



Gestione dell'autenticazione

Active IQ Unified Manager 9.9

NetApp
April 05, 2024

Sommario

Gestione dell'autenticazione	1
Attivazione dell'autenticazione remota	1
Disattivazione dei gruppi nidificati dall'autenticazione remota	2
Impostazione dei servizi di autenticazione	3
Aggiunta di server di autenticazione	4
Verifica della configurazione dei server di autenticazione	5
Modifica dei server di autenticazione	6
Eliminazione dei server di autenticazione	7
Autenticazione con Active Directory o OpenLDAP	7
Attivazione dell'autenticazione SAML	8
Requisiti del provider di identità	9
Modifica del provider di identità utilizzato per l'autenticazione SAML	10
Disattivazione dell'autenticazione SAML	11
Registrazione dell'audit	12
Descrizione delle finestre di autenticazione e delle finestre di dialogo	14

Gestione dell'autenticazione

È possibile attivare l'autenticazione utilizzando LDAP o Active Directory sul server Unified Manager e configurarlo per l'utilizzo con i server per l'autenticazione degli utenti remoti.

Inoltre, è possibile attivare l'autenticazione SAML in modo che gli utenti remoti vengano autenticati tramite un provider di identità sicuro (IdP) prima di poter accedere all'interfaccia utente Web di Unified Manager.

Attivazione dell'autenticazione remota

È possibile attivare l'autenticazione remota in modo che il server Unified Manager possa comunicare con i server di autenticazione. Gli utenti del server di autenticazione possono accedere all'interfaccia grafica di Unified Manager per gestire i dati e gli oggetti di storage.

Prima di iniziare

È necessario disporre del ruolo di amministratore dell'applicazione.



Il server Unified Manager deve essere connesso direttamente al server di autenticazione. È necessario disattivare tutti i client LDAP locali come SSSD (System Security Services Daemon) o NSLCD (Name Service LDAP Caching Daemon).

A proposito di questa attività

È possibile attivare l'autenticazione remota utilizzando Open LDAP o Active Directory. Se l'autenticazione remota è disattivata, gli utenti remoti non possono accedere a Unified Manager.

L'autenticazione remota è supportata su LDAP e LDAPS (Secure LDAP). Unified Manager utilizza 389 come porta predefinita per le comunicazioni non protette e 636 come porta predefinita per le comunicazioni protette.



Il certificato utilizzato per autenticare gli utenti deve essere conforme al formato X.509.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Generale > autenticazione remota**.
2. Selezionare la casella **Enable remote Authentication...** (attiva autenticazione remota...).
3. Nel campo **Servizio di autenticazione**, selezionare il tipo di servizio e configurare il servizio di autenticazione.

Per tipo di autenticazione...	Inserire le seguenti informazioni...
Active Directory	<ul style="list-style-type: none"> • Nome dell'amministratore del server di autenticazione in uno dei seguenti formati: <ul style="list-style-type: none"> ◦ domainname . username ◦ username@domainname ◦ Bind Distinguished Name (Utilizzando la notazione LDAP appropriata) • Password dell'amministratore • Nome distinto di base (utilizzando la notazione LDAP appropriata)
Aprire LDAP	<ul style="list-style-type: none"> • Nome distinto di binding (nella notazione LDAP appropriata) • Associare la password • Nome distinto di base

Se l'autenticazione di un utente di Active Directory richiede molto tempo o si verifica un timeout, il server di autenticazione probabilmente impiega molto tempo per rispondere. La disattivazione del supporto per i gruppi nidificati in Unified Manager potrebbe ridurre il tempo di autenticazione.

Se si seleziona l'opzione Usa connessione protetta per il server di autenticazione, Unified Manager comunica con il server di autenticazione utilizzando il protocollo SSL (Secure Sockets Layer).

1. Aggiungere server di autenticazione e verificare l'autenticazione.
2. Fare clic su **Save** (Salva).

Disattivazione dei gruppi nidificati dall'autenticazione remota

Se l'autenticazione remota è attivata, è possibile disattivare l'autenticazione dei gruppi nidificati in modo che solo i singoli utenti e non i membri del gruppo possano autenticarsi in remoto in Unified Manager. È possibile disattivare i gruppi nidificati quando si desidera migliorare i tempi di risposta per l'autenticazione di Active Directory.

Prima di iniziare

- È necessario disporre del ruolo di amministratore dell'applicazione.
- La disattivazione dei gruppi nidificati è applicabile solo quando si utilizza Active Directory.

A proposito di questa attività

La disattivazione del supporto per i gruppi nidificati in Unified Manager potrebbe ridurre il tempo di autenticazione. Se il supporto di gruppi nidificati è disattivato e se un gruppo remoto viene aggiunto a Unified Manager, i singoli utenti devono essere membri del gruppo remoto per autenticarsi in Unified Manager.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Generale > autenticazione remota**.
2. Selezionare la casella **Disable Nested Group Lookup** (Disattiva ricerca gruppi nidificati).
3. Fare clic su **Save** (Salva).

Impostazione dei servizi di autenticazione

I servizi di autenticazione consentono l'autenticazione di utenti remoti o gruppi remoti in un server di autenticazione prima di fornire loro l'accesso a Unified Manager. È possibile autenticare gli utenti utilizzando servizi di autenticazione predefiniti (ad esempio Active Directory o OpenLDAP) o configurando il proprio meccanismo di autenticazione.

Prima di iniziare

- È necessario aver attivato l'autenticazione remota.
- È necessario disporre del ruolo di amministratore dell'applicazione.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Generale > autenticazione remota**.
2. Selezionare uno dei seguenti servizi di autenticazione:

Se si seleziona...	Quindi...
Active Directory	<ol style="list-style-type: none">1. Immettere il nome e la password dell'amministratore.2. Specificare il nome distinto di base del server di autenticazione. Ad esempio, se il nome di dominio del server di autenticazione è ou@domain.com, il nome distinto di base è <code>cn=ou,dc=domain,dc=com</code>.
OpenLDAP	<ol style="list-style-type: none">1. Immettere il nome distinto e la password di bind.2. Specificare il nome distinto di base del server di autenticazione. Ad esempio, se il nome di dominio del server di autenticazione è ou@domain.com, il nome distinto di base è <code>cn=ou,dc=domain,dc=com</code>.

Se si seleziona...	Quindi...
Altri	<ol style="list-style-type: none"> 1. Immettere il nome distinto e la password di bind. 2. Specificare il nome distinto di base del server di autenticazione. Ad esempio, se il nome di dominio del server di autenticazione è <code>ou@domain.com</code>, il nome distinto di base è <code>cn=ou,dc=domain,dc=com</code>. 3. Specificare la versione del protocollo LDAP supportata dal server di autenticazione. 4. Immettere il nome utente, l'appartenenza al gruppo, il gruppo di utenti e gli attributi del membro.



Se si desidera modificare il servizio di autenticazione, è necessario eliminare tutti i server di autenticazione esistenti e aggiungere nuovi server di autenticazione.

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

Aggiunta di server di autenticazione

È possibile aggiungere server di autenticazione e abilitare l'autenticazione remota sul server di gestione in modo che gli utenti remoti all'interno del server di autenticazione possano accedere a Unified Manager.

Prima di iniziare


- Devono essere disponibili le seguenti informazioni:
 - Nome host o indirizzo IP del server di autenticazione
 - Numero di porta del server di autenticazione
- È necessario aver attivato l'autenticazione remota e configurato il servizio di autenticazione in modo che il server di gestione possa autenticare utenti o gruppi remoti nel server di autenticazione.
- È necessario disporre del ruolo di amministratore dell'applicazione.

A proposito di questa attività

Se il server di autenticazione che si sta aggiungendo fa parte di una coppia ad alta disponibilità (ha) (utilizzando lo stesso database), è possibile aggiungere anche il server di autenticazione partner. Ciò consente al server di gestione di comunicare con il partner quando uno dei server di autenticazione non è raggiungibile.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Generale > autenticazione remota**.
2. Attivare o disattivare l'opzione **Usa connessione protetta**:

Se si desidera...	Quindi...
Abilitarlo	<ol style="list-style-type: none"> 1. Selezionare l'opzione Usa connessione protetta. 2. Nella sezione Authentication Servers (Server di autenticazione), fare clic su Add (Aggiungi) 3. Nella finestra di dialogo Add Authentication Server (Aggiungi server di autenticazione), immettere il nome di autenticazione o l'indirizzo IP (IPv4 o IPv6) del server. 4. Nella finestra di dialogo autorizza host, fare clic su Visualizza certificato. 5. Nella finestra di dialogo Visualizza certificato, verificare le informazioni del certificato, quindi fare clic su Chiudi. 6. Nella finestra di dialogo autorizza host, fare clic su Si. <div style="border: 1px solid #ccc; padding: 10px; margin-top: 20px;">  <p>Quando si attiva l'opzione Usa autenticazione connessione sicura, Unified Manager comunica con il server di autenticazione e visualizza il certificato. Unified Manager utilizza 636 come porta predefinita per comunicazioni sicure e il numero di porta 389 per comunicazioni non sicure.</p> </div>
Disattivarlo	<ol style="list-style-type: none"> 1. Deselezionare l'opzione Usa connessione protetta. 2. Nella sezione Authentication Servers (Server di autenticazione), fare clic su Add (Aggiungi) 3. Nella finestra di dialogo Add Authentication Server (Aggiungi server di autenticazione), specificare il nome host o l'indirizzo IP (IPv4 o IPv6) del server e i dettagli della porta. 4. Fare clic su Aggiungi.

Il server di autenticazione aggiunto viene visualizzato nell'area Server.

1. Eseguire un'autenticazione di prova per confermare che è possibile autenticare gli utenti nel server di autenticazione aggiunto.

Verifica della configurazione dei server di autenticazione

È possibile convalidare la configurazione dei server di autenticazione per garantire che il server di gestione sia in grado di comunicare con essi. È possibile convalidare la

configurazione ricercando un utente remoto o un gruppo remoto dai server di autenticazione e autenticandoli utilizzando le impostazioni configurate.

Prima di iniziare

- È necessario aver attivato l'autenticazione remota e configurato il servizio di autenticazione in modo che il server Unified Manager possa autenticare l'utente remoto o il gruppo remoto.
- È necessario aggiungere i server di autenticazione in modo che il server di gestione possa cercare l'utente remoto o il gruppo remoto da questi server e autenticarli.
- È necessario disporre del ruolo di amministratore dell'applicazione.

A proposito di questa attività

Se il servizio di autenticazione è impostato su Active Directory e si sta convalidando l'autenticazione degli utenti remoti che appartengono al gruppo primario del server di autenticazione, le informazioni sul gruppo primario non vengono visualizzate nei risultati dell'autenticazione.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Generale > autenticazione remota**.
2. Fare clic su **Test Authentication**.
3. Nella finestra di dialogo **Test User**, specificare il nome utente e la password dell'utente remoto o il nome utente del gruppo remoto, quindi fare clic su **Test**.

Se si sta autenticando un gruppo remoto, non è necessario immettere la password.

Modifica dei server di autenticazione

È possibile modificare la porta utilizzata dal server Unified Manager per comunicare con il server di autenticazione.

Prima di iniziare

È necessario disporre del ruolo di amministratore dell'applicazione.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Generale > autenticazione remota**.
2. Selezionare la casella **Disable Nested Group Lookup** (Disattiva ricerca gruppi nidificati).
3. Nell'area **Authentication Servers** (Server di autenticazione), selezionare il server di autenticazione che si desidera modificare, quindi fare clic su **Edit** (Modifica).
4. Nella finestra di dialogo **Edit Authentication Server** (Modifica server di autenticazione), modificare i dettagli della porta.
5. Fare clic su **Save** (Salva).

Eliminazione dei server di autenticazione

È possibile eliminare un server di autenticazione se si desidera impedire al server Unified Manager di comunicare con il server di autenticazione. Ad esempio, se si desidera modificare un server di autenticazione con cui il server di gestione sta comunicando, è possibile eliminare il server di autenticazione e aggiungere un nuovo server di autenticazione.

Prima di iniziare

È necessario disporre del ruolo di amministratore dell'applicazione.

A proposito di questa attività

Quando si elimina un server di autenticazione, gli utenti remoti o i gruppi del server di autenticazione non potranno più accedere a Unified Manager.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Generale > autenticazione remota**.
2. Selezionare uno o più server di autenticazione che si desidera eliminare, quindi fare clic su **Delete** (Elimina).
3. Fare clic su **Sì** per confermare la richiesta di eliminazione.

Se l'opzione **Usa connessione sicura** è attivata, i certificati associati al server di autenticazione vengono cancellati insieme al server di autenticazione.

Autenticazione con Active Directory o OpenLDAP

È possibile attivare l'autenticazione remota sul server di gestione e configurare il server di gestione per comunicare con i server di autenticazione in modo che gli utenti all'interno dei server di autenticazione possano accedere a Unified Manager.

È possibile utilizzare uno dei seguenti servizi di autenticazione predefiniti o specificare un servizio di autenticazione personalizzato:

- Microsoft Active Directory



Non è possibile utilizzare Microsoft Lightweight Directory Services.

- OpenLDAP

È possibile selezionare il servizio di autenticazione richiesto e aggiungere i server di autenticazione appropriati per consentire agli utenti remoti nel server di autenticazione di accedere a Unified Manager. Le credenziali per utenti o gruppi remoti vengono gestite dal server di autenticazione. Il server di gestione utilizza il protocollo LDAP (Lightweight Directory Access Protocol) per autenticare gli utenti remoti all'interno del server di autenticazione configurato.

Per gli utenti locali creati in Unified Manager, il server di gestione gestisce il proprio database di nomi utente e

password. Il server di gestione esegue l'autenticazione e non utilizza Active Directory o OpenLDAP per l'autenticazione.

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 dell'applicazione.
- 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. Nel riquadro di spostamento a sinistra, fare clic su **General > SAML Authentication**.
2. Selezionare la casella di controllo **Enable SAML Authentication** (attiva autenticazione SAML).

Vengono visualizzati i campi necessari per configurare la connessione IdP.

3. 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).

4. 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.

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

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

6. 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. È possibile modificare il timeout della sessione GUI facendo clic su **General > Feature Settings > Inactivity Timeout**.

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” (autenticazione moduli), altrimenti gli utenti potrebbero ricevere un errore durante la disconnessione da Unified Manager . 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:

["Disattiva il controllo di revoca per fiducia della parte che si basa"](#)
 - 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.

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. Nel riquadro di spostamento a sinistra, fare clic su **General > SAML Authentication**.
2. 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).

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

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

5. 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.

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. Nel riquadro di spostamento a sinistra, fare clic su **General > SAML Authentication**.
2. Deselezionare la casella di controllo **Enable SAML Authentication** (attiva autenticazione SAML).
3. Fare clic su **Save** (Salva).

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

4. 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.

Registrazione dell'audit

È possibile rilevare se i registri di controllo sono stati compromessi con l'utilizzo dei registri di controllo. Tutte le attività eseguite da un utente vengono monitorate e registrate nei registri di controllo. I controlli vengono eseguiti per tutte le funzionalità dell'interfaccia utente e delle API` esposte pubblicamente di Active IQ Unified Manager.

Per visualizzare e accedere a tutti i file di log di audit disponibili in Active IQ Unified Manager, è possibile utilizzare la visualizzazione file del log di audit. I file nella visualizzazione file del registro di controllo sono elencati in base alla data di creazione. Questa vista visualizza le informazioni di tutti i log di controllo acquisiti dall'installazione o dall'aggiornamento al presente nel sistema. Ogni volta che si esegue un'azione in Unified Manager, le informazioni vengono aggiornate e sono disponibili nei registri. Lo stato di ciascun file di log viene acquisito utilizzando l'attributo "file Integrity Status", che viene monitorato attivamente per rilevare la manomissione o l'eliminazione del file di log. I registri di controllo possono avere uno dei seguenti stati quando i registri di controllo sono disponibili nel sistema:

Stato	Descrizione
ATTIVO	File in cui vengono attualmente registrati i log.
NORMALE	File inattivo, compresso e memorizzato nel sistema.
MANOMESSO	File che è stato compromesso da un utente che ha modificato manualmente il file.
MANUAL_DELETE	File eliminato da un utente autorizzato.
ROLLOVER_DELETE	File che è stato eliminato a causa dell'annullamento in base a criteri di configurazione a rotazione.
UNEXPECTED_DELETE	File eliminato per motivi sconosciuti.

La pagina Registro di controllo include i seguenti pulsanti di comando:

- Configurare

- Eliminare
- Scarica

Il pulsante **DELETE** consente di eliminare qualsiasi registro di controllo elencato nella vista registri di controllo. È possibile eliminare un registro di controllo e, facoltativamente, fornire un motivo per eliminare il file, in modo da poter determinare un'eliminazione valida in futuro. La colonna REASON (MOTIVO) elenca il motivo insieme al nome dell'utente che ha eseguito l'operazione di eliminazione.



L'eliminazione di un file di log causerà l'eliminazione del file dal sistema, ma la voce nella tabella DB non verrà eliminata.

È possibile scaricare i registri di controllo da Active IQ Unified Manager utilizzando il pulsante **DOWNLOAD** nella sezione registri di controllo ed esportare i file di registro di controllo. I file contrassegnati con "NORMAL" o "MANOMESSI" vengono scaricati in un file compresso .zip formato.

Quando viene generato un bundle AutoSupport completo, il bundle di supporto include file di log di audit sia archiviati che attivi. Tuttavia, quando viene generato un bundle di supporto leggero, include solo i registri di controllo attivi. I registri di controllo archiviati non sono inclusi.

Configurazione dei registri di audit

È possibile utilizzare il pulsante **Configura** nella sezione registri di controllo per configurare i criteri di rolling per i file di registro di controllo e per attivare la registrazione remota per i registri di controllo.

A proposito di questa attività

È possibile impostare i valori nei CAMPI **MAX FILE SIZE** e **AUDIT LOG RETENTION DAYS** in base alla quantità e alla frequenza desiderate dei dati che si desidera memorizzare nel sistema. Il valore nel campo **TOTAL AUDIT LOG SIZE** (DIMENSIONE TOTALE REGISTRO DI CONTROLLO) è la dimensione dei dati totali del registro di controllo presenti nel sistema. La policy di rollover è determinata dai valori nel campo **GIORNI DI CONSERVAZIONE DEL REGISTRO DI CONTROLLO, dimensione DEL FILE MAX e DIMENSIONE TOTALE DEL REGISTRO DI CONTROLLO**. Quando la dimensione del backup del registro di controllo raggiunge il valore configurato in **TOTAL AUDIT LOG SIZE**, il file archiviato per primo viene cancellato. Ciò significa che il file meno recente viene cancellato. Tuttavia, la voce del file continua a essere disponibile nel database ed è contrassegnata come "Elimina rollover". Il valore **GIORNI di CONSERVAZIONE del REGISTRO DI CONTROLLO** corrisponde al numero di giorni in cui i file di registro di controllo vengono conservati. Viene eseguito il rollover di qualsiasi file precedente al valore impostato in questo campo.

Fasi

1. Fare clic su **Audit Logs > * > Configura***.
2. Inserire i valori nelle voci **MAX FILE SIZE, TOTAL AUDIT LOG SIZE e AUDIT LOG RETENTION DAYS**.

Se si desidera attivare la registrazione remota, selezionare **Enable Remote Logging** (attiva registrazione remota).

Abilitazione della registrazione remota dei registri di controllo

È possibile selezionare la casella di controllo **Enable Remote Logging** (attiva registrazione remota) nella finestra di dialogo Configure Audit Logs (Configura registri di

controllo) per attivare la registrazione remota dell'audit. È possibile utilizzare questa funzione per trasferire i registri di controllo a un server Syslog remoto. In questo modo, è possibile gestire i registri di controllo in caso di limiti di spazio.

A proposito di questa attività

La registrazione remota dei registri di controllo fornisce un backup a prova di manomissione nel caso in cui i file di registro di controllo sul server Active IQ Unified Manager vengano manomessi.

Fasi

1. Nella finestra di dialogo **Configura registri di controllo**, selezionare la casella di controllo **attiva registrazione remota**.

Vengono visualizzati ulteriori campi per configurare la registrazione remota.

2. Immettere il **NOME HOST** e la **PORTA** del server remoto a cui si desidera connettersi.
3. Nel campo **CERTIFICATO CA DEL SERVER**, fare clic su **SFOGLIA** per selezionare un certificato pubblico del server di destinazione.

Il certificato deve essere caricato in `.pem` formato. Questo certificato deve essere ottenuto dal server Syslog di destinazione e non deve essere scaduto. Il certificato deve contenere il "hostname" selezionato come parte di `SubjectAltName (SAN)`.

4. Immettere i valori per i seguenti campi: **CHARSET**, **TIMEOUT CONNESSIONE**, **RITARDO DI RICONNESSIONE**.

I valori devono essere espressi in millisecondi per questi campi.

5. Selezionare il formato Syslog e la versione del protocollo TLS richiesti nei campi **FORMAT** e **PROTOCOL**.
6. Selezionare la casella di controllo **Enable Client Authentication** (attiva autenticazione client) se il server Syslog di destinazione richiede l'autenticazione basata su certificato.

Prima di salvare la configurazione del registro di controllo, sarà necessario scaricare il certificato di autenticazione del client e caricarlo sul server Syslog, altrimenti la connessione non avrà esito positivo. A seconda del tipo di server Syslog, potrebbe essere necessario creare un hash del certificato di autenticazione del client.

Esempio: Syslog-ng richiede la creazione di un <hash> del certificato utilizzando il comando `openssl x509 -noout -hash -in cert.pem`, quindi collegare simbolicamente il certificato di autenticazione del client a un file denominato dopo <hash> .0.

7. Fare clic su **Save** (Salva) per configurare la connessione con il server e attivare la registrazione remota.

Verrà reindirizzato alla pagina Audit Logs (registri di controllo).

Descrizione delle finestre di autenticazione e delle finestre di dialogo

È possibile attivare l'autenticazione LDAP dalla pagina Setup/Authentication (Configurazione/autenticazione).

Pagina Remote Authentication (autenticazione remota)

È possibile utilizzare la pagina Remote Authentication (autenticazione remota) per configurare Unified Manager in modo che comunichi con il server di autenticazione per autenticare gli utenti remoti che tentano di accedere all'interfaccia utente Web di Unified Manager.

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Dopo aver selezionato la casella di controllo Enable remote Authentication (attiva autenticazione remota), è possibile attivare l'autenticazione remota utilizzando un server di autenticazione.

- **Servizio di autenticazione**

Consente di configurare il server di gestione per autenticare gli utenti nei provider di servizi di directory, ad esempio Active Directory, OpenLDAP o specificare il proprio meccanismo di autenticazione. È possibile specificare un servizio di autenticazione solo se è stata attivata l'autenticazione remota.

- **Active Directory**

- Nome amministratore

Specifica il nome dell'amministratore del server di autenticazione.

- Password

Specifica la password per accedere al server di autenticazione.

- Nome distinto di base

Specifica la posizione degli utenti remoti nel server di autenticazione. Ad esempio, se il nome di dominio del server di autenticazione è `ou@domain.com`, il nome distinto di base è `cn=ou,dc=domain,dc=com`.

- Disattiva ricerca gruppi nidificati

Specifica se attivare o disattivare l'opzione di ricerca di gruppi nidificati. Per impostazione predefinita, questa opzione è disattivata. Se si utilizza Active Directory, è possibile accelerare l'autenticazione disattivando il supporto per i gruppi nidificati.

- USA connessione sicura

Specifica il servizio di autenticazione utilizzato per comunicare con i server di autenticazione.

- **OpenLDAP**

- Associa nome distinto

Specifica il nome distinto di binding utilizzato insieme al nome distinto di base per trovare gli utenti remoti nel server di autenticazione.

- Password bind

Specifica la password per accedere al server di autenticazione.

- Nome distinto di base

Specifica la posizione degli utenti remoti nel server di autenticazione. Ad esempio, se il nome di dominio del server di autenticazione è [ou@domain.com](#), il nome distinto di base è `cn=ou,dc=domain,dc=com`.

- USA connessione sicura

Specifica che il protocollo LDAP sicuro viene utilizzato per comunicare con i server di autenticazione LDAPS.

- **Altri**

- Associa nome distinto

Specifica il nome distinto di binding utilizzato insieme al nome distinto di base per trovare gli utenti remoti nel server di autenticazione configurato.

- Password bind

Specifica la password per accedere al server di autenticazione.

- Nome distinto di base

Specifica la posizione degli utenti remoti nel server di autenticazione. Ad esempio, se il nome di dominio del server di autenticazione è [ou@domain.com](#), il nome distinto di base è `cn=ou,dc=domain,dc=com`.

- Versione del protocollo

Specifica la versione LDAP (Lightweight Directory Access Protocol) supportata dal server di autenticazione. È possibile specificare se la versione del protocollo deve essere rilevata automaticamente o impostata su 2 o 3.

- Attributo User Name

Specifica il nome dell'attributo nel server di autenticazione che contiene i nomi di accesso dell'utente da autenticare dal server di gestione.

- Attributo Group Membership

Specifica un valore che assegna l'appartenenza al gruppo di server di gestione agli utenti remoti in base a un attributo e a un valore specificati nel server di autenticazione dell'utente.

- UGID

Se gli utenti remoti sono inclusi come membri di un oggetto GroupOfUniqueNames nel server di autenticazione, questa opzione consente di assegnare l'appartenenza al gruppo di server di gestione agli utenti remoti in base a un attributo specificato nell'oggetto GroupOfUniqueNames.

- Disattiva ricerca gruppi nidificati

Specifica se attivare o disattivare l'opzione di ricerca di gruppi nidificati. Per impostazione predefinita, questa opzione è disattivata. Se si utilizza Active Directory, è possibile accelerare l'autenticazione disattivando il supporto per i gruppi nidificati.

- Membro

Specifica il nome dell'attributo utilizzato dal server di autenticazione per memorizzare informazioni sui singoli membri di un gruppo.

- User Object Class (Classe oggetto utente)

Specifica la classe di oggetti di un utente nel server di autenticazione remoto.

- Group Object Class (Classe oggetti gruppo)

Specifica la classe di oggetti di tutti i gruppi nel server di autenticazione remoto.

- USA connessione sicura

Specifica il servizio di autenticazione utilizzato per comunicare con i server di autenticazione.



Se si desidera modificare il servizio di autenticazione, assicurarsi di eliminare tutti i server di autenticazione esistenti e aggiungere nuovi server di autenticazione.

Area Authentication Servers

L'area Authentication Servers (Server di autenticazione) visualizza i server di autenticazione con cui il server di gestione comunica per individuare e autenticare gli utenti remoti. Le credenziali per utenti o gruppi remoti vengono gestite dal server di autenticazione.

• Pulsanti di comando

Consente di aggiungere, modificare o eliminare i server di autenticazione.

- Aggiungi

Consente di aggiungere un server di autenticazione.

Se il server di autenticazione che si sta aggiungendo fa parte di una coppia ad alta disponibilità (utilizzando lo stesso database), è possibile aggiungere anche il server di autenticazione partner. Ciò consente al server di gestione di comunicare con il partner quando uno dei server di autenticazione non è raggiungibile.

- Modifica

Consente di modificare le impostazioni di un server di autenticazione selezionato.

- Eliminare

Elimina i server di autenticazione selezionati.

• Nome o indirizzo IP

Visualizza il nome host o l'indirizzo IP del server di autenticazione utilizzato per autenticare l'utente sul server di gestione.

• Porta

Visualizza il numero di porta del server di autenticazione.

• Verifica dell'autenticazione

Questo pulsante convalida la configurazione del server di autenticazione autenticando un utente o un gruppo remoto.

Durante il test, se si specifica solo il nome utente, il server di gestione ricerca l'utente remoto nel server di autenticazione, ma non autenticare l'utente. Se si specificano sia il nome utente che la password, il server di gestione ricerca e autentica l'utente remoto.

Non è possibile verificare l'autenticazione se l'autenticazione remota è disattivata.

Pagina SAML Authentication

È possibile utilizzare la pagina SAML Authentication per configurare Unified Manager in modo che autentichi gli utenti remoti utilizzando 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, selezionare la casella di controllo Enable SAML Authentication (attiva autenticazione SAML) per abilitare l'autenticazione utilizzando un provider di identità sicuro.

• IDP URI

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

URI di esempio ADFS:

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

URI di esempio Shibboleth:

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

• Metadati IdP

I metadati IdP in formato XML.

Se l'URL IdP è accessibile dal server di Unified Manager, fare clic sul pulsante **Fetch IdP Metadata** (Scarica metadati IdP) per compilare questo campo.

• Sistema host (FQDN)

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

• URI host

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

- **Metadati host**

I metadati del sistema host in formato XML.

Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.