Verwenden Sie SAML

SANtricity 11.7

NetApp
February 12, 2024

Inhalt

Verwenden Sie SAML

SAML konfigurieren

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 jedes 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 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

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

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

System Manager. 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**.

   Auf der Seite wird eine Übersicht der Konfigurationsschritte angezeigt.

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

   Das Dialogfeld „Datei des Identitätsanbieters importieren“ 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. 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 Dateien des Dienstanbieters exportieren 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 **Export** 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.

Schritte

1. Klicken Sie auf den Link für **Mapping System Manager** Rollen.

   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. Reguläre Ausdrücke werden unterstützt. Diese speziellen regulären Ausdruckszeichen müssen mit einem umgekehrten Schrägstrich entgangen werden (\) Wenn sie nicht Teil eines regulären Ausdrucksmusters sind: \.[]{}()<>*+-=!?^	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

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 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.

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 bestätigen wird geöffnet.

2. Typ `enable`, Und klicken Sie dann auf **Aktivieren**.
3. 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.

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

Ergebnisse

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**.

3. Wählen Sie **Export**.

   Das Dialogfeld Dateien des Dienstanbieters exportieren 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**.