Systemhärtung

StorageGRID 11.8

NetApp
May 10, 2024

Inhalt

Systemhärtung

Systemhärtung: Übersicht

Systemhärtung ist der Prozess, bei dem so viele Sicherheitsrisiken wie möglich durch ein StorageGRID System beseitigt werden.

Dieses Dokument bietet einen Überblick über die StorageGRID-spezifischen Härtungsrichtlinien. Diese Richtlinien sind eine Ergänzung zu branchenüblichen Best Practices zur Systemhärtung. In diesen Richtlinien wird beispielsweise davon ausgegangen, dass Sie für StorageGRID starke Passwörter verwenden, HTTPS statt HTTP verwenden und sofern verfügbar die zertifikatbasierte Authentifizierung aktivieren.

Bei der Installation und Konfiguration von StorageGRID können Sie diese Richtlinien nutzen, um alle vorgeschriebenen Sicherheitsziele bezüglich Vertraulichkeit, Integrität und Verfügbarkeit des Informationssystems zu erfüllen.

StorageGRID folgt dem "NetApp Richtlinie zur Bearbeitung von Schwachstellen". Gemeldete Schwachstellen werden gemäß dem Prozess der Reaktion auf Produktsicherheitsvorfälle überprüft und behoben.

Allgemeine Überlegungen zur Erhöhung der StorageGRID-Systeme

Beim Härten eines StorageGRID Systems sind folgende Punkte zu beachten:

- Welches der drei implementierten StorageGRID-Netzwerke ist implementiert? Alle StorageGRID-Systeme müssen das Grid-Netzwerk verwenden, aber Sie können auch das Admin-Netzwerk, das Client-Netzwerk oder beide verwenden. Jedes Netzwerk weist unterschiedliche Sicherheitsüberlegungen auf.
- Die Art der Plattformen, die Sie für die einzelnen Nodes Ihres StorageGRID Systems verwenden. StorageGRID Nodes können auf VMware Virtual Machines innerhalb einer Container-Engine auf Linux-Hosts oder als dedizierte Hardware-Appliances implementiert werden. Jeder Plattformtyp verfügt über eigene Best Practices zur Härtung.
- Wie vertrauenswürdig sind die Mandantenkonten? Wenn Sie ein Service-Provider mit nicht vertrauenswürdigen Mandantenkonten sind, haben Sie andere Sicherheitsbedenken als, wenn Sie nur vertrauenswürdige interne Mandanten verwenden.
- Welche Sicherheitsanforderungen und -Konventionen von Ihrem Unternehmen erfüllt werden? Möglicherweise müssen Sie bestimmte gesetzliche oder unternehmensbezogene Anforderungen einhalten.

Hardening-Richtlinien für Software Upgrades

Sie müssen Ihr StorageGRID-System und die zugehörigen Services immer auf dem neuesten Stand halten, um sich gegen Angriffe zu wehren.

Upgrades auf StorageGRID Software

Sofern möglich, sollten Sie ein Upgrade der StorageGRID Software auf das neueste Hauptversion oder auf das vorherige Hauptversion durchführen. Durch die aktuelle Nutzung von StorageGRID lässt sich die Zeit bis zur aktiven Nutzung bekannter Schwachstellen reduzieren und gleichzeitig die Angriffsfläche insgesamt verringern. Darüber hinaus enthalten die neuesten StorageGRID Versionen häufig Funktionen zur Erhöhung der Sicherheit, die in früheren Versionen nicht enthalten sind.

Konsultieren Sie die "NetApp Interoperabilitäts-Matrix-Tool" (IMT), um zu ermitteln, welche Version der StorageGRID-Software Sie verwenden sollen. Wenn ein Hotfix erforderlich ist, priorisiert NetApp die Erstellung von Updates der letzten Versionen. Einige Patches sind möglicherweise nicht mit früheren Versionen kompatibel.

- Die neuesten StorageGRID Versionen und Hotfixes können Sie unter herunterladen "NetApp Downloads: StorageGRID".
- Informationen zum Aktualisieren der StorageGRID-Software finden Sie im "Upgrade-Anweisungen".
- Informationen zum Anwenden eines Hotfix finden Sie im "StorageGRID Hotfix Verfahren".

Upgrades auf externe Dienste

Externe Services können Schwachstellen aufweisen, die StorageGRID indirekt beeinträchtigen. Sie sollten sicherstellen, dass die Services, von denen StorageGRID abhängig sind, immer auf dem neuesten Stand sind. Zu diesen Services gehören LDAP, KMS (oder KMIP Server), DNS und NTP.

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

Upgrades auf Hypervisoren

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

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

Upgrades auf Linux-Knoten

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

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

Hardening Guidelines for StorageGRID Networks

Das StorageGRID System unterstützt bis zu drei Netzwerkschnittstellen pro Grid Node. So können Sie das Netzwerk für jeden einzelnen Grid Node so konfigurieren, dass er Ihren Sicherheits- und Zugriffsanforderungen entspricht.

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

Richtlinien für Grid Network

Sie müssen ein Grid-Netzwerk für den gesamten internen StorageGRID-Datenverkehr konfigurieren. Alle Grid-Nodes sind im Grid-Netzwerk und müssen mit allen anderen Nodes kommunizieren können.

Befolgen Sie bei der Konfiguration des Grid-Netzwerks die folgenden Richtlinien:

- Stellen Sie sicher, dass das Netzwerk von nicht vertrauenswürdigen Clients, wie denen im offenen Internet, geschützt ist.
- Wenn möglich, verwenden Sie das Grid-Netzwerk ausschließlich für den internen Datenverkehr. Sowohl

das Admin-Netzwerk als auch das Client-Netzwerk haben zusätzliche Firewall-Einschränkungen, die externen Datenverkehr zu internen Diensten blockieren. Die Verwendung des Grid-Netzwerks für externen Client-Datenverkehr wird unterstützt, aber diese Verwendung bietet weniger Schutzebenen.

- Wenn die StorageGRID Implementierung mehrere Datacenter umfasst, verwenden Sie ein virtuelles privates Netzwerk (VPN) oder eine vergleichbare Position im Grid-Netzwerk, um den internen Datenverkehr zusätzlich zu schützen.
- Einige Wartungsverfahren erfordern einen sicheren SSH-Zugriff (Shell) auf Port 22 zwischen dem primären Admin-Node und allen anderen Grid-Nodes. Verwenden Sie eine externe Firewall, um den SSH-Zugriff auf vertrauenswürdige Clients zu beschränken.

Richtlinien für Admin Network

Das Admin-Netzwerk wird normalerweise für administrative Aufgaben verwendet (vertrauenswürdige Mitarbeiter, die den Grid Manager oder SSH verwenden) und für die Kommunikation mit anderen vertrauenswürdigen Services wie LDAP, DNS, NTP oder KMS (oder KMIP Server). StorageGRID ist jedoch nicht intern durchsetzen.

Wenn Sie das Admin-Netzwerk verwenden, befolgen Sie die folgenden Richtlinien:

- Blockieren Sie alle internen Traffic-Ports im Admin-Netzwerk. Siehe "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 Client Network

Das Client-Netzwerk wird typischerweise für Mandanten und zur Kommunikation mit externen Services wie dem CloudMirror Replikationsservice oder einem anderen Plattformservice verwendet. StorageGRID ist jedoch nicht intern durchsetzen.

Wenn Sie das Client-Netzwerk verwenden, befolgen Sie die folgenden Richtlinien:

- Blockieren Sie alle internen Traffic-Ports im Client-Netzwerk. Siehe "Liste der internen Ports".
- Eingehende Clientdatenverkehr nur an explizit konfigurierten Endpunkten akzeptieren. Weitere Informationen finden Sie unter "Management der Firewall-Kontrollen".

Hardening-Richtlinien für StorageGRID-Knoten

StorageGRID Nodes können auf VMware Virtual Machines innerhalb einer Container-Engine auf Linux-Hosts oder als dedizierte Hardware-Appliances implementiert werden. Jeder Plattformtyp und jeder Node-Typ verfügt über eigene Best Practices zur Härtung.

Steuern Sie den Remote-IPMI-Zugriff auf BMC

Sie können den Remote-IPMI-Zugriff für alle Appliances aktivieren oder deaktivieren, die einen BMC enthalten. Die Remote-IPMI-Schnittstelle ermöglicht jedem Benutzer mit einem BMC-Konto und Passwort den Zugriff auf Ihre StorageGRID-Geräte auf niedriger Ebene. 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 **CONFIGURATION** > **Security** > **Security settings** > **Appliances**:

- 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 IPMI-Zugriff auf den BMC zu aktivieren.

Firewall-Konfiguration

Im Rahmen des System-Hardening-Prozesses müssen Sie externe Firewall-Konfigurationen überprüfen und ändern, damit der Datenverkehr nur von den IP-Adressen und den Ports akzeptiert wird, von denen er unbedingt benötigt wird.

StorageGRID verfügt über eine interne Firewall auf jedem Node, die die Sicherheit Ihres Grids erhöht, indem Sie den Netzwerkzugriff auf den Node kontrollieren können. Sollten Sie "Interne Firewall-Kontrollen verwalten" Um den Netzwerkzugriff auf allen Ports zu verhindern, mit Ausnahme der Ports, die für Ihre spezifische Grid-Bereitstellung erforderlich sind. Die Konfigurationsänderungen, die Sie auf der Seite Firewall-Steuerung vornehmen, werden für jeden Knoten bereitgestellt.

Sie können insbesondere diese Bereiche managen:

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

Diese interne Firewall bietet zwar eine zusätzliche Schutzschicht gegen häufig vorgängige Bedrohungen, sie macht aber keine externe Firewall erforderlich.

Eine Liste aller internen und externen Ports, die von StorageGRID verwendet werden, finden Sie unter "Referenz für Netzwerk-Ports".

Deaktivieren Sie nicht verwendete Dienste

Bei allen StorageGRID-Knoten sollten Sie den Zugriff auf nicht genutzte Services deaktivieren oder blockieren. Wenn Sie beispielsweise nicht planen, den Clientzugriff auf die Audit-Freigaben für NFS zu konfigurieren, blockieren oder deaktivieren Sie den Zugriff auf diese Services.

Virtualisierung, Container und gemeinsam genutzte Hardware

Vermeiden Sie bei allen StorageGRID Nodes die Ausführung von StorageGRID auf derselben physischen Hardware wie die nicht vertrauenswürdige Software. Setzen Sie nicht voraus, dass ein Hypervisor-Schutz Malware den Zugriff auf StorageGRID geschützte Daten verhindert, wenn sich sowohl StorageGRID als auch Malware auf derselben physischen Hardware befinden. So nutzen beispielsweise die Meltdown- und Specter-Angriffe kritische Schwachstellen in modernen Prozessoren und ermöglichen Programmen, Daten im Arbeitsspeicher auf demselben Computer zu stehlen.

Schutz von Nodes während der Installation

Erlauben Sie nicht vertrauenswürdigen Benutzern den Zugriff auf StorageGRID-Knoten über das Netzwerk, wenn die Knoten installiert werden. Nodes sind erst dann vollständig sicher, wenn sie sich dem Grid

angeschlossen haben.

Richtlinien für Admin-Nodes

Admin Nodes stellen Managementservices wie Systemkonfiguration, Monitoring und Protokollierung bereit. Wenn Sie sich beim Grid Manager oder dem Tenant Manager anmelden, stellen Sie eine Verbindung zu einem Admin-Node her.

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

- Sichern Sie alle Admin-Knoten von nicht vertrauenswürdigen Clients, wie denen im offenen Internet. Stellen Sie sicher, dass kein nicht vertrauenswürdiger Client auf einen beliebigen Admin-Node im Grid-Netzwerk, auf das Admin-Netzwerk oder auf das Client-Netzwerk zugreifen kann.
- StorageGRID-Gruppen steuern den Zugriff auf Grid Manager- und Mandantenmanager-Funktionen. Gewähren Sie jeder Gruppe von Benutzern die erforderlichen Mindestberechtigungen für ihre Rolle, und verwenden Sie den schreibgeschützten Zugriffsmodus, um zu verhindern, dass Benutzer die Konfiguration ändern.
- Verwenden Sie bei der Verwendung von StorageGRID Load Balancer-Endpunkten Gateway-Nodes anstelle von Admin-Nodes für nicht vertrauenswürdigen Client-Datenverkehr.
- Wenn Sie nicht vertrauenswürdige Mandanten haben, erlauben Sie ihnen keinen direkten Zugriff auf den Mandantenmanager oder die Mandantenmanagement-API. Verwenden Sie stattdessen ein Mandantenportal oder ein externes Mandantenmanagement-System, das mit der Mandantenmanagement-API interagiert.
- Optional können Sie einen Administrator-Proxy verwenden, um die AutoSupport-Kommunikation zwischen Admin-Nodes und der NetApp-Unterstützung besser zu steuern. Siehe die Schritte für "Erstellen eines Admin-Proxy".
- Verwenden Sie optional die eingeschränkten 8443- und 9443-Ports, um die Kommunikation zwischen Grid Manager und Tenant Manager voneinander zu trennen. Blockieren Sie den gemeinsam genutzten Port 443 und beschränken Sie Mandantenanforderungen auf Port 9443, um zusätzlichen Schutz zu bieten.
- Verwenden Sie optional separate Admin-Nodes für Grid-Administratoren und Mandantenbenutzer.

Weitere Informationen finden Sie in den Anweisungen für "Administration von StorageGRID".

Richtlinien für Storage-Nodes

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

- Nicht vertrauenswürdige Clients dürfen keine direkte Verbindung zu Storage-Nodes herstellen. Verwenden Sie einen Load Balancer-Endpunkt, der von einem Gateway-Node oder einem Load Balancer eines Drittanbieters bereitgestellt 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 Nutzung von Plattformdiensten. Siehe die Schritte für "Erstellen eines Mandantenkontos".
- Verwenden Sie einen Drittanbieter-Load-Balancer für nicht vertrauenswürdigen Client-Datenverkehr. Der Lastausgleich von Drittanbietern bietet mehr Kontrolle und zusätzlichen Schutz vor Angriffen.
- Verwenden Sie optional einen Storage Proxy, um mehr Kontrolle über Cloud-Storage-Pools und die Kommunikation der Plattformservices von Storage Nodes zu externen Services zu erhalten. Siehe die Schritte für "Erstellen eines Speicherproxys".

- Optional können Sie über das Client-Netzwerk eine Verbindung zu externen Diensten herstellen. Wählen Sie dann **CONFIGURATION** > **Security** > **Firewall Control** > **UnTrusted Client Networks** aus und geben Sie an, dass das Client-Netzwerk auf dem Storage Node nicht vertrauenswürdig ist. Der Speicherknoten akzeptiert keinen eingehenden Datenverkehr im Client-Netzwerk mehr, aber er erlaubt weiterhin ausgehende Anfragen für Platform Services.

Richtlinien für Gateway-Nodes

Gateway-Knoten stellen eine optionale Schnittstelle zum Lastausgleich bereit, über die Client-Anwendungen eine Verbindung zu StorageGRID herstellen können. Befolgen Sie die folgenden Richtlinien zum Sichern aller Gateway-Knoten in Ihrem StorageGRID System:

- Konfigurieren und verwenden Sie Load Balancer-Endpunkte. Siehe "Überlegungen zum Lastausgleich".
- Verwenden Sie für nicht vertrauenswürdigen Client-Datenverkehr einen Drittanbieter-Load-Balancer zwischen Client und Gateway-Node oder Storage-Nodes. Der Lastausgleich von Drittanbietern bietet mehr Kontrolle und zusätzlichen Schutz vor Angriffen. Wenn Sie einen Load Balancer eines Drittanbieters verwenden, kann der Netzwerk-Traffic optional auch so konfiguriert werden, dass er über einen internen Load Balancer-Endpunkt geleitet oder direkt an Storage Nodes gesendet wird.
- Wenn Sie Load Balancer-Endpunkte verwenden, lassen Sie optional Clients über das Client-Netzwerk verbinden. Wählen Sie dann **CONFIGURATION** > **Security** > **Firewall Control** > **UnTrusted Client Networks** aus und geben Sie an, dass das Client-Netzwerk auf dem Gateway Node nicht vertrauenswürdig ist. Der Gateway-Node akzeptiert nur eingehenden Datenverkehr an den Ports, die explizit als Load Balancer-Endpunkte konfiguriert wurden.

Richtlinien für die Nodes von Hardware-Appliances

StorageGRID Hardware-Appliances wurden speziell für den Einsatz in einem StorageGRID System entwickelt. Einige Geräte können als Storage-Nodes verwendet werden. Andere Appliances können als Admin-Nodes oder Gateway-Nodes verwendet werden. Appliance-Nodes können mit softwarebasierten Nodes kombiniert oder voll entwickelten All-Appliance-Grids implementiert werden.

Beachten Sie diese Richtlinien zum Schutz aller Hardware-Appliance-Nodes in Ihrem StorageGRID System:

- Wenn die Appliance SANtricity System Manager zum Management des Storage Controllers verwendet, verhindern Sie, dass nicht vertrauenswürdige Clients über das Netzwerk auf SANtricity System Manager zugreifen.
- Wenn die Appliance über einen Baseboard Management Controller (BMC) verfügt, beachten Sie, dass der BMC-Management-Port einen niedrigen Hardwarezugriff ermöglicht. Schließen Sie den BMC-Management-Port nur an ein sicheres, vertrauenswürdiges, internes Management-Netzwerk an. Wenn kein solches Netzwerk verfügbar ist, lassen Sie den BMC-Management-Port unverbunden oder blockiert, es sei denn, eine BMC-Verbindung wird vom technischen Support angefordert.
- Wenn die Appliance die Remote-Verwaltung der Controller-Hardware über Ethernet mit dem IPMI-Standard (Intelligent Platform Management Interface) unterstützt, blockieren Sie den nicht vertrauenswürdigen Datenverkehr auf Port 623.

Sie können den Remote-IPMI-Zugriff für alle Appliances aktivieren oder deaktivieren, die einen BMC enthalten. Die Remote-IPMI-Schnittstelle ermöglicht jedem Benutzer mit einem BMC-Konto und Passwort den Zugriff auf Ihre StorageGRID-Geräte auf niedriger Ebene. 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 **CONFIGURATION** > **Security** > **Security settings** > **Appliances** und deaktivieren Sie das Kontrollkästchen **Remote-IPMI-Zugriff aktivieren**.
Verwenden Sie in der Grid-Management-API den privaten Endpunkt: `PUT /private/bmc`.

- Bei Appliance-Modellen mit SED-, FDE- oder FIPS-NL-SAS-Laufwerken, die Sie mit SANtricity System Manager managen, "Aktivieren und konfigurieren Sie die SANtricity-Laufwerksicherheit".
- Für Appliance-Modelle, die SED- oder FIPS-NVMe-SSDs enthalten und die Sie mit dem StorageGRID Appliance Installer und Grid Manager managen, "Aktivieren und konfigurieren Sie die StorageGRID-Laufwerkverschlüsselung".
- Bei Appliances ohne SED-, FDE- oder FIPS-Laufwerke aktivieren und konfigurieren Sie die StorageGRID Software-Node-Verschlüsselung "Verwendung 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.

Richtlinien für die Härtung von Zertifikaten

Sie sollten die während der Installation erstellten Standardzertifikate durch eigene benutzerdefinierte Zertifikate ersetzen.

Für viele Unternehmen entspricht das selbstsignierte digitale Zertifikat für den StorageGRID-Webzugriff nicht den Richtlinien für die Informationssicherheit. Auf Produktionssystemen sollten Sie ein CA-signiertes digitales Zertifikat zur Verwendung bei der Authentifizierung von StorageGRID installieren.

Sie sollten insbesondere anstelle der folgenden Standardzertifikate benutzerdefinierte Serverzertifikate verwenden:

- **Zertifikat der Verwaltungsschnittstelle**: Zur Sicherung des Zugriffs auf den Grid Manager, den Tenant Manager, die Grid Management API und die Tenant Management API.
- **S3- und Swift-API-Zertifikat**: Dient zum sicheren Zugriff auf Storage-Nodes und Gateway-Nodes, die S3- und Swift-Client-Anwendungen zum Hochladen und Herunterladen von Objektdaten verwenden.

Siehe "Verwalten von Sicherheitszertifikaten" Für Details und Anweisungen.

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

Wenn Sie benutzerdefinierte Serverzertifikate verwenden, befolgen Sie die folgenden Richtlinien:

- Zertifikate sollten ein haben *`subjectAltName`* Das stimmt mit DNS-Einträgen für StorageGRID überein. Weitere Informationen finden Sie in Abschnitt 4.2.1.6, „alternativer Antragstellername“ in "RFC 5280: PKIX-Zertifikat und CRL-Profil".

- Wenn möglich, vermeiden Sie die Verwendung von Platzhalterzertifikaten. Eine Ausnahme dieser Richtlinie ist das Zertifikat für einen S3-Endpunkt im virtuellen Hosted-Stil, der die Verwendung eines Platzhalters erfordert, wenn Bucket-Namen nicht im Voraus bekannt sind.
- Wenn Sie Wildcards in Zertifikaten verwenden müssen, sollten Sie weitere Schritte zur Reduzierung der Risiken Unternehmen. Verwenden Sie ein Platzhalter-Muster z. B. `*.s3.example.com`Und verwenden Sie nicht die `s3.example.com` Suffix für andere Applikationen Dieses Muster funktioniert auch mit Path-Style S3-Zugriff, z. B. `dc1-s1.s3.example.com/mybucket`.
- Legen Sie die Ablaufzeiten für das Zertifikat auf kurz (z. B. 2 Monate) fest, und automatisieren Sie die Zertifikatrotation mithilfe der Grid Management API. Dies ist besonders wichtig für Platzhalterzertifikate.

Darüber hinaus sollten Kunden bei der Kommunikation mit StorageGRID strenge Hostnamen-Kontrollen verwenden.

Richtlinien für die Härtung von TLS- und SSH-Richtlinien

Sie können eine Sicherheitsrichtlinie auswählen, um festzulegen, welche Protokolle und Chiffren zum Aufbau sicherer TLS-Verbindungen mit Clientanwendungen und sicherer SSH-Verbindungen zu internen StorageGRID-Diensten verwendet werden.

Die Sicherheitsrichtlinie steuert, wie TLS und SSH Daten in Bewegung verschlüsseln. Als Best Practice sollten Sie Verschlüsselungsoptionen deaktivieren, die für die Anwendungskompatibilität nicht erforderlich sind. Verwenden Sie die moderne Standardrichtlinie, es sei denn, Ihr System muss Common Criteria-konform sein oder Sie müssen andere Chiffren verwenden.

Siehe "Verwalten Sie die TLS- und SSH-Richtlinie" Für Details und Anweisungen.

Andere Hinweise zur Verhärtung

Beachten Sie zusätzlich die Hinweise zur Verhärtung von StorageGRID-Netzwerken und -Knoten die Härtungsrichtlinien für andere Bereiche des StorageGRID-Systems.

Protokolle und Prüfmeldungen

Sichern Sie StorageGRID-Protokolle und die Ausgabe von Prüfnachrichten sicher. StorageGRID-Protokolle und Audit-Meldungen bieten wertvolle Informationen aus Sicht der Support- und Systemverfügbarkeit. Darüber hinaus handelt es sich bei den Informationen und Details der StorageGRID-Protokolle und der Ausgabe von Audit-Meldungen in der Regel um sensible Daten.

Konfigurieren Sie StorageGRID, um Sicherheitsereignisse an einen externen Syslog-Server zu senden. Wenn Sie syslog-Export verwenden, wählen Sie TLS und RELP/TLS für die Transportprotokolle aus.

Siehe "Referenz für Protokolldateien" Weitere Informationen zu StorageGRID-Protokollen. Siehe "Audit-Meldungen" Weitere Informationen zu StorageGRID-Überwachungsmeldungen.

NetApp AutoSupport

Mit der AutoSupport Funktion von StorageGRID können Sie den Zustand Ihres Systems proaktiv überwachen und automatisch Pakete an die NetApp Support Website, 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 die Aktivierung, da AutoSupport

die Identifizierung von Problemen und die Behebung von Problemen beschleunigt, wenn es auf Ihrem StorageGRID System zu Problemen kommt.

AutoSupport unterstützt HTTPS, HTTP und SMTP für Transportprotokolle. Aufgrund der sensiblen Natur von AutoSupport-Paketen empfiehlt NetApp dringend die Verwendung von HTTPS als Standard-Transportprotokoll für das Senden von AutoSupport-Paketen an NetApp.

Cross-Origin Resource Sharing (CORS)

Sie können CORS (Cross-Origin Resource Sharing) für einen S3-Bucket konfigurieren, wenn Webapplikationen in anderen Domänen auf diesen Bucket und die Objekte in diesem Bucket zugreifen sollen. Im Allgemeinen sollten Sie CORS nur aktivieren, wenn dies erforderlich ist. Wenn CORS erforderlich ist, beschränken Sie es auf vertrauenswürdige Herkunft.

Siehe die Schritte für "Konfigurieren der Cross-Origin Resource Sharing (CORS)".

Externe Sicherheitsgeräte

Eine vollständige Härtungslösung muss auch Sicherheitsmechanismen außerhalb von StorageGRID berücksichtigen. Der Einsatz zusätzlicher Infrastrukturgeräte zum Filtern und zur Einschränkung des Zugriffs auf StorageGRID ist eine effektive Möglichkeit, eine anspruchsvolle Sicherheit zu schaffen und zu erhalten. Zu diesen externen Sicherheitsgeräten gehören Firewalls, Intrusion Prevention Systems (IPSs) und andere Sicherheitsgeräte.

Für nicht vertrauenswürdigen Client-Datenverkehr wird ein Load Balancer eines Drittanbieters empfohlen. Der Lastausgleich von Drittanbietern bietet mehr Kontrolle und zusätzlichen Schutz vor Angriffen.

Ransomware-Minderung

Befolgen Sie die Empfehlungen in, um Ihre Objektdaten vor Ransomware-Angriffen zu schützen "Ransomware-Verteidigung mit StorageGRID".