Gestisci le impostazioni di autenticazione SAML

Active IQ Unified Manager

NetApp
October 15, 2025

Sommario

Gestisci le impostazioni di autenticazione SAML

Dopo aver configurato le impostazioni di autenticazione remota, è possibile abilitare 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.

Si noti che solo gli utenti remoti avranno accesso all'interfaccia utente grafica di Unified Manager dopo aver abilitato l'autenticazione SAML. Gli utenti locali e gli utenti di manutenzione non potranno accedere all'interfaccia utente. Questa configurazione non ha alcun impatto sugli utenti che accedono alla console di manutenzione.

Requisiti del fornitore 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 richieste affinché la connessione a Unified Manager abbia successo.

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 fornitore di servizi (SP) nello standard Security Assertion Markup Language (SAML).

Standard di crittografia supportati

- Standard di crittografia avanzata (AES): AES-128 e AES-256
- Algoritmo hash sicuro (SHA): SHA-1 e SHA-256

Fornitori di identità convalidati

- Shibboleth
- Servizi federativi di Active Directory (ADFS)

Requisiti di configurazione ADFS

- È necessario definire tre regole di attestazione nel seguente ordine, necessarie affinché Unified Manager analizzi le risposte SAML di ADFS per questa voce di trust della relying party.

Regola di rivendicazione	Valore
Nome account SAM	ID nome
Nome account SAM	urna:oid:0.9.2342.19200300.100.1.1
Gruppi di token — Nome non qualificato	urna:oid:1.3.6.1.4.1.5923.1.5.1.1

- È necessario impostare il metodo di autenticazione su "Autenticazione tramite moduli" altrimenti gli utenti potrebbero ricevere un errore quando escono da Unified Manager. Segui questi passaggi:

a. Aprire la console di gestione ADFS.

b. Fare clic sulla cartella Criteri di autenticazione nella vista ad albero a sinistra.

c. In Azioni sulla destra, fare clic su Modifica criterio di autenticazione primaria globale.

d. Impostare il metodo di autenticazione Intranet su “Autenticazione basata su moduli” anziché sul valore predefinito “Autenticazione Windows”.

- In alcuni casi l’accesso tramite IdP viene rifiutato quando il certificato di sicurezza di Unified Manager è firmato da una CA. Esistono due soluzioni alternative per risolvere questo problema:
  - Seguire le istruzioni identificate nel collegamento per disattivare il controllo di revoca sul server ADFS per la parte affidabile associata al certificato CA concatenato:

    "Disabilita il controllo di revoca per trust della parte affidabile"

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

Altri requisiti di configurazione

- Lo sfasamento dell’orologio di Unified Manager è impostato su 5 minuti, quindi la differenza di orario tra il server IdP e il server Unified Manager non può essere superiore a 5 minuti, altrimenti l’autenticazione fallirà.

Abilita l’autenticazione SAML

È possibile abilitare 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 andata a buon fine.
- È necessario aver creato almeno un utente remoto o un gruppo remoto con il ruolo di amministratore dell’applicazione.
- Il provider di identità (IdP) deve essere supportato da Unified Manager e deve essere configurato.
- È necessario disporre dell’URL e dei metadati dell’IdP.
- È necessario avere accesso al server IdP.

Dopo aver abilitato l’autenticazione SAML da Unified Manager, gli utenti non potranno accedere all’interfaccia utente grafica finché l’IdP non sarà stato configurato con le informazioni sull’host del server Unified Manager. Pertanto, prima di iniziare il processo di configurazione, è necessario essere pronti a completare entrambe le parti della connessione. 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 aver abilitato l’autenticazione SAML. Gli utenti locali e gli utenti di manutenzione non potranno accedere all’interfaccia utente. Questa configurazione non ha alcun impatto 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.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale** > **Autenticazione SAML**.
2. Selezionare la casella di controllo **Abilita autenticazione SAML**.

   Vengono visualizzati i campi necessari per configurare la connessione IdP.

3. Immettere l'URI IdP e i metadati IdP necessari 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 **Recupera metadati IdP** dopo aver immesso l'URI IdP per popolare automaticamente il campo Metadati IdP.

4. Copiare l'URI dei metadati dell'host Unified Manager oppure salvare i metadati dell'host in un file di testo XML.

   È possibile configurare il server IdP con queste informazioni in questo momento.

5. Fare clic su **Salva**.

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

6. Fare clic su **Conferma e disconnetti** e Unified Manager verrà riavviato.

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

Se non è ancora stato fatto, accedi al tuo IdP e inserisci l'URI e i metadati del server Unified Manager per completare la configurazione.

Quando si utilizza ADFS come provider di identità, l'interfaccia utente grafica di Unified Manager non rispetta il timeout di ADFS e continuerà a funzionare finché non verrà raggiunto il timeout della sessione di Unified Manager. È possibile modificare il timeout della sessione GUI facendo clic su **Generale** > **Impostazioni funzionalità** > **Timeout di inattività**.

Cambia il 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 e dei metadati dell'IdP.
- È necessario avere accesso all'IdP.

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

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale** > **Autenticazione SAML**.
2. Immettere il nuovo URI IdP e i metadati IdP necessari per connettere il server Unified Manager all'IdP.

Se l'IdP è accessibile direttamente dal server Unified Manager, è possibile fare clic sul pulsante **Recupera metadati IdP** dopo aver immesso l'URL dell'IdP per popolare automaticamente il campo Metadati IdP.

3. Copiare l'URI dei metadati di Unified Manager oppure salvare i metadati in un file di testo XML.
4. Fare clic su **Salva configurazione**.

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

5. Fare clic su **OK**.

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

La prossima volta 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.

Aggiorna le impostazioni di autenticazione SAML dopo la modifica del certificato di sicurezza di Unified Manager

Qualsiasi modifica al certificato di sicurezza HTTPS installato sul server Unified Manager richiede l'aggiornamento delle impostazioni di configurazione dell'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 sicurezza per il sistema.

Dopo aver modificato il certificato di sicurezza e riavviato il server Unified Manager, l'autenticazione SAML non funzionerà e gli utenti non saranno in grado di accedere all'interfaccia grafica di Unified Manager. È necessario aggiornare le impostazioni di autenticazione SAML sia sul server IdP che sul server Unified Manager per riabilitare l'accesso all'interfaccia utente.

Passi

1. Accedi alla console di manutenzione.
2. Nel **Menu principale**, immettere il numero per l'opzione **Disabilita autenticazione SAML**.

   Viene visualizzato un messaggio per confermare che si desidera disabilitare 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 ed effettuare l'accesso utilizzando le credenziali dell'utente addetto alla manutenzione.
4. Nella pagina **Configurazione/Autenticazione**, seleziona la scheda **Autenticazione SAML** e configura la connessione IdP.
5. Copiare l'URI dei metadati dell'host Unified Manager oppure salvare i metadati dell'host in un file di testo XML.
6. Fare clic su **Salva**.

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

7. Fare clic su **Conferma e disconnetti** e Unified Manager verrà riavviato.
8. Accedi al tuo server IdP e inserisci l'URI e i metadati del server Unified Manager per completare la

configurazione.

Fornitore di identità	Fasi di configurazione
ADFS	a. Eliminare la voce di trust della relying party esistente nell'interfaccia utente grafica di gestione ADFS. b. Aggiungere una nuova voce di trust della parte affidabile utilizzando `saml_sp_metadata.xml` dal server Unified Manager aggiornato. c. Definire le tre regole di claim necessarie affinché Unified Manager analizzi le risposte SAML di ADFS per questa voce di trust della relying party. d. Riavviare il servizio ADFS di Windows.
Shibboleth	a. Aggiorna 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 torni online.

9. Accedi a Unified Manager e verifica che l'autenticazione SAML funzioni come previsto tramite il tuo IdP.

Disabilitare l'autenticazione SAML

È possibile disabilitare 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 disabilitata, i provider di servizi di directory configurati, come Active Directory o LDAP, eseguono l'autenticazione di accesso.

Dopo aver disabilitato l'autenticazione SAML, gli utenti locali e gli utenti di manutenzione potranno accedere all'interfaccia utente grafica, oltre agli utenti remoti configurati.

È anche possibile disabilitare l'autenticazione SAML tramite la console di manutenzione di Unified Manager se non si ha accesso all'interfaccia utente grafica.

Unified Manager viene riavviato automaticamente dopo aver disabilitato l'autenticazione SAML.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale** > **Autenticazione SAML**.
2. Deseleziona la casella di controllo **Abilita autenticazione SAML**.
3. Fare clic su **Salva**.

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

4. Fare clic su **Conferma e disconnetti** e Unified Manager verrà riavviato.

La prossima volta 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 dell'IdP.

Accedi al tuo IdP ed elimina l'URI e i metadati del server Unified Manager.

Disabilitare l'autenticazione SAML dalla console di manutenzione

Potrebbe essere necessario disabilitare l'autenticazione SAML dalla console di manutenzione quando non è possibile accedere all'interfaccia utente grafica di Unified Manager. Ciò potrebbe verificarsi in caso di configurazione errata o se l'IdP non è accessibile.

Prima di iniziare

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

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

È anche possibile disabilitare l'autenticazione SAML dalla pagina Configurazione/Autenticazione nell'interfaccia utente.

Unified Manager viene riavviato automaticamente dopo aver disabilitato l'autenticazione SAML.

Passi

1. Accedi alla console di manutenzione.
2. Nel **Menu principale**, immettere il numero per l'opzione **Disabilita autenticazione SAML**.

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

3. Digitare **y**, quindi premere Invio; Unified Manager verrà riavviato.

La prossima volta 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 dell'IdP.

Se necessario, accedi al tuo IdP ed elimina l'URL e i metadati del server Unified Manager.

Pagina di autenticazione SAML

È possibile utilizzare la pagina Autenticazione SAML per configurare Unified Manager in modo che autentichi gli utenti remoti tramite SAML tramite un provider di identità sicuro (IdP) prima che possano accedere all'interfaccia utente Web di Unified Manager.

- Per creare o modificare la configurazione SAML è necessario disporre del ruolo di amministratore

dell'applicazione.

- È necessario aver configurato l'autenticazione remota.
- È necessario aver configurato almeno un utente remoto o un gruppo remoto.

Dopo aver configurato l'autenticazione remota e gli utenti remoti, è possibile selezionare la casella di controllo Abilita autenticazione SAML per abilitare l'autenticazione tramite un provider di identità sicuro.

- **URI IdP**

  L'URI per accedere all'IdP dal server Unified Manager. Di seguito sono elencati alcuni esempi di URI.

  URI di esempio ADFS:

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

  Esempio di URI di Shibboleth:

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

- **Metadati IdP**

  Metadati IdP in formato XML.

  Se l'URL dell'IdP è accessibile dal server Unified Manager, è possibile fare clic sul pulsante **Recupera metadati IdP** per popolare questo campo.

- **Sistema host (FQDN)**

  FQDN del sistema host Unified Manager come definito durante l'installazione. Se necessario, è possibile modificare questo valore.

- **URI host**

  L'URI per accedere al sistema host Unified Manager dall'IdP.

- **Metadati host**

  Metadati del sistema host in formato XML.

Informazioni sul copyright

Informazioni sul marchio commerciale