Configurare le impostazioni di sicurezza

StorageGRID software

NetApp
February 12, 2026

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

- 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 **Configurazione** > **Sicurezza** > **Impostazioni di sicurezza**.

   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 le schede per conoscere le policy disponibili.

Compatibilità moderna (impostazione predefinita)

Utilizza il criterio predefinito se hai bisogno di una crittografia avanzata e non hai requisiti particolari. Questa policy è compatibile con la maggior parte dei client TLS e SSH.

Compatibilità con le versioni precedenti

Utilizzare il criterio di compatibilità Legacy se sono necessarie 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.

Criteri comuni

Se hai bisogno della certificazione Common Criteria, utilizza la politica Common Criteria.

FIPS rigoroso

Utilizzare la politica FIPS strict se è richiesta la certificazione Common Criteria e si deve utilizzare il modulo NetApp Cryptographic Security Module (NCSM) 3.0.8 o NetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64 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.

Il modulo NCSM 3.0.8 e NetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64 vengono utilizzati nelle seguenti operazioni:

- NCSM
  - Connessioni TLS tra i seguenti servizi: ADC, AMS, CMN, DDS, LDR, SSM, NMS, mgmt-api, nginx, nginx-gw e cache-svc
  - Connessioni TLS tra i client e il servizio nginx-gw (endpoint del bilanciatore del carico)
  - Connessioni TLS tra i client e il servizio LDR
  - Crittografia del contenuto dell'oggetto per SSE-S3, SSE-C e impostazione di crittografia dell'oggetto archiviato
  - connessioni SSH

  Per ulteriori informazioni, fare riferimento al programma di convalida degli algoritmi crittografici del NIST"Certificato n. 4838" .

- Modulo API di crittografia del kernel NetApp StorageGRID

  Il modulo API NetApp StorageGRID Kernel Crypto è presente solo sulle piattaforme VM e appliance StorageGRID .

  - Raccolta di entropia
  - Crittografia dei nodi

  Per ulteriori informazioni, fare riferimento al programma di convalida degli algoritmi crittografici del NIST"Certificati #A6242 attraverso #A6257" E"Certificato di entropia n. E223" .

Nota: Dopo aver selezionato questa policy,"eseguire un riavvio progressivo" affinché tutti i nodi attivino l'NCSM. Utilizzare **Manutenzione** > **Riavvio progressivo** per avviare e monitorare i riavvii.

Personalizzato

Creare un criterio personalizzato se è necessario applicare le proprie crittografia.

Facoltativamente, se StorageGRID ha requisiti di crittografia FIPS 140, abilitare la funzionalità Modalità FIPS per utilizzare il modulo NCSM 3.0.8 e NetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64:

a. Imposta il `fipsMode` parametro a `true` .

b. Quando richiesto,"eseguire un riavvio progressivo" affinché tutti i nodi attivino i moduli di crittografia. Utilizzare **Manutenzione** > **Riavvio progressivo** per avviare e monitorare i riavvii.

c. Selezionare **Supporto** > **Diagnostica** per visualizzare le versioni attive del modulo FIPS.

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 sicurezzasegue.

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 **Configurazione** > **Sicurezza** > **Impostazioni di sicurezza**.
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 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 "Come funziona SSO" .

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 **Configurazione** > **Sicurezza** > **Impostazioni di sicurezza**.
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 i 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**.

Gestisci l'accesso SSH esterno

Gestisci l'accesso SSH per il traffico in entrata nella griglia bloccando o consentendo l'accesso esterno. La gestione dell'accesso esterno SSH non ha alcun impatto sul traffico tra i nodi della griglia.

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

Per migliorare la sicurezza del sistema, l'accesso SSH esterno è bloccato per impostazione predefinita. Se devi eseguire attività che richiedono l'accesso SSH in ingresso, come la risoluzione dei problemi, consenti temporaneamente l'accesso esterno. Una volta completata l'attività, blocca l'accesso esterno.

Fasi

1. Selezionare **Configurazione** > **Sicurezza** > **Impostazioni di sicurezza**.
2. Selezionare la scheda **Blocca SSH**.
3. Utilizzare l'opzione **Blocca accesso SSH in ingresso** per gestire l'accesso SSH esterno:
   a. Selezionare la casella di controllo per bloccare l'accesso (impostazione predefinita).
   b. Deseleziona la casella di controllo per consentire l'accesso.

      Richiede l'accesso sulla porta 22 tra il laptop di servizio e tutti gli altri nodi della griglia. Una volta completata l'attività di manutenzione, rimuovere l'accesso alla porta 22.

4. Selezionare **Salva**.