Zugriffsmanagement

SANtricity 11.5

NetApp
February 12, 2024

Inhalt

Zugriffsmanagement

Konzepte

Funktionsweise von Access Management

Die Zugriffsverwaltung ist eine Methode zur Einrichtung der Benutzerauthentifizierung in SANtricity System Manager. Zur Authentifizierung müssen sich Benutzer bei diesen Systemen mit ihren zugewiesenen Anmeldedaten anmelden.

Die Konfiguration der Zugriffsverwaltung und die Benutzerauthentifizierung funktionieren wie folgt:

1. Ein Administrator meldet sich bei System Manager mit einem Benutzerprofil an, das die Berechtigungen für Sicherheitsadministrator enthält.

   > 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.

2. Der Administrator navigiert in der Benutzeroberfläche zur Zugriffsverwaltung. Das Storage Array ist vorkonfiguriert zur Verwendung von lokalen Benutzerrollen, bei denen es sich um die Implementierung von RBAC-Funktionen (rollenbasierte Zugriffssteuerung) handelt.
3. Der Administrator konfiguriert eine oder mehrere der folgenden Authentifizierungsmethoden:
   - **Lokale Benutzerrollen** — Authentifizierung wird über im Storage Array erzwungene RBAC-Funktionen gemanagt. Lokale Benutzerrollen umfassen vordefinierte Benutzerprofile und Rollen mit spezifischen 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 im Speicher-Array eingebetteten 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.
4. Der Administrator stellt Benutzern die Anmeldeinformationen für System Manager zur Verfügung.
5. Benutzer melden sich beim System an, indem sie ihre Anmeldedaten eingeben.

   > Wenn die Authentifizierung mit SAML und einem SSO (Single Sign On) verwaltet wird, umgehen das System möglicherweise das Anmeldedialogfeld von System Manager.

   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.

- Ermöglicht dem Benutzer den Zugriff auf Aufgaben in der Benutzeroberfläche.
- Zeigt den Benutzernamen oben rechts in der Schnittstelle an.

In System Manager verfügbare Aufgaben

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

- **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.

Eine nicht verfügbare Aufgabe ist entweder ausgegraut oder wird in der Benutzeroberfläche nicht angezeigt. Beispielsweise kann ein Benutzer mit der Rolle „Monitor“ alle Informationen zu Volumes anzeigen, jedoch keinen Zugriff auf Funktionen zum Ändern des Volumes haben. Die Registerkarten für Funktionen wie **Kopierdienste** und **zum Workload hinzufügen** sind ausgegraut; nur Einstellungen anzeigen/bearbeiten sind verfügbar.

Benutzerzugriff auf den SANtricity Storage Manager

Wenn lokale Benutzerrollen und Verzeichnisdienste konfiguriert sind, müssen Benutzer Anmeldeinformationen eingeben, bevor eine der folgenden Funktionen im Enterprise Management Window (EMW) ausgeführt wird:

- Umbenennen des Speicher-Arrays
- Aktualisieren der Controller-Firmware
- Laden einer Speicherarray-Konfiguration
- Ausführen eines Skripts
- Es wird versucht, einen aktiven Vorgang auszuführen, wenn eine nicht verwendete Sitzung abgelaufen ist

Wenn SAML für ein Speicher-Array konfiguriert ist, können Benutzer EMW nicht zum ermitteln oder Managen von Speicher für dieses Array verwenden.

Terminologie für das Zugriffsmanagement

Erfahren Sie, wie die Bedingungen für das Zugriffsmanagement auf Ihr Storage Array Anwendung finden.

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

Laufzeit	Beschreibung
Verbindlich	Bindevorgänge werden zur Authentifizierung von Clients auf dem Verzeichnisserver verwendet. Binding erfordert in der Regel Konto- und Kennwortanmeldeinformationen, aber einige Server erlauben anonyme Bindevorgänge.
CA	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.
Zertifikat	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).
IDP	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.
LDAP	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.
RBAC	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. RBAC-Kontrollen werden auf dem Storage Array durchgesetzt und umfassen vordefinierte Rollen.

Laufzeit	Beschreibung
SAML	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 integrierte SAML-Funktion des Speicherarrays ist SAML2.0-konform für Identitätsbehauptung, Authentifizierung und Autorisierung.
SP	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.
SSO	Bei Single Sign On (SSO) handelt es sich um einen Authentifizierungsservice, mit dem ein Satz an Anmeldeinformationen auf mehrere Anwendungen zugreifen kann.

Berechtigungen für zugeordnete Rollen

Die auf dem Storage-Array erzwungenen RBAC-Funktionen (rollenbasierte Zugriffssteuerung) umfassen vordefinierte Benutzerprofile, die mit einer oder mehreren zugewiesenen Rollen ausgestattet sind. Jede Rolle umfasst Berechtigungen für den Zugriff auf Aufgaben in SANtricity System Manager.

Auf Benutzerprofile und zugeordnete Rollen kann über das Menü:Einstellungen[Zugriffsmanagement > Lokale Benutzerrollen] in der Benutzeroberfläche eines System Managers zugegriffen werden.

Die Rollen ermöglichen Benutzern den Zugriff auf Aufgaben wie folgt:

- **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.

Wenn ein Benutzer über keine Berechtigungen für eine bestimmte Aufgabe verfügt, ist diese Aufgabe entweder ausgegraut oder wird nicht in der Benutzeroberfläche angezeigt.

Zugriffsverwaltung mit lokalen Benutzerrollen

Administratoren können für das Zugriffsmanagement die im Storage Array erzwungenen RBAC-Funktionen (rollenbasierte Zugriffssteuerung) nutzen. Diese Funktionen werden als „lokale Benutzerrollen“ bezeichnet.

Konfigurationsworkflow

Lokale Benutzerrollen sind für das Speicher-Array vorkonfiguriert. Um lokale Benutzerrollen für die Authentifizierung zu verwenden, können Administratoren Folgendes tun:

1. Ein Administrator meldet sich bei SANtricity System Manager mit einem Benutzerprofil an, das Berechtigungen für Sicherheitsadministratoren enthält.

   Der `admin` Der Benutzer hat vollen Zugriff auf alle Funktionen im System.

2. Ein Administrator überprüft die Benutzerprofile, die vordefiniert sind und nicht geändert werden können.
3. Optional weist der Administrator jedem Benutzerprofil neue Passwörter zu.
4. 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.

Zugriffsmanagement mit Verzeichnisdiensten

Für die Zugriffsverwaltung können Administratoren 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:

1. Ein Administrator meldet sich bei SANtricity System Manager mit einem Benutzerprofil an, das Berechtigungen für Sicherheitsadministratoren enthält.

   Der `admin` Der Benutzer hat vollen Zugriff auf alle Funktionen im System.

2. Der Administrator gibt die Konfigurationseinstellungen für den LDAP-Server ein. Zu den Einstellungen gehören der Domain-Name, die URL und die Bind-Kontoinformationen.
3. Wenn der LDAP-Server ein sicheres Protokoll (LDAPS) verwendet, lädt der Administrator eine Zertifikatskette für die Authentifizierung zwischen dem LDAP-Server und dem Speicher-Array hoch.

4. Nachdem die Serververbindung hergestellt wurde, ordnet der Administrator die Benutzergruppen den Rollen des Speicherarrays zu. Diese Rollen sind vordefiniert und können nicht geändert werden.
5. Der Administrator testet die Verbindung zwischen dem LDAP-Server und dem Speicher-Array.
6. 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.

Zugriffsmanagement mit SAML

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:

1. Ein Administrator meldet sich bei System Manager mit einem Benutzerprofil an, das die Berechtigungen für Sicherheitsadministrator enthält.

   Der `admin` Der Benutzer hat vollständigen Zugriff auf alle Funktionen in System Manager.

2. Der Administrator wechselt zur Registerkarte **SAML** unter Zugriffsverwaltung.
3. 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. Zum Konfigurieren der Kommunikation mit dem Storage-Array lädt der Administrator die IdP-Metadatendatei aus dem IdP-System herunter und lädt die Datei anschließend mit System Manager zum Hochladen auf das Storage-Array ein.
4. 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 System Manager zum Exportieren einer Service-Provider-Metadatendatei für jeden Controller. Aus dem IdP-System importiert der Administrator diese Metadatendateien in das IdP.

   Administratoren sollten außerdem sicherstellen, dass das IdP die Möglichkeit unterstützt, eine Name-ID bei der Authentifizierung zurückzugeben.

5. Der Administrator ordnet die Rollen des Storage-Arrays den in IdP definierten Benutzerattributen zu. Dazu verwendet der Administrator System Manager zum Erstellen der Zuordnungen.
6. Der Administrator testet die SSO-Anmeldung an der IdP-URL. Dieser Test stellt sicher, dass das Storage-Array und das IdP kommunizieren können.

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.

7. In System Manager aktiviert der Administrator SAML für das Storage-Array.
8. 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 die folgenden Clients nicht auf Storage-Array-Services und -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

Anleitungen

Zeigen Sie lokale Benutzerrollen an

Auf der Registerkarte Lokale Benutzerrollen können Sie die Zuordnungen der Benutzerprofile zu den Standardrollen anzeigen. Diese Zuordnungen sind Teil der RBAC (rollenbasierte Zugriffssteuerung), die im Storage Array 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 Benutzerprofile und Zuordnungen können nicht geändert werden. Es können nur Passwörter geändert werden.

Schritte

1. Wählen Sie Menü:Einstellungen[Zugriffsverwaltung].
2. Wählen Sie die Registerkarte * Lokale Benutzerrollen* aus.

   Die Benutzerprofile sind in der Tabelle aufgeführt:

- **Root Admin** (admin) — Super-Administrator, der Zugriff auf alle Funktionen im System hat. Dieses Benutzerprofil enthält alle Rollen.
- **Storage Admin** (Storage) — der Administrator für die gesamte Storage-Bereitstellung verantwortlich. Dieses Benutzerprofil umfasst die folgenden Rollen: Storage-Administrator, Support-Administrator und Monitor.
- **Security Admin** (Security) — der für die Sicherheitskonfiguration verantwortliche Benutzer, einschließlich Zugriffsverwaltung, Zertifikatverwaltung und Secure-Enabled Drive-Funktionen. Dieses Benutzerprofil umfasst die folgenden Rollen: Security Admin und Monitor.
- **Support Admin** (Support) — der Benutzer ist verantwortlich für Hardware-Ressourcen, Ausfalldaten und Firmware-Upgrades. Dieses Benutzerprofil umfasst die folgenden Rollen: Unterstützen Sie Admin und Monitor.
- **Monitor** (Monitor) — Ein Benutzer mit schreibgeschütztem Zugriff auf das System. Dieses Benutzerprofil enthält nur die Rolle Monitor.

Passwörter ändern

Sie können die Benutzerpasswörter für jedes Benutzerprofil in Access Management 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 von Kennwörtern entfernt, wenn sie eingestellt 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.

Durch Ändern des Passworts in System Manager wird es auch in der Befehlszeilenschnittstelle (CLI) geändert. Außerdem führen Kennwortänderungen dazu, dass die aktive Sitzung des Benutzers beendet wird.

Schritte

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

   Die Schaltfläche **Passwort ändern** steht zur Verfügung.

4. Wählen Sie **Passwort Ändern**.

   Das Dialogfeld **Passwort ändern** wird geöffnet.

5. Wenn für lokale Benutzerpasswörter keine Mindestkennwortlänge festgelegt ist, können Sie das Kontrollkästchen aktivieren, damit der ausgewählte Benutzer ein Kennwort für den Zugriff auf das Speicher-Array eingeben muss. Anschließend können Sie das neue Passwort für den ausgewählten Benutzer eingeben.
6. Geben Sie Ihr lokales Administratorpasswort ein und klicken Sie dann auf **Ändern**.

Ergebnis

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

Ändern Sie die Einstellungen für das lokale Benutzerpasswort

Sie können die erforderliche Mindestlänge für alle neuen oder aktualisierten lokalen Benutzerpasswörter im Speicher-Array festlegen. Sie können lokalen Benutzern auch ohne Eingabe eines Kennworts den Zugriff auf das Speicher-Array erlauben.

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 wirkt sich nicht auf vorhandene lokale Benutzerpasswörter aus.
- 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 Speicher-Array zugreifen möchten.

Schritte

1. Wählen Sie Menü:Einstellungen[Zugriffsverwaltung].
2. Wählen Sie die Registerkarte * Lokale Benutzerrollen* aus.
3. Wählen Sie die Schaltfläche **Einstellungen anzeigen/bearbeiten**.

   Das Dialogfeld **Lokale Benutzerpasswörteinstellungen** wird geöffnet.

4. Führen Sie einen der folgenden Schritte aus:
   - Um lokalen Benutzern den Zugriff auf das Speicher-Array 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“ und 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.

5. Klicken Sie Auf **Speichern**.

Verzeichnisserver hinzufügen

Um die Authentifizierung für die Zugriffsverwaltung zu konfigurieren, können Sie die Kommunikation zwischen dem Speicher-Array und einem LDAP-Server herstellen und die LDAP-Benutzergruppen den vordefinierten Rollen des Arrays zuordnen.

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 den vordefinierten Rollen des Speicher-Arrays zugeordnet.

> ⓘ Während des Verfahrens zum Hinzufügen eines LDAP-Servers wird die alte Verwaltungsschnittstelle deaktiviert. Die alte Managementoberfläche (Symbol) ist eine Methode der Kommunikation zwischen dem Storage-Array und dem Management-Client. Wenn die Option deaktiviert ist, nutzen das Storage-Array und der Management-Client eine sicherere Kommunikationsmethode (REST-API über HTTPS).

Schritte

1. Wählen Sie Menü:Einstellungen[Zugriffsverwaltung].
2. Wählen Sie auf der Registerkarte **Directory Services** die Option **Add Directory Server** aus.

   Das Dialogfeld **Directory Server hinzufügen** wird geöffnet.

3. Geben Sie auf der Registerkarte **Server-Einstellungen** die Anmeldeinformationen für den LDAP-Server ein.

Felddetails

Einstellung	Beschreibung
Konfigurationseinstellungen	Domäne(en)
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.	Server-URL
Geben Sie die URL für den Zugriff auf den LDAP-Server in Form von ein `ldap[s]://` *`host:port`*.	Zertifikat hochladen (optional)
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.	Konto binden (optional)
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-Benutzer“ heißt, können Sie einen Wert wie „CN=bindact,CN=users,DC=cpoc,DC=local“ eingeben.	Bindepasswort (optional)
Dieses Feld wird angezeigt, wenn Sie oben ein Bindungskonto eingeben. Geben Sie das Passwort für das Bindekonto ein.	Testen Sie die Serververbindung, bevor Sie sie hinzufügen

Einstellung	Beschreibung
Aktivieren Sie dieses Kontrollkästchen, wenn Sie sicherstellen möchten, dass das Speicher-Array 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.	**Berechtigungs-Einstellungen**
Basis-DN suchen	Geben Sie den LDAP-Kontext ein, um nach Benutzern zu suchen, normalerweise in Form von `CN=Users, DC=copc, DC=local`.
Attribut Benutzername	Geben Sie das Attribut ein, das zur Authentifizierung an die Benutzer-ID gebunden ist. Beispiel: `sAMAccountName`.
Gruppenattribut(e)	Geben Sie eine Liste der Gruppenattribute für den Benutzer ein, die für die Zuordnung von Gruppen zu Rollen verwendet werden. Beispiel: `memberOf, managedObjects`.

4. Klicken Sie auf die Registerkarte **Rollenzuordnung**.
5. Weisen Sie den vordefinierten Rollen LDAP-Gruppen zu. Einer Gruppe können mehrere Rollen zugewiesen sein.

Felddetails

Einstellung	Beschreibung
Zuordnungen	Gruppen-DN
Geben Sie den Group Distinguished Name (DN) für die zu zugeordnete LDAP-Benutzergruppe an.	Rollen

Die Überwachungsrolle ist für alle Benutzer, einschließlich des Administrators, erforderlich. Der System Manager funktioniert ohne die vorhandene Monitorrolle nicht ordnungsgemäß für alle Benutzer.

6. Klicken Sie auf **Weitere Zuordnungen hinzufügen**, um weitere Gruppen-zu-Rolle-Zuordnungen einzugeben.
7. 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.

Bearbeiten Sie die Einstellungen des Verzeichnisservers und die Rollenzuordnungen

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

1. Wählen Sie Menü:Einstellungen[Zugriffsverwaltung].
2. Wählen Sie die Registerkarte **Directory Services** aus.
3. Wenn mehr als ein Server definiert ist, wählen Sie den Server aus der Tabelle aus, den Sie bearbeiten möchten.
4. Wählen Sie **Einstellungen Anzeigen/Bearbeiten**.

   Das Dialogfeld **Directory Server Settings** wird geöffnet.

5. Ändern Sie auf der Registerkarte **Server-Einstellungen** die gewünschten Einstellungen.

Einstellung	Beschreibung
Konfigurationseinstellungen	Domäne(en)
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.	Server-URL
Die URL für den Zugriff auf den LDAP-Server in Form von `ldap[s]://host:port`.	Konto binden (optional)
Das schreibgeschützte Benutzerkonto für Suchabfragen am LDAP-Server und für die Suche in den Gruppen.	Bindepasswort (optional)
Das Kennwort für das Bindekonto. (Dieses Feld wird angezeigt, wenn ein Bindekonto eingegeben wird.)	Testen Sie vor dem Speichern die Serververbindung

Einstellung	Beschreibung
Überprüft, ob das Speicher-Array mit der LDAP-Serverkonfiguration kommunizieren kann. Der Test wird ausgeführt, nachdem Sie unten im Dialogfeld auf Speichern geklickt haben. 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.	**Berechtigungseinstellungen**
Basis-DN suchen	Der LDAP-Kontext für die Suche nach Benutzern, in der Regel in Form von `CN=Users, DC=copc, DC=local`.
Attribut Benutzername	Das Attribut, das zur Authentifizierung an die Benutzer-ID gebunden ist. Beispiel: `sAMAccountName`.
Gruppenattribut(e)	Eine Liste der Gruppenattribute für den Benutzer, die für die Zuordnung von Gruppen zu Rollen verwendet werden. Beispiel: `memberOf, managedObjects`.

6. Ändern Sie auf der Registerkarte **Rollenzuordnung** die gewünschte Zuordnung.

Einstellung	Beschreibung
Zuordnungen	Gruppen-DN
Der Domain-Name für die LDAP-Benutzergruppe, die zugeordnet werden soll.	Rollen

> Die Überwachungsrolle ist für alle Benutzer, einschließlich des Administrators, erforderlich. Der System Manager funktioniert ohne die vorhandene Monitorrolle nicht ordnungsgemäß für alle Benutzer.

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

Ergebnis

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

Verzeichnisserver entfernen

Um die Verbindung zwischen einem Verzeichnisserver und dem Speicher-Array 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

1. Wählen Sie Menü:Einstellungen[Zugriffsverwaltung].
2. Wählen Sie die Registerkarte **Directory Services** aus.
3. Wählen Sie in der Liste den Verzeichnisserver aus, den Sie löschen möchten.
4. Klicken Sie Auf **Entfernen**.

   Das Dialogfeld **Directory Server entfernen** wird geöffnet.

5. 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.

Konfigurieren Sie SAML

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.

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.

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

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
- Schritt 2: Exportieren Sie die Dateien des Dienstanbieters
- Schritt 3: Rollen zuordnen
- Schritt 4: SSO-Anmeldung testen
- Schritt 5: SAML aktivieren

Schritt 1: Laden Sie die IdP-Metadatendatei hoch

Um das Storage-Array mit IdP-Verbindungsinformationen bereitzustellen, importieren Sie IdP-Metadaten in System Manager.

Bevor Sie beginnen

- Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden die Zugriffsverwaltungsfunktionen nicht angezeigt.
- 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 die IdP-Server- und -Controller-Uhren synchronisiert werden (entweder über einen NTP-Server oder durch Anpassen der Controller-Uhreinstellungen).
- Eine IdP-Metadatendatei wird vom IdP-System heruntergeladen und ist auf dem lokalen System verfügbar, das für den Zugriff auf System Manager verwendet wird.

Über diese Aufgabe

In dieser Aufgabe laden Sie eine Metadatendatei aus dem IdP in den System Manager hoch. Das IdP-System benötigt diese Metadaten, um Authentifizierungsanforderungen an die richtige URL weiterzuleiten und die erhaltenen Antworten zu validieren. Sie müssen nur eine Metadatendatei für das Storage-Array hochladen, selbst wenn es zwei Controller gibt.

Schritte

1. Wählen Sie Menü:Einstellungen[Zugriffsverwaltung].
2. Wählen Sie die Registerkarte **SAML** aus.

   Auf der Seite wird eine Übersicht der Konfigurationsschritte angezeigt.

3. Klicken Sie auf den Link * Import Identity Provider (IdP) file*.

Das Dialogfeld **Import Identity Provider File** wird geöffnet.

4. 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.

5. 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.

Bevor Sie beginnen

- Sie kennen die IP-Adresse oder den Domain-Namen der einzelnen Controller im Storage-Array.

Über diese Aufgabe

In dieser Aufgabe exportieren Sie Metadaten aus den Controllern (eine Datei für jeden Controller). Die IdP benötigt diese Metadaten, um eine Vertrauensbeziehung zu den Controllern aufzubauen und Autorisierungsanforderungen zu bearbeiten. Die Datei enthält Informationen wie den Domänennamen oder die IP-Adresse des Controllers, sodass das IdP mit den Service-Providern kommunizieren kann.

Schritte

1. Klicken Sie auf den Link **Export Service Provider Files**.

   Das Dialogfeld **Export Service Provider Files** wird geöffnet.

2. 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. Wenn das Speicher-Array zwei Controller enthält, wiederholen Sie diesen Schritt für den zweiten Controller im Feld **Controller B**.

   Nachdem Sie auf Exportieren geklickt haben, werden die Metadaten des Dienstanbieters auf Ihr lokales System heruntergeladen. Notieren Sie sich, wo die Datei gespeichert ist.

3. Suchen Sie im lokalen System die Metadatendatei(en) des Serviceanbieters, die Sie exportiert haben.

   Es gibt eine XML-formatierte Datei für jeden Controller.

4. Importieren Sie vom IdP-Server die Metadatendatei(en) des Dienstanbieters, um die Vertrauensbeziehung herzustellen. Sie können die Dateien entweder direkt importieren oder manuell die Controller-Informationen aus den Dateien eingeben.

Schritt 3: Rollen zuordnen

Um Benutzern Autorisierung und Zugriff auf System 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 System Manager importiert.
- Für die Vertrauensbeziehung wird für jeden Controller eine Metadatendatei des Dienstanbieters in das IdP-System importiert.

Über diese Aufgabe

In dieser Aufgabe verwenden Sie System Manager, um IdP-Gruppen den lokalen Benutzerrollen zuzuordnen.

Schritte

1. Klicken Sie auf den Link, um System Manager-Rollen zuzuordnen.

   Das Dialogfeld **Rollenzuordnung** wird geöffnet.

2. Weisen Sie den vordefinierten Rollen IdP-Benutzerattribute und -Gruppen zu. Einer Gruppe können mehrere Rollen zugewiesen sein.

   Felddetails

Einstellung	Beschreibung
Zuordnungen	Benutzerattribut
Geben Sie das Attribut (z. B. „Mitglied von“) für die zuzuordnenden SAML-Gruppe an.	Attributwert
Geben Sie den Attributwert für die zu zugeordnete Gruppe an.	Rollen

   Die Überwachungsrolle ist für alle Benutzer, einschließlich des Administrators, erforderlich. Der System Manager funktioniert ohne die vorhandene Monitorrolle nicht ordnungsgemäß für alle Benutzer.

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

   Rollenzuordnungen können geändert werden, nachdem SAML aktiviert ist.

4. 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 System Manager importiert.
- Für die Vertrauensbeziehung wird für jeden Controller eine Metadatendatei des Dienstanbieters in das IdP-System importiert.

Schritte

1. Klicken Sie auf den Link **SSO-Login testen**.

   Zum Eingeben von SSO-Anmeldedaten wird ein Dialogfeld geöffnet.

2. Geben Sie die Anmeldeinformationen für einen Benutzer mit Sicherheitsadministratorrechten und Überwachungsberechtigungen ein.

   Ein Dialogfeld wird geöffnet, während das System die Anmeldung testet.

3. 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-Adressen in den SP-Metadatendateien sind korrekt.

Schritt 5: SAML aktivieren

Ihr letzter Schritt ist die Aktivierung der SAML-Benutzerauthentifizierung.

Bevor Sie beginnen

- Die IdP-Metadatendatei wird in System Manager importiert.
- Für die Vertrauensbeziehung wird für jeden Controller eine Metadatendatei des Dienstanbieters in das IdP-System importiert.
- Mindestens ein Monitor und eine Sicherheitsadministratorzuordnung sind konfiguriert.

Über diese Aufgabe

In dieser Aufgabe wird beschrieben, wie die SAML-Konfiguration für die Benutzerauthentifizierung abgeschlossen wird. Während dieses Prozesses werden Sie vom System auch aufgefordert, eine SSO-Anmeldung zu testen. Der SSO-Anmelde-Test wird im vorherigen Schritt beschrieben.

> **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

1. Wählen Sie auf der Registerkarte **SAML** den Link **SAML** aktivieren.

   Das Dialogfeld **SAML aktivieren** wird geöffnet.

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

Ergebnis

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

SAML-Rollenzuordnungen ändern

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

1. Wählen Sie Menü:Einstellungen[Zugriffsverwaltung].
2. Wählen Sie die Registerkarte **SAML** aus.
3. Wählen Sie **Rollenzuordnung**.

   Das Dialogfeld **Rollenzuordnung** wird geöffnet.

4. Weisen Sie den vordefinierten Rollen IdP-Benutzerattribute und -Gruppen zu. Einer Gruppe können mehrere Rollen zugewiesen sein.

   Achten Sie darauf, dass Sie Ihre Berechtigungen nicht entfernen, während SAML aktiviert ist, oder Sie verlieren den Zugriff auf System Manager.

   Felddetails

Einstellung	Beschreibung
Zuordnungen	Benutzerattribut
Geben Sie das Attribut (z. B. „Mitglied von“) für die zuzuordnenden SAML-Gruppe an.	Attributwert
Geben Sie den Attributwert für die zu zugeordnete Gruppe an.	Rollen

   Die Überwachungsrolle ist für alle Benutzer, einschließlich des Administrators, erforderlich. Der System Manager funktioniert ohne die vorhandene Monitorrolle nicht ordnungsgemäß für alle Benutzer.

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

Ergebnis

Nach Abschluss dieser Aufgabe werden alle aktiven Benutzersitzungen beendet. Nur Ihre aktuelle

Benutzersitzung bleibt erhalten.

Exportieren Sie SAML-Dienstanbieter-Dateien

Bei Bedarf können die Metadaten von Service-Providern für das Storage-Array exportiert und die Datei(en) in das IdP-System (Identity Provider) importiert werden.

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 aus den Controllern (eine Datei für jeden Controller). Die IdP benötigt diese Metadaten, um eine Vertrauensbeziehung zu den Controllern aufzubauen 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

1. Wählen Sie Menü:Einstellungen[Zugriffsverwaltung].
2. Wählen Sie die Registerkarte **SAML** aus.
3. Wählen Sie **Export**.

   Das Dialogfeld **Export Service Provider Files** wird geöffnet.

4. Klicken Sie für jeden Controller auf **Exportieren**, um die Metadatendatei auf Ihrem lokalen System zu speichern.

   Die Domain-Name-Felder für jeden Controller sind schreibgeschützt.

   Notieren Sie sich, wo die Datei gespeichert ist.

5. Suchen Sie im lokalen System die Metadatendatei(en) des Serviceanbieters, die Sie exportiert haben.

   Es gibt eine XML-formatierte Datei für jeden Controller.

6. Importieren Sie vom IdP-Server die Metadatendatei(en) des Dienstanbieters. Sie können die Dateien entweder direkt importieren oder manuell die Controller-Informationen von ihnen eingeben.
7. Klicken Sie Auf **Schließen**.

Zeigen Sie die Aktivität des Prüfprotokolls an

Durch die Anzeige von Prüfprotokollen können Benutzer mit Sicherheitsadministratorberechtigungen Benutzeraktionen, Authentifizierungsfehler, ungültige Anmeldeversuche und die Lebensdauer der Benutzersitzung überwachen.

Bevor Sie beginnen

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

Schritte

1. Wählen Sie Menü:Einstellungen[Zugriffsverwaltung].
2. Wählen Sie die Registerkarte **Prüfprotokoll** aus.

   Prüfprotokoll-Aktivität erscheint im Tabellenformat, das die folgenden Informationspalten enthält:

   - **Datum/Uhrzeit** — Zeitstempel, wann das Speicherarray das Ereignis erkannt hat (in GMT).
   - **Benutzername** — der Benutzername, der dem Ereignis zugeordnet ist. Bei nicht authentifizierten Aktionen im Speicher-Array wird „N/A“ als Benutzername angezeigt. Nicht authentifizierte Aktionen können vom internen Proxy oder einem anderen Mechanismus ausgelöst werden.
   - **Statuscode** — HTTP-Statuscode der Operation (200, 400 usw.) und beschreibenden Text, der dem Ereignis zugeordnet ist.
   - **URL abgerufen** — vollständige URL (einschließlich Host) und Abfragezeichenfolge.
   - **Client-IP-Adresse** — IP-Adresse des Clients, der dem Ereignis zugeordnet ist.
   - **Quelle** — Logging-Quelle, die mit dem Ereignis verknüpft ist, kann System Manager, CLI, Web Services oder Support Shell sein.
3. Verwenden Sie die Auswahl auf der Seite „Überwachungsprotokoll“, um Ereignisse anzuzeigen und zu verwalten.

Auswahldetails

Auswahl	Beschreibung
Zeigt Ereignisse aus dem…	Grenzwerte für Ereignisse, die nach Datumsbereich angezeigt werden (letzte 24 Stunden, letzte 7 Tage, letzte 30 Tage oder ein benutzerdefinierter Datumsbereich).
Filtern	Begrenzungsereignisse, die durch die in das Feld eingegebenen Zeichen angezeigt werden. Verwenden Sie Anführungszeichen (") für eine genaue Wortabgleiche, geben Sie ein `OR` Um ein oder mehrere Wörter zurückzugeben, oder geben Sie einen Bindestrich (--) ein, um Wörter auszulassen.
Aktualisierung	Wählen Sie **Aktualisieren**, um die Seite auf die aktuellen Ereignisse zu aktualisieren.
Einstellungen Anzeigen/Bearbeiten	Wählen Sie **Einstellungen anzeigen/bearbeiten** aus, um ein Dialogfeld zu öffnen, in dem Sie eine vollständige Protokollrichtlinie und eine Ebene der zu protokollierenden Aktionen festlegen können.
Löschen von Ereignissen	Wählen Sie **Löschen** aus, um ein Dialogfeld zu öffnen, in dem Sie alte Ereignisse von der Seite entfernen können.
Spalten ein-/ausblenden	Klicken Sie auf das Spaltensymbol **ein-/ausblenden** So wählen Sie zusätzliche Spalten aus, die in der Tabelle angezeigt werden sollen. Weitere Spalten sind: • **Methode** — die HTTP-Methode (z. B. POST, GET, DELETE usw.). • **CLI Befehl ausgeführt** — der CLI-Befehl (Grammatik) ausgeführt für Secure CLI Anfragen. • **CLI Rückgabestatus** — Ein CLI-Statuscode oder eine Anforderung für Eingabedateien vom Client. • **Symbol-Verfahren** — das Symbol-Verfahren ausgeführt. • **SSH Event Type** — Secure Shell (SSH) Ereignistyp, wie Login, Logout und Login_fail. • **SSH Session PID** — Prozess-ID-Nummer der SSH-Sitzung. • **SSH Sitzungsdauer(en)** — die Anzahl der Sekunden, die der Benutzer angemeldet war.
Spaltenfilter ein- oder ausschalten	Klicken Sie auf das Symbol **Umschalten** Zum Öffnen von Filterfeldern für jede Spalte. Geben Sie in ein Spaltenfeld Zeichen ein, um die durch diese Zeichen angezeigten Ereignisse einzuschränken. Klicken Sie erneut auf das Symbol, um die Filterfelder zu schließen.
Änderungen rückgängig machen	Klicken Sie auf das Symbol **Rückgängig** Um die Tabelle auf die Standardkonfiguration zurückzugeben.

Auswahl	Beschreibung
Exportieren	Klicken Sie auf **Exportieren**, um die Tabellendaten in einer kommagetrennten Datei (CSV) zu speichern.

Richtlinien für Prüfprotokolle definieren

Sie können die Überschreibungsrichtlinie und die im Audit-Protokoll aufgezeichneten Ereignistypen ändern.

Bevor Sie beginnen

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

Über diese Aufgabe

Dieser Task beschreibt, wie die Einstellungen für das Überwachungsprotokoll geändert werden, einschließlich der Richtlinie zum Überschreiben alter Ereignisse und der Richtlinie für die Aufzeichnung von Ereignistypen.

Schritte

1. Wählen Sie Menü:Einstellungen[Zugriffsverwaltung].
2. Wählen Sie die Registerkarte **Prüfprotokoll** aus.
3. Wählen Sie **Einstellungen Anzeigen/Bearbeiten**.

   Das Dialogfeld **Audit Log Settings** wird geöffnet.

4. Ändern Sie die Überschreibungsrichtlinie oder die Arten der aufgezeichneten Ereignisse.

Felddetails

Einstellung	Beschreibung
Überschreibungsrichtlinie	Legt die Richtlinie zum Überschreiben alter Ereignisse fest, wenn die maximale Kapazität erreicht ist: • **Die ältesten Ereignisse im Audit-Protokoll können überschrieben werden, wenn das Audit-Protokoll voll ist** — überschreibt die alten Ereignisse, wenn das Audit-Protokoll 50,000 Datensätze erreicht. • **Das manuelle Löschen von Audit-Protokollereignissen ist erforderlich** — gibt an, dass Ereignisse nicht automatisch gelöscht werden; stattdessen erscheint eine Schwellenwertwarnung im festgelegten Prozentsatz. Ereignisse müssen manuell gelöscht werden. Wenn die Überschreibungsrichtlinie deaktiviert ist und die Einträge des Prüfprotokolls die maximale Grenze erreichen, wird Benutzern der Zugriff auf System Manager ohne die Berechtigung des Sicherheitsadministrators verweigert. Um den Systemzugriff für Benutzer ohne Sicherheitsadministrator-Berechtigungen wiederherzustellen, muss ein Benutzer, der der Rolle Sicherheitsadministrator zugewiesen ist, die alten Ereignisdatensätze löschen. Überschreibungsrichtlinien gelten nicht, wenn ein Syslog-Server für die Archivierung von Audit-Protokollen konfiguriert ist.

Einstellung	Beschreibung
Level der zu protokollierenden Aktionen	Legt die Arten von zu protokollierenden Ereignissen fest: • **Änderungsereignisse aufzeichnen** — zeigt nur Ereignisse an, bei denen eine Benutzeraktion eine Systemänderung beinhaltet. • **Alle Änderungen und schreibgeschützten Ereignisse** — zeigt alle Ereignisse an, einschließlich einer Benutzeraktion, die das Lesen oder Herunterladen von Informationen beinhaltet.

5. Klicken Sie Auf **Speichern**.

Löschen von Ereignissen aus dem Auditprotokoll

Sie können das Audit-Protokoll von alten Ereignissen löschen, wodurch das Suchen durch Ereignisse leichter zu verwalten ist. Sie haben die Möglichkeit, alte Ereignisse beim Löschen in einer CSV-Datei (kommagetrennte Werte) zu speichern.

Bevor Sie beginnen

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

Über diese Aufgabe

Diese Aufgabe beschreibt, wie alte Ereignisse aus dem Prüfprotokoll entfernt werden.

Schritte

1. Wählen Sie Menü:Einstellungen[Zugriffsverwaltung].
2. Wählen Sie die Registerkarte **Prüfprotokoll** aus.
3. Wählen Sie **Löschen**.

   Das Dialogfeld **Prüfprotokoll löschen** wird geöffnet.

4. Wählen Sie oder geben Sie die Anzahl der ältesten Ereignisse ein, die Sie löschen möchten.
5. Wenn Sie die gelöschten Ereignisse in eine CSV-Datei exportieren möchten (empfohlen), lassen Sie das Kontrollkästchen aktiviert. Sie werden aufgefordert, einen Dateinamen und Speicherort einzugeben, wenn Sie im nächsten Schritt auf **Löschen** klicken. Wenn Sie keine Ereignisse in einer CSV-Datei speichern möchten, aktivieren Sie das Kontrollkästchen, um die Auswahl aufzuheben.
6. Klicken Sie Auf **Löschen**.

   Ein Bestätigungsdialogfeld wird geöffnet.

7. Typ `delete` Klicken Sie im Feld auf **Löschen**.

   Die ältesten Ereignisse werden von der Seite „Überwachungsprotokoll“ entfernt.

Syslog-Server für Audit-Protokolle konfigurieren

Wenn Sie Auditprotokolle auf einem externen Syslog-Server archivieren möchten, können Sie die Kommunikation zwischen diesem Server und dem Speicher-Array konfigurieren. Nach der Verbindungsherstellung werden Audit-Protokolle automatisch auf dem Syslog-Server gespeichert.

Bevor Sie beginnen

- Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden die Zugriffsverwaltungsfunktionen nicht angezeigt.
- Die Syslog-Serveradresse, das Protokoll und die Portnummer müssen verfügbar sein. Bei der Serveradresse kann es sich um einen vollständig qualifizierten Domänennamen, eine IPv4-Adresse oder eine IPv6-Adresse handeln.
- Wenn Ihr Server ein sicheres Protokoll verwendet (z. B. TLS), muss auf Ihrem lokalen System ein Zertifikat für Zertifizierungsstellen (CA) verfügbar sein. CA-Zertifikate identifizieren Website-Eigentümer für sichere Verbindungen zwischen Servern und Clients.

Schritte

1. Wählen Sie Menü:Einstellungen[Zugriffsverwaltung].
2. Wählen Sie auf der Registerkarte **Audit Log** die Option **Configure Syslog Servers** aus.

   Das Dialogfeld **Syslog Server konfigurieren** wird geöffnet.

3. Klicken Sie Auf **Hinzufügen**.

   Das Dialogfeld **Syslog Server** hinzufügen wird geöffnet.

4. Geben Sie Informationen für den Server ein, und klicken Sie dann auf **Hinzufügen**.
   - Serveradresse — Geben Sie einen vollständig qualifizierten Domänennamen, eine IPv4-Adresse oder eine IPv6-Adresse ein.
   - Protokoll — Wählen Sie ein Protokoll aus der Dropdown-Liste aus (z. B. TLS, UDP oder TCP).
   - Zertifikat hochladen (optional) – Wenn Sie das TLS-Protokoll ausgewählt haben und noch kein signiertes CA-Zertifikat hochgeladen haben, klicken Sie auf Durchsuchen, um eine Zertifikatdatei hochzuladen. Audit-Protokolle werden nicht ohne vertrauenswürdiges Zertifikat auf einem Syslog-Server archiviert.

     > Wenn das Zertifikat später ungültig wird, schlägt der TLS-Handshake fehl. Als Ergebnis wird eine Fehlermeldung in das Auditprotokoll geschrieben und Meldungen werden nicht mehr an den Syslog-Server gesendet. Um dieses Problem zu lösen, müssen Sie das Zertifikat auf dem Syslog-Server beheben und dann zum Menü:Einstellungen[Audit-Protokoll > Syslog-Server konfigurieren > Alle testen] wechseln.

   - Port — Geben Sie die Portnummer für den Syslog-Empfänger ein. Nach dem Klicken auf **Hinzufügen** wird das Dialogfeld **Syslog Server konfigurieren** geöffnet und der konfigurierte Syslog-Server auf der Seite angezeigt.
5. Um die Serververbindung mit dem Speicher-Array zu testen, wählen Sie **Alle testen**.

Ergebnis

Nach der Konfiguration werden alle neuen Audit-Protokolle an den Syslog-Server gesendet. Frühere Protokolle

werden nicht übertragen.

Bearbeiten Sie die Syslog-Servereinstellungen für Audit-Protokolldatensätze

Sie können die Einstellungen für den Syslog-Server ändern, der für die Archivierung von Audit-Protokollen verwendet wird, und auch ein neues Zertifikat für die Zertifizierungsstelle (Certificate Authority, CA) für den Server hochladen.

Bevor Sie beginnen

- Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden die Zugriffsverwaltungsfunktionen nicht angezeigt.
- Die Syslog-Serveradresse, das Protokoll und die Portnummer müssen verfügbar sein. Bei der Serveradresse kann es sich um einen vollständig qualifizierten Domänennamen, eine IPv4-Adresse oder eine IPv6-Adresse handeln.
- Wenn Sie ein neues CA-Zertifikat hochladen, muss das Zertifikat auf Ihrem lokalen System verfügbar sein.

Schritte

1. Wählen Sie Menü:Einstellungen[Zugriffsverwaltung].
2. Wählen Sie auf der Registerkarte **Audit Log** die Option **Configure Syslog Servers** aus.

   Konfigurierte Syslog-Server werden auf der Seite angezeigt.

3. Um die Serverinformationen zu bearbeiten, wählen Sie rechts neben dem Servernamen das Symbol **Bearbeiten** (Bleistift) aus und nehmen Sie die gewünschten Änderungen in den folgenden Feldern vor:
   - Serveradresse — Geben Sie einen vollständig qualifizierten Domänennamen, eine IPv4-Adresse oder eine IPv6-Adresse ein.
   - Protokoll — Wählen Sie ein Protokoll aus der Dropdown-Liste aus (z. B. TLS, UDP oder TCP).
   - Port — Geben Sie die Portnummer für den Syslog-Empfänger ein.
4. Wenn Sie das Protokoll in das sichere TLS-Protokoll (entweder von UDP oder TCP) geändert haben, klicken Sie auf **Vertrautes Zertifikat importieren**, um ein CA-Zertifikat hochzuladen.
5. Um die neue Verbindung mit dem Speicher-Array zu testen, wählen Sie **Alle testen**.

Ergebnis

Nach der Konfiguration werden alle neuen Audit-Protokolle an den Syslog-Server gesendet. Frühere Protokolle werden nicht übertragen.

FAQs

Warum kann ich mich nicht anmelden?

Wenn Sie beim Versuch, sich bei System Manager anzumelden, einen Fehler erhalten, überprüfen Sie die möglichen Ursachen.

Fehler beim Anmelden bei System Manager können aus einem der folgenden Gründe auftreten:

- Sie haben einen falschen Benutzernamen oder ein falsches Passwort eingegeben.
- Sie verfügen über unzureichende Berechtigungen.

- Der Verzeichnisserver (falls konfiguriert) ist möglicherweise nicht verfügbar. Wenn dies der Fall ist, melden Sie sich mit einer lokalen Benutzerrolle an.
- Sie haben mehrmals versucht, sich erfolglos anzumelden, was den Sperrmodus ausgelöst hat. Warten Sie 10 Minuten, bis Sie sich erneut anmelden können.
- Eine Sperrbedingung wurde ausgelöst und Ihr Prüfprotokoll ist möglicherweise voll. Wechseln Sie zu Zugriffsmanagement und löschen Sie alte Ereignisse aus dem Revisionsprotokoll.
- SAML-Authentifizierung ist aktiviert. Aktualisieren Sie Ihren Browser, um sich anzumelden.

Aus einem der folgenden Gründe können Anmeldefehler bei einem Remote-Speicher-Array auftreten:

- Sie haben ein falsches Kennwort eingegeben.
- Sie haben mehrmals versucht, sich erfolglos anzumelden, was den Sperrmodus ausgelöst hat. Warten Sie 10 Minuten, um sich erneut anzumelden.
- Die maximale Anzahl an Client-Verbindungen, die auf dem Controller verwendet werden, wurde erreicht. Suchen Sie nach mehreren Benutzern oder Clients.

Was muss ich vor dem Hinzufügen eines Verzeichnisservers wissen?

Stellen Sie vor dem Hinzufügen eines Verzeichnisservers in der Zugriffsverwaltung sicher, dass Sie die folgenden 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.

Was muss ich über die Zuordnung von Speicher-Array-Rollen wissen?

Bevor Sie Gruppen zu Rollen zuordnen, lesen Sie die folgenden Richtlinien durch.

Die integrierten RBAC-Funktionen (rollenbasierte Zugriffssteuerung) des Storage-Arrays umfassen folgende Rollen:

- **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.

Verzeichnisdienste

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.
- Die Überwachungsrolle ist für alle Benutzer, einschließlich des Administrators, erforderlich. Der System Manager funktioniert ohne die vorhandene Monitorrolle nicht ordnungsgemäß für alle Benutzer.

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.
- Die Überwachungsrolle ist für alle Benutzer, einschließlich des Administrators, erforderlich. Der System Manager funktioniert ohne die vorhandene Monitorrolle nicht ordnungsgemäß für alle Benutzer.

Welche externen Verwaltungstools können von dieser Änderung betroffen sein?

Wenn Sie bestimmte Änderungen in System Manager vornehmen, z. B. das Wechseln der Managementoberfläche oder die Verwendung von SAML für eine Authentifizierungsmethode, sind einige externe Tools und Funktionen möglicherweise von der Verwendung eingeschränkt.

Managementoberfläche

Tools, die direkt mit der älteren Managementoberfläche (Symbol), z. B. SANtricity SMI-S Provider oder OnCommand Insight (OCI), kommunizieren, funktionieren nur, wenn die Einstellung für die ältere Managementoberfläche aktiviert ist. Darüber hinaus können Sie keine alten CLI-Befehle verwenden oder Spiegelungsvorgänge durchführen, wenn diese Einstellung deaktiviert ist.

Weitere Informationen erhalten Sie vom technischen Support.

SAML-Authentifizierung

Wenn SAML aktiviert ist, können die folgenden Clients nicht auf Storage-Array-Services und -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

Weitere Informationen erhalten Sie vom technischen Support.

Was muss ich vor der Konfiguration und Aktivierung von SAML wissen?

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 die IdP-Server- und -Controller-Uhren synchronisiert werden (entweder über einen NTP-Server oder durch Anpassen der Controller-Uhreinstellungen).
- Eine IdP-Metadatendatei wird vom IdP-System heruntergeladen und ist auf dem lokalen System verfügbar, das für den Zugriff auf System Manager verwendet wird.
- Sie kennen die IP-Adresse oder den Domain-Namen der einzelnen Controller im Storage-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

Welche Arten von Ereignissen werden im Auditprotokoll aufgezeichnet?

Das Revisionsprotokoll kann Änderungsereignisse oder sowohl Änderungs- als auch schreibgeschützte Ereignisse aufzeichnen.

Abhängig von den Richtlinieneinstellungen werden die folgenden Ereignistypen angezeigt:

- **Änderungsereignisse** — Benutzeraktionen aus System Manager heraus, die Änderungen am System, z. B. die Bereitstellung von Speicher, mit sich bringen.
- **Modifizierung und schreibgeschützte Ereignisse** — Benutzeraktionen, die Änderungen am System beinhalten, sowie Ereignisse, die Informationen anzeigen oder herunterladen, wie zum Beispiel die Anzeige von Volume-Zuweisungen.

Was muss ich vor der Konfiguration eines Syslog-Servers wissen?

Sie können Audit-Protokolle auf einem externen Syslog-Server archivieren.

Beachten Sie vor der Konfiguration eines Syslog-Servers die folgenden Richtlinien.

- Stellen Sie sicher, dass Sie die Serveradresse, das Protokoll und die Portnummer kennen. Bei der Serveradresse kann es sich um einen vollständig qualifizierten Domänennamen, eine IPv4-Adresse oder eine IPv6-Adresse handeln.
- Wenn Ihr Server ein sicheres Protokoll verwendet (z. B. TLS), muss auf Ihrem lokalen System ein Zertifikat für Zertifizierungsstellen (CA) verfügbar sein. CA-Zertifikate identifizieren Website-Eigentümer für sichere Verbindungen zwischen Servern und Clients.
- Nach der Konfiguration werden alle neuen Audit-Protokolle an den Syslog-Server gesendet. Frühere Protokolle werden nicht übertragen.
- Die **Überschreibrichtlinie**-Einstellungen (verfügbar unter „Ansicht/Bearbeiten“-Einstellungen) beeinflussen nicht, wie Protokolle mit einer Syslog-Serverkonfiguration verwaltet werden.
- Auditprotokolle folgen dem Nachrichtenformat RFC 5424.

Der Syslog-Server empfängt keine Audit-Protokolle mehr. Was mache ich?

Wenn Sie einen Syslog-Server mit einem TLS-Protokoll konfiguriert haben, kann der Server keine Meldungen empfangen, wenn das Zertifikat aus irgendeinem Grund ungültig wird. Eine Fehlermeldung über das ungültige Zertifikat wird im Auditprotokoll veröffentlicht.

Um dieses Problem zu lösen, müssen Sie zuerst das Zertifikat für den Syslog-Server reparieren. Wenn eine gültige Zertifikatskette vorhanden ist, gehen Sie zu Menü:Einstellungen[Audit Log > Syslog-Server konfigurieren > Alle testen].