Verwalten von SAML-Authentifizierungseinstellungen

Active IQ Unified Manager 9.10

NetApp
December 18, 2023

Inhalt

Verwalten von SAML-Authentifizierungseinstellungen

Nachdem Sie die Remote-Authentifizierungseinstellungen konfiguriert haben, können Sie die SAML-Authentifizierung (Security Assertion Markup Language) aktivieren, sodass Remote-Benutzer von einem sicheren Identitäts-Provider (IdP) authentifiziert werden, bevor sie auf die Unified Manager Web-UI zugreifen können.

Beachten Sie, dass nur Remote-Benutzer Zugriff auf die grafische Benutzeroberfläche von Unified Manager haben, nachdem die SAML-Authentifizierung aktiviert wurde. Lokale Benutzer und Wartungbenutzer können nicht auf die Benutzeroberfläche zugreifen. Diese Konfiguration hat keine Auswirkungen auf Benutzer, die auf die Wartungskonsole zugreifen.

Anforderungen an Identitätsanbieter

Wenn Sie Unified Manager für die Verwendung eines Identitäts-Providers (IdP) konfigurieren, um die SAML-Authentifizierung für alle Remote-Benutzer durchzuführen, müssen Sie einige erforderliche Konfigurationseinstellungen beachten, damit die Verbindung zu Unified Manager erfolgreich hergestellt wird.

Sie müssen die Unified Manager-URI und die Metadaten im IdP-Server eingeben. Sie können diese Informationen von der Seite Unified ManagerSAML Authentication kopieren. Unified Manager gilt im SAML-Standard (Security Assertion Markup Language) als Service Provider (SP).

Unterstützte Verschlüsselungsstandards

- Advanced Encryption Standard (AES): AES-128 und AES-256
- Sicherer Hash-Algorithmus (SHA): SHA-1 und SHA-256

Validierte Identitätsanbieter

- Shibboleth
- Active Directory Federation Services (ADFS)

ADFS-Konfigurationsanforderungen

- Sie müssen drei Antragsregeln in der folgenden Reihenfolge definieren, die erforderlich sind, damit Unified Manager ADFS SAML-Antworten für diesen Vertrauenseintrag der Treuhandgesellschaft analysieren kann.

Forderungsregel	Wert
SAM-Account-Name	Name-ID
SAM-Account-Name	Urne:oid:0.9.2342.19200300.100.1.1
Token-Gruppen — Unqualifizierter Name	Urne:oid:1.3.6.1.4.1.5923.1.5.1.1

- Sie müssen die Authentifizierungsmethode auf „`Forms Authentication`“ setzen, oder Benutzer erhalten möglicherweise einen Fehler beim Abmelden von Unified Manager. Führen Sie hierzu folgende Schritte aus:
  a. Öffnen Sie die ADFS-Verwaltungskonsole.
  b. Klicken Sie in der linken Strukturansicht auf den Ordner Authentication Policies.
  c. Klicken Sie unter Aktionen auf der rechten Seite auf Globale primäre Authentifizierungsrichtlinie bearbeiten.
  d. Setzen Sie die Intranet-Authentifizierungsmethode auf „`Forms Authentication`“ anstatt auf die Standardauthentifizierung „`Windows Authentication`“.
- In einigen Fällen wird die Anmeldung über das IdP abgelehnt, wenn das Unified Manager-Sicherheitszertifikat CA-signiert ist. Es gibt zwei Problemumgehungen zur Lösung dieses Problems:
  - Befolgen Sie die Anweisungen im Link, um die Widerrufs-Prüfung auf dem ADFS-Server für verkettete CA-Zertifikat zugeordnete abhängige Partei zu deaktivieren:

    "Deaktivieren Sie die Überprüfung der Widerruferstellung pro Vertrauen der Vertrauensgruppe"
  - Der CA-Server befindet sich im ADFS-Server, um die Zertifiktanforderung des Unified Manager-Servers zu signieren.

Sonstige Konfigurationsanforderungen

- Die Unified Manager-Taktskew ist auf 5 Minuten eingestellt, sodass der Zeitunterschied zwischen dem IdP-Server und dem Unified Manager-Server nicht mehr als 5 Minuten betragen kann oder die Authentifizierung fehlschlägt.

Aktivieren der SAML-Authentifizierung

Sie können die SAML-Authentifizierung (Security Assertion Markup Language) aktivieren, sodass Remote-Benutzer von einem Secure Identity Provider (IdP) authentifiziert werden, bevor sie auf die Web-UI von Unified Manager zugreifen können.

Was Sie brauchen

- Sie müssen die Remote-Authentifizierung konfiguriert und bestätigt haben, dass sie erfolgreich ist.
- Sie müssen mindestens einen Remote-Benutzer oder eine Remote-Gruppe mit der Rolle „Anwendungsadministrator“ erstellt haben.
- Der Identitäts-Provider (IdP) muss von Unified Manager unterstützt und konfiguriert werden.
- Sie müssen über die IdP-URL und die Metadaten verfügen.
- Sie müssen Zugriff auf den IdP-Server haben.

Nachdem Sie die SAML-Authentifizierung von Unified Manager aktiviert haben, können Benutzer erst dann auf die grafische Benutzeroberfläche zugreifen, wenn das IdP mit den Hostinformationen des Unified Manager-Servers konfiguriert wurde. Daher müssen Sie darauf vorbereitet sein, beide Teile der Verbindung abzuschließen, bevor Sie mit dem Konfigurationsprozess beginnen. Das IdP kann vor oder nach der Konfiguration von Unified Manager konfiguriert werden.

Nach Aktivierung der SAML-Authentifizierung haben nur Remote-Benutzer Zugriff auf die grafische Benutzeroberfläche von Unified Manager. Lokale Benutzer und Wartungbenutzer können nicht auf die

Benutzeroberfläche zugreifen. Diese Konfiguration hat keine Auswirkungen auf Benutzer, die auf die Wartungskonsole, die Unified Manager-Befehle oder Zapis zugreifen.

> Unified Manager wird automatisch neu gestartet, nachdem Sie die SAML-Konfiguration auf dieser Seite abgeschlossen haben.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **SAML Authentifizierung**.
2. Aktivieren Sie das Kontrollkästchen * SAML-Authentifizierung aktivieren*.

   Die Felder, die zum Konfigurieren der IdP-Verbindung erforderlich sind, werden angezeigt.

3. Geben Sie die IdP-URI und die IdP-Metadaten ein, die erforderlich sind, um den Unified Manager-Server mit dem IdP-Server zu verbinden.

   Wenn der IdP-Server direkt über den Unified Manager-Server erreichbar ist, können Sie nach Eingabe der IdP-URI auf die Schaltfläche **IdP-Metadaten abrufen** klicken, um das Feld IdP-Metadaten automatisch zu füllen.

4. Kopieren Sie den Unified Manager-Host-Metadaten-URI, oder speichern Sie die Host-Metadaten in eine XML-Textdatei.

   Sie können den IdP-Server derzeit mit diesen Informationen konfigurieren.

5. Klicken Sie Auf **Speichern**.

   Es wird ein Meldungsfeld angezeigt, um zu bestätigen, dass Sie die Konfiguration abschließen und Unified Manager neu starten möchten.

6. Klicken Sie auf **Bestätigen und Abmelden** und Unified Manager wird neu gestartet.

Wenn autorisierte Remote-Benutzer das nächste Mal versuchen, auf die grafische Benutzeroberfläche von Unified Manager zuzugreifen, geben sie ihre Anmeldedaten auf der Anmeldeseite IdP statt auf der Anmeldeseite von Unified Manager ein.

Wenn noch nicht abgeschlossen ist, greifen Sie auf Ihr IdP zu, und geben Sie den URI und die Metadaten des Unified Manager-Servers ein, um die Konfiguration abzuschließen.

> Wenn Sie ADFS als Identitäts-Provider verwenden, wird die Unified Manager-GUI nicht das ADFS-Timeout-Timeout erfüllt und funktioniert weiter, bis das Timeout der Unified Manager-Sitzung erreicht ist. Sie können das Timeout der GUI-Sitzung ändern, indem Sie auf **Allgemein** > **Feature-Einstellungen** > **Inaktivität Timeout** klicken.

Ändern des Identitäts-Providers, der für die SAML-Authentifizierung verwendet wird

Sie können den Identitäts-Provider (IdP), den Unified Manager zur Authentifizierung von Remote-Benutzern verwendet, ändern.

Was Sie brauchen

- Sie müssen über die IdP-URL und die Metadaten verfügen.

- Sie müssen Zugriff auf die IdP haben.

Der neue IdP kann vor oder nach der Konfiguration von Unified Manager konfiguriert werden.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **SAML Authentifizierung**.
2. Geben Sie die neue IdP-URI und die IdP-Metadaten ein, die erforderlich sind, um den Unified Manager-Server mit dem IdP zu verbinden.

   Wenn der IdP direkt über den Unified Manager-Server aufgerufen werden kann, können Sie nach Eingabe der IdP-URL auf die Schaltfläche **IdP-Metadaten abrufen** klicken, um das Feld IdP-Metadaten automatisch auszufüllen.

3. Kopieren Sie den Unified Manager-Metadaten-URI oder speichern Sie die Metadaten in eine XML-Textdatei.
4. Klicken Sie Auf **Konfiguration Speichern**.

   Es wird ein Meldungsfeld angezeigt, um zu bestätigen, dass Sie die Konfiguration ändern möchten.

5. Klicken Sie auf **OK**.

Greifen Sie auf den neuen IdP zu, und geben Sie die URI und die Metadaten des Unified Manager-Servers ein, um die Konfiguration abzuschließen.

Wenn die autorisierten Remote-Benutzer das nächste Mal versuchen, auf die grafische Benutzeroberfläche von Unified Manager zuzugreifen, geben sie ihre Anmeldeinformationen auf der neuen Anmeldeseite für IdP anstelle der alten Anmeldeseite ein.

SAML-Authentifizierungseinstellungen werden nach Änderung des Unified Manager-Sicherheitszertifikats aktualisiert

Jede Änderung am HTTPS-Sicherheitszertifikat, das auf dem Unified Manager-Server installiert ist, erfordert, dass Sie die Einstellungen für die SAML-Authentifizierung aktualisieren. Das Zertifikat wird aktualisiert, wenn Sie das Hostsystem umbenennen, eine neue IP-Adresse für das Hostsystem zuweisen oder das Sicherheitszertifikat für das System manuell ändern.

Nach der Änderung des Sicherheitszertifikats und dem Neustart des Unified Manager-Servers funktioniert die SAML-Authentifizierung nicht, und Benutzer können nicht auf die grafische Benutzeroberfläche von Unified Manager zugreifen. Sie müssen die SAML-Authentifizierungseinstellungen sowohl auf dem IdP-Server als auch auf dem Unified Manager-Server aktualisieren, um den Zugriff auf die Benutzeroberfläche wieder zu aktivieren.

Schritte

1. Melden Sie sich bei der Wartungskonsole an.
2. Geben Sie im **Hauptmenü** die Nummer für die Option **SAML-Authentifizierung deaktivieren** ein.

   Es wird eine Meldung angezeigt, die bestätigt, dass die SAML-Authentifizierung deaktiviert und Unified Manager neu gestartet werden soll.

3. Starten Sie die Unified Manager-Benutzeroberfläche mit der aktualisierten FQDN- oder IP-Adresse, akzeptieren Sie das aktualisierte Serverzertifikat in Ihrem Browser und melden Sie sich mit den Anmeldeinformationen für den Wartungsbenutzer an.
4. Wählen Sie auf der Seite **Setup/Authentifizierung** die Registerkarte **SAML Authentication** aus und konfigurieren Sie die IdP-Verbindung.
5. Kopieren Sie den Unified Manager-Host-Metadaten-URI, oder speichern Sie die Host-Metadaten in eine XML-Textdatei.
6. Klicken Sie Auf **Speichern**.

   Es wird ein Meldungsfeld angezeigt, um zu bestätigen, dass Sie die Konfiguration abschließen und Unified Manager neu starten möchten.

7. Klicken Sie auf **Bestätigen und Abmelden** und Unified Manager wird neu gestartet.
8. Greifen Sie auf Ihren IdP-Server zu, und geben Sie die URI und die Metadaten des Unified Manager-Servers ein, um die Konfiguration abzuschließen.

Identitäts-Provider	Konfigurationsschritte
ADFS	a. Löschen Sie den vorhandenen Vertrauenseintrag der Vertrauensantragenden Partei in der ADFS-Management-GUI. b. Fügen Sie mit dem einen neuen Vertrauenseintrag einer Vertrauensbasis hinzu `saml_sp_metadata.xml` Über den aktualisierten Unified Manager-Server aus. c. Definieren Sie die drei Forderungsregeln, die für Unified Manager erforderlich sind, um ADFS SAML-Antworten für diesen Vertrauenseintrag der Vertrauensbasis zu analysieren. d. Starten Sie den ADFS Windows-Dienst neu.
Shibboleth	a. Aktualisieren Sie den neuen FQDN des Unified Manager-Servers in das `attribute-filter.xml` Und `relying-party.xml` Dateien: b. Starten Sie den Apache Tomcat Webserver neu und warten Sie, bis Port 8005 online ist.

9. Melden Sie sich bei Unified Manager an und stellen Sie sicher, dass die SAML-Authentifizierung über Ihr IdP wie erwartet funktioniert.

Deaktivieren der SAML-Authentifizierung

Sie können die SAML-Authentifizierung deaktivieren, wenn Sie die Authentifizierung von Remote-Benutzern über einen sicheren Identitäts-Provider (IdP) beenden möchten, bevor sie sich in der Web-UI von Unified Manager anmelden können. Wenn die SAML-Authentifizierung deaktiviert ist, führen die konfigurierten Verzeichnisdienstanbieter wie Active Directory oder LDAP eine Anmeldeauthentifizierung durch.

Nachdem Sie die SAML-Authentifizierung deaktiviert haben, können lokale Benutzer und Wartungbenutzer zusätzlich zu konfigurierten Remote-Benutzern auf die grafische Benutzeroberfläche zugreifen.

Sie können die SAML-Authentifizierung auch über die Unified Manager-Wartungskonsole deaktivieren, wenn Sie keinen Zugriff auf die grafische Benutzeroberfläche haben.

> Unified Manager wird automatisch neu gestartet, nachdem die SAML-Authentifizierung deaktiviert ist.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **SAML Authentifizierung**.
2. Deaktivieren Sie das Kontrollkästchen * SAML-Authentifizierung aktivieren*.
3. Klicken Sie Auf **Speichern**.

   Es wird ein Meldungsfeld angezeigt, um zu bestätigen, dass Sie die Konfiguration abschließen und Unified Manager neu starten möchten.

4. Klicken Sie auf **Bestätigen und Abmelden** und Unified Manager wird neu gestartet.

Wenn Remote-Benutzer das nächste Mal versuchen, auf die grafische Benutzeroberfläche von Unified Manager zuzugreifen, geben sie ihre Anmeldedaten auf der Anmeldeseite von Unified Manager anstelle der IdP-Anmeldeseite ein.

Greifen Sie auf Ihren IdP zu und löschen Sie die URI und die Metadaten des Unified Manager-Servers.

Deaktivieren der SAML-Authentifizierung über die Wartungskonsole

Wenn kein Zugriff auf die Unified Manager GUI besteht, müssen Sie möglicherweise die SAML-Authentifizierung von der Wartungskonsole aus deaktivieren. Dies kann bei einer Fehlkonfiguration oder bei nicht zugänglichem IdP auftreten.

Was Sie brauchen

Sie müssen als Wartungbenutzer Zugriff auf die Wartungskonsole haben.

Wenn die SAML-Authentifizierung deaktiviert ist, führen die konfigurierten Verzeichnisdienstanbieter wie Active Directory oder LDAP eine Anmeldeauthentifizierung durch. Lokale Benutzer und Wartungbenutzer können zusätzlich zu konfigurierten Remote-Benutzern auf die grafische Benutzeroberfläche zugreifen.

Sie können die SAML-Authentifizierung auch über die Seite Setup/Authentifizierung in der UI deaktivieren.

> Unified Manager wird automatisch neu gestartet, nachdem die SAML-Authentifizierung deaktiviert ist.

Schritte

1. Melden Sie sich bei der Wartungskonsole an.
2. Geben Sie im **Hauptmenü** die Nummer für die Option **SAML-Authentifizierung deaktivieren** ein.

   Es wird eine Meldung angezeigt, die bestätigt, dass die SAML-Authentifizierung deaktiviert und Unified

Manager neu gestartet werden soll.

3. Geben Sie **y** ein, und drücken Sie dann die Eingabetaste, und Unified Manager wird neu gestartet.

Wenn Remote-Benutzer das nächste Mal versuchen, auf die grafische Benutzeroberfläche von Unified Manager zuzugreifen, geben sie ihre Anmeldedaten auf der Anmeldeseite von Unified Manager anstelle der IdP-Anmeldeseite ein.

Greifen Sie bei Bedarf auf Ihr IdP zu, und löschen Sie die URL und Metadaten des Unified Manager-Servers.

Seite SAML Authentication

Mithilfe der Seite SAML Authentication kann Unified Manager für die Authentifizierung von Remote-Benutzern mit SAML über einen sicheren Identitäts-Provider (IdP) konfiguriert werden, bevor sie sich bei der Web-UI von Unified Manager anmelden können.

- Sie müssen über die Anwendungsadministratorrolle verfügen, um die SAML-Konfiguration zu erstellen oder zu ändern.
- Sie müssen die Remote-Authentifizierung konfiguriert haben.
- Sie müssen mindestens einen Remote-Benutzer oder eine Remote-Gruppe konfiguriert haben.

Nachdem die Remote-Authentifizierung und Remote-Benutzer konfiguriert wurden, können Sie das Kontrollkästchen SAML-Authentifizierung aktivieren aktivieren aktivieren auswählen, um die Authentifizierung über einen sicheren Identitätsanbieter zu aktivieren.

- **IdP URI**

  Der URI für den Zugriff auf das IdP vom Unified Manager-Server aus. Beispiel-URIs sind unten aufgeführt.

  ADFS-Beispiel-URI:

  ```
  https://win2016-dc.ntap2016.local/federationmetadata/2007-
  06/federationmetadata.xml
  ```

  Shibboleth Beispiel URI:

  ```
  https://centos7.ntap2016.local/idp/shibboleth
  ```

- **IdP-Metadaten**

  Die IdP-Metadaten im XML-Format.

  Wenn über den Unified Manager-Server auf die IdP-URL zugegriffen werden kann, können Sie auf die Schaltfläche **IdP-Metadaten abrufen** klicken, um dieses Feld auszufüllen.

- **Host-System (FQDN)**

  Der FQDN des Unified Manager-Hostsystems, wie bei der Installation definiert. Sie können diesen Wert bei Bedarf ändern.

- **Host-URI**

Die URI für den Zugriff auf das Unified Manager-Hostsystem von der IdP aus.

- **Host-Metadaten**

  Die Metadaten des Host-Systems im XML-Format.