Configurare le impostazioni di sicurezza

StorageGRID software

NetApp
December 03, 2025

Sommario

Configurare le impostazioni di sicurezza

Gestire la politica TLS e SSH

La policy TLS e SSH determina quali protocolli e cifrari vengono utilizzati per stabilire connessioni TLS sicure con le applicazioni client e connessioni SSH sicure con i servizi StorageGRID interni.

La policy di sicurezza controlla il modo in cui TLS e SSH crittografano i dati in movimento. In generale, utilizzare il criterio di compatibilità moderna (predefinito), a meno che il sistema non debba essere conforme ai Common Criteria o non sia necessario utilizzare altri cifrari.

Alcuni servizi StorageGRID non sono stati aggiornati per utilizzare le cifrature in queste policy.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un"browser web supportato" .
- Tu hai il"Permesso di accesso root" .

Seleziona una politica di sicurezza

Passi

1. Selezionare **CONFIGURAZIONE** > **Sicurezza** > **Impostazioni di sicurezza**.

   La scheda **Criteri TLS e SSH** mostra i criteri disponibili. La policy attualmente attiva è contrassegnata da un segno di spunta verde nel riquadro della policy.

2. Esamina i riquadri per scoprire le policy disponibili.

Politica	Descrizione
Compatibilità moderna (predefinita)	Utilizzare il criterio predefinito se è necessaria una crittografia avanzata e a meno che non si abbiano requisiti particolari. Questa policy è compatibile con la maggior parte dei client TLS e SSH.
Compatibilità legacy	Utilizza questa policy se hai bisogno di opzioni di compatibilità aggiuntive per i client più vecchi. Le opzioni aggiuntive presenti in questa policy potrebbero renderla meno sicura rispetto alla policy di compatibilità moderna.

Politica	Descrizione
Criteri comuni	Utilizzare questa politica se è necessaria la certificazione Common Criteria.
FIPS rigoroso	Utilizzare questa policy se è richiesta la certificazione Common Criteria e si deve utilizzare NetApp Cryptographic Security Module 3.0.8 per le connessioni client esterne agli endpoint del bilanciatore del carico, Tenant Manager e Grid Manager. L'utilizzo di questa policy potrebbe ridurre le prestazioni. **Nota**: Dopo aver selezionato questa policy, tutti i nodi devono essere"riavviato in modo progressivo" per attivare il modulo di sicurezza crittografica NetApp . Utilizzare **Manutenzione** > **Riavvio progressivo** per avviare e monitorare i riavvii.
Costume	Crea una policy personalizzata se devi applicare i tuoi cifrari.

3. Per visualizzare i dettagli sui cifrari, i protocolli e gli algoritmi di ogni policy, seleziona **Visualizza dettagli**.
4. Per modificare la policy corrente, seleziona **Usa policy**.

   Accanto a **Criterio attuale** nel riquadro del criterio appare un segno di spunta verde.

Crea una policy di sicurezza personalizzata

È possibile creare una policy personalizzata se è necessario applicare cifrari personalizzati.

Passi

1. Dal riquadro della policy più simile alla policy personalizzata che desideri creare, seleziona **Visualizza dettagli**.
2. Selezionare **Copia negli appunti**, quindi selezionare **Annulla**.

3. Dal riquadro **Criterio personalizzato**, seleziona **Configura e usa**.

4. Incolla il JSON che hai copiato e apporta le modifiche necessarie.
5. Seleziona **Utilizza policy**.

   Accanto a **Criterio attuale** nel riquadro Criterio personalizzato appare un segno di spunta verde.

6. Facoltativamente, seleziona **Modifica configurazione** per apportare ulteriori modifiche alla nuova policy personalizzata.

Ripristina temporaneamente la politica di sicurezza predefinita

Se hai configurato un criterio di sicurezza personalizzato, potresti non essere in grado di accedere a Grid Manager se il criterio TLS configurato non è compatibile con"certificato del server configurato" .

È possibile ripristinare temporaneamente i criteri di sicurezza predefiniti.

Passi

1. Accedi a un nodo di amministrazione:
   a. Immettere il seguente comando: `ssh admin@Admin_Node_IP`
   b. Inserisci la password elencata nel `Passwords.txt` file.
   c. Immettere il seguente comando per passare alla root: `su -`
   d. Inserisci la password elencata nel `Passwords.txt` file.

      Quando si accede come root, il prompt cambia da `$` A `#` .

2. Esegui il seguente comando:

   ```
   restore-default-cipher-configurations
   ```

3. Da un browser Web, accedi a Grid Manager sullo stesso nodo di amministrazione.
4. Segui i passaggi inSeleziona una politica di sicurezza per configurare nuovamente la policy.

Configurare la sicurezza della rete e degli oggetti

È possibile configurare la sicurezza di rete e degli oggetti per crittografare gli oggetti archiviati, per impedire determinate richieste S3 o per consentire alle connessioni client ai nodi di archiviazione di utilizzare HTTP anziché HTTPS.

Crittografia degli oggetti memorizzati

La crittografia degli oggetti archiviati consente la crittografia di tutti i dati degli oggetti quando vengono acquisiti tramite S3. Per impostazione predefinita, gli oggetti archiviati non sono crittografati, ma è possibile scegliere di crittografarli utilizzando l'algoritmo di crittografia AES-128 o AES-256. Quando si abilita l'impostazione, tutti gli oggetti appena acquisiti vengono crittografati, ma non viene apportata alcuna modifica agli oggetti archiviati esistenti. Se si disabilita la crittografia, gli oggetti attualmente crittografati rimangono crittografati, ma gli oggetti appena acquisiti non vengono crittografati.

L'impostazione di crittografia degli oggetti archiviati si applica solo agli oggetti S3 che non sono stati crittografati tramite crittografia a livello di bucket o di oggetto.

Per maggiori dettagli sui metodi di crittografia StorageGRID , vedere"Esaminare i metodi di crittografia StorageGRID" .

Impedisci la modifica del client

Impedisci modifiche al client è un'impostazione a livello di sistema. Quando è selezionata l'opzione **Impedisci modifiche client**, le seguenti richieste vengono rifiutate.

API REST S3

- Richieste DeleteBucket
- Qualsiasi richiesta di modifica dei dati di un oggetto esistente, dei metadati definiti dall'utente o del tagging degli oggetti S3

Abilita HTTP per le connessioni del nodo di archiviazione

Per impostazione predefinita, le applicazioni client utilizzano il protocollo di rete HTTPS per tutte le connessioni dirette ai nodi di archiviazione. Facoltativamente, è possibile abilitare HTTP per queste connessioni, ad esempio quando si testa una griglia non di produzione.

Utilizzare HTTP per le connessioni ai nodi di archiviazione solo se i client S3 devono effettuare connessioni HTTP direttamente ai nodi di archiviazione. Non è necessario utilizzare questa opzione per i client che utilizzano solo connessioni HTTPS o per i client che si connettono al servizio Load Balancer (perché è possibile"configurare ogni endpoint del bilanciatore del carico" per utilizzare HTTP o HTTPS).

Vedere"Riepilogo: indirizzi IP e porte per le connessioni client" per scoprire quali porte utilizzano i client S3 quando si connettono ai nodi di archiviazione tramite HTTP o HTTPS.

Seleziona le opzioni

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un"browser web supportato" .
- Hai i permessi di accesso Root.

Passi

1. Selezionare **CONFIGURAZIONE** > **Sicurezza** > **Impostazioni di sicurezza**.
2. Selezionare la scheda **Rete e oggetti**.
3. Per la crittografia degli oggetti archiviati, utilizzare l'impostazione **Nessuno** (predefinita) se non si desidera che gli oggetti archiviati vengano crittografati oppure selezionare **AES-128** o **AES-256** per crittografare gli oggetti archiviati.
4. Facoltativamente, seleziona **Impedisci modifica client** se vuoi impedire ai client S3 di effettuare richieste specifiche.

   > Se si modifica questa impostazione, ci vorrà circa un minuto prima che la nuova impostazione venga applicata. Il valore configurato viene memorizzato nella cache per migliorare le prestazioni e il ridimensionamento.

5. Facoltativamente, selezionare **Abilita HTTP per le connessioni ai nodi di archiviazione** se i client si connettono direttamente ai nodi di archiviazione e si desidera utilizzare le connessioni HTTP.

Prestare attenzione quando si abilita HTTP per una griglia di produzione perché le richieste verranno inviate non crittografate.

6. Seleziona **Salva**.

Modificare le impostazioni di sicurezza dell'interfaccia

Le impostazioni di sicurezza dell'interfaccia consentono di controllare se gli utenti vengono disconnessi se rimangono inattivi per un periodo di tempo superiore a quello specificato e se una traccia dello stack viene inclusa nelle risposte di errore dell'API.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un"browser web supportato" .
- Hai"Permesso di accesso root" .

Informazioni su questo compito

La pagina **Impostazioni di sicurezza** include le impostazioni **Timeout di inattività del browser** e **Stack trace dell'API di gestione**.

Timeout di inattività del browser

Indica per quanto tempo il browser di un utente può rimanere inattivo prima che l'utente venga disconnesso. Il valore predefinito è 15 minuti.

Il timeout di inattività del browser è controllato anche da quanto segue:

- Un timer StorageGRID separato e non configurabile, incluso per la sicurezza del sistema. Il token di autenticazione di ciascun utente scade 16 ore dopo l'accesso dell'utente. Quando scade l'autenticazione di un utente, l'utente viene automaticamente disconnesso, anche se il timeout di inattività del browser è disabilitato o il valore per il timeout del browser non è stato raggiunto. Per rinnovare il token, l'utente deve effettuare nuovamente l'accesso.
- Impostazioni di timeout per il provider di identità, presupponendo che l'accesso Single Sign-On (SSO) sia abilitato per StorageGRID.

  Se l'SSO è abilitato e il browser di un utente scade, l'utente deve reinserire le proprie credenziali SSO per accedere nuovamente a StorageGRID . Vedere "Configurare l'accesso singolo" .

Stack trace dell'API di gestione

Controlla se viene restituita una traccia dello stack nelle risposte di errore dell'API Grid Manager e Tenant Manager.

Questa opzione è disabilitata per impostazione predefinita, ma potrebbe essere opportuno abilitare questa funzionalità per un ambiente di prova. In generale, negli ambienti di produzione è consigliabile lasciare la traccia dello stack disabilitata per evitare di rivelare dettagli software interni quando si verificano errori API.

Passi

1. Selezionare **CONFIGURAZIONE** > **Sicurezza** > **Impostazioni di sicurezza**.
2. Selezionare la scheda **Interfaccia**.
3. Per modificare l'impostazione del timeout di inattività del browser:
   a. Espandi la fisarmonica.

b. Per modificare il periodo di timeout, specificare un valore compreso tra 60 secondi e 7 giorni. Il timeout predefinito è 15 minuti.

c. Per disattivare questa funzione, deselezionare la casella di controllo.

d. Seleziona **Salva**.

La nuova impostazione non ha effetto sugli utenti che hanno effettuato l'accesso. Gli utenti devono effettuare nuovamente l'accesso o aggiornare il browser affinché la nuova impostazione di timeout abbia effetto.

4. Per modificare l'impostazione per la traccia dello stack dell'API di gestione:

a. Espandi la fisarmonica.

b. Selezionare la casella di controllo per restituire una traccia dello stack nelle risposte di errore dell'API Grid Manager e Tenant Manager.

Lasciare la traccia dello stack disabilitata negli ambienti di produzione per evitare di rivelare dettagli software interni quando si verificano errori API.

c. Seleziona **Salva**.

Informazioni sul copyright

Informazioni sul marchio commerciale