SANtricity Unified Manager

SANtricity 11.9

NetApp
February 14, 2025

This PDF was generated from https://docs.netapp.com/de-de/e-series-santricity/um-admin/overview-interface-unified.html on February 14, 2025. Always check docs.netapp.com for the latest.

Inhalt

Management mehrerer Arrays mit SANtricity Unified Manager 7

Hauptschnittstelle

Übersicht über die SANtricity Unified Manager Schnittstelle

SANtricity Unified Manager ist eine webbasierte Schnittstelle, mit der Sie mehrere Storage Arrays in einer Ansicht managen können.

Hauptseite

Wenn Sie sich bei Unified Manager anmelden, öffnet sich die Hauptseite zu **Verwalten - Alle**. Auf dieser Seite können Sie eine Liste der erkannten Speicher-Arrays in Ihrem Netzwerk durchblättern, ihren Status anzeigen und Vorgänge auf einem einzelnen Array oder einer Gruppe von Arrays durchführen.

Navigationsleiste rechts in der Seitenleiste

Die Funktionen von Unified Manager können über die Navigationsleiste in der Seitenleiste aufgerufen werden.

Werden	Beschreibung
Managen	Erkennung von Speicher-Arrays im Netzwerk, Starten von SANtricity System Manager für ein Array, Importieren von Einstellungen von einem Array in mehrere Arrays und Verwalten von Array-Gruppen Aktivieren Sie die Kontrollkästchen neben den Array-Namen, um Vorgänge für sie auszuführen, z. B. das Importieren von Einstellungen und das Erstellen von Array-Gruppen. Die Ellipsen am Ende jeder Zeile bieten ein Inline-Menü für Operationen auf einem einzelnen Array, wie z. B. Umbenennen.
Betrieb	Zeigen Sie den Fortschritt von Batch-Operationen an, z. B. den Import von Einstellungen von einem Array in ein anderes. Einige Vorgänge sind nicht verfügbar, wenn ein Speicherarray einen nicht optimalen Status hat.
Zertifikatmanagement	Verwalten von Zertifikaten zur Authentifizierung zwischen Browsern und Clients.
Zugriffsmanagement	Einrichtung der Benutzerauthentifizierung für die Unified Manager Schnittstelle
Unterstützung	Optionen für technischen Support, Ressourcen und Ansprechpartner

Schnittstelleneinstellungen und Hilfe

Oben rechts in der Benutzeroberfläche können Sie auf die Hilfe und andere Dokumentation zugreifen. Sie können auch auf Verwaltungsoptionen zugreifen, die über das Dropdown-Menü neben Ihrem Anmeldenamen verfügbar sind.

Benutzeranmeldungen und Passwörter

Der aktuelle Benutzer, der am System angemeldet ist, wird oben rechts auf der Schnittstelle angezeigt.

Weitere Informationen zu Benutzern und Kennwörtern finden Sie unter:

- "Legen Sie den Schutz des Admin-Passworts fest"
- "Ändern Sie das Admin-Passwort"
- "Passwörter für lokale Benutzerprofile ändern"

Unterstützte Browser

Auf SANtricity Unified Manager kann über verschiedene Browsertypen zugegriffen werden.

Die folgenden Browser und Versionen werden unterstützt.

Browser	Mindestversion
Google Chrome	89
Mozilla Firefox	80
Safari	14
Microsoft Edge	90

Der Web Services Proxy muss installiert und für den Browser verfügbar sein.

Legen Sie den Schutz des Admin-Passworts fest

Sie müssen SANtricity Unified Manager mit einem Administratorkennwort konfigurieren, um ihn vor unbefugtem Zugriff zu schützen.

Admin-Passwort und Benutzerprofile

Wenn Sie Unified Manager zum ersten Mal starten, werden Sie aufgefordert, ein Administratorpasswort festzulegen. Jeder Benutzer mit dem Admin-Passwort kann Konfigurationsänderungen an den Speicher-Arrays vornehmen.

Zusätzlich zum Admin-Passwort enthält die Unified Manager-Schnittstelle vorkonfigurierte Benutzerprofile mit einer oder mehreren Rollen, die ihnen zugeordnet sind. Weitere Informationen finden Sie unter "Funktionsweise von Access Management".

Die Benutzer und Zuordnungen können nicht geändert werden. Es können nur Passwörter geändert werden. Informationen zum Ändern von Passwörtern finden Sie unter:

- "Ändern Sie das Admin-Passwort"
- "Passwörter für lokale Benutzerprofile ändern"

Session-Timeouts

Die Software fordert Sie zur Eingabe des Passworts nur einmal während einer einzigen Verwaltungssitzung auf. Eine Sitzung läuft nach 30 Minuten Inaktivität standardmäßig aus. Zu diesem Zeitpunkt müssen Sie das Passwort erneut eingeben. Wenn ein anderer Benutzer von einem anderen Management-Client auf die Software zugreift und das Passwort während der Sitzung ändert, werden Sie beim nächsten Versuch eines Konfigurationsvorgangs oder einer Ansicht aufgefordert, ein Passwort einzugeben.

Aus Sicherheitsgründen können Sie versuchen, ein Passwort nur fünf Mal einzugeben, bevor die Software den Status „Sperre“ eingibt. In diesem Zustand lehnt die Software nachfolgende Passwortversuche ab. Sie müssen 10 Minuten warten, um den Status „Normal“ zurückzusetzen, bevor Sie erneut versuchen, ein Passwort einzugeben.

Sie können Sitzungszeitausfälle anpassen oder Sitzungszeitausfälle komplett deaktivieren. Weitere Informationen finden Sie unter "Verwalten von Sitzungszeitungen".

Ändern Sie das Admin-Passwort

Sie können das Admin-Passwort ändern, das für den Zugriff auf SANtricity Unified Manager verwendet wird.

Bevor Sie beginnen

- Sie müssen als lokaler Administrator angemeldet sein, der Root-Admin-Berechtigungen enthält.
- Sie müssen das aktuelle Admin-Passwort kennen.

Über diese Aufgabe

Beachten Sie bei der Auswahl eines Passworts die folgenden Richtlinien:

- Bei Passwörtern wird die Groß-/Kleinschreibung berücksichtigt.
- Nachgestellte Leerzeichen werden nicht aus Kennwörtern entfernt, wenn sie gesetzt sind. Achten Sie darauf, Leerzeichen einzugeben, wenn diese im Passwort enthalten waren.
- Um die Sicherheit zu erhöhen, verwenden Sie mindestens 15 alphanumerische Zeichen, und ändern Sie das Passwort häufig.

Schritte

1. Wählen Sie Menü:Einstellungen[Zugriffsverwaltung].
2. Wählen Sie die Registerkarte * Lokale Benutzerrollen* aus.
3. Wählen Sie den **admin**-Benutzer aus der Tabelle aus.

   Die Schaltfläche Kennwort ändern steht zur Verfügung.

4. Wählen Sie **Passwort Ändern**.

   Das Dialogfeld Kennwort ändern wird geöffnet.

5. Wenn für lokale Benutzerpasswörter keine Mindestkennwortlänge festgelegt ist, aktivieren Sie das Kontrollkästchen, damit der Benutzer ein Kennwort für den Zugriff auf das System eingeben muss.
6. Geben Sie das neue Passwort in die beiden Felder ein.
7. Geben Sie Ihr lokales Administratorpasswort ein, um diesen Vorgang zu bestätigen, und klicken Sie dann auf **Ändern**.

Verwalten von Sitzungszeitungen

Sie können Timeouts für SANtricity Unified Manager konfigurieren, sodass Benutzer inaktive Sitzungen nach einer bestimmten Zeit getrennt werden.

Über diese Aufgabe

Standardmäßig beträgt das Sitzungszeitlimit für Unified Manager 30 Minuten. Sie können diese Zeit anpassen oder Sitzungszeitausfälle ganz deaktivieren.

> Wenn Access Management unter Verwendung der in das Array integrierten SAML-Funktionen (Security Assertion Markup Language) konfiguriert wird, kann es zu einer Sitzungszeitüberschreitung kommen, wenn die SSO-Sitzung des Benutzers die maximale Grenze erreicht. Dies kann vor dem Timeout der System Manager-Sitzung auftreten.

Schritte

1. Wählen Sie in der Menüleiste den Dropdown-Pfeil neben Ihrem Benutzernamen aus.
2. Wählen Sie **Zeitüberschreitung der Sitzung aktivieren/deaktivieren**.

   Das Dialogfeld „Session-Timeout aktivieren/deaktivieren“ wird geöffnet.

3. Verwenden Sie die Spinner-Regler, um die Zeit in Minuten zu erhöhen oder zu verringern.

   Die minimale Zeitüberschreitung, die Sie einstellen können, beträgt 15 Minuten.

   > Deaktivieren Sie zum Deaktivieren der Sitzungszeitzeiten das Kontrollkästchen **Zeitdauer festlegen…**.

4. Klicken Sie Auf **Speichern**.

Storage-Arrays durchführt

Übersicht über die Bestandsaufnahme

Zum Managen von Storage-Ressourcen müssen Sie zuerst die Storage-Arrays im Netzwerk erkennen.

Wie entdecke ich Arrays?

Verwenden Sie die Seite Hinzufügen/Entdecken, um die zu verwaltenden Speicher-Arrays im Netzwerk Ihres Unternehmens zu suchen und hinzuzufügen. Sie können mehrere Arrays ermitteln oder ein einziges Array erkennen. Dazu geben Sie Netzwerk-IP-Adressen ein, und Unified Manager versucht dann individuelle Verbindungen zu jeder IP-Adresse in diesem Bereich.

Weitere Informationen:

- "Überlegungen bei der Array-Ermittlung"
- "Erkennung mehrerer Storage-Arrays"
- "Erkennen Sie ein einzelnes Array"

Wie managt ich Arrays?

Nachdem Sie Arrays entdeckt haben, gehen Sie zur Seite **Verwalten - Alle**. Auf dieser Seite können Sie eine Liste der erkannten Speicher-Arrays in Ihrem Netzwerk durchblättern, ihren Status anzeigen und Vorgänge auf einem einzelnen Array oder einer Gruppe von Arrays durchführen.

Wenn Sie ein einzelnes Array verwalten möchten, können Sie es auswählen und System Manager öffnen.

Weitere Informationen:

- "Überlegungen für den Zugriff auf System Manager"
- "Management eines individuellen Storage Arrays"
- "Anzeigen des Status des Speicherarrays"

Konzepte

Überlegungen bei der Array-Ermittlung

Bevor SANtricity Unified Manager Storage-Ressourcen anzeigen und verwalten kann, muss er die Storage-Arrays ermitteln, die Sie im Netzwerk Ihres Unternehmens managen möchten. Sie können mehrere Arrays ermitteln oder ein einziges Array erkennen.

Erkennung mehrerer Storage-Arrays

Wenn Sie mehrere Arrays ermitteln möchten, geben Sie einen Netzwerk-IP-Adressbereich ein, und Unified Manager versucht dann individuelle Verbindungen zu jeder IP-Adresse in diesem Bereich. Jedes erfolgreich erreichte Speicher-Array wird auf der Seite „Entdecken“ angezeigt und kann Ihrer Management-Domäne hinzugefügt werden.

Erkennen eines einzelnen Speicher-Arrays

Wenn Sie ein einzelnes Array ermitteln möchten, geben Sie für einen der Controller im Speicher-Array die einzelne IP-Adresse ein, und das individuelle Speicher-Array wird hinzugefügt.

> Unified Manager erkennt und zeigt nur die einzelne IP-Adresse oder IP-Adresse innerhalb eines dem Controller zugewiesenen Bereichs an. Wenn diesen Controllern alternative Controller oder IP-Adressen zugewiesen sind, die außerhalb dieser einzelnen IP-Adresse oder des IP-Adressbereichs liegen, werden sie von Unified Manager nicht ermittelt oder angezeigt. Sobald Sie jedoch das Speicher-Array hinzufügen, werden alle zugehörigen IP-Adressen ermittelt und in der Ansicht Verwalten angezeigt.

Benutzeranmeldeinformationen

Im Rahmen des Erkennungsvorgangs müssen Sie für jedes Speicherarray, das Sie hinzufügen möchten, das Administratorpasswort angeben.

Zertifikate für Webservices

Im Rahmen der Bestandsaufnahme überprüft Unified Manager, ob die erkannten Speicher-Arrays Zertifikate von einer vertrauenswürdigen Quelle verwenden. Unified Manager verwendet zwei Arten von zertifikatbasierter Authentifizierung für alle Verbindungen, die es mit dem Browser herstellt:

- * Vertrauenswürdige Zertifikate*

Bei Arrays, die von Unified Manager entdeckt wurden, müssen Sie möglicherweise zusätzliche vertrauenswürdige Zertifikate installieren, die von der Zertifizierungsstelle bereitgestellt werden.

Verwenden Sie die Schaltfläche **Import**, um diese Zertifikate zu importieren. Wenn Sie zuvor mit diesem Array verbunden haben, sind ein oder beide Controller-Zertifikate entweder abgelaufen, annulliert oder fehlen ein Stammzertifikat oder ein Zwischenzertifikat in der Zertifikatkette. Sie müssen das abgelaufene oder widersetzte Zertifikat ersetzen oder das fehlende Stammzertifikat oder Zwischenzertifikat hinzufügen, bevor Sie das Speicher-Array verwalten.

- **Selbstsignierte Zertifikate**

  Es können auch selbstsignierte Zertifikate verwendet werden. Wenn der Administrator versucht, Arrays zu ermitteln, ohne signierte Zertifikate zu importieren, zeigt Unified Manager ein Fehlerdialogfeld an, in dem der Administrator das selbstsignierte Zertifikat akzeptieren kann. Das selbstsignierte Zertifikat des Speicher-Arrays wird als vertrauenswürdig gekennzeichnet und das Speicher-Array wird Unified Manager hinzugefügt.

  Wenn Sie den Verbindungen zum Speicher-Array nicht vertrauen, wählen Sie **Abbrechen** und validieren Sie die Sicherheitszertifikatstrategie des Speicher-Arrays, bevor Sie das Speicher-Array zu Unified Manager hinzufügen.

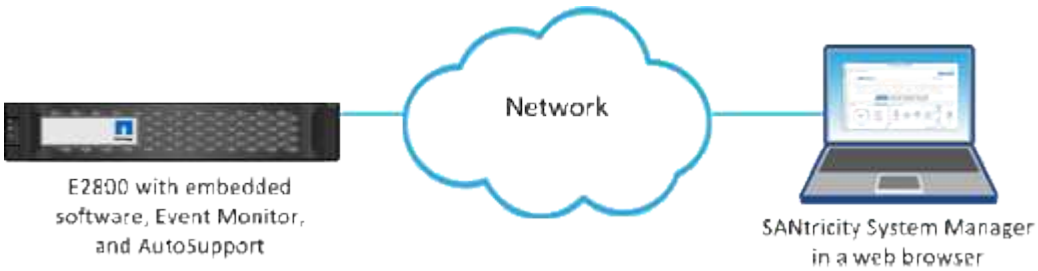
Überlegungen für den Zugriff auf SANtricity System Manager

Sie wählen ein oder mehrere Speicher-Arrays aus und öffnen SANtricity System Manager mit der Option Start, wenn Sie Speicher-Arrays konfigurieren und verwalten möchten.

System Manager ist eine eingebettete Applikation auf den Controllern, die über einen Ethernet-Management-Port mit dem Netzwerk verbunden ist. Es umfasst alle Array-basierten Funktionen.

Um auf System Manager zugreifen zu können, müssen Sie Folgendes haben:

- Eines der hier aufgeführten Array-Modelle: "E-Series Hardware im Überblick"
- Eine Out-of-Band-Verbindung zu einem Netzwerk-Management-Client mit einem Webbrowser.



Arrays erkennen

Erkennung mehrerer Storage-Arrays

Sie erkennen mehrere Arrays, um alle Speicher-Arrays im Subnetz zu erkennen, in dem sich der Verwaltungsserver befindet, und um automatisch die ermittelten Arrays zu Ihrer Verwaltungsdomäne hinzuzufügen.

Bevor Sie beginnen

- Sie müssen mit einem Benutzerprofil angemeldet sein, das die Berechtigungen für den Sicherheitsadministrator enthält.
- Das Speicher-Array muss ordnungsgemäß eingerichtet und konfiguriert sein.
- Passwörter für das Storage-Array müssen mithilfe der Kachel „System Manager Access Management“ eingerichtet werden.
- Um nicht vertrauenswürdige Zertifikate zu lösen, müssen Sie vertrauenswürdige Zertifikatdateien von einer Zertifizierungsstelle (CA) haben, und die Zertifikatdateien sind auf Ihrem lokalen System verfügbar.

Das Erkennen von Arrays ist ein mehrstufiges Verfahren.

Schritt 1: Geben Sie die Netzwerkadresse ein

Sie geben einen Netzwerkaddress Range ein, um im lokalen Subnetzwerk zu suchen. Jedes erfolgreich erreichte Speicher-Array wird auf der Seite Erkennung angezeigt und kann Ihrer Management-Domäne hinzugefügt werden.

Wenn Sie den Ermittlungsvorgang aus irgendeinem Grund beenden möchten, klicken Sie auf **Erkennung stoppen**.

Schritte

1. Wählen Sie auf der Seite Verwalten die Option **Hinzufügen/Entdecken**.

   Das Dialogfeld Hinzufügen/Entdecken wird angezeigt.

2. Wählen Sie das Optionsfeld **Alle Speicher-Arrays in einem Netzwerkbereich** aus.
3. Geben Sie die Startnetzwerkadresse und die Endung der Netzwerkadresse ein, um im lokalen Teilnetzwerk zu suchen, und klicken Sie dann auf **Erkennung starten**.

   Der Erkennungsvorgang wird gestartet. Dieser Erkennungsvorgang kann mehrere Minuten dauern. Die Tabelle auf der Seite „Entdecken“ wird bei der Erkennung der Speicher-Arrays ausgefüllt.

   Wenn keine verwaltbaren Arrays erkannt werden, überprüfen Sie, ob die Speicher-Arrays ordnungsgemäß mit Ihrem Netzwerk verbunden sind und die zugewiesenen Adressen innerhalb der Reichweite liegen. Klicken Sie auf **Neue Ermittlungsparameter**, um zur Seite Hinzufügen/Entdecken zurückzukehren.

4. Überprüfen Sie die Liste der erkannten Speicher-Arrays.
5. Aktivieren Sie das Kontrollkästchen neben einem beliebigen Speicher-Array, das Sie Ihrer Management-Domäne hinzufügen möchten, und klicken Sie dann auf **Weiter**.

   Unified Manager führt eine Überprüfung der Anmeldeinformationen für jedes Array durch, das Sie der Management-Domäne hinzufügen. Möglicherweise müssen Sie alle selbstsignierten Zertifikate und nicht vertrauenswürdigen Zertifikate, die mit diesem Array verknüpft sind, auflösen.

6. Klicken Sie auf **Weiter**, um mit dem nächsten Schritt im Assistenten fortzufahren.

Schritt 2: Lösen Sie selbst signierte Zertifikate während der Ermittlung

Während der Bestandsaufnahme überprüft das System, ob die Speicher-Arrays Zertifikate von einer vertrauenswürdigen Quelle verwenden.

Schritte

1. Führen Sie einen der folgenden Schritte aus:
   - Wenn Sie den Verbindungen zu den erkannten Speicherarrays vertrauen, fahren Sie mit der nächsten Karte im Assistenten fort. Die selbstsignierten Zertifikate werden als vertrauenswürdig markiert und die Speicher-Arrays werden zu Unified Manager hinzugefügt.
   - Wenn Sie den Verbindungen zu den Speicher-Arrays nicht vertrauen, wählen Sie **Abbrechen** und validieren Sie die Sicherheitszertifikatstrategie jedes Speicherarrays, bevor Sie eine dieser Verbindungen zu Unified Manager hinzufügen.
2. Klicken Sie auf **Weiter**, um mit dem nächsten Schritt im Assistenten fortzufahren.

Schritt 3: Lösen Sie nicht vertrauenswürdige Zertifikate während der Ermittlung

Nicht vertrauenswürdige Zertifikate treten auf, wenn ein Speicher-Array versucht, eine sichere Verbindung zu Unified Manager herzustellen, die Verbindung jedoch nicht als sicher bestätigt werden kann. Während der Array-Ermittlung können Sie nicht vertrauenswürdige Zertifikate auflösen, indem Sie ein Zertifikat (CA-Zertifikat) importieren, das von einem vertrauenswürdigen Dritten ausgestellt wurde.

Möglicherweise müssen Sie zusätzliche vertrauenswürdige CA-Zertifikate installieren, wenn eine der folgenden Optionen zutrifft:

- Sie haben kürzlich ein Speicher-Array hinzugefügt.
- Ein oder beide Zertifikate sind abgelaufen.
- Ein oder beide Zertifikate werden widerrufen.
- Ein oder beide Zertifikate fehlen ein Stammzertifikat oder ein Zwischenzertifikat.

Schritte

1. Aktivieren Sie das Kontrollkästchen neben einem beliebigen Speicherarray, für das Sie nicht vertrauenswürdige Zertifikate auflösen möchten, und wählen Sie dann die Schaltfläche **Importieren**.

   Es wird ein Dialogfeld zum Importieren der vertrauenswürdigen Zertifikatdateien geöffnet.

2. Klicken Sie auf **Durchsuchen**, um die Zertifikatdateien für die Speicher-Arrays auszuwählen.

   Die Dateinamen werden im Dialogfeld angezeigt.

3. Klicken Sie Auf **Import**.

   Die Dateien werden hochgeladen und validiert.

   > Jedes Speicherarray mit nicht vertrauenswürdigen Zertifikatproblemen, die nicht gelöst wurden, wird Unified Manager nicht hinzugefügt.

4. Klicken Sie auf **Weiter**, um mit dem nächsten Schritt im Assistenten fortzufahren.

Schritt 4: Geben Sie Passwörter ein

Sie müssen die Passwörter für die Speicher-Arrays eingeben, die Sie Ihrer Management-Domäne hinzufügen möchten.

Schritte

1. Geben Sie das Passwort für jedes Speicher-Array ein, das Sie zu Unified Manager hinzufügen möchten.
2. **Optional:** Speicher-Arrays einer Gruppe zuordnen: Wählen Sie aus der Dropdown-Liste die gewünschte

Gruppe aus, die mit den ausgewählten Speicher-Arrays verknüpft werden soll.

3. Klicken Sie Auf **Fertig Stellen**.

Nachdem Sie fertig sind

Die Speicher-Arrays werden Ihrer Management-Domäne hinzugefügt und der ausgewählten Gruppe zugeordnet (falls angegeben).

Es kann mehrere Minuten dauern, bis Unified Manager eine Verbindung zu den angegebenen Storage-Arrays hergestellt hat.

Erkennen Sie ein einzelnes Array

Verwenden Sie die Option Single Storage Array hinzufügen/erkennen, um ein einzelnes Speicher-Array manuell zu ermitteln und dem Netzwerk Ihres Unternehmens hinzuzufügen.

Bevor Sie beginnen

- Das Speicher-Array muss ordnungsgemäß eingerichtet und konfiguriert sein.
- Passwörter für das Storage-Array müssen mithilfe der Kachel „System Manager Access Management“ eingerichtet werden.

Schritte

1. Wählen Sie auf der Seite Verwalten die Option **Hinzufügen/Entdecken**.

   Das Dialogfeld Hinzufügen/Entdecken wird angezeigt.

2. Wählen Sie das Optionsfeld **Entdecken Sie ein einzelnes Speicherarray**.
3. Geben Sie die IP-Adresse für einen der Controller im Speicher-Array ein, und klicken Sie dann auf **Erkennung starten**.

   Es kann mehrere Minuten dauern, bis sich Unified Manager mit dem angegebenen Storage-Array verbindet.

   Die Meldung Speicher-Array nicht zugänglich wird angezeigt, wenn die Verbindung zur IP-Adresse des angegebenen Controllers nicht erfolgreich ist.

4. Lösen Sie gegebenenfalls selbstsignierte Zertifikate, wenn Sie dazu aufgefordert werden.

   Im Rahmen der Bestandsaufnahme überprüft das System, ob die erkannten Speicher-Arrays Zertifikate von einer vertrauenswürdigen Quelle verwenden. Wenn ein digitales Zertifikat für ein Speicherarray nicht gefunden werden kann, werden Sie aufgefordert, das nicht von einer anerkannten Zertifizierungsstelle (CA) signierte Zertifikat zu lösen, indem eine Sicherheitsausnahme hinzugefügt wird.

5. Lösen Sie ggf. nicht vertrauenswürdige Zertifikate, wenn Sie dazu aufgefordert werden.

   Nicht vertrauenswürdige Zertifikate treten auf, wenn ein Speicher-Array versucht, eine sichere Verbindung zu Unified Manager herzustellen, die Verbindung jedoch nicht als sicher bestätigt werden kann. Lösen Sie nicht vertrauenswürdige Zertifikate, indem Sie ein Zertifikat der Zertifizierungsstelle (CA) importieren, das von einem vertrauenswürdigen Dritten ausgestellt wurde.

6. Klicken Sie Auf **Weiter**.

7. **Optional:** das erkannte Speicher-Array einer Gruppe zuordnen: Wählen Sie aus der Dropdown-Liste die gewünschte Gruppe aus, die mit dem Speicher-Array verknüpft werden soll.

   Die Gruppe „Alle“ ist standardmäßig ausgewählt.

8. Geben Sie das Administratorkennwort für das Speicherarray ein, das Sie Ihrer Management-Domäne hinzufügen möchten, und klicken Sie dann auf **OK**.

Nachdem Sie fertig sind

Das Speicher-Array wird Unified Manager hinzugefügt und, falls angegeben, wird es auch der ausgewählten Gruppe hinzugefügt.

Wenn die automatische Erfassung von Support-Daten aktiviert ist, werden Support-Daten automatisch für ein von Ihnen hinzufügsames Speicher-Array erfasst.

Management von Arrays

Anzeigen des Status des Speicherarrays

SANtricity Unified Manager zeigt den Status jedes erkannten Speicher-Arrays an.

Gehen Sie zur Seite **Verwalten - Alle**. Auf dieser Seite können Sie den Status der Verbindung zwischen dem Web Services Proxy und diesem Speicher-Array anzeigen.

Die Statusanzeigen sind in der folgenden Tabelle beschrieben.

Status	Zeigt An
Optimal	Das Storage-Array befindet sich in einem optimalen Zustand. Es gibt keine Zertifikatprobleme und das Passwort ist gültig.
Ungültiges Kennwort	Es wurde ein ungültiges Kennwort für das Speicher-Array angegeben.
Nicht Vertrauenswürdiges Zertifikat	Eine oder mehrere Verbindungen mit dem Speicher-Array sind nicht vertrauenswürdig, da das HTTPS-Zertifikat entweder selbst signiert ist und noch nicht importiert wurde, oder das Zertifikat eine CA-Signatur hat und die Stamm- und Intermediate-CA-Zertifikate nicht importiert wurden.
Erfordert Aufmerksamkeit	Es liegt ein Problem mit dem Speicher-Array vor, das Ihr Eingreifen erfordert, um es zu beheben.
Verriegeln	Das Storage-Array befindet sich in einem gesperrten Zustand.
Unbekannt	Das Speicher-Array wurde noch nie kontaktiert. Dies kann vorkommen, wenn der Web Services Proxy gestartet wird und noch keine Kontakte zum Speicher-Array hergestellt wurden oder das Speicher-Array offline ist und seit dem Start des Web Services Proxy noch nie kontaktiert wurde.
Offline	Der Web Services Proxy hatte sich bereits zuvor an das Speicher-Array gewandt, doch inzwischen sind sämtliche Verbindungen verloren gegangen.

Management eines individuellen Storage Arrays

Sie können die Option Start verwenden, um den Browser-basierten SANtricity-System-Manager für ein oder mehrere Storage-Arrays zu öffnen, wenn Sie Managementvorgänge ausführen möchten.

Schritte

1. Wählen Sie auf der Seite Verwalten ein oder mehrere Storage Arrays aus, die Sie managen möchten.
2. Klicken Sie Auf **Start**.

   Das System öffnet ein neues Fenster und zeigt die Anmeldeseite von System Manager an.

3. Geben Sie Ihren Benutzernamen und Ihr Passwort ein und klicken Sie dann auf **Anmelden**.

Ändern Sie die Passwörter für das Speicherarray

Sie können die Passwörter aktualisieren, die für die Anzeige und den Zugriff auf Speicher-Arrays in SANtricity Unified Manager verwendet werden.

Bevor Sie beginnen

- Sie müssen mit einem Benutzerprofil angemeldet sein, das Storage Admin-Berechtigungen enthält.
- Sie müssen das aktuelle Passwort für das Speicher-Array kennen, das in System Manager festgelegt ist.

Über diese Aufgabe

In dieser Aufgabe geben Sie das aktuelle Passwort für ein Speicher-Array ein, damit Sie in Unified Manager darauf zugreifen können. Dies kann notwendig sein, wenn das Array-Passwort in System Manager geändert wurde und jetzt auch in Unified Manager geändert werden muss.

Schritte

1. Wählen Sie auf der Seite Verwalten ein oder mehrere Speicher-Arrays aus.
2. Menü wählen:Sonstige Aufgaben[Storage Array-Passwörter angeben].
3. Geben Sie für jedes Speicherarray das Kennwort oder die Passwörter ein, und klicken Sie dann auf **Speichern**.

Entfernen Sie die Storage-Arrays von SANtricity Unified Manager

Sie können ein oder mehrere Storage Arrays entfernen, wenn Sie es nicht mehr über SANtricity Unified Manager managen möchten.

Über diese Aufgabe

Sie können nicht auf die von Ihnen entfernenden Speicher-Arrays zugreifen. Sie können jedoch eine Verbindung zu einem der entfernten Speicher-Arrays herstellen, indem Sie einen Browser direkt auf seine IP-Adresse oder den Host-Namen zeigen.

Das Entfernen eines Speicher-Arrays hat keinerlei Auswirkungen auf das Speicher-Array oder seine Daten. Wenn ein Speicher-Array versehentlich entfernt wird, kann es erneut hinzugefügt werden.

Schritte

1. Wählen Sie die Seite **Verwalten** aus.

2. Wählen Sie ein oder mehrere Speicherarrays aus, die Sie entfernen möchten.
3. Menü wählen:Sonstige Aufgaben[Speicher-Array entfernen].

   Das Storage Array wird aus allen Ansichten in SANtricity Unified Manager entfernt.

Einstellungen werden importiert

Einstellungen Importübersicht

Mit der Funktion „Einstellungen importieren“ können Sie einen Batch-Vorgang zum Importieren der Einstellungen von einem Array in mehrere Arrays durchführen. Diese Funktion spart Zeit, wenn Sie mehrere Arrays im Netzwerk konfigurieren müssen.

Welche Einstellungen können importiert werden?

Sie können Alarmmethoden, AutoSupport-Konfigurationen, Verzeichnisdienste-Konfigurationen, Storage-Konfigurationen (z. B. Volume-Gruppen und Pools) und Systemeinstellungen (wie den automatischen Lastausgleich) importieren.

Weitere Informationen:

- "Funktionsweise der Importeinstellungen"
- "Anforderungen für die Replizierung von Storage-Konfigurationen"

Wie führe ich einen Batch-Import durch?

Öffnen Sie System Manager auf einem Storage Array, das als Quelle verwendet werden soll, und konfigurieren Sie die gewünschten Einstellungen. Gehen Sie dann von Unified Manager zur Seite Verwalten und importieren Sie die Einstellungen in ein oder mehrere Arrays.

Weitere Informationen:

- "Warnungseinstellungen importieren"
- "AutoSupport-Einstellungen importieren"
- "Einstellungen für Verzeichnisdienste importieren"
- "Importieren der Speicherkonfigurationseinstellungen"
- "Systemeinstellungen importieren"

Konzepte

Funktionsweise der Importeinstellungen

Mit SANtricity Unified Manager können Sie Einstellungen von einem Storage-Array in mehrere Storage-Arrays importieren. Die Funktion „Importeinstellungen“ ist ein Batch-Vorgang, der Zeit spart, wenn Sie mehrere Arrays im Netzwerk konfigurieren müssen.

Für den Import verfügbare Einstellungen

Die folgenden Konfigurationen können in mehrere Arrays importiert werden:

- **Alerts** - Alerting-Methoden, um wichtige Ereignisse mithilfe von E-Mail, Syslog-Server oder SNMP-Server an Administratoren zu senden.
- **AutoSupport** — Eine Funktion, die den Zustand eines Speicherarrays überwacht und automatische Entsendungen an den technischen Support sendet.
- **Directory Services** — eine Methode der Benutzerauthentifizierung, die über einen LDAP-Server (Lightweight Directory Access Protocol) und einen Verzeichnisdienst, wie Microsoft Active Directory verwaltet wird.
- **Speicherkonfiguration** — Konfigurationen im Zusammenhang mit folgenden:
  - Volumes (nur Thick Volumes und nicht Repository Volumes)
  - Volume-Gruppen und -Pools
  - Zuweisung von Hot-Spare-Laufwerken
- **Systemeinstellungen** — Konfigurationen in Bezug auf folgende Komponenten:
  - Medien-Scan-Einstellungen für ein Volume
  - SSD-Einstellungen
  - Automatischer Lastausgleich (ohne Berichterstellung für Hostkonnektivität)

Konfigurationsworkflow

So importieren Sie Einstellungen:

1. Konfigurieren Sie die Einstellungen in einem Speicher-Array, das als Quelle verwendet werden soll, mit System Manager.
2. Sichern Sie auf den Storage Arrays, die als Ziele verwendet werden sollen, ihre Konfiguration mit System Manager.
3. Gehen Sie von Unified Manager auf die Seite **Verwalten** und importieren Sie die Einstellungen.
4. Überprüfen Sie auf der Seite **Operationen** die Ergebnisse der Importeinstellungen.

Anforderungen für die Replizierung von Storage-Konfigurationen

Bevor Sie eine Speicherkonfiguration von einem Speicher-Array in ein anderes importieren, überprüfen Sie die Anforderungen und Richtlinien.

Shelfs

- Die Shelfs, in denen sich die Controller befinden, müssen auf den Quell- und Ziel-Arrays identisch sein.
- Shelf IDs müssen auf den Quell- und Ziel-Arrays identisch sein.
- Erweiterungs-Shelfs müssen in denselben Steckplätzen mit denselben Laufwerktypen bestückt werden (wenn das Laufwerk in der Konfiguration verwendet wird, ist die Position nicht verwendeter Laufwerke unwichtig).

Controller

- Der Controller-Typ kann sich zwischen Quell- und Ziel-Arrays unterscheiden (beispielsweise beim Import von einer E2800 in eine E5700), aber der RBOD-Gehäusetyp muss identisch sein.

- Die HICs, einschließlich der da-Fähigkeiten des Hosts, müssen identisch sein zwischen den Quell- und Ziel-Arrays.
- Der Import von einer Duplex-Konfiguration in eine Simplex-Konfiguration wird nicht unterstützt. Der Import von Simplex in Duplex ist jedoch zulässig.
- FDE-Einstellungen sind beim Importvorgang nicht enthalten.

Status

- Die Ziel-Arrays müssen den optimalen Status haben.
- Das Quell-Array muss nicht im optimalen Status sein.

Storage

- Die Laufwerkskapazität kann zwischen den Quell- und Ziel-Arrays variieren, solange die Volume-Kapazität auf dem Ziel größer ist als die Quelle. (In einem Ziel-Array sind unter Umständen neuere Laufwerke mit höherer Kapazität enthalten, die durch den Replizierungsvorgang nicht vollständig in Volumes konfiguriert wären.)
- Laufwerk-Pool-Volumes mit einer Größe von mindestens 64 TB auf dem Quell-Array verhindern den Importvorgang auf den Zielen.
- Thin Volumes sind beim Importvorgang nicht enthalten.

Verwenden Sie Batch-Importe

Warnungseinstellungen importieren

Sie können Alarmkonfigurationen von einem Speicher-Array in andere Speicher-Arrays importieren. Dieser Batch-Betrieb spart Zeit, wenn Sie mehrere Arrays im Netzwerk konfigurieren müssen.

Bevor Sie beginnen

- Warnmeldungen werden in System Manager für das Speicherarray konfiguriert, das als Quelle verwendet werden soll (Menü:Einstellungen[Warnungen]).
- Die vorhandene Konfiguration für die Ziel-Speicher-Arrays wird in System Manager gesichert (Menü:Einstellungen[System > Speicherarray-Konfiguration speichern]).

Über diese Aufgabe

Sie können E-Mail-, SNMP- oder Syslog-Warnungen für den Importvorgang auswählen. Die importierten Einstellungen umfassen:

- **E-Mail-Benachrichtigungen** — Eine E-Mail-Server-Adresse und die E-Mail-Adressen der Alarmempfänger.
- **Syslog Alerts** — Eine Syslog-Serveradresse und ein UDP-Port.
- **SNMP Alerts** — Ein Community-Name und IP-Adresse für den SNMP-Server.

Schritte

1. Klicken Sie auf der Seite Verwalten auf **Einstellungen importieren**.

   Der Assistent für Importeinstellungen wird geöffnet.

2. Wählen Sie im Dialogfeld Einstellungen auswählen entweder **E-Mail-Alarme**, **SNMP-Alarme** oder **Syslog-Warnungen** aus und klicken Sie dann auf **Weiter**.

   Zum Auswählen des Quell-Arrays wird ein Dialogfeld geöffnet.

3. Wählen Sie im Dialogfeld Quelle auswählen das Array mit den Einstellungen aus, die Sie importieren möchten, und klicken Sie dann auf **Weiter**.
4. Wählen Sie im Dialogfeld Ziele auswählen ein oder mehrere Arrays aus, um die neuen Einstellungen zu erhalten.

   Speicher-Arrays mit Firmware unter 8.50 stehen nicht zur Auswahl. Darüber hinaus wird ein Array nicht in diesem Dialogfeld angezeigt, wenn Unified Manager nicht mit dem Array kommunizieren kann (z. B. wenn es offline ist oder wenn es über Zertifikat-, Kennwort- oder Netzwerkprobleme verfügt).

5. Klicken Sie Auf **Fertig Stellen**.

   Auf der Seite Operationen werden die Ergebnisse des Importvorgangs angezeigt. Wenn der Vorgang fehlschlägt, können Sie auf die Zeile klicken, um weitere Informationen anzuzeigen.

Ergebnisse

Die Ziel-Storage-Arrays sind jetzt so konfiguriert, dass sie Warnmeldungen per E-Mail, SNMP oder Syslog an Administratoren senden.

AutoSupport-Einstellungen importieren

Sie können eine AutoSupport-Konfiguration von einem Speicher-Array in andere Speicher-Arrays importieren. Dieser Batch-Betrieb spart Zeit, wenn Sie mehrere Arrays im Netzwerk konfigurieren müssen.

Bevor Sie beginnen

- AutoSupport ist in System Manager für das Storage-Array konfiguriert, das als Quelle verwendet werden soll (Menü:Support[Support Center]).
- Die vorhandene Konfiguration für die Ziel-Speicher-Arrays wird in System Manager gesichert (Menü:Einstellungen[System > Speicherarray-Konfiguration speichern]).

Über diese Aufgabe

Zu den importierten Einstellungen gehören die separaten Funktionen (Basic AutoSupport, AutoSupport OnDemand und Remote Diagnostics), das Wartungsfenster, die Bereitstellungsmethode, Und dem Versandplan.

Schritte

1. Klicken Sie auf der Seite Verwalten auf **Einstellungen importieren**.

   Der Assistent für Importeinstellungen wird geöffnet.

2. Wählen Sie im Dialogfeld Einstellungen auswählen die Option **AutoSupport** aus und klicken Sie dann auf **Weiter**.

   Zum Auswählen des Quell-Arrays wird ein Dialogfeld geöffnet.

3. Wählen Sie im Dialogfeld Quelle auswählen das Array mit den Einstellungen aus, die Sie importieren möchten, und klicken Sie dann auf **Weiter**.
4. Wählen Sie im Dialogfeld Ziele auswählen ein oder mehrere Arrays aus, um die neuen Einstellungen zu erhalten.

> Speicher-Arrays mit Firmware unter 8.50 stehen nicht zur Auswahl. Darüber hinaus wird ein Array nicht in diesem Dialogfeld angezeigt, wenn Unified Manager nicht mit dem Array kommunizieren kann (z. B. wenn es offline ist oder wenn es über Zertifikat-, Kennwort- oder Netzwerkprobleme verfügt).

5. Klicken Sie Auf **Fertig Stellen**.

   Auf der Seite Operationen werden die Ergebnisse des Importvorgangs angezeigt. Wenn der Vorgang fehlschlägt, können Sie auf die Zeile klicken, um weitere Informationen anzuzeigen.

Ergebnisse

Die Ziel-Storage-Arrays sind nun mit denselben AutoSupport-Einstellungen wie das Quell-Array konfiguriert.

Einstellungen für Verzeichnisdienste importieren

Sie können eine Konfiguration für Verzeichnisdienste von einem Speicher-Array in andere Speicher-Arrays importieren. Dieser Batch-Betrieb spart Zeit, wenn Sie mehrere Arrays im Netzwerk konfigurieren müssen.

Bevor Sie beginnen

- Verzeichnisdienste werden in System Manager für das Speicherarray konfiguriert, das als Quelle verwendet werden soll (Menü:Einstellungen[Zugriffsmanagement]).
- Die vorhandene Konfiguration für die Ziel-Speicher-Arrays wird in System Manager gesichert (Menü:Einstellungen[System > Speicherarray-Konfiguration speichern]).

Über diese Aufgabe

Zu den importierten Einstellungen gehören der Domänenname und die URL eines LDAP-Servers (Lightweight Directory Access Protocol) sowie die Zuordnungen der Benutzergruppen des LDAP-Servers zu den vordefinierten Rollen des Speicher-Arrays.

Schritte

1. Klicken Sie auf der Seite Verwalten auf **Einstellungen importieren**.

   Der Assistent für Importeinstellungen wird geöffnet.

2. Wählen Sie im Dialogfeld Einstellungen auswählen die Option **Verzeichnisdienste** aus und klicken Sie dann auf **Weiter**.

   Zum Auswählen des Quell-Arrays wird ein Dialogfeld geöffnet.

3. Wählen Sie im Dialogfeld Quelle auswählen das Array mit den Einstellungen aus, die Sie importieren möchten, und klicken Sie dann auf **Weiter**.
4. Wählen Sie im Dialogfeld Ziele auswählen ein oder mehrere Arrays aus, um die neuen Einstellungen zu erhalten.

Speicher-Arrays mit Firmware unter 8.50 stehen nicht zur Auswahl. Darüber hinaus wird ein Array nicht in diesem Dialogfeld angezeigt, wenn Unified Manager nicht mit dem Array kommunizieren kann (z. B. wenn es offline ist oder wenn es über Zertifikat-, Kennwort- oder Netzwerkprobleme verfügt).

5. Klicken Sie Auf **Fertig Stellen**.

   Auf der Seite Operationen werden die Ergebnisse des Importvorgangs angezeigt. Wenn der Vorgang fehlschlägt, können Sie auf die Zeile klicken, um weitere Informationen anzuzeigen.

Ergebnisse

Die Ziel-Storage-Arrays sind nun mit denselben Verzeichnisdiensten konfiguriert wie das Quell-Array.

Systemeinstellungen importieren

Sie können die Systemkonfiguration von einem Speicher-Array in andere Speicher-Arrays importieren. Dieser Batch-Betrieb spart Zeit, wenn Sie mehrere Arrays im Netzwerk konfigurieren müssen.

Bevor Sie beginnen

- Systemeinstellungen sind in System Manager für das Speicherarray konfiguriert, das als Quelle verwendet werden soll.
- Die vorhandene Konfiguration für die Ziel-Speicher-Arrays wird in System Manager gesichert (Menü:Einstellungen[System > Speicherarray-Konfiguration speichern]).

Über diese Aufgabe

Importierte Einstellungen umfassen Medien-Scan-Einstellungen für ein Volume, SSD-Einstellungen für Controller und automatischen Lastausgleich (ohne Berichterstellung für Host-Konnektivität).

Schritte

1. Klicken Sie auf der Seite Verwalten auf **Einstellungen importieren**.

   Der Assistent für Importeinstellungen wird geöffnet.

2. Wählen Sie im Dialogfeld Einstellungen auswählen die Option **System** aus und klicken Sie dann auf **Weiter**.

   Zum Auswählen des Quell-Arrays wird ein Dialogfeld geöffnet.

3. Wählen Sie im Dialogfeld Quelle auswählen das Array mit den Einstellungen aus, die Sie importieren möchten, und klicken Sie dann auf **Weiter**.
4. Wählen Sie im Dialogfeld Ziele auswählen ein oder mehrere Arrays aus, um die neuen Einstellungen zu erhalten.

   Speicher-Arrays mit Firmware unter 8.50 stehen nicht zur Auswahl. Darüber hinaus wird ein Array nicht in diesem Dialogfeld angezeigt, wenn Unified Manager nicht mit dem Array kommunizieren kann (z. B. wenn es offline ist oder wenn es über Zertifikat-, Kennwort- oder Netzwerkprobleme verfügt).

5. Klicken Sie Auf **Fertig Stellen**.

Auf der Seite Operationen werden die Ergebnisse des Importvorgangs angezeigt. Wenn der Vorgang fehlschlägt, können Sie auf die Zeile klicken, um weitere Informationen anzuzeigen.

Ergebnisse

Die Ziel-Storage-Arrays sind nun mit denselben Systemeinstellungen wie das Quell-Array konfiguriert.

Importieren der Speicherkonfigurationseinstellungen

Sie können die Speicherkonfiguration von einem Speicher-Array in andere Speicher-Arrays importieren. Dieser Batch-Betrieb spart Zeit, wenn Sie mehrere Arrays im Netzwerk konfigurieren müssen.

Bevor Sie beginnen

- Storage ist in SANtricity System Manager für das Storage-Array konfiguriert, das Sie als Quelle verwenden möchten.
- Die vorhandene Konfiguration für die Ziel-Speicher-Arrays wird in System Manager gesichert (Menü:Einstellungen[System > Speicherarray-Konfiguration speichern]).
- Quell- und Ziel-Arrays müssen die folgenden Anforderungen erfüllen:
  - Die Shelfs, in denen sich die Controller befinden, müssen identisch sein.
  - Shelf-IDs müssen identisch sein.
  - Erweiterungs-Shelfs müssen in denselben Steckplätzen mit denselben Laufwerkstypen bestückt werden.
  - Der Typ des RBOD-Gehäuses muss identisch sein.
  - Die HICs, einschließlich der Data Assurance-Funktionen des Hosts, müssen identisch sein.
  - Die Ziel-Arrays müssen den optimalen Status haben.
  - Die Volume-Kapazität auf dem Ziel-Array ist größer als die Kapazität des Quell-Arrays.
- Sie verstehen die folgenden Einschränkungen:
  - Der Import von einer Duplex-Konfiguration in eine Simplex-Konfiguration wird nicht unterstützt. Der Import von Simplex in Duplex ist jedoch zulässig.
  - Laufwerk-Pool-Volumes mit einer Größe von mindestens 64 TB auf dem Quell-Array verhindern den Importvorgang auf den Zielen.
  - Thin Volumes sind beim Importvorgang nicht enthalten.

Über diese Aufgabe

Zu den importierten Einstellungen gehören konfigurierte Volumes (nur Thick- und nicht-Repository-Volumes), Volume-Gruppen, Pools und Hot-Spare-Laufwerkszuordnungen.

Schritte

1. Klicken Sie auf der Seite Verwalten auf **Einstellungen importieren**.

   Der Assistent für Importeinstellungen wird geöffnet.

2. Wählen Sie im Dialogfeld Einstellungen auswählen die Option **Speicherkonfiguration** aus und klicken Sie dann auf **Weiter**.

   Zum Auswählen des Quell-Arrays wird ein Dialogfeld geöffnet.

3. Wählen Sie im Dialogfeld Quelle auswählen das Array mit den Einstellungen aus, die Sie importieren möchten, und klicken Sie dann auf **Weiter**.
4. Wählen Sie im Dialogfeld Ziele auswählen ein oder mehrere Arrays aus, um die neuen Einstellungen zu erhalten.

> Speicher-Arrays mit Firmware unter 8.50 stehen nicht zur Auswahl. Darüber hinaus wird ein Array nicht in diesem Dialogfeld angezeigt, wenn Unified Manager nicht mit dem Array kommunizieren kann (z. B. wenn es offline ist oder wenn es über Zertifikat-, Kennwort- oder Netzwerkprobleme verfügt).

5. Klicken Sie Auf **Fertig Stellen**.

   Auf der Seite Operationen werden die Ergebnisse des Importvorgangs angezeigt. Wenn der Vorgang fehlschlägt, können Sie auf die Zeile klicken, um weitere Informationen anzuzeigen.

Ergebnisse

Die Ziel-Storage-Arrays sind nun mit derselben Storage-Konfiguration wie das Quell-Array konfiguriert.

FAQs

Welche Einstellungen werden importiert?

Die Funktion „Importeinstellungen“ ist ein Batch-Vorgang, bei dem Konfigurationen von einem Speicher-Array auf mehrere Speicher-Arrays geladen werden. Die während dieses Vorgangs importierten Einstellungen hängen davon ab, wie das Quell-Speicher-Array in SANtricity System Manager konfiguriert ist.

Die folgenden Einstellungen können in mehrere Speicher-Arrays importiert werden:

- **E-Mail-Alarme** — Einstellungen beinhalten eine E-Mail-Server-Adresse und die E-Mail-Adressen der Warnungsempfänger.
- **Syslog Alerts** — Einstellungen beinhalten eine Syslog-Serveradresse und einen UDP-Port.
- **SNMP Alerts** — Einstellungen beinhalten einen Community-Namen und eine IP-Adresse für den SNMP-Server.
- **AutoSupport** — Einstellungen umfassen die separaten Funktionen (Basic AutoSupport, AutoSupport OnDemand und Remote Diagnostics), das Wartungsfenster, die Bereitstellungsmethode, Und dem Versandplan.
- **Directory Services** — die Konfiguration umfasst den Domänennamen und die URL eines LDAP-Servers (Lightweight Directory Access Protocol) sowie die Zuordnungen für die Benutzergruppen des LDAP-Servers zu den vordefinierten Rollen des Speicher-Arrays.
- **Speicherkonfiguration** — Konfigurationen umfassen Volumes (nur dicke und nur nicht-Repository-Volumes), Volume-Gruppen, Pools und Hot-Spare-Laufwerkszuordnungen.
- **Systemeinstellungen** — Konfigurationen umfassen Medien-Scan-Einstellungen für ein Volume, SSD-Cache für Controller und automatischen Lastausgleich (ohne Berichterstellung über Hostkonnektivität).

Warum sehe ich nicht all meine Storage Arrays?

Während des Vorgangs „Importeinstellungen“ stehen einige Ihrer Speicherarrays

möglicherweise nicht im Dialogfeld „Zielauswahl“ zur Verfügung.

Speicher-Arrays werden möglicherweise aus den folgenden Gründen nicht angezeigt:

- Die Firmware-Version ist unter 8.50.
- Das Speicher-Array ist offline.
- Das System kann nicht mit diesem Array kommunizieren (z. B. verfügt das Array über Zertifikat-, Passwort- oder Netzwerkprobleme).

Array-Gruppen

Gruppenübersicht

Auf der Seite „Gruppen managen“ können Sie eine Reihe von Speicher-Array-Gruppen erstellen, um die Verwaltung zu erleichtern.

Was sind Array-Gruppen?

Sie können Ihre physische und virtualisierte Infrastruktur managen, indem Sie eine Reihe von Storage-Arrays gruppieren. Möglicherweise möchten Sie Storage-Arrays gruppieren, um die Ausführung von Überwachungs- oder Reporting-Aufgaben zu erleichtern.

Es gibt zwei Arten von Gruppen:

- **Alle Gruppe** — die All-Gruppe ist die Standardgruppe und umfasst alle Speicher-Arrays, die in Ihrem Unternehmen entdeckt wurden. Auf die Gruppe Alle kann über die Hauptansicht zugegriffen werden.
- **Vom Benutzer erstellte Gruppe** — Eine vom Benutzer erstellte Gruppe enthält die Speicherarrays, die Sie manuell auswählen, um diese Gruppe hinzuzufügen. Auf von Benutzern erstellte Gruppen kann über die Hauptansicht zugegriffen werden.

Wie konfiguriere ich Gruppen?

Auf der Seite „Gruppen verwalten“ können Sie eine Gruppe erstellen und dieser Gruppe Arrays hinzufügen.

Weitere Informationen:

- "Speicherarray-Gruppe konfigurieren"

Speicherarray-Gruppe konfigurieren

Sie erstellen Speichergruppen und fügen dann Speicher-Arrays zu den Gruppen hinzu.

Das Konfigurieren von Gruppen ist ein zweistufiges Verfahren.

Schritt 1: Gruppe erstellen

Sie erstellen zuerst eine Gruppe. Die Speichergruppe definiert, welche Laufwerke den Speicher bereitstellen, aus dem das Volume besteht.

Schritte

1. Wählen Sie auf der Seite Verwalten die Option MENU:Gruppen verwalten[Speicherarray-Gruppe erstellen].

2. Geben Sie im Feld **Name** einen Namen für die neue Gruppe ein.
3. Wählen Sie die Speicher-Arrays aus, die Sie der neuen Gruppe hinzufügen möchten.
4. Klicken Sie Auf **Erstellen**.

Schritt 2: Speicher-Array zu Gruppe hinzufügen

Sie können einer vom Benutzer erstellten Gruppe einen oder mehrere Speicher-Arrays hinzufügen.

Schritte

1. Wählen Sie in der Hauptansicht **Verwalten** aus, und wählen Sie dann die Gruppe aus, der Sie Speicher-Arrays hinzufügen möchten.
2. Wählen Sie Menü:Gruppen verwalten[Speicher-Arrays zu Gruppe hinzufügen].
3. Wählen Sie die Speicher-Arrays aus, die Sie der Gruppe hinzufügen möchten.
4. Klicken Sie Auf **Hinzufügen.**

Entfernen Sie Speicher-Arrays aus der Gruppe

Sie können ein oder mehrere verwaltete Speicher-Arrays aus einer Gruppe entfernen, wenn Sie sie nicht mehr aus einer bestimmten Speichergruppe verwalten möchten.

Über diese Aufgabe

Das Entfernen von Speicher-Arrays aus einer Gruppe hat keinerlei Auswirkungen auf das Speicher-Array oder seine Daten. Wenn das Storage Array von System Manager gemanagt wird, können Sie es weiterhin mit Ihrem Browser verwalten. Wenn ein Speicher-Array versehentlich aus einer Gruppe entfernt wird, kann es erneut hinzugefügt werden.

Schritte

1. Wählen Sie auf der Seite Verwalten die Option MENU:Gruppen verwalten[Speicher-Arrays aus Gruppe entfernen].
2. Wählen Sie im Dropdown-Menü die Gruppe aus, die die zu entfernenden Speicher-Arrays enthält, und klicken Sie dann auf das Kontrollkästchen neben jedem Speicher-Array, das Sie aus der Gruppe entfernen möchten.
3. Klicken Sie Auf **Entfernen**.

Speicherarray-Gruppe löschen

Sie können eine oder mehrere Speicherarraygruppen entfernen, die nicht mehr benötigt werden.

Über diese Aufgabe

Bei diesem Vorgang wird nur die Speicherarraygruppe gelöscht. Die der gelöschten Gruppe zugeordneten Speicher-Arrays bleiben über die Ansicht Alle verwalten oder eine andere Gruppe, der sie zugeordnet ist, zugänglich.

Schritte

1. Wählen Sie auf der Seite Verwalten die Option MENU:Gruppen verwalten[Speicherarray-Gruppe löschen].
2. Wählen Sie eine oder mehrere Speicherarray-Gruppen aus, die Sie löschen möchten.
3. Klicken Sie Auf **Löschen**.

Benennen Sie die Speicherarray-Gruppe um

Sie können den Namen einer Speicherarraygruppe ändern, wenn der aktuelle Name nicht mehr aussagekräftig oder zutreffend ist.

Über diese Aufgabe

Berücksichtigen Sie diese Richtlinien bitte.

- Ein Name kann aus Buchstaben, Zahlen und den Sonderzeichen Unterstrich (_), Bindestrich (-) und Pfund (#) bestehen. Wenn Sie andere Zeichen auswählen, wird eine Fehlermeldung angezeigt. Sie werden aufgefordert, einen anderen Namen auszuwählen.
- Beschränken Sie den Namen auf 30 Zeichen. Alle führenden und nachgestellten Leerzeichen im Namen werden gelöscht.
- Verwenden Sie einen eindeutigen, aussagekräftigen Namen, der leicht zu verstehen und zu merken ist.
- Vermeiden Sie beliebige Namen oder Namen, die in Zukunft schnell ihre Bedeutung verlieren würden.

Schritte

1. Wählen Sie in der Hauptansicht **Verwalten** aus, und wählen Sie dann die Speicherarray-Gruppe aus, die Sie umbenennen möchten.
2. Wählen Sie Menü:Gruppen verwalten[Speicherarray-Gruppe umbenennen].
3. Geben Sie im Feld **Gruppenname** einen neuen Namen für die Gruppe ein.
4. Klicken Sie Auf **Umbenennen.**

Upgrades

Übersicht zum Upgrade Center

Im Upgrade Center können Sie SANtricity OS Software und NVSRAM Upgrades für mehrere Storage Arrays managen.

Wie funktionieren Upgrades?

Sie laden die neueste Betriebssystemsoftware herunter und aktualisieren dann ein oder mehrere Arrays.

Workflow-Upgrade

Die folgenden Schritte ermöglichen einen grundlegenden Workflow bei der Durchführung von Software-Upgrades.

1. Sie laden die aktuelle SANtricity OS Softwaredatei von der Support-Website herunter. (Auf der Support-Seite ist ein Link von Unified Manager verfügbar) Speichern Sie die Datei auf dem Management-Host-System (dem Host, auf dem Sie in einem Browser auf Unified Manager zugreifen), und entpacken Sie die Datei anschließend.
2. In Unified Manager laden Sie die Softwaredatei des SANtricity-Betriebssystems und die NVSRAM-Datei in das Repository (ein Bereich des Web-Services-Proxyservers, auf dem Dateien gespeichert sind). Sie können Dateien entweder über das Menü:Upgrade Center[Upgrade SANtricity OS Software oder über Upgrade Center > Software-Repository verwalten] hinzufügen.
3. Nachdem die Dateien in das Repository geladen wurden, können Sie die Datei auswählen, die für das Upgrade verwendet werden soll. Wählen Sie auf der Seite Software Upgrade SANtricity OS

(Menü:Upgrade Center [Upgrade SANtricity OS Software]) die Software-Datei SANtricity OS und die NVSRAM-Datei aus. Nach Auswahl einer Softwaredatei wird auf dieser Seite eine Liste kompatibler Speicher-Arrays angezeigt. Anschließend wählen Sie die Speicher-Arrays aus, die Sie mit der neuen Software aktualisieren möchten. (Sie können nicht inkompatible Arrays auswählen.)

4. Anschließend können Sie eine sofortige Softwareübertragung und -Aktivierung starten oder die Dateien zu einem späteren Zeitpunkt für die Aktivierung aktivieren. Während des Upgrades führt Unified Manager die folgenden Aufgaben aus:
   a. Durchführung einer Integritätsprüfung für die Speicher-Arrays, um festzustellen, ob Bedingungen vorhanden sind, die das Upgrade möglicherweise verhindern. Wenn Arrays die Integritätsprüfung nicht bestanden haben, können Sie das jeweilige Array überspringen und das Upgrade für die anderen fortsetzen. Alternativ können Sie den gesamten Prozess beenden und die Arrays, die nicht bestanden haben, beheben.
   b. Überträgt die Upgrade-Dateien an jeden Controller.
   c. Bootet die Controller neu und aktiviert die neue SANtricity OS Software, die jeweils einen Controller umfasst. Während der Aktivierung wird die vorhandene SANtricity OS-Datei durch die neue Datei ersetzt.

      Sie können auch angeben, dass die Software zu einem späteren Zeitpunkt aktiviert wird.

Sofortiges oder stufenweise Upgrade

Sie können das Upgrade sofort aktivieren oder es für einen späteren Zeitpunkt aktivieren. Aus folgenden Gründen können Sie sich später aktivieren:

- **Tageszeit** — die Aktivierung der Software kann eine lange Zeit dauern, so dass Sie möglicherweise warten möchten, bis I/O-Lasten leichter sind. Je nach I/O-Last und Cache-Größe kann ein Controller-Upgrade in der Regel zwischen 15 und 25 Minuten dauern. Die Controller starten neu und führen einen Failover während der Aktivierung durch. Dadurch kann die Performance bis zum Abschluss des Upgrades unter Umständen niedriger sein als üblich.
- **Paketyp** — möglicherweise möchten Sie die neue Software und Firmware auf einem Speicher-Array testen, bevor Sie die Dateien auf anderen Speicher-Arrays aktualisieren.

Um die stufenweise Software zu aktivieren, gehen Sie zum Menü:Support[Upgrade Center] und klicken Sie im Bereich SANtricity OS-Controller-Software-Upgrade auf **Aktivieren**.

Zustandsprüfung

Eine Integritätsprüfung wird im Rahmen des Upgrade-Prozesses ausgeführt, Sie können aber auch vor dem Start eine Integritätsprüfung separat durchführen (siehe Menü:Upgrade Center [Health Check vor dem Upgrade]).

Bei der Integritätsprüfung werden alle Storage-Systemkomponenten bewertet, um sicherzustellen, dass das Upgrade fortgesetzt werden kann. Die folgenden Bedingungen können das Upgrade verhindern:

- Ausgefallene zugewiesene Laufwerke
- Hot Spares werden verwendet
- Unvollständige Volume-Gruppen
- Exklusive Vorgänge ausgeführt
- Fehlende Volumes

- Controller befindet sich im Status „nicht optimal“
- Übermäßige Anzahl von Ereignisprotokollereignissen
- Fehler bei der Validierung der Konfigurationsdatenbank
- Laufwerke mit alten Versionen von DACstore

Was muss ich vor einem Upgrade beachten?

Vor dem Upgrade mehrerer Storage-Arrays sollten Sie die wichtigsten Überlegungen in Ihrer Planung durchgehen.

Aktuelle Versionen

Sie können die aktuellen Softwareversionen des SANtricity Betriebssystems von der Seite Verwalten von Unified Manager für jedes erkannte Storage-Array anzeigen. Die Version wird in der Spalte SANtricity OS Software angezeigt. Die Informationen zu Controller-Firmware und NVSRAM finden Sie in einem Popup-Dialogfeld, wenn Sie in den einzelnen Zeilen auf die SANtricity OS-Version klicken.

Andere Komponenten müssen aktualisiert werden

Im Rahmen des Upgrades müssen Sie eventuell auch den Multipath-/Failover-Treiber oder den HBA-Treiber des Hosts aktualisieren, damit der Host korrekt mit den Controllern interagieren kann.

Informationen zur Kompatibilität finden Sie im "NetApp Interoperabilitätsmatrix". Lesen Sie auch die Verfahren in den Express-Leitfäden für Ihr Betriebssystem. Express-Leitfäden finden Sie im "E-Series und SANtricity Dokumentation".

Dual-Controller

Wenn ein Storage-Array zwei Controller enthält und ein Multipath-Treiber installiert ist, kann das Storage-Array die I/O-Verarbeitung während des Upgrades fortsetzen. Während des Upgrades erfolgt der folgende Vorgang:

1. Controller A Failover aller LUNs zu Controller B
2. Das Upgrade erfolgt bei Controller A
3. Controller A nimmt seine LUNs und alle Controller B LUNs wieder auf.
4. Upgrade erfolgt auf Controller B.

Nach Abschluss des Upgrades müssen Sie Volumes möglicherweise manuell zwischen den Controllern neu verteilen, um sicherzustellen, dass die Volumes wieder zum korrekten Controller zurückkehren.

Aktualisieren von Software und Firmware

Führen Sie eine Integritätsprüfung vor dem Upgrade durch

Eine Zustandsprüfung wird im Rahmen des Upgrade-Prozesses ausgeführt, doch vor Beginn kann zusätzlich ein Systemcheck separat durchgeführt werden. Bei der Integritätsprüfung werden Komponenten des Storage-Arrays bewertet, um sicherzustellen, dass das Upgrade fortgesetzt werden kann.

Schritte

1. Wählen Sie in der Hauptansicht **Verwalten** und dann Menü:Upgrade Center[Health Check Pre-Upgrade].

Das Dialogfeld Integritätsprüfung vor dem Upgrade wird geöffnet und zeigt alle erkannten Speichersysteme an.

2. Filtern oder sortieren Sie bei Bedarf die Speichersysteme in der Liste, sodass Sie alle Systeme, die sich derzeit nicht im optimalen Zustand befinden, anzeigen können.
3. Aktivieren Sie die Kontrollkästchen für die Speichersysteme, die Sie durch die Integritätsprüfung ausführen möchten.
4. Klicken Sie Auf **Start**.

   Der Fortschritt wird im Dialogfeld angezeigt, während die Integritätsprüfung durchgeführt wird.

5. Wenn die Integritätsprüfung abgeschlossen ist, können Sie rechts neben jeder Zeile auf die Ellipsen (…) klicken, um weitere Informationen anzuzeigen und andere Aufgaben auszuführen.

> Wenn Arrays die Integritätsprüfung nicht bestanden haben, können Sie das jeweilige Array überspringen und das Upgrade für die anderen fortsetzen. Alternativ können Sie den gesamten Prozess beenden und die Arrays, die nicht bestanden haben, beheben.

Upgrade von SANtricity OS

Aktualisieren Sie ein oder mehrere Storage-Arrays mit der neuesten Software und NVSRAM, um sicherzustellen, dass Sie über alle neuesten Funktionen und Fehlerbehebungen verfügen. Der NVSRAM-Controller ist eine Controller-Datei, die die Standardeinstellungen für die Controller angibt.

Bevor Sie beginnen

- Die neuesten Dateien des SANtricity Betriebssystems sind auf dem Host-System verfügbar, auf dem der SANtricity Web Services Proxy und Unified Manager ausgeführt werden.
- Sie wissen, ob Sie Ihr Software-Upgrade jetzt oder später aktivieren möchten.

  Aus folgenden Gründen können Sie sich später aktivieren:

  - **Tageszeit** — die Aktivierung der Software kann eine lange Zeit dauern, so dass Sie möglicherweise warten möchten, bis I/O-Lasten leichter sind. Der Failover der Controller während der Aktivierung ist möglich, sodass die Performance bis zum Abschluss des Upgrades unter Umständen niedriger ist als üblich.
  - **Art des Pakets** — möglicherweise möchten Sie die neue Betriebssystemsoftware auf einem Speicher-Array testen, bevor Sie die Dateien auf anderen Speicher-Arrays aktualisieren.

> Auf Systemen muss SANtricity OS 11.70.5 ausgeführt werden, um ein Upgrade auf 11.80.x oder höher durchzuführen.

Über diese Aufgabe

```
[NOTE]
====
Risiko eines Datenverlusts oder einer Beschädigung des Storage Arrays:
Nehmen Sie während des Upgrades keine Änderungen am Storage Array vor.
Halten Sie den Strom für das Speicher-Array aufrecht.
```

```
====
.Schritte
. Wenn Ihr Storage Array nur einen Controller oder einen Multipath-Treiber
enthält, beenden Sie die I/O-Aktivitäten des Storage Arrays, um
Applikationsfehler zu vermeiden. Wenn Ihr Storage Array über zwei
Controller verfügt und Sie einen Multipath-Treiber installiert haben,
müssen Sie die I/O-Aktivität nicht stoppen.
. Wählen Sie in der Hauptansicht *Verwalten* aus, und wählen Sie dann ein
oder mehrere Speicher-Arrays aus, die Sie aktualisieren möchten.
. Wählen Sie MENU:Upgrade Center[Upgrade SANtricity OS Software].
+
Die Seite SANtricity OS-Software aktualisieren wird angezeigt.

. Laden Sie das neueste Software-Paket für SANtricity OS von der NetApp
Support-Website auf Ihren lokalen Computer herunter.
+
.. Klicken Sie auf *Neue Datei zum Software-Repository hinzufügen*.
.. Klicken Sie auf den Link, um die neuesten *SANtricity OS Downloads* zu
finden.
.. Klicken Sie auf den Link *Letzte Version herunterladen*.
.. Folgen Sie den restlichen Anweisungen, um die SANtricity OS-Datei und
die NVSRAM-Datei auf Ihren lokalen Computer herunterzuladen.


+
[NOTE]
====
In Version 8.42 und höher ist digital signierte Firmware erforderlich.
Wenn Sie versuchen, nicht signierte Firmware herunterzuladen, wird ein
Fehler angezeigt und der Download wird abgebrochen.

====
. Wählen Sie die Betriebssystemsoftware und die NVSRAM-Datei aus, die Sie
zum Aktualisieren der Controller verwenden möchten:
+
.. Wählen Sie aus der Dropdown-Liste *Select a SANtricity OS Software
file* die Betriebssystemdatei aus, die Sie auf Ihren lokalen Rechner
heruntergeladen haben.
+
Wenn mehrere Dateien verfügbar sind, werden die Dateien vom neuesten Datum
bis zum ältesten Datum sortiert.

+
[NOTE]
====
```

Das Software-Repository enthält alle Softwaredateien, die dem Web Services Proxy zugeordnet sind. Wenn die Datei nicht angezeigt wird, die Sie verwenden möchten, klicken Sie auf den Link *Neue Datei zum Software-Repository hinzufügen*, um zu dem Speicherort zu navigieren, an dem sich die Betriebssystemdatei befindet, die Sie hinzufügen möchten.

====
.. Wählen Sie im Dropdown-Menü *Select an NVSRAM file* die gewünschte Controllerdatei aus.
+
Wenn es mehrere Dateien gibt, werden die Dateien vom neuesten Datum bis zum ältesten Datum sortiert.

. Überprüfen Sie in der Tabelle kompatibler Speicher-Arrays die Speicherarrays, die mit der ausgewählten Betriebssystemsoftware kompatibel sind, und wählen Sie dann die Arrays aus, die aktualisiert werden sollen.
+
** Die Speicherarrays, die Sie in der Ansicht Verwalten ausgewählt haben und mit der ausgewählten Firmware-Datei kompatibel sind, werden standardmäßig in der Tabelle kompatible Speicherarrays ausgewählt.
** Die Speicher-Arrays, die nicht mit der ausgewählten Firmware-Datei aktualisiert werden können, können in der kompatiblen Speicher-Array-Tabelle nicht wie im Status *inkompatibel* angegeben ausgewählt werden.

. *Optional:* um die Software-Datei auf die Speicher-Arrays zu übertragen, ohne sie zu aktivieren, wählen Sie das Kontrollkästchen *Betriebssystemsoftware auf die Speicher-Arrays übertragen, als bereitgestellt markieren und zu einem späteren Zeitpunkt aktivieren*.
. Klicken Sie Auf *Start*.
. Je nachdem, ob Sie jetzt oder später aktiviert haben, führen Sie einen der folgenden Schritte aus:
+
** Geben Sie *TRANSFER* ein, um zu bestätigen, dass Sie die vorgeschlagenen Betriebssystemversionen auf den Arrays übertragen möchten, die Sie für die Aktualisierung ausgewählt haben, und klicken Sie dann auf *Transfer*.
+
Um die übertragene Software zu aktivieren, wählen Sie MENU:Upgrade Center[Staged OS Software aktivieren].

** Geben Sie *UPGRADE* ein, um zu bestätigen, dass Sie die vorgeschlagenen Betriebssystemversionen auf den Arrays übertragen und aktivieren möchten, die Sie aktualisieren möchten, und klicken Sie dann auf *Upgrade*.

```
+
Das System überträgt die Softwaredatei auf jedes Speicherarray, das Sie
für die Aktualisierung ausgewählt haben, und aktiviert diese Datei durch
einen Neustart.



+
Während des Aktualisierungsvorgangs treten folgende Aktionen auf:

+
** Im Rahmen des Upgrades wird eine Integritätsprüfung vor dem Upgrade
ausgeführt. Bei der Integritätsprüfung vor dem Upgrade werden alle
Komponenten des Storage Arrays bewertet, um sicherzustellen, dass das
Upgrade fortgesetzt werden kann.
** Wenn eine Integritätsprüfung für ein Speicherarray fehlschlägt, wird
das Upgrade abgebrochen. Sie können auf die Ellipsen (...) klicken und
*Protokoll speichern* wählen, um die Fehler zu überprüfen. Sie können auch
den Fehler der Integritätsprüfung überschreiben und dann auf *Weiter*
klicken, um mit dem Upgrade fortzufahren.
** Sie können den Upgrade-Vorgang nach der Integritätsprüfung vor dem
Upgrade abbrechen.


. *Optional:* nach Abschluss des Upgrades sehen Sie eine Liste der für ein
bestimmtes Speicherarray aktualisierten Versionen, indem Sie auf die
Ellipsen (...) klicken und dann *Protokoll speichern* wählen.
+
Die Datei wird im Ordner Downloads für Ihren Browser mit dem Namen
gespeichert `upgrade_log-<date>.json`.




[[ID59142ffd677abee66ce4ff4c29fa8886]]
= Aktivieren Sie die stufenweise Betriebssystemsoftware
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Sie können die Software-Datei sofort aktivieren oder bis zu einem
angenehmeren Zeitpunkt warten. Bei diesem Verfahren wird davon
```

ausgegangen, dass Sie die Softwaredatei zu einem späteren Zeitpunkt aktivieren.

.Über diese Aufgabe
Sie können die Firmware-Dateien übertragen, ohne sie zu aktivieren. Aus folgenden Gründen können Sie sich später aktivieren:

* *Tageszeit* -- die Aktivierung der Software kann eine lange Zeit dauern, so dass Sie möglicherweise warten möchten, bis I/O-Lasten leichter sind. Die Controller starten neu und führen einen Failover während der Aktivierung durch. Dadurch kann die Performance bis zum Abschluss des Upgrades unter Umständen niedriger sein als üblich.
* *Paketyp* -- möglicherweise möchten Sie die neue Software und Firmware auf einem Speicher-Array testen, bevor Sie die Dateien auf anderen Speicher-Arrays aktualisieren.

[NOTE]
====
Sie können den Aktivierungsvorgang nach dem Start nicht beenden.

====
.Schritte
. Wählen Sie in der Hauptansicht *Verwalten*. Klicken Sie bei Bedarf auf die Spalte Status, um oben auf der Seite alle Storage Arrays mit dem Status „OS Upgrade (Aktivierung ausstehend)“ zu sortieren.
. Wählen Sie einen oder mehrere Speicher-Arrays aus, für die Sie Software aktivieren möchten, und wählen Sie dann Menü:Upgrade Center[Activate Staged OS Software].
+
Während des Aktualisierungsvorgangs treten folgende Aktionen auf:

+
** Im Rahmen der Aktivierung wird eine Integritätsprüfung vor dem Upgrade ausgeführt. Bei der Integritätsprüfung vor dem Upgrade werden alle Komponenten des Storage-Arrays bewertet, um sicherzustellen, dass die Aktivierung fortgesetzt werden kann.
** Wenn eine Integritätsprüfung für ein Speicherarray fehlschlägt, wird die Aktivierung angehalten. Sie können auf die Ellipsen (...) klicken und *Protokoll speichern* wählen, um die Fehler zu überprüfen. Sie können auch den Fehler der Integritätsprüfung überschreiben und dann auf *Weiter* klicken, um mit der Aktivierung fortzufahren.
** Sie können den Aktivierungsvorgang nach der Integritätsprüfung vor dem Upgrade abbrechen. Nach erfolgreichem Abschluss der Integritätsprüfung vor dem Upgrade erfolgt die Aktivierung. Die Aktivierungszeiten hängen von der Konfiguration des Speicherarrays und den Komponenten ab, die Sie

```
aktivieren.


. *Optional:* nach Abschluss der Aktivierung sehen Sie eine Liste dessen,
was für ein bestimmtes Speicherarray aktiviert wurde, indem Sie auf die
Ellipsen (...) klicken und dann *Protokoll speichern* wählen.
+
Die Datei wird im Ordner Downloads für Ihren Browser mit dem Namen
gespeichert `activate_log-<date>.json`.




[[ID961d38534289a5798a1d95261b8a664e]]
= Software-Repository managen
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Das Software-Repository enthält alle Softwaredateien, die dem Web Services
Proxy zugeordnet sind.

Wenn Sie die Datei nicht sehen, die Sie verwenden möchten, können Sie
mithilfe der Option Software-Repository verwalten eine oder mehrere
SANtricity-Betriebssystemdateien auf das Hostsystem importieren, auf dem
der Webservices-Proxy und Unified Manager ausgeführt werden. Sie können
auch festlegen, dass eine oder mehrere SANtricity OS-Dateien gelöscht
werden sollen, die im Software-Repository verfügbar sind.

.Bevor Sie beginnen
Wenn Sie SANtricity OS-Dateien hinzufügen, stellen Sie sicher, dass die
Betriebssystemdateien auf Ihrem lokalen System verfügbar sind.

.Schritte
. Wählen Sie in der Hauptansicht *Verwalten* und dann Menü:Upgrade
Center[Software-Repository verwalten].
+
Das Dialogfeld Software-Repository verwalten wird angezeigt.

. Führen Sie eine der folgenden Aktionen aus:
+
[cols="25h,~"]
```

```
|===
| Option | Tun Sie das


 a|
Importieren
 a|
.. Klicken Sie Auf *Import.*
.. Klicken Sie auf *Durchsuchen* und navigieren Sie dann zu dem
Speicherort, an dem die Betriebssystemdateien gespeichert werden sollen.
+
Betriebssystemdateien haben einen ähnlichen Dateinamen wie `N2800-830000-
000.dlp`.

.. Wählen Sie eine oder mehrere Betriebssystemdateien aus, die Sie
hinzufügen möchten, und klicken Sie dann auf *Import*.




 a|
Löschen
 a|
.. Wählen Sie eine oder mehrere Betriebssystemdateien aus, die Sie aus dem
Software-Repository entfernen möchten.
.. Klicken Sie Auf *Löschen*.


|===


.Ergebnisse
Wenn Sie den Import ausgewählt haben, werden die Dateien hochgeladen und
validiert. Wenn Sie „Löschen“ ausgewählt haben, werden die Dateien aus dem
Software-Repository entfernt.



[[ID01b75a9c77f5bd2158d1e9573b220706]]
= Software für das überstaltete Betriebssystem löschen
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
Sie können die stufenweise Betriebssystemsoftware entfernen, um
sicherzustellen, dass eine ausstehende Version zu einem späteren Zeitpunkt
nicht versehentlich aktiviert wird. Das Entfernen der stufenweisen
Betriebssystemsoftware hat keine Auswirkungen auf die aktuelle Version,
die auf den Speicher-Arrays ausgeführt wird.

.Schritte
. Wählen Sie in der Hauptansicht *Verwalten* und dann Menü:Upgrade
Center[Staged OS Software löschen].
+
Das Dialogfeld „Staged OS Software löschen“ wird geöffnet und listet alle
erkannten Speichersysteme mit ausstehender Software oder NVSRAM auf.

. Filtern oder sortieren Sie die Speichersysteme in der Liste, falls
erforderlich, so dass Sie alle Systeme mit stufenweise Software anzeigen
können.
. Aktivieren Sie die Kontrollkästchen für die Speichersysteme mit
ausstehender Software, die Sie löschen möchten.
. Klicken Sie Auf *Löschen*.
+
Der Status des Vorgangs wird im Dialogfeld angezeigt.




:leveloffset: -1


:leveloffset: -1


= Spiegelung

:leveloffset: +1


[[IDacaa2c2093454f9a16b842a8462231f5]]
= Spiegelung – Übersicht
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
```

```
Mithilfe der Spiegelungsfunktionen können Daten entweder asynchron oder
synchron zwischen einem lokalen Storage-Array und einem Remote-Storage-
Array repliziert werden.

[NOTE]
====
Synchrones Spiegeln ist auf dem EF600 oder EF300 Storage-System nicht
verfügbar.

====


== Was ist Spiegelung?

SANtricity-Applikationen beinhalten zwei Arten von Spiegelung: Asynchron
und synchron. Die asynchrone Spiegelung kopiert Daten-Volumes nach Bedarf
oder nach einem Zeitplan. So werden Ausfallzeiten, die auf
Datenbeschädigung oder -Verlust zurückzuführen sind, minimiert oder
vermieden. Bei der synchronen Spiegelung werden Daten-Volumes in Echtzeit
repliziert, um eine kontinuierliche Verfügbarkeit zu gewährleisten.

Weitere Informationen:

* xref:{relative_path}mirroring-overview.html["Funktionsweise von
Spiegelung"]
* xref:{relative_path}mirroring-terminology.html["Terminologie wird
gespiegelt"]




== Wie konfiguriere ich Spiegelung?

Sie konfigurieren asynchrone oder synchrone Spiegelung in Unified Manager
und managen dann die Synchronisierung mit System Manager.

Weitere Informationen:

* xref:{relative_path}mirroring-configuration-workflow.html["Spiegelung
des Konfigurations-Workflows"]
* xref:{relative_path}requirements-for-using-mirroring.html["Anforderungen
für die Verwendung von Spiegelung"]
* xref:{relative_path}create-asynchronous-mirrored-pair-um.html["Erstellen
eines asynchronen gespiegelten Paares"]
* xref:{relative_path}create-synchronous-mirrored-pair-um.html["Erstellen
eines synchronen gespiegelten Paares"]
```

```
= Konzepte

:leveloffset: +1


[[ID01e35d4b6f1366f0b6ee06684aa32850]]
= Funktionsweise von Spiegelung
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
SANtricity Unified Manager enthält Konfigurationsoptionen für die
SANtricity-Spiegelungsfunktionen, mit denen Administratoren Daten zur
Datensicherung zwischen zwei Storage Arrays replizieren können.

[NOTE]
====
Synchrones Spiegeln ist auf dem EF600 oder EF300 Storage-System nicht
verfügbar.

====


== Arten der Spiegelung

SANtricity-Applikationen beinhalten zwei Arten von Spiegelung: Asynchron
und synchron.

Die asynchrone Spiegelung kopiert Daten-Volumes nach Bedarf oder nach
einem Zeitplan. So werden Ausfallzeiten, die auf Datenbeschädigung oder
-Verlust zurückzuführen sind, minimiert oder vermieden. Das asynchrone
Spiegeln erfasst den Status des primären Volumes zu einem bestimmten
Zeitpunkt und kopiert nur die Daten, die sich seit der letzten
Bildaufzeichnung geändert haben. Der primäre Standort kann sofort
aktualisiert werden, während der sekundäre Standort mit der Bandbreite
aktualisiert werden kann. Die Informationen werden im Cache gespeichert
und später gesendet, sobald Netzwerkressourcen verfügbar sind. Diese Art
der Spiegelung ist ideal für periodische Prozesse wie Backups und
Archivierungen.

Bei der synchronen Spiegelung werden Daten-Volumes in Echtzeit repliziert,
```

```
um eine kontinuierliche Verfügbarkeit zu gewährleisten. Der Zweck besteht
darin, ein Recovery Point Objective (RPO) von null Datenverlust zu
erreichen, indem eine Kopie wichtiger Daten verfügbar ist, falls auf einem
der beiden Storage Arrays ein Ausfall auftritt. Die Kopie ist zu jedem
Zeitpunkt identisch mit den Produktionsdaten. Jedes Mal, wenn ein
Schreibvorgang auf dem primären Volume ausgeführt wird, wird auf dem
sekundären Volume ein Schreibvorgang vorgenommen. Der Host erhält keine
Bestätigung, dass der Schreibvorgang erfolgreich war, bis das sekundäre
Volume mit den Änderungen auf dem primären Volume aktualisiert wurde.
Diese Art von Spiegelung ist ideal für Business Continuity-Zwecke wie
Disaster Recovery.



== Unterschiede zwischen Spiegelungstypen

In der folgenden Tabelle werden die Hauptunterschiede zwischen den beiden
Spiegelungstypen beschrieben.

[cols="1a,1a,1a"]
|===
| Attribut | Asynchron | Synchron


 a|
Replikationsmethode
 a|
Zeitpunktgenau: Die Spiegelung wird nach Bedarf oder automatisch gemäß
einem benutzerdefinierten Zeitplan durchgeführt.
 a|
Continuous -- die Spiegelung wird automatisch kontinuierlich ausgeführt
und kopiert die Daten von jedem Host-Schreibvorgang.



 a|
Entfernung
 a|
Unterstützt große Entfernungen zwischen den Arrays. In der Regel ist die
Entfernung nur durch die Fähigkeiten des Netzwerks und der Channel-
Erweiterungstechnologie begrenzt.
 a|
Beschränkt auf kürzere Entfernungen zwischen den Arrays. In der Regel muss
die Entfernung ca. 10 km (6.2 Meilen) vom lokalen Storage-Array entfernt
sein, um die Anforderungen bezüglich Latenz und Applikations-Performance
zu erfüllen.
```

```
 a|
Kommunikationsmethode
 a|
Einem standardmäßigen IP- oder Fibre Channel-Netzwerk an.
 a|
Nur Fibre Channel-Netzwerk.



 a|
Volume-Typen
 a|
Standard oder Thin
 a|
Nur Standard.

|===



[[ID0bd54cdd1951d5a37e458c0a55f8ff0c]]
= Spiegelung des Konfigurations-Workflows
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
In SANtricity Unified Manager wird die asynchrone oder synchrone
Spiegelung konfiguriert und anschließend mit SANtricity System Manager die
Synchronisierung verwaltet.



== Workflow für asynchrone Spiegelung

Die asynchrone Spiegelung umfasst den folgenden Workflow:

. Die Erstkonfiguration in Unified Manager durchführen:
+
.. Wählen Sie das lokale Speicher-Array als Quelle für den Datentransfer
aus.
.. Erstellen oder Auswählen einer vorhandenen SpiegelungsConsistency
Group: Dies ist ein Container für das primäre Volume auf dem lokalen Array
```

```
und dem sekundären Volume auf dem Remote-Array. Das primäre und sekundäre
Volume werden als „gespiegeltes Paar“ bezeichnet. Wenn Sie zum ersten Mal
die Spiegelkonsistent-Gruppe erstellen, legen Sie fest, ob Sie manuelle
oder geplante Synchronisierungen durchführen möchten.
.. Wählen Sie ein primäres Volume aus dem lokalen Speicher-Array aus, und
bestimmen Sie dann die reservierte Kapazität. Die reservierte Kapazität
ist die physisch zugewiesene Kapazität, die für den Kopiervorgang
verwendet werden soll.
.. Wählen Sie ein Remote-Speicher-Array als Ziel des Transfers, ein
sekundäres Volume, und legen Sie dann seine reservierte Kapazität fest.
.. Beginnen Sie den ersten Datentransfer vom primären Volume zum
sekundären Volume. Je nach Volume-Größe kann dieser erste Transfer mehrere
Stunden dauern.


. Den Fortschritt der ersten Synchronisierung überprüfen:
+
.. Starten Sie in Unified Manager den System Manager für das lokale Array.
.. Zeigen Sie in System Manager den Status des Spiegelungsvorgangs an.
Nach Abschluss der Spiegelung ist der Status des gespiegelten Paares
„optimal“.


. Optional können Sie nachfolgende Datentransfers in System Manager neu
terminieren oder manuell durchführen. Es werden nur neue und geänderte
Blöcke vom primären Volume auf das sekundäre Volume übertragen.
+
[NOTE]
====
Da die asynchrone Replizierung periodisch erfolgt, kann das System die
geänderten Blöcke konsolidieren und Netzwerkbandbreite sparen. Der
Schreibdurchsatz und die Schreiblatenz sind nur minimal beeinträchtigt.

====




== Workflow für synchrones Spiegeln

Die synchrone Spiegelung umfasst den folgenden Workflow:

. Die Erstkonfiguration in Unified Manager durchführen:
+
.. Wählen Sie ein lokales Speicher-Array als Quelle für den Datentransfer
aus.
.. Wählen Sie ein primäres Volume aus dem lokalen Speicher-Array aus.
```

```
.. Wählen Sie ein Remote-Speicher-Array als Ziel für den Datentransfer
aus, und wählen Sie dann ein sekundäres Volume aus.
.. Wählen Sie Synchronisierungsprioritäten und Neusynchronisierung aus.
.. Beginnen Sie den ersten Datentransfer vom primären Volume zum
sekundären Volume. Je nach Volume-Größe kann dieser erste Transfer mehrere
Stunden dauern.


. Den Fortschritt der ersten Synchronisierung überprüfen:
+
.. Starten Sie in Unified Manager den System Manager für das lokale Array.
.. Zeigen Sie in System Manager den Status des Spiegelungsvorgangs an.
Nach Abschluss der Spiegelung ist der Status des gespiegelten Paares
„optimal“. Die beiden Arrays versuchen, während des normalen Betriebs
synchronisiert zu bleiben. Es werden nur neue und geänderte Blöcke vom
primären Volume auf das sekundäre Volume übertragen.


. Optional können Sie die Synchronisierungseinstellungen in System Manager
ändern.
+
[NOTE]
====
Da die synchrone Replizierung kontinuierlich erfolgt, muss die
Replizierungsverbindung zwischen den beiden Standorten ausreichend
Bandbreitenkapazität bereitstellen.

====




[[ID6560fee41abaf458fbd6181daa721cd9]]
= Terminologie wird gespiegelt
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Erfahren Sie, wie die Spiegelungsbedingungen auf Ihr Storage-Array
angewendet werden.

[cols="25h,~"]
|===
| Laufzeit | Beschreibung
```

a|
Lokales Storage-Array
a|
Das lokale Storage-Array ist das Storage-Array, auf dem Sie arbeiten.

a|
Spiegelung der Konsistenzgruppe
a|
Eine gespiegelte Konsistenzgruppe ist ein Container für ein oder mehrere gespiegelte Paare. Für asynchrone Spiegelungsvorgänge müssen Sie eine Konsistenzgruppe erstellen. Alle gespiegelten Paare in einer Gruppe werden gleichzeitig resynchronisiert, sodass ein konsistenter Wiederherstellungspunkt beibehalten wird.

Bei der synchronen Spiegelung werden keine Konsistenzgruppen verwendet.

a|
Gespiegeltes Paar
a|
Ein gespiegeltes Paar besteht aus zwei Volumes, einem primären Volume und einem sekundären Volume.

Bei der asynchronen Spiegelung gehört ein gespiegeltes Paar immer einer gespiegelten Konsistenzgruppe an. Schreibvorgänge werden zunächst auf dem primären Volume durchgeführt und dann auf das sekundäre Volume repliziert. Jedes gespiegelte Paar in einer Spiegelkonsistent-Gruppe verwendet dieselben Synchronisierungseinstellungen.

a|
Primäres Volume
a|
Das primäre Volume eines gespiegelten Paars ist das zu spiegelnden Quell-Volume.

a|
Remote Storage Array
a|

```
Das Remote Storage Array wird in der Regel als sekundärer Standort
bezeichnet, der in der Regel ein Replikat der Daten in einer
Spiegelungskonfiguration enthält.



 a|
Reservierte Kapazität
 a|
Reservierte Kapazität ist die zugewiesene physische Kapazität, die für
jeden Kopierdienst- und Storage-Objekt verwendet wird. Er ist nicht direkt
vom Host lesbar.

Diese Volumes sind erforderlich, damit der Controller permanent
Informationen speichern kann, die erforderlich sind, um die Spiegelung in
einem Betriebszustand zu halten. Sie enthalten Informationen wie Delta-
Protokolle und Copy-on-Write-Daten.



 a|
Sekundäres Volume
 a|
Das sekundäre Volume eines gespiegelten Paars befindet sich normalerweise
an einem sekundären Standort und enthält ein Replikat der Daten.



 a|
Synchronisierung
 a|
Die Synchronisierung erfolgt bei der ersten Synchronisierung zwischen dem
lokalen Speicher-Array und dem Remote-Speicher-Array. Die Synchronisierung
findet auch statt, wenn primäre und sekundäre Volumes nach einer
Kommunikationsunterbrechung nicht mehr synchronisiert werden. Wenn die
Kommunikationsverbindung wieder funktioniert, werden alle nicht
replizierten Daten mit dem Storage-Array des sekundären Volumes
synchronisiert.

|===



[[IDbd42cff28f67f7eef72784dd8db41f65]]
= Anforderungen für die Verwendung von Spiegelung
:allow-uri-read:
:experimental:
```

```
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Wenn Sie die Spiegelung konfigurieren möchten, beachten Sie die folgenden
Anforderungen.



== Unified Manager

* Der Web Services Proxy-Dienst muss ausgeführt werden.
* Unified Manager muss auf Ihrem lokalen Host über eine HTTPS-Verbindung
ausgeführt werden.
* Unified Manager muss gültige SSL-Zertifikate für das Speicher-Array
anzeigen. Sie können ein selbstsigniertes Zertifikat akzeptieren oder Ihr
eigenes Sicherheitszertifikat mit Unified Manager installieren und zum
Menü:Zertifikat[Zertifikatverwaltung] navigieren.




== Storage-Arrays durchführt

[NOTE]
====
Synchrones Spiegeln ist auf dem EF600 oder EF300 Storage-Array nicht
verfügbar.

====
* Sie müssen über zwei Storage-Arrays verfügen.
* Jedes Speicher-Array muss zwei Controller haben.
* Die beiden Storage Arrays müssen in Unified Manager erkannt werden.
* Jeder Controller im primären Array und im sekundären Array muss über
einen konfigurierten Ethernet-Managementport verfügen und mit dem Netzwerk
verbunden sein.
* Die Speicher-Arrays verfügen über eine Firmware-Version von mindestens
7.84. (Beide können unterschiedliche OS-Versionen ausführen.)
* Sie müssen das Passwort für die lokalen und Remote-Speicher-Arrays
kennen.
* Sie benötigen genügend freie Kapazität auf dem Remote-Speicher-Array, um
ein sekundäres Volume zu erstellen, das dem primären Volume entspricht
oder dessen Größe Sie spiegeln möchten.
* Asynchrones Spiegeln wird auf Controllern mit Fibre Channel (FC)- oder
iSCSI-Host-Ports unterstützt, während synchrones Spiegeln nur auf
```

Controllern mit FC Host-Ports unterstützt wird.

== Konnektivitätsanforderungen erfüllen

Für die Spiegelung über eine FC-Schnittstelle (asynchron oder synchron) ist Folgendes erforderlich:

* Jeder Controller des Storage-Arrays ordnet den am höchsten nummerierten FC-Host-Port der Spiegelung zu.
* Wenn der Controller sowohl Basis-FC-Ports als auch Host-Schnittstellenkarten (HIC) FC-Ports hat, ist der Port mit der höchsten Nummer auf einer HIC. Alle Hosts, die am dedizierten Port angemeldet sind, werden abgemeldet, und es werden keine Anmeldeanforderungen für den Host akzeptiert. I/O-Anfragen auf diesem Port werden nur von Controllern akzeptiert, die an Spiegelungsvorgängen beteiligt sind.
* Die dedizierten Spiegelungs-Ports müssen an eine FC-Fabric-Umgebung angeschlossen werden, die den Verzeichnisdienst und die Nameservice-Schnittstellen unterstützt. Insbesondere werden FC-AL und Point-to-Point nicht als Konnektivitätsoptionen zwischen den Controllern unterstützt, die an gespiegelten Beziehungen beteiligt sind.

Die Spiegelung über eine iSCSI-Schnittstelle (nur asynchron) erfordert Folgendes:

* Im Gegensatz zu FC erfordert iSCSI keinen dedizierten Port. Wenn Sie asynchrone Spiegelung in iSCSI-Umgebungen einsetzen, müssen Sie keine der Front-End iSCSI-Ports des Storage-Arrays für die asynchrone Spiegelung verwenden. Diese Ports werden sowohl für asynchronen Spiegeldatenverkehr als auch für Array-I/O-Verbindungen gemeinsam genutzt.
* Der Controller verfügt über eine Liste der Remote-Speichersysteme, mit denen der iSCSI-Initiator versucht, eine Sitzung einzurichten. Der erste Port, der eine iSCSI-Verbindung erfolgreich herstellt, wird für die anschließende Kommunikation mit dem Remote-Speicher-Array verwendet. Wenn die Kommunikation fehlschlägt, wird eine neue Sitzung unter Verwendung aller verfügbaren Ports versucht.
* ISCSI-Ports werden auf Array-Ebene für Port konfiguriert. Intercontroller Kommunikation für Konfigurationsnachrichten und Datentransfer verwendet die globalen Einstellungen, einschließlich Einstellungen für:
+
** VLAN: Sowohl lokale als auch Remote-Systeme müssen die gleiche VLAN-Einstellung für die Kommunikation haben

```
** ISCSI-Listening-Port
** Jumbo-Frames
** Ethernet-Priorität



[NOTE]
====
Die iSCSI-Intercontroller-Kommunikation muss einen Host-Connect-Port und
nicht den Management-Ethernet-Port verwenden.

====


== Kandidaten für gespiegelte Volumes

* RAID-Level, Caching-Parameter und Segmentgröße können auf den primären
und sekundären Volumes eines gespiegelten Paars unterschiedlich sein.
+

NOTE: Bei EF600- und EF300-Controllern müssen die primären und sekundären
Volumes eines asynchronen gespiegelten Paares dasselbe Protokoll, Tray-
Level, Segmentgröße, Sicherheitstyp und RAID-Level erfüllen. Nicht
geeignete asynchrone gespiegelte Paare werden nicht in der Liste der
verfügbaren Volumes angezeigt.

* Das sekundäre Volume muss mindestens so groß sein wie das primäre
Volume.
* Ein Volume kann nur an einer Spiegelbeziehung beteiligt sein.
* Für ein synchrones gespiegeltes Paar müssen die primären und sekundären
Volumes Standard-Volumes sein. Es können keine dünnen Volumes oder
Snapshot Volumes sein.
* Für die synchrone Spiegelung gibt es eine Begrenzung für die Anzahl der
Volumes, die auf einem bestimmten Storage Array unterstützt werden.
Stellen Sie sicher, dass die Anzahl der konfigurierten Volumes in Ihrem
Speicher-Array kleiner als das unterstützte Limit ist. Wenn das synchrone
Spiegeln aktiv ist, werden die zwei reservierten Kapazitäts-Volumes, die
erstellt werden, mit der Volume-Obergrenze verglichen.
* Beim asynchronen Spiegeln müssen das primäre Volume und das sekundäre
Volume dieselben Laufwerksicherheitsfunktionen aufweisen.
+
** Wenn das primäre Volume FIPS-fähig ist, muss das sekundäre Volume FIPS-
fähig sein.
** Wenn das primäre Volume FDE-fähig ist, muss das sekundäre Volume FDE-
fähig sein.
** Wenn das primäre Volume keine Laufwerkssicherheit verwendet, darf das
```

sekundäre Volume keine Laufwerkssicherheit verwenden.

== Reservierte Kapazität

Asynchrones Spiegeln:

* Ein reserviertes Kapazitäts-Volume ist für ein primäres Volume und ein sekundäres Volume in einem gespiegelten Paar für das Protokollieren von Schreibinformationen erforderlich, um nach einem Controller-Reset und anderen temporären Unterbrechungen wiederherzustellen.
* Da sowohl das primäre Volume als auch das sekundäre Volume in einem gespiegelten Paar zusätzliche reservierte Kapazität benötigen, müssen Sie sicherstellen, dass auf beiden Storage-Arrays in der Spiegelbeziehung freie Kapazität verfügbar ist.

Synchrones Spiegeln:

* Für ein primäres Volume und ein sekundäres Volume zur Protokollierung von Schreibinformationen zum Wiederherstellen nach Controller-Resets und anderen vorübergehenden Unterbrechungen ist die reservierte Kapazität erforderlich.
* Die reservierten Kapazitäts-Volumes werden automatisch bei aktivierter synchronen Spiegelung erstellt. Da sowohl das primäre Volume als auch das sekundäre Volume in einem gespiegelten Paar reservierte Kapazität benötigen, müssen Sie sicherstellen, dass auf beiden Storage-Arrays, die an der Beziehung zur synchronen Spiegelung beteiligt sind, ausreichend freie Kapazität zur Verfügung steht.

== Laufwerkssicherheit

* Wenn Sie sichere Laufwerke verwenden, müssen das primäre und das sekundäre Volume über kompatible Sicherheitseinstellungen verfügen. Diese Beschränkung wird nicht durchgesetzt, deshalb müssen Sie sie selbst überprüfen.
* Bei Verwendung von sicheren Laufwerken sollten das primäre Volume und das sekundäre Volume denselben Laufwerkstyp verwenden. Diese Beschränkung wird nicht durchgesetzt, deshalb müssen Sie sie selbst überprüfen.
* Wenn Sie Data Assurance (da) verwenden, müssen das primäre Volume und

```
das sekundäre Volume über dieselben da-Einstellungen verfügen.




:leveloffset: -1


= Konfigurieren Sie die Spiegelung

:leveloffset: +1


[[IDb39a3b0dbb55f966908028187fdcabb2]]
= Erstellen eines asynchronen gespiegelten Paares
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Zum Konfigurieren der asynchronen Spiegelung erstellen Sie ein
gespiegeltes Paar, das ein primäres Volume auf dem lokalen Array und ein
sekundäres Volume des Remote-Arrays umfasst.

.Bevor Sie beginnen
Bevor Sie ein gespiegeltes Paar erstellen, erfüllen Sie die folgenden
Anforderungen für Unified Manager:

* Der Web Services Proxy-Dienst muss ausgeführt werden.
* Unified Manager muss auf Ihrem lokalen Host über eine HTTPS-Verbindung
ausgeführt werden.
* Unified Manager muss gültige SSL-Zertifikate für das Speicher-Array
anzeigen. Sie können ein selbstsigniertes Zertifikat akzeptieren oder Ihr
eigenes Sicherheitszertifikat mit Unified Manager installieren und zum
Menü:Zertifikat[Zertifikatverwaltung] navigieren.


Stellen Sie außerdem sicher, dass Sie die folgenden Anforderungen an
Storage Arrays und Volumes erfüllen:

* Jedes Speicher-Array muss zwei Controller haben.
* Die beiden Storage Arrays müssen in Unified Manager erkannt werden.
* Jeder Controller im primären Array und im sekundären Array muss über
einen konfigurierten Ethernet-Managementport verfügen und mit dem Netzwerk
```

verbunden sein.
* Die Speicher-Arrays verfügen über eine Firmware-Version von mindestens 7.84. (Beide können unterschiedliche OS-Versionen ausführen.)
* Sie müssen das Passwort für die lokalen und Remote-Speicher-Arrays kennen.
* Sie benötigen genügend freie Kapazität auf dem Remote-Speicher-Array, um ein sekundäres Volume zu erstellen, das dem primären Volume entspricht oder dessen Größe Sie spiegeln möchten.
* Ihre lokalen und Remote-Speicher-Arrays sind über eine Fibre Channel Fabric- oder iSCSI-Schnittstelle verbunden.
* Sie haben sowohl die primären als auch die sekundären Volumes erstellt, die Sie in der asynchronen Spiegelbeziehung verwenden möchten.
* Das sekundäre Volume muss mindestens so groß sein wie das primäre Volume.

.Über diese Aufgabe
Der Prozess zum Erstellen eines asynchronen gespiegelten Paares ist ein mehrstufiges Verfahren.

== Schritt 1: Erstellen oder wählen Sie eine gespiegelte Konsistenzgruppe aus

In diesem Schritt erstellen Sie eine neue Konsistenzgruppe für die Spiegelung, oder wählen Sie eine vorhandene Konsistenzgruppe aus. Eine gespiegelte Konsistenzgruppe ist ein Container für die primären und sekundären Volumes (das gespiegelte Paar) und gibt die gewünschte Resynchronisierung (manuell oder automatisch) für alle Paare in der Gruppe an.

.Schritte
. Wählen Sie auf der Seite *Verwalten* das lokale Speicher-Array aus, das Sie für die Quelle verwenden möchten.
. Wählen Sie Menü:Aktionen[Asynchronous Mirrored Pair erstellen].
+
Der Assistent Asynchronous Mirrored Pair erstellen wird geöffnet.

. Wählen Sie entweder eine vorhandene SpiegelungsConsistency Group aus oder erstellen Sie eine neue Konsistenzgruppe.
+
Um eine vorhandene Gruppe auszuwählen, stellen Sie sicher, dass *eine vorhandene SpiegelungsConsistency Group* ausgewählt ist, und wählen Sie dann die Gruppe aus der Tabelle aus. Eine Konsistenzgruppe kann mehrere gespiegelte Paare enthalten.

+
Gehen Sie zum Erstellen einer neuen Gruppe wie folgt vor:

+
.. Wählen Sie *Eine neue Spiegelkonsistent-Gruppe* aus und klicken Sie dann auf *Weiter*.
.. Geben Sie einen eindeutigen Namen ein, der am besten die Daten auf den Volumes beschreibt, die zwischen den beiden Speicher-Arrays gespiegelt werden. Ein Name kann nur aus Buchstaben, Zahlen und den Sonderzeichen Unterstrichen (_), Bindestrich (-) und dem Hash-Zeichen (#) bestehen. Ein Name darf 30 Zeichen nicht überschreiten und darf keine Leerzeichen enthalten.
.. Wählen Sie das Remote Storage Array aus, auf dem Sie eine Mirror-Beziehung zum lokalen Speicher-Array herstellen möchten.
+
[NOTE]
====
Wenn Ihr Remote-Speicher-Array passwortgeschützt ist, fordert das System zur Eingabe eines Kennworts auf.

====
.. Wählen Sie aus, ob Sie die gespiegelten Paare manuell oder automatisch synchronisieren möchten:
+
*** *Manuell* -- Wählen Sie diese Option, um die Synchronisierung für alle gespiegelten Paare innerhalb dieser Gruppe manuell zu starten. Beachten Sie, dass Sie, wenn Sie später eine Neusynchronisierung durchführen möchten, System Manager für das primäre Speicher-Array starten und dann zum Menü:Speicher[Asynchronous Mirroring] wechseln müssen, die Gruppe auf der Registerkarte *Mirror Consistency Groups* auswählen und dann Menü:Mehr[manuell neu synchronisieren] auswählen.
*** *Automatisch* -- Wählen Sie das gewünschte Intervall in *Minuten*, *Stunden* oder *Tagen* aus, vom Beginn des vorherigen Updates bis zum Beginn des nächsten Updates. Wenn beispielsweise das Synchronisierungsintervall auf 30 Minuten eingestellt ist und der Synchronisationsprozess um 4:00 Uhr beginnt, beginnt der nächste Vorgang um 4:30 Uhr

.. Wählen Sie die gewünschten Warnmeldungseinstellungen aus:
+
*** Geben Sie bei manuellen Synchronisierungen den Schwellenwert (definiert durch den Prozentsatz der verbleibenden Kapazität) für den Zeitpunkt an, an dem Benachrichtigungen empfangen werden.
*** Für automatische Synchronisierungen können Sie drei Arten der Alarmierung festlegen: Wenn die Synchronisierung in einer bestimmten

Zeitspanne nicht abgeschlossen wurde, wenn die Daten der Wiederherstellungspunkt auf dem Remote-Array älter als ein bestimmtes Zeitlimit sind und sich die reservierte Kapazität einem bestimmten Schwellenwert nähert (definiert durch den Prozentsatz der verbleibenden Kapazität).

. Wählen Sie *Weiter* und gehen Sie zu <<Schritt 2: Wählen Sie das primäre Volumen>>.
+
Wenn Sie eine neue gespiegelte Konsistenzgruppe definiert haben, erstellt Unified Manager zuerst die gespiegelte Konsistenzgruppe im lokalen Storage Array und erstellt dann die gespiegelte Konsistenzgruppe im Remote-Storage-Array. Sie können die gespiegelte Konsistenzgruppe anzeigen und verwalten, indem Sie System Manager für jedes Array starten.

+
[NOTE]
====
Wenn Unified Manager die SpiegelungsConsistency Group erfolgreich auf dem lokalen Speicher-Array erstellt, diese aber nicht auf dem Remote-Speicher-Array erstellt, wird die SpiegelConsistency Group automatisch aus dem lokalen Speicher-Array gelöscht. Wenn ein Fehler auftritt, während Unified Manager versucht, die gespiegelte Konsistenzgruppe zu löschen, müssen Sie sie manuell löschen.

====

== Schritt 2: Wählen Sie das primäre Volumen

In diesem Schritt wählen Sie das primäre Volume aus, das in der Spiegelbeziehung verwendet werden soll, und weisen seine reservierte Kapazität zu. Wenn Sie ein primäres Volume auf dem lokalen Speicher-Array auswählen, zeigt das System eine Liste aller berechtigten Volumes für dieses gespiegelte Paar an. Alle Volumes, die nicht für die Verwendung geeignet sind, werden in dieser Liste nicht angezeigt.

Alle Volumes, die Sie der Spiegelungs-Consistency Group auf dem lokalen Speicher-Array hinzufügen, besitzen die primäre Rolle in der Spiegelbeziehung.

.Schritte

. Wählen Sie aus der Liste der berechtigten Volumes ein Volume aus, das Sie als primäres Volume verwenden möchten, und klicken Sie dann auf *Weiter*, um die reservierte Kapazität zuzuweisen.
. Wählen Sie aus der Liste der teilnahmeberechtigten Kandidaten die reservierte Kapazität für das primäre Volume aus.
+
Beachten Sie folgende Richtlinien:

+
** Die Standardeinstellung für die reservierte Kapazität ist 20 % der Kapazität des Basis-Volumes, und in der Regel reicht diese Kapazität aus. Wenn Sie den Prozentsatz ändern, klicken Sie auf *Kandidaten aktualisieren*.
** Die erforderliche Kapazität variiert abhängig von der Häufigkeit und Größe der I/O-Schreibvorgänge auf dem primären Volume und wie lange Sie die Kapazität beibehalten müssen.
** Im Allgemeinen wählen Sie eine größere Kapazität für reservierte Kapazität aus, wenn eine oder beide Bedingungen vorhanden sind:
+
*** Sie beabsichtigen, das gespiegelte Paar für einen langen Zeitraum zu halten.
*** Ein großer Prozentsatz an Datenblöcken ändert sich auf dem primären Volume aufgrund von hoher I/O-Aktivität. Mithilfe von historischen Performance-Daten oder anderen Betriebssystem-Utilities können Sie typische I/O-Aktivitäten für das primäre Volume ermitteln.

. Wählen Sie *Weiter* und gehen Sie zu <<Schritt 3: Wählen Sie das sekundäre Volumen>>.

== Schritt 3: Wählen Sie das sekundäre Volumen

In diesem Schritt wählen Sie das sekundäre Volume aus, das in der Spiegelbeziehung verwendet werden soll, und weisen seine reservierte Kapazität zu. Wenn Sie ein sekundäres Volume auf dem Remote-Speicher-Array auswählen, zeigt das System eine Liste aller berechtigten Volumes für dieses gespiegelte Paar an. Alle Volumes, die nicht für die Verwendung geeignet sind, werden in dieser Liste nicht angezeigt.

Alle Volumes, die Sie der Spiegelungs-Konsistenzgruppe auf dem Remote-Speicher-Array hinzufügen, übernehmen die sekundäre Rolle in der Spiegelbeziehung.

.Schritte
. Wählen Sie aus der Liste der berechtigten Volumes ein Volume aus, das Sie als sekundäres Volume im gespiegelten Paar verwenden möchten, und klicken Sie dann auf *Weiter*, um die reservierte Kapazität zuzuweisen.
. Wählen Sie aus der Liste der teilnahmeberechtigten Kandidaten die reservierte Kapazität für das sekundäre Volume aus.
+
Beachten Sie folgende Richtlinien:

+
** Die Standardeinstellung für die reservierte Kapazität ist 20 % der Kapazität des Basis-Volumes, und in der Regel reicht diese Kapazität aus. Wenn Sie den Prozentsatz ändern, klicken Sie auf *Kandidaten aktualisieren*.
** Die erforderliche Kapazität variiert abhängig von der Häufigkeit und Größe der I/O-Schreibvorgänge auf dem primären Volume und wie lange Sie die Kapazität beibehalten müssen.
** Im Allgemeinen wählen Sie eine größere Kapazität für reservierte Kapazität aus, wenn eine oder beide Bedingungen vorhanden sind:
+
*** Sie beabsichtigen, das gespiegelte Paar für einen langen Zeitraum zu halten.
*** Ein großer Prozentsatz an Datenblöcken ändert sich auf dem primären Volume aufgrund von hoher I/O-Aktivität. Mithilfe von historischen Performance-Daten oder anderen Betriebssystem-Utilities können Sie typische I/O-Aktivitäten für das primäre Volume ermitteln.

. Wählen Sie *Fertig stellen*, um die asynchrone Spiegelsequenz abzuschließen.

.Ergebnisse
Unified Manager führt die folgenden Aktionen durch:

* Startet die erste Synchronisierung zwischen dem lokalen Speicher-Array und dem Remote-Speicher-Array.
* Legt die reservierte Kapazität für das gespiegelte Paar auf dem lokalen Speicher-Array und auf dem Remote-Speicher-Array fest.

NOTE: Wenn es sich bei dem zu spiegelnden Volume um ein Thin Volume handelt, werden während der ersten Synchronisierung nur die

```
bereitgestellten Blöcke (zugewiesene Kapazität statt gemeldete Kapazität)
auf das sekundäre Volume übertragen. Dadurch wird die Datenmenge
reduziert, die übertragen werden muss, um die erste Synchronisierung
abzuschließen.



[[ID6a5078ed1f5a2dde4fc8a30c3f1a1c75]]
= Erstellen eines synchronen gespiegelten Paares
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Zur Konfiguration der synchronen Spiegelung erstellen Sie ein gespiegeltes
Paar, das ein primäres Volume auf dem lokalen Array und ein sekundäres
Volume des Remote-Arrays umfasst.

[NOTE]
====
Diese Funktion steht nicht auf dem EF600 oder EF300-Storage-System zur
Verfügung.

====
.Bevor Sie beginnen
Bevor Sie ein gespiegeltes Paar erstellen, erfüllen Sie die folgenden
Anforderungen für Unified Manager:

* Der Web Services Proxy-Dienst muss ausgeführt werden.
* Unified Manager muss auf Ihrem lokalen Host über eine HTTPS-Verbindung
ausgeführt werden.
* Unified Manager muss gültige SSL-Zertifikate für das Speicher-Array
anzeigen. Sie können ein selbstsigniertes Zertifikat akzeptieren oder Ihr
eigenes Sicherheitszertifikat mit Unified Manager installieren und zum
Menü:Zertifikat[Zertifikatverwaltung] navigieren.


Stellen Sie außerdem sicher, dass Sie die folgenden Anforderungen an
Storage Arrays und Volumes erfüllen:

* Die beiden Storage Arrays, die Sie für die Spiegelung verwenden möchten,
werden in Unified Manager entdeckt.
* Jedes Speicher-Array muss zwei Controller haben.
* Jeder Controller im primären Array und im sekundären Array muss über
```

einen konfigurierten Ethernet-Managementport verfügen und mit dem Netzwerk verbunden sein.
* Die Speicher-Arrays verfügen über eine Firmware-Version von mindestens 7.84. (Beide können unterschiedliche OS-Versionen ausführen.)
* Sie müssen das Passwort für die lokalen und Remote-Speicher-Arrays kennen.
* Ihre lokalen und Remote-Speicher-Arrays sind über eine Fibre Channel Fabric verbunden.
* Sie haben sowohl die primären als auch die sekundären Volumes erstellt, die Sie in der Beziehung zur synchronen Spiegelung verwenden möchten.
* Das primäre Volume muss ein Standard-Volume sein. Es kann sich nicht um ein Thin-Volume oder ein Snapshot-Volume handelt.
* Das sekundäre Volume muss ein Standard-Volume sein. Es kann sich nicht um ein Thin-Volume oder ein Snapshot-Volume handelt.
* Das sekundäre Volume sollte mindestens so groß sein wie das primäre Volume.

.Über diese Aufgabe
Das Erstellen von synchronen gespiegelten Paaren ist ein mehrstufiges Verfahren.

== Schritt 1: Wählen Sie das primäre Volumen

In diesem Schritt wählen Sie das primäre Volume aus, das in der Beziehung zur synchronen Spiegelung verwendet werden soll. Wenn Sie ein primäres Volume auf dem lokalen Speicher-Array auswählen, zeigt das System eine Liste aller berechtigten Volumes für dieses gespiegelte Paar an. Alle Volumes, die nicht für die Verwendung geeignet sind, werden in dieser Liste nicht angezeigt. Das ausgewählte Volume besitzt die primäre Rolle in der Spiegelbeziehung.

.Schritte
. Wählen Sie auf der Seite *Verwalten* das lokale Speicher-Array aus, das Sie für die Quelle verwenden möchten.
. Menü wählen:Aktionen[Synchronous Mirrored Pair erstellen].
+
Der Assistent Synchronous Mirrored Pair erstellen wird geöffnet.

. Wählen Sie aus der Liste der berechtigten Volumes ein Volume aus, das Sie als primäres Volume in der Spiegelung verwenden möchten.
. Wählen Sie *Weiter* und gehen Sie zu <<Schritt 2: Wählen Sie das sekundäre Volumen>>.

```
== Schritt 2: Wählen Sie das sekundäre Volumen

In diesem Schritt wählen Sie das sekundäre Volume aus, das in der
Spiegelbeziehung verwendet werden soll. Wenn Sie ein sekundäres Volume auf
dem Remote-Speicher-Array auswählen, zeigt das System eine Liste aller
berechtigten Volumes für dieses gespiegelte Paar an. Alle Volumes, die
nicht für die Verwendung geeignet sind, werden in dieser Liste nicht
angezeigt. Das ausgewählte Volumen hält die sekundäre Rolle in der
Spiegelbeziehung.

.Schritte
. Wählen Sie das Remote Storage Array aus, auf dem Sie eine Mirror-
Beziehung zum lokalen Speicher-Array herstellen möchten.
+
[NOTE]
====
Wenn Ihr Remote-Speicher-Array passwortgeschützt ist, fordert das System
zur Eingabe eines Kennworts auf.

====
+
** Die Liste der Storage-Arrays wird nach ihrem Storage-Array-Namen
benannt. Wenn Sie kein Speicher-Array genannt haben, wird es als
„unbenannt“ aufgeführt.
** Wenn das zu verwendende Speicher-Array nicht in der Liste aufgeführt
ist, stellen Sie sicher, dass es in Unified Manager erkannt wurde.


. Wählen Sie aus der Liste der berechtigten Volumes ein Volume aus, das
Sie als sekundäres Volume in der Spiegelung verwenden möchten.
+
[NOTE]
====
Wird ein sekundäres Volume mit einer Kapazität ausgewählt, die größer als
das primäre Volume ist, so ist die nutzbare Kapazität auf die Größe des
primären Volumes beschränkt.

====
. Klicken Sie auf *Weiter* und gehen Sie zu <<Schritt 3:
Synchronisierungseinstellungen auswählen>>.




== Schritt 3: Synchronisierungseinstellungen auswählen
```

In diesem Schritt wählen Sie die Einstellungen aus, die bestimmen, wie Daten nach einer Kommunikationsunterbrechung synchronisiert werden. Sie können die Priorität festlegen, mit der der Controller-Eigentümer des primären Volumes nach einer Kommunikationsunterbrechung Daten mit dem sekundären Volume neu synchronisiert. Sie müssen außerdem die Resynchronisierung-Richtlinie entweder manuell oder automatisch auswählen.

.Schritte
. Verwenden Sie den Schieberegler, um die Synchronisationspriorität festzulegen.
+
Die Synchronisierungspriorität legt fest, wie viele der Systemressourcen verwendet werden, um die erste Synchronisierung abzuschließen und die Neusynchronisierung nach einer Kommunikationsunterbrechung im Vergleich zu Service-I/O-Anforderungen zu ermöglichen.

+
Die in diesem Dialogfeld festgelegte Priorität gilt sowohl für das primäre Volume als auch für das sekundäre Volume. Sie können die Rate für das primäre Volume zu einem späteren Zeitpunkt ändern, indem Sie zu System Manager wechseln und Menü:Storage[Synchronous Mirroring > More > Edit Settings] auswählen.

+
Es gibt fünf Prioritätsraten für die Synchronisierung:

+
** Am Niedrigsten
** Niedrig
** Mittel
** Hoch
** Höchste
+
Wenn die Synchronisierungspriorität auf die niedrigste Rate eingestellt ist, wird die I/O-Aktivität priorisiert und die Neusynchronisierung dauert länger. Wenn die Synchronisierungspriorität auf die höchste Rate festgelegt ist, wird der Neusynchronisierung nach Priorität geordnet, aber die I/O-Aktivität für das Speicher-Array ist möglicherweise betroffen.

. Wählen Sie aus, ob Sie die gespiegelten Paare auf dem Remote-Speicher-Array entweder manuell oder automatisch neu synchronisieren möchten.
+
** *Manuell* (die empfohlene Option) -- Wählen Sie diese Option aus, damit

die Synchronisierung manuell fortgesetzt werden muss, nachdem die Kommunikation auf einem gespiegelten Paar wiederhergestellt wurde. Diese Option bietet die beste Möglichkeit für die Wiederherstellung von Daten.
** *Automatisch* -- Wählen Sie diese Option, um die Neusynchronisierung automatisch zu starten, nachdem die Kommunikation auf einem gespiegelten Paar wiederhergestellt wurde.
+
Um die Synchronisierung manuell fortzusetzen, wählen Sie System Manager und Menü:Speicherung[Synchronous Mirroring], markieren Sie das gespiegelte Paar in der Tabelle, und wählen Sie unter *Mehr* *Resume*.

. Klicken Sie auf *Fertig stellen*, um die Synchronspiegelung abzuschließen.

.Ergebnisse
Wenn die Spiegelung aktiviert ist, führt das System folgende Aktionen durch:

* Startet die erste Synchronisierung zwischen dem lokalen Speicher-Array und dem Remote-Speicher-Array.
* Legt die Synchronisierungspriorität und die Resynchronisierungsrichtlinie fest.
* Behält sich den Port mit der höchsten Nummer der HIC des Controllers bei der Datenübertragung mit gespiegelten Daten vor.
+
Auf diesem Port empfangene I/O-Anfragen werden nur von dem bevorzugten Remote-Controller-Eigentümer des sekundären Volumes im gespiegelten Paar akzeptiert. (Reservierungen für das primäre Volume sind zulässig.)

* Erstellt zwei reservierte Kapazitäts-Volumes, eines für jeden Controller, die zum Protokollieren von Schreibinformationen für die Wiederherstellung nach Controller-Resets und anderen temporären Unterbrechungen verwendet werden.
+
Die Kapazität eines jeden Volumes beträgt 128 MiB. Wenn die Volumes jedoch in einen Pool aufgenommen werden, wird 4 gib für jedes Volume reserviert.

.Nachdem Sie fertig sind
Wechseln Sie zu System Manager und wählen Sie MENU:Startseite[Vorgänge in Bearbeitung anzeigen], um den Fortschritt des Synchronspiegelung-Vorgangs anzuzeigen. Dieser Vorgang kann langwierig sein und die System-Performance beeinträchtigen.

```
:leveloffset: -1


= FAQs

:leveloffset: +1


[[ID1d608a80f65b1a03aee1ba62cb64f43e]]
= Was muss ich wissen, bevor ich eine gespiegelte Konsistenzgruppe
erstellt?
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Befolgen Sie die folgenden Richtlinien, bevor Sie eine gespiegelte
Konsistenzgruppe erstellen.

Erfüllen Sie die folgenden Anforderungen für Unified Manager:

* Der Web Services Proxy-Dienst muss ausgeführt werden.
* Unified Manager muss auf Ihrem lokalen Host über eine HTTPS-Verbindung
ausgeführt werden.
* Unified Manager muss gültige SSL-Zertifikate für das Speicher-Array
anzeigen. Sie können ein selbstsigniertes Zertifikat akzeptieren oder Ihr
eigenes Sicherheitszertifikat mit Unified Manager installieren und zum
Menü:Zertifikat[Zertifikatverwaltung] navigieren.


Erfüllen Sie außerdem die folgenden Anforderungen an Storage-Arrays:

* Die beiden Storage Arrays müssen in Unified Manager erkannt werden.
* Jedes Speicher-Array muss zwei Controller haben.
* Jeder Controller im primären Array und im sekundären Array muss über
einen konfigurierten Ethernet-Managementport verfügen und mit dem Netzwerk
verbunden sein.
* Die Speicher-Arrays verfügen über eine Firmware-Version von mindestens
7.84. (Beide können unterschiedliche OS-Versionen ausführen.)
* Sie müssen das Passwort für die lokalen und Remote-Speicher-Arrays
kennen.
```

```
* Ihre lokalen und Remote-Speicher-Arrays sind über eine Fibre Channel
Fabric- oder iSCSI-Schnittstelle verbunden.


[NOTE]
====
Synchrones Spiegeln ist auf dem EF600 oder EF300 Storage-System nicht
verfügbar.

====



[[ID6db1bd821e8c5e71dd4453338008df27]]
= Was muss ich vor der Erstellung eines gespiegelten Paares wissen?
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Befolgen Sie vor dem Erstellen eines gespiegelten Paares diese
Richtlinien.

* Sie müssen über zwei Storage-Arrays verfügen.
* Jedes Speicher-Array muss zwei Controller haben.
* Die beiden Storage Arrays müssen in Unified Manager erkannt werden.
* Jeder Controller im primären Array und im sekundären Array muss über
einen konfigurierten Ethernet-Managementport verfügen und mit dem Netzwerk
verbunden sein.
* Die Speicher-Arrays verfügen über eine Firmware-Version von mindestens
7.84. (Beide können unterschiedliche OS-Versionen ausführen.)
* Sie müssen das Passwort für die lokalen und Remote-Speicher-Arrays
kennen.
* Sie benötigen genügend freie Kapazität auf dem Remote-Speicher-Array, um
ein sekundäres Volume zu erstellen, das dem primären Volume entspricht
oder dessen Größe Sie spiegeln möchten.
* Asynchrones Spiegeln wird auf Controllern mit Fibre Channel (FC)- oder
iSCSI-Host-Ports unterstützt, während synchrones Spiegeln nur auf
Controllern mit FC Host-Ports unterstützt wird.


[NOTE]
====
Synchrones Spiegeln ist auf dem EF600 oder EF300 Storage-System nicht
verfügbar.
```

```
====



[[ID2e807fc9008ed36c4c089b0ca66933bf]]
= Warum sollte ich diesen Prozentsatz ändern?
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Die reservierte Kapazität ist normalerweise 20 % des Basis-Volumes für
asynchrone Spiegelungsvorgänge. In der Regel ist diese Kapazität
ausreichend.

Die benötigte Kapazität ist abhängig von Häufigkeit und Größe der I/O-
Schreibvorgänge auf dem Basis-Volume und wie lange Sie den Kopierdienst
des Storage-Objekts verwenden möchten. Im Allgemeinen wählen Sie einen
größeren Prozentsatz für die reservierte Kapazität aus, wenn eine oder
beide Bedingungen vorhanden sind:

* Wenn sich der Kopierdienst eines bestimmten Storage-Objekts sehr lange
Lebensdauer hat.
* Wenn sich ein großer Prozentsatz an Datenblöcken auf dem Basis-Volume
aufgrund von hoher I/O-Aktivität ändert. Mithilfe von historischen
Performance-Daten oder anderen Betriebssystem-Dienstprogrammen können Sie
die typischen I/O-Aktivitäten für das Basis-Volume ermitteln.




[[IDd2f630c1981f8cc5be44b58a8fe49428]]
= Warum kann ich mehr als einen Kandidaten für reservierte Kapazität
sehen?
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Wenn sich mehrere Volumes in einem Pool oder einer Volume-Gruppe befinden,
die dem für das Storage-Objekt ausgewählten Kapazitätsprozentsatz
entsprechen, werden mehrere Kandidaten angezeigt.
```

```
Sie können die Liste der empfohlenen Kandidaten aktualisieren, indem Sie
den Prozentsatz des physischen Speicherplatzes ändern, den Sie im Basis-
Volume für Kopierdienste reservieren möchten. Die besten Kandidaten werden
basierend auf Ihrer Auswahl angezeigt.



[[ID9bd5b63c6e88f6abcbf81c577d1eb6d6]]
= Warum sehe ich nicht alle meine Bände?
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Wenn Sie ein primäres Volume für ein gespiegeltes Paar auswählen, werden
in einer Liste alle berechtigten Volumes angezeigt.

Alle Volumes, die nicht für die Verwendung geeignet sind, werden in dieser
Liste nicht angezeigt. Volumes sind aus folgenden Gründen möglicherweise
nicht verfügbar:

* Die Lautstärke ist nicht optimal.
* Das Volume beteiligt sich bereits an einer Spiegelbeziehung.
* Für das synchrone Spiegeln müssen primäre und sekundäre Volumes eines
gespiegelten Paars Standard-Volumes sein. Es können keine dünnen Volumes
oder Snapshot Volumes sein.
* Bei der asynchronen Spiegelung müssen Thin Volumes die automatische
Erweiterung aktiviert haben.



NOTE: Bei EF600- und EF300-Controllern müssen die primären und sekundären
Volumes eines asynchronen gespiegelten Paares dasselbe Protokoll, Tray-
Level, Segmentgröße, Sicherheitstyp und RAID-Level erfüllen. Nicht
geeignete asynchrone gespiegelte Paare werden nicht in der Liste der
verfügbaren Volumes angezeigt.



[[IDbdfe32d918941b147d8f4861a266b9c3]]
= Warum sehe ich nicht alle Volumes auf dem Remote-Speicher-Array?
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
```

```
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Wenn Sie ein sekundäres Volume auf dem Remote-Speicher-Array auswählen,
werden alle für dieses gespiegelte Paar geeigneten Volumes in einer Liste
angezeigt.

Alle Volumes, die nicht für die Verwendung geeignet sind, werden in dieser
Liste nicht angezeigt. Die Volumes können aus den folgenden Gründen nicht
berechtigt sein:

* Das Volume ist ein nicht standardmäßiges Volume, wie z. B. ein Snapshot-
Volume.
* Die Lautstärke ist nicht optimal.
* Das Volume beteiligt sich bereits an einer Spiegelbeziehung.
* Bei der asynchronen Spiegelung stimmen die Thin Volume-Attribute des
primären Volumes und des sekundären Volumes nicht überein.
* Wenn Sie Data Assurance (da) verwenden, müssen das primäre Volume und
das sekundäre Volume über dieselben da-Einstellungen verfügen.
+
** Wenn das primäre Volume mit da aktiviert ist, muss das sekundäre Volume
mit da aktiviert sein.
** Wenn das primäre Volume nicht da aktiviert ist, darf das sekundäre
Volume nicht als da-aktiviert verwendet werden.


* Beim asynchronen Spiegeln müssen das primäre Volume und das sekundäre
Volume dieselben Laufwerksicherheitsfunktionen aufweisen.
+
** Wenn das primäre Volume FIPS-fähig ist, muss das sekundäre Volume FIPS-
fähig sein.
** Wenn das primäre Volume FDE-fähig ist, muss das sekundäre Volume FDE-
fähig sein.
** Wenn das primäre Volume keine Laufwerkssicherheit verwendet, darf das
sekundäre Volume keine Laufwerkssicherheit verwenden.




[[ID43d0e086d99e419ebd82de3bf3ef1267]]
= Welche Auswirkungen hat die Synchronisierungspriorität auf die
Synchronisierungsraten?
:allow-uri-read:
:icons: font
```

```
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Die Synchronisierungspriorität definiert, wie viel Verarbeitungszeit für
Synchronisierungsaktivitäten im Verhältnis zur Systemleistung zugewiesen
wird.

Der Controller-Eigentümer des primären Volume führt diesen Vorgang im
Hintergrund durch. Gleichzeitig verarbeitet der Controller-Inhaber lokale
I/O-Schreibvorgänge auf das primäre Volume und verbundene Remote-
Schreibvorgänge auf das sekundäre Volume. Da durch die Resynchronisierung
der Controller-Verarbeitungsressourcen von der I/O-Aktivität umgeleitet
werden, kann eine Neusynchronisierung die Performance der Host-Applikation
nach sich ziehen.

Beachten Sie diese Richtlinien, um zu ermitteln, wie lange eine
Synchronisierungspriorität dauern könnte und wie sich die
Synchronisierungsprioritäten auf die Systemleistung auswirken können.

Diese Prioritätsraten sind verfügbar:

* Am Niedrigsten
* Niedrig
* Mittel
* Hoch
* Höchste


Die niedrigste Prioritätsrate unterstützt die System-Performance, die
Neusynchronisierung dauert jedoch länger. Die höchste Prioritätsrate
unterstützt eine Neusynchronisierung, aber die System-Performance ist
möglicherweise beeinträchtigt.

Diese Leitlinien entsprechen ungefähr den Unterschieden zwischen den
Prioritäten.

[cols="45h,~"]
|===
| Prioritätsrate für vollständige Synchronisierung | Verstrichene Zeit im
Vergleich zur höchsten Synchronisationsrate


 a|
Am Niedrigsten
 a|
```

```
Etwa achtmal so lange wie bei der höchsten Prioritätsrate.



 a|
Niedrig
 a|
Etwa sechsmal so lange wie bei der höchsten Prioritätsrate.



 a|
Mittel
 a|
Etwa dreieinhalb Mal so lang wie bei der höchsten Prioritätsrate.



 a|
Hoch
 a|
Etwa doppelt so lange wie bei der höchsten Prioritätsrate.

|===
Volume-Größe und Host-I/O-Rate-Lasten wirken sich auf den Vergleich der
Synchronisierungszeit aus.



[[ID94cb14d5c5fd0d4a1fcb9964a641f4b1]]
= Warum wird empfohlen, eine manuelle Synchronisierungsrichtlinie zu
verwenden?
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Die manuelle Neusynchronisierung wird empfohlen, da Sie damit den
Neusynchronisierung so verwalten können, dass dadurch keine Möglichkeit
zum Wiederherstellen von Daten besteht.

Wenn Sie eine automatische Resynchronisierung verwenden und während der
Neusynchronisierung intermittierende Kommunikationsprobleme auftreten,
können die Daten auf dem sekundären Volume vorübergehend beschädigt
werden. Nach Abschluss der Resynchronisierung werden die Daten korrigiert.
```

```
:leveloffset: -1


:leveloffset: -1


= Zertifikate

:leveloffset: +1


[[ID2201d72871fc4652a44cec6ecbbcee66]]
= Zertifikatübersicht
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Mit der Zertifikatverwaltung können Sie Zertifikatsignierungsanforderungen
(CSRs) erstellen, Zertifikate importieren und vorhandene Zertifikate
verwalten.



== Was sind Zertifikate?

_Zertifikate_ sind digitale Dateien, die Online-Einheiten wie Websites und
Server für eine sichere Kommunikation im Internet identifizieren. Es gibt
zwei Arten von Zertifikaten: Ein _signiertes Zertifikat_ wird von einer
Zertifizierungsstelle (CA) validiert und ein _selbst-signiertes
Zertifikat_ wird vom Eigentümer des Unternehmens anstelle eines Dritten
validiert.

Weitere Informationen:

* xref:{relative_path}how-certificates-work-unified.html["Funktionsweise
von Zertifikaten"]
* xref:{relative_path}certificate-terminology-unified.html["Terminologie
des Zertifikats"]
```

```
== Wie konfiguriere ich Zertifikate?

In der Zertifikatverwaltung können Sie Zertifikate für die Management
Station konfigurieren, die Unified Manager hostet, und auch Zertifikate
für die Controller in den Arrays importieren.

Weitere Informationen:

* xref:{relative_path}use-ca-signed-certificate-um.html["Verwenden Sie CA-
signierte Zertifikate für das Managementsystem"]
* xref:{relative_path}import-array-certificates-unified.html["Importieren
Sie Zertifikate für Arrays"]




= Konzepte

:leveloffset: +1


[[IDf878763f9db2768aa1156e834a6959a9]]
= Funktionsweise von Zertifikaten
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Zertifikate sind digitale Dateien, die Online-Einheiten wie Websites und
Server für eine sichere Kommunikation im Internet identifizieren.



== Signierte Zertifikate

Zertifikate stellen sicher, dass die Webkommunikation in verschlüsselter
Form, privat und unverändert, nur zwischen dem angegebenen Server und dem
angegebenen Client übertragen wird. Mit Unified Manager können Sie
Zertifikate für den Browser auf einem Host-Managementsystem und die
Controller in den ermittelten Speicher-Arrays verwalten.

Ein Zertifikat kann von einer vertrauenswürdigen Behörde signiert werden,
oder es kann selbst signiert werden. „Unterzeichnen“ bedeutet einfach,
dass jemand die Identität des Eigentümers validiert und festgestellt hat,
```

dass seine Geräte vertrauenswürdig sind. Die Storage Arrays werden mit einem automatisch generierten, selbstsignierten Zertifikat auf jedem Controller ausgeliefert. Sie können weiterhin die selbst signierten Zertifikate verwenden oder CA-signierte Zertifikate für eine sicherere Verbindung zwischen den Controllern und den Host-Systemen erhalten.

[NOTE]
====
Auch wenn CA-signierte Zertifikate einen besseren Schutz bieten (zum Beispiel die Verhinderung von man-in-the-Middle-Angriffen), verlangen sie auch Gebühren, die teuer sein können, wenn Sie ein großes Netzwerk haben. Im Gegensatz dazu sind selbstsignierte Zertifikate weniger sicher, aber sie sind kostenlos. Daher werden selbst signierte Zertifikate am häufigsten für interne Testumgebungen eingesetzt, nicht in Produktionsumgebungen.

====
Ein signiertes Zertifikat wird von einer Zertifizierungsstelle (CA) validiert, einer vertrauenswürdigen Drittorganisation. Signierte Zertifikate enthalten Angaben über den Eigentümer der Einheit (in der Regel Server oder Website), Datum der Zertifikatausgabe und -Ablauf, gültige Domains für das Unternehmen und eine digitale Signatur bestehend aus Buchstaben und Zahlen.

Wenn Sie einen Browser öffnen und eine Webadresse eingeben, führt Ihr System eine Zertifikatprüfung im Hintergrund durch, um zu bestimmen, ob Sie eine Verbindung zu einer Website herstellen, die ein gültiges, von einer Zertifizierungsstelle signiertes Zertifikat enthält. In der Regel enthält eine mit einem signierten Zertifikat gesicherte Website ein Vorhängeschloss-Symbol und eine https-Bezeichnung in der Adresse. Wenn Sie versuchen, eine Verbindung zu einer Website herzustellen, die kein CA-signiertes Zertifikat enthält, zeigt Ihr Browser eine Warnung an, dass die Website nicht sicher ist.

Die CA führt Schritte durch, um Ihre Identität während des Anwendungsprozesses zu überprüfen. Sie senden möglicherweise eine E-Mail an Ihr registriertes Unternehmen, überprüfen Ihre Geschäftsadresse und führen eine HTTP- oder DNS-Verifizierung durch. Wenn der Anwendungsprozess abgeschlossen ist, sendet die Zertifizierungsstelle digitale Dateien zum Laden auf einem Host-Managementsystem. In der Regel umfassen diese Dateien eine Kette des Vertrauens, wie folgt:

* *Root* -- an der Spitze der Hierarchie befindet sich das Stammzertifikat, welches einen privaten Schlüssel enthält, der zum Signieren anderer Zertifikate verwendet wird. Das Root identifiziert eine bestimmte CA-Organisation. Wenn Sie dieselbe Zertifizierungsstelle für

alle Netzwerkgeräte verwenden, benötigen Sie nur ein Stammzertifikat.
* *Intermediate* -- Abzweigung von der Wurzel sind die Zwischenzertifikate. Die CA gibt ein oder mehrere Zwischenzertifikate aus, die als Zwischenzertifikate zwischen geschützten Root- und Serverzertifikaten fungieren sollen.
* *Server* -- unten in der Kette befindet sich das Server-Zertifikat, welches Ihre spezifische Entität, wie z.B. eine Website oder ein anderes Gerät, identifiziert. Jeder Controller in einem Storage Array benötigt ein separates Serverzertifikat.

== Selbstsignierte Zertifikate

Jeder Controller im Speicher-Array verfügt über ein vorinstalliertes, selbstsigniertes Zertifikat. Ein selbst signiertes Zertifikat ähnelt einem CA-signierten Zertifikat, außer dass es vom Eigentümer des Unternehmens anstelle eines Dritten validiert wird. Wie ein Zertifikat mit einer Zertifizierungsstelle enthält auch ein selbstsigniertes Zertifikat einen eigenen privaten Schlüssel und stellt sicher, dass Daten verschlüsselt und über eine HTTPS-Verbindung zwischen einem Server und einem Client gesendet werden.

Selbstsignierte Zertifikate werden von Browsern nicht „`Trusted`". Jedes Mal, wenn Sie versuchen, eine Verbindung zu einer Website herzustellen, die nur ein selbstsigniertes Zertifikat enthält, wird im Browser eine Warnmeldung angezeigt. Sie müssen in der Warnmeldung auf einen Link klicken, der Ihnen die Nutzung der Website ermöglicht. Dadurch akzeptieren Sie im Wesentlichen das selbstsignierte Zertifikat.

== Zertifikate für Unified Manager

Die Unified Manager-Schnittstelle wird mit dem Web Services Proxy auf einem Host-System installiert. Wenn Sie einen Browser öffnen und eine Verbindung zu Unified Manager herstellen möchten, versucht der Browser, durch die Suche nach einem digitalen Zertifikat zu überprüfen, ob der Host eine vertrauenswürdige Quelle ist. Wenn der Browser kein von einer Zertifizierungsstelle signiertes Zertifikat für den Server findet, wird eine Warnmeldung angezeigt. Von dort aus können Sie auf der Website fortfahren, um das selbstsignierte Zertifikat für diese Sitzung zu akzeptieren. Oder Sie können signierte digitale Zertifikate von einer Zertifizierungsstelle erhalten, damit die Warnmeldung nicht mehr angezeigt wird.

```
== Zertifikate für Controller

Während einer Unified Manager-Sitzung werden möglicherweise zusätzliche
Sicherheitsmeldungen angezeigt, wenn Sie versuchen, auf einen Controller
zuzugreifen, der kein von einer Zertifizierungsstelle signiertes
Zertifikat hat. In diesem Fall können Sie dem selbst signierten Zertifikat
dauerhaft vertrauen oder die CA-signierten Zertifikate für die Controller
importieren, damit der Web Services Proxy-Server eingehende
Clientanforderungen von diesen Controllern authentifizieren kann.



[[ID9b70aa5ace8e5f25563b06a26ef5e30a]]
= Terminologie des Zertifikats
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Die folgenden Begriffe gelten für das Zertifikatmanagement.

[cols="25h,~"]
|===
| Laufzeit | Beschreibung


 a|
CA
 a|
Eine Zertifizierungsstelle (CA) ist eine vertrauenswürdige Einheit, die
elektronische Dokumente, sogenannte digitale Zertifikate, für Internet-
Sicherheit ausstellt. Diese Zertifikate identifizieren Website-Besitzer,
die sichere Verbindungen zwischen Clients und Servern ermöglichen.



 a|
CSR
 a|
Eine Zertifikatsignierungsanforderung (CSR) ist eine Nachricht, die von
einem Antragsteller an eine Zertifizierungsstelle (CA) gesendet wird. Der
CSR überprüft die Informationen, die die Zertifizierungsstelle zum
ausstellen eines Zertifikats benötigt.
```

a|
Zertifikat
a|
Ein Zertifikat identifiziert den Eigentümer einer Website aus Sicherheitsgründen, wodurch Angreifer die Identität der Website nicht mehr verkörpern können. Das Zertifikat enthält Informationen über den Websiteeigentümer und die Identität des vertrauenswürdigen Unternehmens, der diese Informationen bescheinigt (unterzeichnet).

a|
Zertifikatskette
a|
Eine Dateihierarchie, die den Zertifikaten eine Sicherheitsschicht hinzufügt. In der Regel umfasst die Kette ein Stammzertifikat oben in der Hierarchie, ein oder mehrere Zwischenzertifikate und die Serverzertifikate, die die Entitäten identifizieren.

a|
Zwischenzertifikat
a|
Ein oder mehrere Zwischenzertifikate verzweigen von der Root in der Zertifikatkette. Die CA gibt ein oder mehrere Zwischenzertifikate aus, die als Zwischenzertifikate zwischen geschützten Root- und Serverzertifikaten fungieren sollen.

a|
Schlüsselspeicher
a|
Ein Schlüsselspeicher ist ein Repository auf Ihrem Host-Managementsystem, das private Schlüssel enthält, zusammen mit ihren entsprechenden öffentlichen Schlüsseln und Zertifikaten. Diese Schlüssel und Zertifikate identifizieren Ihre eigenen Einheiten, z. B. die Controller.

a|
Stammzertifikat
a|

Das Stammzertifikat befindet sich oben in der Hierarchie in der Zertifikatskette und enthält einen privaten Schlüssel, der zum Signieren anderer Zertifikate verwendet wird. Das Root identifiziert eine bestimmte CA-Organisation. Wenn Sie dieselbe Zertifizierungsstelle für alle Netzwerkgeräte verwenden, benötigen Sie nur ein Stammzertifikat.

a|
Signiertes Zertifikat
a|
Ein Zertifikat, das von einer Zertifizierungsstelle (CA) validiert wird. Diese Datendatei enthält einen privaten Schlüssel und stellt sicher, dass Daten verschlüsselt zwischen einem Server und einem Client über eine HTTPS-Verbindung gesendet werden. Darüber hinaus enthält ein signiertes Zertifikat Details über den Eigentümer des Unternehmens (in der Regel ein Server oder eine Website) und eine digitale Signatur bestehend aus Buchstaben und Zahlen. Ein signiertes Zertifikat nutzt eine Vertrauenskette und wird daher am häufigsten in Produktionsumgebungen verwendet. Auch als „CA-signiertes Zertifikat" oder als „Managementzertifikat" bezeichnet.

a|
Selbstsigniertes Zertifikat
a|
Ein selbstsigniertes Zertifikat wird vom Eigentümer des Unternehmens validiert. Diese Datendatei enthält einen privaten Schlüssel und stellt sicher, dass Daten verschlüsselt zwischen einem Server und einem Client über eine HTTPS-Verbindung gesendet werden. Es enthält auch eine digitale Signatur, die aus Buchstaben und Zahlen besteht. Ein selbstsigniertes Zertifikat verwendet nicht dieselbe Vertrauenskette wie ein CA-signiertes Zertifikat und wird daher am häufigsten in Testumgebungen eingesetzt. Auch als vorinstalliertes Zertifikat bezeichnet.

a|
Serverzertifikat
a|
Das Server-Zertifikat befindet sich unten in der Zertifikatskette. Es identifiziert Ihre spezifische Einheit, z. B. eine Website oder ein anderes Gerät. Jeder Controller in einem Storage-System benötigt ein separates Serverzertifikat.

```
 a|
Treuhandgeschäft
 a|
Ein Truststore ist ein Repository, das Zertifikate von vertrauenswürdigen
Drittanbietern, wie z. B. CAS, enthält.

|===



:leveloffset: -1


[[ID3a9ca7dd8249ce76453fc64aa258f5a7]]
= Verwenden Sie CA-signierte Zertifikate für das Managementsystem
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Sie können CA-signierte Zertifikate für sicheren Zugriff auf das
Managementsystem, das SANtricity Unified Manager hostet, erhalten und
importieren.

.Bevor Sie beginnen
Sie müssen mit einem Benutzerprofil angemeldet sein, das
Sicherheitsadministratorberechtigungen enthält. Andernfalls werden keine
Zertifikatfunktionen angezeigt.

.Über diese Aufgabe
Die Verwendung von CA-signierten Zertifikaten ist ein dreistufiges
Verfahren.



== Schritt 1: Eine CSR-Datei ausfüllen

Sie müssen zuerst eine CSR-Datei (Certificate Signing Request) generieren,
die Ihre Organisation und das Host-System identifiziert, auf dem der Web
Services Proxy und Unified Manager installiert sind.

[NOTE]
====
```

```
Alternativ können Sie eine CSR-Datei mit einem Tool wie OpenSSL generieren
und zu überspringen <<Schritt 2: CSR-Datei senden>>.

====
.Schritte
. Wählen Sie *Zertifikatverwaltung*.
. Wählen Sie auf der Registerkarte Verwaltung die Option *CSR abschließen*
aus.
. Geben Sie die folgenden Informationen ein, und klicken Sie dann auf
*Weiter*:
+
** *Organisation* -- der vollständige, rechtliche Name Ihres Unternehmens
oder Ihrer Organisation. Fügen Sie Suffixe wie Inc. Oder Corp. Mit ein
** *Organisationseinheit (optional)* -- die Abteilung Ihrer Organisation,
die das Zertifikat bearbeitet.
** *Stadt/Ort* -- die Stadt, in der sich Ihr Hostsystem oder Ihr Geschäft
befindet.
** *Bundesland/Region (optional)* -- der Staat oder die Region, in der
sich Ihr Hostsystem oder Ihr Geschäft befindet.
** *Land ISO Code* -- der zweistellige ISO-Code Ihres Landes
(International Organization for Standardization), wie z. B. die USA.


. Geben Sie die folgenden Informationen über das Hostsystem ein, auf dem
der Web Services Proxy installiert ist:
+
** *Allgemeiner Name* -- die IP-Adresse oder der DNS-Name des Hostsystems,
auf dem der Web Services Proxy installiert ist. Stellen Sie sicher, dass
diese Adresse korrekt ist, sie muss mit den Angaben übereinstimmen, die
Sie für den Zugriff auf Unified Manager im Browser eingeben. Verwenden Sie
kein http:// oder https://. Der DNS-Name kann nicht mit einem Platzhalter
beginnen.
** *Alternative IP-Adressen* -- Wenn der allgemeine Name eine IP-Adresse
ist, können Sie optional weitere IP-Adressen oder Aliase für das Host-
System eingeben. Verwenden Sie für mehrere Einträge ein kommagetrenntes
Format.
** *Alternative DNS-Namen* -- Wenn der gemeinsame Name ein DNS-Name ist,
geben Sie weitere DNS-Namen für das Host-System ein. Verwenden Sie für
mehrere Einträge ein kommagetrenntes Format. Falls es keine alternativen
DNS-Namen gibt, aber Sie im ersten Feld einen DNS-Namen eingegeben haben,
kopieren Sie diesen Namen hier. Der DNS-Name kann nicht mit einem
Platzhalter beginnen.


. Stellen Sie sicher, dass die Host-Informationen richtig sind. Wenn dies
nicht der Fall ist, schlagen die von der Zertifizierungsstelle
```

zurückgegebenen Zertifikate fehl, wenn Sie versuchen, sie zu importieren.
. Klicken Sie Auf *Fertig Stellen*.
. Gehen Sie zu <<Schritt 2: CSR-Datei senden>>.

== Schritt 2: CSR-Datei senden

Nachdem Sie eine CSR-Datei (Certificate Signing Request) erstellt haben, senden Sie sie an eine Certificate Authority (CA), um signierte Managementzertifikate für das System zu erhalten, das Unified Manager und den Web Services Proxy hostet.

NOTE: Systeme der E-Series erfordern ein PEM-Format (Base64 ASCII-Kodierung) für signierte Zertifikate, das die folgenden Dateitypen umfasst: .Pem, .crt, .cer oder .key.

.Schritte
. Suchen Sie die heruntergeladene CSR-Datei.
+
Der Speicherort des Downloads hängt von Ihrem Browser ab.

. Senden Sie die CSR-Datei an eine CA (z. B. Verisign oder DigiCert), und fordern Sie signierte Zertifikate im PEM-Format an.
+
[CAUTION]
====
Nachdem Sie eine CSR-Datei an die CA gesendet haben, generieren SIE keine andere CSR-Datei. Wenn Sie eine CSR generieren, erstellt das System ein privates und öffentliches Schlüsselpaar. Der öffentliche Schlüssel ist Teil der CSR, während der private Schlüssel im Schlüsselspeicher des Systems aufbewahrt wird. Wenn Sie die signierten Zertifikate erhalten und importieren, stellt das System sicher, dass sowohl der private als auch der öffentliche Schlüssel das ursprüngliche Paar sind. Wenn die Schlüssel nicht übereinstimmen, funktionieren die signierten Zertifikate nicht und Sie müssen neue Zertifikate von der CA anfordern.

====
. Wenn die Zertifizierungsstelle die signierten Zertifikate zurückgibt, gehen Sie zu <<Schritt 3: Import Management Zertifikate>>.

== Schritt 3: Import Management Zertifikate

Nachdem Sie von der Zertifizierungsstelle (CA) signierte Zertifikate erhalten haben, importieren Sie die Zertifikate in das Host-System, auf dem die Web Services Proxy- und Unified Manager-Schnittstelle installiert sind.

.Bevor Sie beginnen
* Sie haben von der Zertifizierungsstelle signierte Zertifikate erhalten. Diese Dateien umfassen das Stammzertifikat, ein oder mehrere Zwischenzertifikate und das Serverzertifikat.
* Wenn die CA eine verkettete Zertifikatdatei (z. B. eine .p7b-Datei) lieferte, müssen Sie die verkettete Datei in einzelne Dateien entpacken: Das Stammzertifikat, ein oder mehrere Zwischenzertifikate und das Serverzertifikat. Sie können die Windows verwenden `certmgr` Dienstprogramm zum Auspacken der Dateien (Rechtsklick und wählen Sie Menü:Alle Aufgaben[Export]). Base-64-Kodierung wird empfohlen. Wenn die Exporte abgeschlossen sind, wird für jede Zertifikatdatei in der Kette eine CER-Datei angezeigt.
* Sie haben die Zertifikatdateien auf das Hostsystem kopiert, auf dem der Web Services Proxy ausgeführt wird.

.Schritte
. Wählen Sie *Zertifikatverwaltung*.
. Wählen Sie auf der Registerkarte Verwaltung die Option *Import*.
+
Es wird ein Dialogfeld zum Importieren der Zertifikatdateien geöffnet.

. Klicken Sie auf *Durchsuchen*, um zuerst die Stamm- und Zwischenzertifikatdateien auszuwählen und dann das Serverzertifikat auszuwählen. Wenn Sie die CSR aus einem externen Tool generiert haben, müssen Sie auch die private Schlüsseldatei importieren, die zusammen mit der CSR erstellt wurde.
+
Die Dateinamen werden im Dialogfeld angezeigt.

. Klicken Sie Auf *Import*.

.Ergebnisse
Die Dateien werden hochgeladen und validiert. Die Zertifikatinformationen werden auf der Seite Zertifikatverwaltung angezeigt.

[[ID22612cf946787e47ca4f6aa1b4b9b0e8]]
= Managementzertifikate zurücksetzen

```
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Sie können das Managementzertifikat in den ursprünglichen, werkseitig
selbstsignierten Status zurücksetzen.

.Bevor Sie beginnen
Sie müssen mit einem Benutzerprofil angemeldet sein, das
Sicherheitsadministratorberechtigungen enthält. Andernfalls werden keine
Zertifikatfunktionen angezeigt.

.Über diese Aufgabe
Diese Aufgabe löscht das aktuelle Managementzertifikat vom Host-System,
auf dem Web Services Proxy und Unified Manager installiert sind. Nach dem
Zurücksetzen des Zertifikats wird das Host-System auf das selbstsignierte
Zertifikat zurückgesetzt.

.Schritte
. Wählen Sie *Einstellungen > Zertifikate*.
. Wählen Sie die Registerkarte *Array Management* und dann *Reset*.
+
Das Dialogfeld „Zertifikat zurücksetzen bestätigen“ wird geöffnet.

. Typ `reset` Klicken Sie im Feld auf *Zurücksetzen*.
+
Nach der Aktualisierung Ihres Browsers kann der Browser den Zugriff auf
die Zielseite blockieren und melden, dass die Website HTTP Strict
Transport Security verwendet. Diese Bedingung tritt auf, wenn Sie wieder
auf selbstsignierte Zertifikate wechseln. Um die Bedingung zu löschen, die
den Zugriff auf das Ziel blockiert, müssen Sie die Browserdaten aus dem
Browser löschen.



.Ergebnisse
Das System setzt auf die Verwendung des selbstsignierten Zertifikats des
Servers zurück. Das System fordert Benutzer daher auf, das selbstsignierte
Zertifikat für ihre Sitzungen manuell anzunehmen.



= Verwenden Sie Array-Zertifikate
```

```
:leveloffset: +1


[[ID4aa5fe86142c54dda24f8f742688ec01]]
= Importieren Sie Zertifikate für Arrays
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Bei Bedarf können Zertifikate für die Speicher-Arrays importiert werden,
sodass sie sich mit dem System authentifizieren können, das SANtricity
Unified Manager hostet. Zertifikate können von einer Zertifizierungsstelle
(CA) signiert oder selbst signiert werden.

.Bevor Sie beginnen
* Sie müssen mit einem Benutzerprofil angemeldet sein, das
Sicherheitsadministratorberechtigungen enthält. Andernfalls werden keine
Zertifikatfunktionen angezeigt.
* Wenn Sie vertrauenswürdige Zertifikate importieren, müssen die
Zertifikate für die Speicher-Array-Controller mit System Manager
importiert werden.


.Schritte
. Wählen Sie *Zertifikatverwaltung*.
. Wählen Sie die Registerkarte * Trusted* aus.
+
Auf dieser Seite werden alle Zertifikate angezeigt, die für die Speicher-
Arrays gemeldet wurden.

. Wählen Sie entweder Menü:Import[Certificates], um ein CA-Zertifikat oder
Menü zu importieren:Importieren[Self-signierte Speicher-Array-
Zertifikate], um ein selbstsigniertes Zertifikat zu importieren.
+
Um die Ansicht einzuschränken, können Sie das Filterfeld *Zertifikate
anzeigen verwenden, das...* ist, oder Sie können die Zertifikatzeilen
sortieren, indem Sie auf eine der Spaltenüberschrift klicken.

. Wählen Sie im Dialogfeld das Zertifikat aus und klicken Sie dann auf
*Import*.
+
Das Zertifikat wird hochgeladen und validiert.
```

```
[[IDf0d7a9aee79c41ab8e8ab6c5265fe904]]
= Vertrauenswürdige Zertifikate löschen
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Sie können ein oder mehrere nicht mehr benötigte Zertifikate löschen, z.
B. ein abgelaufenes Zertifikat.

.Bevor Sie beginnen
Importieren Sie das neue Zertifikat, bevor Sie das alte löschen.

[CAUTION]
====
Beachten Sie, dass das Löschen eines Root- oder Zwischenzertifikats
mehrere Speicher-Arrays beeinflussen kann, da diese Arrays dieselben
Zertifikatdateien gemeinsam nutzen können.

====
.Schritte
. Wählen Sie *Zertifikatverwaltung*.
. Wählen Sie die Registerkarte * Trusted* aus.
. Wählen Sie ein oder mehrere Zertifikate in der Tabelle aus, und klicken
Sie dann auf *Löschen*.
+
[NOTE]
====
Die Funktion *Löschen* steht für vorinstallierte Zertifikate nicht zur
Verfügung.

====
+
Das Dialogfeld Vertrauenswürdiges Zertifikat bestätigen wird geöffnet.

. Bestätigen Sie den Löschvorgang, und klicken Sie dann auf *Löschen*.
+
Das Zertifikat wird aus der Tabelle entfernt.
```

```
[[ID3331e221ac6d4e532b3960ced8646491]]
= Lösen Sie nicht vertrauenswürdige Zertifikate
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Nicht vertrauenswürdige Zertifikate treten auf, wenn ein Speicher-Array
versucht, eine sichere Verbindung zu SANtricity Unified Manager
herzustellen, die Verbindung jedoch nicht als sicher bestätigt.

Auf der Zertifikatsseite können Sie nicht vertrauenswürdige Zertifikate
auflösen, indem Sie ein selbstsigniertes Zertifikat aus dem Speicher-Array
importieren oder ein Zertifikat der Zertifizierungsstelle importieren, das
von einem vertrauenswürdigen Dritten ausgestellt wurde.

.Bevor Sie beginnen
* Sie müssen mit einem Benutzerprofil angemeldet sein, das die
Berechtigungen für den Sicherheitsadministrator enthält.
* Wenn Sie ein von einer Zertifizierungsstelle signiertes Zertifikat
importieren möchten:
+
** Sie haben für jeden Controller im Speicher-Array eine
Zertifikatsignierungsanforderung (.CSR-Datei) generiert und an die CA
gesendet.
** Die CA hat vertrauenswürdige Zertifikatdateien zurückgegeben.
** Die Zertifikatdateien sind auf Ihrem lokalen System verfügbar.




.Über diese Aufgabe
Möglicherweise müssen Sie zusätzliche vertrauenswürdige CA-Zertifikate
installieren, wenn eine der folgenden Optionen zutrifft:

* Sie haben kürzlich ein Speicher-Array hinzugefügt.
* Ein oder beide Zertifikate sind abgelaufen.
* Ein oder beide Zertifikate werden widerrufen.
* Ein oder beide Zertifikate fehlen ein Stammzertifikat oder ein
Zwischenzertifikat.
```

.Schritte
. Wählen Sie *Zertifikatverwaltung*.
. Wählen Sie die Registerkarte * Trusted* aus.
+
Auf dieser Seite werden alle Zertifikate angezeigt, die für die Speicher-Arrays gemeldet wurden.

. Wählen Sie entweder Menü:Import[Certificates], um ein CA-Zertifikat oder Menü zu importieren:Importieren[Self-signierte Speicher-Array-Zertifikate], um ein selbstsigniertes Zertifikat zu importieren.
+
Um die Ansicht einzuschränken, können Sie das Filterfeld *Zertifikate anzeigen verwenden, das...* ist, oder Sie können die Zertifikatzeilen sortieren, indem Sie auf eine der Spaltenüberschrift klicken.

. Wählen Sie im Dialogfeld das Zertifikat aus und klicken Sie dann auf *Import*.
+
Das Zertifikat wird hochgeladen und validiert.

:leveloffset: -1

= Verwalten von Zertifikaten

:leveloffset: +1

[[ID4d44375361ba1edb904fd90b23f7132f]]
= Anzeigen von Zertifikaten
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
Sie können zusammenfassende Informationen für ein Zertifikat anzeigen, das die Organisation, die das Zertifikat verwendet, die Behörde, die das Zertifikat ausgestellt hat, den Gültigkeitszeitraum und die Fingerabdrücke (eindeutige Kennungen) umfasst.

.Bevor Sie beginnen

Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden keine Zertifikatfunktionen angezeigt.

.Schritte
. Wählen Sie *Zertifikatverwaltung*.
. Wählen Sie eine der folgenden Registerkarten aus:
+
** *Management* -- zeigt das Zertifikat für das System, das den Web Services Proxy hostet. Ein Managementzertifikat kann von einer Zertifizierungsstelle (CA) selbst signiert oder genehmigt werden. Die Lösung ermöglicht den sicheren Zugriff auf Unified Manager.
** *Trusted* -- zeigt Zertifikate an, auf die Unified Manager für Speicher-Arrays und andere Remote-Server, z. B. einen LDAP-Server, zugreifen kann. Die Zertifikate können von einer Zertifizierungsstelle (CA) ausgestellt oder selbst signiert werden.

. Um weitere Informationen zu einem Zertifikat anzuzeigen, wählen Sie seine Zeile aus, wählen Sie die Ellipsen am Zeilenende aus und klicken Sie dann auf *Ansicht* oder *Export*.

[[ID678c5180463392a8dd5b85ca85c426a9]]
= Exportieren von Zertifikaten
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
Sie können ein Zertifikat exportieren, um die vollständigen Details anzuzeigen.

.Bevor Sie beginnen
Um die exportierte Datei zu öffnen, müssen Sie über eine Zertifikatanzeige-Anwendung verfügen.

.Schritte
. Wählen Sie *Zertifikatverwaltung*.
. Wählen Sie eine der folgenden Registerkarten aus:
+
** *Management* -- zeigt das Zertifikat für das System, das den Web Services Proxy hostet. Ein Managementzertifikat kann von einer

```
Zertifizierungsstelle (CA) selbst signiert oder genehmigt werden. Die
Lösung ermöglicht den sicheren Zugriff auf Unified Manager.
** *Trusted* -- zeigt Zertifikate an, auf die Unified Manager für
Speicher-Arrays und andere Remote-Server, z. B. einen LDAP-Server,
zugreifen kann. Die Zertifikate können von einer Zertifizierungsstelle
(CA) ausgestellt oder selbst signiert werden.


. Wählen Sie auf der Seite ein Zertifikat aus, und klicken Sie dann am
Ende der Zeile auf die Ellipsen.
. Klicken Sie auf *Exportieren* und speichern Sie dann die
Zertifikatdatei.
. Öffnen Sie die Datei in Ihrer Zertifikatanzeige-Anwendung.




:leveloffset: -1


:leveloffset: -1


= Zugriffsmanagement

:leveloffset: +1


[[IDa9211317bd466f2b38cb2d920046a012]]
= Zugriffsmanagement – Überblick
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Die Zugriffsverwaltung ist eine Methode zur Konfiguration der
Benutzerauthentifizierung in SANtricity Unified Manager.



== Welche Authentifizierungsmethoden sind verfügbar?

Folgende Authentifizierungsmethoden sind verfügbar:

* *Lokale Benutzerrollen* -- Authentifizierung wird über RBAC-Funktionen
```

```
(rollenbasierte Zugriffssteuerung) verwaltet. Lokale Benutzerrollen
umfassen vordefinierte Benutzerprofile und Rollen mit spezifischen
Zugriffsberechtigungen.
* *Directory Services* -- die Authentifizierung wird über einen LDAP-
Server (Lightweight Directory Access Protocol) und einen Verzeichnisdienst
verwaltet, z. B. über Microsoft Active Directory.
* *SAML* -- Authentifizierung wird über einen Identitäts-Provider (IdP)
mit SAML 2.0 verwaltet.


Weitere Informationen:

* xref:{relative_path}how-access-management-works-
unified.html["Funktionsweise von Access Management"]
* xref:{relative_path}access-management-terminology-
unified.html["Terminologie für das Zugriffsmanagement"]
* xref:{relative_path}permissions-for-mapped-roles-
unified.html["Berechtigungen für zugeordnete Rollen"]
* xref:{relative_path}access-management-with-saml.html["SAML"]




== Wie konfiguriere ich Access Management?

Die SANtricity-Software ist für die Verwendung lokaler Benutzerrollen
vorkonfiguriert. Wenn Sie LDAP verwenden möchten, können Sie es auf der
Seite Zugriffsverwaltung konfigurieren.

Weitere Informationen:

* xref:{relative_path}access-management-with-local-user-roles-
unified.html["Zugriffsverwaltung mit lokalen Benutzerrollen"]
* xref:{relative_path}access-management-with-directory-services-
unified.html["Zugriffsmanagement mit Verzeichnisdiensten"]
* xref:{relative_path}configure-saml.html["Konfigurieren Sie SAML"]




= Konzepte

:leveloffset: +1


[[ID6f5e760d32267b1aab920015ac913003]]
= Funktionsweise von Access Management
```

```
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Verwenden Sie die Zugriffsverwaltung, um die Benutzerauthentifizierung in
SANtricity Unified Manager einzurichten.



== Konfigurationsworkflow

Die Zugriffsmanagement-Konfiguration funktioniert wie folgt:

. Ein Administrator meldet sich bei Unified Manager mit einem
Benutzerprofil an, das die Berechtigungen für Sicherheitsadministratoren
enthält.
+
[NOTE]
====
Bei der ersten Anmeldung wird der Benutzername verwendet `admin` Wird
automatisch angezeigt und kann nicht geändert werden. Der `admin` Der
Benutzer hat vollen Zugriff auf alle Funktionen im System. Das Passwort
muss bei der ersten Anmeldung festgelegt werden.

====
. Der Administrator navigiert zur Zugriffsverwaltung in der
Benutzeroberfläche, die vorkonfigurierte lokale Benutzerrollen enthält.
Diese Rollen sind eine Implementierung von RBAC-Funktionen (rollenbasierte
Zugriffssteuerung).
. Der Administrator konfiguriert eine oder mehrere der folgenden
Authentifizierungsmethoden:
+
** *Lokale Benutzerrollen* -- Authentifizierung wird über RBAC-Funktionen
verwaltet. Lokale Benutzerrollen umfassen vordefinierte Benutzer und
Rollen mit bestimmten Zugriffsberechtigungen. Administratoren können diese
lokalen Benutzerrollen als einzige Authentifizierungsmethode verwenden
oder in Kombination mit einem Verzeichnisdienst verwenden. Es ist keine
Konfiguration erforderlich – abgesehen von der Festlegung von Passwörtern
für die Benutzer.
** *Directory Services* -- die Authentifizierung wird über einen LDAP-
Server (Lightweight Directory Access Protocol) und einen Verzeichnisdienst
verwaltet, z. B. über Microsoft Active Directory. Ein Administrator stellt
eine Verbindung zum LDAP-Server her und ordnet die LDAP-Benutzer den
```

lokalen Benutzerrollen zu.
** *SAML* -- Authentifizierung wird über einen Identitäts-Provider (IdP) mit der Security Assertion Markup Language (SAML) 2.0 verwaltet. Ein Administrator stellt die Verbindung zwischen dem IdP-System und dem Storage-Array her und ordnet anschließend die IdP-Benutzer den im Storage-Array eingebetteten lokalen Benutzerrollen zu.

. Der Administrator stellt Benutzern die Anmeldeinformationen für Unified Manager zur Verfügung.
. Benutzer melden sich beim System an, indem sie ihre Anmeldedaten eingeben. Während der Anmeldung führt das System die folgenden Hintergrundaufgaben aus:
+
** Authentifiziert Benutzernamen und Kennwort anhand des Benutzerkontos.
** Legt die Berechtigungen des Benutzers basierend auf den zugewiesenen Rollen fest.
** Bietet dem Benutzer Zugriff auf Funktionen in der Benutzeroberfläche.
** Zeigt den Benutzernamen im oberen Banner an.

== Funktionen in Unified Manager verfügbar

Der Zugriff auf Funktionen hängt von den zugewiesenen Rollen eines Benutzers ab. Dazu gehören:

* *Storage Admin* -- Vollständiger Lese-/Schreibzugriff auf Speicherobjekte auf den Arrays, aber kein Zugriff auf die Sicherheitskonfiguration.
* *Security Admin* -- Zugriff auf die Sicherheitskonfiguration in Access Management und Certificate Management.
* *Support Admin* -- Zugriff auf alle Hardware-Ressourcen auf Speicher-Arrays, Ausfalldaten und MEL-Ereignisse. Kein Zugriff auf Speicherobjekte oder die Sicherheitskonfiguration.
* *Monitor* -- schreibgeschützter Zugriff auf alle Speicherobjekte, aber kein Zugriff auf die Sicherheitskonfiguration.

Eine nicht verfügbare Funktion ist entweder ausgegraut oder wird in der Benutzeroberfläche nicht angezeigt.

```
[[ID7764d469a49c994263e89d22bb414fe6]]
= Terminologie für das Zugriffsmanagement
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Erfahren Sie, wie die Bedingungen für das Zugriffsmanagement für
SANtricity Unified Manager gelten.

[cols="25h,~"]
|===
| Laufzeit | Beschreibung


 a|
Active Directory
 a|
Active Directory (AD) ist ein Microsoft-Verzeichnisdienst, der LDAP für
Windows-Domänennetzwerke verwendet.



 a|
Verbindlich
 a|
Bindevorgänge werden zur Authentifizierung von Clients auf dem
Verzeichnisserver verwendet. Binding erfordert in der Regel Konto- und
Kennwortanmeldeinformationen, aber einige Server erlauben anonyme
Bindevorgänge.



 a|
CA
 a|
Eine Zertifizierungsstelle (CA) ist eine vertrauenswürdige Einheit, die
elektronische Dokumente, sogenannte digitale Zertifikate, für Internet-
Sicherheit ausstellt. Diese Zertifikate identifizieren Website-Besitzer,
die sichere Verbindungen zwischen Clients und Servern ermöglichen.



 a|
Zertifikat
```

a|
Ein Zertifikat identifiziert den Eigentümer einer Website aus Sicherheitsgründen, wodurch Angreifer die Identität der Website nicht mehr verkörpern können. Das Zertifikat enthält Informationen über den Websiteeigentümer und die Identität des vertrauenswürdigen Unternehmens, der diese Informationen bescheinigt (unterzeichnet).

a|
LDAP
a|
Lightweight Directory Access Protocol (LDAP) ist ein Anwendungsprotokoll für den Zugriff auf verteilte Verzeichnisinformationsdienste und die Wartung. Mit diesem Protokoll können viele verschiedene Anwendungen und Dienste eine Verbindung zum LDAP-Server zur Überprüfung von Benutzern herstellen.

a|
RBAC
a|
Die rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC) ist eine Methode zur Regulierung des Zugriffs auf Computer- oder Netzwerkressourcen, basierend auf den Rollen einzelner Benutzer. Unified Manager enthält vordefinierte Rollen.

a|
SAML
a|
Security Assertion Markup Language (SAML) ist ein XML-basierter Standard für die Authentifizierung und Autorisierung zwischen zwei Einheiten. SAML ermöglicht Multi-Faktor-Authentifizierung, bei der Benutzer zwei oder mehr Elemente zur Identitätsnachweise bereitstellen müssen (z. B. ein Passwort und ein Fingerabdruck). Die in das Storage Array integrierte SAML-Funktion ist mit SAML2.0 zur Identitätsprüfung, Authentifizierung und Autorisierung kompatibel.

a|
SSO
a|
Bei Single Sign On (SSO) handelt es sich um einen

```
Authentifizierungsservice, mit dem ein Satz an Anmeldeinformationen auf
mehrere Anwendungen zugreifen kann.



 a|
Web Services Proxy
 a|
Der Web Services Proxy, der Zugriff über HTTPS-Standardmechanismen
bereitstellt, ermöglicht Administratoren die Konfiguration von
Managementservices für Speicher-Arrays. Der Proxy kann auf Windows- oder
Linux-Hosts installiert werden. Die Unified Manager-Schnittstelle ist mit
dem Web Services Proxy verfügbar.

|===



[[IDccb5dd4b0bba81fa77e4e35ec22e0910]]
= Berechtigungen für zugeordnete Rollen
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Die RBAC-Funktionen (rollenbasierte Zugriffssteuerung) umfassen
vordefinierte Benutzer, wobei eine oder mehrere Rollen zugewiesen sind.
Jede Rolle umfasst Berechtigungen für den Zugriff auf Aufgaben in
SANtricity Unified Manager.

Die Rollen ermöglichen Benutzern den Zugriff auf Aufgaben wie folgt:

* *Storage Admin* -- Vollständiger Lese-/Schreibzugriff auf
Speicherobjekte auf den Arrays, aber kein Zugriff auf die
Sicherheitskonfiguration.
* *Security Admin* -- Zugriff auf die Sicherheitskonfiguration in Access
Management und Certificate Management.
* *Support Admin* -- Zugriff auf alle Hardware-Ressourcen auf Speicher-
Arrays, Ausfalldaten und MEL-Ereignisse. Kein Zugriff auf Speicherobjekte
oder die Sicherheitskonfiguration.
* *Monitor* -- schreibgeschützter Zugriff auf alle Speicherobjekte, aber
kein Zugriff auf die Sicherheitskonfiguration.


Wenn ein Benutzer über keine Berechtigungen für eine bestimmte Funktion
```

```
verfügt, ist diese Funktion entweder zur Auswahl nicht verfügbar oder wird
nicht in der Benutzeroberfläche angezeigt.



[[IDf2987e307210c37449a1ffb92f8a199a]]
= Zugriffsverwaltung mit lokalen Benutzerrollen
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Administratoren können die in SANtricity Unified Manager erzwungenen RBAC-
Funktionen (rollenbasierte Zugriffssteuerung) nutzen. Diese Funktionen
werden als „lokale Benutzerrollen“ bezeichnet.



== Konfigurationsworkflow

Lokale Benutzerrollen sind im System vorkonfiguriert. Um lokale
Benutzerrollen für die Authentifizierung zu verwenden, können
Administratoren Folgendes tun:

. Ein Administrator meldet sich bei Unified Manager mit einem
Benutzerprofil an, das die Berechtigungen für Sicherheitsadministratoren
enthält.
+
[NOTE]
====
Der `admin` Der Benutzer hat vollen Zugriff auf alle Funktionen im System.

====
. Ein Administrator überprüft die Benutzerprofile, die vordefiniert sind
und nicht geändert werden können.
. Optional weist der Administrator jedem Benutzerprofil neue Passwörter
zu.
. Benutzer melden sich mit ihren zugewiesenen Anmeldedaten am System an.



== Vereinfachtes

Bei der Verwendung von nur lokalen Benutzerrollen für die
```

```
Authentifizierung können Administratoren die folgenden Verwaltungsaufgaben
ausführen:

* Passwörter ändern.
* Legen Sie eine Mindestlänge für Passwörter fest.
* Benutzern erlauben, sich ohne Passwörter anzumelden.




[[ID363c3a4c941eb63fd93a822d5c99c4ea]]
= Zugriffsmanagement mit Verzeichnisdiensten
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Administratoren können einen LDAP-Server (Lightweight Directory Access
Protocol) und einen Verzeichnisdienst wie Microsoft Active Directory
verwenden.



== Konfigurationsworkflow

Wenn ein LDAP-Server und ein Verzeichnisdienst im Netzwerk verwendet
werden, funktioniert die Konfiguration wie folgt:

. Ein Administrator meldet sich bei Unified Manager mit einem
Benutzerprofil an, das die Berechtigungen für Sicherheitsadministratoren
enthält.
+
[NOTE]
====
Der `admin` Der Benutzer hat vollen Zugriff auf alle Funktionen im System.

====
. Der Administrator gibt die Konfigurationseinstellungen für den LDAP-
Server ein. Zu den Einstellungen gehören der Domain-Name, die URL und die
Bind-Kontoinformationen.
. Wenn der LDAP-Server ein sicheres Protokoll (LDAPS) verwendet, lädt der
Administrator eine Zertifikatskette für die Authentifizierung zwischen dem
LDAP-Server und dem Hostsystem, auf dem der Web Services Proxy installiert
ist, hoch.
. Nachdem die Serververbindung hergestellt wurde, ordnet der Administrator
```

die Benutzergruppen den lokalen Benutzerrollen zu. Diese Rollen sind vordefiniert und können nicht geändert werden.
. Der Administrator testet die Verbindung zwischen dem LDAP-Server und dem Web Services Proxy.
. Benutzer melden sich mit ihren zugewiesenen LDAP/Directory Services-Anmeldedaten am System an.

== Vereinfachtes

Bei der Verwendung von Verzeichnisdiensten zur Authentifizierung können Administratoren die folgenden Verwaltungsaufgaben ausführen:

* Fügen Sie einen Verzeichnisserver hinzu.
* Bearbeiten der Einstellungen des Verzeichnisservers.
* Zuordnen von LDAP-Benutzern zu lokalen Benutzerrollen.
* Entfernen Sie einen Verzeichnisserver.
* Passwörter ändern.
* Legen Sie eine Mindestlänge für Passwörter fest.
* Benutzern erlauben, sich ohne Passwörter anzumelden.

[[ID8d4bade247b8eb0d163a42a68ad50331]]
= Zugriffsmanagement mit SAML
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
Für die Zugriffsverwaltung können Administratoren die in das Array integrierten Funktionen der Security Assertion Markup Language (SAML) 2.0 verwenden.

== Konfigurationsworkflow

Die SAML-Konfiguration funktioniert wie folgt:

. Ein Administrator meldet sich bei Unified Manager mit einem Benutzerprofil an, das Sicherheitsadministratorberechtigungen enthält.

```
+
[NOTE]
====
Der `admin` Der Benutzer hat vollständigen Zugriff auf alle Funktionen in
System Manager.

====
. Der Administrator wechselt zur Registerkarte *SAML* unter
Zugriffsverwaltung.
. Ein Administrator konfiguriert die Kommunikation mit dem Identity
Provider (IdP). Ein IdP ist ein externes System, mit dem
Anmeldeinformationen von einem Benutzer angefordert werden und
festgestellt wird, ob der Benutzer erfolgreich authentifiziert wurde. Um
die Kommunikation mit dem Speicher-Array zu konfigurieren, lädt der
Administrator die IdP-Metadatendatei vom IdP-System herunter und lädt die
Datei dann mithilfe von Unified Manager auf das Speicher-Array hoch.
. Ein Administrator stellt eine Vertrauensbeziehung zwischen dem
Dienstanbieter und dem IdP her. Ein Dienstanbieter steuert die
Benutzerautorisierung. In diesem Fall fungiert der Controller im Speicher-
Array als Service Provider. Zum Konfigurieren der Kommunikation verwendet
der Administrator Unified Manager, um eine Service Provider-Metadatendatei
für den Controller zu exportieren. Vom IdP-System importiert der
Administrator dann die Metadatendatei in das IdP.
+
[NOTE]
====
Administratoren sollten außerdem sicherstellen, dass das IdP die
Möglichkeit unterstützt, eine Name-ID bei der Authentifizierung
zurückzugeben.

====
. Der Administrator ordnet die Rollen des Storage-Arrays den in IdP
definierten Benutzerattributen zu. Dazu verwendet der Administrator
Unified Manager zum Erstellen der Zuordnungen.
. Der Administrator testet die SSO-Anmeldung an der IdP-URL. Dieser Test
stellt sicher, dass das Storage-Array und das IdP kommunizieren können.
+
[CAUTION]
====
Sobald SAML aktiviert ist, können Sie sie über die Benutzeroberfläche
nicht deaktivieren oder die IdP-Einstellungen bearbeiten. Wenn Sie die
SAML-Konfiguration deaktivieren oder bearbeiten müssen, wenden Sie sich an
den technischen Support, um Hilfe zu erhalten.

====
. Über Unified Manager aktiviert der Administrator SAML für das Storage-
```

```
Array.
. Benutzer melden sich mit ihren SSO-Anmeldedaten am System an.



== Vereinfachtes

Bei der Verwendung von SAML zur Authentifizierung können Administratoren
die folgenden Managementaufgaben ausführen:

* Neue Rollenzuordnungen ändern oder erstellen
* Exportieren Sie die Dateien von Dienstanbietern



== Zugriffsbeschränkungen

Wenn SAML aktiviert ist, können Benutzer Speicher für dieses Array nicht
über die vorhandene Storage Manager-Schnittstelle ermitteln oder
verwalten.

Außerdem können die folgenden Clients nicht auf Services und Ressourcen
des Speicherarrays zugreifen:

* Enterprise Management-Fenster (EMW)
* Befehlszeilenschnittstelle (CLI)
* Software Developer Kits (SDK)-Clients
* In-Band-Clients
* REST-API-Clients für die HTTP-Standardauthentifizierung
* Melden Sie sich mithilfe des standardmäßigen REST-API-Endpunkts an



:leveloffset: -1


= Lokale Benutzerrollen verwenden

:leveloffset: +1


[[ID77c4ab0ee911ddb98114bebadc420ea3]]
= Zeigen Sie lokale Benutzerrollen an
:allow-uri-read:
```

```
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Auf der Registerkarte Lokale Benutzerrollen können Sie die Zuordnungen der
Benutzer zu den Standardrollen anzeigen. Diese Zuordnungen sind Teil der
RBAC (rollenbasierte Zugriffssteuerung), die im Web Services Proxy für
SANtricity Unified Manager durchgesetzt wird.

.Bevor Sie beginnen
Sie müssen mit einem Benutzerprofil angemeldet sein, das
Sicherheitsadministratorberechtigungen enthält. Andernfalls werden die
Zugriffsverwaltungsfunktionen nicht angezeigt.

.Über diese Aufgabe
Die Benutzer und Zuordnungen können nicht geändert werden. Es können nur
Passwörter geändert werden.

.Schritte
. Wählen Sie *Zugriffsmanagement*.
. Wählen Sie die Registerkarte * Lokale Benutzerrollen* aus.
+
Die Benutzer sind in der Tabelle aufgeführt:

+
** *Admin* -- Super-Administrator, der Zugriff auf alle Funktionen im
System hat. Dieser Benutzer enthält alle Rollen.
** *Storage* -- der Administrator, der für die gesamte Storage-
Bereitstellung verantwortlich ist. Dieser Benutzer umfasst die folgenden
Rollen: Storage-Administrator, Support-Administrator und Monitor.
** *Sicherheit* -- der für die Sicherheitskonfiguration verantwortliche
Benutzer, einschließlich Zugriffsverwaltung und Zertifikatverwaltung.
Dieser Benutzer umfasst die folgenden Rollen: Security Admin und Monitor.
** *Support* -- der Benutzer, der für Hardware-Ressourcen, Ausfalldaten
und Firmware-Upgrades verantwortlich ist. Dieser Benutzer enthält die
folgenden Rollen: Unterstützen Sie Admin und Monitor.
** *Monitor* -- ein Benutzer mit schreibgeschütztem Zugriff auf das
System. Dieser Benutzer enthält nur die Rolle „Monitor“.
** *rw* (lesen/schreiben) -- dieser Benutzer enthält die folgenden Rollen:
Speicheradministrator, Supportadministrator und Monitor.
** *Ro* (schreibgeschützt) -- dieser Benutzer enthält nur die Rolle
Monitor.
```

```
[[ID3405a8bad80116301aaaf549165d12c5]]
= Passwörter für lokale Benutzerprofile ändern
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Sie können die Benutzerpasswörter für jeden Benutzer in der
Zugriffsverwaltung ändern.

.Bevor Sie beginnen
* Sie müssen als lokaler Administrator angemeldet sein, der Root-Admin-
Berechtigungen enthält.
* Sie müssen das lokale Administratorkennwort kennen.


.Über diese Aufgabe
Beachten Sie bei der Auswahl eines Passworts die folgenden Richtlinien:

* Alle neuen lokalen Benutzerpasswörter müssen die aktuelle Einstellung
für ein Mindestpasswort erfüllen oder überschreiten (unter „Einstellungen
anzeigen/bearbeiten“).
* Bei Passwörtern wird die Groß-/Kleinschreibung berücksichtigt.
* Nachgestellte Leerzeichen werden nicht aus Kennwörtern entfernt, wenn
sie gesetzt sind. Achten Sie darauf, Leerzeichen einzugeben, wenn diese im
Passwort enthalten waren.
* Um die Sicherheit zu erhöhen, verwenden Sie mindestens 15
alphanumerische Zeichen, und ändern Sie das Passwort häufig.


.Schritte
. Wählen Sie *Zugriffsmanagement*.
. Wählen Sie die Registerkarte * Lokale Benutzerrollen* aus.
. Wählen Sie einen Benutzer aus der Tabelle aus.
+
Die Schaltfläche Kennwort ändern steht zur Verfügung.

. Wählen Sie *Passwort Ändern*.
+
Das Dialogfeld Kennwort ändern wird geöffnet.

. Wenn für lokale Benutzerpasswörter keine Mindestkennwortlänge festgelegt
```

```
ist, können Sie das Kontrollkästchen aktivieren, damit der Benutzer ein
Passwort für den Zugriff auf das System eingeben muss.
. Geben Sie das neue Kennwort für den ausgewählten Benutzer in die beiden
Felder ein.
. Geben Sie Ihr lokales Administratorpasswort ein, um diesen Vorgang zu
bestätigen, und klicken Sie dann auf *Ändern*.


.Ergebnisse
Wenn der Benutzer derzeit angemeldet ist, wird die aktive Sitzung des
Benutzers durch die Kennwortänderung beendet.



[[ID47a8415e1e1a6088723fa19c41cd46af]]
= Ändern Sie die Einstellungen für das lokale Benutzerpasswort
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Sie können die erforderliche Mindestlänge für alle neuen oder
aktualisierten lokalen Benutzerpasswörter festlegen. Außerdem können
lokale Benutzer ohne Eingabe eines Kennworts auf das System zugreifen.

.Bevor Sie beginnen
Sie müssen als lokaler Administrator angemeldet sein, der Root-Admin-
Berechtigungen enthält.

.Über diese Aufgabe
Beachten Sie die folgenden Richtlinien, wenn Sie die Mindestlänge für
lokale Benutzerpasswörter festlegen:

* Die Einstellung von Änderungen hat keine Auswirkung auf vorhandene
lokale Benutzerpasswörter.
* Die Mindestlänge für lokale Benutzerpasswörter muss zwischen 0 und 30
Zeichen liegen.
* Alle neuen lokalen Benutzerpasswörter müssen die aktuelle
Mindestlängeneinstellung erfüllen oder überschreiten.
* Legen Sie keine Mindestlänge für das Passwort fest, wenn lokale Benutzer
ohne Eingabe eines Kennworts auf das System zugreifen möchten.


.Schritte
. Wählen Sie *Zugriffsmanagement*.
```

```
. Wählen Sie die Registerkarte * Lokale Benutzerrollen* aus.
. Wählen Sie *Einstellungen Anzeigen/Bearbeiten*.
+
Das Dialogfeld Einstellungen für das lokale Benutzerpasswort wird
geöffnet.

. Führen Sie einen der folgenden Schritte aus:
+
** Um lokalen Benutzern den Zugriff auf das System zu ermöglichen _ohne_
ein Passwort einzugeben, deaktivieren Sie das Kontrollkästchen „Alle
lokalen Benutzerpasswörter müssen mindestens sein“.
** Um eine Mindestkennwortlänge für alle lokalen Benutzerpasswörter
festzulegen, aktivieren Sie das Kontrollkästchen „Alle lokalen
Benutzerpasswörter müssen mindestens sein“. Verwenden Sie dann das
Spinner-Feld, um die erforderliche Mindestlänge für alle lokalen
Benutzerpasswörter festzulegen.
+
Neue lokale Benutzerpasswörter müssen die aktuelle Einstellung erfüllen
oder überschreiten.



. Klicken Sie Auf *Speichern*.




:leveloffset: -1


= Verzeichnisdienste verwenden

:leveloffset: +1


[[ID97d75be010520c2751259db2956d7eb9]]
= Verzeichnisserver hinzufügen
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Um die Authentifizierung für die Zugriffsverwaltung zu konfigurieren,
stellen Sie eine Kommunikation zwischen einem LDAP-Server und dem Host
her, auf dem der Web Services Proxy für SANtricity Unified Manager
```

```
ausgeführt wird. Anschließend ordnen Sie die LDAP-Benutzergruppen den
lokalen Benutzerrollen zu.

.Bevor Sie beginnen
* Sie müssen mit einem Benutzerprofil angemeldet sein, das
Sicherheitsadministratorberechtigungen enthält. Andernfalls werden die
Zugriffsverwaltungsfunktionen nicht angezeigt.
* Benutzergruppen müssen in Ihrem Verzeichnisdienst definiert sein.
* LDAP-Serveranmeldeinformationen müssen verfügbar sein, einschließlich
Domänenname, Server-URL und optional Benutzername und Kennwort für das
Bindekonto.
* Bei LDAPS-Servern mit einem sicheren Protokoll muss die Zertifikatskette
des LDAP-Servers auf Ihrem lokalen Computer installiert sein.


.Über diese Aufgabe
Das Hinzufügen eines Verzeichnisservers ist ein zweistufiger Prozess.
Geben Sie zuerst den Domain-Namen und die URL ein. Wenn Ihr Server ein
sicheres Protokoll verwendet, müssen Sie auch ein CA-Zertifikat zur
Authentifizierung hochladen, wenn es von einer nicht standardmäßigen
Signierungsbehörde signiert ist. Wenn Sie über Anmeldedaten für ein
Bindekonto verfügen, können Sie auch Ihren Benutzernamen und Ihr Kennwort
eingeben. Als Nächstes werden die Benutzergruppen des LDAP-Servers lokalen
Benutzerrollen zugeordnet.

.Schritte
. Wählen Sie *Zugriffsmanagement*.
. Wählen Sie auf der Registerkarte *Directory Services* die Option *Add
Directory Server* aus.
+
Das Dialogfeld Add Directory Server wird geöffnet.

. Geben Sie auf der Registerkarte *Server-Einstellungen* die
Anmeldeinformationen für den LDAP-Server ein.
+
.Felddetails
[%collapsible]
====
[cols="25h,~"]
|===
| Einstellung | Beschreibung


 a|
*Konfigurationseinstellungen*
```

 a|
Domäne(en)
 a|
Geben Sie den Domänennamen des LDAP-Servers ein. Geben Sie für mehrere Domänen die Domänen in eine kommagetrennte Liste ein. Der Domänenname wird in der Anmeldung (_username_@_Domain_) verwendet, um anzugeben, gegen welchen Verzeichnisserver sich authentifizieren soll.

 a|
Server-URL
 a|
Geben Sie die URL für den Zugriff auf den LDAP-Server in Form von ein `ldap[s]://*host*:*port*`.

 a|
Zertifikat hochladen (optional)
 a|

NOTE: Dieses Feld wird nur angezeigt, wenn ein LDAPS-Protokoll im obigen Feld Server-URL angegeben wird.

Klicken Sie auf *Durchsuchen* und wählen Sie ein CA-Zertifikat zum Hochladen aus. Dies ist das vertrauenswürdige Zertifikat oder die Zertifikatskette, die für die Authentifizierung des LDAP-Servers verwendet wird.

 a|
Konto binden (optional)
 a|
Geben Sie ein schreibgeschütztes Benutzerkonto ein, um Suchanfragen auf dem LDAP-Server und für die Suche in den Gruppen durchzuführen. Geben Sie den Kontonamen im LDAP-Format ein. Wenn der Bindebenutzer beispielsweise „bind-Konto“ heißt, können Sie einen Wert wie eingeben `CN=bindacct,CN=Users,DC=cpoc,DC=local`.

 a|
Bindepasswort (optional)
 a|

NOTE: Dieses Feld wird angezeigt, wenn Sie ein Bindungskonto eingeben.

Geben Sie das Passwort für das Bindekonto ein.

a|
Testen Sie die Serververbindung, bevor Sie sie hinzufügen
a|
Aktivieren Sie dieses Kontrollkästchen, wenn Sie sicherstellen möchten, dass das System mit der eingegebenen LDAP-Serverkonfiguration kommunizieren kann. Der Test erfolgt, nachdem Sie unten im Dialogfeld auf *Hinzufügen* geklickt haben.

Wenn dieses Kontrollkästchen aktiviert ist und der Test fehlschlägt, wird die Konfiguration nicht hinzugefügt. Sie müssen den Fehler beheben oder das Kontrollkästchen deaktivieren, um den Test zu überspringen und die Konfiguration hinzuzufügen.

a|
Berechtigungseinstellungen

a|
Basis-DN suchen
a|
Geben Sie den LDAP-Kontext ein, um nach Benutzern zu suchen, normalerweise in Form von `CN=Users, DC=cpoc, DC=local`.

a|
Attribut Benutzername
a|
Geben Sie das Attribut ein, das zur Authentifizierung an die Benutzer-ID gebunden ist. Beispiel: `sAMAccountName`.

a|
Gruppenattribut(e)
a|
Geben Sie eine Liste der Gruppenattribute für den Benutzer ein, die für

```
die Zuordnung von Gruppen zu Rollen verwendet werden. Beispiel: `memberOf,
managedObjects`.

|===
====
. Klicken Sie auf die Registerkarte *Rollenzuordnung*.
. Weisen Sie den vordefinierten Rollen LDAP-Gruppen zu. Einer Gruppe
können mehrere Rollen zugewiesen sein.
+
.Felddetails
[%collapsible]
====
[cols="25h,~"]
|===
| Einstellung | Beschreibung


 a|
*Zuordnungen*



 a|
Gruppen-DN
 a|
Geben Sie den Group Distinguished Name (DN) für die zu zugeordnete LDAP-
Benutzergruppe an. Reguläre Ausdrücke werden unterstützt. Diese speziellen
regulären Ausdruckszeichen müssen mit einem umgekehrten Schrägstrich (\)
entgangen werden, wenn sie nicht Teil eines regulären Ausdrucksmusters
sind: \.[]{}()<>*+-=!?^



 a|
Rollen
 a|
Klicken Sie in das Feld, und wählen Sie eine der lokalen Benutzerrollen
aus, die dem Gruppen-DN zugeordnet werden sollen. Sie müssen jede Rolle,
die Sie für diese Gruppe aufnehmen möchten, einzeln auswählen. Die
Monitorrolle ist erforderlich, um sich in SANtricity Unified Manager mit
den anderen Rollen anzumelden. Die zugeordneten Rollen umfassen die
folgenden Berechtigungen:

** *Storage Admin* -- Vollständiger Lese-/Schreibzugriff auf
Speicherobjekte auf den Arrays, aber kein Zugriff auf die
Sicherheitskonfiguration.
** *Security Admin* -- Zugriff auf die Sicherheitskonfiguration in Access
```

```
Management und Certificate Management.
** *Support Admin* -- Zugriff auf alle Hardware-Ressourcen auf Speicher-
Arrays, Ausfalldaten und MEL-Ereignisse. Kein Zugriff auf Speicherobjekte
oder die Sicherheitskonfiguration.
** *Monitor* -- schreibgeschützter Zugriff auf alle Speicherobjekte, aber
kein Zugriff auf die Sicherheitskonfiguration.


|===
====
+

NOTE: Die Überwachungsrolle ist für alle Benutzer, einschließlich des
Administrators, erforderlich.

. Klicken Sie auf *Weitere Zuordnungen hinzufügen*, um weitere Gruppen-zu-
Rolle-Zuordnungen einzugeben.
. Wenn Sie mit den Zuordnungen fertig sind, klicken Sie auf *Hinzufügen*.
+
Das System führt eine Validierung durch und stellt sicher, dass das
Speicher-Array und der LDAP-Server kommunizieren können. Wenn eine
Fehlermeldung angezeigt wird, überprüfen Sie die im Dialogfeld
eingegebenen Anmeldeinformationen, und geben Sie die Informationen ggf.
erneut ein.




[[IDee85257b82a94bcba04035f07c5b7baa]]
= Bearbeiten Sie die Einstellungen des Verzeichnisservers und die
Rollenzuordnungen
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Wenn Sie zuvor einen Verzeichnisserver in der Zugriffsverwaltung
konfiguriert haben, können Sie dessen Einstellungen jederzeit ändern. Zu
den Einstellungen gehören die Informationen zur Serververbindung und die
Zuordnungen von Gruppen zu Rollen.

.Bevor Sie beginnen
* Sie müssen mit einem Benutzerprofil angemeldet sein, das
Sicherheitsadministratorberechtigungen enthält. Andernfalls werden die
```

```
Zugriffsverwaltungsfunktionen nicht angezeigt.
* Ein Verzeichnisserver muss definiert werden.


.Schritte
. Wählen Sie *Zugriffsmanagement*.
. Wählen Sie die Registerkarte *Directory Services* aus.
. Wenn mehr als ein Server definiert ist, wählen Sie den Server aus der
Tabelle aus, den Sie bearbeiten möchten.
. Wählen Sie *Einstellungen Anzeigen/Bearbeiten*.
+
Das Dialogfeld Verzeichnisservereinstellungen wird geöffnet.

. Ändern Sie auf der Registerkarte *Server-Einstellungen* die gewünschten
Einstellungen.
+
.Felddetails
[%collapsible]
====
[cols="25h,~"]
|===
| Einstellung | Beschreibung


 a|
*Konfigurationseinstellungen*



 a|
Domäne(en)
 a|
Der/die Domänenname(n) des/der LDAP-Server(e). Geben Sie für mehrere
Domänen die Domänen in eine kommagetrennte Liste ein. Der Domänenname wird
in der Anmeldung (_username_@_Domain_) verwendet, um anzugeben, gegen
welchen Verzeichnisserver sich authentifizieren soll.



 a|
Server-URL
 a|
Die URL für den Zugriff auf den LDAP-Server in Form von
`ldap[s]://host:port`.
```

```
 a|
Konto binden (optional)
 a|
Das schreibgeschützte Benutzerkonto für Suchabfragen am LDAP-Server und
für die Suche in den Gruppen.



 a|
Bindepasswort (optional)
 a|
Das Kennwort für das Bindekonto. (Dieses Feld wird angezeigt, wenn ein
Bindekonto eingegeben wird.)



 a|
Testen Sie vor dem Speichern die Serververbindung
 a|
Überprüft, ob das System mit der LDAP-Serverkonfiguration kommunizieren
kann. Der Test erfolgt nach dem Klicken auf *Speichern*. Wenn dieses
Kontrollkästchen aktiviert ist und der Test fehlschlägt, wird die
Konfiguration nicht geändert. Sie müssen den Fehler beheben oder das
Kontrollkästchen deaktivieren, um den Test zu überspringen und die
Konfiguration erneut zu bearbeiten.



 a|
*Berechtigungseinstellungen*



 a|
Basis-DN suchen
 a|
Der LDAP-Kontext für die Suche nach Benutzern, in der Regel in Form von
`CN=Users, DC=cpoc, DC=local`.



 a|
Attribut Benutzername
 a|
Das Attribut, das zur Authentifizierung an die Benutzer-ID gebunden ist.
Beispiel:
`sAMAccountName`.
```

```
 a|
Gruppenattribut(e)
 a|
Eine Liste der Gruppenattribute für den Benutzer, die für die Zuordnung
von Gruppen zu Rollen verwendet werden. Beispiel:
`memberOf, managedObjects`.

|===
====
. Ändern Sie auf der Registerkarte *Rollenzuordnung* die gewünschte
Zuordnung.
+
.Felddetails
[%collapsible]
====
[cols="25h,~"]
|===
| Einstellung | Beschreibung


 a|
*Zuordnungen*



 a|
Gruppen-DN
 a|
Der Domain-Name für die LDAP-Benutzergruppe, die zugeordnet werden soll.
Reguläre Ausdrücke werden unterstützt. Diese speziellen regulären
Ausdruckszeichen müssen mit einem umgekehrten Schrägstrich (\) entgangen
werden, wenn sie nicht Teil eines regulären Ausdrucksmusters sind:

\.[]{}()<>*+-=!?^



 a|
Rollen
 a|
Die Rollen, die dem Gruppen-DN zugeordnet werden sollen. Sie müssen jede
Rolle, die Sie für diese Gruppe aufnehmen möchten, einzeln auswählen. Die
Monitorrolle ist erforderlich, um sich in SANtricity Unified Manager mit
den anderen Rollen anzumelden. Dazu gehören folgende Rollen:
```

```
** *Storage Admin* -- Vollständiger Lese-/Schreibzugriff auf
Speicherobjekte auf den Arrays, aber kein Zugriff auf die
Sicherheitskonfiguration.
** *Security Admin* -- Zugriff auf die Sicherheitskonfiguration in Access
Management und Certificate Management.
** *Support Admin* -- Zugriff auf alle Hardware-Ressourcen auf Speicher-
Arrays, Ausfalldaten und MEL-Ereignisse. Kein Zugriff auf Speicherobjekte
oder die Sicherheitskonfiguration.
** *Monitor* -- schreibgeschützter Zugriff auf alle Speicherobjekte, aber
kein Zugriff auf die Sicherheitskonfiguration.


|===
====
+

NOTE: Die Überwachungsrolle ist für alle Benutzer, einschließlich des
Administrators, erforderlich.

. Klicken Sie auf *Weitere Zuordnungen hinzufügen*, um weitere Gruppen-zu-
Rolle-Zuordnungen einzugeben.
. Klicken Sie Auf *Speichern*.


.Ergebnisse
Nach Abschluss dieser Aufgabe werden alle aktiven Benutzersitzungen
beendet. Nur Ihre aktuelle Benutzersitzung bleibt erhalten.



[[ID8b549a4e39d8353b9b2084b0e704727e]]
= Verzeichnisserver entfernen
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Um die Verbindung zwischen einem Verzeichnisserver und dem Web Services
Proxy zu unterbrechen, können Sie die Serverinformationen von der Seite
Zugriffsverwaltung entfernen. Sie möchten diese Aufgabe möglicherweise
ausführen, wenn Sie einen neuen Server konfiguriert haben und den alten
dann entfernen möchten.

.Bevor Sie beginnen
```

```
Sie müssen mit einem Benutzerprofil angemeldet sein, das
Sicherheitsadministratorberechtigungen enthält. Andernfalls werden die
Zugriffsverwaltungsfunktionen nicht angezeigt.

.Über diese Aufgabe
Nach Abschluss dieser Aufgabe werden alle aktiven Benutzersitzungen
beendet. Nur Ihre aktuelle Benutzersitzung bleibt erhalten.

.Schritte
. Wählen Sie *Zugriffsmanagement*.
. Wählen Sie die Registerkarte *Directory Services* aus.
. Wählen Sie in der Liste den Verzeichnisserver aus, den Sie löschen
möchten.
. Klicken Sie Auf *Entfernen*.
+
Das Dialogfeld Verzeichnisserver entfernen wird geöffnet.

. Typ `remove` Klicken Sie im Feld auf *Entfernen*.
+
Die Konfigurationseinstellungen des Verzeichnisservers, die
Berechtigungseinstellungen und Rollenzuordnungen werden entfernt. Benutzer
können sich nicht mehr mit Anmeldeinformationen von diesem Server
anmelden.




:leveloffset: -1


= Verwenden Sie SAML

:leveloffset: +1


[[IDe0e6a8b240d965e669f952153cf8d669]]
= Konfigurieren Sie SAML
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Zum Konfigurieren der Authentifizierung für das Zugriffsmanagement können
```

Sie die im Speicher-Array integrierten SAML-Funktionen (Security Assertion Markup Language) verwenden. Mit dieser Konfiguration wird eine Verbindung zwischen einem Identitätsanbieter und dem Speicheranbieter hergestellt.

.Bevor Sie beginnen
* Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden die Zugriffsverwaltungsfunktionen nicht angezeigt.
* Sie müssen die IP-Adresse oder den Domänennamen des Controllers im Speicher-Array kennen.
* Ein IdP-Administrator hat ein IdP-System konfiguriert.
* Ein IdP-Administrator hat sichergestellt, dass der IdP die Möglichkeit unterstützt, eine Name-ID bei der Authentifizierung zurückzugeben.
* Ein Administrator hat sichergestellt, dass der IdP-Server und die Controller-Uhr synchronisiert werden (entweder über einen NTP-Server oder durch Anpassung der Controller-Uhreinstellungen).
* Eine IdP-Metadatendatei wird vom IdP-System heruntergeladen und ist auf dem lokalen System verfügbar, das für den Zugriff auf Unified Manager verwendet wird.

.Über diese Aufgabe
Ein Identitäts-Provider (IdP) ist ein externes System, mit dem Anmeldeinformationen von einem Benutzer angefordert und festgestellt werden können, ob dieser Benutzer erfolgreich authentifiziert wurde. Der IdP kann so konfiguriert werden, dass er Multi-Faktor-Authentifizierung bietet und eine beliebige Benutzerdatenbank, wie z. B. Active Directory, verwendet. Ihr Sicherheitsteam ist für die Instandhaltung des IdP verantwortlich. Ein Service-Provider (SP) ist ein System, das die Benutzerauthentifizierung und den Zugriff steuert. Wenn Access Management mit SAML konfiguriert ist, fungiert das Storage-Array als Dienstanbieter für die Anforderung der Authentifizierung vom Identity Provider. Um eine Verbindung zwischen dem IdP und dem Storage-Array herzustellen, teilen Sie Metadatendateien zwischen diesen beiden Einheiten gemeinsam. Als Nächstes ordnen Sie die IdP-Benutzereinheiten den Storage-Array-Rollen zu. Und schließlich testen Sie die Verbindung und SSO-Anmeldedaten, bevor Sie SAML aktivieren.

[NOTE]
====
SAML und Directory Services. Wenn Sie SAML aktivieren, wenn die Verzeichnisdienste als Authentifizierungsmethode konfiguriert sind, ersetzt SAML die Verzeichnisdienste in Unified Manager. Wenn Sie SAML später deaktivieren, wird die Konfiguration der Verzeichnisdienste wieder in die vorherige Konfiguration zurückgeführt.

```
====
[CAUTION]
====
*Bearbeiten und Deaktivieren.* Sobald SAML aktiviert ist, können Sie es
nicht über die Benutzeroberfläche deaktivieren, noch können Sie die IdP-
Einstellungen bearbeiten. Wenn Sie die SAML-Konfiguration deaktivieren
oder bearbeiten müssen, wenden Sie sich an den technischen Support, um
Hilfe zu erhalten.

====
Die Konfiguration der SAML-Authentifizierung erfolgt in mehreren
Schritten.



== Schritt 1: Laden Sie die IdP-Metadatendatei hoch

Um IdP-Verbindungsinformationen für das Storage-Array bereitzustellen,
importieren Sie IdP-Metadaten in Unified Manager. Das IdP-System benötigt
diese Metadaten, um Authentifizierungsanforderungen an die richtige URL
weiterzuleiten und die erhaltenen Antworten zu validieren.

.Schritte
. Wählen Sie Menü:Einstellungen[Zugriffsverwaltung].
. Wählen Sie die Registerkarte *SAML* aus.
+
Auf der Seite wird eine Übersicht der Konfigurationsschritte angezeigt.

. Klicken Sie auf den Link * Import Identity Provider (IdP) file*.
+
Das Dialogfeld „Datei des Identitätsanbieters importieren“ wird geöffnet.

. Klicken Sie auf *Durchsuchen*, um die IdP-Metadatendatei auszuwählen und
auf Ihr lokales System hochzuladen.
+
Nach der Auswahl der Datei wird die IdP-Entity-ID angezeigt.

. Klicken Sie Auf *Import*.



== Schritt 2: Exportieren Sie die Dateien des Dienstanbieters

Um eine Vertrauensbeziehung zwischen dem IdP und dem Storage-Array
herzustellen, importieren Sie die Metadaten des Service-Providers in das
IdP. Das IdP benötigt diese Metadaten, um eine Vertrauensbeziehung zum
```

Controller herzustellen und Autorisierungsanforderungen zu verarbeiten. Die Datei enthält Informationen wie den Domänennamen oder die IP-Adresse des Controllers, sodass das IdP mit den Service-Providern kommunizieren kann.

.Schritte
. Klicken Sie auf den Link *Export Service Provider Files*.
+
Das Dialogfeld Dateien des Dienstanbieters exportieren wird geöffnet.

. Geben Sie die Controller-IP-Adresse oder den DNS-Namen in das Feld *Controller A* ein, und klicken Sie dann auf *Exportieren*, um die Metadatendatei auf Ihrem lokalen System zu speichern.
+
Nachdem Sie auf *Export* geklickt haben, werden die Metadaten des Dienstanbieters auf Ihr lokales System heruntergeladen. Notieren Sie sich, wo die Datei gespeichert ist.

. Suchen Sie vom lokalen System aus die XML-formatierte Service Provider-Metadatendatei, die Sie exportiert haben.
. Importieren Sie vom IdP-Server die Metadatendatei des Dienstanbieters, um die Vertrauensbeziehung herzustellen. Sie können die Datei entweder direkt importieren oder die Controller-Informationen manuell aus der Datei eingeben.

== Schritt 3: Rollen zuordnen

Um Benutzern die Autorisierung und den Zugriff auf Unified Manager zu ermöglichen, müssen Sie die IdP-Benutzerattribute und Gruppenmitgliedschaften den vordefinierten Rollen des Speicherarrays zuordnen.

.Bevor Sie beginnen
* Ein IdP-Administrator hat Benutzerattribute und Gruppenmitgliedschaften im IdP-System konfiguriert.
* Die IdP-Metadatendatei wird in Unified Manager importiert.
* Für die Vertrauensstellung wird eine Service Provider-Metadatendatei für den Controller in das IdP-System importiert.

.Schritte
. Klicken Sie auf den Link für *Mapping Unified Manager*-Rollen.
+
Das Dialogfeld Rollenzuordnung wird geöffnet.

```
. Weisen Sie den vordefinierten Rollen IdP-Benutzerattribute und -Gruppen
zu. Einer Gruppe können mehrere Rollen zugewiesen sein.
+
.Felddetails
[%collapsible]
====
[cols="25h,~"]
|===
| Einstellung | Beschreibung


 a|
*Zuordnungen*



 a|
Benutzerattribut
 a|
Geben Sie das Attribut (z. B. „Mitglied von“) für die zuzuordnenden SAML-
Gruppe an.



 a|
Attributwert
 a|
Geben Sie den Attributwert für die zu zugeordnete Gruppe an. Reguläre
Ausdrücke werden unterstützt. Diese speziellen regulären Ausdruckszeichen
müssen mit einem umgekehrten Schrägstrich entgangen werden (`\`Wenn sie
nicht Teil eines regulären Ausdrucksmusters sind: \.[]{}()<>*+-=!?^



 a|
Rollen
 a|
Klicken Sie in das Feld, und wählen Sie eine der Rollen des Speicherarrays
aus, die dem Attribut zugeordnet werden sollen. Sie müssen jede Rolle
einzeln auswählen, die Sie einschließen möchten. Die Rolle Monitor ist
zusammen mit den anderen Rollen für die Anmeldung bei Unified Manager
erforderlich. Die Sicherheitsadministratorrolle ist auch für mindestens
eine Gruppe erforderlich.

Die zugeordneten Rollen umfassen die folgenden Berechtigungen:
```

** *Storage Admin* -- Vollzugriff auf die Speicherobjekte (z. B. Volumes und Disk Pools), aber kein Zugriff auf die Sicherheitskonfiguration.
** *Security Admin* -- Zugriff auf die Sicherheitskonfiguration in Access Management, Zertifikatverwaltung, Audit Log Management und die Möglichkeit, die alte Management-Schnittstelle (Symbol) ein- oder auszuschalten.
** *Support Admin* -- Zugriff auf alle Hardware-Ressourcen auf dem Speicher-Array, Ausfalldaten, MEL-Ereignisse und Controller-Firmware-Upgrades. Kein Zugriff auf Speicherobjekte oder die Sicherheitskonfiguration.
** *Monitor* -- schreibgeschützter Zugriff auf alle Speicherobjekte, aber kein Zugriff auf die Sicherheitskonfiguration.

|===
====
+
[NOTE]
====
Die Überwachungsrolle ist für alle Benutzer, einschließlich des Administrators, erforderlich. Unified Manager funktioniert für keinen Benutzer ordnungsgemäß, ohne dass die Überwachungsfunktion vorhanden ist.

====
. Klicken Sie auf *Weitere Zuordnungen hinzufügen*, um weitere Gruppen-zu-Rolle-Zuordnungen einzugeben.
+
[NOTE]
====
Rollenzuordnungen können geändert werden, nachdem SAML aktiviert ist.

====
. Wenn Sie mit den Zuordnungen fertig sind, klicken Sie auf *Speichern*.

== Schritt 4: SSO-Anmeldung testen

Um sicherzustellen, dass das IdP-System und das Speicherarray kommunizieren können, können Sie optional eine SSO-Anmeldung testen. Dieser Test wird auch während des letzten Schritts zur Aktivierung von SAML durchgeführt.

.Bevor Sie beginnen
* Die IdP-Metadatendatei wird in Unified Manager importiert.
* Für die Vertrauensstellung wird eine Service Provider-Metadatendatei für

den Controller in das IdP-System importiert.

.Schritte
. Klicken Sie auf den Link *SSO-Login testen*.
+
Zum Eingeben von SSO-Anmeldedaten wird ein Dialogfeld geöffnet.

. Geben Sie die Anmeldeinformationen für einen Benutzer mit Sicherheitsadministratorrechten und Überwachungsberechtigungen ein.
+
Ein Dialogfeld wird geöffnet, während das System die Anmeldung testet.

. Suchen Sie nach einer Meldung für den erfolgreichen Test. Wenn der Test erfolgreich abgeschlossen wurde, fahren Sie mit dem nächsten Schritt zur Aktivierung von SAML fort.
+
Wenn der Test nicht erfolgreich abgeschlossen wird, wird eine Fehlermeldung mit weiteren Informationen angezeigt. Stellen Sie sicher, dass:

+
** Der Benutzer gehört zu einer Gruppe mit Berechtigungen für Security Admin und Monitor.
** Die Metadaten, die Sie für den IdP-Server hochgeladen haben, sind korrekt.
** Die Controller-Adresse in den SP-Metadatendateien ist korrekt.

== Schritt 5: SAML aktivieren

Der letzte Schritt besteht darin, die SAML-Konfiguration für die Benutzerauthentifizierung abzuschließen. Während dieses Prozesses werden Sie vom System auch aufgefordert, eine SSO-Anmeldung zu testen. Der SSO-Anmelde-Test wird im vorherigen Schritt beschrieben.

.Bevor Sie beginnen
* Die IdP-Metadatendatei wird in Unified Manager importiert.
* Für die Vertrauensstellung wird eine Service Provider-Metadatendatei für den Controller in das IdP-System importiert.
* Mindestens ein Monitor und eine Sicherheitsadministratorzuordnung sind konfiguriert.

```
[CAUTION]
====
*Bearbeiten und Deaktivieren.* Sobald SAML aktiviert ist, können Sie es
nicht über die Benutzeroberfläche deaktivieren, noch können Sie die IdP-
Einstellungen bearbeiten. Wenn Sie die SAML-Konfiguration deaktivieren
oder bearbeiten müssen, wenden Sie sich an den technischen Support, um
Hilfe zu erhalten.

====
.Schritte
. Wählen Sie auf der Registerkarte *SAML* den Link *SAML* aktivieren.
+
Das Dialogfeld SAML aktivieren bestätigen wird geöffnet.

. Typ `enable`, Und klicken Sie dann auf *Aktivieren*.
. Geben Sie die Benutzeranmeldeinformationen für einen SSO-Anmeldetest
ein.


.Ergebnisse
Nachdem das System SAML aktiviert hat, werden alle aktiven Sitzungen
beendet und die Authentifizierung von Benutzern über SAML beginnt.



[[ID16988a5d681bdb1dbf953b74b0191417]]
= SAML-Rollenzuordnungen ändern
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Wenn Sie zuvor SAML für Access Management konfiguriert haben, können Sie
die Rollenzuordnungen zwischen den IdP-Gruppen und den vordefinierten
Rollen des Speicherarrays ändern.

.Bevor Sie beginnen
* Sie müssen mit einem Benutzerprofil angemeldet sein, das
Sicherheitsadministratorberechtigungen enthält. Andernfalls werden die
Zugriffsverwaltungsfunktionen nicht angezeigt.
* Ein IdP-Administrator hat Benutzerattribute und Gruppenmitgliedschaften
im IdP-System konfiguriert.
* SAML wurde konfiguriert und aktiviert.
```

```
.Schritte
. Wählen Sie Menü:Einstellungen[Zugriffsverwaltung].
. Wählen Sie die Registerkarte *SAML* aus.
. Wählen Sie *Rollenzuordnung*.
+
Das Dialogfeld Rollenzuordnung wird geöffnet.

. Weisen Sie den vordefinierten Rollen IdP-Benutzerattribute und -Gruppen
zu. Einer Gruppe können mehrere Rollen zugewiesen sein.
+
[CAUTION]
====
Achten Sie darauf, dass Sie Ihre Berechtigungen nicht entfernen, während
SAML aktiviert ist, sonst verlieren Sie den Zugriff auf Unified Manager.

====
+
.Felddetails
[%collapsible]
====
[cols="25h,~"]
|===
| Einstellung | Beschreibung


 a|
*Zuordnungen*



 a|
Benutzerattribut
 a|
Geben Sie das Attribut (z. B. „Mitglied von“) für die zuzuordnenden SAML-
Gruppe an.



 a|
Attributwert
 a|
Geben Sie den Attributwert für die zu zugeordnete Gruppe an.
```

```
 a|
Rollen
 a|
Klicken Sie in das Feld, und wählen Sie eine der Rollen des Speicherarrays
aus, die dem Attribut zugeordnet werden sollen. Sie müssen jede Rolle, die
Sie für diese Gruppe aufnehmen möchten, einzeln auswählen. Die Rolle
Monitor ist zusammen mit den anderen Rollen für die Anmeldung bei Unified
Manager erforderlich. Eine Sicherheitsadministratorrolle muss mindestens
einer Gruppe zugewiesen werden. Die zugeordneten Rollen umfassen die
folgenden Berechtigungen:

** *Storage Admin* -- Vollzugriff auf die Speicherobjekte (z. B. Volumes
und Disk Pools), aber kein Zugriff auf die Sicherheitskonfiguration.
** *Security Admin* -- Zugriff auf die Sicherheitskonfiguration in Access
Management, Zertifikatverwaltung, Audit Log Management und die
Möglichkeit, die alte Management-Schnittstelle (Symbol) ein- oder
auszuschalten.
** *Support Admin* -- Zugriff auf alle Hardware-Ressourcen auf dem
Speicher-Array, Ausfalldaten, MEL-Ereignisse und Controller-Firmware-
Upgrades. Kein Zugriff auf Speicherobjekte oder die
Sicherheitskonfiguration.
** *Monitor* -- schreibgeschützter Zugriff auf alle Speicherobjekte, aber
kein Zugriff auf die Sicherheitskonfiguration.


|===
====
+

NOTE: Die Überwachungsrolle ist für alle Benutzer, einschließlich des
Administrators, erforderlich. Unified Manager funktioniert für keinen
Benutzer ordnungsgemäß, ohne dass die Überwachungsfunktion vorhanden ist.

. Klicken Sie optional auf *Weitere Zuordnungen hinzufügen*, um weitere
Gruppen-zu-Rolle-Zuordnungen einzugeben.
. Klicken Sie Auf *Speichern*.


.Ergebnisse
Nach Abschluss dieser Aufgabe werden alle aktiven Benutzersitzungen
beendet. Nur Ihre aktuelle Benutzersitzung bleibt erhalten.



[[ID47380f05821a593c1645ad203b88af11]]
= Exportieren Sie SAML-Dienstanbieter-Dateien
:allow-uri-read:
```

```
:experimental:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Bei Bedarf können Sie Service-Provider-Metadaten für das Speicher-Array
exportieren und die Datei erneut in das Identity Provider (IdP)-System
importieren.

.Bevor Sie beginnen
* Sie müssen mit einem Benutzerprofil angemeldet sein, das
Sicherheitsadministratorberechtigungen enthält. Andernfalls werden die
Zugriffsverwaltungsfunktionen nicht angezeigt.
* SAML wurde konfiguriert und aktiviert.


.Über diese Aufgabe
In dieser Aufgabe exportieren Sie Metadaten vom Controller. Das IdP
benötigt diese Metadaten, um eine Vertrauensbeziehung zum Controller
herzustellen und Authentifizierungsanforderungen zu verarbeiten. Die Datei
enthält Informationen wie den Domänennamen des Controllers oder die IP-
Adresse, die das IdP zum Senden von Anforderungen verwenden kann.

.Schritte
. Wählen Sie Menü:Einstellungen[Zugriffsverwaltung].
. Wählen Sie die Registerkarte *SAML* aus.
. Wählen Sie *Export*.
+
Das Dialogfeld Dateien des Dienstanbieters exportieren wird geöffnet.

. Klicken Sie auf *Export*, um die Metadatendatei auf Ihrem lokalen System
zu speichern.
+
[NOTE]
====
Das Feld für den Domänennamen ist schreibgeschützt.

====
+
Notieren Sie sich, wo die Datei gespeichert ist.

. Suchen Sie vom lokalen System aus die XML-formatierte Service Provider-
Metadatendatei, die Sie exportiert haben.
. Importieren Sie vom IdP-Server die Metadatendatei des Dienstanbieters.
```

```
Sie können die Datei entweder direkt importieren oder die Controller-
Informationen manuell eingeben.
. Klicken Sie Auf *Schließen*.




:leveloffset: -1


= FAQs

:leveloffset: +1


[[IDda769de267f87478431b9926aa582990]]
= Warum kann ich mich nicht anmelden?
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Wenn Sie bei der Anmeldung einen Fehler erhalten, überprüfen Sie diese
möglichen Ursachen.

Aus einem der folgenden Gründe können Anmeldefehler auftreten:

* Sie haben einen falschen Benutzernamen oder ein falsches Passwort
eingegeben.
* Sie verfügen über unzureichende Berechtigungen.
* Sie haben mehrmals versucht, sich erfolglos anzumelden, was den
Sperrmodus ausgelöst hat. Warten Sie 10 Minuten, bis Sie sich erneut
anmelden können.
* SAML-Authentifizierung ist aktiviert. Aktualisieren Sie Ihren Browser,
um sich anzumelden.




[[IDfa44ecd859c205e097f0f26697d699b8]]
= Was muss ich vor dem Hinzufügen eines Verzeichnisservers wissen?
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
Bevor Sie einen Verzeichnisserver in Access Management hinzufügen, müssen
Sie bestimmte Anforderungen erfüllen.

* Benutzergruppen müssen in Ihrem Verzeichnisdienst definiert sein.
* LDAP-Serveranmeldeinformationen müssen verfügbar sein, einschließlich
Domänenname, Server-URL und optional Benutzername und Kennwort für das
Bindekonto.
* Bei LDAPS-Servern mit einem sicheren Protokoll muss die Zertifikatskette
des LDAP-Servers auf Ihrem lokalen Computer installiert sein.




[[ID5996ca1f56dcdf5e1f67e7a8ace832bf]]
= Was muss ich über die Zuordnung von Speicher-Array-Rollen wissen?
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Überprüfen Sie die Richtlinien, bevor Sie Gruppen zu Rollen zuordnen.

Die RBAC-Funktionen (rollenbasierte Zugriffssteuerung) umfassen folgende
Rollen:

* *Storage Admin* -- Vollständiger Lese-/Schreibzugriff auf
Speicherobjekte auf den Arrays, aber kein Zugriff auf die
Sicherheitskonfiguration.
* *Security Admin* -- Zugriff auf die Sicherheitskonfiguration in Access
Management und Certificate Management.
* *Support Admin* -- Zugriff auf alle Hardware-Ressourcen auf Speicher-
Arrays, Ausfalldaten und MEL-Ereignisse. Kein Zugriff auf Speicherobjekte
oder die Sicherheitskonfiguration.
* *Monitor* -- schreibgeschützter Zugriff auf alle Speicherobjekte, aber
kein Zugriff auf die Sicherheitskonfiguration.


[NOTE]
====
Die Überwachungsrolle ist für alle Benutzer, einschließlich des
Administrators, erforderlich.
```

```
====
Wenn Sie einen LDAP-Server (Lightweight Directory Access Protocol) und
Verzeichnisdienste verwenden, stellen Sie sicher, dass:

* Ein Administrator hat im Verzeichnisdienst Benutzergruppen definiert.
* Sie kennen die Gruppen-Domain-Namen für die LDAP-Benutzergruppen.




== SAML

Wenn Sie die im Speicher-Array integrierten SAML-Funktionen (Security
Assertion Markup Language) verwenden, stellen Sie sicher, dass:

* Ein IdP-Administrator (Identity Provider) hat im IdP-System
Benutzerattribute und Gruppenmitgliedschaften konfiguriert.
* Sie kennen die Namen der Gruppenmitgliedschaft.
* Sie kennen den Attributwert für die zu zugeordnete Gruppe. Reguläre
Ausdrücke werden unterstützt. Diese speziellen regulären Ausdruckszeichen
müssen mit einem umgekehrten Schrägstrich entgangen werden (`\`) Wenn sie
nicht Teil eines regulären Ausdrucksmusters sind:
+
[listing]
----
\.[]{}()<>*+-=!?^$|
----
* Die Überwachungsrolle ist für alle Benutzer, einschließlich des
Administrators, erforderlich. Unified Manager funktioniert für keinen
Benutzer ordnungsgemäß, ohne dass die Überwachungsfunktion vorhanden ist.




[[IDe0ab60b76cd5b712fef9c83fcb9514f7]]
= Was muss ich vor der Konfiguration und Aktivierung von SAML wissen?
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Bevor Sie die SAML-Funktionen (Security Assertion Markup Language) für die
Authentifizierung konfigurieren und aktivieren, müssen Sie sicherstellen,
dass Sie die folgenden Anforderungen erfüllen und SAML-Einschränkungen
verstehen.
```

== Anforderungen

Bevor Sie beginnen, stellen Sie sicher, dass:

* Ein Identitäts-Provider (IdP) ist in Ihrem Netzwerk konfiguriert. Ein IdP ist ein externes System, mit dem Anmeldeinformationen von einem Benutzer angefordert werden und festgestellt wird, ob der Benutzer erfolgreich authentifiziert wurde. Ihr Sicherheitsteam ist für die Instandhaltung des IdP verantwortlich.
* Ein IdP-Administrator hat Benutzerattribute und Gruppen im IdP-System konfiguriert.
* Ein IdP-Administrator hat sichergestellt, dass der IdP die Möglichkeit unterstützt, eine Name-ID bei der Authentifizierung zurückzugeben.
* Ein Administrator hat sichergestellt, dass der IdP-Server und die Controller-Uhr synchronisiert werden (entweder über einen NTP-Server oder durch Anpassung der Controller-Uhreinstellungen).
* Eine IdP-Metadatendatei wird vom IdP-System heruntergeladen und ist auf dem lokalen System verfügbar, auf dem der Zugriff auf Unified Manager erfolgt.
* Sie kennen die IP-Adresse oder den Domain-Namen des Controllers im Speicher-Array.

== Einschränkungen

Zusätzlich zu den oben genannten Anforderungen sollten Sie sich mit den folgenden Einschränkungen vertraut machen:

* Sobald SAML aktiviert ist, können Sie sie über die Benutzeroberfläche nicht deaktivieren oder die IdP-Einstellungen bearbeiten. Wenn Sie die SAML-Konfiguration deaktivieren oder bearbeiten müssen, wenden Sie sich an den technischen Support, um Hilfe zu erhalten. Es wird empfohlen, die SSO-Anmeldungen zu testen, bevor Sie SAML im letzten Konfigurationsschritt aktivieren. (Das System führt auch einen SSO-Anmeldetest vor Aktivierung von SAML durch.)
* Wenn Sie SAML zukünftig deaktivieren, stellt das System automatisch die vorherige Konfiguration wieder her (lokale Benutzerrollen und/oder Verzeichnisdienste).
* Wenn Verzeichnisdienste derzeit für die Benutzerauthentifizierung konfiguriert sind, überschreibt SAML diese Konfiguration.
* Wenn SAML konfiguriert ist, können die folgenden Clients nicht auf Speicher-Array-Ressourcen zugreifen:

```
+
** Enterprise Management-Fenster (EMW)
** Befehlszeilenschnittstelle (CLI)
** Software Developer Kits (SDK)-Clients
** In-Band-Clients
** REST-API-Clients für die HTTP-Standardauthentifizierung
** Melden Sie sich mithilfe des standardmäßigen REST-API-Endpunkts an




[[IDabbcb2dbd18105c8431a01b4ee4ac4cd]]
= Welche lokalen Benutzer gibt es?
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Lokale Benutzer sind im System vordefiniert und enthalten bestimmte
Berechtigungen.

Zu den lokalen Benutzern gehören:

* *Admin* -- Super-Administrator, der Zugriff auf alle Funktionen im
System hat. Dieser Benutzer enthält alle Rollen. Das Passwort muss bei der
ersten Anmeldung festgelegt werden.
* *Storage* -- der Administrator, der für die gesamte Storage-
Bereitstellung verantwortlich ist. Dieser Benutzer umfasst die folgenden
Rollen: Storage-Administrator, Support-Administrator und Monitor. Dieses
Konto wird deaktiviert, bis ein Kennwort festgelegt ist.
* *Sicherheit* -- der für die Sicherheitskonfiguration verantwortliche
Benutzer, einschließlich Zugriffsverwaltung und Zertifikatverwaltung.
Dieser Benutzer umfasst die folgenden Rollen: Security Admin und Monitor.
Dieses Konto wird deaktiviert, bis ein Kennwort festgelegt ist.
* *Support* -- der Benutzer, der für Hardware-Ressourcen, Ausfalldaten und
Firmware-Upgrades verantwortlich ist. Dieser Benutzer enthält die
folgenden Rollen: Unterstützen Sie Admin und Monitor. Dieses Konto wird
deaktiviert, bis ein Kennwort festgelegt ist.
* *Monitor* -- ein Benutzer mit schreibgeschütztem Zugriff auf das System.
Dieser Benutzer enthält nur die Rolle „Monitor“. Dieses Konto wird
deaktiviert, bis ein Kennwort festgelegt ist.
* *rw* (lesen/schreiben) -- dieser Benutzer enthält die folgenden Rollen:
Speicheradministrator, Supportadministrator und Monitor. Dieses Konto wird
```

deaktiviert, bis ein Kennwort festgelegt ist.
* *Ro* (schreibgeschützt) -- dieser Benutzer enthält nur die Rolle Monitor. Dieses Konto wird deaktiviert, bis ein Kennwort festgelegt ist.

:leveloffset: -1

:leveloffset: -1

:leveloffset: -1

:leveloffset: -1

<<<
Copyright-Informationen

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter link:http://www.netapp.com/TM\[http://www.netapp.com/TM^] aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.