Dell EMC PowerStore

Sicherheitskonfigurationsleitfaden

1.x

July 2020
Rev. A02

Anmerkungen, Vorsichtshinweise und Warnungen

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

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

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

Inhaltsverzeichnis

Weitere Ressourcen **5**

Kapitel 1: Authentifizierung und Zugriff **6**
Authentifizieren und Verwalten von Nutzerkonten, Rollen und Berechtigungen 6
Werkseitige Standardverwaltung 6
Sitzungsregeln 7
Anforderungen an Nutzername und Kennwort 7
ESXi-Kennwörter 7
Rollen und Berechtigungen 8
Nutzerkontoverwaltung basierend auf Rollenberechtigungen 11
Zurücksetzen der Kennwörter für Administrator- und Servicekonten 11
Zertifikate 14
Anzeigen von Zertifikaten 14
Sichere Kommunikation zwischen PowerStore-Appliances in einem Cluster 14
Sichere Kommunikation für Replikation und Datenimport 14
Unterstützung für die vSphere Storage API for Storage Awareness 15
CHAP-Authentifizierung 16
Konfigurieren von CHAP 17
Externer SSH-Zugriff 17
Konfigurieren des externen SSH-Zugriffs 17
SSH Sitzungen 18
Kennwort für das Servicekonto 18
SSH-Autorisierung 18
Appliance-Serviceskripts 18
Ethernet-Serviceportschnittstelle und IPMItool für Appliance-Node 19
NFS secure 19
Sicherheit auf Dateisystemobjekten 20
Dateisystemzugriff in einer Multiprotokollumgebung 21
Benutzerzuordnung 21
Zugriffs-Policies für NFS, SMB und FTP 26
Zugangsdaten für Sicherheit auf Dateiebene 26
Überblick über Common Antivirus Agent (CAVA) 28
Codesignierung 28

Kapitel 2: Kommunikationssicherheitseinstellungen **29**
Portnutzung 29
Appliance-Netzwerkports 29
Appliance-Netzwerkports in Bezug auf Dateien 31
Netzwerkports in Verbindung mit PowerStore X-Modell-Appliances 34

Kapitel 3: Auditing **36**
Auditing 36

Kapitel 4: Datensicherheitseinstellungen **37**

Data-at-Rest-Verschlüsselung....37
Verschlüsselungsaktivierung....37
Verschlüsselungsstatus....37
Key-Management....38
Keystore-Backupdatei....38
Neuverwendung eines Laufwerks in einer Appliance mit aktivierter Verschlüsselung....39
Austauschen eine Basisgehäuses und von Nodes bei einem System mit aktivierter Verschlüsselung....39
Zurücksetzen einer Appliance auf die Werkseinstellungen....39

Kapitel 5: Sichere Wartungseinstellungen....41
Funktionsbeschreibung von SupportAssist™....41
SupportAssist-Optionen....42
SupportAssist Gateway Connect-Optionen....43
SupportAssist Direct Connect-Optionen....43
Voraussetzungen für SupportAssist Gateway Connect....44
Voraussetzungen für SupportAssist Direct Connect....44
Konfigurieren von SupportAssist....44
Konfigurieren von SupportAssist....44

Anhang A: TLS-Chiffren....46
Unterstützte TLS-Cipher Suites....46

Vorwort

Es werden regelmäßig neue Software- und Hardwareversionen veröffentlicht, um das Produkt kontinuierlich zu verbessern. Einige in diesem Dokument beschriebene Funktionen werden eventuell nicht von allen Versionen der von Ihnen derzeit 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 auf der Seite mit der PowerStore-Dokumentation unter www.dell.com/powerstoredocs.

- **Fehlerbehebung:**

  Informationen zu Produkten, Softwareupdates, Lizenzierung und Service finden Sie unter www.dell.com/support auf der entsprechenden Produktsupportseite.

- **Technischer Support**

  Für technischen Support und Serviceanfragen gehen Sie zu www.dell.com/support und rufen die Seite **Serviceanfragen** auf. 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.

1

Authentifizierung und Zugriff

Dieses Kapitel enthält die folgenden Informationen:

Themen:

- Authentifizieren und Verwalten von Nutzerkonten, Rollen und Berechtigungen
- Zertifikate
- Sichere Kommunikation zwischen PowerStore-Appliances in einem Cluster
- Sichere Kommunikation für Replikation und Datenimport
- Unterstützung für die vSphere Storage API for Storage Awareness
- CHAP-Authentifizierung
- Konfigurieren von CHAP
- Externer SSH-Zugriff
- Konfigurieren des externen SSH-Zugriffs
- NFS secure
- Sicherheit auf Dateisystemobjekten
- Dateisystemzugriff in einer Multiprotokollumgebung
- Überblick über Common Antivirus Agent (CAVA)
- Codesignierung

Authentifizieren und Verwalten von Nutzerkonten, Rollen und Berechtigungen

Die Authentifizierung des Zugriffs auf den Cluster wird mit den Zugangsdaten eines Nutzerkontos durchgeführt. Nutzerkonten werden erstellt und anschließend über die Seite **Users** gemanagt, auf die im PowerStore Manager über **Settings** > **Users** > **Users** zugegriffen werden kann. Die erforderlichen Autorisierungen hängen von der dem Nutzerkonto zugewiesenen Rolle ab. Wenn der Nutzer die Netzwerkadresse des Clusters als URL in einen Webbrowser eingibt, wird ihm eine Anmeldeseite angezeigt, auf der er sich als lokaler Nutzer authentifizieren kann. Die vom Nutzer eingegebenen Zugangsdaten werden geprüft und eine Sitzung wird auf dem System erstellt. Anschließend kann der Nutzer das Cluster innerhalb der Möglichkeiten der ihm zugewiesenen Rolle überwachen und managen.

Der Cluster authentifiziert seine Nutzer durch die Validierung von Nutzernamen und Kennwörtern über eine sichere Verbindung mit dem Managementserver.

Werkseitige Standardverwaltung

Ihre Appliance weist standardmäßige werkseitige Nutzerkontoeinstellungen für den Erstzugriff und die Erstkonfiguration der Appliance auf.

ANMERKUNG: Bei den Versionen 1.0.x wird empfohlen, PowerStore zunächst über die PowerStore Manager-Benutzeroberfläche und nicht über die API-, CLI-, oder Serviceskriptschnittstellen zu konfigurieren. Dadurch wird sichergestellt, dass alle Standardkennwörter geändert werden.

Kontotyp	Benutzername	Kennwort	Rechte
Systemmanagement	admin	Password123#	Administratorrechte für das Zurücksetzen von Standardkennwörtern, die Konfiguration von Appliance-Einstellungen und das Verwalten von Nutzerkonten
Service	Service	Service	Durchführen von Servicevorgängen. **ANMERKUNG:** Der Servicenutzer ist für den SSH-Zugriff (Secure Shell) gedacht. Sie können

Kontotyp	Benutzername	Kennwort	Rechte
			sich nicht als Servicenutzer bei PowerStore Manager anmelden.

Sitzungsregeln

Sitzungen auf dem Cluster weisen die folgenden Eigenschaften auf:

- Ablaufzeit = 1 Stunde

  ANMERKUNG: Der Benutzer wird automatisch vom Cluster abgemeldet, nachdem die Sitzung eine Stunde lang inaktiv war.
- Das Sitzungs-Timeout ist nicht konfigurierbar.

Anforderungen an Nutzername und Kennwort

Nutzernamen des Systemkontos müssen die folgenden Anforderungen erfüllen:

Einschränkung	Nutzername
Struktur	Muss mit einem alphanumerischen Zeichen beginnen und enden.
Fall	Bei allen Nutzernamen wird zwischen Groß-und Kleinschreibung unterschieden.
Mindestanzahl an alphanumerischen Zeichen	1
Maximale Anzahl an alphanumerischen Zeichen	64
Unterstützte Sonderzeichen	. (Punkt)

Kennwörter des Systemkontos müssen die folgenden Anforderungen erfüllen:

Einschränkung	Passwortanforderungen
Mindestanzahl an Zeichen	8
Mindestanzahl an großgeschriebenen Zeichen	1
Mindestanzahl an kleingeschriebenen Zeichen	1
Mindestanzahl an numerischen Zeichen	1
Mindestanzahl an Sonderzeichen • Unterstützte Zeichen: ! @ # $ % ^ * _ ~ ? **ANMERKUNG:** Das Kennwort darf kein einfaches Anführungszeichen ('), kaufmännisches und-Zeichen (&) oder Leerzeichen enthalten.	1
Maximale Anzahl an Zeichen	40

ANMERKUNG: Die letzten fünf Kennwörter können nicht wiederverwendet werden. Ein vorheriges Kennwort kann wiederverwendet werden, nachdem es fünf Mal übersprungen wurde.

ESXi-Kennwörter

Das standardmäßige Root-Kennwort für ESXi auf einer PowerStore X model-Appliance hat das folgende Format: ***<Service_Tag>*_123!**, wobei *<Service_Tag>* die 7-stellige Dell Service-Tag-Nummer für die Appliance ist.

Ändern Sie das standardmäßige ESXi-Kennwort erst, nachdem die erste Clusterkonfiguration abgeschlossen ist. Weitere Informationen zum Ändern eines ESXi-Kennworts finden Sie in der Dokumentation zu VMware ESXi.

VORSICHT: Es ist wichtig, dass Sie das ESXi-Kennwort nicht verlieren. Wenn ESXi ausfällt und Sie nicht über das Kennwort verfügen, muss die Appliance neu initialisiert werden. Diese Vorgehensweise ist für ESXi normal, allerdings kann die Neuinitialisierung aufgrund eines verlorenen Kennworts zu Datenverlust führen.

VORSICHT: Das standardmäßige ESXi-Kennwort wird für jede PowerStore X model-Appliance eindeutig konfiguriert. Das Kennwort wird zur Authentifizierung mit dem ESXi-Host verwendet, wenn die Nodes in der Appliance einem vCenter-Cluster hinzugefügt werden. Wenn Sie das Standardkennwort vor der vollständigen Konfiguration des Clusters ändern, müssen Sie die Appliance erneut initialisieren.

Rollen und Berechtigungen

Mithilfe von rollenbasierten Zugriffskontrollen können Nutzern verschiedene Berechtigungen zugewiesen werden. Dies bietet die Möglichkeit, Administratorrollen aufzuteilen, um sie besser an Fähigkeiten und Verantwortlichkeiten auszurichten.

Das System unterstützt die folgenden Rollen und Berechtigungen:

ANMERKUNG: Ein ✓ in einem Feld kennzeichnet eine unterstützte Berechtigung für diese Rolle, während ein unmarkiertes Feld angibt, dass die Berechtigung für diese Rolle nicht unterstützt wird.

Aufgabe	Operator	VM-Administrator	Sicherheitsadministrator	Speicheradministrator	Administrator
Ändern des lokalen Systemkennworts	✓	✓	✓	✓	✓
Anzeigen von Systemeinstellungen, Status und Performance-Informationen	✓		✓	✓	✓
Ändern der Systemeinstellungen					✓
Erstellen, Ändern, Löschen von Ressourcen und Schutz-Policys und Aktivieren/Deaktivieren von SSH				✓	✓
Verbinden mit vCenter		✓		✓	✓
Anzeigen einer Liste mit lokalen Konten			✓		✓
Hinzufügen, Löschen oder Ändern eines lokalen Kontos			✓		✓
Anzeigen von Systemspeicherinformationen mithilfe von vCenter Server, der mit dem VASA-Anbieter des Systems verbunden ist, und Registrierung/erneute Registrierung der VMware-Zertifizierungsstelle (VMCA)/des Zertifikats der Zertifizierungsstelle		✓			✓

Rollen und Berechtigungen in Bezug auf Dateien

Das System unterstützt die folgenden Rollen und Berechtigungen in Bezug auf Dateien:

ANMERKUNG: Ein ✓ in einem Feld kennzeichnet eine unterstützte Berechtigung für diese Rolle, während ein unmarkiertes Feld angibt, dass die Berechtigung für diese Rolle nicht unterstützt wird.

Aufgabe	Operator	VM-Administrator	Sicherheitsadministrator	Speicheradministrator	Administrator
Sehen Sie sich Folgendes an: • Dateisystemwarnmeldungen • NAS-Serverliste • Dateisystemliste • Liste der Dateinutzerquoten • Liste der Routen für die Dateischnittstelle • Liste der Dateischnittstellen • Liste der SMB-Shares • NFS-Exportliste	✓		✓	✓	✓
Sehen Sie sich Folgendes an: • Liste von Datei-DNS-Servern oder einen bestimmten DNS-Server • Liste von Datei-FTP-Servern oder einen bestimmten FTP-Server • Liste von Dateischnittstellen oder eine bestimmte Dateischnittstelle • Liste von Routen für die Dateischnittstelle oder eine bestimmte Schnittstellenroute • Liste von Datei-Kerberos-Servern oder einen bestimmten Kerberos-Server • Liste von Datei-LDAP-Servern oder einen bestimmten LDAP-Server • Liste von Datei-NDMP-Servern oder einen bestimmten NDMP-Server • Liste von Datei-NIS-Servern oder einen bestimmten NIS-Server • Liste von Dateisystemen oder ein bestimmtes Dateisystem • Liste von Dateistrukturquoten oder eine bestimmte Dateistrukturquote • Liste von Dateinutzerquoten oder eine bestimmte Nutzerquote • Liste von Dateivirenschutzprogrammen oder ein bestimmtes Dateivirenschutzprogramm • Liste von NAS-Servern oder einen bestimmten NAS-Server • Liste von NFS-Exporten oder einen bestimmten NFS-Export • Liste von NFS-Servern oder einen bestimmten NFS-Server • Liste von SMB-Servern oder einen bestimmten SMB-Server	✓		✓	✓	✓

Aufgabe	Operator	VM-Administrator	Sicherheitsadministrator	Speicheradministrator	Administrator
• Liste von SMB-Freigaben oder eine bestimmte SMB-Freigabe					
Einen bestimmten NAS-Server hinzufügen, ändern, löschen oder pingen oder ein Kennwort, Hosts oder Gruppen auf einen bestimmten NAS-Server hochladen				✓	✓
Kennwort oder Hosts eines bestimmten NAS-Servers anzeigen			✓		✓
Ein Dateisystem hinzufügen oder ein bestimmtes Dateisystem auf einem vorhandenen NAS-Server ändern oder löschen				✓	✓
Einen Clone oder Snapshot zu einem bestimmten Dateisystem hinzufügen oder ein bestimmtes Dateisystem aktualisieren oder wiederherstellen oder die Quote eines bestimmten Dateisystems aktualisieren				✓	✓
Eine Dateistrukturquote hinzufügen oder eine bestimmte Dateistrukturquote ändern, löschen oder aktualisieren				✓	✓
Eine Dateinutzerquote hinzufügen oder eine bestimmte Dateinutzerquote ändern, löschen oder aktualisieren				✓	✓
Ein Dateivirenschutzprogramm hinzufügen oder ein bestimmtes Dateivirenschutzprogramm ändern oder löschen oder eine bestimmte Konfiguration eines Dateivirenschutzprogramms hochladen					✓
Eine bestimmte Konfiguration eines Dateivirenschutzprogramms herunterladen			✓		✓
Einen SMB- oder NFS-Server hinzufügen oder einen bestimmten SMB- oder NFS-Server ändern, löschen, verbinden oder trennen				✓	✓
Eine SMB-Freigabe hinzufügen oder eine bestimmte SMB-Freigabe ändern oder löschen				✓	✓
Einen NFS-Export hinzufügen oder einen bestimmten NFS-Export ändern oder löschen				✓	✓
Eine Dateischnittstelle hinzufügen oder eine bestimmte Dateischnittstelle ändern oder löschen				✓	✓

Aufgabe	Operator	VM-Administrator	Sicherheitsadministrator	Speicheradministrator	Administrator
Eine Dateischnittstellenroute hinzufügen oder eine bestimmte Dateischnittstellenroute ändern oder löschen				✓	✓
Einen Datei-DNS-, Datei-FTP-, Datei-Kerberos-, Datei-LDAP-, Datei-NDMP- oder Datei-NIS-Server hinzufügen oder einen bestimmten Datei-DNS-, Datei-FTP-, Datei-Kerberos-, Datei-LDAP-, Datei-NDMP- oder Datei-NIS-Server ändern oder löschen				✓	✓
Eine Datei-Kerberos-Keytab hochladen					✓
Eine Datei-Kerberos-Keytab herunterladen	✓		✓		✓
Eine Datei-LDAP-Konfiguration oder ein LDAP-Zertifikat hochladen					✓
Ein Datei-LDAP-Zertifikat herunterladen			✓		✓

Nutzerkontoverwaltung basierend auf Rollenberechtigungen

Ein Nutzer mit der Rolle eines Administrators oder Sicherheitsadministrators kann Folgendes in Bezug auf die Nutzerkontoverwaltung durchführen:

- Erstellen eines neuen Nutzerkontos
- Löschen aller Nutzerkonten, mit Ausnahme des integrierten Administratorkontos.

  ANMERKUNG: Das integrierte Administratorkonto kann nicht gelöscht werden.
- Ändern der Rolle eines Nutzers
- Zurücksetzen eines Nutzerkennworts
- Sperren oder Entsperren eines anderes Nutzerkontos

  ANMERKUNG: Angemeldete Nutzer mit einer Administrator- oder Sicherheitsadministratorrolle können ihr eigenes Konto nicht sperren.

Angemeldete Nutzer können ihr eigenes Nutzerkonto nicht löschen. Mit Ausnahme von Nutzern mit der Rolle des Sicherheitsadministrators oder Administrators können angemeldete Nutzer nur ihr eigenes Kennwort ändern. Nutzer müssen ihr altes Kennwort eingeben, um es zu ändern. Angemeldete Nutzer können Ihr eigenes Kennwort nicht zurücksetzen, ihre eigene Rolle nicht ändern und Ihre eigenen Konten weder sperren noch entsperren.

Das integrierte Administratorkontoprofil (mit Administratorrolle) kann weder bearbeitet noch gesperrt werden.

Wenn entweder die Rolle oder der Sperrstatus eines Nutzers geändert wird, der Benutzer gelöscht wird oder sein Kennwort von einem Sicherheitsadministrator oder Administrator geändert wird, werden alle an diesen Nutzer gebundenen Sitzungen ungültig.

ANMERKUNG: Wenn Nutzer ihre eigenen Kennwörter in der Sitzung aktualisieren, bleibt die Sitzung aktiv.

Zurücksetzen der Kennwörter für Administrator- und Servicekonten

Mit der Appliance wird ein Standardadministratornutzerkonto bereitgestellt, mit dessen Hilfe Sie die Erstkonfiguration durchführen können. Zudem wird ein Standardservicenutzerkonto bereitgestellt, mit dem Sie spezielle Servicefunktionen durchführen können. Es wird empfohlen, dass Sie PowerStore anfänglich mithilfe der PowerStore Manager-Benutzeroberfläche statt einer anderen Methode wie der REST API oder der CLI konfigurieren. Durch die Verwendung der PowerStore Manager-Nutzeroberfläche wird sichergestellt, dass alle Standardkennwörter geändert werden. Wenn Sie die neu festgelegten Kennwörter vergessen haben, können Sie sie auf die Standardwerte zurücksetzen.

Die Methode zum Zurücksetzen dieser Kennwörter hängt davon ab, ob Ihre Appliance eine PowerStore T model oder eine PowerStore X model ist. Verwenden Sie die für Ihre Appliance geltende Methode, um das Admin- und/oder Servicekennwort zurückzusetzen.

Zurücksetzen der Kennwörter für Administrator- und Servicekonten auf Standardwerte in einer PowerStore T model-Appliance

Info über diese Aufgabe

Bei einer PowerStore T model-Appliance ist die primäre Methode zum Zurücksetzen der Administrator- oder Servicenutzerkennwörter die Verwendung eines USB-Laufwerks. Unterstützte Dateisysteme sind FAT32 und ISO 9660.

ANMERKUNG: Führen Sie, um das Kennwort zurückzusetzen, wenn sich die Appliance im Servicemodus befindet, die folgenden Schritte aus, mit einem Unterschied. Wenden Sie das Zurücksetzen von USB auf jeden Node an. Dadurch wird sichergestellt, dass Sie nach dem Zurücksetzen des Systems in den Normalmodus bei der PowerStore Manager-Anmeldung aufgefordert werden, ein neues Kennwort für den Administrator und die Servicenutzer einzugeben.

Schritte

1. Wenn das USB-Laufwerk formatiert ist, fahren Sie mit dem nächsten Schritt fort. Verwenden Sie andernfalls eine Eingabeaufforderung wie `format <d:> /FS:FAT32` zum Formatieren des Laufwerks.

   Dabei steht `d:` für den Laufwerksbuchstaben des USB-Laufwerks, das Sie in Ihren Laptop oder PC eingesetzt haben.

2. Legen Sie die Bezeichnung mit folgendem Befehl fest:

   ```
   label d:
   RSTPWD
   ```

   ANMERKUNG: Die Appliance kann das USB-Laufwerk ohne die Bezeichnung `RSTPWD` nicht einhängen. Fügen Sie nach der Bezeichnung des USB-Laufwerks eine leere Datei für die Kontokennwörter ein, die Sie zurücksetzen möchten. Sie können das Admin- und/oder Servicekontokennwort zurücksetzen.

3. Um eine leere Datei auf dem Laufwerk zu erstellen, verwenden Sie bei Bedarf einen oder beide der folgenden Befehle:

   ```
   copy NUL d:\admin
   copy NUL d:\service
   ```

4. Setzen Sie das USB-Laufwerk in den USB-Port eines der beiden Nodes der Appliance ein, warten Sie 10 Sekunden und entfernen Sie es wieder.
   Für jedes Konto, das Sie zurücksetzen, wird das Kennwort jetzt auf den Standardwert festgelegt.
5. Stellen Sie über einen Browser eine Verbindung mit dem Cluster mithilfe der Cluster-IP-Adresse her und melden Sie sich mit dem standardmäßigen anfänglichen Kennwort (**`Password123#`**) als Administrator an.
   Eine Eingabeaufforderung zum Zurücksetzen der Administrator- und/oder Servicekennwörter sollte angezeigt werden. Wenn Sie das Servicekennwort mithilfe von Secure Shell (SSH) zurücksetzen möchten, lautet das anfängliche Standardkennwort für das Servicekonto **`service`**.
6. Ändern Sie das Administratorkennwort von der Standardeinstellung in ein benutzerdefiniertes Kennwort.
7. Wenn Sie das Kennwort für das Servicekonto auf einen anderen Wert als das Administratorkennwort setzen möchten, deaktivieren Sie das zugehörige Kontrollkästchen.

Ergebnisse

Wenden Sie sich an Ihren Serviceanbieter, wenn Sie nach der Ausführung dieses Verfahrens weiterhin nicht bei der Anmeldung aufgefordert werden, das Kennwort zurückzusetzen.

Zurücksetzen der Kennwörter für Administrator- und Servicekonten auf Standardwerte in einer PowerStore X model-Appliance

Voraussetzungen

Bringen Sie Namen des primären Node Ihrer primären Appliance in Erfahrung (z. B. PSTX-44W1BW2-A und PowerStore D6013). Falls erforderlich, generieren Sie die Datei `reset.iso`.

Info über diese Aufgabe

Verwenden Sie für eine PowerStore X model-Appliance ein ISO-Image und hängen Sie es über vSphere ein. Vorab erstellte Image-Dateien können von www.dell.com/support heruntergeladen werden. Sie können auch ein eigenes Image von einem Linux-System mit einem oder beiden der folgenden Befehle erstellen, je nachdem, welche Kennwörter zurückgesetzt werden müssen:

```
mkdir iso
touch iso/admin
touch iso/service
mkisofs -V RSTPWD -o reset.iso iso
```

ANMERKUNG: Das ISO-Image `reset.iso` muss sich auf einem Datenspeicher befinden, bevor es von vSphere als virtuelle CD eingehängt werden kann.

ANMERKUNG: Zum Zurücksetzen des Kennworts, wenn sich die Appliance im Servicemodus befindet, gehen Sie folgendermaßen vor, mit zwei Unterschieden. Erstens müssen Sie das ISO-Image in den Datenspeicher PRIVATE-C9P42W2.A.INTERNAL der virtuellen Maschine (VM) des Controllers selbst hochladen, da der öffentliche Datenspeicher nicht verfügbar ist. Laden Sie zweitens die Datei `reset.iso` hoch und wenden Sie sie auf beide Controller-VM-Nodes A und B an. Mit dieser Aktion wird sichergestellt, dass Sie, wenn sich das System wieder im Normalmodus befindet und der Zugang zu PowerStore Manager verfügbar ist, aufgefordert werden, ein neues Kennwort sowohl für den Admin als auch für die Nutzer des Service einzugeben.

Schritte

1. Wählen Sie in vSphere unter **Storage** die PowerStore X model-Appliance aus.

   Beispiel: **DataCenter-WX-D6013** > **PowerStore D6013**

2. Wählen Sie unter **Files** die Option **ISOs** aus.
3. Wählen Sie **Upload** aus und laden Sie die Datei `reset.iso` hoch, entweder die zuvor erstellte Image-Datei von www.dell.com/support oder Ihre eigene Image-Datei, die Sie auf einem Linux-System erstellt haben.
   Die Datei `reset.iso` wird im Ordner **ISOs** angezeigt.
4. Wählen Sie in vSphere unter **Host and Clusters** den primären Node der primären PowerStore X model-Appliance im Cluster aus.

   Beispiel: **DataCenter-WX-D6013** > **Cluster WX-D6013** > **PSTX-44W1BW2-A**

5. Klicken Sie unter **Summary** auf **CD/DVD drive 1** und wählen Sie **Connect to datastore ISO file** aus.
   Das Fenster **Choose an ISO image to mount** wird angezeigt.
6. Klicken Sie unter **Datastores** auf die primäre PowerStore X model-Appliance im Cluster und wählen Sie den Ordner **ISOs** aus.
   Die Datei `reset.iso` sollte unter **Contents** angezeigt werden.
7. Wählen Sie die Datei `reset.iso` aus und klicken Sie auf **OK**.
   Unter **Summary** sollte **CD/DVD drive 1** ca. 10 Sekunden lang als **Connected** angezeigt werden und dann zu **Disconnected** wechseln. Das Administratorkennwort für das Cluster oder das Servicekennwort oder beide sind jetzt auf die Standardeinstellung zurückgesetzt.
8. Stellen Sie über einen Browser eine Verbindung mit dem Cluster mithilfe der Cluster-IP-Adresse her und melden Sie sich mit dem standardmäßigen anfänglichen Kennwort (**`Password123#`**) als Administrator an.
   Eine Eingabeaufforderung zum Zurücksetzen der Administrator- und/oder Servicekennwörter sollte angezeigt werden. Wenn Sie das Servicekennwort mithilfe von Secure Shell (SSH) zurücksetzen möchten, lautet das anfängliche Standardkennwort für das Servicekonto **`service`**.
9. Ändern Sie das Administratorkennwort von der Standardeinstellung in ein benutzerdefiniertes Kennwort.
10. Wenn Sie das Kennwort für das Servicekonto auf einen anderen Wert als das Administratorkennwort setzen möchten, deaktivieren Sie das zugehörige Kontrollkästchen.

Ergebnisse

Wenden Sie sich an Ihren Serviceanbieter, wenn Sie nach der Ausführung dieses Verfahrens weiterhin nicht bei der Anmeldung aufgefordert werden, das Kennwort zurückzusetzen.

Zertifikate

Die Daten im Zertifikatspeicher von PowerStore sind persistent. Im Zertifikatspeicher werden die folgenden Arten von Zertifikaten gespeichert:

- Zertifikate der Zertifizierungsstelle
- Clientzertifikate
- Serverzertifikate

Anzeigen von Zertifikaten

Info über diese Aufgabe

Die folgenden Informationen werden in PowerStore Manager für jedes auf der Appliance gespeicherte Zertifikat angezeigt:

- `Service`
- `Type`
- `Scope`
- `Issued by`
- `Valid`
- `Valid to`
- `Issued to`

ANMERKUNG: Verwenden Sie die REST API oder CLI, um zusätzliche Zertifikatinformationen anzuzeigen.

Um Zertifikatinformationen anzuzeigen, führen Sie die folgenden Schritte aus:

Schritte

1. Starten Sie den PowerStore Manager.
2. Klicken Sie auf **Settings** und unter **Security** auf **Certificates**.
   Informationen zu den auf der Appliance gespeicherten Zertifikaten werden angezeigt.
3. Zum Anzeigen der Zertifikatkette, die ein Zertifikat und zugehörige Informationen für einen Service enthält, klicken Sie auf den jeweiligen Service.
   View Certificate Chain wird angezeigt und enthält Informationen über die Kette der Zertifikate, die das Zertifikat bilden.

Sichere Kommunikation zwischen PowerStore-Appliances in einem Cluster

Bei der Clustererstellung erstellt der primäre Node der Cluster-Master-Appliance ein Zertifikat der Zertifizierungsstelle (CA), auch als Cluster-CA bezeichnet. Die Master-Appliance übergibt das Cluster-CA-Zertifikat an die dem Cluster beitretenden Appliances.

Jede PowerStore-Appliance in einem Cluster erzeugt ein eigenes, eindeutiges IPsec-Zertifikat, das vom Cluster-CA-Zertifikat signiert wird. Die sensiblen Daten, die PowerStore-Appliances über ihr Clusternetzwerk übertragen, sind durch IPsec und TLS geschützt, sodass die Sicherheit und Integrität der Daten erhalten bleibt.

Sichere Kommunikation für Replikation und Datenimport

PowerStore hat eine Zertifikat- und Zugangsdateninfrastruktur, die den Austausch von Server- und Clientzertifikaten und Nutzeranmeldedaten ermöglicht. Dieser Prozess umfasst:

- Abrufen und Validieren des Serverzertifikats während des TLS-Handshake
- Hinzufügen des vertrauenswürdigen CA-Zertifikats vom Remotesystem zum Zugangsdatenspeicher
- Hinzufügen des vertrauenswürdigen Server-/Clientzertifikats zum Zugangsdatenspeicher

- Unterstützung bei der Einrichtung sicherer Verbindungen, sobald die Vertrauensstellung eingerichtet ist

PowerStore unterstützt die folgenden Funktionen zum Management von Zertifikaten:

- Für die Replikation muss ein Zertifikataustausch zwischen zwei PowerStore-Clustern stattfinden, damit eine vertrauenswürdige Kommunikation hergestellt werden kann. Für die Replikation zwischen PowerStore-Clustern muss die bidirektionale Vertrauensstellung zwischen den Clustern eingerichtet werden, um die gegenseitige TLS-Authentifizierung bei der Ausgabe von REST-Replikationssteuerungsanforderungen zu ermöglichen.
- Zum Erstellen eines Datenimports muss ein persistenter Zertifikats- und Zugangsdatenaustausch stattfinden, damit eine sichere Verbindung zwischen einem Dell EMC Speichersystem (VNX-, Unity-, Storage Center (SC)- oder Peer Storage (PS)-System) und einem PowerStore-Cluster hergestellt werden kann.

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 besteht aus mehreren Komponenten, die eingehende VASA-API-Anforderungen bedienen. Das VASA-API-Gateway, das alle eingehenden VASA-APIs entgegennimmt, wird auf der primären Appliance (diejenige mit der Floating-Management-IP) in einem PowerStore-Cluster bereitgestellt. ESXi-Hosts und vCenter Server verbinden sich mit dem VASA-Anbieter und erhalten Informationen über verfügbare Speichertopologie, Funktionen und Status. vCenter Server stellt diese Informationen später vSphere-Clients bereit. VASA wird von VMware-Clients, und nicht von PowerStore Manager-Clients verwendet.

Der vSphere-Nutzer muss die Instanz des VASA-Anbieters als Anbieter der VASA-Informationen für den Cluster konfigurieren. Wenn die primäre Appliance ausfällt, wird der zugehörige Prozess zusammen mit dem VASA-Anbieter auf der Appliance neu gestartet, die die nächste primäre Appliance ist. Für die IP-Adresse wird ein automatisches Failover durchgeführt. Intern ist im Protokoll ein Fehler zu sehen, wenn Konfigurationsänderungsereignisse vom neu aktivierten VASA-Anbieter abgerufen werden. Daraufhin wird jedoch automatisch eine Neusynchronisation der VASA-Objekte ohne Nutzereingriff durchgeführt.

PowerStore bietet VASA 3.0-Schnittstellen für vSphere 6.5 und 6.7.

VASA 3.0 unterstützt Virtual Volumes (VVols). VASA 3.0 unterstützt Schnittstellen zur Abfrage von Speicherabstraktionen wie VVols und Speichercontainer. Diese Informationen helfen dem Speicher-Policy-basiertem Management (Storage Policy Based Management, SPBM) bei Entscheidungen zur Platzierung des virtuellen Laufwerks und zur Compliance. VASA 3.0 unterstützt auch Schnittstellen für die Bereitstellung und das Management des Lebenszyklus von VVols, die für das Backup virtueller Laufwerke verwendet werden. 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 PowerStore Manager-Onlinehilfe.

Authentifizierung im Zusammenhang mit VASA

Um eine Verbindung von vCenter zum PowerStore Manager-VASA-Anbieter zu initiieren, geben Sie die folgenden Informationen im vSphere-Client ein:

- URL des VASA-Anbieters im folgenden Format bei VASA 3.0: https://<Management-IP-Adresse>:8443/version.xml.
- Nutzername eines PowerStore Manager-Nutzers (die Rolle muss entweder VM-Administrator oder Administrator sein).
  ANMERKUNG: Die VM-Administratorrolle dient ausschließlich als Mittel zur Registrierung von Zertifikaten.
- Das diesem Nutzer zugeordnete Kennwort.

Die hier verwendeten PowerStore Manager-Zugangsdaten werden nur in diesem ersten Verbindungsschritt verwendet. Wenn die PowerStore Manager-Zugangsdaten für den Zielcluster gültig sind, wird das Zertifikat von vCenter Server automatisch beim Cluster registriert. Mit diesem Zertifikat werden alle nachfolgenden Anforderungen authentifiziert, die von vCenter stammen. Keine manuellen Schritte sind zum Installieren oder Hochladen dieses Zertifikats zum VASA-Anbieter 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 VASA-Anbieter-URL und die Anmeldedaten mitteilt. Der vCenter-Server verwendet die URL, die Anmeldedaten und das SSL-Zertifikat des VASA-Anbieters, um eine sichere Verbindung mit dem VASA-Anbieter herzustellen. Eine vCenter-Sitzung endet, wenn eines der folgenden Ereignisse eintritt:

- Ein Administrator entfernt den VASA-Anbieter 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 vCenter Server-Service die SSL-Verbindung nicht wiederherstellen kann, wird eine neue 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 VASA-Anbieter. In VASA 3.0 fungiert vCenter Server als die VMware-Zertifizierungsstelle (VMCA). Der VASA-Anbieter überträgt auf Anforderung ein selbstsigniertes Zertifikat nach Autorisierung der Anfrage. Er fügt das VMCA-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 VASA-Anbieter mithilfe des Storage Monitoring Service (SMS)-Zertifikats des Clients authentifiziert, das mit dem zuvor registrierten Stammsignierungszertifikat validiert wird. Ein VASA-Anbieter generiert eindeutige Kennungen für Speicherentitätsobjekte und vCenter Server nutzt die Kennungen zum Anfordern von Daten für eine bestimmte Entität.

Ein VASA-Anbieter nutzt SSL-Zertifikate und die VASA-Sitzungskennung zum Validieren von VASA-Sitzungen. Nachdem die Sitzung hergestellt wurde, muss ein VASA-Anbieter das SSL-Zertifikat und die VASA-Sitzungskennung validieren, der mit jedem Funktionsaufruf über vCenter Server verknüpft ist. Der VASA-Anbieter verwendet das im Truststore gespeicherte VMCA-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 VASA-Anbieter 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 VASA-Anbieter.

VORSICHT: SMS ruft bei einem 3.0-VASA-Anbieter nicht die `unregisterVASACertificate`-Funktion auf. Aus diesem Grund kann der VASA-Anbieter auch nach Aufhebung der Registrierung weiterhin sein vom SMS erhaltenes VMCA-signiertes Zertifikat verwenden.

CHAP-Authentifizierung

Das Challenge Handshake Authentication Protocol (CHAP) ist eine Methode zur Authentifizierung von iSCSI-Initiatoren (Hosts) und Zielen (Volumes und Snapshots). CHAP stellt iSCSI-Speicher bereit und sorgt für ein sicheres, standardmäßiges Speicherprotokoll. Die Authentifizierung hängt von einem geheimen Schlüssel (ähnlich einem Kennwort) ab, der dem Authentifikator und dem Peer bekannt ist. Es werden zwei Varianten des CHAP-Protokolls unterschieden:

- Die einseitige CHAP-Authentifizierung ermöglicht es dem iSCSI-Ziel, den Initiator zu authentifizieren. Wenn ein Initiator versucht, eine Verbindung zu einem Ziel herzustellen (im Normalmodus oder über den Ermittlungsmodus), stellt er dem Ziel einen Nutzernamen und ein Kennwort bereit.
- Die gegenseitige CHAP-Authentifizierung wird zusätzlich zur einseitigen CHAP-Authentifizierung angewendet. Gegenseitiges CHAP ermöglicht es, dass sich das iSCSI-Ziel und der Initiator gegenseitig authentifizieren. Jedes von der Gruppe präsentierte iSCSI-Ziel wird vom iSCSI-Initiator authentifiziert. Wenn ein Initiator versucht, eine Verbindung zu einem Ziel herzustellen, stellt das Ziel dem Initiator einen Nutzernamen und ein Kennwort bereit. Der Initiator vergleicht den bereitgestellten Nutzernamen und das Kennwort mit den Informationen, die er zur Verfügung hat. Wenn sie übereinstimmen, kann der Initiator eine Verbindung zum Ziel herstellen.

ANMERKUNG: Wenn CHAP in Ihrer Umgebung verwendet wird, wird empfohlen, dass Sie die CHAP-Authentifizierung einrichten und aktivieren, bevor Sie Volumes für den Datenempfang vorbereiten. Wenn Sie Laufwerke für den Empfang von Daten vorbereiten, bevor Sie die CHAP-Authentifizierung eingerichtet und aktiviert haben, können Sie den Zugriff auf die Volumes verlieren.

PowerStore unterstützt den iSCSI CHAP-Erkennungsmodus nicht. Die folgende Tabelle zeigt die Einschränkungen von PowerStore in Bezug auf den iSCSI CHAP-Erkennungsmodus.

Tabelle 1. Einschränkungen für den iSCSI CHAP-Erkennungsmodus

CHAP-Modus	Einzelmodus (Initiator aktiviert)	Gegenseitiger Modus (Initiator und Ziel aktiviert)
Erkennung	PowerStore wird den Host nicht authentifizieren (herausfordern). Die Authentifizierung kann nicht verwendet werden, um die Ermittlung von Zielen zu verhindern. Dies führt nicht zu ungeplantem Zugriff auf Nutzerdaten.	PowerStore antwortet nicht auf eine Authentifizierungsanforderung (Herausforderung) von einem Host und die Erkennung schlägt fehl, wenn der Host PowerStore herausfordert.

Tabelle 1. Einschränkungen für den iSCSI CHAP-Erkennungsmodus (fortgesetzt)

CHAP-Modus	Einzelmodus (Initiator aktiviert)	Gegenseitiger Modus (Initiator und Ziel aktiviert)
Normal	Funktioniert wie erwartet. Die Zugangsdaten werden getestet von PowerStore.	Funktioniert wie erwartet. Die Zugangsdaten werden übertragen von PowerStore.

Für die Remotereplikation zwischen einer Quell- und einer Ziel-Appliance erkennt der Verifizierungs- und Aktualisierungsprozess Änderungen in den lokalen und Remotesystemen und stellt Datenverbindungen wieder her, wobei auch die CHAP-Einstellungen berücksichtigt werden.

Konfigurieren von CHAP

Die einseitige (durch den Initiator) oder gegenseitige (durch den Initiator und das Ziel) Authentifizierung mit CHAP kann auf einem PowerStore-Cluster aktiviert werden. CHAP kann für eine Clusterimplementierung einer Appliance oder mehrere PowerStore-Appliances und externe Hosts aktiviert werden.

Wenn die einseitige Authentifizierung aktiviert ist, müssen der Nutzername und das Kennwort für jeden Initiator eingegeben werden, wenn externe Hosts hinzugefügt werden. Wenn die gegenseitige Authentifizierung aktiviert ist, müssen auch der Nutzername und das Kennwort für das Cluster eingegeben werden. Wenn ein Host hinzugefügt und Initiatoren mit aktiviertem CHAP hinzugefügt werden, muss das Initiatorkennwort einmalig vergeben sein. Sie können nicht für alle Initiatoren eines Hosts das gleiche Kennwort verwenden. Die genaue CHAP-Konfiguration eines externen Hosts ist unterschiedlich. Um diese Funktion nutzen zu können, müssen Sie mit dem Betriebssystem des Hosts und dem Konfigurationsvorgang vertraut sein.

ANMERKUNG: Das Aktivieren von CHAP, sobald Hosts auf dem System konfiguriert sind, führt zu einer Unterbrechung der externen Hosts. Es führt zu einer I/O-Unterbrechung, bis die Konfigurationen auf dem externen Host und auf der Appliance eingerichtet sind. Es wird empfohlen, dass Sie vor dem Hinzufügen externer Hosts zur Appliance entscheiden, welche Art von CHAP-Konfiguration Sie implementieren möchten.

Wenn Sie CHAP aktivieren, nachdem Hosts hinzugefügt wurden, müssen Sie die Initiatoren jedes Hosts aktualisieren. Wenn CHAP aktiviert ist, können Sie keinen Host zu einer Hostgruppe hinzufügen, die keine CHAP-Zugangsdaten hat. Wenn CHAP aktiviert wurde und Sie einen Host zu einem späteren Zeitpunkt hinzufügen, wählen Sie im PowerStore Manager unter **Compute** die Option **Hosts & Host Groups** aus, um den Host manuell zu registrieren. Sie müssen Zugangsdaten zu Authentifizierungszwecken auf iSCSI-Ebene eingeben. Kopieren Sie in diesem Fall die IQN vom Host und fügen Sie dann die zugehörigen CHAP-Zugangsdaten für jeden Initiator hinzu.

Konfigurieren Sie CHAP für ein Cluster mit einer der folgenden Methoden:

- **CHAP**: Eine Seite mit CHAP-Einstellungen, auf die Sie im PowerStore Manager zugreifen können (klicken Sie auf **Settings** und wählen Sie unter **Security** die Option **CHAP**) aus.
- REST-API-Server: Eine Anwendungsschnittstelle, die REST-API-Anforderungen zur Konfiguration der CHAP-Einstellungen empfangen kann. Weitere Informationen über die REST API finden Sie im *PowerStore REST API Reference Guide*.

Klicken Sie, um den Status von CHAP zu bestimmen, im PowerStore Manager auf **Settings** und wählen Sie unter **Security** die Option **CHAP** aus.

Externer SSH-Zugriff

Jede Appliance kann optional den externen Secure Shell (SSH)-Zugriff auf den SSH-Port der Appliance-IP-Adresse ermöglichen, wodurch der Nutzer die Servicefunktion auf dem primären Node einer Appliance nutzen kann. Die IP-Adresse der Appliance wird zwischen den beiden Nodes der Appliance ausgetauscht, wenn sich die primäre Zuschreibung ändert. Wenn die externe SSH deaktiviert ist, wird der SSH-Zugriff nicht zugelassen.

Wenn eine Appliance erstmals installiert und nicht konfiguriert ist, ist SSH standardmäßig aktiviert, sodass die Appliance gewartet werden kann, wenn Probleme auftreten, bevor Sie zu einem Cluster hinzugefügt wird. Bei der Erstellung eines neuen Clusters oder bei einem Clusterbeitritt muss SSH bei allen Appliances zunächst deaktiviert sein.

Konfigurieren des externen SSH-Zugriffs

Sie können den externen Zugriff auf Appliances in einem Cluster über SSH mithilfe einer der folgenden Methoden konfigurieren:

- **SSH Management**: Eine Seite mit SSH-Einstellungen, auf die Sie im PowerStore Manager zugreifen können (klicken Sie auf **Settings** und wählen Sie unter **Security** die Option **SSH Management** aus).
- REST-API-Server: Eine Anwendungsschnittstelle, die REST-API-Anforderungen zur Konfiguration der SSH-Einstellungen empfangen kann. Weitere Informationen über die REST API finden Sie im *PowerStore REST API Reference Guide*.
- `svc_service_config` : Ein Servicebefehl, den Sie als Servicenutzer direkt auf der Appliance eingeben können. Weitere Informationen zu diesem Befehl finden Sie im *PowerStore Service Scripts Guide*.

Klicken Sie, um den Status von SSH auf Appliances innerhalb eines Clusters zu bestimmen, im PowerStore Manager auf **Settings** und wählen Sie unter **Security** die Option **SSH Management** aus. Sie können auch auf einer oder mehreren von Ihnen ausgewählten Appliances SSH aktivieren oder deaktivieren.

Wenn der SSH-Service erfolgreich aktiviert wurde, verwenden Sie einen beliebigen SSH-Client, um sich bei der Appliance-IP-Adresse anzumelden. Der Zugriff auf die Appliance erfordert Servicenutzeranmeldedaten.

Über das Servicekonto können Benutzer folgende Funktionen durchführen:

- Ausführung spezieller Appliance-Serviceskripts für das Monitoring und das Troubleshooting von Systemeinstellungen und Vorgängen des Appliance-Systems
- 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.

Für maximale Appliance-Sicherheit wird empfohlen, die externe SSH-Serviceschnittstelle jederzeit deaktiviert zu lassen, es sei denn, sie ist für die Durchführung von Servicevorgängen auf der Appliance erforderlich. Deaktivieren Sie die SSH-Schnittstelle nach der Durchführung der erforderlichen Servicevorgänge wieder, um dafür zu sorgen, dass die Appliance sicher bleibt.

SSH Sitzungen

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

Kennwort für das Servicekonto

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

Während der Erstkonfiguration der Appliance müssen Sie das Standardkennwort für den Service ändern. Es gelten dieselben Kennworteinschränkungen wie für Systemmanagementkonten (siehe Anforderungen an Nutzername und Kennwort auf Seite 7).

SSH-Autorisierung

Die Servicekontoautorisierung basiert auf folgendem:

- Anwendungsisolierung: PowerStore-Software verwendet die Containertechnologie, die Anwendungsisolierung bereitstellt. Zugriff auf den Appliance-Service wird durch den Servicecontainer bereitgestellt, nur ein Satz von Serviceskripten und ein Satz von Linux-Befehlen sind verfügbar. Das Servicekonto hat nicht die Möglichkeit, auf andere Container zuzugreifen, die das Dateisystem bedienen und I/O für Nutzer blockieren.
- Linux-Dateisystemberechtigungen: Die meisten Linux-Tools und Dienstprogramme, die den Systembetrieb in irgendeiner Weise modifizieren, sind für den Servicenutzer nicht verfügbar, sie erfordern Superuser-Kontoberechtigungen. 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.
- Zugriffskontrollen: Neben der Anwendungsisolierung, die durch die Containertechnologie bereitgestellt wird, verwendet der Zugriffskontrolllistenmechanismus (ACL) auf der Appliance eine Liste mit sehr spezifischen Regeln, um den Zugriff auf Systemressourcen durch das Servicekonto explizit zu gewähren oder zu verweigern. Diese Regeln geben Servicekontoberechtigungen für andere Bereiche der Appliance an, die ansonsten nicht durch standardmäßige Linux-Dateisystemberechtigungen definiert werden.

Appliance-Serviceskripts

Auf der Softwareversion der Appliance sind eine Reihe von Skripts zur Problemdiagnose, Systemkonfiguration und Systemrecovery installiert. Diese Skripts stellen ausführliche Informationen und eine geringere Systemkontrolle bereit, als über PowerStore Manager verfügbar ist. In *PowerStore Service Scripts Guide* werden diese Skripts mit gängigen Fallbeispielen beschrieben.

Ethernet-Serviceportschnittstelle und IPMItool für Appliance-Node

Ihre Appliance ermöglicht den Konsolenzugriff über einen Ethernetserviceport, der sich in jedem Node 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 Node herstellt. Das IPMItool ist ein Windows-Dienstprogramm, das einen sicheren Kommunikationskanal zum Zugriff auf die Node-Konsole einer Appliance aushandelt. Dieses Dienstprogramm erfordert physischen Zugriff zum Aktivieren der Konsole.

Die Node-Ethernet-Serviceportschnittstelle bietet dieselben Funktionen wie die SSH-Serviceschnittstelle (Service-LAN-Schnittstelle) und unterliegt auch denselben Einschränkungen. Nutzer greifen auf die Schnittstelle allerdings über eine Ethernetportverbindung und nicht über einen SSH-Client zu. Diese Schnittstelle wurde für Vertriebsmitarbeiter entwickelt, die eine Verbindung mit der Appliance herstellen können, ohne Ihr Netzwerk zu stören. Eine dedizierte Managementkonsole ist nicht erforderlich.

Diese Schnittstelle bietet eine direkte Punkt-zu-Punkt-, nicht routingfähige Verbindung. Servicemitarbeiter können die Service-LAN-Schnittstelle für die Konsolenausgabe, SSH-Zugriff auf den PowerStore-Servicecontainer und PowerStore Manager einschließlich des ICW (Assistent für die Erstkonfiguration) verwenden. Der SSH-Zugriff auf den Servicecontainer über die Service-LAN-Schnittstelle ist immer aktiviert und kann nicht deaktiviert werden. Sie managen jedoch die Zugangsdaten für das Servicekonto.

Eine Liste der Serviceskripte finden Sie im *PowerStore Service Scripts Guide*.

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 Kennwörter. Darüber hinaus werden keinerlei Kennwörter 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 Verschlüsselungsschlüssel 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. Von diesem Nutzerprinzipal erstellt der Server die Zugangsdaten dieses Nutzers durch Abfragen des aktiven UDS (Unix Directory Service). 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 über den PowerStore Manager konfiguriert werden.

Dateiprotokollbeziehungen

Für Kerberos ist Folgendes erforderlich:

- DNS: Sie müssen den DNS-Namen anstelle von IP-Adressen verwenden.
- NTP: PowerStore muss über einen konfigurierten NTP-Server verfügen.

  ANMERKUNG: Kerberos ist abhängig von der korrekten Zeitsynchronisation zwischen KDC, Servern und Client im Netzwerk.
- UDS: Dieses dient der Erstellung von Zugangsdaten.
- Hostname: Kerberos arbeitet mit Namen, nicht mit IP-Adressen.

NFS secure verwendet abhängig vom Wert des Hostnamens einen oder zwei Serviceprinzipalnamen (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, wo 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:

- Realm name (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 plus 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 Nutzer 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 Zugangsdaten 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.

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.

ANMERKUNG: Wenn das ältere SMB1-Protokoll in Ihrer Umgebung unterstützt werden muss, kann es mithilfe des Servicebefehls `svc_nas_cifssupport` aktiviert werden. Weitere Informationen zu diesem Befehl erhalten Sie im *PowerStore Service Scripts Guide*.

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 die 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.

ANMERKUNG: Weitere Informationen über das Konfigurieren und Verwalten von NAS-Servern in Bezug auf Multiprotokollfreigabe, Nutzerzuordnung, Zugriffs-Policies und Nutzeranmeldedaten erhalten Sie in der PowerStore Manager-Onlinehilfe.

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

ANMERKUNG: 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:

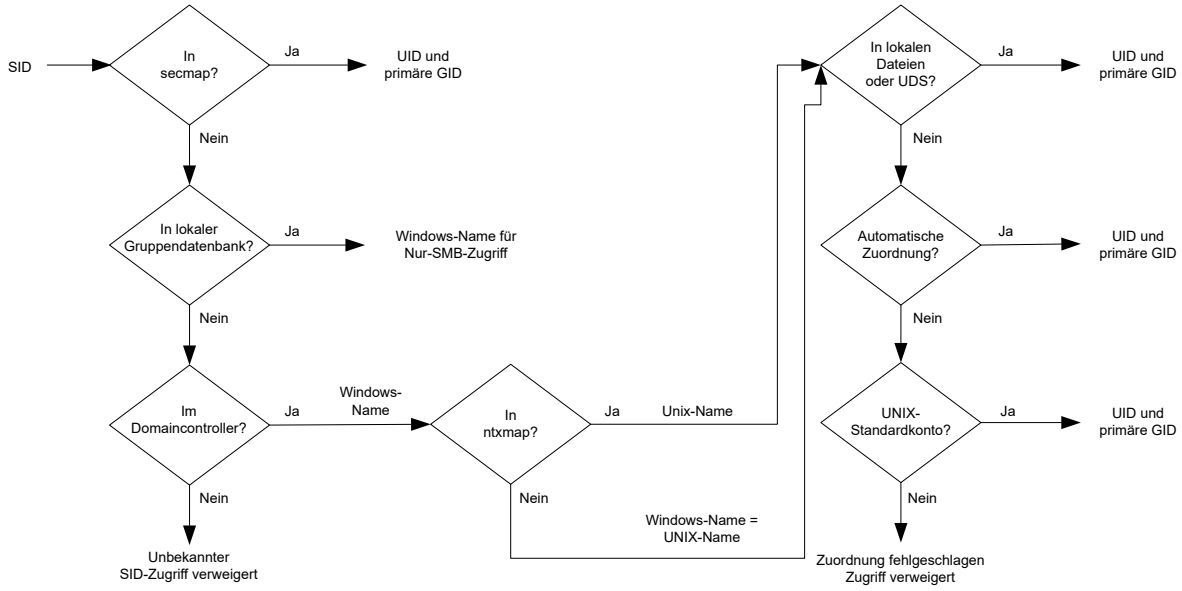

Abbildung 1. Prozess für die Auflösung einer SID in eine UID, die primäre GID-Zuordnung

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:

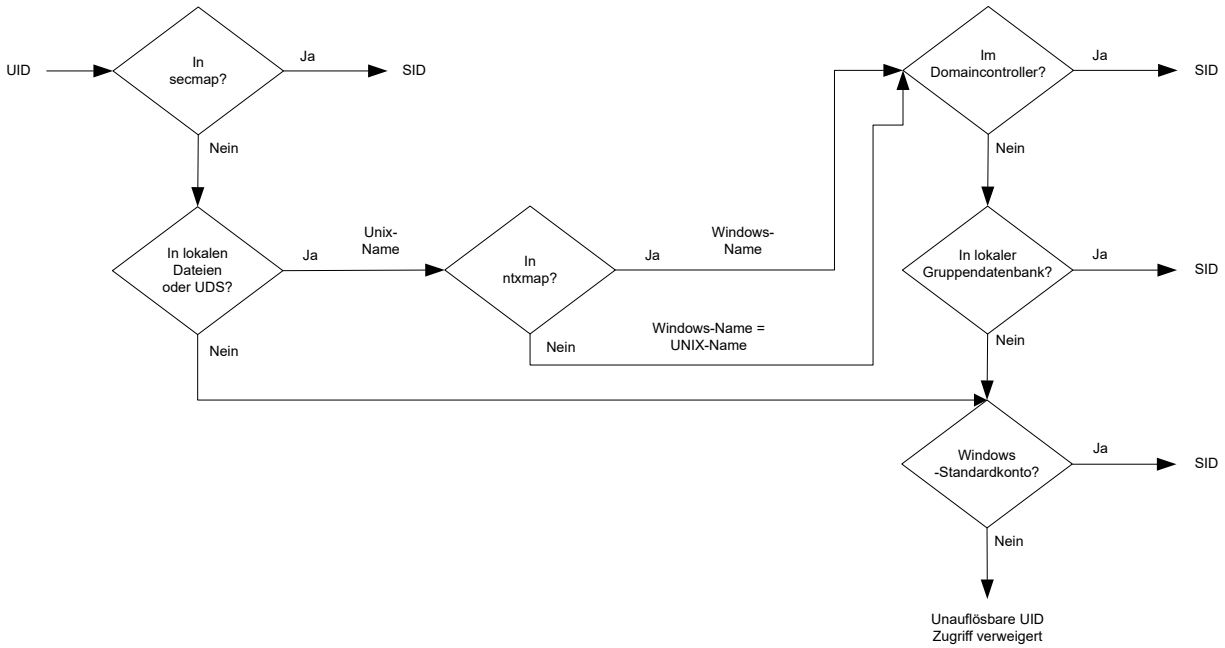

Abbildung 2. Prozess für die Auflösung einer UID in eine SID-Zuordnung

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:

Zugriffs-Policy	Beschreibung
Nativ (Standardeinstellung)	• 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. • 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 (wenn das Format für den Nutzernamen `domain\user` oder `user@domain` ist) oder eine UNIX-Authentifizierung sein (bei anderen Formaten des Nutzernamens). 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.

Zugangsdaten für Sicherheit auf Dateiebene

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

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

- Zur Erstellung von Windows-Zugangsdaten für eine SMB-Anforderung.
- Zur Erstellung von Windows-Zugangsdaten für eine NFS-Anforderung, wenn die Zugriffs-Policy für das Dateisystem Windows ist.

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

Ein persistenter Zugangsdatencache wird für Folgendes verwendet:

- Windows-Zugangsdaten, 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 Zugangsdatenoption 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-Zugangsdaten 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-Zugangsdaten 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-Zugangsdaten des Windows-Standardbenutzers verwendet.

ANMERKUNG: 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-Standardnutzer 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 Nutzer verweigert.

ANMERKUNG: Der UNIX-Standardnutzer kann ein gültiger vorhandener UNIX-Kontoname sein oder das neue Format `@uid=`*`xxxx`*`,gid=`*`yyyy`*`@` aufweisen, wobei *xxxx* und *yyyy* für die numerischen Dezimalwerte der UID bzw. für die primäre GID stehen. Diese Werte können auf dem System über den PowerStore Manager konfiguriert werden.

UNIX-Zugangsdaten für NFS-Anforderungen

Zur Verarbeitung von NFS Anforderungen für ein Nur-NFS- oder Multiprotokolldateisystem mit einer Unix- oder nativen Zugriffs-Policy müssen Unix-Zugangsdaten verwendet werden. Die UNIX-Zugangsdaten werden immer in jeder Anforderung integriert; allerdings sind die Zugangsdaten auf 16 Extragruppen beschränkt. Die Eigenschaft `extendedUnixCredEnabled` des NFS-Servers bietet die Möglichkeit, Zugangsdaten 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-Zugangsdaten verwendet.

ANMERKUNG: Für sicheren NFS-Zugriff werden die Zugangsdaten immer mit dem UDS erstellt.

UNIX-Zugangsdaten 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-Zugangsdaten 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-Zugangsdaten enthalten. Beim Zugriff auf ein Dateisystem mit einer UNIX-Zugriffs-Policy wird die ID des Benutzers zum Abfragen der UDS verwendet, um die UNIX-Zugangsdaten zu erstellen, ähnlich wie bei der Erstellung von erweiterten Zugangsdaten für NFS. Die UID ist für das Quotenmanagement erforderlich.

Windows-Zugangsdaten 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.

ANMERKUNG: 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.

Überblick über Common Antivirus Agent (CAVA)

Common AntiVirus Agent (CAVA) bietet eine Virenschutzlösung für Clients, die einen NAS-Server verwenden. 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.

Warum ist Virenschutz wichtig?

Das Speichersystem ist aufgrund seiner Architektur gegen das Eindringen von Viren resistent. Der NAS-Server führt mithilfe eines eingebetteten Betriebssystems den Datenzugriff in Echtzeit aus. Drittanbieter können auf diesem Betriebssystem keine Programme ausführen, die Viren enthalten. Obwohl die Betriebssystemsoftware gegen Viren geschützt ist, muss auf Windows-Clients, die auf das Speichersystem zugreifen, ebenfalls ein Virenschutz installiert sein. Der Virenschutz auf Clients reduziert das Risiko, dass sie eine infizierte Datei auf dem Server speichern, und schützt sie, wenn sie eine infizierte Datei öffnen. Diese Virenschutzlösung besteht aus einer Kombination aus Betriebssystemsoftware, einem CAVA-Agenten und einer Antivirus-Engine eines Drittanbieters. Die CAVA-Software und eine Drittanbieter-Virenschutz-Engine muss auf einem Windows-Server in der Domain installiert sein.

Weitere Informationen zu CAVA, das ein Teil von Common Event Enabler (CEE) ist, finden Sie unter *Using the Common Event Enabler on Windows Platforms* auf www.dell.com/powerstoredocs.

Codesignierung

PowerStore wurde entwickelt, um Softwareupgrades für neue Versionen und Patch-Versionen zu akzeptieren. Ein Master-GNU-Privacy-Guard-Schlüssel (GPG) signiert alle PowerStore-Softwarepakete und Dell EMC steuert diesen GPG-Schlüssel. Der PowerStore-Softwareupgradeprozess überprüft die Signatur des Softwarepakets und lehnt ungültige Signaturen ab, die auf eine mögliche Manipulation oder Beschädigung hindeuten könnten. Der Überprüfungsschritt ist in den Upgradeprozess integriert und die Signatur des Softwarepakets wird in der Phase vor der Installation automatisch überprüft.

2

Kommunikationssicherheitseinstellungen

Dieser Abschnitt enthält die folgenden Themen:

Themen:

- Portnutzung

Portnutzung

In den folgenden Abschnitten sind die Netzwerkports und die zugehörigen Services der Appliance dargestellt. Die Appliance dient unter verschiedenen Umständen als Netzwerkclient, zum Beispiel bei der Kommunikation mit einem vCenter Server. In diesen Fällen initiiert die Appliance die Kommunikation und die Netzwerkinfrastruktur muss diese Verbindungen unterstützen.

ANMERKUNG: Weitere Informationen zu Ports finden Sie im Wissensdatenbank-Artikel 542240, *PowerStore: Customer Network Firewall Rules - TCP/UDP Ports*. Navigieren Sie zu https://www.dell.com/support/kbdoc/en-us/542240. Mit dem Tool „Customer Network Firewall Rules“ können Sie die Liste der Firewallregeln und -ports filtern und überprüfen, die für Ihre PowerStore-Bereitstellung relevant sind.

Appliance-Netzwerkports

In der folgenden Tabelle sind die Netzwerkports und die zugehörigen Services der Appliance dargestellt.

Tabelle 2. Appliance-Netzwerkports

Port	Service	Protokoll	Zugriffsrichtung	Beschreibung
22	SSH-Client, SupportAssist Connect Home	TCP	Bidirektional	• Lässt SSH-Zugriff zu (falls aktiviert). • Erforderlich für SupportAssist Connect Home. Ist der Port geschlossen, sind Managementverbindungen über SSH nicht verfügbar.
25	SMTP	TCP	Ausgehend	Ermöglicht der Appliance das Senden von E-Mails. Ist dieser Port geschlossen, sind E-Mail-Benachrichtigungen nicht verfügbar.
26	SSH-Client	TCP	Bidirektional	SSH-Zugriff auf Port 22 wird auf diesen Port umgeleitet. Ist der Port geschlossen, sind Managementverbindungen über SSH nicht verfügbar.
53	DNS	TCP/UDP	Ausgehend	Wird verwendet, um DNS-Abfragen an den DNS-Server zu übertragen. Ist dieser Port geschlossen, funktioniert die DNS-Namensauflösung nicht.
80, 8080, 8128	SupportAssist	TCP	Ausgehend	Wird für SupportAssist-Proxyverbindung verwendet.
123	NTP	TCP/UDP	Ausgehend	NTP-Zeitsynchronisation. Ist der Port geschlossen, wird die Zeit zwischen Appliances nicht synchronisiert.

Tabelle 2. Appliance-Netzwerkports (fortgesetzt)

Port	Service	Protokoll	Zugriffsrichtung	Beschreibung
443	HTTPS	TCP	Bidirektional	Sicherer HTTP-Datenverkehr zu PowerStore Manager. Ist dieser Port geschlossen, ist keine Kommunikation mit der Appliance möglich.
500	IPsec (IKEv2)	UDP	Bidirektional	Damit IPsec trotz Firewalls funktioniert, öffnen Sie UDP-Port 500 und lassen Sie die IP-Protokollnummern 50 und 51 in eingehenden und ausgehenden Firewallfiltern zu. UDP-Port 500 sollte geöffnet werden, damit ISAKMP-Datenverkehr (Internet Security Association and Key Management Protocol) durch Ihre Firewalls weitergeleitet werden kann. Die IP-Protokoll-ID 50 sollte so festgelegt werden, dass die Weiterleitung von IPsec-ESP-Datenverkehr (Encapsulating Security Protocol) zulässig ist. Die IP-Protokoll-ID 51 sollte so festgelegt werden, dass AH-Datenverkehr (Authentication Header) weitergeleitet werden kann. Ist dieser Port geschlossen, ist die IPsec-Verbindung zwischen den PowerStore-Appliances nicht verfügbar.
587	SMTP	TCP	Ausgehend	Ermöglicht der Appliance das Senden von E-Mails. Ist dieser Port geschlossen, sind E-Mail-Benachrichtigungen nicht verfügbar.
3033	Importieren	TCP/UDP	Ausgehend	Erforderlich für den Speicherimport von Legacy-EqualLogic Peer-Speicher und Compellent Storage Center-Systemen.
3260	iSCSI	TCP	• Eingehend für Host- und ESXi-Hostzugriff • Bidirektional für Replikation • Ausgehend für Speicherimport	Erforderlich, um den folgenden Zugriff auf iSCSI-Services bereitzustellen: • Externer Host-iSCSI-Zugriff • Externer oder PowerStore-integrierter ESXi-Host-iSCSI-Zugriff • Inter-Cluster-Zugriff für Replikation • Speicherimportzugriff von Legacy-EqualLogic Peer-Speicher, Compellent Storage Center-, Unity- und VNX2-Systemen Falls geschlossen, sind iSCSI-Services nicht verfügbar. Wird von der Datenmobilität zur Unterstützung einer angemessenen Replikationsperformance bei einer Verbindung mit niedriger Latenz verwendet.
3261	Datenmobilität	TCP	Bidirektional	Wird von der Datenmobilität zur Unterstützung einer angemessenen Replikationsperformance bei einer Verbindung mit hoher Latenz verwendet.
5353	Multicast-DNS (mDNS)	UDP	Bidirektional	Multicast-DNS-Abfrage. Ist dieser Port geschlossen, funktioniert die mDNS-Namensauflösung nicht.
8443	VASA, SupportAssist	TCP	• Eingehend für VASA • Ausgehend für SupportAssist	• Erforderlich für den VASA Vendor Provider für VASA 3.0.

Tabelle 2. Appliance-Netzwerkports (fortgesetzt)

Port	Service	Protokoll	Zugriffsrichtung	Beschreibung
				• Erforderlich für die zugehörigen SupportAssist Connect Home-Funktionen.
8443, 50443, 55443 oder 60443	Windows-Import-Host-Agent, Linux-Import-Host-Agent oder VMware-Import-Host-Agent	TCP	Ausgehend	Einer dieser Ports muss geöffnet sein, wenn der Datenspeicher von Legacy-Speichersystemen importiert wird.
9443	SupportAssist	TCP	Ausgehend	Erforderlich für SupportAssist REST API in Bezug auf Connect Home.

Appliance-Netzwerkports in Bezug auf Dateien

In der folgenden Tabelle sind die Netzwerkports und die zugehörigen Services der Appliance dargestellt, die sich auf Dateien beziehen.

ANMERKUNG: Ausgehende Ports sind kurzlebig.

Tabelle 3. Appliance-Netzwerkports in Bezug auf Dateien

Port	Service	Protokoll	Zugriffsrichtung	Beschreibung
20	FTP	TCP	Ausgehend	Für FTP-Datenübertragung verwendeter Port. Dieser Port kann durch Aktivieren von FTP geöffnet werden. Authentifizierung wird auf Port 21 durchgeführt und vom FTP-Protokoll definiert.
21	FTP	TCP	Eingehend	Port 21 ist der Kontrollport, den der FTP-Service auf eingehende FTP-Anforderungen überwacht.
22	SFTP	TCP	Eingehend	Warnmeldungen über SFTP (FTP über SSH) SFTP ist ein Client-/Serverprotokoll. Nutzer können mithilfe von SFTP Dateiübertragungen auf einer Appliance im lokalen Subnetz durchführen. Ermöglicht ausgehende FTP-Kontrollverbindungen. Ist der Port geschlossen, ist FTP nicht verfügbar.
53	DNS	TCP/UDP	Ausgehend	Wird verwendet, um DNS-Abfragen an den DNS-Server zu übertragen. Ist dieser Port geschlossen, funktioniert die DNS-Namensauflösung nicht. Erforderlich für SMB v1.
88	Kerberos	TCP/UDP	Ausgehend	Erforderlich für Kerberos-Authentifizierungsservices.
111	RPC bind (für SDNAS-Namespaces; andernfalls Hostservice)	TCP/UDP	Bidirektional	Wird vom Standard-Portmapper oder dem rpcbind-Service geöffnet und ist ein zusätzlicher Appliance-Netzwerkservice. Er kann nicht beendet werden. Per Definition kann ein Clientsystem bei einer Netzwerkverbindung zum Port diesen abfragen. Es wird keine Authentifizierung durchgeführt.

Tabelle 3. Appliance-Netzwerkports in Bezug auf Dateien (fortgesetzt)

Port	Service	Protokoll	Zugriffsrichtung	Beschreibung
123	NTP	UDP	Ausgehend	NTP-Zeitsynchronisation. Ist der Port geschlossen, wird die Zeit zwischen Appliances nicht synchronisiert.
135	Microsoft RPC	TCP	Eingehend	Mehrere Zwecke für Microsoft Client. Auch verwendet für NDMP.
137	Microsoft Netbios WINS	UDP; TCP/UDP	Eingehend, Ausgehend	Der NETBIOS Name Service ist mit den Appliance-SMB-Dateifreigabeservices verbunden und eine Kernkomponente dieser Funktion (Wins). Wenn dieser Port deaktiviert ist, deaktiviert er alle SMB-bezogenen Services.
138	Microsoft Netbios BROWSE	UDP	Ausgehend	Der NETBIOS Datagram Service ist mit den Appliance-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.
139	Microsoft CIFS	TCP	Bidirektional	Der NETBIOS Session Service ist mit den Appliance-SMB-Dateifreigabeservices verbunden und eine Kernkomponente dieser Funktion. Wenn SMB-Services aktiviert sind, ist dieser Port geöffnet. Er ist insbesondere für SMB v1 erforderlich.
389	LDAP	TCP/UDP	Ausgehend	Nicht sichere LDAP-Abfragen. Ist dieser Port geschlossen, sind nicht sichere LDAP-Authentifizierungsabfragen nicht verfügbar. Sicheres LDAP ist als Alternative konfigurierbar.
445	Microsoft SMB	TCP	Eingehend	SMB (auf dem Domain Controller) und SMB-Verbindungsport für Windows 2000-Clients und höher. Clients mit befugtem Zugriff auf die Appliance-SMB-Services benötigen für den fortlaufenden Betrieb eine Netzwerkverbindung zum Port. Eine Deaktivierung dieses Ports deaktiviert alle SMB-bezogenen Services. Ist Port 139 ebenfalls deaktiviert, wird die SMB-Dateifreigabe deaktiviert.
464	Kerberos	TCP/UDP	Ausgehend	Erforderlich für Kerberos-Authentifizierungsservices und SMB.
500	IPsec (IKEv2)	UDP	Bidirektional	Damit IPsec trotz Firewalls funktioniert, öffnen Sie UDP-Port 500 und lassen Sie die IP-Protokollnummern 50 und 51 in eingehenden und ausgehenden Firewallfiltern zu. UDP-Port 500 sollte geöffnet werden, damit ISAKMP-Datenverkehr (Internet Security Association and Key Management Protocol) durch Ihre Firewalls weitergeleitet werden kann. Die IP-Protokoll-ID 50 sollte so festgelegt werden, dass die Weiterleitung von IPsec-ESP-Datenverkehr (Encapsulating Security Protocol) zulässig ist. Die IP-Protokoll-ID 51 sollte so festgelegt werden, dass AH-Datenverkehr (Authentication Header) weitergeleitet werden kann. Ist

Tabelle 3. Appliance-Netzwerkports in Bezug auf Dateien (fortgesetzt)

Port	Service	Protokoll	Zugriffsrichtung	Beschreibung
				dieser Port geschlossen, ist die IPsec-Verbindung zwischen den PowerStore-Appliances nicht verfügbar.
636	LDAPS	TCP/UDP	Ausgehend	Sichere LDAP-Abfragen. Ist dieser Port geschlossen, sind sichere LDAP-Authentifizierungsabfragen nicht verfügbar.
1234	NFS mountd	TCP/UDP	Bidirektional	Verwendet für den Mount-Service, der eine Kernkomponente des NFS-Services (Versionen 2, 3 und 4) ist.
2.000	SSHD	TCP	Eingehend	SSHD für Wartung (optional)
2049	NFS I/O	TCP/UDP	Bidirektional	Verwendet für die Bereitstellung von NFS-Services.
3268	LDAP	UDP	Ausgehend	Nicht sichere LDAP-Abfragen. Ist dieser Port geschlossen, sind nicht sichere LDAP-Authentifizierungsabfragen nicht verfügbar.
4.000	STATD für NFSv3	TCP/UDP	Bidirektional	Wird für die Bereitstellung von NFS-statd-Services verwendet. statd ist der Dateisperrmonitor von NFS und nutzt lockd, um Absturz- und Recovery-Funktionen für NFS zu bieten. Ist dieser Port geschlossen, sind NAS-statd-Services nicht verfügbar.
4001	NLMD für NFSv3	TCP/UDP	Bidirektional	Wird für die Bereitstellung von NFS-lockd-Services verwendet. lockd ist der NFS-Daemon für Dateisperren. Er verarbeitet Sperranfragen von NFS-Clients und arbeitet mit dem statd-Daemon zusammen. Ist dieser Port geschlossen, sind NAS-lockd-Services nicht verfügbar.
4002	RQUOTAD für NFSv3	TCP/UDP; UDP	Eingehend, Ausgehend	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.
4.003	XATTRPD (erweitertes Dateiattribut)	TCP/UDP	Eingehend	Erforderlich für das Management von Dateiattributen in einer Umgebung mit mehreren Protokollen.
4658	PAX (NAS-Serverarchiv)	TCP	Eingehend	PAX ist ein Appliance-Archivprotokoll, das mit Standard-UNIX-Bandformaten arbeitet.
8888	RCPD (Replikationsdatenpfad)	TCP	Eingehend	Vom Replikator (auf der sekundären Seite) verwendet. Der Port wird vom Replikator offen gelassen, sobald Daten repliziert werden müssen. Nach dem Starten gibt es keine Möglichkeit, den Service zu beenden.
10.000	NDMP	TCP	Eingehend	• Ermöglicht die Kontrolle von Backup und Recovery eines NDMP (Network Data Management Protocol)-Servers über eine Netzwerkbackupanwendung ohne Installation von Drittanbietersoftware auf dem Server. In einer Appliance fungiert der NAS-Server als NDMP-Server.

Tabelle 3. Appliance-Netzwerkports in Bezug auf Dateien (fortgesetzt)

Port	Service	Protokoll	Zugriffsrichtung	Beschreibung
				• Der NDMP-Service kann deaktiviert werden, wenn keine NDMP-Bandsicherung 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.
[10500,10531]	Von NDMP reservierter Bereich für dynamische NDMP-Ports	TCP	Eingehend	Verwenden Sie für Drei-Wege-Backup/Restore-Sitzungen die NAS-Server Ports 10500 bis 10531.
12228	Virenschutzprüfservice	TCP	Ausgehend	Erforderlich für den Virenschutzprüfservice.

Netzwerkports in Verbindung mit PowerStore X-Modell-Appliances

In der folgenden Tabelle sind die Netzwerkports und die zugehörigen Services der PowerStore X model-Appliances dargestellt.

Tabelle 4. Netzwerkports in Verbindung mit PowerStore X model-Appliances

Port	Service	Protokoll	Zugriffsrichtung	Beschreibung
22	SSH-Server	TCP	Eingehend	Lässt SSH-Zugriff zu (falls aktiviert). Ist der Port geschlossen, sind Managementverbindungen über SSH nicht verfügbar.
80, 9000	vSphere Web Access	TCP	Eingehend	Zugriff auf vSphere Update Manager Webclient-Plug-in für vSphere Webclient.
427	CIM Service Location Protocol (SLP)	TCP/UDP	Bidirektional	Der CIM-Client verwendet das Service Location Protocol, Version 2 (SLPv2), um CIM-Server zu finden.
443	vSphere Webclient	TCP	Eingehend	Wird für Clientverbindungen verwendet.
902	Network File Copy (NFC), VMware vCenter, vSphere Webclient	TCP	• Bidirektional für NFC • Ausgehend für VMware vCenter • Eingehend für vSphere Webclient	• NFC bietet einen Dateityp-fähigen FTP-Dienst für vSphere-Komponenten. ESXi verwendet NFC für Vorgänge wie das standardmäßige Kopieren und Verschieben von Daten zwischen Datenspeichern. • VMware vCenter-Agent • Für vSphere Webclient, für Clientverbindungen verwendet.
5900, 5901, 5902, 5903, 5904	RFB-Protokoll	TCP	Eingehend	Remotezugriff auf grafische Benutzeroberflächen wie VNC.
5988	CIM (Common Information Model)-Server	TCP	Eingehend	Server für CIM.
5989	CIM Secure Server	TCP	Eingehend	Server für CIM.

Tabelle 4. Netzwerkports in Verbindung mit PowerStore X model-Appliances (fortgesetzt)

Port	Service	Protokoll	Zugriffsrichtung	Beschreibung
6999	NSX Virtual Distributed Logical Router, rabbitmqproxy	UDP	• Bidirektionaler Service für NSX Virtual Distributed Router • Ausgehend für rabbitmqproxy	• Für den Service NSX Virtual Distributed Router wird der Firewallport, der diesem Service zugeordnet ist, geöffnet, wenn NSX VIBs installiert und das VDR-Modul erstellt wird. Wenn keine VDR-Instanzen mit dem Host verknüpft sind, muss der Port nicht geöffnet sein. • Für rabbitmqproxy, ein Proxy, der auf dem ESXi-Host ausgeführt wird. Dieser Proxy erlaubt, dass Anwendungen, die innerhalb von virtuellen Maschinen ausgeführt werden, mit den AMQP-Brokern kommunizieren, die in der vCenter-Netzwerk-Domain ausgeführt werden. Die virtuelle Maschine muss nicht im Netzwerk sein, d. h. es ist keine NIC erforderlich. Stellen Sie sicher, dass die IP-Adressen der ausgehenden Verbindung mindestens die Broker in Verwendung oder die zukünftigen Broker umfassen. Sie können Broker später hinzufügen, um zu skalieren.
8.000	vMotion	TCP	Bidirektional	Erforderlich für die Migration von virtuellen Maschinen mit vMotion. ESXi-Hosts überwachen Port 8000 für TCP-Verbindungen von Remote-ESXi Hosts für vMotion-Datenverkehr.
8100, 8200, 8300	Fehlertoleranz	TCP/UDP	Bidirektional	Wird für den Datenverkehr zwischen Hosts für vSphere Fehlertoleranz (FT) verwendet.
8301, 8302	DVSSync	UDP	Bidirektional	DVSSync-Ports werden zum Synchronisieren von Zuständen verteilter virtueller Ports zwischen Hosts verwendet, auf denen VMware FT Aufnahme/Wiedergabe aktiviert ist. Bei Hosts, die virtuelle primäre oder Backupmaschinen ausführen, müssen diese Ports geöffnet sein. Auf Hosts, die VMware FT nicht verwenden, müssen diese Ports nicht geöffnet sein.
9080	I/O-Filter	TCP	Ausgehend	Wird von der Speicherfunktion „I/O-Filter“ verwendet.
31031	vSphere Replication, VMware Site Recovery Manager	TCP	Ausgehend	Wird für den kontinuierlichen Replikationsdatenverkehr von vSphere Replication und VMware Site Recovery Manager verwendet.
44046	vSphere Replication, VMware Site Recovery Manager	TCP	Ausgehend	Wird für den kontinuierlichen Replikationsdatenverkehr von vSphere Replication und VMware Site Recovery Manager verwendet.

3

Auditing

Dieses Kapitel enthält die folgenden Informationen:

Themen:

- Auditing

Auditing

Auditing bietet eine Verlaufsansicht der Nutzeraktivitäten auf dem System. Ein Nutzer mit der Rolle eines Administrators, Sicherheitsadministrators oder Speicheradministrators kann die REST API verwenden, um Konfigurationsänderungsereignisse auf dem System zu suchen und anzuzeigen. Die Ereignisse, die auditiert werden, beziehen sich nicht nur auf die Sicherheit, alle festgelegten Vorgänge (d. h. POST/PATCH/DELETE) werden auditiert.

Andere Schnittstellen, wie z. B. die PowerStore Manager-Benutzeroberfläche und die CLI, können zum Suchen und Anzeigen von Auditereignissen verwendet werden.

4

Datensicherheitseinstellungen

Dieser Abschnitt enthält die folgenden Themen:

Themen:

- Data-at-Rest-Verschlüsselung
- Verschlüsselungsaktivierung
- Verschlüsselungsstatus
- Key-Management
- Keystore-Backupdatei
- Neuverwendung eines Laufwerks in einer Appliance mit aktivierter Verschlüsselung
- Austauschen eine Basisgehäuses und von Nodes bei einem System mit aktivierter Verschlüsselung
- Zurücksetzen einer Appliance auf die Werkseinstellungen

Data-at-Rest-Verschlüsselung

Data-at-Rest-Verschlüsselung (D@RE) in PowerStore nutzt FIPS 140-2 validierte selbstverschlüsselnde Festplatten (SEDS) für primären Speicher (NVMe SSD, NVMe SCM und SAS SSD). Das NVRAM-Zwischenspeichergerät ist verschlüsselt, aber derzeit nicht FIPS-140-2-validiert.

Die Verschlüsselung wird auf jeder Festplatte durchgeführt, bevor die Daten auf den Datenträger geschrieben werden. Dadurch werden die Daten auf dem Laufwerk vor Diebstahl oder Verlust und dem Versuch geschützt, sie durch Zerlegen des Laufwerks direkt auszulesen. Die Verschlüsselung bietet außerdem die Möglichkeit, schnell und sicher Informationen auf einem Laufwerk so zu löschen, dass sie nicht wiederherstellbar sind. Neben dem Schutz vor Bedrohungen durch das physische Entfernen von Medien können die Medien auch neu verwendet werden. Hierfür muss der zum Schutz der zuvor auf diesem Medium gespeicherten Daten verwendete Verschlüsslungsschlüssel zerstört werden.

Das Lesen verschlüsselter Daten erfordert einen Authentifizierungsschlüssel, um das Laufwerk zu entsperren. Nur authentifizierte SEDs können entsperrt werden. Nach dem Entsperren der Festplatte werden die Daten zurück in ihre ursprüngliche Form entschlüsselt.

Die PowerStore-Appliance muss alle SEDs enthalten. Wenn Sie versuchen, eine nicht selbstverschlüsselnde Festplatte zu einer Appliance hinzuzufügen, gibt die Appliance einen Fehler aus. Außerdem werden unverschlüsselte Appliances nicht in einem verschlüsselten Cluster unterstützt.

Verschlüsselungsaktivierung

Die Data-at-Rest-Verschlüsselung auf PowerStore-Appliances wird werkseitig eingestellt. In allen Ländern, die den Import einer Appliance erlauben, die Verschlüsselung unterstützt, ist die Verschlüsselung standardmäßig aktiviert. Nach der Aktivierung kann die Verschlüsselung nicht mehr deaktiviert werden. In allen Ländern, in denen der Import einer Appliance, die Verschlüsselung unterstützt, nicht zulässig ist, wird die Data-at-Rest-Verschlüsselung deaktiviert.

ANMERKUNG: Appliances, die die Data-at-Rest-Verschlüsselung nicht unterstützen, dürfen nicht mit zusammen mit verschlüsselten Appliances verwendet werden.

Verschlüsselungsstatus

Der Verschlüsselungsstatus für eine Appliance wird für den folgenden Ebenen angezeigt:

- Clusterebene
- Appliance-Ebene
- Laufwerksebene

Der Verschlüsselungsstatus auf Clusterebene zeigt, ob eine Appliance-Verschlüsselung aktiviert ist. Er hängt nicht mit dem Laufwerksstatus zusammen.

Der Verschlüsselungsstatus einer Appliance kann wie folgt lauten:

- Encrypted: Die Verschlüsselungsfunktion ist auf der Appliance aktiviert.
- Unencrypted: Die Verschlüsselungsfunktion wird auf der Appliance nicht unterstützt.
- Encrypting: Wird während des Vorgangs der Verschlüsselungsaktivierung angezeigt. Wenn der Verschlüsselungsvorgang erfolgreich abgeschlossen wurde, wird der Verschlüsselungsstatus auf Clusterebene als „Encrypted“ angezeigt.

Der Verschlüsselungsstatus auf Laufwerksebene wird für jedes Laufwerk in einer Appliance angegeben und kann wie folgt lauten:

- Encrypted: Das Laufwerk ist verschlüsselt. Dies ist der typische Status eines Laufwerks in einer Appliance, die verschlüsselungsfähig ist.
- Encrypting: In der Appliance wird gerade die Verschlüsselung auf dem Laufwerk aktiviert. Dieser Status kann bei der erstmaligen Aktivierung der Verschlüsselung auf einer Appliance oder beim Hinzufügen von neuen Laufwerken zu einer konfigurierten Appliance zu sehen sein.
- Disabled: Beim Laufwerk kann aufgrund von landesspezifischen Importeinschränkungen keine Verschlüsselung aktiviert sein. Wenn ein Laufwerk diesen Status meldet, gilt er ebenso für alle anderen Laufwerke im Cluster.
- Unknown: Die Appliance hat noch nicht versucht, die Verschlüsselung auf dem Laufwerk zu aktivieren. Dieser Status kann bei der erstmaligen Aktivierung der Verschlüsselung auf einer Appliance oder beim Hinzufügen von neuen Laufwerken zu einer konfigurierten Appliance zu sehen sein.
- Unsupported: Das Laufwerk unterstützt keine Verschlüsselung.
- Foreign: Das Laufwerk wird unterstützt, ist jedoch durch eine andere Appliance gesperrt. Es muss für diese Appliance außer Betrieb gesetzt werden, bevor es verwendet werden kann.

Key-Management

Ein integrierter Key Manager Service (KMS) wird auf dem aktiven Node jeder PowerStore-Appliance ausgeführt. Mit diesem Service wird der lokale Keystore-Datei-Lockbox-Speicher zur Unterstützung des automatischen Verschlüsselungsschlüsselbackups auf System- und Startlaufwerken verwaltet. Außerdem steuert er den Prozess der Sperrung und Entsperrung der selbstverschlüsselnden Festplatten (Self-Encrypting Drives, SEDs) auf der Appliance und ist für die Verwaltung des lokalen Keystore-Inhalts für die Appliance zuständig. Die lokale Keystore-Datei wird mit einem 256-Bit-AES-Schlüssel verschlüsselt und der Keystore-Datei-Lockbox-Speicher nutzt die BSAFE-Technologie von RSA.

Der KMS erzeugt während der Initialisierung der Appliance automatisch einen zufälligen Authentifizierungsschlüssel für SEDs. Jedes Laufwerk, einschließlich derjenigen, die später der Appliance hinzugefügt werden, verfügt über einen eindeutigen Authentifizierungsschlüssel, der bei der Sperrung und Entsperrung von SEDs verwendet wird. Mit einem Verschlüsselungsschlüssel werden die Authentifizierungs- und Verschlüsselungsschlüssel im Keystore-Dateispeicher und ad hoc in der Appliance verschlüsselt. Medienverschlüsselungsschlüssel werden auf der dedizierten Hardware der SEDs gespeichert und es kann nicht darauf zugegriffen werden. Wenn die Verschlüsselung aktiviert ist, werden alle Authentifizierungsschlüssel innerhalb der Appliance gespeichert.

Keystore-Backupdatei

Der KMS unterstützt das Erstellen und Herunterladen eines Backups der Keystore-Archivdatei außerhalb der Appliance. Dieses sogenannte Off-Appliance-Backup reduziert die Wahrscheinlichkeit eines schwerwiegenden Schlüsselverlusts, durch den eine Appliance oder ein Cluster unbrauchbar werden würde. Wenn beim Initiieren eines Keystore-Clusterbackups eine bestimmte Appliance nicht verfügbar ist, wird der allgemeine Vorgang erfolgreich ausgeführt, aber es wird eine Warnung ausgegeben, dass das Backup keine Keystore-Dateien für alle Appliances im Cluster enthält und dass der Vorgang erneut versucht werden sollte, wenn die Offline-Appliance verfügbar ist.

ANMERKUNG: Die primäre Appliance in einem Cluster enthält eine Keystore-Clusterarchivdatei mit einer Kopie der Keystore-Backups jeder Appliance, die im Cluster erkannt wird, einschließlich der primären Appliance.

Wenn Änderungen an der Konfiguration eines Systems innerhalb des Clusters auftreten, die zu Änderungen am Keystore führen, wird empfohlen, dass Sie eine neue Keystore-Archivdatei für den Download erzeugen. Es kann jeweils nur ein Backupdownloadvorgang der Keystore-Archivdatei ausgeführt werden.

ANMERKUNG: Es wird dringend empfohlen, dass Sie die erzeugte Keystore-Archivdatei an einen externen, sicheren Speicherort herunterladen. Wenn die Keystore-Dateien auf einem System beschädigt und nicht mehr zugänglich sind, wird das System in den Servicemodus versetzt. In diesem Fall sind zur Behebung die Keystore-Backupdatei und ein Serviceprojekt erforderlich.

Zum Sichern der Keystore-Archivdatei ist die Nutzerrolle Administrator oder Speicheradministrator erforderlich. Zum Sichern der Keystore-Archivdatei klicken Sie auf **Settings** und wählen Sie unter **Security** die Option **Encryption** aus. Klicken Sie auf der Seite **Encryption** unter **Lockbox Backup** auf **Download Keystore Backup**.

ANMERKUNG: Wenden Sie sich an Ihren Serviceanbieter, um das Keystore-Backup im Falle eines Fehlers wiederherzustellen.

Neuverwendung eines Laufwerks in einer Appliance mit aktivierter Verschlüsselung

Info über diese Aufgabe

Eine selbstverschlüsselnde Festplatte (Self-Encrypting Drive, SED) wird gesperrt, wenn eine Appliance initialisiert oder wenn sie in eine bereits initialisierte Appliance eingesetzt wird. Die Festplatte kann nicht in einem anderen System verwendet werden, ohne dass sie zunächst entsperrt wird. Die gesperrte Festplatte ist nicht nutzbar, wenn sie in eine andere Appliance eingesetzt und der Verschlüsselungsstatus in der neuen Appliance als `Foreign` angezeigt wird. Die Festplatte kann in der anderen Appliance neu verwendet werden, allerdings gehen dabei alle vorhandenen Daten verloren.

Gehen Sie wie folgt vor, um eine Festplatte mit dem `Foreign`-Verschlüsselungsstatus auf einer Appliance neu zu verwenden:

Schritte

1. Notieren Sie sich die PSID (Physische Sicherheit-ID), die sich auf dem Etikett auf der Rückseite der Festplatte befindet. Die PSID muss im Rahmen des Prozesses der Neuverwendung angegeben werden.
2. Klicken Sie im PowerStore Manager auf **Hardware**, wählen Sie die Appliance aus und wählen Sie die Karte **Hardware** aus.
3. Wählen Sie die Festplatte aus, die Sie neu verwenden möchten.
   Der Verschlüsselungsstatus für die Festplatte unter **Encryption Status** sollte als `Foreign` angezeigt werden.
4. Klicken Sie auf **Repurpose Drive**.
   Das Popup-Menü **Repurpose Drive** wird angezeigt.
5. Geben Sie die PSID der Festplatte ein und klicken Sie auf **Apply**.

Ergebnisse

Die Festplatte wird in der Appliance als neue Festplatte neu verwendet und ihr Verschlüsselungsstatus ändert sich abschließend in `Encrypted`.

Austauschen eine Basisgehäuses und von Nodes bei einem System mit aktivierter Verschlüsselung

Zum Austauschen eines base enclosure und von nodes bei einer Appliance mit aktivierter Verschlüsselung ist ein Serviceprojekt erforderlich.

Zurücksetzen einer Appliance auf die Werkseinstellungen

Mit dem Serviceskript `svc_factory_reset` wird ein einzelner Appliance-Cluster auf den Werkszustand zurückgesetzt und alle Nutzerdaten und permanenten Konfigurationen werden gelöscht.

Für Multi-Appliance-Cluster kann `svc_factory_reset` nicht auf den sekundären Appliances ausgeführt werden. Stattdessen muss das Serviceskript `svc_remove_appliance` ausgeführt werden. Dieses Skript setzt eine sekundäre Appliance in den Werkszustand zurück und löscht alle Nutzerdaten und permanenten Konfigurationen. Wenn nur die primäre Appliance im Cluster bleibt, können Sie `svc_factory_reset` ausführen, um diese Appliance zurückzusetzen.

ANMERKUNG: Es wird empfohlen, dass diese Skripte nur von einem qualifizierten Serviceanbieter ausgeführt werden.

Weitere Informationen zu diesen Skripten finden Sie im *PowerStore Service Scripts Guide*.

5

Sichere Wartungseinstellungen

Dieses Kapitel enthält die folgenden Informationen:

Themen:

- Funktionsbeschreibung von SupportAssist
- SupportAssist-Optionen
- SupportAssist Gateway Connect-Optionen
- SupportAssist Direct Connect-Optionen
- Voraussetzungen für SupportAssist Gateway Connect
- Voraussetzungen für SupportAssist Direct Connect
- Konfigurieren von SupportAssist
- Konfigurieren von SupportAssist

Funktionsbeschreibung von SupportAssist™

Die SupportAssist-Funktion bietet eine IP-basierte Verbindung, über die der Dell EMC Support Fehlerdateien und Warnmeldungen von Ihrer Appliance erhält und ein Remote-Troubleshooting durchführen kann, wodurch eine schnelle und effiziente Behebung möglich ist.

ANMERKUNG: Es wird dringend empfohlen, die SupportAssist-Funktion zu aktivieren, um die Problemdiagnose zu beschleunigen, Troubleshooting durchzuführen und das Problem schneller zu beheben. Wenn Sie die SupportAssist-Funktion nicht aktivieren, müssen Sie Appliance-Informationen eventuell manuell sammeln, um den Dell EMC Support beim Troubleshooting und der Problemlösung für die Appliance zu unterstützen. Auf der Appliance muss die SupportAssist-Funktion aktiviert sein, damit Daten an CloudIQ gesendet werden können. Weitere Informationen zu CloudIQ finden Sie unter www.dell.com/support. Melden Sie sich an, und suchen Sie die CloudIQ-Seite **Product Support**.

SupportAssist und Sicherheit

Bei jedem Schritt des Remoteverbindungsprozesses der SupportAssist-Funktion kommen mehrere Sicherheitsebenen zum Tragen, die dafür sorgen, dass Sie und Dell EMC die Lösung ohne Sicherheitsbedenken nutzen können:

- Die komplette Kommunikation an Dell EMC wird von Ihrem Standort aus und niemals von einer externen Quelle gesendet und mit 256-Bit-AES-Verschlüsselung gesichert (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 Dell EMC erfolgt mit Authentifizierung in beiden Richtungen durch digitale RSA®-Zertifikate.
- Nur autorisierte Dell EMC Customer Service-Experten mit einer gültigen Zwei-Faktor-Authentifizierung können die digitalen Zertifikate zur Anzeige einer Benachrichtigung von Ihrem Standort herunterladen.
- Mit der optionalen Anwendung SupportAssist v3 Policy Manager können Sie den Zugriff des Dell EMC Support basierend auf Ihren eigenen Richtlinien und Anforderungen gewähren oder einschränken. Außerdem umfasst die Anwendung ein detailliertes Auditprotokoll.

SupportAssist-Verwaltung

Sie können die SupportAssist-Funktion mit dem PowerStore Manager oder der REST API verwalten. Sie können den Service aktivieren oder deaktivieren und die entsprechenden Informationen angeben, die für die ausgewählte SupportAssist-Option erforderlich sind.

ANMERKUNG: Die Optionen **Gateway Connect with remote assist** und **Gateway Connect ohne remote assist** für zentralisierte SupportAssist unterstützen keine hohe Verfügbarkeit (High Availability, HA). Diese Optionen stellen keine Failover-Fähigkeit auf einem aktiven HA-SupportAssist-Cluster bereit. Wenn die PowerStore-Appliance auf einem einzelnen HA-Gateway-

Clusterserver (die einzige Konfigurationsoption) bereitgestellt wird, besteht keine Failover-Fähigkeit für den noch funktionierenden Gatewayserver im Cluster. Wenn der HA-Gatewayserver, mit dem die Appliance verbunden ist, ausfällt, beendet die Appliance die Übertragung aller ausgehenden Dateien, z. B. Call-Home- und CloudIQ-Dateien, an den Dell EMC Support. Die eingehende SupportAssist-Verbindung für den Remotezugriff zur Appliance funktioniert nach wie vor mit dem noch funktionierenden HA-Gatewayserver im Cluster. Außerdem sollte die SupportAssist-Option **Gateway Connect with remote assist** und **Gateway Connect without remote assist** nur auf der festgelegten primären Appliance auf dem System konfiguriert werden.

Die Appliance selbst implementiert keine Policies. Wenn Sie den Remotezugriff auf Ihre Appliance stärker kontrollieren möchten, können Sie Autorisierungsrechte mithilfe eines Policy Manager festlegen. 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 Ihre Appliance zugreift. Weitere Informationen über den Policy Manager finden Sie unter www.dell.com/support. Rufen Sie nach der Anmeldung die entsprechende **Support by Product**-Seite auf und suchen Sie den Link für die technische Dokumentation zu diesem SupportAssist-Produkt.

SupportAssist-Kommunikation

ANMERKUNG: SupportAssist können nicht auf PowerStore-Modellen aktiviert werden, die mit IPv6 für das Managementnetzwerk konfiguriert wurden. SupportAssist wird nicht über IPv6 unterstützt. Außerdem ist eine Neukonfiguration des Managementnetzwerks von IPv4 auf IPv6 nicht zulässig, wenn SupportAssist auf einem Cluster konfiguriert ist.

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

Der **Connection Status** von SupportAssist zeigt den Status der Verbindung zwischen PowerStore und der Dell EMC Back-End-Support Services und die Servicequalität der Verbindung an. Der Verbindungsstatus wird über einen Zeitraum von fünf Minuten festgelegt und die Servicequalität der Verbindung wird über 24 Stunden festgelegt. Der **Connection Status** der Verbindung kann basierend auf einer der Appliances im Cluster als eine der folgenden angezeigt werden:

- `Unavailable` – Es sind keine Verbindungsdaten verfügbar. Sie haben möglicherweise den Kontakt zu einer Appliance verloren oder SupportAssist wurde gerade aktiviert und es sind nicht genügend Daten vorhanden, um den Status zu bestimmen.
- `Disabled` – SupportAssist wurde nicht aktiviert.
- `Not connected` – Die Verbindung wurde getrennt. Fünf aufeinanderfolgende KeepAlive-Ausfälle wurden erkannt.
- `Reconnecting` – PowerStore versucht, die Verbindung nach Verbindungsverlust wiederherzustellen. Fünf aufeinanderfolgende erfolgreiche KeepAlive-Anforderungen werden benötigt, um zu einem verbundenen Status zurückzukehren.

Der **Connection Status** der Verbindung kann als einer der folgenden basierend auf dem Durchschnitt aller Appliances im Cluster angezeigt werden, wenn PowerStore mit den Dell EMC Back-End-Support Services verbunden ist:

- `Evaluating` – Die Servicequalität für die Verbindung ist für die ersten 24 Stunden nach der ersten Initialisierung von SupportAssist unbestimmt.
- `Good` – 80 % oder mehr der aufeinanderfolgenden KeepAlive-Anforderungen waren erfolgreich.
- `Fair` – Zwischen 50 % und 80 % der aufeinanderfolgenden KeepAlive-Anforderungen waren erfolgreich.
- `Poor` – Weniger als 50 % der aufeinanderfolgenden KeepAlive-Anforderungen waren erfolgreich.

SupportAssist-Optionen

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

Folgende SupportAssist-Optionen sind verfügbar, mit denen Appliance-Informationen an den Dell EMC Support für ein Remote-Troubleshooting gesendet werden kann:

- Gateway Connect ohne Remotezugriff: für zentralisiertes SupportAssist und Ausführungen auf einem vom Kunden bereitgestellten Gatewayserver mit bidirektionaler Dateiübertragung, einschließlich:
  - Call Homes
  - CloudIQ-Unterstützung
  - Softwarebenachrichtigungen
  - Betriebsumgebungs-/Firmwaredownload vom Dell EMC Support zum Cluster

  Der SupportAssist-Gatewayserver ist der zentrale Einstiegs- und Ausstiegspunkt für alle IP-basierten SupportAssist-Aktivitäten für die Appliances, die mit dem Gateway verknüpft sind.

- Gateway Connect mit Remotezugriff: für zentralisiertes SupportAssist und Ausführungen auf einem vom Kunden bereitgestellten Gatewayserver mit derselben bidirektionalen Dateiübertragung wie Gateway Connect ohne Remotezugriff, aber mit Remotezugriff für Dell EMC Supportmitarbeiter.
- Direct Connect ohne Remotezugriff: für verteiltes SupportAssist, das auf einzelnen Appliances mit derselben bidirektionalen Dateiübertragung ausgeführt wird wie Gateway Connect ohne Remotezugriff.
- Direct Connect mit Remotezugriff: für verteiltes SupportAssist, das auf einzelnen Appliances mit derselben bidirektionalen Dateiübertragung wie Gateway Connect ohne Remotezugriff ausgeführt wird, aber mit Remotezugriff für Dell EMC Supportmitarbeiter.

Eine weitere Option, „Disabled“, ist zwar verfügbar, wird aber nicht empfohlen. Wenn Sie diese Option auswählen, erhält der Dell EMC Support keine Benachrichtigungen über Probleme mit der Appliance. Sie müssen Appliance-Informationen möglicherweise manuell sammeln, um Supportmitarbeiter beim Troubleshooting und bei der Behebung von Problemen mit der Appliance zu unterstützen.

SupportAssist Gateway Connect-Optionen

SupportAssist Gateway Connect wird auf einem Gatewayserver ausgeführt. Wenn Sie entweder die Option **Gateway Connect without remote access** oder die Option **Gateway Connect with remote access** auswählen, wird Ihre Appliance anderen Appliances in einem SupportAssist-Cluster hinzugefügt. Der Cluster befindet sich hinter einer einzigen, gemeinsamen, (zentralen) sicheren Verbindung zwischen den Dell EMC Supportservern und einem arrayexternen Gatewayserver. Der Gatewayserver ist der zentrale Einstiegs- und Ausstiegspunkt für alle IP-basierten Dell EMC SupportAssist-Aktivitäten für die Appliances, die mit dem Gateway verknüpft sind.

Der Gatewayserver ist eine Lösung für Remotesupport, die auf einem oder mehreren vom Kunden bereitgestellten dedizierten Servern installiert ist. Der Gatewayserver fungiert als Kommunikationsbroker zwischen den zugehörigen Appliances und Dell EMC.

Weitere Informationen zu SupportAssist-Gateway finden Sie auf der SupportAssist-Produktseite der Dell Support-Website (www.dell.com/support).

Wenn Sie die Appliance so konfigurieren möchten, dass die Option **Gateway Connect without remote access** oder die Option **Gateway Connect with remote access** für SupportAssist verwendet wird, müssen Sie die IP-Adresse und die Portnummer (9443 ist der Standardwert) des Gatewayservers angeben. Stellen Sie außerdem sicher, dass der Port zwischen dem Gatewayserver und der Appliance geöffnet ist.

ANMERKUNG: Der Gatewayserver muss funktionsfähig sein, bevor Sie die Appliance für seine Verwendung konfigurieren können. Appliances können nur über den PowerStore Manager zum Gateway hinzugefügt werden. Wenn die Appliance vom Gatewayserver aus hinzugefügt wird, scheint sie verbunden zu sein, jedoch können Systeminformationen nicht erfolgreich gesendet werden.

SupportAssist Direct Connect-Optionen

SupportAssist Direct Connect wird direkt auf dem primären Node jeder Appliance ausgeführt. In einem Cluster stellt jede Appliance eine eigene Verbindung zum Dell EMC Support her. Der Datenverkehr wird nicht über die primäre Appliance in einem Cluster geroutet. SupportAssist kann jedoch nur auf Clusterebene verwaltet werden, d. h. alle Änderungen werden auf alle Appliances im Cluster angewendet.

Aktivieren und konfigurieren Sie SupportAssist Direct Connect über die Seite **Support Assist**, auf die über **Settings** zugegriffen werden kann und die unter **Support** in der PowerStore Manager angezeigt wird. Diese Aktionen richten die Appliance so ein, dass eine sichere Verbindung zwischen ihr selbst und Dell EMC Support verwendet wird. Sie können eine der folgenden Optionen für Remoteserviceverbindungen für SupportAssist Direct Connect auswählen:

- **Direct Connect without remote access**
- **Direct Connect with remote access**

Wenn Sie die Option **Direct Connect without remote access** auswählen und die Endnutzer-Lizenzvereinbarung (EULA) akzeptieren, stellt die Appliance eine sichere Verbindung zum Dell EMC Support her. Diese Option ermöglicht die bidirektionale Dateiübertragung zum und vom Dell EMC Support. Gegebenenfalls können Sie die Verbindung von der Appliance zu einem zugehörigen Proxyserver (optional) konfigurieren. Falls erforderlich, können Sie ein Upgrade auf Direct Connect mit Remotezugriffkonfiguration zu einem späteren Zeitpunkt durchführen.

Wenn Sie die Option **Direct Connect with Remote Access** auswählen und die Endnutzer-Lizenzvereinbarung (EULA) akzeptieren, stellt die Appliance eine sichere Verbindung zum Dell EMC Support her. Diese Option ermöglicht die Remotezugriff-Serviceverbindung für die Appliance zum und vom Dell EMC Support zusammen mit einer bidirektionalen Dateiübertragung. Gegebenenfalls können Sie die Verbindung von der Appliance zu einem Policy Manager (optional) und allen zugehörigen Proxyservern (optional) über den PowerStore Manager konfigurieren.

Wenn eine neue Appliance zu einem vorhandenen Cluster hinzugefügt wird, erkennt sie die SupportAssist-Clustereinstellungen und wird automatisch konfiguriert. Wenn SupportAssist Direct Connect derzeit aktiviert ist, wird dies automatisch auf der neuen Appliance aktiviert.

Es sind keine weiteren Aktionen erforderlich. Wenn SupportAssist Direct Connect nicht aktiviert werden kann, verhindert dies nicht das Hinzufügen der Appliance.

Voraussetzungen für SupportAssist Gateway Connect

Die folgenden Voraussetzungen gelten für die SupportAssist-Implementierungen **Gateway Connect without remote access** und **Gateway Connect with remote access**:

- Netzwerkverkehr (HTTPS) muss auf Port 9443 (oder einem vom Kunden definierten Port) zwischen der Appliance und dem SupportAssist-Gatewayserver zugelassen sein.
- SupportAssist muss Version 4.0.5 oder Version 3.38 aufweisen.

ANMERKUNG: Eine Appliance darf nie manuell zu einem Gatewayserver hinzugefügt oder von diesem entfernt werden. Verwenden Sie immer den PowerStore Manager SupportAssist-Konfigurationsassistenten, um eine Appliance zu einem Gatewayserver hinzuzufügen oder von ihm zu entfernen.

Voraussetzungen für SupportAssist Direct Connect

Die folgenden Voraussetzungen gelten für die SupportAssist-Implementierungen mit **Direct Connect without remote access** und mit **Direct Connect with remote access**:

- Netzwerkverkehr (HTTPS) muss an den Ports 443 und 8443 (ausgehend) für den Dell EMC Support 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.

Die folgende Voraussetzung gilt nur für die SupportAssist-Implementierung mit **Direct Connect with Remote Access**:

- Falls Ihre Implementierung einen Policy Manager für eine bessere Steuerung des Remotezugriffs auf die Appliance umfasst, müssen Sie dies bei der Konfiguration der SupportAssist-Funktion angeben.

Konfigurieren von SupportAssist

Sie können SupportAssist mithilfe einer der folgenden Methoden für eine Appliance konfigurieren:

- Assistent für die Erstkonfiguration: eine Benutzeroberfläche, die Sie durch die anfängliche Einrichtung von PowerStore Manager führt und das System für die Nutzung vorbereitet.
- **Support Assist**: Eine Einstellungsseite, auf die Sie über den PowerStore Manager zugreifen können (klicken Sie auf **Settings** und wählen Sie unter **Support** die Option **SupportAssist** aus).
- REST-API-Server: Eine Anwendungsschnittstelle, die REST-API-Anforderungen zur Konfiguration der SupportAssist-Einstellungen empfangen kann. Weitere Informationen über die REST API finden Sie im PowerStore REST API Reference Guide.

Um den Status der SupportAssist-Funktion zu bestimmen, klicken Sie auf **Settings** und wählen Sie unter **Support** die Option **SupportAssist** im PowerStore Manager aus.

Konfigurieren von SupportAssist

Info über diese Aufgabe

Gehen Sie wie folgt vor, um SupportAssist mithilfe des PowerStore Manager zu konfigurieren:

ANMERKUNG: Das Ändern der Option **Direct Connect with remote access** auf die Option **Direct Connect without remote access** oder **Gateway Connect** erfordert Unterstützung durch Dell EMC Supportmitarbeiter.

Schritte

1. Klicken Sie auf **Settings** und wählen Sie unter **Support** die Option **SupportAssist** aus.
2. Wenn der Status von SupportAssist als „Disabled“ angezeigt wird, klicken Sie auf das Steuersymbol **SupportAssist**, um SupportAssist zu aktivieren.

   Obwohl die SupportAssist-Funktion deaktiviert werden kann, wird dies nicht empfohlen.

Die Schaltfläche sollte sich nach rechts verschieben und die Anzeige sollte sich ändern zu `Enabled`. Der **Connection Status** ändert sich jedoch erst, nachdem Sie die erforderlichen Konfigurationsinformationen eingegeben und auf **Apply** geklickt haben.

3. Unter **SupportAssist** ist das Kontrollkästchen **Connect to CloudIQ** standardmäßig aktiviert. Wenn Sie keine Dateien an CloudIQ senden möchten, deaktivieren Sie das Kontrollkästchen. Lassen Sie das Kontrollkästchen andernfalls aktiviert.
4. Wählen Sie in der Liste unter **Type** die SupportAssist-Option aus, die Sie verwenden möchten.
5. Je nachdem, welche SupportAssist-Option Sie ausgewählt haben, führen Sie danach einen der folgenden Schritte aus:
   - Für die Optionen **Gateway Connect without remote access** oder **Gateway Connect with remote access**:
     - Geben Sie die IP-Adresse des Gatewayservers an.
       ANMERKUNG: Der Gatewayserver muss funktionsfähig sein, bevor Sie die Appliance für seine Verwendung konfigurieren können.
     - Wenn der Port, der für die Verbindung mit dem Gatewayserver verwendet wird, sich von der Standardeinstellung (9443) unterscheidet, wählen Sie mithilfe der Steuerelemente die Nummer des Ports aus, der in Ihrem Netzwerk verwendet werden soll.
   - Für die Option **Direct Connect without remote access**:
     - Wenn für Ihre Netzwerkverbindung ein Proxyserver verwendet wird, geben Sie die IP-Adresse des Proxyservers an.
       ANMERKUNG: Der Proxyserver muss funktionsfähig sein, bevor Sie Ihr System für seine Verwendung konfigurieren können.
     - Verwenden Sie die Steuerelemente, um die Nummer des Ports auszuwählen, der für die Verbindung mit dem Proxyserver in Ihrem Netzwerk verwendet werden soll.
   - Für die Option **Direct Connect with Remote Access**:
     - Wenn für Ihre Netzwerkverbindung ein Proxyserver verwendet wird, geben Sie die IP-Adresse des Proxyservers an.
       ANMERKUNG: Der Proxyserver muss funktionsfähig sein, bevor Sie Ihre Appliance für seine Verwendung konfigurieren können.
     - Verwenden Sie die Steuerelemente, um die Nummer des Ports auszuwählen, der für die Verbindung mit dem Proxyserver in Ihrem Netzwerk verwendet werden soll.
     - Wenn Sie beabsichtigen, einen Policy Manager für die Steuerung des Remotezugriffs auf das System zu verwenden, geben Sie die IP-Adresse des Policy Manager an.
       ANMERKUNG: Der Policy Manager muss funktionsfähig sein, bevor Sie die Appliance für seine Verwendung konfigurieren können.
     - Wenn der Port, der für die Verbindung mit dem Policy Manager verwendet wird, sich vom Standardwert (9443) unterscheidet, geben Sie die Nummer des Ports ein.
6. Je nachdem, welche SupportAssist-Option Sie ausgewählt haben, führen Sie danach einen der folgenden Schritte aus:
   - Gehen Sie für die Option **Direct Connect without remote access** oder für die Option **Direct Connect with remote access** zum nächsten Schritt.
   - Wählen Sie für die Option **Gateway Connect without remote access** oder für die Option **Gateway Connect with Remote Access** die Option **Test Connection** aus, um den Status der Verbindung zum Gatewayserver zu überprüfen.

   ANMERKUNG: Wenn der Konnektivitätsstatus im Status `Transitioning` bleibt und sich nach einigen Minuten nicht ändert (nach der Zeit, die zum Testen der Verbindung erforderlich sein sollte), wenden Sie sich an den Onlinesupport.
7. Wählen Sie **Send Test Alert**, um eine Testwarnmeldung an den Dell EMC Support zu senden und die End-to-End-Konnektivität zu prüfen.
8. Stellen Sie sicher, dass die angezeigten Kontaktinformationen korrekt sind. Korrigieren Sie alle Informationen, die falsch oder veraltet scheinen.

   Ihre SupportAssist-Kontaktinformationen sind wichtig für eine schnelle Reaktion auf Supportprobleme und müssen genau und aktuell sein.
9. Wählen Sie **Apply** aus, um die SupportAssist-Konfigurationsinformationen beizubehalten.

A

TLS-Chiffren

Dieser Anhang enthält folgende Informationen:

Themen:

- Unterstützte TLS-Cipher Suites

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 Cipher Suites über TLS für die Appliance und die zugehörigen Ports aufgeführt.

Tabelle 5. Standardmäßige, von der Appliance unterstützte Cipher Suites über TLS

Cipher Suites	Protokolle	Ports
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	TLSv1.2	443, 8443
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	TLSv1.2	443, 8443
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	TLSv1.2	443, 8443
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	TLSv1.2	443, 8443
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	TLSv1.2	443, 8443
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	TLSv1.2	443, 8443
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	TLSv1.2	443, 8443
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	TLSv1.2	443, 8443
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	TLSv1.2	443, 8443
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	TLSv1.2	443, 8443
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	TLSv1.2	443, 8443
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	TLSv1.2	443, 8443
TLS_RSA_WITH_AES_128_CBC_SHA	TLSv1.2	443, 8443
TLS_RSA_WITH_AES_128_CBC_SHA256	TLSv1.2	443, 8443
TLS_RSA_WITH_AES_128_GCM_SHA256	TLSv1.2	443, 8443
TLS_RSA_WITH_AES_256_CBC_SHA	TLSv1.2	443, 8443
TLS_RSA_WITH_AES_256_CBC_SHA256	TLSv1.2	443, 8443
TLS_RSA_WITH_AES_256_GCM_SHA384	TLSv1.2	443, 8443