Konfigurieren der Sicherheitseinstellungen

StorageGRID software

NetApp
October 21, 2025

Inhalt

Konfigurieren der Sicherheitseinstellungen

Verwalten der TLS- und SSH-Richtlinie

Die TLS- und SSH-Richtlinie bestimmt, welche Protokolle und Chiffren zum Herstellen sicherer TLS-Verbindungen mit Clientanwendungen und sicherer SSH-Verbindungen zu internen StorageGRID Diensten verwendet werden.

Die Sicherheitsrichtlinie steuert, wie TLS und SSH übertragene Daten verschlüsseln. Verwenden Sie im Allgemeinen die moderne Kompatibilitätsrichtlinie (Standard), es sei denn, Ihr System muss Common Criteria-kompatibel 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 beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Root-Zugriffsberechtigung" .

Wählen Sie eine Sicherheitsrichtlinie

Schritte

1. Wählen Sie **KONFIGURATION** > **Sicherheit** > **Sicherheitseinstellungen**.

   Auf der Registerkarte **TLS- und SSH-Richtlinien** werden die verfügbaren Richtlinien angezeigt. Die aktuell aktive Richtlinie wird durch ein grünes Häkchen auf der Richtlinienkachel gekennzeichnet.

2. Sehen Sie sich die Kacheln an, um mehr über die verfügbaren Richtlinien zu erfahren.

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

Politik	Beschreibung
Legacy-Kompatibilität	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 streng	Verwenden Sie diese Richtlinie, wenn Sie eine Common Criteria-Zertifizierung benötigen und das NetApp Cryptographic Security Module 3.0.8 für externe Clientverbindungen zu Load Balancer-Endpunkten, Tenant Manager und Grid Manager verwenden müssen. Die Verwendung dieser Richtlinie kann die Leistung beeinträchtigen. **Hinweis**: Nachdem Sie diese Richtlinie ausgewählt haben, müssen alle Knoten"rollierend neu gestartet" um das NetApp Cryptographic Security Module zu aktivieren. Verwenden Sie **Wartung** > **Rollierender Neustart**, um Neustarts zu initiieren und zu überwachen.
Brauch	Erstellen Sie eine benutzerdefinierte Richtlinie, wenn Sie Ihre eigenen Chiffren anwenden müssen.

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

   Auf der Richtlinienkachel wird neben **Aktuelle Richtlinie** ein grünes Häkchen angezeigt.

Erstellen einer benutzerdefinierten 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 die Zwischenablage kopieren** und dann **Abbrechen**.

3. Wählen Sie auf der Kachel **Benutzerdefinierte Richtlinie** die Option **Konfigurieren und verwenden** aus.
4. Fügen Sie das kopierte JSON ein und nehmen Sie die erforderlichen Änderungen vor.
5. Wählen Sie **Richtlinie verwenden**.

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

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

Vorübergehend zur Standardsicherheitsrichtlinie zurückkehren

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

Sie können vorübergehend zur Standardsicherheitsrichtlinie zurückkehren.

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 Passwort ein, das in der `Passwords.txt` Datei.
   c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
   d. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei.

      Wenn Sie als Root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Zu `#` .

2. Führen Sie den folgenden Befehl aus:

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

3. Greifen Sie über einen Webbrowser auf den Grid Manager auf demselben Admin-Knoten zu.
4. Befolgen Sie die Schritte inWählen Sie eine Sicherheitsrichtlinie um die Richtlinie erneut zu konfigurieren.

Konfigurieren der Netzwerk- und Objektsicherheit

Sie können die Netzwerk- und Objektsicherheit so konfigurieren, dass gespeicherte Objekte verschlüsselt werden, bestimmte S3-Anfragen verhindert werden oder Clientverbindungen zu Speicherknoten HTTP statt HTTPS verwenden.

Gespeicherte Objektverschlüsselung

Die Verschlüsselung gespeicherter Objekte ermöglicht die Verschlüsselung aller Objektdaten, wenn diese über S3 aufgenommen werden. Standardmäßig werden gespeicherte Objekte nicht verschlüsselt, Sie können die Objekte jedoch mit dem Verschlüsselungsalgorithmus AES-128 oder AES-256 verschlüsseln. Wenn Sie die Einstellung aktivieren, werden alle neu aufgenommenen Objekte verschlüsselt, es werden jedoch keine Änderungen an vorhandenen gespeicherten Objekten vorgenommen. Wenn Sie die Verschlüsselung deaktivieren, bleiben aktuell verschlüsselte Objekte verschlüsselt, neu aufgenommene Objekte werden jedoch nicht verschlüsselt.

Die Einstellung „Gespeicherte Objektverschlüsselung“ gilt nur für S3-Objekte, die nicht durch Verschlüsselung auf Bucket- oder Objektebene verschlüsselt wurden.

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

Client-Änderungen verhindern

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

S3 REST API

- DeleteBucket-Anfragen
- Alle Anfragen zum Ändern der Daten eines vorhandenen Objekts, benutzerdefinierter Metadaten oder S3-Objekt-Tagging

Aktivieren Sie HTTP für Storage Node-Verbindungen

Standardmäßig verwenden Clientanwendungen das HTTPS-Netzwerkprotokoll für alle direkten Verbindungen zu Speicherknoten. Sie können HTTP für diese Verbindungen optional aktivieren, beispielsweise beim Testen eines Nicht-Produktionsrasters.

Verwenden Sie HTTP für Speicherknotenverbindungen nur, wenn S3-Clients HTTP-Verbindungen direkt zu Speicherknoten 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"Konfigurieren Sie jeden Load Balancer-Endpunkt" um entweder HTTP oder HTTPS zu verwenden).

Sehen"Zusammenfassung: IP-Adressen und Ports für Clientverbindungen" um zu erfahren, welche Ports S3-Clients verwenden, wenn sie über HTTP oder HTTPS eine Verbindung zu Speicherknoten herstellen.

Ausführung wählen

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .

- Sie verfügen über Root-Zugriffsberechtigung.

Schritte

1. Wählen Sie **KONFIGURATION** > **Sicherheit** > **Sicherheitseinstellungen**.
2. Wählen Sie die Registerkarte **Netzwerk und Objekte**.
3. Verwenden Sie für die Verschlüsselung gespeicherter Objekte die Einstellung **Keine** (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** aus, wenn Sie verhindern möchten, dass S3-Clients bestimmte Anfragen stellen.

   Wenn Sie diese Einstellung ändern, dauert es etwa eine Minute, bis die neue Einstellung übernommen wird. Der konfigurierte Wert wird aus Leistungs- und Skalierungsgründen zwischengespeichert.

5. Wählen Sie optional **HTTP für Speicherknotenverbindungen aktivieren** aus, wenn Clients eine direkte Verbindung zu Speicherknoten herstellen und Sie HTTP-Verbindungen verwenden möchten.

   Seien Sie vorsichtig, wenn Sie HTTP für ein Produktionsraster aktivieren, da Anfragen unverschlüsselt gesendet werden.

6. Wählen Sie **Speichern**.

Ändern der Schnittstellensicherheitseinstellungen

Über die Sicherheitseinstellungen der Schnittstelle können Sie steuern, ob Benutzer abgemeldet werden, wenn sie länger als die angegebene Zeit inaktiv sind, und ob in den API-Fehlerantworten ein Stacktrace enthalten sein soll.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Du hast"Root-Zugriffsberechtigung" .

Informationen zu diesem Vorgang

Die Seite **Sicherheitseinstellungen** enthält die Einstellungen **Browser-Inaktivitäts-Timeout** und **Management-API-Stack-Trace**.

Browser-Inaktivitäts-Timeout

Gibt an, wie lange der Browser eines Benutzers inaktiv sein kann, bevor der Benutzer abgemeldet wird. Der Standardwert beträgt 15 Minuten.

Das Timeout für Browserinaktivität wird auch durch Folgendes gesteuert:

- Ein separater, nicht konfigurierbarer StorageGRID Timer, der zur Systemsicherheit enthalten ist. Das Authentifizierungstoken jedes Benutzers läuft 16 Stunden nach der Anmeldung des Benutzers ab. Wenn die Authentifizierung eines Benutzers abläuft, wird dieser Benutzer automatisch abgemeldet, auch wenn das Inaktivitätstimeout 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 Identitätsanbieter, vorausgesetzt, Single Sign-On (SSO) ist für

StorageGRID aktiviert.

Wenn SSO aktiviert ist und es beim Browser eines Benutzers zu einer Zeitüberschreitung kommt, muss der Benutzer seine SSO-Anmeldeinformationen erneut eingeben, um wieder auf StorageGRID zugreifen zu können. Sehen "Konfigurieren der einmaligen Anmeldung" .

Stapelüberwachung der Verwaltungs-API

Steuert, ob in den Fehlerantworten der Grid Manager- und Tenant Manager-API ein Stacktrace zurückgegeben wird.

Diese Option ist standardmäßig deaktiviert, Sie möchten diese Funktion jedoch möglicherweise für eine Testumgebung aktivieren. Im Allgemeinen sollten Sie den Stacktrace in Produktionsumgebungen deaktiviert lassen, um zu vermeiden, dass beim Auftreten von API-Fehlern interne Softwaredetails preisgegeben werden.

Schritte

1. Wählen Sie **KONFIGURATION** > **Sicherheit** > **Sicherheitseinstellungen**.
2. Wählen Sie die Registerkarte **Schnittstelle**.
3. So ändern Sie die Einstellung für das Inaktivitäts-Timeout des Browsers:
   a. Erweitern Sie das Akkordeon.
   b. Um die Zeitüberschreitungsdauer zu ändern, geben Sie einen Wert zwischen 60 Sekunden und 7 Tagen an. Das Standard-Timeout beträgt 15 Minuten.
   c. Um diese Funktion zu deaktivieren, deaktivieren Sie das Kontrollkästchen.
   d. Wählen Sie **Speichern**.

      Die neue Einstellung wirkt sich nicht auf Benutzer aus, die derzeit angemeldet sind. Benutzer müssen sich erneut anmelden oder ihren Browser aktualisieren, damit die neue Timeout-Einstellung wirksam wird.

4. So ändern Sie die Einstellung für den Management-API-Stack-Trace:
   a. Erweitern Sie das Akkordeon.
   b. Aktivieren Sie das Kontrollkästchen, um in den Fehlerantworten der Grid Manager- und Tenant Manager-API einen Stacktrace zurückzugeben.

      

      Lassen Sie den Stacktrace in Produktionsumgebungen deaktiviert, um zu vermeiden, dass beim Auftreten von API-Fehlern interne Softwaredetails preisgegeben werden.

   c. Wählen Sie **Speichern**.