Configurare le impostazioni di sicurezza

StorageGRID 11.7

NetApp
April 12, 2024

Sommario

Configurare le impostazioni di sicurezza

Gestire i criteri TLS e SSH

I criteri TLS e SSH determinano i protocolli e le crittografia utilizzati per stabilire connessioni TLS sicure con le applicazioni client e connessioni SSH sicure ai servizi StorageGRID interni.

Il criterio di sicurezza controlla il modo in cui TLS e SSH crittografano i dati in movimento. In generale, utilizzare il criterio di compatibilità moderno (predefinito), a meno che il sistema non debba essere conforme ai criteri comuni o non sia necessario utilizzare altre crittografia.

Alcuni servizi StorageGRID non sono stati aggiornati per utilizzare le crittografia di questi criteri.

Prima di iniziare

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

Selezionare una policy di sicurezza

Fasi

1. Selezionare **CONFIGURATION** > **Security** > **Security settings**.

   La scheda **TLS and SSH policies** (Criteri TLS e SSH) mostra i criteri disponibili. Il criterio attualmente attivo è contrassegnato da un segno di spunta verde sul riquadro del criterio.

2. Consulta i riquadri per scoprire le policy disponibili.

Policy	Descrizione
Compatibilità moderna (impostazione predefinita)	Utilizzare il criterio predefinito se è necessaria una crittografia avanzata e se non si dispone di requisiti speciali. Questo criterio è compatibile con la maggior parte dei client TLS e SSH.
Compatibilità con le versioni precedenti	Utilizzare questo criterio se sono necessarie ulteriori opzioni di compatibilità per i client meno recenti. Le opzioni aggiuntive di questa policy potrebbero renderla meno sicura rispetto alla moderna policy di compatibilità.

Policy	Descrizione
Criteri comuni	Utilizzare questa policy se si richiede la certificazione Common Criteria.
FIPS rigoroso	Utilizzare questa policy se si richiede la certificazione Common Criteria e si desidera utilizzare NetApp Cryptographic Security Module 3.0.0 per le connessioni client esterne agli endpoint del bilanciamento del carico, a Tenant Manager e a Grid Manager. L'utilizzo di questo criterio potrebbe ridurre le performance.
Personalizzato	Creare un criterio personalizzato se è necessario applicare le proprie crittografia.

3. Per visualizzare i dettagli relativi a crittografia, protocolli e algoritmi di ogni policy, selezionare **Visualizza dettagli**.
4. Per modificare la policy corrente, selezionare **Usa policy**.

   Un segno di spunta verde viene visualizzato accanto a **policy corrente** nel riquadro del criterio.

Creare una policy di sicurezza personalizzata

È possibile creare una policy personalizzata se è necessario applicare le proprie crittografia.

Fasi

1. Dal riquadro del criterio più simile al criterio personalizzato che si desidera creare, selezionare **Visualizza dettagli**.
2. Selezionare **Copia negli Appunti**, quindi selezionare **Annulla**.

3. Dal riquadro **Custom policy**, selezionare **Configure and use** (Configura e utilizza).
4. Incollare il JSON copiato e apportare le modifiche necessarie.
5. Selezionare **Usa policy**.

Un segno di spunta verde viene visualizzato accanto a **Current policy** (policy corrente) nel riquadro Custom policy (policy personalizzate).

6. Facoltativamente, selezionare **Edit Configuration** (Modifica configurazione) per apportare ulteriori modifiche al nuovo criterio personalizzato.

Ripristinare temporaneamente il criterio di protezione predefinito

Se è stato configurato un criterio di protezione personalizzato, potrebbe non essere possibile accedere a Grid Manager se il criterio TLS configurato non è compatibile con "certificato server configurato".

È possibile ripristinare temporaneamente i criteri di protezione predefiniti.

Fasi

1. Accedere a un nodo amministratore:
   a. Immettere il seguente comando: `ssh admin@Admin_Node_IP`
   b. Immettere la password elencata in `Passwords.txt` file.
   c. Immettere il seguente comando per passare a root: `su -`
   d. Immettere la password elencata in `Passwords.txt` file.

      Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

2. Eseguire il seguente comando:

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

3. Da un browser Web, accedere a Grid Manager sullo stesso nodo di amministrazione.
4. Seguire la procedura descritta in Selezionare una policy di sicurezza per configurare nuovamente il criterio.

Configurare la sicurezza della rete e degli oggetti

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

Crittografia degli oggetti memorizzati

La crittografia degli oggetti memorizzati consente la crittografia di tutti i dati degli oggetti durante l'acquisizione tramite S3. Per impostazione predefinita, gli oggetti memorizzati non vengono crittografati, ma è possibile scegliere di crittografare gli oggetti utilizzando l'algoritmo di crittografia AES-128 o AES-256. Quando si attiva l'impostazione, tutti gli oggetti inseriti di recente vengono crittografati, ma non vengono apportate modifiche agli oggetti memorizzati esistenti. Se si disattiva la crittografia, gli oggetti attualmente crittografati rimangono crittografati, ma gli oggetti appena acquisiti non vengono crittografati.

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

Per ulteriori informazioni sui metodi di crittografia StorageGRID, vedere "Esaminare i metodi di crittografia StorageGRID".

Impedire la modifica del client

Impedisci modifica client è un'impostazione a livello di sistema. Quando si seleziona l'opzione **Impedisci modifica client**, le seguenti richieste vengono rifiutate.

API REST S3

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

API Swift REST

- Eliminare le richieste di container
- Richiede di modificare qualsiasi oggetto esistente. Ad esempio, le seguenti operazioni sono negate: Put Overwrite (Inserisci sovrascrittura), Delete (Elimina), Metadata Update (aggiornamento metadati) e così via.

Abilitare HTTP per le connessioni dei nodi di storage

Per impostazione predefinita, le applicazioni client utilizzano il protocollo di rete HTTPS per qualsiasi connessione diretta ai nodi di storage. È possibile attivare il protocollo HTTP per queste connessioni, ad esempio durante il test di un grid non di produzione.

Utilizzare HTTP per le connessioni dei nodi di storage solo se i client S3 e Swift devono stabilire connessioni HTTP direttamente ai nodi di storage. 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 ciascun endpoint del bilanciamento del carico" Per utilizzare HTTP o HTTPS).

Vedere "Riepilogo: Indirizzi IP e porte per le connessioni client" Per sapere quali porte S3 e i client Swift utilizzano per la connessione ai nodi di storage utilizzando HTTP o HTTPS.

Selezionare le opzioni

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Si dispone dell'autorizzazione di accesso root.

Fasi

1. Selezionare **CONFIGURATION** > **Security** > **Security settings**.
2. Selezionare la scheda **rete e oggetti**.
3. Per la crittografia degli oggetti memorizzati, utilizzare l'impostazione **None** (predefinita) se non si desidera crittografare gli oggetti memorizzati oppure selezionare **AES-128** o **AES-256** per crittografare gli oggetti memorizzati.
4. Se si desidera impedire ai client S3 e Swift di effettuare richieste specifiche, selezionare **Impedisci modifica client**.

> Se si modifica questa impostazione, l'applicazione della nuova impostazione richiede circa un minuto. Il valore configurato viene memorizzato nella cache per le prestazioni e la scalabilità.

5. Se si desidera utilizzare connessioni HTTP, selezionare **Enable HTTP for Storage Node Connections** (attiva HTTP per connessioni nodo di storage) se i client si connettono direttamente ai nodi di storage.

> Prestare attenzione quando si attiva HTTP per una griglia di produzione perché le richieste verranno inviate senza crittografia.

6. Selezionare **Salva**.

Modificare il timeout di inattività del browser

È possibile controllare se gli utenti di Grid Manager e Tenant Manager vengono disconnessi se rimangono inattivi per più di un certo periodo di tempo.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Si dispone dell'autorizzazione di accesso root.

A proposito di questa attività

Il timeout di inattività del browser viene impostato per impostazione predefinita su 15 minuti. Se il browser di un utente non è attivo per questo periodo di tempo, l'utente viene disconnesso.

Se necessario, è possibile aumentare o ridurre il periodo di timeout impostando l'opzione **Disconnetti utenti inattivi dopo**.

Il timeout di inattività del browser è controllato anche da:

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

  Se SSO è attivato e il browser dell'utente si disinserisce, l'utente deve immettere nuovamente le proprie credenziali SSO per accedere nuovamente a StorageGRID. Vedere "Configurare il single sign-on".

Fasi

1. Selezionare **CONFIGURATION** > **Security** > **Security settings**.
2. Selezionare la scheda **Timeout inattività browser**.
3. Nel campo **Disconnetti utenti inattivi dopo**, specificare un periodo di timeout del browser compreso tra 60 secondi e 7 giorni.

   È possibile specificare il periodo di timeout del browser in secondi, minuti, ore o giorni.

4. Selezionare **Salva**. Se un browser rimane inattivo per il periodo di tempo specificato, l'utente viene disconnesso da Grid Manager o da Tenant Manager.

   La nuova impostazione non influisce sugli utenti attualmente registrati. Gli utenti devono effettuare nuovamente l'accesso o aggiornare il browser per rendere effettiva la nuova impostazione di timeout.