Konfigurieren Sie die Sicherheitseinstellungen

StorageGRID

NetApp
November 04, 2025

This PDF was generated from https://docs.netapp.com/de-de/storagegrid-117/admin/manage-tls-ssh-policy.html on November 04, 2025. Always check docs.netapp.com for the latest.

Inhalt

Konfigurieren Sie die Sicherheitseinstellungen . . . 1
- Verwalten Sie die TLS- und SSH-Richtlinie . . . 1
  - Wählen Sie eine Sicherheitsrichtlinie aus . . . 1
  - Erstellen Sie eine benutzerdefinierte Sicherheitsrichtlinie . . . 2
  - Vorübergehendes Zurücksetzen auf die Standard-Sicherheitsrichtlinie . . . 3
- Konfigurieren Sie die Netzwerk- und Objektsicherheit . . . 4
  - Verschlüsselung gespeicherter Objekte . . . 4
  - Client-Änderung verhindern . . . 4
  - Aktivieren Sie HTTP für Storage Node-Verbindungen . . . 4
  - Wählen Sie Optionen aus . . . 5
- Zeitlimit für Inaktivität des Browsers ändern . . . 5

Konfigurieren Sie die Sicherheitseinstellungen

Verwalten Sie die TLS- und SSH-Richtlinie

Die TLS- und SSH-Richtlinie legt fest, welche Protokolle und Chiffren verwendet werden, um sichere TLS-Verbindungen mit Clientanwendungen und sichere SSH-Verbindungen zu internen StorageGRID-Diensten herzustellen.

Die Sicherheitsrichtlinie steuert, wie TLS und SSH Daten in Bewegung verschlüsseln. Verwenden Sie im Allgemeinen die moderne Kompatibilitätsrichtlinie (Standard), es sei denn, Ihr System muss Common Criteria-konform sein oder Sie müssen andere Chiffren verwenden.

> Einige StorageGRID-Dienste wurden nicht aktualisiert, um die Chiffren in diesen Richtlinien zu verwenden.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben die "Root-Zugriffsberechtigung".

Wählen Sie eine Sicherheitsrichtlinie aus

Schritte

1. Wählen Sie **CONFIGURATION** > **Security** > **Security settings**.

   Auf der Registerkarte **TLS und SSH Policies** werden die verfügbaren Richtlinien angezeigt. Die derzeit aktive Richtlinie wird durch ein grünes Häkchen auf der Kachel „Richtlinie“ gekennzeichnet.

2. Lesen Sie die Kacheln, um mehr über die verfügbaren Richtlinien zu erfahren.

Richtlinie	Beschreibung
Moderne Kompatibilität (Standard)	Verwenden Sie die Standardrichtlinie, wenn Sie eine starke Verschlüsselung benötigen und wenn Sie keine besonderen Anforderungen haben. Diese Richtlinie ist mit den meisten TLS- und SSH-Clients kompatibel.

Richtlinie	Beschreibung
Kompatibilität mit älteren Systemen	Verwenden Sie diese Richtlinie, wenn Sie zusätzliche Kompatibilitätsoptionen für ältere Clients benötigen. Die zusätzlichen Optionen in dieser Richtlinie machen sie möglicherweise weniger sicher als die moderne Kompatibilitätsrichtlinie.
Gemeinsame Kriterien	Verwenden Sie diese Richtlinie, wenn Sie eine Common Criteria-Zertifizierung benötigen.
FIPS-strikt	Verwenden Sie diese Richtlinie, wenn Sie eine Common Criteria-Zertifizierung benötigen und das NetApp Cryptographic Security Module 3.0.0 für externe Client-Verbindungen zu Load Balancer-Endpunkten, Tenant Manager und Grid Manager verwenden müssen. Die Verwendung dieser Richtlinie kann die Performance beeinträchtigen.
Individuell	Erstellen Sie eine benutzerdefinierte Richtlinie, wenn Sie Ihre eigenen Chiffren anwenden müssen.

3. Um Details zu den Chiffren, Protokollen und Algorithmen der einzelnen Richtlinien anzuzeigen, wählen Sie **Details anzeigen**.
4. Um die aktuelle Richtlinie zu ändern, wählen Sie **Richtlinie verwenden**.

   Ein grünes Häkchen erscheint neben **Aktuelle Richtlinie** auf der Policy-Kachel.

Erstellen Sie eine benutzerdefinierte Sicherheitsrichtlinie

Sie können eine benutzerdefinierte Richtlinie erstellen, wenn Sie Ihre eigenen Chiffren anwenden müssen.

Schritte

1. Wählen Sie auf der Kachel der Richtlinie, die der benutzerdefinierten Richtlinie, die Sie erstellen möchten, am ähnlichsten ist, **Details anzeigen** aus.
2. Wählen Sie **in Zwischenablage kopieren**, und wählen Sie dann **Abbrechen**.

3. Wählen Sie in der Kachel **Benutzerdefinierte Richtlinie** die Option **Konfigurieren und Verwenden** aus.
4. Fügen Sie die JSON ein, die Sie kopiert haben, und nehmen Sie alle erforderlichen Änderungen vor.
5. Wählen Sie **Richtlinie verwenden**.

   Auf der Kachel „Benutzerdefinierte Richtlinie“ wird ein grünes Häkchen neben **Aktuelle Richtlinie** angezeigt.

6. Wählen Sie optional **Konfiguration bearbeiten**, um weitere Änderungen an der neuen benutzerdefinierten Richtlinie vorzunehmen.

Vorübergehendes Zurücksetzen auf die Standard-Sicherheitsrichtlinie

Wenn Sie eine benutzerdefinierte Sicherheitsrichtlinie konfiguriert haben, können Sie sich möglicherweise nicht beim Grid Manager anmelden, wenn die konfigurierte TLS-Richtlinie nicht mit dem kompatibel ist "Serverzertifikat konfiguriert".

Sie können vorübergehend auf die Standard-Sicherheitsrichtlinie zurücksetzen.

Schritte

1. Melden Sie sich bei einem Admin-Knoten an:
   a. Geben Sie den folgenden Befehl ein: `ssh admin@Admin_Node_IP`
   b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
   c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
   d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

      Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

2. Führen Sie den folgenden Befehl aus:

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

3. Greifen Sie über einen Webbrowser auf den Grid Manager auf demselben Admin-Node zu.
4. Befolgen Sie die Schritte unter Wählen Sie eine Sicherheitsrichtlinie aus Um die Richtlinie erneut zu

konfigurieren.

Konfigurieren Sie die Netzwerk- und Objektsicherheit

Sie können die Netzwerk- und Objektsicherheit so konfigurieren, dass gespeicherte Objekte verschlüsselt, bestimmte S3- und Swift-Anforderungen verhindert oder Client-Verbindungen zu Storage-Nodes HTTP anstelle von HTTPS verwenden.

Verschlüsselung gespeicherter Objekte

Die gespeicherte Objektverschlüsselung ermöglicht die Verschlüsselung aller Objektdaten bei der Aufnahme über S3. Gespeicherte Objekte werden standardmäßig nicht verschlüsselt, aber Sie können Objekte mit dem AES-128- oder AES-256-Verschlüsselungsalgorithmus verschlüsseln. Wenn Sie die Einstellung aktivieren, werden alle neu aufgenommenen Objekte verschlüsselt, aber es werden keine Änderungen an vorhandenen gespeicherten Objekten vorgenommen. Wenn Sie die Verschlüsselung deaktivieren, bleiben derzeit verschlüsselte Objekte verschlüsselt, neu aufgenommene Objekte werden jedoch nicht verschlüsselt.

Die Einstellung für die Verschlüsselung gespeicherter Objekte ist nur für S3-Objekte anwendbar, die nicht durch Verschlüsselung auf Bucket-Ebene oder Objekt-Ebene verschlüsselt wurden.

Weitere Informationen zu Verschlüsselungsmethoden von StorageGRID finden Sie unter "Prüfen Sie die StorageGRID Verschlüsselungsmethoden".

Client-Änderung verhindern

Die Einstellung „Client-Änderung verhindern“ ist eine systemweite Einstellung. Wenn die Option **Client-Änderung verhindern** ausgewählt ist, werden die folgenden Anfragen abgelehnt.

S3-REST-API

- Bucket-Anforderungen löschen
- Alle Anforderungen, die das Ändern von Daten eines vorhandenen Objekts, benutzerdefinierter Metadaten oder S3-Objekt-Tagging zum Einsatz kommen

Swift REST API

- Container-Anforderungen löschen
- Anträge zum Ändern vorhandener Objekte. Beispielsweise werden folgende Vorgänge verweigert: Put Overwrite, Delete, Metadata Update usw.

Aktivieren Sie HTTP für Storage Node-Verbindungen

Standardmäßig verwenden Clientanwendungen das HTTPS-Netzwerkprotokoll für alle direkten Verbindungen zu Storage-Nodes. Optional können Sie HTTP für diese Verbindungen aktivieren, z. B. beim Testen eines nicht produktiven Grids.

Verwenden Sie HTTP für Storage-Node-Verbindungen nur, wenn S3- und Swift-Clients HTTP-Verbindungen direkt zu Storage-Nodes herstellen müssen. Sie müssen diese Option nicht für Clients verwenden, die nur HTTPS-Verbindungen verwenden, oder für Clients, die eine Verbindung zum Load Balancer-Dienst herstellen (weil Sie dies können "Konfigurieren Sie jeden Endpunkt der Lastverteilung" Zur Verwendung von HTTP oder HTTPS).

Siehe "Zusammenfassung: IP-Adressen und Ports für Client-Verbindungen" Um zu erfahren, welche Ports S3 und Swift-Clients bei der Verbindung zu Storage-Nodes über HTTP oder HTTPS verwenden.

Wählen Sie Optionen aus

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben Root-Zugriffsberechtigung.

Schritte

1. Wählen Sie **CONFIGURATION** > **Security** > **Security settings**.
2. Wählen Sie die Registerkarte **Netzwerk und Objekte**.
3. Verwenden Sie für die Verschlüsselung gespeicherter Objekte die Einstellung **None** (Standard), wenn Sie keine Verschlüsselung gespeicherter Objekte wünschen, oder wählen Sie **AES-128** oder **AES-256**, um gespeicherte Objekte zu verschlüsseln.
4. Wählen Sie optional **Client-Änderung verhindern**, wenn Sie S3- und Swift-Clients daran hindern möchten, spezifische Anforderungen zu stellen.

   Wenn Sie diese Einstellung ändern, dauert es etwa eine Minute, bis die neue Einstellung angewendet wird. Der konfigurierte Wert wird für Performance und Skalierung zwischengespeichert.

5. Wählen Sie optional **HTTP für Storage Node-Verbindungen aktivieren**, wenn Clients direkt mit Storage Nodes verbunden sind und Sie HTTP-Verbindungen verwenden möchten.

   Gehen Sie vorsichtig vor, wenn Sie HTTP für ein Produktions-Grid aktivieren, da die Anforderungen unverschlüsselt gesendet werden.

6. Wählen Sie **Speichern**.

Zeitlimit für Inaktivität des Browsers ändern

Sie können steuern, ob Grid Manager und Tenant Manager-Benutzer abgemeldet werden, wenn sie länger als eine bestimmte Zeit inaktiv sind.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben Root-Zugriffsberechtigung.

Über diese Aufgabe

Das Zeitlimit für die Inaktivität des Browsers beträgt standardmäßig 15 Minuten. Wenn der Browser eines Benutzers für diese Zeit nicht aktiv ist, wird der Benutzer abgemeldet.

Bei Bedarf können Sie die Sperrzeit erhöhen oder verringern, indem Sie die Option * Inaktive Benutzer abmelden nach* einstellen.

Das Zeitlimit für die Inaktivität des Browsers wird auch durch Folgendes gesteuert:

- Ein separater, nicht konfigurierbarer StorageGRID-Timer, der für die Systemsicherheit enthalten ist.

Standardmäßig läuft das Authentifizierungs-Token jedes Benutzers 16 Stunden nach der Anmeldung des Benutzers ab. Wenn die Authentifizierung eines Benutzers abläuft, wird dieser Benutzer automatisch abgemeldet, auch wenn das Zeitlimit für die Inaktivität des Browsers deaktiviert ist oder der Wert für das Browsertimeout nicht erreicht wurde. Um das Token zu erneuern, muss sich der Benutzer erneut anmelden.

- Timeout-Einstellungen für den Identitäts-Provider, vorausgesetzt, Single Sign-On (SSO) ist für StorageGRID aktiviert.

  Wenn SSO aktiviert ist und der Browser eines Benutzers eine Zeitdauer ausläuft, muss der Benutzer seine SSO-Anmeldeinformationen erneut eingeben, um erneut auf StorageGRID zuzugreifen. Siehe "Konfigurieren Sie Single Sign-On".

Schritte

1. Wählen Sie **CONFIGURATION** > **Security** > **Security settings**.
2. Wählen Sie die Registerkarte **Browser Inaktivität Timeout**.
3. Geben Sie im Feld **Abmelden inaktiver Benutzer nach** einen Browser-Timeout-Zeitraum zwischen 60 Sekunden und 7 Tagen an.

   Sie können die Zeitüberschreitung des Browsers in Sekunden, Minuten, Stunden oder Tagen angeben.

4. Wählen Sie **Speichern**. Wenn ein Browser für die angegebene Zeit inaktiv ist, wird der Benutzer vom Grid Manager oder Tenant Manager abgemeldet.

   Die neue Einstellung hat keine Auswirkung auf die derzeit angemeldenen Benutzer. Benutzer müssen sich erneut anmelden oder ihre Browser aktualisieren, damit die neue Timeout-Einstellung wirksam wird.

Copyright-Informationen

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.