

Dell EMC Unity™-Produktreihe Secure Remote Services Requirements and Configuration

Version 5.x

Anmerkungen, Vorsichtshinweise und Warnungen

 **ANMERKUNG:** HINWEIS enthält wichtige Informationen, mit denen Sie Ihr Produkt besser nutzen können.

 **VORSICHT:** ACHTUNG deutet auf mögliche Schäden an der Hardware oder auf den Verlust von Daten hin und zeigt, wie Sie das Problem vermeiden können.

 **WARNUNG:** WARNUNG weist auf ein potenzielles Risiko für Sachschäden, Verletzungen oder den Tod hin.

Weitere Ressourcen.....	4
Chapter 1: Einführung.....	5
Benefits of ESRS.....	5
Informationen über Remoteserviceoptionen.....	5
Funktionsbeschreibung.....	7
Chapter 2: Anforderungen und Konfiguration.....	9
Voraussetzungen für ESRS.....	9
Anforderungen für Integrated ESRS.....	9
Anforderungen für Centralized ESRS.....	10
Dell EMC Online Support-Konto mit vollständigem Zugriff.....	10
So konfigurieren Sie ESRS.....	11
Chapter 3: Konfiguration von Remotesupport mithilfe von Unisphere.....	13
Konfigurieren von Remotesupport.....	13
Konfigurieren von Integrated ESRS(nur physische Bereitstellungen).....	15
Chapter 4: Konfiguration von Remotesupport über die CLI.....	17
Overview of configuring Remote Support using the CLI.....	17
Konfigurieren oder Ändern der Einstellungen für Support und Proxyserver.....	18
Konfigurieren oder Ändern der Systemkontaktinformationen.....	19
Konfigurieren oder Ändern der Supportanmeldedaten.....	20
Configure Centralized ESRS with the Unisphere CLI.....	20
Aktivieren oder Ändern von Centralized ESRS.....	20
Prüfen der Netzwerkverbindung von Centralized ESRS.....	21
Testen des Centralized EMC Secure Remote Support.....	22
Configure Integrated ESRS with the Unisphere CLI.....	23
Prüfen der Bereitschaft der Supportanmeldedaten für Integrated EMC Secure Remote Support.....	23
Aktivieren oder Ändern von Integrated ESRS.....	23
Prüfen der Netzwerkverbindung von Integrated ESRS.....	24
Anfordern eines Zugriffscodes für Integrated ESRS.....	24
Validieren des Zugriffscodes für Integrated ESRS.....	25
Testen von Integrated EMC Secure Remote Support.....	25
Konfigurieren oder Ändern der Einstellungen für Policy Manager und Proxyserver.....	26
Chapter 5: Troubleshooting.....	28
ESRS kann nicht aktiviert werden.....	28
Verwenden von RSA-Anmeldedaten zur Konfiguration von ESRS.....	29
ESRS hat ein Verbindungsproblem gemeldet.....	29

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

Hier erhalten Sie Hilfe

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

Produktinformationen

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

Fehlerbehebung:

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

Einführung

In diesem Kapitel wird die ESRS-Funktion (EMC Secure Remote Services) vorgestellt.

Folgende Themen werden behandelt:

Themen:

- [Benefits of ESRS](#)
- [Informationen über Remoteserviceoptionen](#)
- [Funktionsbeschreibung](#)

Benefits of ESRS

The embedded ESRS feature in Unity deployments provides a highly secure, remote connection between your Unity environment and Dell EMC. A connection that, once made, can unlock a wide range of benefits and services like:

- Automated health checks.
- 24x7 predictive wellness monitoring.
- Remote issue analysis and diagnosis.
- An enhanced Online Support experience with actionable, real-time data-driven insight into your global Dell EMC environment through the MyService360 dashboard.
- Remote delivery of Dell EMC's service and support.
- CloudIQ, a software-as-a-service cloud management dashboard that provides intelligent analytics about performance, capacity, and configuration for health-based reporting and remediation. ESRS must be enabled on your storage system to send data to CloudIQ.

Informationen über Remoteserviceoptionen

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

- Centralized ESRS
- Integrated ESRS (nur physische Bereitstellungen) mit einem der folgenden Typen von Optionen für Remoteserviceverbindungen:
 - Ausgehend/Eingehend
 - Nur ausgehend

Die vierte Option, „Deaktiviert“, ist zwar verfügbar, wird aber nicht empfohlen. Wenn Sie diese Option auswählen, erhält der Supportcenter keine Benachrichtigungen über Probleme mit dem Speichersystem. Sie müssen Systeminformationen möglicherweise manuell sammeln, um Supportmitarbeiter beim Troubleshooting und bei der Behebung von Problemen mit dem Speichersystem zu unterstützen.

 **ANMERKUNG:** Damit Sie ESRS konfigurieren können, müssen Sie gültige Supportanmeldedaten angeben.

Centralized ESRS

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. Sie können ein primäres und ein sekundäres Gateway für ESRS für hohe Verfügbarkeit konfigurieren, falls auf eines der Gateways nicht zugegriffen werden kann. Beide Gateways müssen sich im selben Cluster befinden, um Unterbrechungen zu minimieren, wenn ein Gateway ein Failover zum anderen durchführt.

Weitere Informationen zu ESRS Gateway und Policy Manager finden Sie auf der ESRS-Produktseite beim Online Support (<https://Support.EMC.com>).

Um Ihr Speichersystem für die Verwendung von Centralized ESRS zu konfigurieren, müssen Sie nur die IP-Adresse des ESRS Gateway bereitstellen und darauf achten, dass der Port 9443 zwischen dem Gateway und dem Speichersystem offen ist. Stellen Sie außerdem sicher, dass Port 443 für den (ausgehenden) Netzwerkverkehr offen ist.

ANMERKUNG: Speichersysteme können nur von Unisphere zum ESRS Gateway hinzugefügt werden. Wenn das Speichersystem vom Gatewayserver aus hinzugefügt wird, scheint es verbunden zu sein, jedoch können Systeminformationen nicht erfolgreich gesendet werden.

Integrated ESRS (nur physische Bereitstellungen)

ANMERKUNG: Diese Funktion ist in Ihrer Implementierung möglicherweise nicht verfügbar.

Integrated ESRS wird direkt auf dem Speichersystem ausgeführt. Wenn Sie diese Option auswählen, richten Sie das Speichersystem so ein, dass eine sichere Verbindung zwischen dem Speichersystem und dem Supportcenter verwendet wird. Sie können eine der folgenden Optionen für Remoteserviceverbindungen für Integrated ESRS auswählen:

- Ausgehende/eingehende Verbindung (Standardeinstellung) vom Speichersystem zum Supportcenter und vom Supportcenter zum Speichersystem zwecks Remotezugriff über HTTPS.
- Nur ausgehende Verbindung vom Speichersystem zum Supportcenter über HTTPS.

Wenn Sie die Option für die ausgehende/eingehende Verbindung auswählen, wird eine sichere Verbindung zwischen dem Speichersystem und dem Supportcenter eingerichtet. Mit dieser Option werden Funktionen für Remoteserviceverbindungen für die Remoteübertragung zum und vom Supportcenter mit dem Speichersystem aktiviert. Konfigurieren Sie die Verbindung zwischen dem Speichersystem und einem Policy Manager (optional) sowie allen zugehörigen Proxyservern (optional) entweder über Unisphere oder über die Befehlszeilenoberfläche (CLI).

Wenn Sie die Option für die ausschließlich ausgehende Verbindung auswählen, wird eine sichere Verbindung zwischen dem Speichersystem und dem Supportcenter eingerichtet. Mit dieser Option werden Funktionen für Remoteserviceverbindungen für die Remoteübertragung zum Supportcenter aus dem Speichersystem aktiviert.

Um das Speichersystem für die Verwendung von Integrated ESRS zu konfigurieren, müssen Sie folgende Aufgaben ausführen:

1. Geben Sie gültige Supportanmeldedaten ein, andernfalls können Sie keine ESRS-Bereitschaftsprüfung oder ESRS-Konfiguration durchführen.
2. Führen Sie eine Bereitschaftsprüfung durch (optional, jedoch dringend empfohlen).
3. Wenn Sie die Bereitschaftsprüfung übersprungen haben, akzeptieren Sie die Lizenzvereinbarung für die Funktion.
4. Führen Sie die Netzwerkprüfung durch.

ANMERKUNG: Damit die Netzwerkprüfung und ESRS-Funktionen ausgeführt werden können, müssen mehrere Ports von Ihren Firewall-/Netzwerkeinstellungen zugelassen werden. Die Ports 443 und 8443 sind für ausgehende Verbindungen und die Ports 80 und 443 für eingehende Verbindungen erforderlich. Wenn auch die für den globalen Proxyserver angezeigten Einstellungen geändert werden müssen, bearbeiten Sie sie und führen Sie dann die Netzwerkprüfung durch.

5. Für eingehende/ausgehende Remoteserviceverbindungen müssen Sie die erforderlichen Kontaktdaten des Kunden für das Speichersystem angeben, sofern sie noch nicht angegeben wurden. Dieser Schritt gilt nicht für ausschließlich ausgehende Remoteserviceverbindungen.
6. Fordern Sie einen Zugriffscode für die Überprüfung per E-Mail an (eine zusätzliche Authentifizierungsebene) und übermitteln Sie den Zugriffscode für die Validierung, um mit dem ESRS-Aktivierungsprozess fortzufahren.
7. Überprüfen Sie den Status der ESRS-Verbindung des Systems mit dem Supportcenter.
8. Konfigurieren Sie den Policy Manager für eingehende/ausgehende Remoteserviceverbindungen (sofern eine zusätzliche Sicherheitsebene erforderlich ist). Für den Policy Manager muss Port 8090 (Standard) oder der vom Kunden angegebene

Port für ausgehenden Datenverkehr geöffnet sein. Wenn er zur Verwendung von SSL konfiguriert ist, muss Port 8443 offen sein.

9. Geben Sie an, ob Daten an CloudIQ gesendet werden sollen.

Wenn „Nur Ausgehend“ die aktuelle ESRS-Konfiguration auf dem Speichersystem ist, können Sie die Proxyserverinformationen (sofern zutreffend) bearbeiten und die Option für Remoteserviceverbindungen in „Ausgehend/Eingehend“ ändern. Beim Ändern der Option für Remoteserviceverbindungen in „Ausgehend/Eingehend“ müssen Sie auch die erforderlichen Kontaktdaten des Kunden für das Speichersystem angeben, sofern sie noch nicht angegeben wurden, und gegebenenfalls den Policy Manager konfigurieren.

Wenn „Ausgehend/Eingehend“ die aktuelle ESRS-Konfiguration auf dem Speichersystem ist, können Sie die Proxyserverinformationen (sofern zutreffend) sowie die Kontakt- und Systeminformationen ändern. Sie können jedoch die Option für Remoteserviceverbindungen nicht von „Ausgehend/Eingehend“ auf „Nur Ausgehend“ ändern. Diese Änderung wird nicht unterstützt.

Funktionsbeschreibung

Die ESRS-Funktion bietet eine IP-basierte Verbindung, über die der Support Fehlerdateien und Warnmeldungen von Ihrem Speichersystem erhält und ein Remote-Troubleshooting durchführen kann, wodurch eine schnelle und effiziente Behebung möglich ist.

i ANMERKUNG: Es wird dringend empfohlen, die ESRS-Funktion zu aktivieren, um die Problemdiagnose zu beschleunigen, ein Troubleshooting durchzuführen und das Problem schneller zu beheben. Wenn Sie ESRS nicht aktivieren, müssen Sie Systeminformationen eventuell manuell sammeln, um den Support beim Troubleshooting und der Lösung von Problemen mit dem Speichersystem zu unterstützen. Auf dem System muss ESRS aktiviert sein, damit Daten an CloudIQ gesendet werden können.

ESRS und Sicherheit

Bei jedem Schritt des Remoteverbindungsprozesses von ESRS kommen mehrere Sicherheitsebenen zum Tragen, die dafür sorgen, dass Sie und der Support die Lösung ohne Sicherheitsbedenken nutzen können:

- Die komplette Kommunikation wird von Ihrem Standort aus und niemals von einer externen Quelle gesendet und ist mit einer 256-Bit-AES-Verschlüsselung versehen (AES = Advanced Encryption Standard).
- Die IP-basierte Architektur wird in Ihre vorhandene Infrastruktur integriert, wobei die Sicherheit Ihrer Umgebung erhalten bleibt.
- Die Kommunikation zwischen Ihrem Standort und dem Supportcenter erfolgt mit Authentifizierung in beiden Richtungen durch digitale RSA®-Zertifikate.
- Nur autorisierte Kundenserviceexperten mit einer gültigen Zwei-Faktor-Authentifizierung können die digitalen Zertifikate zur Anzeige einer Benachrichtigung von Ihrem Standort herunterladen.
- Mit der optionalen ESRS v3 Policy Manager-Anwendung, die nur für Integrated ESRS mit eingehender/ausgehender Verbindung gilt, können Sie den Supportzugriff basierend auf Ihren eigenen Guidelines und Anforderungen gewähren oder einschränken. Außerdem umfasst die Anwendung ein detailliertes Auditprotokoll.

ESRS-Management

Sie können ESRS mithilfe von Unisphere, der UEMCLI oder der REST-API managen. Sie können den Service aktivieren oder deaktivieren, die Einstellungen des globalen Proxyservers ändern, einen Policy Manager einrichten (nur physische Bereitstellungen) und Supportkontoanmeldedaten für vollständigen Zugriff angeben. Letztere sind erforderlich, damit ESRS funktioniert.

Policies können vom Speichersystem nicht implementiert werden. Wenn Sie den Remotezugriff auf Ihr Speichersystem stärker kontrollieren möchten, können Sie Autorisierungsberechtigungen mithilfe eines Policy Managers festlegen (gilt für Integrated ESRS mit eingehender/ausgehender Verbindung). Die Policy Manager-Softwarekomponente kann auf einem kundenseitig bereitgestellten Server installiert werden. Der Policy Manager kontrolliert den Remote-Zugriff auf Ihre Geräte, speichert ein Auditprotokoll mit Angaben zu Remote-Verbindungen und unterstützt Dateiübertragungsvorgänge. Damit können Sie kontrollieren, wer mit welcher Methode wann auf das Speichersystem zugreift. Weitere Informationen über den Policy Manager finden Sie auf der Online Support-Website (<https://support.emc.com/>). Rufen Sie nach der Anmeldung die entsprechende Produktseite auf und suchen Sie den Link für die technische Dokumentation zu diesem ESRS-Produkt.

Die integrierte ESRS-Funktion (nur physische Bereitstellungen) ist als gemanagter Service in die Betriebsumgebung des Speichersystems integriert. Diese Funktion ist in Ihrer Implementierung möglicherweise nicht verfügbar. Die integrierte Implementierung beinhaltet die Hochverfügbarkeitsfunktion (HA), die die Überwachung des ESRS-Services ermöglicht und für das Failover vom primären Speicherprozessor (SP) zum Backupspeicherprozessor zuständig ist, falls ersterer ausfällt. HA übernimmt bei einem Ausfall von ESRS den Neustart des Service. Die Betriebsumgebung ist für die permanente Bereitstellung der Konfiguration und der Zertifikate zuständig, die für eine ordnungsgemäße Funktion von ESRS erforderlich sind.

Mit Centralized ESRS können Sie sowohl ein primäres Gateway als auch ein sekundäres Gateway so konfigurieren, dass hohe Verfügbarkeit (HA) innerhalb des VE-Clusters im Netzwerk möglich ist. Wenn das primäre Gateway ausfällt, führt das Unity-System automatisch ein Failover zum sekundären Gateway im Netzwerk für ESRS- und Cloud-IQ-Konnektivität durch. Die Konfiguration des primären Gateways ist obligatorisch, während die Konfiguration des sekundären Gateways optional ist.

 **ANMERKUNG:** Sobald das primäre und das sekundäre Gateway für Centralized ESRS konfiguriert wurden, können Sie das primäre Gateway nicht auf das sekundäre Gateway ändern. Um dies zu erreichen, müssen Sie Centralized ESRS zunächst deaktivieren und dann mit der entsprechenden Gateway-Reihenfolge erneut aktivieren.

ESRS wird im vollständigen Servicemodus unterstützt (beide SPs arbeiten im Servicemodus). Falls ESRS bereits aktiviert wurde, arbeitet das System entsprechend der Konfiguration. Wurde ESRS noch nicht aktiviert, können Sie den Service vorübergehend aktivieren. In diesem Fall wird die Konfiguration nicht beibehalten, wenn das Speichersystem den normalen Betrieb wieder aufnimmt.

ESRS-Kommunikation

Damit ESRS funktioniert, ist Zugriff auf einen DNS-Server erforderlich.

Standardmäßig versucht ESRS, über einen konfigurierten Proxyserver mit den Back-end-Systemen des Supportcenters zu kommunizieren. Wenn kein Proxyserver zur Verfügung steht, versucht ESRS, den Proxyserver zu umgehen und direkt mit den Back-end-Systemen des Supportcenters zu kommunizieren.

Anforderungen und Konfiguration

Dieses Kapitel enthält die Anforderungen der ESRS-Funktion sowie eine Funktionsbeschreibung. Es wird außerdem die Vorgehensweise zur Bereitstellung der Funktion erläutert.

Folgende Themen werden behandelt:

Themen:

- [Voraussetzungen für ESRS](#)
- [Anforderungen für Integrated ESRS](#)
- [Anforderungen für Centralized ESRS](#)
- [Dell EMC Online Support-Konto mit vollständigem Zugriff](#)
- [So konfigurieren Sie ESRS](#)

Voraussetzungen für ESRS

Als Voraussetzung für die Aktivierung von ESRS auf dem Speichersystem müssen Sie über Folgendes verfügen:

- OE (Operating Environment) Version 4.0 oder höher.
- Auf dem Speichersystem muss mindestens ein DNS-Server konfiguriert sein.
- Uneingeschränkter Zugriff auf das Supportcenter (<https://support.emc.com/>) über das Internet mithilfe von HTTPS (bei Umgebungen ohne Proxy).
- Online Support-Konto mit vollständigem Zugriff (erfordert bestimmte Anmeldedaten, die mit der Standort-ID verknüpft sind; die Standort-ID ist wiederum mit der Systemseriennummer verknüpft).
- **ANMERKUNG:** Wenn es ein Problem mit Ihrem Onlinesupportkonto gibt, können Supportmitarbeiter Ihnen dabei helfen, ESRS mithilfe ihrer RSA-Anmeldedaten zu konfigurieren.
- Dynamische IP-Adressen (DHCP) dürfen nicht für Komponenten der ESRS Gateway-Server, der Policy Manager-Server oder gemanagte Geräte verwendet werden.
- Netzwerkdatenverkehr über Port 443 ist für die einwandfreie Funktion von ESRS erforderlich und wird für Mitarbeiter des Remotesupports benötigt, um viele Reparaturen mithilfe von ESRS auszuführen.
- SSL-Prüfung, Zertifikatvalidierung und Zertifikat-Proxying sind für ESRS-Netzwerkdatenverkehr nicht zulässig.
- **ANMERKUNG:** Wenn Sie DHCP zum Zuweisen von IP-Adressen zu ESRS-Komponenten (ESRS Gateway-Server, Policy Manager-Server oder gemanagte Geräte) verwenden, müssen diese statische IP-Adressen aufweisen. Leases für IP-Adressen, die diese Geräte verwenden, können nicht so festgelegt werden, dass sie ablaufen. Es wird empfohlen, dass Sie den Geräten, die von ESRS gemanagt werden sollen, statische IP-Adressen zuweisen.

Anforderungen für Integrated ESRS

Die folgenden Anforderungen beziehen sich nur auf die Implementierung von Integrated ESRS:

- Netzwerkdatenverkehr (HTTPS) muss auf den Ports 443 und 8443 (ausgehend) zum Supportcenter zulässig sein. Ein Fehler beim Öffnen von Port 8443 führt zu erheblichen Performanceeinbußen (30 bis 45 %). Ein Fehler beim Öffnen beider Ports führt möglicherweise zu einer Verzögerung bei der Behebung von Problemen mit dem Endgerät.
- Falls Ihre ESRS-Implementierung einen Policy Manager für die stärkere Kontrolle des Remotezugriffs auf das Speichersystem umfasst, müssen Sie dies bei der Konfiguration der ESRS-Funktion angeben.
- **ANMERKUNG:** Ein Policy Manager gilt nur für Integrated ESRS mit eingehender/ausgehender Verbindung.
- Wenn die ESRS-Implementierung einen Proxyserver umfasst, über den das Speichersystem die Verbindung zu einem Policy Manager herstellt, müssen Sie dies bei der Konfiguration der ESRS-Funktion angeben.

Anforderungen für Centralized ESRS

Die folgende Anforderung bezieht sich nur auf die Implementierung von Centralized ESRS:

- Netzwerkdatenverkehr (HTTPS) muss auf Port 9443 zwischen dem Unity-System und dem ESRS Gateway-Server zugelassen sein. Darüber hinaus ist Netzwerkverkehr über Port 443 für ESRS-Funktionalität erforderlich.
- Die Betriebsumgebung des ESRS Gateway-Servers muss Version 3.12.00.04 oder höher aufweisen.

ANMERKUNG: Versuchen Sie nie, ein Unity-System manuell zu einem ESRS Gateway-Server hinzuzufügen oder von diesem zu entfernen. Verwenden Sie immer den ESRS Unisphere Configuration Wizard, um ein Speichersystem zu einem Gatewayserver hinzuzufügen oder von diesem zu entfernen.

Dell EMC Online Support-Konto mit vollständigem Zugriff

Für die Konfiguration von ESRS auf einem Speichersystem muss ein aktives Konto mit vollständigem Zugriff auf der Dell EMC Online Support-Website eingerichtet sein. Dieses Konto verknüpft bestimmte Anmeldedaten mit einer bestimmten Organisation und E-Mail-Domain. Bei der Konfiguration von ESRS auf dem Speichersystem müssen Sie diese Anmeldedaten (bestehend aus einem Benutzernamen und einem Passwort) angeben, um den ESRS-Kommunikationskanal für das System zu aktivieren.

Während der EMC Secure Remote Support-Bereitschaftsprüfung wird möglicherweise eine Meldung angezeigt, dass Ihre Supportanmeldedaten nicht mit einem Kundenkonto verknüpft sind. Dies kann darauf hinweisen, dass Sie von einem Konto mit eingeschränkten Zugriffsrechten (Light-Konto) auf ein Konto mit vollständigen Zugriffsrechten aktualisieren müssen. Weitere Informationen zum Upgrade auf ein Konto mit vollständigen Zugriffsrechten erhalten Sie in den folgenden Schritten. Andernfalls müssen Sie sich hinsichtlich der Probleme mit der Registrierung der Supportanmeldedaten möglicherweise an Ihren Serviceanbieter wenden.

ANMERKUNG: Support mit vollständigem Zugriff wird nur den Kunden gewährt, die über direkten Online Support verfügen.

Ersteinrichtung eines Online Support-Kontos

Bei der Ersteinrichtung eines Online Support-Kontos verfügt Ihr Konto möglicherweise zunächst über eingeschränkte Zugriffsrechte und ist nicht mit einem Unternehmensprofil verknüpft. Wenn Ihr Unternehmen kein Profil beim Online Support eingerichtet hat, wird das Konto mit einer E-Mail-Adresse, einem Benutzernamen und einem Passwort erstellt, jedoch ohne Unternehmenszugehörigkeit. Wenn Sie das Konto einrichten, erhalten Sie eine E-Mail mit einem Bestätigungslink. Sie können auf diesen Link klicken, sich bei der Online Support-Website anmelden, Ihr Konto aktivieren und – sofern es als Konto mit eingeschränkten Zugriffsrechten (Light-Konto) eingerichtet ist – (optional) die Aktualisierung des Kontostatus auf vollständige Zugriffsrechte anfordern.

ANMERKUNG: Ein Konto mit eingeschränkten Zugriffsrechten reicht aus, um Speichersysteme zu registrieren und zu lizenzieren. Allerdings ist es mit einem Konto, das nur über eingeschränkte Zugriffsrechte verfügt, nicht möglich, ESRS für ein Speichersystem zu konfigurieren.

Aktualisieren auf vollständige Zugriffsrechte

Wenn Ihr Online Support-Konto zunächst als Konto mit eingeschränkten Zugriffsrechten aktiviert wird, können Sie weitere Informationen angeben, um vollständige Zugriffsrechte anzufordern.

Wenn Ihr Unternehmen bereits über ein Profil auf der Online Support-Website verfügt, müssen Sie möglicherweise die Standort-ID auswählen. Daraufhin werden Sie Ihrem Unternehmen zugeordnet und können ESRS auf dem Speichersystem konfigurieren.

Zum Anfordern eines neuen Kundenprofils auf der Online Support-Website sind folgende Angaben erforderlich:

Erforderliche Informationen	Beschreibung
Beziehung zu Dell EMC	Geben Sie an, ob Ihr Unternehmen ein Partner, Zulieferer oder Kunde von Dell EMC Produkten ist.

Erforderliche Informationen	Beschreibung
Standort-ID	Wählen Sie eine vorhandene Standort-ID aus (falls diese für Ihr Unternehmen bereits erstellt wurde), oder wählen Sie Ihr Unternehmen in einer Datenbank mit Unternehmensprofilen aus.

ANMERKUNG: Die mit dem anfänglich erstellten Konto mit eingeschränkten Zugriffsrechten verknüpfte E-Mail-Adresse wird als geschäftliche E-Mail-Domain mit dem neuen Kundenprofil verknüpft.

Wenn Sie bei der Validierung Ihres Kontos mit eingeschränkten Zugriffsrechten Unternehmensinformationen angegeben haben, wird Ihre Anfrage innerhalb von 24 bis 48 Stunden bearbeitet. Sie erhalten dann eine E-Mail mit einer Bestätigung der Kontostatusänderung auf vollständige Zugriffsrechte. Die E-Mail enthält einen Bestätigungslink, auf den Sie klicken, um sich anzumelden und die vollständigen Supportzugriffsrechte für das Online Support-System zu aktivieren.

Nach der Aktivierung der vollständigen Supportzugriffsrechte für den Online Support können Sie mithilfe der Kontoanmeldedaten die ESRS-Funktion auf Ihren Speichersystemen konfigurieren, die mit Ihrem Unternehmen verknüpft sind.

So konfigurieren Sie ESRS

In Unisphere können Sie Remotesupport für ein Speichersystem mithilfe einer der folgenden Methoden konfigurieren:

- Assistent für die Erstkonfiguration: Ein Assistent für die Konfiguration der globalen Speichersystemeinstellungen, der ausgeführt wird, wenn Sie das erste Mal über Unisphere auf das System zugreifen.
- Überblick: Eine Serviceseite für das Speichersystem, auf die Sie von Unisphere aus zugreifen können (**System > Service > Überblick**).
- ESRS: Eine Seite mit ESRS-Einstellungen, auf die Sie von Unisphere aus zugreifen können (**Einstellungen > Supportkonfiguration**).
- UEMCLI: Eine Befehlszeilenoberfläche mit Befehlen, die Sie über eine Eingabeaufforderung auf einem Microsoft Windows- bzw. Unix-/Linux-Host auf einem System ausführen können, um ESRS-Einstellungen zu konfigurieren. Informationen zu CLI-Befehlen im Zusammenhang mit ESRS finden Sie im *Benutzerhandbuch zur Unisphere-Befehlszeilenoberfläche*.
- Unisphere Management REST-API-Server: Eine Anwendungsoberfläche, über die REST-API-Anforderungen zur Konfiguration der ESRS-Einstellungen empfangen werden können. Informationen zur Unisphere Management REST-API finden Sie im *Unisphere Management REST-API-Programmierhandbuch*.

Navigieren Sie zur Ermittlung des Status der ESRS-Funktion in Unisphere zu **System > Service > Überblick**. ESRS ist aktiviert, wenn ein Häkchen in einem grünen Kreis unter **EMC Secure Remote Support Services** angezeigt wird.

Konfigurieren Sie bei der Aktivierung der ESRS-Funktion auf einem Speichersystem die folgenden Einstellungen:

- ANMERKUNG:** Sie müssen gültige Supportanmeldedaten (Benutzername und Passwort, die einem aktiven Onlinesupportkonto mit vollständigen Zugriffsrechten zugeordnet sind) angeben, damit Sie ESRS konfigurieren können.
- ESRS: Der vom Speichersystem verwendete ESRS-Typ: „Centralized“ oder „Integrated“ („Ausgehend/Eingehend“ oder „Nur ausgehend“). Sie können ESRS zwar deaktivieren, dies wird jedoch nicht empfohlen.
 - Lizenzvereinbarung (nur Integrated ESRS): Die ESRS-Endbenutzer-Lizenzvereinbarung (EULA) muss akzeptiert werden, um Integrated ESRS konfigurieren und verwenden zu können.
 - Netzwerkprüfung (optional, Einstellungen werden nur für Integrated ESRS angezeigt): Mit dieser Methode wird überprüft, ob das Netzwerk für die ESRS-Konfiguration bereit ist. Sofern verfügbar, wird sie zum Bearbeiten der globalen Proxyserverinformationen verwendet:
 - Protokoll: Protokoll für die Kommunikation mit einem Proxyserver, der für den Kommunikationskanal verwendet wird. Die verfügbaren Optionen sind HTTP an Port 3128 (Standardport) und SOCKS (das Standardprotokoll) an Port 1080 (Standardport).

ANMERKUNG: Bei Auswahl von SOCKS oder HTTP wird automatisch der zugehörige Standardport zur Proxyserveradresse hinzugefügt. Gegebenenfalls kann ein anderer Port über Unisphere oder UEMCLI- bzw. REST-Befehle angegeben werden.
 - Proxyserveradresse: Netzwerkadresse, die mit dem globalen Datenverkehr des Proxyservers verknüpft werden soll.

ANMERKUNG: Wenn Sie die Protokollauswahl nach Angabe einer IP-Adresse ändern, wird der angehängte Port automatisch in den Standardwert für das Protokoll geändert, es sei denn, es wurde ein anderer Port als der Standardport über UEMCLI- oder REST-Befehle festgelegt.
 - Anmeldedaten: Benutzername und Passwort eines Kontos, das für den Zugriff auf das Proxyserversystem verwendet wird.

- Kontakt- und Systemstandortinformationen (Einstellungen werden nur für Integrated ESRS mit eingehender/ausgehender Verbindung angezeigt): Informationen, die bearbeitet werden können und vom Support zum Reagieren auf Ihre Supportprobleme verwendet werden.
 - E-Mail-Bestätigung: Anfordern eines Zugriffscode und nachfolgende Authentifizierung der E-Mail-Adresse.
 - Informationen für Policy Manager (optional, Einstellungen werden nur für Integrated ESRS mit eingehender/ausgehender Verbindung angezeigt): Policy Manager-Informationen für den ESRS-Kommunikationskanal:
 - Protokoll: Protokoll für die Kommunikation mit einem Policy Manager-System, das für den ESRS-Kommunikationskanal verwendet wird.
 - Proxyserveradresse: Netzwerkadresse und Portnummer, die mit dem Datenverkehr des Policy-Servers verknüpft werden sollen.
 - Proxyserverinformationen für Policy Manager (optional, Einstellungen werden nur für Integrated ESRS mit eingehender/ausgehender Verbindung angezeigt): Bei Verwendung eines Policy Managers der vom ESRS Policy Manager verwendete Proxyserver:
 - Protokoll: Protokoll für die Kommunikation mit einem vom Policy Manager verwendeten Proxyserver.
 - Proxyserveradresse: Netzwerkadresse und Portnummer, die mit dem vom Policy Manager verwendeten Proxyserver verknüpft werden sollen.
 - Anmeldedaten: Benutzername und Passwort eines Kontos, mit dem auf den vom Policy Manager verwendeten Proxyserver zugegriffen wird.
 - Daten an CloudIQ senden (Das Kontrollkästchen wird nur für Integrated ESRS angezeigt und ist standardmäßig ausgewählt (aktiviert). Deaktivieren Sie das Kontrollkästchen, um das Senden von Daten an CloudIQ zu deaktivieren (nicht empfohlen).): CloudIQ ist ein SaaS-Cloudmanagementdashboard, das für intelligente Analysen zu Performance, Kapazität und Konfiguration für Reporting und Fehlerbehebung auf Grundlage der Systemintegrität verwendet wird.
-  **ANMERKUNG:** CloudIQ ist standardmäßig aktiviert, wenn Centralized ESRS aktiviert ist. Um CloudIQ für Centralized ESRS zu deaktivieren oder erneut zu aktivieren, gehen Sie in Unisphere zu **Einstellungen > Supportkonfiguration > CloudIQ**.

Proxyserver (nur integriertes ESRS)

Die Proxyservereinstellungen für das System müssen bereits im Rahmen der Erstkonfiguration des Systems konfiguriert worden sein. Überprüfen Sie diese Einstellungen bei der Konfiguration einer integrierten ESRS-Implementierung und nehmen Sie erforderliche Änderungen vor.

Policy Manager (gilt nur für Integrated ESRS mit eingehender/ausgehender Verbindung)

Falls das Speichersystem Autorisierungsrechte mithilfe eines Policy Managers festlegt, müssen Sie dies bei der Konfiguration von ESRS angeben. Falls der Policy Manager die Verbindung zum Speichersystem über einen Proxyserver herstellt, müssen Sie dies bei der Konfiguration von ESRS angeben. Falls für den Policy Manager-Proxyserver eine Authentifizierung erforderlich ist (SOCKS wird nur mit Authentifizierung unterstützt), müssen Sie dies während der ESRS-Konfiguration angeben und Anmeldedaten für den Proxyserver eingeben. Für die Authentifizierung müssen ein Benutzername und ein Passwort angegeben werden.

Weitere Informationen über den Policy Manager finden Sie im *Betriebsleitfaden für den Secure Remote Services Policy Manager* auf der Online Support-Website (<https://Support.EMC.com>).

Konfiguration von Remotesupport mithilfe von Unisphere

In diesem Kapitel wird der Prozess zum Provisioning der ESRS-Funktion mit der Unisphere-Benutzeroberfläche erläutert.

Folgende Themen werden behandelt:

Themen:

- Konfigurieren von Remotesupport
- Konfigurieren von Integrated ESRS(nur physische Bereitstellungen)

Konfigurieren von Remotesupport

Voraussetzungen

Wenn Ihre IT-Umgebung erfordert, dass das Speichersystem über einen Proxyserver verbunden werden muss, überprüfen Sie, ob der Proxyserver konfiguriert ist, bevor Sie fortfahren, indem Sie die Seite **Einstellungen > Supportkonfiguration > Proxyserver** prüfen.

Info über diese Aufgabe

Führen Sie zum Konfigurieren von Remotesupport mithilfe von Unisphere die folgenden Schritte aus:

Schritte

1. Wählen Sie das Symbol **Einstellungen** und wählen Sie dann **Supportkonfiguration**.
2. Wenn Ihre Anmeldedaten noch nicht angegeben sind, wählen Sie **Supportanmeldedaten** aus, um Ihre Supportanmeldedaten, d. h. Ihren Benutzernamen und Ihr Passwort, anzugeben. Anderenfalls fahren Sie mit dem nächsten Schritt fort.
Wenn Sie keine gültigen Supportanmeldedaten angeben, können Sie keine Supportvertragsinformationen anzeigen und nicht zu den Online-Supportproduktseiten navigieren.
3. Wählen Sie **EMC Secure Remote Services** aus.
Es wird empfohlen, vor der Konfiguration von ESRS eine Bereitschaftsprüfung durchzuführen, um festzustellen, ob ESRS konfiguriert werden kann. Klicken Sie zur Umgehung der Bereitschaftsprüfung einfach auf **Konfigurieren** und fahren Sie mit Schritt 6 fort.
4. Klicken Sie auf **Bereitschaftsprüfung**.
5. Wählen Sie in **ESRS-Bereitschaftsprüfung** die ESRS-Option aus, die Sie verwenden möchten.

Option	Beschreibung
Integriert (nur physische Bereitstellungen)	Bevor die Bereitschaftsprüfung ausgeführt wird, muss die ESRS-EULA (Endbenutzer-Lizenzvereinbarung) akzeptiert werden. Nachdem die Lizenzvereinbarung akzeptiert wurde, klicken Sie auf Weiter , um die Prüfung durchzuführen.  ANMERKUNG: Nachdem die Lizenzvereinbarung akzeptiert wurde, wird sie nicht erneut angezeigt.
Zentralisiert	Bevor die Bereitschaftsprüfung ausgeführt wird, wird die minimal erforderliche Softwareversion des Gatewayservers angezeigt und die Gatewaynetzwerkadresse muss angegeben werden. Nachdem die Gatewaynetzwerkadresse eingegeben wurde, klicken Sie auf Weiter , um die Prüfung auszuführen.

Nachdem die Bereitschaftsprüfung ausgeführt wurde, geschieht eines der folgenden Ereignisse:

- Wenn keine Fehler gefunden werden, wird ein grüner Kreis mit einem Häkchen und eine Erfolgsmeldung angezeigt. Klicken Sie entweder auf **EMC Secure Remote Support konfigurieren** und wechseln Sie zu Schritt 6, um die Konfiguration von EMC Secure Remote Support fortzusetzen, oder klicken Sie auf **Schließen**, um zu den **Einstellungen** für EMC Secure Remote Support zurückzukehren und die Konfiguration zu einem späteren Zeitpunkt fortzusetzen.
- Wenn Fehler angezeigt werden, beheben Sie etwaige Probleme und klicken Sie auf **Erneut überprüfen**, um sicherzustellen, dass ESRS konfiguriert werden kann, oder klicken Sie auf **Schließen** und beheben Sie die Probleme zu einem späteren Zeitpunkt.

6. Geben Sie in **Konfigurieren von ESRS** die entsprechenden Informationen zu ESRS-Optionen an.

Option	Beschreibung
Centralized: Überwachen mit einer zentralisierten ESRS-Konfiguration	a. Geben Sie die Primäre Gatewaynetzwerkadresse des ESRS Gateway-Servers an, der verwendet wird, um die Verbindung zum Unternehmen EMC herzustellen, und stellen Sie sicher, dass Port 9443 zwischen dem Gatewayserver und dem Speichersystem geöffnet ist. i ANMERKUNG: RSA-Anmeldedaten können für primäre Gatewaykonfigurationen ohne Kundensupportkonto verwendet werden. Dies ermöglicht die Konfiguration von Centralized ESRS, während die Anmeldedaten für das Supportkonto am Back-End erstellt und validiert werden. b. Geben Sie optional eine Sekundäre Gatewaynetzwerkadresse für ESRS High Availability (HA) ein. Das zweite Gateway muss im selben ESRS HA-Cluster wie die Primäre Gatewaynetzwerkadresse konfiguriert werden. i ANMERKUNG: Wenn RSA-Berechtigungen für das primäre Gateway verwendet wurden, müssen Sie auch verwendet werden, um die Konfiguration eines sekundären Gateways abzuschließen. i ANMERKUNG: CloudIQ ist standardmäßig aktiviert, wenn Centralized ESRS aktiviert ist. Um CloudIQ für Centralized ESRS zu deaktivieren oder erneut zu aktivieren, gehen Sie in Unisphere zu Einstellungen > Supportkonfiguration > CloudIQ.
Integrated: Überwachen mit dem integrierten ESRS-Client dieses Speichersystems (nur physische Bereitstellungen)	Diese Funktion ist in Ihrer Implementierung möglicherweise nicht verfügbar. Sie müssen den ESRS-Konfigurationsprozess durchlaufen und die ESRS-EULA akzeptieren. Sie können auswählen, ob Ihr Remoteserviceanbieter nur ausgehende oder eingehende/ausgehende Verbindungen unterstützen soll und ob Daten an CloudIQ gesendet werden sollen. Die Verwendung von Policy Manager und Proxyservern ist optional und gilt nur bei Auswahl von Integrated ESRS mit eingehender/ausgehender Verbindung. Nach der Auswahl können Sie einen Policy Manager und Proxyservereinstellungen konfigurieren. i ANMERKUNG: (Die ESRS-EULA wird nicht angezeigt, wenn sie im Rahmen der Bereitschaftsprüfung akzeptiert wurde.)
Remoteservices nicht aktivieren	Es wird davon abgeraten, Remoteservices nicht zu aktivieren. Das Aktivieren von Remoteservices beschleunigt die Problemdiagnose und verkürzt die Zeit bis zur Problembehebung.

Nächste Schritte

Testen Sie nach der Konfiguration von ESRS immer die Konnektivität. Dieser Prozess prüft, ob die Verbindung funktioniert, und führt dazu, dass das Unternehmen EMC das System erkennt und dessen Status von "Unbekannt" aktualisiert. Klicken Sie unter einer der folgenden Optionen auf **Testen**:

- **Dashboard > System > Service** unter **EMC Secure Remote Services**
- **Einstellungen > Supportkonfiguration > EMC Secure Remote Services**

Wenn Sie die ESRS-Konfigurationsinformationen ändern (erneut bereitstellen) müssen, wählen Sie **Ändern** aus. Der Assistent **Konfigurieren von ESRS** wird angezeigt, in dem Sie Änderungen vornehmen können.

i **ANMERKUNG:** Wenn der Status als **Im Übergangsstadium** verbleibt und sich nach einigen Minuten nicht ändert (der Zeit, die zum Testen der Verbindung erforderlich sein sollte), wenden Sie sich an den Online Support.

Konfigurieren von Integrated ESRS(nur physische Bereitstellungen)

Voraussetzungen

Sie haben **Integrated** in **EMC Secure Remote Services** ausgewählt und der Assistent zum **Konfigurieren von ESRS** wird angezeigt.

Info über diese Aufgabe

Gehen Sie zum Abschließen der Konfiguration von Integrated ESRS wie folgt vor:

Schritte

1. Akzeptieren Sie die ESRS-Anwenderlizenzvereinbarung (EULA).

Die ESRS-EULA muss akzeptiert werden, um Integrated ESRS konfigurieren und verwenden zu können.

 **ANMERKUNG:** Wenn die Lizenzvereinbarung während der Ausführung der Bereitschaftsprüfung akzeptiert wurde, bevor Sie ESRS konfigurieren, wird sie nicht erneut angezeigt.

2. Führen Sie eine Netzwerkprüfung durch. Wenn ein Proxyserver für das Speichersystem konfiguriert wurde, können Sie gegebenenfalls Änderungen vornehmen, indem Sie neben **Verbinden über einen Proxyserver** auf das Bleistiftsymbol klicken und die entsprechenden Informationen im angezeigten Dialogfeld eingeben.

 **ANMERKUNG:** Auf dieser Seite vorgenommene Änderungen gelten für die globalen Proxyeinstellungen für das Speichersystem.

Wenn Sie die Seite „Netzwerkprüfung“ übermitteln und die Serverdetails eingegeben wurden, werden Netzwerktests durchgeführt, um die Verbindung zwischen dem Gerät und dem Core-Node zu prüfen. Bei Auswahl von Integrated ESRS mit eingehender/ausgehender Verbindung werden die Back-end GAS (Global Access Server) ebenfalls in den Netzwerktests miteinbezogen. Die Netzwerkverbindung von ESRS zu allen erforderlichen Back-end-Servern wird geprüft. Wenn die Tests nicht erfolgreich verlaufen – was bedeutet, dass das Gerät keine Verbindung mit einigen oder allen Back-end-Servern herstellen kann –, werden die Ergebnisse im oberen Bereich der Seite des Assistenten angezeigt. Überprüfen Sie in diesem Fall, ob die entsprechenden Hosts und Ports (443 und 8443) der Firewall für Back-end-Server geöffnet sind. Alle Tests müssen erfolgreich sein. Sie sind verantwortlich für die Behebung von Proxyserver- und Firewallproblemen, die sich auf die Verbindung mit der ESRS-Infrastruktur auswirken.

3. Überprüfen Sie die Informationen zu den Kundenkontaktdaten. (Diese Überprüfung wird nur angezeigt und gilt nur, wenn Sie Integrated ESRS mit eingehender/ausgehender Verbindung ausgewählt haben.)

Klicken Sie zum Hinzufügen oder Ändern von Kontaktdaten des Kunden auf das Bleistiftsymbol neben **Kontaktinformationen** und geben Sie die entsprechenden Informationen in das angezeigte Dialogfeld ein. Diese Informationen sind erforderlich, um die ESRS-Konfiguration fortzusetzen. Stellen Sie sicher, dass die Informationen korrekt sind. Der Support verwendet diese Informationen, um auf Ihre Supportprobleme zu reagieren.

4. Führen Sie den E-Mail-Überprüfungsprozess aus.

Dieser Schritt fügt eine zusätzliche Authentifizierungsebene hinzu und stellt sicher, dass Sie der richtige Benutzer und autorisiert sind, ESRS auf dem Speichersystem zu aktivieren.

- a. Wählen Sie **Zugriffscodes senden** aus, um die Anforderung eines Zugriffscode zu initiieren.

Der erzeugte Zugriffscode ist ein PIN-Code mit 8 Ziffern, der vom Zeitpunkt der Erstellung 30 Minuten lang gültig ist. Sie müssen den Assistenten innerhalb dieses Zeitraums abschließen. Wenn Sie **Zugriffscodes senden** während des Zeitraums von 30 Minuten für dieses Verfahren erneut auswählen, wird der vorherige Code automatisch ungültig und Sie müssen den neuesten Code verwenden.

Anschließend wird ein Zugriffscode an die mit den Supportanmeldedaten des Supportkontos verknüpfte E-Mail-Adresse gesendet. Eine Meldung oben auf der Seite informiert Sie, dass Sie Ihren E-Mail-Posteingang prüfen sollten.

- b. Geben Sie den Zugriffscode, den Sie per E-Mail erhalten haben, in das Feld **Zugriffscodes** ein.

Wenn bei diesem E-Mail-Überprüfungsprozess oder beim Prozess der Einrichtung eines Supportkontos Probleme auftreten, können Supportmitarbeiter **Alternative nur für Support-Mitarbeiter** auswählen und ihre RSA-Anmeldedaten verwenden. In diesem Fall wird der E-Mail-Überprüfungsprozess übersprungen.

Wenn RSA-Support-Anmeldeinformationen verwendet werden, wird ein zweites Popup-Fenster angezeigt, in dem Supportmitarbeiter aufgefordert werden, die RSA-Support-Anmeldeinformationen erneut einzugeben.

5. (Optional, gilt nur, wenn Sie Integrated ESRS ausgewählt haben.) Wenn das Speichersystem Autorisierungsberechtigungen mithilfe eines Policy Managers festlegt, wählen Sie **Policy Manager** aus und geben Sie die entsprechenden Informationen

für den Policy Manager ein. Wenn der Policy Manager einen Proxyserver verwendet, wählen Sie **Proxyserver für Policy Manager verwenden** aus und geben Sie die entsprechenden Informationen für den Proxyserver ein. Wenn Sie keinen Policy Manager verwenden, fahren Sie mit Schritt 6 fort.

Das Dialogfeld **Policy Manager** wird angezeigt. Wenn Sie einen Policy Manager verwenden, muss dieser installiert und betriebsbereit sein. Es wird empfohlen, die SSL-Stärke auf „Hoch“ festzulegen.

6. Das Kontrollkästchen **Daten an CloudIQ senden** ist standardmäßig ausgewählt (aktiviert). Deaktivieren Sie das Kontrollkästchen, um das Versenden von Daten an CloudIQ zu deaktivieren (nicht empfohlen).

CloudIQ kann nach Abschluss der ESRS-Konfiguration über **Einstellungen > Supportkonfiguration > CloudIQ** aktiviert oder deaktiviert werden.

Sobald ESRS erfolgreich konfiguriert wurde, werden die entsprechenden Zertifikate installiert, ESRS wird bereitgestellt und beim Supportcenter registriert und die Seite **Ergebnisse** wird angezeigt.

7. Überprüfen Sie den Bereich **Übersicht** auf der Seite **Service (Dashboard > System > Service)**, um den Status der ESRS-Verbindung anzuzeigen.

Nächste Schritte

Testen Sie nach der Konfiguration von ESRS immer die Konnektivität. Dieser Prozess prüft, ob die Verbindung funktioniert, und führt dazu, dass EMC das System erkennt und dessen Status von "Unbekannt" aktualisiert. Klicken Sie unter einer der folgenden Optionen auf **Testen**:

- **Dashboard > System > Service** unter **EMC Secure Remote Services**
- **Einstellungen > Supportkonfiguration > EMC Secure Remote Services**

 **ANMERKUNG:** Wenn der Status als "Im Übergangsstadium" zu verbleiben scheint und sich nicht nach 20 Minuten ändert (der Zeit, die zum Testen der Verbindung erforderlich sein sollte), wenden Sie sich an den Support.

 **ANMERKUNG:** Policy Manager kann nach der Konfiguration von ESRS konfiguriert oder geändert werden, indem Sie auf die Option **Bearbeiten** auf der Seite **Einstellungen > Supportkonfiguration > EMC Secure Remote Support Services** klicken.

Wenn Sie die ESRS-Konfigurationsinformationen ändern (erneut bereitstellen) müssen, wählen Sie **Ändern** aus. Der Assistent **Konfigurieren von ESRS** wird angezeigt, in dem Sie Änderungen vornehmen können.

- Für Integrated ESRS mit nur ausgehender Verbindung:
 - Wenn ein Proxyserver für das Speichersystem konfiguriert wurde, können Sie gegebenenfalls Änderungen vornehmen, indem Sie neben **Verbinden über einen Proxyserver** auf das Bleistiftsymbol klicken und die entsprechenden Informationen im angezeigten Dialogfeld eingeben.
 - Sie können den ESRS-Typ in „Integrated (eingehend/ausgehend)“ oder „Centralized“ ändern und die entsprechenden Informationen angeben.
- Für Integrated ESRS mit eingehender/ausgehender Verbindung:
 - Wenn ein Proxyserver für das Speichersystem konfiguriert wurde, können Sie gegebenenfalls Änderungen vornehmen, indem Sie neben **Verbinden über einen Proxyserver** auf das Bleistiftsymbol klicken und die entsprechenden Informationen im angezeigten Dialogfeld eingeben.
 - Der Informationsbereich **Kontaktinformationen und Systemstandort überprüfen** im ESRS-Assistenten wird mit einer Bearbeitungsoption (Stiftsymbol) neben **Kontaktinformationen** und **Systeminformationen** aktiviert. Es können alle Systeminformationen mit Ausnahme der Standort-ID-Nummer aktualisiert werden.
 - Sie können den ESRS-Typ von „Integrated (eingehend/ausgehend)“ in „Centralized“ ändern und die entsprechenden Informationen angeben.

 **ANMERKUNG:** Sobald Integrated ESRS für eingehende/ausgehende Verbindung konfiguriert ist, kann es nicht wieder zu nur ausgehender Verbindung geändert werden.

Konfiguration von Remotesupport über die CLI

In diesem Kapitel wird der Prozess zum Provisioning der ESRS-Funktion mithilfe der UEMCLI erläutert. Eine vollständige Dokumentation dieser und zugehöriger Befehle finden Sie im *Benutzerhandbuch zur Unisphere-Befehlszeilenoberfläche*.

Folgende Themen werden behandelt:

Themen:

- Overview of configuring Remote Support using the CLI
- Konfigurieren oder Ändern der Einstellungen für Support und Proxyserver
- Konfigurieren oder Ändern der Systemkontaktinformationen
- Konfigurieren oder Ändern der Supportanmeldedaten
- Configure Centralized ESRS with the Unisphere CLI
- Configure Integrated ESRS with the Unisphere CLI
- Konfigurieren oder Ändern der Einstellungen für Policy Manager und Proxyserver

Overview of configuring Remote Support using the CLI

Users have the option to provision Integrated ESRS with the UEMCLI.

Voraussetzungen

This topic provides an overview of the chronological steps required for configuring ESRS using the CLI. Refer to the subsequent sections of this chapter for the detailed command usage and examples for each of these steps.

Schritte

1. Optionally, configure the use of a proxy server with the `/sys/support/config set` command.
2. Set the Customer Contact Data Information using the `/sys/info set` command.
3. Set your support account credentials using the `sys/support/account set` command.
4. Enable and configure the type of ESRS you want to use:
 - a. For Centralized ESRS:
 - i. Enable ESRS and configure settings using the `/sys/support/esrsc set` command.
 - ii. Check the network connectivity from the primary or secondary Centralized ESRS gateway to the Dell EMC servers using the `/sys/support/esrsc checkNetwork` command.
 - iii. After Centralized ESRS is enabled, test the configuration by sending a test Call Home to Dell EMC using the `/sys/support/esrsc testcommand`.
 - b. For Integrated ESRS:
 - i. Check that the support account associated with your system is configured and ready for ESRS connectivity using the `/sys/support/esrsi checkSupportAccountReadiness` command.
 - ii. Check the network connectivity from the Integrated ESRS client to the Dell EMC servers using the `/sys/support/esrsi checkNetwork` command.
 - iii. Enable ESRS and configure settings using the `/sys/support/esrsi set` command. This command allows you to accept the EULA and select the type of Integrated ESRS--one-way or two-way.
 - iv. Optionally request an access code to be sent to the email account user using the `/sys/support/esrsi requestAccessCode` command.

 **ANMERKUNG:** The access code is for additional verification purposes and expires after 30 minutes.

- v. If you requested an access code, validate the access code you received using the `/sys/support/esrsi validateAccessCode -accessCode` command.
 - vi. Test the ESRS configuration using the `/sys/support/esrsi testcommand`.
5. Optionally, configure the Policy Manager and policy proxy server attributes using the `/sys/support/esrsi/policymgr set` command.

Konfigurieren oder Ändern der Einstellungen für Support und Proxyserver

Ändern Sie die Attribute der Supportkonfiguration.

Format

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

Aktionsqualifizierer

Qualifizierer	Beschreibung
<code>-enableSupportProxy</code>	Gibt an, ob der Proxyserver aktiviert oder deaktiviert werden soll. Gültige Werte: • yes • no
<code>-supportProxyAddr</code>	Geben Sie den Namen oder die IP-Adresse des Support-Services-Proxyservers an.
<code>-supportProxyPort</code>	Geben Sie den Port des Support-Services-Proxyservers an.
<code>-supportProxyUser</code>	Geben Sie den Benutzernamen eines Kontos auf dem Support-Services-Proxyserver an.
<code>-supportProxyPasswd</code>	Geben Sie das Passwort für das Konto des Support-Services-Proxyservers an.
<code>-supportProxyPasswdSecure</code>	Gibt das Passwort im sicheren Modus an – der Benutzer wird aufgefordert, das Passwort einzugeben.
<code>-supportProxyProtocol</code>	Geben Sie für die Kommunikation mit dem Support-Services-Proxyserver das verwendete Protokoll an. Gültige Werte: • http • socks <i>i</i> ANMERKUNG: Bei den Werten wird zwischen Groß- und Kleinschreibung unterschieden.
<code>-autoUpdateContracts</code>	Geben Sie an, ob das System seine Serviceverträge automatisch einmal pro Woche aktualisiert. Gültige Werte: • yes • no <i>i</i> ANMERKUNG: Bei den Werten wird zwischen Groß- und Kleinschreibung unterschieden.
<code>-enableCloudMgmt</code>	Geben Sie an, ob das Senden von Daten an CloudIQ auf dem System aktiviert ist. Gültige Werte: • yes • no

Qualifizierer	Beschreibung
	 ANMERKUNG: Bei den Werten wird zwischen Groß- und Kleinschreibung unterschieden.

Beispiel

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

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

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

Operation completed successfully.
```

Konfigurieren oder Ändern der Systemkontaktinformationen

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

Format

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

Aktionsqualifizierer

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

Beispiel

Mit dem folgenden Befehl können Sie die folgenden Systeminformationen ändern:

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

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

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

Konfigurieren oder Ändern der Supportanmeldedaten

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

Format

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

Aktionsqualifizierer

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

Beispiel

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

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

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

Configure Centralized ESRS with the Unisphere CLI

The following sections describe how to configure and test Centralized ESRS using the CLI.

Aktivieren oder Ändern von Centralized ESRS

Aktivieren oder ändern Sie die Konfiguration von Centralized ESRS.

Format

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

Aktionsqualifizierer

Qualifizierer	Beschreibung
-enable	Gibt an, ob Centralized ESRS aktiviert oder deaktiviert werden soll. Gültige Werte: • yes • no  ANMERKUNG: Wenn ESRS deaktiviert ist, können andere Parameter nicht geändert werden.
-address	Gibt die IP-Adresse des Centralized ESRS VE-Servers an, mit dem die Verbindung hergestellt wird.
-port	Gibt die Nummer des Ports an, der für eine Verbindung zum Centralized ESRS verwendet wird.
-secondAddress	Geben Sie den Netzwerknamen oder die IP-Adresse des sekundären Centralized ESRS VE-Servers an.
-secondPort	Geben Sie die Nummer des Ports an, der für eine Verbindung zum primären Centralized ESRS VE-Server verwendet wird.  ANMERKUNG: Das sekundäre Gateway muss sich im selben Cluster wie der primäre Gateway befinden.

Beispiel 1

Der folgende Befehl spezifiziert die Parameter des Centralized ESRS:

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

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

Operation completed successfully.
```

Beispiel 2

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

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

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

Operation completed successfully.
```

Prüfen der Netzwerkverbindung von Centralized ESRS

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

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

Format

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

Aktionsqualifizierer

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

Beispiel

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

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

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

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

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

Testen des Centralized EMC Secure Remote Support

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

Format

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

Beispiel 1

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

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

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

Beispiel 2

Das folgende Beispiel zeigt die erfolgreiche Ausführung dieses Befehls.

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

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

```
Operation completed successfully.
```

 **ANMERKUNG:** Ein erfolgreicher Vorgang weist darauf hin, dass der Test erfolgreich durchgeführt wurde und nicht, dass die Verbindung selbst erfolgreich war. Anders gesagt: Es wird darauf hingewiesen, dass CallHome gesendet wurde, aber

nicht, ob es vom EMC Secure Remote Support-Server empfangen wurde. Zum Prüfen des Status des tatsächlichen Tests melden Sie sich bei Service 360 an, um die aktuellen Service-Requests (SRs) einzusehen. Wenn CallHome vom EMC Secure Remote Support-Server empfangen wurde, wird der Verbindungstest als automatisch geschlossener CallHome-SR angezeigt.

Configure Integrated ESRS with the Unisphere CLI

The following sections describe how to configure and test Integrated ESRS using the CLI.

Prüfen der Bereitschaft der Supportanmeldedaten für Integrated EMC Secure Remote Support

Vor dem Konfigurieren des EMC Secure Remote Support überprüfen Sie, ob die für Ihr System konfigurierten Anmeldedaten des Supportkontos ordnungsgemäß in der Online Support-Datenbank registriert sind.

Format

```
/sys/support/esrsi checkSupportAccountReadiness
```

Beispiel

Das folgende Beispiel zeigt, dass der Befehl erfolgreich ausgeführt wird, wobei die Supportanmeldedaten ordnungsgemäß konfiguriert sind.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/esrsi  
checkSupportAccountReadiness
```

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

```
Operation completed successfully.
```

Aktivieren oder Ändern von Integrated ESRS

Aktivieren oder ändern Sie die Konfiguration von Integrated ESRS.

Format

```
/sys/support/esrsi set {-enable {yes|no}}{-acceptEula yes|-type {oneWay|twoWay}}
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-enable	Gibt an, ob ESRS aktiviert, erneut aktiviert oder deaktiviert werden soll. Gültige Werte: • yes • no  ANMERKUNG: Wenn ESRS deaktiviert ist, können andere Parameter nicht geändert werden.
-acceptEula	Gibt an, ob die Endbenutzerlizenz akzeptiert wird. Gültiger Wert: • yes

Qualifizierer	Beschreibung
	 ANMERKUNG: Wenn die ESRS-EULA nicht akzeptiert wird, kann für Integrated ESRS nichts konfiguriert werden.
-type	Gibt an, welche Art von Integrated ESRS verwendet werden soll. Gültige Werte: • oneWay (nur ausgehend) • twoWay (Ausgehend/Eingehend) (Standard)

Beispiel

Mit dem folgenden Befehl wird Integrated ESRS aktiviert, die EULA akzeptiert und der Typ des Integrated ESRS festgelegt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/esrsi set -enable yes -acceptEula yes -type oneWay
```

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

Operation completed successfully.
```

Prüfen der Netzwerkverbindung von Integrated ESRS

Prüfen Sie die Netzwerkverbindung von dem Integrated ESRS-Client zu den EMC Servern. Wenn ein Fehler auftritt, kann Integrated ESRS nicht aktiviert werden.

Format

```
/sys/support/esrsi checkNetwork
```

Beispiel

Mit dem folgenden Befehl wird die Netzwerkverbindung für Integrated ESRS angezeigt:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/esrsi checkNetwork
```

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

Operation failed. Error code: 0x6400bc8
Remote Support cannot be enabled at this time, because the system cannot contact some
required EMC servers: esrghoprd02.emc.com:443/8443,esrghoprd03.emc.com:8443/443. Please
refer to online help for this error code to resolve the issue. (Error Code:0x6400bc8)
```

Anfordern eines Zugriffscode für Integrated ESRS

Fordern Sie einen Zugriffscode für Integrated ESRS an. Dieser Zugriffscode wird per E-Mail an den Benutzer des E-Mail-Kontos gesendet. Der Zugriffscode ist nur 30 Minuten lang gültig. Bei diesem Prozess wird eine zusätzliche Authentifizierungsstufe hinzugefügt und sichergestellt, dass Sie der richtige Benutzer und autorisiert sind, ESRS auf dem Speichersystem zu aktivieren.

Format

```
/sys/support/esrsi requestAccessCode
```


Beispiel

Mit dem folgenden Befehl wird die Anforderung eines Zugriffscodes als Teil des E-Mail-Überprüfungsprozess für Integrated ESRS gesendet:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/esrsi requestAccessCode
```

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

```
1:      Recipient email address = sxxxxxxx@mail.com
```

Validieren des Zugriffscodes für Integrated ESRS

Validieren Sie den Zugriffscode für Integrated ESRS, der per E-Mail an den Benutzer des E-Mail-Kontos gesendet wurde. Der Zugriffscode ist nur 30 Minuten lang gültig.

Format

```
/sys/support/esrsi validateAccessCode -accessCode <value>
```

Beispiel

Mit folgendem Befehl wird die unten gezeigte Antwort zur Validierung des Zugriffscodes ausgegeben:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/esrsi validateAccessCode  
-accessCode 76507252
```

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

```
Operation completed successfully.
```

Testen von Integrated EMC Secure Remote Support

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

Format

```
/sys/support/esrsi test
```

Beispiel 1

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

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

```
Operation failed. Error code: 0x6400bad  
Not supported since Integrated Secure Remote Support is not enabled. (Error  
Code:0x6400bad)
```

Beispiel 2

Das folgende Beispiel zeigt die erfolgreiche Ausführung dieses Befehls.

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

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

Operation completed successfully.
```

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

Konfigurieren oder Ändern der Einstellungen für Policy Manager und Proxyserver

Konfigurieren oder ändern Sie die Attribute von Policy Manager und Proxyserver.

Format

```
/sys/support/esrsi/policymgr set [ -enable { yes | no } ] [ -address <value> ] [ -port <value> ] [ -protocol { http | https } ] [ sslStrength { high | medium | low } ] [ -enableProxy { yes | no } ] [ -proxyAddr <value> ] [ -proxyPort <value> ] [ -proxyUser <value> { -proxyPasswd <value> | -proxyPasswdSecure } ] [ -proxyProtocol { http | socks } ]
```

Aktionsqualifizierer

Qualifizierer	Beschreibung
-enable	Gibt an, ob der ESRS Policy Manager aktiviert oder deaktiviert werden soll. Gültige Werte: • yes • no ANMERKUNG: Wenn der ESRS Policy Manager deaktiviert ist, können andere Policy Manager-Parameter nicht geändert werden.
-address	Gibt die Adresse des Policy Manager an, die für Integrated ESRS konfiguriert werden soll.
-port	Gibt die Portnummer des Policy Manager-Servers an, die für Integrated ESRS konfiguriert werden soll.
-protocol	Gibt das Protokoll an, das der Policy Manager-Server verwenden soll.
-sslStrength	Gibt die SSL-Stärke des ESRS Policy Manager an (gilt nur, wenn das Protokoll HTTPS ist). Gültige Werte: • high • medium • low
-enableProxy	Gibt an, dass der Policy Manager-Proxyserver aktiviert werden soll. Gültige Werte: • yes • no

Qualifizierer	Beschreibung
	 ANMERKUNG: Wenn der ESRS Policy Manager deaktiviert ist, können andere Policy Manager-Proxyserverparameter nicht geändert werden.
-proxyAddr	Gibt die Adresse des Policy-Proxyservers an.
-proxyPort	Gibt die Portnummer des Policy-Proxyservers an.
-proxyUser	Gibt den Benutzernamen für das Konto auf dem Policy Manager-Proxyserver an.
-proxyPasswd	Gibt das Passwort für das Konto auf dem Policy Manager-Proxyserver an.
-proxyProtocol	Gibt das Protokoll an, das der Policy Manager-Proxyserver verwenden soll.

Beispiel

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/esrsi/policymgr set -enable
no
```

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

Operation completed successfully.
```

Troubleshooting

The service command **svc_esrs_ve** allows the user to perform basic tasks on ESRS VE, such as checking the status of the service and network or cleaning up the configuration. For more information, refer to the *Dell EMC Unity™ Service Commands Technical Notes* document.

This chapter provides information about the probable causes of problems that you may encounter when enabling and running the ESRS feature and the recommended actions to take to resolve them.

Topics include:

Themen:

- [ESRS kann nicht aktiviert werden](#)
- [ESRS hat ein Verbindungsproblem gemeldet](#)

ESRS kann nicht aktiviert werden

Wenn die ESRS-Funktion nicht aktiviert werden kann, finden Sie im Folgenden eine Liste der möglichen Ursachen sowie die Schritte, mit denen Sie das Problem beheben können.

Tabelle 1. Problemlösung: Die ESRS-Funktion kann nicht aktiviert werden.

Mögliche Ursache	Empfohlene Aktion
Sie haben möglicherweise falsche Anmeldedaten angegeben oder kein Upgrade auf ein Supportkonto mit vollständigem Zugriff vorgenommen. Es kann bis zu 48 Stunden dauern, bevor Ihr anfänglich erstelltes Konto mit Supportanmeldedaten mit vollständigem Zugriff aktiviert wird.	Überprüfen Sie Folgendes: • Die von Ihnen angegebenen Anmeldedaten sind identisch mit denen, die bei der Registrierung des Speichersystems beim Online Support verwendet wurden. • Für Ihr Konto wurde ein Upgrade auf ein Supportkonto mit vollständigen Zugriffsrechten (registrierter Benutzer mit Zugriff auf den Standort, an dem sich das installierte Speichersystem befindet) durchgeführt. ANMERKUNG: Melden Sie sich beim Online Support (https://Support.EMC.com) an, um festzustellen, ob die angegebenen Anmeldedaten gültig sind. Falls Sie Ihr Speichersystem noch nicht registriert haben, führen Sie die Registrierung jetzt durch. Sollten Sie nach Ausführung dieser Schritte weiterhin keinen Zugriff auf die Website erhalten, senden Sie eine E-Mail an support@emc.com.
Die von Ihnen eingegebenen Anmeldedaten sind gültig, sie sind jedoch nicht mit der Standort-ID des Standorts verknüpft, an dem sich das Speichersystem befindet. Eine Standort-ID wird in Supportsystemen für jeden Standort innerhalb Ihres Unternehmens erstellt, an dem EMC Produkte installiert sind.	Überprüfen Sie die Nummer Ihrer Standort-ID auf der Online Support-Website: 1. Melden Sie sich mit Ihren Anmeldedaten beim Online Support an. 2. Wählen Sie Servicecenter aus. 3. Klicken Sie auf der Seite „Servicecenter“ unter „Standorte und Verträge“ auf Standort verwalten. 4. Vergewissern Sie sich, dass der Standort, an dem das VNXe-Gerät installiert ist, im Bereich „Meine Sites“ aufgeführt ist. ANMERKUNG: Sie können auch nach einer Site suchen und diese Site der Liste „Meine Sites“ hinzufügen. Wenn keine Standort-ID verfügbar oder die richtige Standort-ID nicht aufgeführt ist, müssen Sie Ihren Vertriebsmitarbeiter

Tabelle 1. Problemlösung: Die ESRS-Funktion kann nicht aktiviert werden. (fortgesetzt)

Mögliche Ursache	Empfohlene Aktion
	vor Ort benachrichtigen, um eine ID anzufordern. Wenn ein Partner die Installation ausführt, muss er die Anforderung entweder an die Install Base Group oder an seinen Vertriebsmitarbeiter übermitteln. Wenn das Unity-System unter der falschen Standort-ID aufgeführt ist, finden Sie unter <i>KB 489840</i> weitere Informationen zum Ändern der Standort-ID, die dem System zugeordnet ist.

Verwenden von RSA-Anmeldedaten zur Konfiguration von ESRS

Es gibt einige Fälle, in denen Ihre Kundensupport-Anmeldedaten nicht vollständig eingerichtet oder auf den Servern des Back-End-Support validiert wurden. In 4.x-Versionen wurde dadurch die Konfiguration von ESRS verhindert. Während des Besuchs vor Ort oder über eine Remote-Telefonkonferenz können Supportmitarbeiter Ihre RSA-Anmeldedaten eingeben, um die Anforderung eines vollständig konfigurierten Kundensupportkontos zu umgehen.

ESRS hat ein Verbindungsproblem gemeldet

Wenn der ESRS-Service nicht mehr verbunden ist, finden Sie im Folgenden eine Liste der möglichen Ursachen sowie die Aktionen, mit denen Sie das Problem beheben können.

Tabelle 2. Problembehebung: Die ESRS-Funktion ist nicht mehr verbunden.

Mögliche Ursache	Empfohlene Aktion
Der DNS-Server (Domain Name System) wird nicht ausgeführt oder ist nicht vorhanden.	Gehen Sie folgendermaßen vor: 1. Vergewissern Sie sich, dass der in Unisphere konfigurierte DNS-Server korrekt angegeben ist. 2. Aktivieren Sie SSH, melden Sie sich als Dienst an, und führen Sie den Befehl ping aus, um sicherzustellen, dass das Speichersystem die IP-Adresse des DNS-Servers pingen kann. 3. Verwenden Sie das Nslookup-Tool zusammen mit einem der ESRS-Hostnamen, um festzustellen, ob der DNS-Server diesen Hostnamen korrekt auflösen kann. Sollte dies nicht der Fall sein oder wenn der Ping-Test für den DNS-Server fehlschlägt, wenden Sie sich an Ihren Netzwerkadministrator.
Ein Policy Manager ist konfiguriert, aber nicht erreichbar.	Überprüfen Sie, ob der Policy Manager online ist. Rufen Sie in Unisphere Einstellungen > Supportkonfiguration > EMC Secure Remote Service auf und überprüfen Sie, ob die Policy Manager-Einstellungen für Protokoll, Port und Netzwerkname/IP-Adresse richtig konfiguriert sind.
Die ESRS-Verbindung ist funktionsfähig, Sie können jedoch keine Remote-Sitzungen starten. Möglicherweise ist der Global Access Server (GAS) nicht erreichbar. GAS-Server werden nur für Remote-Sitzungen verwendet.	Gehen Sie folgendermaßen vor: • Wenn die Verbindung einen Kunden-Proxyserver umfasst, vergewissern Sie sich, dass er erreichbar ist. • Überprüfen Sie, ob die entsprechenden Firewallhosts und -ports (443 und 8443) für EMC geöffnet sind.
Ein mit ESRS Centralized-Implementierung konfiguriertes System hat Probleme mit HTTP-Keep-Alive und erscheint nicht verbunden zu sein.	Vergewissern Sie sich, dass der Port 9443 offen ist, um REST-API-Aufrufe aus dem Speichersystem zum ESRS Gateway zuzulassen.