



Configurare le impostazioni di sicurezza

StorageGRID 11.9

NetApp
November 08, 2024

Sommario

- Configurare le impostazioni di sicurezza 1
 - Gestire i criteri TLS e SSH 1
 - Configurare la sicurezza della rete e degli oggetti 3
 - Modificare le impostazioni di sicurezza dell'interfaccia 5

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

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["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 questo criterio se si richiede la certificazione Common Criteria e si deve utilizzare il modulo di protezione Cryptographic NetApp 3.0.8 per connessioni client esterne agli endpoint di bilanciamento del carico, a Gestore tenant e a Gestione griglia. L'utilizzo di questo criterio potrebbe ridurre le performance. Nota: Dopo aver selezionato questo criterio, tutti i nodi devono "riavviato in modo scorrevole" attivare il modulo di protezione crittografica NetApp. Utilizzare manutenzione > riavvio in sequenza per avviare e riavviare il monitor. |
| 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 nel `Passwords.txt` file.
 - c. Immettere il seguente comando per passare alla directory principale: `su -`
 - d. Immettere la password elencata nel `Passwords.txt` file.

Quando si è collegati 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. Per configurare nuovamente il criterio, procedere come [Selezionare una policy di sicurezza](#) segue.

Configurare la sicurezza della rete e degli oggetti

È possibile configurare la protezione della rete e degli oggetti per crittografare gli oggetti archiviati, impedire determinate richieste S3 o consentire alle connessioni client ai nodi di archiviazione 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

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

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 al nodo di archiviazione solo se i client S3 devono stabilire 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 (poiché è possibile ["configurare ciascun endpoint del bilanciamento del carico"](#) utilizzare HTTP o HTTPS).

Vedere ["Riepilogo: Indirizzi IP e porte per le connessioni client"](#) per informazioni sulle porte utilizzate dai client S3 durante la connessione ai nodi di archiviazione tramite HTTP o HTTPS.

Selezionare le opzioni

Prima di iniziare

- L'utente ha 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 di eseguire 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 le impostazioni di sicurezza dell'interfaccia

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

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Autorizzazione di accesso root"](#).

A proposito di questa attività

La pagina **Impostazioni di protezione** include le impostazioni **Timeout inattività browser** e **traccia stack 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. L'impostazione predefinita è 15 minuti.

Il timeout di inattività del browser è controllato anche da:

- Un timer StorageGRID separato, non configurabile, incluso per la sicurezza del sistema. Ogni token di autenticazione dell'utente scade 16 ore dopo l'accesso. Quando l'autenticazione dell'utente scade, l'utente viene automaticamente disconnesso, anche se il timeout di inattività del browser è disattivato o non è stato raggiunto il valore per il 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"](#).

Traccia stack API di gestione

Controlla se una traccia di stack viene restituita nelle risposte di errore delle API di Gestione griglia e di Gestione tenant.

Questa opzione è disattivata per impostazione predefinita, ma potrebbe essere necessario attivarla per un ambiente di test. In generale, è necessario lasciare disattivata la traccia dello stack negli ambienti di produzione per evitare di rivelare i dettagli del software interno quando si verificano errori API.

Fasi

1. Selezionare **CONFIGURATION > Security > Security settings**.
2. Selezionare la scheda **interfaccia**.
3. Per modificare l'impostazione del timeout di inattività del browser:
 - a. Espandere la fisarmonica.

- b. Per modificare il periodo di timeout, specificare un valore compreso tra 60 secondi e 7 giorni. Il timeout predefinito è di 15 minuti.
- c. Per disattivare questa funzione, deselezionare la casella di controllo.
- d. Selezionare **Salva**.

La nuova impostazione non influisce sugli utenti che hanno effettuato l'accesso. Per rendere effettiva la nuova impostazione di timeout, gli utenti devono eseguire nuovamente l'accesso o aggiornare il browser.

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

- a. Espandere la fisarmonica.
- b. Selezionare la casella di controllo per restituire una traccia di stack nelle risposte agli errori di API di Gestione griglia e di Gestione tenant.



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

- c. Selezionare **Salva**.

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.