zeitraum fehlgeschlagener Anmeldungen (`-maxFailedLogins`) und die Sperrdauer (`-lockoutPeriod`) müssen mit einem Wert angegeben werden, wenn die Einstellung für den Zeitraum fehlgeschlagener Anmeldungen (`-failedLoginPeriod`) festgelegt ist. Der Wert `-noFailedLoginPeriod` bedeutet, dass die Anzahl der aufeinanderfolgenden fehlgeschlagenen Anmeldungen innerhalb eines Zeitraums nicht aufgezeichnet wird. Darüber hinaus müssen `-noMaxFailedLogins` und `-noLockoutPeriod` angegeben werden, wenn `-noFailedLoginPeriod` festgelegt ist. Weitere Informationen zu diesen Einstellungen erhalten Sie unter Deaktivierung/Reaktivierung der Zählung fehlgeschlagener Anmeldungen auf Seite 93.

Sperrdauer
Die Einstellung für die Sperrdauer steht für den Zeitraum in Sekunden, in denen das lokale Benutzerkonto gesperrt ist, wenn die maximale Anzahl der aufeinanderfolgenden fehlgeschlagenen Anmeldungen innerhalb dieses festgelegten Zeitfensters erreicht wurde. Der Zeitraum kann im Bereich von 1 bis 86.400 Sekunden

konfiguriert werden. Wenn Benutzerkontoeinstellungen ohne Festlegung der Sperrdauer aktiviert werden, beträgt der Standardwert 3600 Sekunden. Wenn Benutzerkontoeinstellungen deaktiviert sind, erfolgt für die Sperrdauer keine Angabe.

Hinweis

Die Einstellungen für die maximale Anzahl fehlgeschlagener Anmeldungen (`-maxFailedLogins`) und der Zeitraum fehlgeschlagener Anmeldungen (`-failedLoginPeriod`) müssen mit einem Wert angegeben werden, wenn die Einstellung für die Sperrdauer (`-lockoutPeriod`) festgelegt ist. Der Wert `-noLockoutPeriod` bedeutet, dass das Konto nicht gesperrt wird, weil es die Anforderung für die maximale Anzahl fehlgeschlagener Anmeldungen innerhalb der Anforderung für den Zeitraum fehlgeschlagener Anmeldungen erfüllt. Darüber hinaus müssen `-noMaxFailedLogins` und `-noFailedLoginPeriod` angegeben werden, wenn `-noLockoutPeriod` festgelegt ist. Weitere Informationen zu diesen Einstellungen erhalten Sie unter Deaktivierung/Reaktivierung der Zählung fehlgeschlagener Anmeldungen auf Seite 93.

Deaktivierung/Reaktivierung der Zählung fehlgeschlagener Anmeldungen

Ein Benutzer mit der Rolle eines Administrators oder Sicherheitsadministrators kann alle Anmeldeeinschränkungen deaktivieren, indem er `-noMaxFailedLogins`, `-noFailedLoginPeriod` und `-noLockoutPeriod` gleichzeitig in einem Befehl festlegt, zum Beispiel:

```
uemcli -d 10.0.0.1 -u Local/admin -p MyPassword456! /user/account/
settings set -noMaxFailedLogins -noFailedLoginPeriod -noLockoutPeriod
```

⚠ ACHTUNG

Es ist nicht empfehlenswert, diesen Befehl im STIG-Modus auszuführen. Während diese Einstellung aktiviert ist, kann ein Brute-Force-Angriff auf Passwörter zugelassen werden, da keine Überprüfung durchgeführt wird.

Um alle Anmeldeeinschränkungen erneut zu aktivieren, legen Sie gleichzeitig `-maxFailedLogins`, `-failedLoginPeriod` und `-lockoutPeriod` mit Werten in einem Befehl fest, zum Beispiel:

```
uemcli -d 10.0.0.1 -u Local/admin -p MyPassword456! /user/account/
settings set -maxFailedLogins 3 -failedLoginPeriod 900 -lockoutPeriod
3600
```

Timeout einer Sitzung im Leerlauf

Die Einstellung für das Timeout einer Sitzung im Leerlauf steht für den Zeitraum in Sekunden, in denen eine Sitzung eines Benutzers inaktiv sein kann, bevor die Sitzung automatisch beendet wird. Der Zeitraum kann im Bereich von 1 bis 3.600 Sekunden konfiguriert werden. Wenn Benutzerkontoeinstellungen ohne Festlegung des Timeout einer Sitzung im Leerlauf aktiviert werden, beträgt der Standardwert 600 Sekunden. Wenn Benutzerkontoeinstellungen deaktiviert sind, erfolgt für das Timeout einer Sitzung im Leerlauf keine Angabe. Diese Einstellung gilt sowohl für lokale als auch für LDAP-Benutzerkonten.

Hinweis

Der Wert `-noSessionIdleTimeout` bedeutet, dass bei Sitzungen nie ein Timeout aufgrund von Inaktivität auftritt.

Aktivieren der Standardadministratorsperre
Die Einstellung für Aktivieren der Standardadministratorsperre gib an, ob die manuelle und automatische Kontosperrfunktion auf das lokale Standard-Administratorbenutzerkonto angewendet wird. Diese Einstellung kann mit `yes` oder `no` konfiguriert werden. Wenn Benutzerkontoeinstellungen ohne Festlegung dieser Einstellung aktiviert werden, lautet der Standardwert `no`. Der Wert `no` bedeutet, dass die manuelle und automatische Kontosperrfunktion nicht auf das lokale standardmäßige Konto des Administratorbenutzers angewendet wird.

Manuelle Kontosperrung-/entsperrung (nur physische Bereitstellungen)

Ein Benutzer mit der Administratorrolle kann Benutzerkonten manuell sperren/entsperren. Nachdem ein Benutzerkonto manuell gesperrt wurde, kann sich der Benutzer nicht erfolgreich authentifizieren, selbst wenn die Anmeldedaten gültig sind. Außerdem bleibt das Benutzerkonto gesperrt, bis ein Administrator es manuell entsperrt.

Im Folgenden ist eine Zusammenfassung der Beschränkungen für die manuelle Sperrung/Entsperrung angegeben:

- Die Funktion ist nur über die UEMCLI verfügbar: `/user/account/ -id <administrator_id> set -locked {yes|no}`.
- Dieser Befehl kann nur von einem Benutzer mit der Administratorrolle ausgeführt werden.
- Das Standardadministratorkonto kann nicht gesperrt/entsperrt werden.
- Ein Benutzer kann sein eigenes Konto nicht sperren/entsperren.
- Der Befehl gibt einen Fehler zurück, wenn er bei deaktiviertem STIG-Modus verwendet wird.

Physische Sicherheitskontrollen (nur physische Bereitstellungen)

Der Bereich, in dem sich das Speichersystem befindet, muss so ausgewählt und angepasst werden, dass für die physische Sicherheit des Speichersystems gesorgt ist. Dies umfasst einfache Maßnahmen, z. B. ausreichend Türen und Schlösser, nur autorisierten und überwachten physischen Zugriff auf das System, eine zuverlässige Stromquelle und standardmäßige Best Practices für die Verkabelung.

Ferner müssen folgende Speichersystemkomponenten mit besonderer Vorsicht behandelt werden:

- Taste zum Zurücksetzen des Passworts: Setzt die standardmäßigen werkseitigen Passwörter für das Standardadministratorkonto und das Servicekonto für das Speichersystem temporär zurück, bis ein Administrator das Passwort zurücksetzt.
- SP-Ethernet-Serviceportverbindung: Ermöglicht authentifizierten Zugriff über eine SP-Ethernet-Serviceportverbindung.

Virenschutz

Das Speichersystem unterstützt Common AntiVirus Agent (CAVA). CAVA, eine Komponente des Common Event Enabler (CEE), bietet eine Virenschutzlösung für

Clients mit einem Speichersystem. Sie nutzt ein Branchenstandard-SMB-Protokoll in einer Microsoft Windows Server-Umgebung. CAVA nutzt Virenschutzsoftware von Drittanbietern, um bekannte Viren zu identifizieren und zu eliminieren, bevor sie Dateien im Speichersystem infizieren können. Das CEE-Installationsprogramm, das das CAVA-Installationsprogramm umfasst, und die CEE-Versionshinweise sind für die Unity-Produktreihe, Unity VSA, Unity Hybrid oder Unity All Flash auf Online Support unter **Support nach Produkt Downloads** > **Vollständige Version** verfügbar.

ANHANG A

TLS-Chiffren

In diesem Anhang werden die TLS-Chiffren aufgeführt, die vom Speichersystem unterstützt werden.

Folgende Themen werden behandelt:

Unterstützte TLS-Cipher Suites

Eine Cipher Suite definiert einen Satz von Technologien zum Sichern der TLS-Kommunikation:

- Schlüsselaustauschalgorithmus (wie der zur Datenverschlüsselung verwendete geheime Schlüssel vom Client an den Server kommuniziert wird). Beispiele: RSA-Schlüssel oder Diffie-Hellman (DH)
- Authentifizierungsmethode (wie Hosts die Identität von Remotehosts authentifizieren können). Beispiele: RSA-Zertifikat, DSS-Zertifikat oder keine Authentifizierung
- Verschlüsselungsverfahren (wie Daten verschlüsselt werden). Beispiele: AES (256 oder 128 Bit)
- Hash-Algorithmus (Sichern von Daten durch eine Methode, um festzustellen, ob Daten geändert wurden). Beispiele: SHA-2 oder SHA-1

Die unterstützten Cipher Suites kombinieren alle diese Elemente.

In der folgenden Liste sind die OpenSSL-Namen der SSL- oder TLS-Cipher Suites für das Speichersystem und die zugehörigen Ports aufgeführt.

Tabelle 20 Standardmäßige bzw. unterstützte SSL- oder TLS-Cipher Suites, die vom Speichersystem unterstützt werden

Cipher Suites	Protokolle	Ports
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	TLSv1, TLSv1.1, TLSv1.2	443, 8443, 8444
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	TLSv1, TLSv1.1, TLSv1.2	443, 8443, 8444
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	TLSv1.2	443, 8443, 8444
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	TLSv1.2	443, 8443, 8444
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	TLSv1.2	443, 8443, 8444
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	TLSv1.2	443, 8443, 8444
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	TLSv1, TLSv1.1, TLSv1.2	443, 8443, 8444
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	TLSv1, TLSv1.1, TLSv1.2	443, 8443, 8444
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	TLSv1.2	443, 8443, 8444
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	TLSv1.2	443, 8443, 8444
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	TLSv1.2	443, 8443, 8444

Tabelle 20 Standardmäßige bzw. unterstützte SSL- oder TLS-Cipher Suites, die vom Speichersystem unterstützt werden (Fortsetzung)

Cipher Suites	Protokolle	Ports
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	TLSv1.2	443, 8443, 8444
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	TLSv1, TLSv1.1, TLSv1.2	5989
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	TLSv1.2	5989
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	TLSv1.2	5989
TLS_RSA_WITH_AES_128_CBC_SHA	TLSv1, TLSv1.1, TLSv1.2	5989
TLS_RSA_WITH_AES_128_CBC_SHA256	TLSv1.2	5989
TLS_RSA_WITH_AES_256_CBC_SHA	TLSv1, TLSv1.1, TLSv1.2	5989
TLS_RSA_WITH_AES_256_CBC_SHA256	TLSv1.2	5989

ANHANG B

LDAP-Konfiguration

In diesem Anhang wird beschrieben, wie das Unity-System konfiguriert wird, um sich mit einem LDAP-Server für die Authentifizierung zu verbinden, und wie LDAP-Benutzern und -Gruppen Rollen zugewiesen werden.

Folgende Themen werden behandelt:

Informationen über die Konfiguration von LDAP

Das Lightweight Directory Access Protocol (LDAP) ist ein Anwendungsprotokoll zur Abfrage und Bearbeitung von Verzeichnisdiensten, die in TCP/IP-Netzwerken ausgeführt werden. LDAP ermöglicht ein zentrales Management der Netzwerkauthentifizierung und Autorisierungsvorgänge. Durch die Integration von Unisphere-Benutzern in eine vorhandene LDAP-Umgebung kann der Managementzugriff basierend auf etablierten Benutzer- und Gruppenkonten im LDAP-Verzeichnis gesteuert werden.

Bevor Sie LDAP konfigurieren, müssen Sie das Unity-System konfigurieren, um sich mit einem DNS-Server zu verbinden. Diese Aktion ist erforderlich, um die IP-Adresse und den vollständig qualifizierten Hostnamen für jeden LDAP-Server aufzulösen, der konfiguriert ist.

Vernetzte Komponenten authentifizieren sich beim Datenaustausch gegenseitig durch Zertifikate. Für eine sichere Kommunikation zwischen zwei vernetzten Komponenten muss eine Komponente dem Zertifikat der anderen Komponente vertrauen (es akzeptieren). Unisphere verwendet die Zertifikatstandards SSL/TLS und X.509, um die Client(Speichersystem)- und Server(LDAP)-Kommunikation zu sichern. Das Unity-System verlangt, dass die Zertifikatskettendatei hochgeladen wird, um das Serverzertifikat, das vom LDAP-Server empfangen wird, ordnungsgemäß zu überprüfen, wenn die TLS-Sitzung eingerichtet wird.

Nach der Konfiguration der LDAP-Einstellungen für das Unity-System können Sie Benutzermanagementfunktionen durchführen. Beispiel: Sie können die Zugriffsberechtigungen für Unisphere basierend auf vorhandenen Benutzern und Gruppen im Rahmen einer bestehenden LDAP-Verzeichnisstruktur zuweisen.

Folgen Sie dieser Abfolge von Schritten, um LDAP auf einem Unity-System zu konfigurieren:

1. Konfigurieren des DNS-Servers

   Hinweis

   Nur erforderlich, wenn Hostnamen für die LDAP-IP-Adressen verwendet werden oder wenn die dynamische LDAP-Funktion verwendet wird. Ansonsten ist dieser Schritt optional.

2. Konfigurieren Sie den LDAP-Server.
3. Überprüfen Sie die LDAP-Serververbindung.
4. Konfigurieren Sie LDAPS für den LDAP-Server.
5. Überprüfen Sie die LDAP-Serververbindung mit dem LDAPS-Protokoll.
6. Konfigurieren Sie LDAP-Benutzer und -Gruppen.

Hinweis

Die *Unisphere-Onlinehilfe* bietet weitere Informationen zu LDAP und DNS und zu den Schritte zum Konfigurieren des Unity-Systems, um sich mit einem LDAP-Server und einem DNS-Server zu verbinden, und wie man LDAP-Benutzern und-Gruppen Rollen zuweist und diese verwaltet.

Konfigurieren des DNS-Servers

DNS muss vor der Konfiguration des LDAP-Servers konfiguriert werden, um die LDAP-Serveradressen aufzulösen. Dies ist erforderlich, um sicherzustellen, dass die IP-Adresse und der vollständig qualifizierte Hostname bei jedem LDAP-Server aufgelöst werden können.

Führen Sie zum Konfigurieren des DNS die folgenden Schritte aus:

Vorgehensweise

1. Klicken Sie in Unisphere auf das Zahnradsymbol in der oberen Menüleiste, um die Seite **Einstellungen** anzuzeigen.
2. Klicken Sie im linken Bereich unter **Verwaltung** auf **DNS-Server**.

   Die Seite **Domainnamensserver managen** wird angezeigt.
3. Führen Sie je nach Ihrer Konfiguration einen der folgenden Schritte durch:
   - Wenn das System so konfiguriert ist, dass die DNS-Serveradressen von einer Remotequelle abgerufen werden, wählen Sie **DNS-Serveradresse automatisch erhalten** aus.
   - Wählen Sie für einen DNS-Server, auf dem der LDAP-Server konfiguriert ist, **DNS-Serveradresse manuell konfigurieren** aus und geben Sie mindestens eine IP-Adresse ein. Wenn die LDAP-Server manuell mit IP-Adressen konfiguriert werden sollen, müssen sich die LDAP-Server auf dem DNS-Server sowohl in Forward- als auch Reverse-Lookupzonen befinden.
4. Sobald die DNS-Serveradressen konfiguriert sind, klicken Sie auf **Anwenden**, um die DNS-Serverkonfiguration zu speichern.

Konfigurieren des LDAP-Servers

Die LDAP-Serverkonfiguration besteht darin, die Konfigurationsinformationen anzugeben, die für die Verbindung mit dem LDAP-Server benötigt werden.

Führen Sie zum Konfigurieren von LDAP die folgenden Schritte aus:

Vorgehensweise

1. Klicken Sie in Unisphere auf das Zahnradsymbol in der oberen Menüleiste, um die Seite **Einstellungen** anzuzeigen.
2. Klicken Sie im linken Bereich unter **Benutzer und Gruppen** auf **Verzeichnisdienste**.

   Die Seite **Anmeldeinformationen für LDAP-Server konfigurieren** wird angezeigt.
3. Geben Sie bei **Domainname** den Domainnamen des LDAP-Authentifizierungsservers ein.

   Der Domainname muss ausgefüllt werden, wenn die LDAP-Serverkonfiguration erstellt wird. Danach wird er ausgegraut, weil er nicht verändert werden kann, ohne die LDAP-Serverkonfiguration zu löschen und neu zu erstellen.
4. Geben Sie bei **Distinguished Name** den Distinguished Name des LDAP-Benutzers mit Administratorrechten ein.

   Der Distinguished Name sollte in einem der folgenden Formate angegeben werden:
   - LDAP-Format (z. B. `cn=Administrator,cn=Users,dc=mycompany,dc=com`)

- <*user*>@<*domain*>-Format (z. B. **Administrator@mycompany.com**)
- <*domain*>/<*user*>-Format (z. B. **mycompany.com/Administrator**)

5. Geben Sie bei **Passwort** das Passwort für den Benutzer ein, der in **Distinguished Name** angegeben ist.
6. Wenn der LDAP-Server einen anderen Port für LDAP verwendet als die Standardportnummer 389, ändern Sie den Port in die gewünschte Portnummer.

   Geben Sie zum Beispiel Port 3268 für LDAP mit Forest-Level-Authentifizierung an. (`nsroot.net` anstatt `nam.nsroot.net` mit LDAP zu verwenden, erlaubt Kunden, die gesamte Active Directory (AD)-Gesamtstruktur (Port 3268) abzufragen, statt nur die AD-Domain (TCP-Port 389). Außerdem basiert die AD-Rollenzuordnung auf Gruppenbereichen für lokale Domaingruppen und universelle Gruppen. Dies ermöglicht es Endbenutzern, das AD anhand eines entsprechenden Bereichs nach Bedarf zu durchsuchen und unnötige Gruppensuchen zu vermeiden.) Es wird dringend empfohlen, LDAP vor der Konfiguration von Secure LDAP (LDAPS) zu konfigurieren und zu verifizieren. Dadurch wird jegliches Troubleshooting minimiert, das bei der Aktivierung von LDAPS erforderlich sein kann.
7. Führen Sie in **Serveradresse** einen der folgenden Schritte aus:
   - Um eine Serveradresse manuell hinzuzufügen, klicken Sie auf **Hinzufügen**, um das Dialogfeld **LDAP-Server** anzuzeigen, geben Sie die IP-Adresse oder den vollständig qualifizierten Hostnamen ein und klicken Sie auf **OK**. Um eine Serveradresse zu entfernen, wählen Sie die Adresse im Textfeld aus klicken Sie auf **Entfernen**.
   - Um die Serveradressen automatisch von DNS abzurufen, klicken Sie auf **Automatische Erkennung**.
8. Wenn der LDAP-Server für Benutzer oder Gruppe oder beides einen anderen Suchpfad hat als der standardmäßige `cn=Users,dc=`, klicken Sie auf **Erweitert**.

   Das Dialogfeld **Erweitert** wird angezeigt.
9. Aktualisieren Sie im Fenster **Erweitert** die Suchpfade oder andere Felder nach Bedarf und klicken Sie dann auf **OK**, um die erweiterten Konfigurationsänderungen zu speichern.

   Wenn Sie z. B. Forest-Level-Authentifizierung konfigurieren, wählen Sie **Erweitert** aus, um auf das Fenster **Erweitert** zuzugreifen, und geben Sie **`userPrincipalName`** im Feld **Benutzer-ID-Attribut** an. Wenn der LDAP-Server einen anderen Suchpfad als den Standardsuchpfad (cn=Users,dc=) für Benutzer, Gruppen oder beides hat, greifen Sie auf das Fenster **Erweitert** zu, um die Suchpfade oder andere Eigenschaften nach Bedarf zu aktualisieren.
10. Nachdem alle LDAP-Konfigurationsdaten angegeben wurden, klicken Sie auf **Anwenden**, um die Konfiguration zu speichern.

    Wenn **Automatische Erkennung** ausgewählt wurde, um die Serveradressen automatisch von DNS abzurufen, werden die von DNS abgerufenen Serveradressen in **Serveradresse** ausgegraut angezeigt.

Weitere Erfordernisse

Nachdem die LDAP-Serverkonfiguration gespeichert wurde und um das Risiko zu vermeiden, dass Daten nicht verfügbar sind, müssen Sie die Konfiguration überprüfen, um zu bestätigen, dass die Verbindung zum LDAP-Server erfolgreich sein wird.

Überprüfen der LDAP-Konfiguration

Hinweis

Um zu verhindern, dass Daten nicht verfügbar sind, müssen Sie die LDAP-Verbindung nach jeder LDAP-Konfigurationsänderung überprüfen.

Gehen Sie folgendermaßen vor, um zu überprüfen, ob die Verbindung zum LDAP-Server erfolgreich sein wird:

Vorgehensweise

1. Klicken Sie auf der Seite **Anmeldeinformationen für LDAP-Server konfigurieren** auf **Verbindung prüfen**.

   Wenn die Konfiguration gültig ist, wird eine Verbindung mit dem LDAP-Server hergestellt und ein grünes Häkchen mit dem Text **Verbindung überprüft** wird angezeigt.
2. Wenn die Überprüfung fehlschlägt, werden folgende Schritte empfohlen, um den Fehler zu beheben:
   a. Überprüfen Sie die Konfigurationsdaten **Anmeldeinformationen für LDAP-Server konfigurieren**, insbesondere **Distinguished Name** (Benutzername), **Passwort** und die **Serveradresse** (IP-Adresse oder Hostname).
   b. Überprüfen Sie, ob der LDAP-Server online ist.
   c. Überprüfen Sie, ob Netzwerkprobleme vorliegen; zum Beispiel Firewallregeln, die den Zugriff auf den LDAP-Port blockieren würden, Netzwerkrouterkonfiguration, welche die Verbindung verhindert, usw.

Konfigurieren von Secure LDAP

Die Konfiguration von Secure LDAP (LDAPS) erfordert Folgendes:

- Konfigurieren des LDAPS-Protokolls und -Ports
- Konfigurieren der Zertifikatskette

Wenn LDAPS konfiguriert ist, verbindet sich das Unity-System über TLS mit dem LDAP-Server. Das Unity-System verlangt, dass die Zertifikatskettendatei hochgeladen wird, um das Serverzertifikat, das vom LDAP-Server empfangen wird, ordnungsgemäß zu überprüfen, wenn die TLS-Sitzung eingerichtet wird.

Das Format der zu hochzuladenden Zertifikatsdatei ist wie folgt:

- Die Zertifikatsdatei muss die Dateierweiterung `cer` aufweisen. Beispiel: `LdapServerChain.cer`
- Alle Zertifikate in der zu hochgeladenen Zertifikatsdatei müssen das PEM-Format aufweisen. Mit PEM formatierte Zertifikate sind ASCII-Textdateien, die mit `-----BEGIN CERTIFICATE-----` beginnen und mit `-----END CERTIFICATE-----` enden.
- Das LDAP-Serverzertifikat muss den Servernamen, wie in der LDAP-Konfiguration angegeben, im Feld „Betreff“ oder „Alternativer Betreffname“ im Zertifikat aufweisen. Dies ist erforderlich, um zu überprüfen, ob das Zertifikat vom gewünschten LDAP-Server ist.
- Wenn das LDAP-Serverzertifikat selbstsigniert ist, wird nur das Serverzertifikat benötigt.

- Wenn das LDAP-Serverzertifikat von einer Zertifizierungsstelle signiert wurde, muss die Zertifikatskette bis zur Stammzertifikatsstelle in der Zertifikatsdatei enthalten sein, die in folgender Reihenfolge hochgeladen werden soll:
  1. Zertifikat der Zwischenzertifikatsstelle (falls vorhanden).
  2. ...
  3. Zertifikat der Stammzertifikatsstelle
  4. Wenn die hochzuladende Datei mehrere Zertifikate enthält, muss sich zwischen jedem Zertifikat eine neue Zeile befinden.

Führen Sie zum Konfigurieren von LDAPS die folgenden Schritte aus:

Vorgehensweise

1. Aktivieren Sie das Kontrollkästchen **LDAPS-Protokoll verwenden** auf der Seite **Anmeldeinformationen für LDAP-Server konfigurieren**.

   Der **Port** wird automatisch in 636 geändert, was die standardmäßige LDAPS-Portnummer ist. Wenn der LDAP-Server einen anderen Port für LDAP verwendet, ändern Sie den Port in die gewünschte Portnummer. Geben Sie zum Beispiel Port 3269 für LDAPS mit Forest-Level-Authentifizierung an. (`nsroot.net` anstatt `nam.nsroot.net` mit LDAP zu verwenden, erlaubt Kunden, die gesamte Active Directory (AD)-Gesamtstruktur (Port 3269) abzufragen, anstatt nur die AD-Domain (TCP-Port 636). Außerdem basiert die AD-Rollenzuordnung auf Gruppenbereichen für lokale Domaingruppen und universelle Gruppen. Dies ermöglicht es Endbenutzern, das AD anhand eines entsprechenden Bereichs nach Bedarf zu durchsuchen und unnötige Gruppensuchen zu vermeiden.) Außerdem wird **Zertifikat hochladen** aktiviert, wenn das Kontrollkästchen **LDAPS-Protokoll verwenden** aktiviert wird.
2. Klicken Sie auf **Zertifikat hochladen**.

   Das Dialogfeld **Datei hochladen** wird angezeigt.
3. Klicken Sie auf **Datei auswählen**.
4. Navigieren Sie zur gewünschten Zertifikatsdatei, wählen Sie dann die Datei aus und klicken Sie auf **Upload starten**.
5. Klicken Sie nach Abschluss des Dateiuploads auf **Anwenden**, um die Konfigurationsänderungen zu speichern.

Weitere Erfordernisse

Sie müssen die Konfiguration nach der Konfiguration von LDAP und dem Hochladen der Serverzertifikatsdatei überprüfen.

Überprüfen der LDAPS-Konfiguration

Hinweis

Um zu verhindern, dass Daten nicht verfügbar sind, müssen Sie die LDAPS-Verbindung nach jeder LDAPS-Konfigurationsänderung überprüfen.

Tun Sie Folgendes, um die LDAPS-Konfiguration zu überprüfen:

Vorgehensweise

1. Klicken Sie auf der Seite **Anmeldeinformationen für LDAP-Server konfigurieren** auf **Verbindung prüfen**.

Wenn die Konfiguration gültig ist, wird eine Verbindung mit dem LDAP-Server hergestellt und ein grünes Häkchen mit dem Text **Verbindung überprüft** wird angezeigt.

2. Wenn die Überprüfung fehlschlägt, werden folgende Schritte empfohlen, um den Fehler zu beheben:
   a. Überprüfen Sie die Konfigurationsdaten **Anmeldeinformationen für LDAP-Server konfigurieren**, insbesondere die Portnummer.
   b. Überprüfen Sie, ob der LDAP-Server online und für LDAPS konfiguriert ist.
   c. Überprüfen Sie, ob die Zertifikate in der hochgeladenen Zertifikatsdatei gültig sind, zum Beispiel, ob sie abgelaufen und in der richtigen Reihenfolge sind.
   d. Überprüfen Sie, ob sich der konfigurierte **Servername** im Feld „Betreff“ oder „Alternativer Betreffname“ im LDAP-Serverzertifikat befindet.
   e. Überprüfen Sie, ob Netzwerkprobleme vorliegen; zum Beispiel Firewallregeln, die den Zugriff auf den LDAPS-Port blockieren würden, usw.

Weitere Erfordernisse

Nachdem der LDAP-Server konfiguriert wurde, müssen ein oder mehrere LDAP-Benutzer oder -Gruppen dem Unity-System hinzugefügt werden, um die Benutzer (oder Gruppen) Rollen zuzuordnen. Andernfalls ist die LDAP-Authentifizierung bei der Anmeldung erfolgreich, aber die Anmeldung schlägt fehl, weil dem Benutzer keine Rolle zugewiesen werden konnte.

Konfigurieren des LDAP-Benutzers

Das Verfahren zur Erstellung einer LDAP-Gruppe im Unity-System ist das gleiche wie das Erstellen eines LDAP-Benutzers, außer dass die LDAP-Gruppe auch auf dem LDAP-Server erstellt werden muss und LDAP-Benutzer als Mitglieder dieser Gruppe hinzugefügt werden. Das Erstellen einer LDAP-Gruppe hat den Vorteil, dass eine LDAP-Gruppe auf dem Unity-System konfiguriert wird und dann mehreren LDAP-Benutzern zugeordnet wird.

Tun Sie Folgendes, um einen LDAP-Benutzer oder eine LDAP-Gruppe zu erstellen:

Hinweis

Der LDAP-Server müssen konfiguriert werden, bevor ein LDAP-Benutzer oder eine LDAP-Gruppe erstellt werden kann.

Vorgehensweise

1. Klicken Sie in Unisphere auf das Zahnradsymbol in der oberen Menüleiste, um die Seite **Einstellungen** anzuzeigen.
2. Klicken Sie im linken Bereich unter **Benutzer und Gruppen** auf **Benutzerverwaltung**.

   Die Seite **Benutzer und Gruppen verwalten** wird angezeigt.
3. Klicken Sie auf das Hinzufügen-Symbol (Pluszeichen).

   Der Assistent **Benutzer oder Gruppe erstellen** wird angezeigt.
4. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie auf **LDAP-Benutzer**.

- Klicken Sie auf **LDAP-Gruppe**.

5. Klicken Sie auf **Weiter**.

   Die Seite **LDAP-Informationen** wird angezeigt, wobei die LDAP-Authority auf der Seite angezeigt wird.

6. Geben Sie bei **LDAP-Benutzer** den Benutzernamen ein, der im LDAP-Server angegeben ist.
7. Klicken Sie auf **Weiter**.

   Die Seite **Rolle** wird angezeigt.

8. Klicken Sie auf das Optionsfeld für die Rolle, die zugewiesen werden soll.
9. Klicken Sie auf **Weiter**.

   Die Seite **Summary** wird angezeigt.

10. Nachdem Sie überprüft haben, dass der LDAP-Benutzername oder -Gruppenname und die Rolle korrekt sind, klicken Sie auf **Fertigstellen**, um den Vorgang abzuschließen, oder auf **Zurück**, um die Benutzerkonfiguration zu ändern.

    Wenn der Benutzer oder die Gruppe erfolgreich erstellt wurde, wird die Seite **Ergebnisse** angezeigt.

11. Klicken Sie auf **Schließen**, um den Assistenten **Benutzer oder Gruppe erstellen** zu schließen.

    Der LDAP-Benutzer oder die LDAP-Gruppe, die gerade hinzugefügt wurde, wird in der Liste der Benutzer auf der Seite **Benutzer und Gruppen verwalten** angezeigt.