Gestione delle impostazioni di autenticazione SAML

OnCommand Unified Manager 9.5

NetApp
December 20, 2023

Sommario

Gestione delle impostazioni di autenticazione SAML

Dopo aver configurato le impostazioni di autenticazione remota, è possibile attivare l'autenticazione SAML (Security Assertion Markup Language) in modo che gli utenti remoti vengano autenticati da un provider di identità sicuro (IdP) prima di poter accedere all'interfaccia utente Web di Unified Manager.

Tenere presente che solo gli utenti remoti avranno accesso all'interfaccia utente grafica di Unified Manager dopo l'attivazione dell'autenticazione SAML. Gli utenti locali e gli utenti di manutenzione non potranno accedere all'interfaccia utente. Questa configurazione non influisce sugli utenti che accedono alla console di manutenzione.

Requisiti del provider di identità

Quando si configura Unified Manager per utilizzare un provider di identità (IdP) per eseguire l'autenticazione SAML per tutti gli utenti remoti, è necessario conoscere alcune impostazioni di configurazione necessarie per consentire la connessione a Unified Manager.

È necessario immettere l'URI e i metadati di Unified Manager nel server IdP. È possibile copiare queste informazioni dalla pagina autenticazione SAML di Unified Manager. Unified Manager è considerato il service provider (SP) nello standard SAML (Security Assertion Markup Language).

Standard di crittografia supportati

- AES (Advanced Encryption Standard): AES-128 e AES-256
- Secure Hash Algorithm (SHA): SHA-1 e SHA-256

Provider di identità validati

- Shibboleth
- Active Directory Federation Services (ADFS)

Requisiti di configurazione di ADFS

- È necessario definire tre regole per le attestazioni nell'ordine seguente, necessarie affinché Unified Manager analizzi le risposte SAML di ADFS per questa voce di trust della parte che si basa.

Regola della richiesta di rimborso	Valore
Nome-account-SAM	ID nome
Nome-account-SAM	urn:oid:0.9.2342.19200300.100.1.1
Gruppi di token — Nome non qualificato	urn:oid:1.3.6.1.4.1.5923.1.5.1.1

- È necessario impostare il metodo di autenticazione su “Forms Authentication” per consentire agli utenti di ricevere un errore durante la disconnessione da Unified Manager quando si utilizza Internet Explorer. Attenersi alla seguente procedura:
  a. Aprire la console di gestione ADFS.
  b. Fare clic sulla cartella Authentication Policies (Criteri di autenticazione) nella vista ad albero a sinistra.
  c. Nella sezione azioni a destra, fare clic su Modifica policy di autenticazione primaria globale.
  d. Impostare il metodo di autenticazione Intranet su “Forms Authentication” invece di “Windows Authentication” predefinito.
- In alcuni casi, l’accesso tramite IdP viene rifiutato quando il certificato di sicurezza di Unified Manager è firmato dalla CA. Esistono due soluzioni alternative per risolvere questo problema:
  - Seguire le istruzioni indicate nel collegamento per disattivare il controllo di revoca sul server ADFS per la parte di base associata al certificato CA concatenato:

    http://www.torivar.com/2016/03/22/adfs-3-0-disable-revocation-check-windows-2012-r2/

  - Fare in modo che il server CA si trovi all’interno del server ADFS per firmare la richiesta di certificazione del server Unified Manager.

Altri requisiti di configurazione

- L’inclinazione dell’orologio di Unified Manager è impostata su 5 minuti, quindi la differenza di tempo tra il server IdP e il server Unified Manager non può superare i 5 minuti o l’autenticazione non riesce.
- Quando gli utenti tentano di accedere a Unified Manager utilizzando Internet Explorer, potrebbe essere visualizzato il messaggio **il sito Web non può visualizzare la pagina**. In questo caso, assicurarsi che questi utenti deselezionino l’opzione “Show friendly HTTP error messages” (Visualizza messaggi di errore HTTP descrittivi) in **Tools** > **Internet Options** > **Advanced** (Strumenti* > **Opzioni Internet** > **Avanzate**).

Attivazione dell’autenticazione SAML

È possibile attivare l’autenticazione SAML (Security Assertion Markup Language) in modo che gli utenti remoti vengano autenticati da un provider di identità sicuro (IdP) prima di poter accedere all’interfaccia utente Web di Unified Manager.

Prima di iniziare

- È necessario aver configurato l’autenticazione remota e verificato che sia stata eseguita correttamente.
- È necessario aver creato almeno un utente remoto o un gruppo remoto con il ruolo di amministratore di OnCommand.
- Il provider di identità (IdP) deve essere supportato da Unified Manager e deve essere configurato.
- È necessario disporre dell’URL IdP e dei metadati.
- È necessario disporre dell’accesso al server IdP.

A proposito di questa attività

Dopo aver abilitato l’autenticazione SAML da Unified Manager, gli utenti non possono accedere all’interfaccia utente grafica fino a quando IdP non è stato configurato con le informazioni sull’host del server Unified Manager. Pertanto, è necessario essere pronti a completare entrambe le parti della connessione prima di

avviare il processo di configurazione. L'IdP può essere configurato prima o dopo la configurazione di Unified Manager.

Solo gli utenti remoti avranno accesso all'interfaccia utente grafica di Unified Manager dopo l'attivazione dell'autenticazione SAML. Gli utenti locali e gli utenti di manutenzione non potranno accedere all'interfaccia utente. Questa configurazione non influisce sugli utenti che accedono alla console di manutenzione, ai comandi di Unified Manager o alle ZAPI.

Unified Manager viene riavviato automaticamente dopo aver completato la configurazione SAML in questa pagina.

Fasi

1. Nella barra degli strumenti, fare clic su  , quindi fare clic su **Authentication** nel menu Setup di sinistra.
2. Nella pagina **Setup/Authentication**, selezionare la scheda **SAML Authentication**.
3. Selezionare la casella di controllo **Enable SAML Authentication** (attiva autenticazione SAML).

   Vengono visualizzati i campi necessari per configurare la connessione IdP.

4. Immettere l'URI IdP e i metadati IdP richiesti per connettere il server Unified Manager al server IdP.

   Se il server IdP è accessibile direttamente dal server Unified Manager, è possibile fare clic sul pulsante **Fetch IdP Metadata** (Scarica metadati IdP) dopo aver immesso l'URI IdP per popolare automaticamente il campo IdP Metadata (metadati IdP).

5. Copiare l'URI dei metadati host di Unified Manager o salvare i metadati host in un file di testo XML.

   In questo momento è possibile configurare il server IdP con queste informazioni.

6. Fare clic su **Save** (Salva).

   Viene visualizzata una finestra di messaggio per confermare che si desidera completare la configurazione e riavviare Unified Manager.

7. Fare clic su **Confirm and Logout** (Conferma e Disconnetti) per riavviare Unified Manager.

Risultati

La volta successiva che gli utenti remoti autorizzati tenteranno di accedere all'interfaccia grafica di Unified Manager, inseriranno le proprie credenziali nella pagina di accesso di IdP anziché nella pagina di accesso di Unified Manager.

Al termine

Se non è già stato completato, accedere all'IdP e immettere l'URI e i metadati del server Unified Manager per completare la configurazione.

Quando si utilizza ADFS come provider di identità, la GUI di Unified Manager non rispetta il timeout ADFS e continuerà a funzionare fino al raggiungimento del timeout della sessione di Unified Manager. Quando Unified Manager viene distribuito su Windows, Red Hat o CentOS, è possibile modificare il timeout della sessione GUI utilizzando il seguente comando CLI di Unified Manager: `um option set absolute.session.timeout=00:15:00`Questo comando imposta il timeout della sessione GUI di Unified Manager su 15 minuti.

Modifica del provider di identità utilizzato per l'autenticazione SAML

È possibile modificare il provider di identità (IdP) utilizzato da Unified Manager per autenticare gli utenti remoti.

Prima di iniziare

- È necessario disporre dell'URL IdP e dei metadati.
- È necessario disporre dell'accesso all'IdP.

A proposito di questa attività

Il nuovo IdP può essere configurato prima o dopo la configurazione di Unified Manager.

Fasi

1. Nella barra degli strumenti, fare clic su , quindi fare clic su **Authentication** nel menu Setup di sinistra.
2. Nella pagina **Setup/Authentication**, selezionare la scheda **SAML Authentication**.
3. Inserire il nuovo URI IdP e i metadati IdP richiesti per connettere il server Unified Manager all'IdP.

   Se l'IdP è accessibile direttamente dal server di Unified Manager, è possibile fare clic sul pulsante **Fetch IdP Metadata** (Scarica metadati IdP) dopo aver immesso l'URL IdP per compilare automaticamente il campo IdP Metadata (metadati IdP).

4. Copiare l'URI dei metadati di Unified Manager o salvare i metadati in un file di testo XML.
5. Fare clic su **Save Configuration** (Salva configurazione).

   Viene visualizzata una finestra di messaggio per confermare che si desidera modificare la configurazione.

6. Fare clic su **OK**.

Al termine

Accedere al nuovo IdP e immettere l'URI e i metadati del server Unified Manager per completare la configurazione.

La volta successiva che gli utenti remoti autorizzati tenteranno di accedere all'interfaccia grafica di Unified Manager, inseriranno le proprie credenziali nella nuova pagina di accesso IdP anziché nella vecchia pagina di accesso IdP.

Aggiornamento delle impostazioni di autenticazione SAML dopo la modifica del certificato di protezione di Unified Manager

Qualsiasi modifica al certificato di protezione HTTPS installato sul server Unified Manager richiede l'aggiornamento delle impostazioni di configurazione per l'autenticazione SAML. Il certificato viene aggiornato se si rinomina il sistema host, si assegna un nuovo indirizzo IP al sistema host o si modifica manualmente il certificato di protezione del sistema.

A proposito di questa attività

Una volta modificato il certificato di protezione e riavviato il server Unified Manager, l'autenticazione SAML non funzionerà e gli utenti non potranno accedere all'interfaccia grafica di Unified Manager. Per riattivare l'accesso all'interfaccia utente, è necessario aggiornare le impostazioni di autenticazione SAML sul server IdP e sul server Unified Manager.

Fasi

1. Accedere alla console di manutenzione.
2. Nel **Menu principale**, inserire il numero dell'opzione **Disattiva autenticazione SAML**.

   Viene visualizzato un messaggio per confermare che si desidera disattivare l'autenticazione SAML e riavviare Unified Manager.

3. Avviare l'interfaccia utente di Unified Manager utilizzando l'FQDN o l'indirizzo IP aggiornato, accettare il certificato del server aggiornato nel browser e accedere utilizzando le credenziali utente di manutenzione.
4. Nella pagina **Setup/Authentication**, selezionare la scheda **SAML Authentication** e configurare la connessione IdP.
5. Copiare l'URI dei metadati host di Unified Manager o salvare i metadati host in un file di testo XML.
6. Fare clic su **Save** (Salva).

   Viene visualizzata una finestra di messaggio per confermare che si desidera completare la configurazione e riavviare Unified Manager.

7. Fare clic su **Confirm and Logout** (Conferma e Disconnetti) per riavviare Unified Manager.
8. Accedere al server IdP e immettere l'URI e i metadati del server Unified Manager per completare la configurazione.

Provider di identità	Fasi di configurazione
ADFS	a. Eliminare la voce di trust esistente della parte che si basa nella GUI di gestione di ADFS. b. Aggiungere una nuova voce di attendibilità della parte che si basa utilizzando `saml_sp_metadata.xml` Dal server Unified Manager aggiornato. c. Definire le tre regole di attestazione richieste da Unified Manager per analizzare le risposte SAML di ADFS per questa voce di attendibilità della parte che si basa. d. Riavviare il servizio Windows di ADFS.
Shibboleth	a. Aggiornare il nuovo FQDN del server Unified Manager in `attribute-filter.xml` e. `relying-party.xml` file. b. Riavviare il server Web Apache Tomcat e attendere che la porta 8005 sia online.

9. Accedere a Unified Manager e verificare che l'autenticazione SAML funzioni come previsto attraverso l'IdP.

Disattivazione dell'autenticazione SAML

È possibile disattivare l'autenticazione SAML quando si desidera interrompere l'autenticazione degli utenti remoti tramite un provider di identità sicuro (IdP) prima che possano accedere all'interfaccia utente Web di Unified Manager. Quando l'autenticazione SAML è disattivata, i provider di servizi di directory configurati, ad esempio Active Directory o LDAP, eseguono l'autenticazione di accesso.

A proposito di questa attività

Una volta disattivata l'autenticazione SAML, gli utenti locali e gli utenti di manutenzione potranno accedere all'interfaccia grafica utente oltre agli utenti remoti configurati.

Se non si dispone dell'accesso all'interfaccia utente grafica, è possibile disattivare l'autenticazione SAML anche utilizzando la console di manutenzione di Unified Manager.

Unified Manager viene riavviato automaticamente dopo la disattivazione dell'autenticazione SAML.

Fasi

1. Nella barra degli strumenti, fare clic su , quindi fare clic su **Authentication** nel menu Setup di sinistra.
2. Nella pagina **Setup/Authentication**, selezionare la scheda **SAML Authentication**.
3. Deselezionare la casella di controllo **Enable SAML Authentication** (attiva autenticazione SAML).
4. Fare clic su **Save** (Salva).

Viene visualizzata una finestra di messaggio per confermare che si desidera completare la configurazione e riavviare Unified Manager.

5. Fare clic su **Confirm and Logout** (Conferma e Disconnetti) per riavviare Unified Manager.

Risultati

La volta successiva che gli utenti remoti tenteranno di accedere all'interfaccia grafica di Unified Manager, inseriranno le proprie credenziali nella pagina di accesso di Unified Manager anziché nella pagina di accesso di IdP.

Al termine

Accedere all'ID ed eliminare l'URI e i metadati del server Unified Manager.

Disattivazione dell'autenticazione SAML dalla console di manutenzione

Potrebbe essere necessario disattivare l'autenticazione SAML dalla console di manutenzione quando non è possibile accedere alla GUI di Unified Manager. Ciò potrebbe verificarsi in caso di errata configurazione o se l'IdP non è accessibile.

Prima di iniziare

È necessario avere accesso alla console di manutenzione come utente di manutenzione.

A proposito di questa attività

Quando l'autenticazione SAML è disattivata, i provider di servizi di directory configurati, ad esempio Active Directory o LDAP, eseguono l'autenticazione di accesso. Gli utenti locali e gli utenti di manutenzione potranno accedere all'interfaccia utente grafica oltre agli utenti remoti configurati.

È inoltre possibile disattivare l'autenticazione SAML dalla pagina Setup/Authentication (Configurazione/autenticazione) dell'interfaccia utente.

Unified Manager viene riavviato automaticamente dopo la disattivazione dell'autenticazione SAML.

Fasi

1. Accedere alla console di manutenzione.
2. Nel **Menu principale**, inserire il numero dell'opzione **Disattiva autenticazione SAML**.

   Viene visualizzato un messaggio per confermare che si desidera disattivare l'autenticazione SAML e riavviare Unified Manager.

3. Digitare **y**, quindi premere Invio per riavviare Unified Manager.

Risultati

La volta successiva che gli utenti remoti tenteranno di accedere all'interfaccia grafica di Unified Manager, inseriranno le proprie credenziali nella pagina di accesso di Unified Manager anziché nella pagina di accesso di IdP.

Al termine

Se necessario, accedere all'IdP ed eliminare l'URL e i metadati del server Unified Manager.