Configura le impostazioni di sicurezza

StorageGRID software

NetApp
July 23, 2026

Sommario

Configura le impostazioni di sicurezza

Gestisci la policy TLS e SSH in StorageGRID

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

La policy di sicurezza controlla come TLS e SSH crittografano i dati in transito. In generale, usa la policy di compatibilità Modern (predefinita), a meno che il tuo sistema non debba essere conforme ai Common Criteria o tu abbia bisogno di usare altri cifrari.

Alcuni servizi StorageGRID non sono stati aggiornati per utilizzare i cifrari in queste policy.

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Permesso di accesso root".

Seleziona una politica di sicurezza

Passaggi

1. Seleziona **Configurazione** > **Sicurezza** > **Impostazioni di sicurezza**.

   La scheda **Policy TLS e SSH** mostra le policy disponibili. La policy attualmente attiva è indicata da un segno di spunta verde sul riquadro della policy.

2. Consulta le schede per conoscere le policy disponibili.

Compatibilità moderna (impostazione predefinita)

Utilizza il criterio predefinito se hai bisogno di una crittografia forte e non hai esigenze particolari. Questo criterio è compatibile con la maggior parte dei client TLS e SSH.

Compatibilità legacy

Utilizza la policy di compatibilità Legacy se hai bisogno di opzioni di compatibilità aggiuntive per i client meno recenti. Le opzioni aggiuntive in questa policy potrebbero renderla meno sicura rispetto alla policy di compatibilità Modern.

Common Criteria

Usa la policy Common Criteria se hai bisogno della certificazione Common Criteria.

FIPS rigoroso

Usa la policy FIPS strict se hai bisogno della certificazione Common Criteria e devi usare il NetApp Cryptographic Security Module (NCSM) 3.0.8 o il NetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64 module per le connessioni client esterne agli endpoint del load balancer, a Tenant Manager e a Grid Manager. L'uso di questa policy potrebbe ridurre le prestazioni.

NCSM 3.0.8 e il modulo 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 di carico)
  - Connessioni TLS tra i client e il servizio LDR
  - Crittografia del contenuto degli oggetti per SSE-S3, SSE-C e l'impostazione di crittografia degli oggetti memorizzati
  - Connessioni SSH

  Per ulteriori informazioni, consulta il NIST Cryptographic Algorithm Validation Program "${post_edited_translations.segment}".

- NetApp StorageGRID modulo API crittografica del kernel

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

  - Raccolta entropia
  - Crittografia dei nodi

  Per ulteriori informazioni, consulta il Programma di convalida degli algoritmi crittografici NIST "Certificati n. A6242 - n. A6257" e "${post_edited_translations.segment}".

Nota: dopo aver selezionato questa policy, "esegui un riavvio progressivo" per tutti i nodi per attivare l'NCSM. Usa **Manutenzione** > **Riavvio progressivo** per avviare e monitorare i riavvii.

Personalizzato

Crea una policy personalizzata se devi applicare i tuoi algoritmi di crittografia.

Facoltativamente, se il tuo StorageGRID ha requisiti di crittografia FIPS 140, abilita la funzionalità della 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 su `true`.

b. Quando richiesto, "esegui un riavvio progressivo" per attivare i moduli di crittografia su tutti i nodi. Usa **Manutenzione** > **Riavvio progressivo** per avviare e monitorare i riavvii.

c. Seleziona **Support** > **Diagnostics** per visualizzare le versioni attive del modulo FIPS.

3. Per vedere i dettagli sui cifrari, i protocolli e gli algoritmi di ciascuna policy, seleziona **Visualizza dettagli**.
4. Per modificare i criteri correnti, seleziona **Usa criteri**.

${post_edited_translations.segment}

Crea una policy di sicurezza personalizzata

Puoi creare una policy personalizzata se hai bisogno di applicare i tuoi algoritmi di crittografia.

Passaggi

1. Dalla sezione della policy più simile alla policy personalizzata che vuoi creare, seleziona **Visualizza dettagli**.
2. ${post_edited_translations.segment}

3. ${post_edited_translations.segment}
4. Incolla il JSON che hai copiato e apporta le modifiche necessarie.
5. ${post_edited_translations.segment}

Accanto a **Politica attuale** nella sezione delle politiche personalizzate compare un segno di spunta verde.

6. ${post_edited_translations.segment}

Ripristina temporaneamente i criteri di sicurezza predefiniti

Se hai configurato una policy di sicurezza personalizzata, potresti non essere in grado di accedere al Grid Manager se la policy TLS configurata è incompatibile con il "certificato server configurato".

Puoi ripristinare temporaneamente la policy di sicurezza predefinita.

Passaggi

1. Accedi a un nodo amministratore:
   a. Inserisci il seguente comando: `ssh admin@Admin_Node_IP`
   b. Inserisci la password indicata nel file `Passwords.txt`.
   c. Inserisci il seguente comando per passare all'utente root: `su -`
   d. Inserisci la password indicata nel file `Passwords.txt`.

   Quando sei connesso come root, il prompt cambia da `$` a `#`.
2. Eseguire il seguente comando:

   ```
   restore-default-cipher-configurations
   ```
3. ${post_edited_translations.segment}
4. Segui i passaggi in Seleziona una politica di sicurezza per configurare nuovamente i criteri.

Configurare la sicurezza di rete e degli oggetti di StorageGRID

Puoi configurare la sicurezza di rete e degli oggetti per crittografare gli oggetti archiviati, impedire determinate richieste S3 o consentire alle connessioni client ai Storage Node di usare HTTP invece di HTTPS.

${post_edited_translations.segment}

La crittografia degli oggetti memorizzati consente la crittografia di tutti i dati degli oggetti al momento dell'acquisizione tramite S3. Per impostazione predefinita, gli oggetti memorizzati non sono crittografati, ma puoi scegliere di crittografarli utilizzando l'algoritmo di crittografia AES-128 o AES-256. Quando abiliti l'impostazione, tutti i nuovi oggetti acquisiti vengono crittografati, ma non viene apportata alcuna modifica agli oggetti memorizzati esistenti. Se disabiliti la crittografia, gli oggetti attualmente crittografati rimangono tali, ma i nuovi oggetti 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 a livello di oggetto.

Per maggiori dettagli sui metodi di crittografia di StorageGRID, vedi "Esamina i metodi di crittografia di StorageGRID".

${post_edited_translations.segment}

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

${post_edited_translations.segment}

- DeleteBucket richieste
- ${post_edited_translations.segment}

Abilita HTTP per le connessioni ai nodi di archiviazione

Per impostazione predefinita, le applicazioni client utilizzano il protocollo di rete HTTPS per qualsiasi connessione diretta ai nodi di storage. Facoltativamente, puoi abilitare l'HTTP per queste connessioni, ad esempio durante il test di una grid non di produzione.

Utilizza HTTP per le connessioni ai nodi di archiviazione solo se i client S3 devono stabilire connessioni HTTP direttamente ai nodi di archiviazione. Non devi usare questa opzione per i client che utilizzano solo connessioni HTTPS o per i client che si connettono al servizio Load Balancer (perché puoi "${post_edited_translations.segment}" usare sia HTTP che HTTPS).

Consulta "Riepilogo: indirizzi IP e porte per le connessioni client" per sapere quali porte utilizzano i client S3 quando si connettono ai Storage Node tramite HTTP o HTTPS.

Seleziona opzioni

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- ${post_edited_translations.segment}

Passaggi

1. Seleziona **Configurazione** > **Sicurezza** > **Impostazioni di sicurezza**.
2. ${post_edited_translations.segment}
3. Per la crittografia degli oggetti memorizzati, usa l'impostazione **Nessuno** (predefinita) se non vuoi che gli oggetti memorizzati siano crittografati, oppure seleziona **AES-128** o **AES-256** per crittografare gli oggetti memorizzati.
4. Seleziona facoltativamente **Impedisci la modifica del client** se vuoi impedire ai client S3 di effettuare richieste specifiche.

   Se modifichi questa impostazione, ci vorrà circa un minuto per applicare la nuova impostazione. Il valore configurato viene memorizzato nella cache per performance e scalabilità.

5. ${post_edited_translations.segment}

   Fai attenzione quando abiliti HTTP per una griglia di produzione perché le richieste verranno inviate senza crittografia.

6. Seleziona **Salva**.

Modificare le impostazioni di sicurezza dell'interfaccia StorageGRID

${post_edited_translations.segment}

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Hai "Permesso di accesso root".

Informazioni su questa attività

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 dai seguenti:

- 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. Quando l'autenticazione di un utente scade, quell'utente viene disconnesso automaticamente, anche se il timeout di inattività del browser è disabilitato o il valore del timeout del browser non è stato raggiunto. Per rinnovare il token, l'utente deve accedere di nuovo.
- ${post_edited_translations.segment}

  Se l'SSO è abilitato e il browser dell'utente va in timeout, l'utente deve reinserire le proprie credenziali SSO per accedere nuovamente a StorageGRID. Vedi "${post_edited_translations.segment}".

${post_edited_translations.segment}

${post_edited_translations.segment}

Questa opzione è disabilitata per impostazione predefinita, ma potresti voler abilitare questa funzionalità per un ambiente di test. In generale, dovresti lasciare la traccia dello stack disabilitata negli ambienti di produzione per evitare di rivelare dettagli interni del software quando si verificano errori API.

Passaggi

1. Seleziona **Configurazione** > **Sicurezza** > **Impostazioni di sicurezza**.
2. ${post_edited_translations.segment}
3. ${post_edited_translations.segment}
   a. Espandi la fisarmonica.
   b. Per modificare il periodo di timeout, specifica un valore compreso tra 60 secondi e 7 giorni. Il timeout predefinito è di 15 minuti.
   c. ${post_edited_translations.segment}
   d. Seleziona **Salva**.

      ${post_edited_translations.segment}

4. ${post_edited_translations.segment}
   a. Espandi la fisarmonica.
   b. Seleziona la casella di controllo per restituire una traccia dello stack nelle risposte di errore delle API di Grid Manager e Tenant Manager.

${post_edited_translations.segment}

c. Seleziona **Salva**.

Gestisci l’accesso SSH esterno in StorageGRID

Gestisci l’accesso SSH per il traffico in entrata nella grid bloccando o consentendo l’accesso esterno. Gestire l’accesso SSH esterno non ha alcun impatto sul traffico tra i nodi nella grid.

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Hai "Permesso di accesso root".

Informazioni su 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 entrata, come la risoluzione dei problemi, consenti temporaneamente l’accesso esterno. Quando hai finito l’attività, blocca l’accesso esterno.

Passaggi

1. Seleziona **Configurazione** > **Sicurezza** > **Impostazioni di sicurezza**.
2. Seleziona la scheda **Blocca SSH**.
3. Usa l’opzione **Blocca l’accesso SSH in entrata** per gestire l’accesso SSH esterno:
   a. ${post_edited_translations.segment}
   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. Rimuovi l’accesso sulla porta 22 quando completi l’attività di manutenzione.

4. Seleziona **Salva**.