Systemhärtung

StorageGRID software

NetApp
October 21, 2025

Inhalt

Systemhärtung

Allgemeine Überlegungen zur Systemhärtung

Unter Systemhärtung versteht man den Prozess, möglichst viele Sicherheitsrisiken aus einem StorageGRID -System zu eliminieren.

Verwenden Sie beim Installieren und Konfigurieren von StorageGRID diese Richtlinien, um alle vorgeschriebenen Sicherheitsziele hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit zu erreichen.

Sie sollten bereits branchenübliche Best Practices zur Systemhärtung verwenden. Verwenden Sie beispielsweise sichere Passwörter für StorageGRID, verwenden Sie HTTPS statt HTTP und aktivieren Sie die zertifikatsbasierte Authentifizierung, sofern verfügbar.

StorageGRID folgt dem "NetApp -Richtlinie zur Handhabung von Sicherheitslücken" . Gemeldete Schwachstellen werden überprüft und gemäß dem Reaktionsprozess für Produktsicherheitsvorfälle behoben.

Beachten Sie beim Härten eines StorageGRID -Systems Folgendes:

- **Welches der drei StorageGRID Netzwerke** haben Sie implementiert? Alle StorageGRID -Systeme müssen das Grid-Netzwerk verwenden, Sie können jedoch auch das Admin-Netzwerk, das Client-Netzwerk oder beide verwenden. Für jedes Netzwerk gelten andere Sicherheitsaspekte.
- **Die Art der Plattformen**, die Sie für die einzelnen Knoten in Ihrem StorageGRID -System verwenden. StorageGRID -Knoten können auf virtuellen VMware-Maschinen, innerhalb einer Container-Engine auf Linux-Hosts oder als dedizierte Hardware-Geräte bereitgestellt werden. Jeder Plattformtyp verfügt über einen eigenen Satz bewährter Verfahren zur Härtung.
- **Wie vertrauenswürdig die Mieterkonten sind**. Wenn Sie ein Dienstanbieter mit nicht vertrauenswürdigen Mandantenkonten sind, haben Sie andere Sicherheitsbedenken, als wenn Sie nur vertrauenswürdige, interne Mandanten verwenden.
- **Welche Sicherheitsanforderungen und Konventionen** Ihre Organisation befolgt. Möglicherweise müssen Sie bestimmte gesetzliche oder unternehmensbezogene Anforderungen erfüllen.

Härtungsrichtlinien für Software-Upgrades

Sie müssen Ihr StorageGRID -System und die zugehörigen Dienste auf dem neuesten Stand halten, um sich vor Angriffen zu schützen.

Upgrades der StorageGRID -Software

Wenn möglich, sollten Sie die StorageGRID -Software auf die neueste Hauptversion oder auf die vorherige Hauptversion aktualisieren. Durch die Aktualisierung von StorageGRID lässt sich die Zeit verkürzen, in der bekannte Schwachstellen aktiv sind, und die gesamte Angriffsfläche wird verringert. Darüber hinaus enthalten die neuesten Versionen von StorageGRID häufig Funktionen zur Sicherheitshärtung, die in früheren Versionen nicht enthalten waren.

Konsultieren Sie die "NetApp Interoperabilitätsmatrix-Tool" (IMT), um zu bestimmen, welche Version der StorageGRID -Software Sie verwenden sollten. Wenn ein Hotfix erforderlich ist, legt NetApp Wert darauf, Updates für die aktuellsten Versionen zu erstellen. Einige Patches sind möglicherweise nicht mit früheren Versionen kompatibel.

- Um die neuesten StorageGRID Versionen und Hotfixes herunterzuladen, gehen Sie zu "NetApp Downloads: StorageGRID" .
- Informationen zum Upgrade der StorageGRID -Software finden Sie im"Upgrade-Anweisungen" .
- Informationen zum Anwenden eines Hotfixes finden Sie im"StorageGRID Hotfix-Verfahren" .

Upgrades auf externe Dienste

Externe Dienste können Schwachstellen aufweisen, die StorageGRID indirekt betreffen. Sie sollten sicherstellen, dass die Dienste, von denen StorageGRID abhängt, auf dem neuesten Stand gehalten werden. Zu diesen Diensten gehören LDAP, KMS (oder KMIP-Server), DNS und NTP.

Eine Liste der unterstützten Versionen finden Sie im "NetApp Interoperabilitätsmatrix-Tool" .

Upgrades auf Hypervisoren

Wenn Ihre StorageGRID -Knoten auf VMware oder einem anderen Hypervisor ausgeführt werden, müssen Sie sicherstellen, dass die Software und Firmware des Hypervisors auf dem neuesten Stand sind.

Eine Liste der unterstützten Versionen finden Sie im "NetApp Interoperabilitätsmatrix-Tool" .

Upgrades auf Linux-Knoten

Wenn Ihre StorageGRID -Knoten Linux-Hostplattformen verwenden, müssen Sie sicherstellen, dass Sicherheitsupdates und Kernelupdates auf das Hostbetriebssystem angewendet werden. Darüber hinaus müssen Sie Firmware-Updates auf anfällige Hardware anwenden, sobald diese Updates verfügbar sind.

Eine Liste der unterstützten Versionen finden Sie im "NetApp Interoperabilitätsmatrix-Tool" .

Härtungsrichtlinien für StorageGRID -Netzwerke

Das StorageGRID -System unterstützt bis zu drei Netzwerkschnittstellen pro Grid-Knoten, sodass Sie die Vernetzung für jeden einzelnen Grid-Knoten entsprechend Ihren Sicherheits- und Zugriffsanforderungen konfigurieren können.

Ausführliche Informationen zu StorageGRID -Netzwerken finden Sie im"StorageGRID -Netzwerktypen" .

Richtlinien für das Grid-Netzwerk

Sie müssen für den gesamten internen StorageGRID Verkehr ein Grid-Netzwerk konfigurieren. Alle Grid-Knoten befinden sich im Grid-Netzwerk und müssen mit allen anderen Knoten kommunizieren können.

Befolgen Sie beim Konfigurieren des Grid-Netzwerks die folgenden Richtlinien:

- Stellen Sie sicher, dass das Netzwerk vor nicht vertrauenswürdigen Clients, wie beispielsweise denen im offenen Internet, geschützt ist.
- Verwenden Sie das Grid-Netzwerk nach Möglichkeit ausschließlich für den internen Verkehr. Sowohl das Admin-Netzwerk als auch das Client-Netzwerk unterliegen zusätzlichen Firewall-Einschränkungen, die den externen Datenverkehr zu internen Diensten blockieren. Die Verwendung des Grid-Netzwerks für externen Client-Verkehr wird unterstützt, diese Verwendung bietet jedoch weniger Schutzebenen.
- Wenn sich die StorageGRID -Bereitstellung über mehrere Rechenzentren erstreckt, verwenden Sie ein virtuelles privates Netzwerk (VPN) oder ein gleichwertiges Netzwerk im Grid-Netzwerk, um zusätzlichen

Schutz für den internen Datenverkehr zu bieten.

- Einige Wartungsverfahren erfordern einen Secure Shell-Zugriff (SSH) auf Port 22 zwischen dem primären Admin-Knoten und allen anderen Grid-Knoten. Verwenden Sie eine externe Firewall, um den SSH-Zugriff auf vertrauenswürdige Clients zu beschränken.

Richtlinien für das Admin-Netzwerk

Das Admin-Netzwerk wird normalerweise für Verwaltungsaufgaben (vertrauenswürdige Mitarbeiter, die den Grid Manager oder SSH verwenden) und für die Kommunikation mit anderen vertrauenswürdigen Diensten wie LDAP, DNS, NTP oder KMS (oder KMIP-Server) verwendet. StorageGRID erzwingt diese Verwendung jedoch nicht intern.

Wenn Sie das Admin-Netzwerk verwenden, befolgen Sie diese Richtlinien:

- Blockieren Sie alle internen Datenverkehrsports im Admin-Netzwerk. Siehe die"Liste der internen Ports" .
- Wenn nicht vertrauenswürdige Clients auf das Admin-Netzwerk zugreifen können, blockieren Sie den Zugriff auf StorageGRID im Admin-Netzwerk mit einer externen Firewall.

Richtlinien für das Client-Netzwerk

Das Client-Netzwerk wird normalerweise für Mandanten und zur Kommunikation mit externen Diensten verwendet, beispielsweise dem CloudMirror-Replikationsdienst oder einem anderen Plattformdienst. StorageGRID erzwingt diese Verwendung jedoch nicht intern.

Wenn Sie das Client-Netzwerk verwenden, befolgen Sie diese Richtlinien:

- Blockieren Sie alle internen Datenverkehrsports im Client-Netzwerk. Siehe die"Liste der internen Ports" .
- Akzeptieren Sie eingehenden Client-Datenverkehr nur auf explizit konfigurierten Endpunkten. Informationen zu"Verwalten von Firewall-Kontrollen" .

Härtungsrichtlinien für StorageGRID Knoten

StorageGRID -Knoten können auf virtuellen VMware-Maschinen, innerhalb einer Container-Engine auf Linux-Hosts oder als dedizierte Hardware-Geräte bereitgestellt werden. Jeder Plattformtyp und jeder Knotentyp verfügt über einen eigenen Satz bewährter Verfahren zur Härtung.

Steuern Sie den Remote-IPMI-Zugriff auf BMC

Sie können den Remote-IPMI-Zugriff für alle Appliances mit einem BMC aktivieren oder deaktivieren. Die Remote-IPMI-Schnittstelle ermöglicht jedem mit einem BMC -Konto und Kennwort den Low-Level-Hardwarezugriff auf Ihre StorageGRID -Geräte. Wenn Sie keinen Remote-IPMI-Zugriff auf den BMC benötigen, deaktivieren Sie diese Option.

- Um den Remote-IPMI-Zugriff auf den BMC im Grid Manager zu steuern, gehen Sie zu **KONFIGURATION** > **Sicherheit** > **Sicherheitseinstellungen** > **Geräte**:
  - Deaktivieren Sie das Kontrollkästchen **Remote-IPMI-Zugriff aktivieren**, um den IPMI-Zugriff auf den BMC zu deaktivieren.
  - Aktivieren Sie das Kontrollkästchen **Remote-IPMI-Zugriff aktivieren**, um den IPMI-Zugriff auf den BMC zu aktivieren.

Firewall-Konfiguration

Im Rahmen der Systemhärtung müssen Sie die Konfigurationen externer Firewalls überprüfen und so ändern, dass Datenverkehr nur von den IP-Adressen und Ports akzeptiert wird, von denen er unbedingt benötigt wird.

StorageGRID umfasst auf jedem Knoten eine interne Firewall, die die Sicherheit Ihres Grids erhöht, indem sie Ihnen die Kontrolle des Netzwerkzugriffs auf den Knoten ermöglicht. Du solltest"Verwalten Sie interne Firewall-Kontrollen" um den Netzwerkzugriff auf allen Ports außer denen zu verhindern, die für Ihre spezifische Grid-Bereitstellung erforderlich sind. Die Konfigurationsänderungen, die Sie auf der Firewall-Steuerungsseite vornehmen, werden auf jedem Knoten bereitgestellt.

Insbesondere können Sie diese Bereiche verwalten:

- **Privilegierte Adressen**: Sie können ausgewählten IP-Adressen oder Subnetzen den Zugriff auf Ports erlauben, die durch Einstellungen auf der Registerkarte „Externen Zugriff verwalten“ geschlossen sind.
- **Externen Zugriff verwalten**: Sie können standardmäßig geöffnete Ports schließen oder zuvor geschlossene Ports wieder öffnen.
- **Nicht vertrauenswürdiges Client-Netzwerk**: Sie können angeben, ob ein Knoten eingehendem Datenverkehr vom Client-Netzwerk vertraut, sowie die zusätzlichen Ports, die geöffnet werden sollen, wenn ein nicht vertrauenswürdiges Client-Netzwerk konfiguriert ist.

Diese interne Firewall bietet zwar eine zusätzliche Schutzebene gegen einige gängige Bedrohungen, macht jedoch eine externe Firewall nicht überflüssig.

Eine Liste aller von StorageGRID verwendeten internen und externen Ports finden Sie unter"Netzwerkportreferenz" .

Deaktivieren Sie nicht verwendete Dienste

Für alle StorageGRID -Knoten sollten Sie den Zugriff auf nicht verwendete Dienste deaktivieren oder blockieren. Wenn Sie beispielsweise DHCP nicht verwenden möchten, schließen Sie Port 68 mit dem Grid Manager. Wählen Sie **KONFIGURATION** > **Firewall-Steuerung** > **Externen Zugriff verwalten**. Ändern Sie dann den Statusschalter für Port 68 von **Offen** auf **Geschlossen**.

Virtualisierung, Container und gemeinsam genutzte Hardware

Vermeiden Sie bei allen StorageGRID -Knoten, StorageGRID auf derselben physischen Hardware wie nicht vertrauenswürdige Software auszuführen. Gehen Sie nicht davon aus, dass der Hypervisor-Schutz Schadsoftware daran hindert, auf durch StorageGRID geschützte Daten zuzugreifen, wenn sich sowohl StorageGRID als auch die Schadsoftware auf derselben physischen Hardware befinden. Beispielsweise nutzen die Meltdown- und Spectre-Angriffe kritische Schwachstellen in modernen Prozessoren aus und ermöglichen es Programmen, Daten im Speicher desselben Computers zu stehlen.

Schützen Sie Knoten während der Installation

Erlauben Sie nicht vertrauenswürdigen Benutzern nicht, über das Netzwerk auf StorageGRID -Knoten zuzugreifen, wenn die Knoten installiert werden. Knoten sind erst dann vollständig sicher, wenn sie dem Netz beigetreten sind.

Richtlinien für Admin-Knoten

Admin-Knoten bieten Verwaltungsdienste wie Systemkonfiguration, Überwachung und Protokollierung. Wenn Sie sich beim Grid Manager oder Tenant Manager anmelden, stellen Sie eine Verbindung zu einem Admin-

Knoten her.

Befolgen Sie diese Richtlinien, um die Admin-Knoten in Ihrem StorageGRID -System zu sichern:

- Schützen Sie alle Admin-Knoten vor nicht vertrauenswürdigen Clients, beispielsweise solchen im offenen Internet. Stellen Sie sicher, dass kein nicht vertrauenswürdiger Client auf einen Admin-Knoten im Grid-Netzwerk, im Admin-Netzwerk oder im Client-Netzwerk zugreifen kann.
- StorageGRID -Gruppen steuern den Zugriff auf die Funktionen Grid Manager und Tenant Manager. Gewähren Sie jeder Benutzergruppe die für ihre Rolle erforderlichen Mindestberechtigungen und verwenden Sie den schreibgeschützten Zugriffsmodus, um zu verhindern, dass Benutzer die Konfiguration ändern.
- Wenn Sie StorageGRID Load Balancer-Endpunkte verwenden, verwenden Sie für nicht vertrauenswürdigen Client-Datenverkehr Gateway-Knoten anstelle von Admin-Knoten.
- Wenn Sie nicht vertrauenswürdige Mandanten haben, gewähren Sie ihnen keinen direkten Zugriff auf den Mandanten-Manager oder die Mandantenverwaltungs-API. Lassen Sie stattdessen nicht vertrauenswürdige Mandanten ein Mandantenportal oder ein externes Mandantenverwaltungssystem verwenden, das mit der Mandantenverwaltungs-API interagiert.
- Verwenden Sie optional einen Admin-Proxy, um mehr Kontrolle über die AutoSupport -Kommunikation von Admin-Knoten zum NetApp Support zu haben. Sehen Sie sich die Schritte für"Erstellen eines Admin-Proxys" .
- Verwenden Sie optional die eingeschränkten Ports 8443 und 9443, um die Kommunikation zwischen Grid Manager und Tenant Manager zu trennen. Blockieren Sie den freigegebenen Port 443 und beschränken Sie die Mieteranfragen auf Port 9443 für zusätzlichen Schutz.
- Verwenden Sie optional separate Admin-Knoten für Grid-Administratoren und Mandantenbenutzer.

Weitere Informationen finden Sie in der Anleitung für"StorageGRID verwalten" .

Richtlinien für Speicherknoten

Speicherknoten verwalten und speichern Objektdaten und Metadaten. Befolgen Sie diese Richtlinien, um die Speicherknoten in Ihrem StorageGRID -System zu sichern.

- Erlauben Sie nicht vertrauenswürdigen Clients nicht, eine direkte Verbindung zu Speicherknoten herzustellen. Verwenden Sie einen Load Balancer-Endpunkt, der von einem Gateway-Knoten oder einem Load Balancer eines Drittanbieters bedient wird.
- Aktivieren Sie keine ausgehenden Dienste für nicht vertrauenswürdige Mandanten. Wenn Sie beispielsweise das Konto für einen nicht vertrauenswürdigen Mandanten erstellen, erlauben Sie dem Mandanten nicht, seine eigene Identitätsquelle zu verwenden, und erlauben Sie nicht die Verwendung von Plattformdiensten. Sehen Sie sich die Schritte für"Erstellen eines Mieterkontos" .
- Verwenden Sie für nicht vertrauenswürdigen Client-Datenverkehr einen Load Balancer eines Drittanbieters. Der Lastenausgleich durch Drittanbieter bietet mehr Kontrolle und zusätzliche Schutzebenen gegen Angriffe.
- Verwenden Sie optional einen Speicherproxy für mehr Kontrolle über Cloud-Speicherpools und die Kommunikation der Plattformdienste von Speicherknoten zu externen Diensten. Sehen Sie sich die Schritte für"Erstellen eines Speicherproxys" .
- Optional können Sie über das Client-Netzwerk eine Verbindung zu externen Diensten herstellen. Wählen Sie dann **KONFIGURATION** > **Sicherheit** > **Firewall-Steuerung** > **Nicht vertrauenswürdige Client-Netzwerke** und geben Sie an, dass das Client-Netzwerk auf dem Speicherknoten nicht vertrauenswürdig ist. Der Speicherknoten akzeptiert keinen eingehenden Datenverkehr mehr im Client-Netzwerk, lässt jedoch weiterhin ausgehende Anfragen für Plattformdienste zu.

Richtlinien für Gateway-Knoten

Gateway-Knoten bieten eine optionale Lastausgleichsschnittstelle, die Clientanwendungen zur Verbindung mit StorageGRID verwenden können. Befolgen Sie diese Richtlinien, um alle Gateway-Knoten in Ihrem StorageGRID System zu sichern:

- Konfigurieren und verwenden Sie Load Balancer-Endpunkte. Sehen "Überlegungen zum Lastenausgleich" .
- Verwenden Sie für nicht vertrauenswürdigen Client-Datenverkehr einen Load Balancer eines Drittanbieters zwischen dem Client und dem Gateway-Knoten oder den Speicherknoten. Der Lastenausgleich durch Drittanbieter bietet mehr Kontrolle und zusätzliche Schutzebenen gegen Angriffe. Wenn Sie einen Load Balancer eines Drittanbieters verwenden, kann der Netzwerkverkehr optional weiterhin so konfiguriert werden, dass er über einen internen Load Balancer-Endpunkt läuft oder direkt an Speicherknoten gesendet wird.
- Wenn Sie Load Balancer-Endpunkte verwenden, können Sie Clients optional über das Client-Netzwerk verbinden. Wählen Sie dann **KONFIGURATION** > **Sicherheit** > **Firewall-Steuerung** > **Nicht vertrauenswürdige Client-Netzwerke** und geben Sie an, dass das Client-Netzwerk auf dem Gateway-Knoten nicht vertrauenswürdig ist. Der Gateway-Knoten akzeptiert eingehenden Datenverkehr nur auf den Ports, die explizit als Endpunkte des Lastenausgleichs konfiguriert sind.

Richtlinien für Hardware-Appliance-Knoten

StorageGRID Hardwaregeräte sind speziell für die Verwendung in einem StorageGRID -System konzipiert. Einige Geräte können als Speicherknoten verwendet werden. Andere Appliances können als Admin-Knoten oder Gateway-Knoten verwendet werden. Sie können Appliance-Knoten mit softwarebasierten Knoten kombinieren oder vollständig entwickelte Grids mit ausschließlich Appliances bereitstellen.

Befolgen Sie diese Richtlinien, um alle Hardware-Appliance-Knoten in Ihrem StorageGRID System zu sichern:

- Wenn das Gerät SANtricity System Manager zur Verwaltung des Speichercontrollers verwendet, verhindern Sie, dass nicht vertrauenswürdige Clients über das Netzwerk auf SANtricity System Manager zugreifen.
- Wenn das Gerät über einen Baseboard Management Controller (BMC) verfügt, beachten Sie, dass der BMC Verwaltungsport einen Low-Level-Hardwarezugriff ermöglicht. Verbinden Sie den BMC Verwaltungsport nur mit einem sicheren, vertrauenswürdigen internen Verwaltungsnetzwerk. Wenn kein solches Netzwerk verfügbar ist, lassen Sie den BMC Verwaltungsport unverbunden oder blockiert, es sei denn, der technische Support fordert eine BMC -Verbindung an.
- Wenn die Appliance die Remoteverwaltung der Controller-Hardware über Ethernet mithilfe des IPMI-Standards (Intelligent Platform Management Interface) unterstützt, blockieren Sie nicht vertrauenswürdigen Datenverkehr auf Port 623.

> Sie können den Remote-IPMI-Zugriff für alle Appliances mit einem BMC aktivieren oder deaktivieren. Die Remote-IPMI-Schnittstelle ermöglicht jedem mit einem BMC -Konto und Kennwort den Low-Level-Hardwarezugriff auf Ihre StorageGRID -Geräte. Wenn Sie keinen Remote-IPMI-Zugriff auf den BMC benötigen, deaktivieren Sie diese Option mit einer der folgenden Methoden: + Gehen Sie im Grid Manager zu **KONFIGURATION** > **Sicherheit** > **Sicherheitseinstellungen** > **Geräte** und deaktivieren Sie das Kontrollkästchen **Remote-IPMI-Zugriff aktivieren**. + Verwenden Sie in der Grid-Management-API den privaten Endpunkt: `PUT /private/bmc` .

- Für Appliance-Modelle mit SED-, FDE- oder FIPS NL-SAS-Laufwerken, die Sie mit SANtricity System Manager verwalten, "Aktivieren und Konfigurieren von SANtricity Drive Security" .

- Für Appliance-Modelle mit SED- oder FIPS-NVMe-SSDs, die Sie mit dem StorageGRID Appliance Installer und Grid Manager verwalten, "Aktivieren und Konfigurieren der StorageGRID -Laufwerkverschlüsselung" .
- Aktivieren und konfigurieren Sie für Appliances ohne SED-, FDE- oder FIPS-Laufwerke die StorageGRID Softwareknotenverschlüsselung "mithilfe eines Key Management Servers (KMS)" .

Härtungsrichtlinien für TLS und SSH

Sie sollten die während der Installation erstellten Standardzertifikate ersetzen und die entsprechende Sicherheitsrichtlinie für TLS- und SSH-Verbindungen auswählen.

Härtungsrichtlinien für Zertifikate

Sie sollten die während der Installation erstellten Standardzertifikate durch Ihre eigenen benutzerdefinierten Zertifikate ersetzen.

Bei vielen Organisationen entspricht das selbstsignierte digitale Zertifikat für den StorageGRID Webzugriff nicht ihren Informationssicherheitsrichtlinien. Auf Produktionssystemen sollten Sie ein von einer Zertifizierungsstelle signiertes digitales Zertifikat zur Authentifizierung von StorageGRID installieren.

Insbesondere sollten Sie benutzerdefinierte Serverzertifikate anstelle dieser Standardzertifikate verwenden:

- **Management-Schnittstellenzertifikat**: Wird verwendet, um den Zugriff auf den Grid Manager, den Tenant Manager, die Grid Management API und die Tenant Management API zu sichern.
- **S3-API-Zertifikat**: Wird verwendet, um den Zugriff auf Speicherknoten und Gateway-Knoten zu sichern, die von S3-Clientanwendungen zum Hoch- und Herunterladen von Objektdaten verwendet werden.

Sehen"Sicherheitszertifikate verwalten" für Details und Anweisungen.

> StorageGRID verwaltet die für Load Balancer-Endpunkte verwendeten Zertifikate separat. Informationen zum Konfigurieren von Load Balancer-Zertifikaten finden Sie unter"Konfigurieren von Load Balancer-Endpunkten" .

Beachten Sie bei der Verwendung benutzerdefinierter Serverzertifikate die folgenden Richtlinien:

- Zertifikate sollten eine *`subjectAltName`* das mit den DNS-Einträgen für StorageGRID übereinstimmt. Weitere Einzelheiten finden Sie in Abschnitt 4.2.1.6, „Alternativer Betreffname“, in "RFC 5280: PKIX-Zertifikat und CRL-Profil" .
- Vermeiden Sie nach Möglichkeit die Verwendung von Platzhalterzertifikaten. Eine Ausnahme von dieser Richtlinie ist das Zertifikat für einen virtuell gehosteten S3-Endpunkt, bei dem die Verwendung eines Platzhalters erforderlich ist, wenn die Bucket-Namen nicht im Voraus bekannt sind.
- Wenn Sie in Zertifikaten Platzhalter verwenden müssen, sollten Sie zusätzliche Schritte unternehmen, um die Risiken zu verringern. Verwenden Sie ein Platzhaltermuster wie `*.s3.example.com` und verwenden Sie nicht die `s3.example.com` Suffix für andere Anwendungen. Dieses Muster funktioniert auch mit S3-Zugriff im Pfadstil, wie z. B. `dc1-s1.s3.example.com/mybucket` .
- Legen Sie kurze Ablaufzeiten für Zertifikate fest (z. B. 2 Monate) und verwenden Sie die Grid Management API, um die Zertifikatrotation zu automatisieren. Dies ist besonders wichtig für Wildcard-Zertifikate.

Darüber hinaus sollten Clients bei der Kommunikation mit StorageGRID eine strenge Hostnamenprüfung durchführen.

Härtungsrichtlinien für TLS- und SSH-Richtlinien

Sie können eine Sicherheitsrichtlinie auswählen, um zu bestimmen, welche Protokolle und Verschlüsselungen 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. Als bewährte Methode sollten Sie Verschlüsselungsoptionen deaktivieren, die für die Anwendungskompatibilität nicht erforderlich sind. Verwenden Sie die standardmäßige moderne Richtlinie, es sei denn, Ihr System muss Common Criteria-kompatibel sein oder Sie müssen andere Chiffren verwenden.

Sehen"Verwalten der TLS- und SSH-Richtlinie" für Details und Anweisungen.

Weitere Härtungsrichtlinien

Zusätzlich zur Befolgung der Härtungsrichtlinien für StorageGRID -Netzwerke und -Knoten sollten Sie die Härtungsrichtlinien für andere Bereiche des StorageGRID Systems befolgen.

Temporäres Installationskennwort

Um das StorageGRID -System während der Installation zu sichern, legen Sie auf der Seite mit dem temporären Installationskennwort in der StorageGRID Installationsbenutzeroberfläche oder in der Installations-API ein Kennwort fest. Wenn dieses Passwort festgelegt ist, gilt es für alle Methoden zur Installation von StorageGRID, einschließlich der Benutzeroberfläche, der Installations-API und `configure-storagegrid.py` Skript.

Weitere Informationen finden Sie unter:

- "Installieren Sie StorageGRID unter Red Hat Enterprise Linux"
- "Installieren Sie StorageGRID unter Ubuntu oder Debian"
- "Installieren Sie StorageGRID auf VMware"
- "Installieren Sie das StorageGRID -Gerät"

Protokolle und Prüfmeldungen

Schützen Sie StorageGRID -Protokolle und die Ausgabe von Prüfnachrichten stets auf sichere Weise. StorageGRID -Protokolle und Prüfmeldungen liefern aus Sicht des Supports und der Systemverfügbarkeit wertvolle Informationen. Darüber hinaus sind die in den Protokollen und Prüfnachrichten von StorageGRID enthaltenen Informationen und Details im Allgemeinen vertraulicher Natur.

Konfigurieren Sie StorageGRID so, dass Sicherheitsereignisse an einen externen Syslog-Server gesendet werden. Wenn Sie den Syslog-Export verwenden, wählen Sie TLS und RELP/TLS als Transportprotokolle aus.

Siehe die"Referenz zu Protokolldateien" Weitere Informationen zu StorageGRID Protokollen. Sehen"Prüfmeldungen" Weitere Informationen zu StorageGRID -Auditmeldungen finden Sie unter.

NetApp AutoSupport

Mit der AutoSupport Funktion von StorageGRID können Sie den Zustand Ihres Systems proaktiv überwachen und automatisch Pakete an die NetApp -Support-Site, das interne Support-Team Ihres Unternehmens oder

einen Support-Partner senden. Standardmäßig ist das Senden von AutoSupport Paketen an NetApp aktiviert, wenn StorageGRID zum ersten Mal konfiguriert wird.

Die AutoSupport Funktion kann deaktiviert werden. NetApp empfiehlt jedoch, es zu aktivieren, da AutoSupport die Problemidentifizierung und -lösung beschleunigt, falls auf Ihrem StorageGRID -System ein Problem auftritt.

AutoSupport unterstützt HTTPS, HTTP und SMTP als Transportprotokolle. Aufgrund der sensiblen Natur von AutoSupport Paketen empfiehlt NetApp dringend, HTTPS als Standardtransportprotokoll zum Senden von AutoSupport Paketen an NetApp zu verwenden.

Cross-Origin-Ressourcenfreigabe (CORS)

Sie können Cross-Origin Resource Sharing (CORS) für einen S3-Bucket konfigurieren, wenn dieser Bucket und die darin enthaltenen Objekte für Webanwendungen in anderen Domänen zugänglich sein sollen. Aktivieren Sie CORS grundsätzlich nur, wenn es erforderlich ist. Wenn CORS erforderlich ist, beschränken Sie es auf vertrauenswürdige Ursprünge.

Sehen Sie sich die Schritte für"Konfigurieren der Cross-Origin-Ressourcenfreigabe (CORS)" .

Externe Sicherheitsgeräte

Eine vollständige Härtungslösung muss Sicherheitsmechanismen außerhalb von StorageGRID berücksichtigen. Die Verwendung zusätzlicher Infrastrukturgeräte zum Filtern und Beschränken des Zugriffs auf StorageGRID ist eine effektive Möglichkeit, eine strenge Sicherheitslage zu etablieren und aufrechtzuerhalten. Zu diesen externen Sicherheitsgeräten gehören Firewalls, Intrusion Prevention Systems (IPS) und andere Sicherheitsgeräte.

Für nicht vertrauenswürdigen Client-Datenverkehr wird ein Load Balancer eines Drittanbieters empfohlen. Der Lastenausgleich durch Drittanbieter bietet mehr Kontrolle und zusätzliche Schutzebenen gegen Angriffe.

Ransomware-Minderung

Schützen Sie Ihre Objektdaten vor Ransomware-Angriffen, indem Sie die Empfehlungen in "Ransomware-Abwehr mit StorageGRID" .