Systemhärtung für StorageGRID

StorageGRID software

NetApp
July 23, 2026

Inhalt

Systemhärtung für StorageGRID

Erfahren Sie mehr über die Systemhärtung für StorageGRID

Die Systemhärtung ist der Prozess, bei dem so viele Sicherheitsrisiken wie möglich aus einem StorageGRID System entfernt werden.

Bei der Installation und Konfiguration von StorageGRID helfen diese Richtlinien dabei, die vorgegebenen Sicherheitsziele hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.

Sie sollten bereits branchenübliche Best Practices zur Systemhärtung anwenden. Beispielsweise verwenden Sie sichere Passwörter für StorageGRID, nutzen HTTPS anstelle von HTTP und aktivieren zertifikatbasierte Authentifizierung, wo verfügbar. Diese Best Practices müssen physische und umweltbezogene Sicherheitsmaßnahmen umfassen, die den physischen Zugriff einschränken sowie das physische Rechenzentrum und die unterstützende Infrastruktur schützen. Es sind zudem alle geltenden regulatorischen Standards und Empfehlungen für Ihr Unternehmen und Ihre Region zu berücksichtigen.

StorageGRID folgt dem "NetApp Richtlinie zur Handhabung von Sicherheitslücken". Gemeldete Schwachstellen werden gemäß dem Prozess zur Reaktion auf Sicherheitsvorfälle des Produkts überprüft und behoben.

Bei der Härtung eines StorageGRID Systems sind die folgenden Punkte zu berücksichtigen:

- **Welches der drei StorageGRID Netzwerke** implementiert wurde. Alle StorageGRID Systeme müssen das Grid Network verwenden, es kann jedoch auch das Admin Network, das Client Network oder beide genutzt werden. Jedes Netzwerk hat unterschiedliche Sicherheitsanforderungen.
- **Die Art der Plattformen**, die Sie für die einzelnen Knoten Ihres StorageGRID Systems verwenden. StorageGRID Knoten können auf VMware virtuellen Maschinen, innerhalb einer Container Engine auf Linux Hosts oder als dedizierte Hardware Appliances bereitgestellt werden. Jede Plattformart verfügt über eigene Best Practices zur Härtung.
- **Wie vertrauenswürdig die Mandantenkonten sind**. Wenn Sie ein Dienstanbieter mit nicht vertrauenswürdigen Mandantenkonten sind, ergeben sich andere Sicherheitsbedenken als bei der ausschließlichen Nutzung vertrauenswürdiger, interner Mandanten.
- **Welche Sicherheitsanforderungen und -konventionen** Ihre Organisation befolgt. Möglicherweise müssen bestimmte behördliche oder unternehmensinterne Anforderungen erfüllt werden.

Härtungsrichtlinien für StorageGRID-Software-Upgrades

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

Upgrades der StorageGRID Software

Wann immer möglich, sollten Sie die StorageGRID Software auf das neueste Hauptrelease oder das vorherige Hauptrelease aktualisieren. StorageGRID auf dem neuesten Stand zu halten, trägt dazu bei, den Zeitraum, in dem bekannte Schwachstellen aktiv sind, zu verkürzen und die gesamte Angriffsfläche zu verringern. Darüber hinaus enthalten die neuesten Versionen von StorageGRID häufig Funktionen zur Sicherheitshärtung, die in früheren Versionen nicht enthalten sind.

Die "NetApp Interoperabilitätsmatrix-Tool" (IMT) gibt Aufschluss darüber, welche Version der StorageGRID

Software verwendet werden sollte. Wenn ein Hotfix erforderlich ist, priorisiert NetApp die Erstellung von Updates für die neuesten Versionen. Einige Patches sind möglicherweise nicht mit früheren Versionen kompatibel.

- Um die aktuellsten StorageGRID Releases und Hotfixes herunterzuladen, gehen Sie zu "NetApp Downloads: StorageGRID".
- Informationen zum Upgrade der StorageGRID Software sind unter "Upgrade Anleitung" zu finden.
- Zum Anwenden eines Hotfixes siehe "StorageGRID Hotfix Verfahren".

Aktualisierungen externer Dienste

Externe Dienste können Sicherheitslücken aufweisen, die StorageGRID indirekt beeinträchtigen. Es sollte sichergestellt werden, dass die von StorageGRID genutzten Dienste stets aktuell sind. Zu diesen Diensten gehören LDAP, KMS (oder KMIP Server), DNS und NTP.

Eine Liste der unterstützten Versionen ist unter "NetApp Interoperabilitätsmatrix-Tool" zu finden.

Upgrades von Hypervisoren

Wenn Ihre StorageGRID-Knoten auf VMware oder einem anderen Hypervisor laufen, muss sichergestellt sein, dass die Hypervisor-Software und -Firmware auf dem neuesten Stand sind.

Eine Liste der unterstützten Versionen ist unter "NetApp Interoperabilitätsmatrix-Tool" zu finden.

Upgrades auf Linux-Knoten

Wenn Ihre StorageGRID-Knoten Linux-Hostplattformen verwenden, muss sichergestellt werden, dass Sicherheitsupdates und Kernel-Updates auf dem Host-Betriebssystem angewendet werden. Zusätzlich sind Firmware-Updates auf gefährdete Hardware anzuwenden, sobald diese Updates verfügbar sind.

Eine Liste der unterstützten Versionen ist unter "NetApp Interoperabilitätsmatrix-Tool" zu finden.

Härtungsrichtlinien für StorageGRID Netzwerke

Das StorageGRID System unterstützt bis zu drei Netzwerkschnittstellen pro Grid-Knoten, sodass die Netzwerkkonfiguration für jeden einzelnen Grid-Knoten an die jeweiligen Sicherheits- und Netzwerkzugriffsanforderungen angepasst werden kann.

Detaillierte Informationen zu StorageGRID Netzwerken sind unter "StorageGRID Netzwerktypen" verfügbar.

Richtlinien für das Grid-Netzwerk

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

Bei der Konfiguration des Grid Network sind folgende Richtlinien zu berücksichtigen:

- Es sollte sichergestellt sein, dass das Netzwerk vor nicht vertrauenswürdigen Clients, wie beispielsweise solchen im offenen Internet, geschützt ist.
- Wenn möglich, ausschließlich das Grid Network für internen Datenverkehr verwenden. Sowohl das Admin Network als auch das Client Network unterliegen zusätzlichen Firewall-Beschränkungen, die externen

Datenverkehr zu internen Diensten blockieren. Die Nutzung des Grid Network für externen Client-Datenverkehr ist unterstützt, bietet jedoch weniger Schutzebenen.

- Wenn sich die StorageGRID Implementierung über mehrere Rechenzentren erstreckt, sollte ein virtuelles privates Netzwerk (VPN) oder ein gleichwertiges System im Grid Netzwerk für zusätzlichen Schutz des internen Datenverkehrs auf dem Grid Netzwerk eingesetzt werden.
- Für einige Wartungsverfahren ist ein Secure Shell (SSH)-Zugriff auf Port 22 zwischen dem primären Admin-Node und allen anderen Grid-Nodes erforderlich. Ein externer Firewall-Schutz beschränkt den SSH-Zugriff auf vertrauenswürdige Clients.

Richtlinien für das Admin Netzwerk

Das Admin Network wird typischerweise für administrative Aufgaben (von vertrauenswürdigen Mitarbeitern über den Grid Manager oder SSH) und zur Kommunikation mit anderen vertrauenswürdigen Diensten wie LDAP, DNS, NTP oder KMS (oder KMIP Server) verwendet. StorageGRID erzwingt diese Nutzung jedoch nicht intern.

Wenn das Admin Network verwendet wird, gelten diese Richtlinien:

- Alle internen Datenverkehrsports im Admin-Netzwerk blockieren. Siehe "Liste der internen Ports".
- Falls nicht vertrauenswürdige Clients auf das Admin-Netzwerk zugreifen können, sollte der Zugriff auf StorageGRID im Admin-Netzwerk mit einer externen Firewall blockiert werden.

Richtlinien für das Client-Netzwerk

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

Wenn Sie das Client-Netzwerk nutzen, gelten folgende Richtlinien:

- Alle internen Datenverkehrsports im Client-Netzwerk blockieren. Siehe "Liste der internen Ports".
- Eingehender Client-Datenverkehr wird nur an explizit konfigurierten Endpunkten akzeptiert. Informationen zu "Verwaltung der Firewall-Steuerung".

Härtungsrichtlinien für StorageGRID Knoten

StorageGRID-Knoten können auf VMware-VMs, innerhalb einer Container-Engine auf Linux-Hosts oder als dedizierte Hardware-Appliances bereitgestellt werden. Jede Plattform und jeder Knotentyp verfügt über eigene Best Practices zur Härtung.

Remote-IPMI-Zugriff auf BMC steuern

Sie können den Remote-IPMI-Zugriff für alle Appliances mit einem BMC aktivieren oder deaktivieren. Die Remote-IPMI-Schnittstelle ermöglicht jedem Benutzer mit einem BMC-Konto und Passwort den hardwarenahen Zugriff auf Ihre StorageGRID Appliances. Wenn kein Remote-IPMI-Zugriff auf das BMC benötigt wird, sollte diese Option deaktiviert werden.

- Um den Remote-IPMI-Zugriff auf den BMC im Grid Manager zu steuern, navigieren Sie zu **Konfiguration** > **Sicherheit** > **Sicherheitseinstellungen** > **Appliances**:
  - Das Kontrollkästchen **Enable remote IPMI access** muss deaktiviert sein, damit der IPMI-Zugriff auf den BMC nicht möglich ist.

- Das Kontrollkästchen **Enable remote IPMI access** aktivieren, um den IPMI-Zugriff auf den BMC zu ermöglichen.

Weitere Informationen zur BMC-Härtung finden sich im "Baseboard Management Controller härten"Informationsblatt zur Cybersicherheit von "National Security Agency (NSA)" und "Cybersecurity and Infrastructure Security Agency (CISA)".

Firewall Konfiguration

Im Rahmen der Systemhärtung ist eine Überprüfung und Anpassung der externen Firewall-Konfigurationen erforderlich, sodass Datenverkehr nur von den IP-Adressen und auf den Ports akzeptiert wird, von denen er unbedingt benötigt wird.

StorageGRID verfügt über eine interne Firewall auf jedem Knoten, die die Sicherheit Ihres Grids erhöht, indem sie Ihnen die Kontrolle über den Netzwerkzugriff auf den Knoten ermöglicht. Es empfiehlt sich, "interne Firewall-Steuerungen verwalten" den Netzwerkzugriff auf alle Ports außer denen zu verhindern, die für Ihre spezifische Grid-Bereitstellung erforderlich sind. Die auf der Firewall-Steuerungsseite vorgenommenen Konfigurationsänderungen werden auf jeden Knoten angewendet.

Konkret lassen sich diese Bereiche verwalten:

- **Privilegierte Adressen**: Ausgewählten IP-Adressen oder Subnetzen kann der Zugriff auf Ports gewährt werden, die durch die Einstellungen auf der Registerkarte „Externen Zugriff verwalten“ geschlossen sind.
- **Externen Zugriff verwalten**: Standardmäßig geöffnete Ports können geschlossen oder zuvor geschlossene Ports wieder geöffnet werden.
- **Nicht vertrauenswürdiges Client-Netzwerk**: Es kann festgelegt werden, ob ein Knoten eingehenden Datenverkehr aus dem Client-Netzwerk als vertrauenswürdig behandelt, sowie welche zusätzlichen Ports geöffnet werden, wenn ein nicht vertrauenswürdiges Client-Netzwerk konfiguriert ist.

Diese interne Firewall bietet zwar eine zusätzliche Schutzebene gegen einige häufige Bedrohungen, entfernt jedoch nicht die Notwendigkeit einer externen Firewall.

Eine Liste aller internen und externen Ports, die von StorageGRID verwendet werden, ist unter "StorageGRID interne Ports" und "Ports für externe Kommunikation" zu finden.

Nicht verwendete Dienste deaktivieren

Für alle StorageGRID-Knoten sollte der Zugriff auf nicht verwendete Dienste deaktiviert oder blockiert werden. Wenn beispielsweise DHCP nicht verwendet wird, kann Port 68 über den Grid Manager geschlossen werden. **Konfiguration** > **Firewall control** > **Manage external access** auswählen. Den Statusschalter für Port 68 von **Open** auf **Closed** ändern.

Virtualisierung, Container und gemeinsam genutzte Hardware

Für alle StorageGRID-Knoten sollte vermieden werden, StorageGRID auf derselben physischen Hardware wie nicht vertrauenswürdige Software auszuführen. Es sollte nicht davon ausgegangen werden, dass Hypervisor-Schutzmechanismen Malware am Zugriff auf StorageGRID-geschützte Daten hindern, wenn sich sowohl StorageGRID als auch die Malware auf derselben physischen Hardware befinden. Beispielsweise nutzen die Meltdown- und Spectre-Angriffe kritische Schwachstellen in modernen Prozessoren aus und ermöglichen Programmen, Daten im Arbeitsspeicher desselben Computers zu stehlen.

Schutz der Knoten während der Installation

Nicht vertrauenswürdigen Benutzern sollte kein Netzwerkzugriff auf StorageGRID-Knoten gewährt werden, während die Knoten installiert werden. Die Knoten sind erst vollständig sicher, nachdem sie dem Grid beigetreten sind.

Physischer Zugriff auf die Hardware sollte eingeschränkt werden

Der physische Zugriff auf StorageGRID Hardware Appliance-Knoten sowie auf VMware Virtual Machine-Hosts und Linux-Hosts, auf denen StorageGRID ausgeführt wird, ist ausschließlich autorisierten Administratoren vorbehalten. Beispiele für physische Zugriffskontrollen sind Schlösser, Wachpersonal, physische Barrieren und Videoüberwachung.

Hardware Appliance-Knoten sind so konzipiert, dass sie ausschließlich von autorisierten Administratoren installiert und betrieben werden. Nicht autorisierten Administratoren darf kein Zugriff auf Hardware Appliance-Knoten gewährt werden.

Richtlinien für Admin-Knoten

Admin Nodes bieten Verwaltungsdienste wie Systemkonfiguration, Überwachung und Protokollierung. Bei der Anmeldung am Grid Manager oder Tenant Manager erfolgt eine Verbindung zu einem Admin Node.

Diese Richtlinien tragen dazu bei, die Admin-Knoten im StorageGRID System abzusichern:

- Alle Admin-Knoten sind vor nicht vertrauenswürdigen Clients, wie beispielsweise solchen aus dem offenen Internet, zu schützen. Es ist sicherzustellen, dass kein nicht vertrauenswürdiger Client auf einen Admin-Knoten im Grid Network, im Admin Network oder im Client Network zugreifen kann.
- StorageGRID Gruppen steuern den Zugriff auf Grid Manager und Tenant Manager Funktionen. Jeder Benutzergruppe werden die für ihre Rolle erforderlichen Mindestberechtigungen gewährt, und der schreibgeschützte Zugriffsmodus verhindert, dass Benutzer die Konfiguration ändern.
- Bei Verwendung von StorageGRID Load Balancer-Endpunkten sind für nicht vertrauenswürdigen Client-Datenverkehr Gateway-Knoten anstelle von Admin-Knoten zu nutzen.
- Wenn Sie nicht vertrauenswürdige Mandanten haben, sollte ihnen kein direkter Zugriff auf den Tenant Manager oder die Tenant Management API gewährt werden. Stattdessen empfiehlt sich für diese Mandanten die Nutzung eines Mandantenportals oder eines externen Mandantenverwaltungssystems, das mit der Tenant Management API interagiert.
- Optional kann ein Admin-Proxy verwendet werden, um die AutoSupport-Kommunikation von Admin-Knoten zu NetApp Support besser zu steuern. Siehe die Schritte für "Erstellen eines Admin-Proxys".
- Optional können die eingeschränkten Ports 8443 und 9443 verwendet werden, um die Kommunikation zwischen Grid Manager und Tenant Manager zu trennen. Der gemeinsam genutzte Port 443 sollte blockiert und Tenant-Anfragen auf Port 9443 beschränkt werden, um zusätzlichen Schutz zu bieten.
- Optional können separate Admin-Knoten für Grid-Administratoren und Mandantenbenutzer genutzt werden.

Weitere Informationen sind in der Anleitung für "Verwaltung von StorageGRID" zu finden.

Richtlinien für Speicherknoten

Speicherknoten verwalten und speichern Objektdaten und Metadaten. Die folgenden Richtlinien tragen zur Absicherung der Speicherknoten im StorageGRID System bei.

- Untrusted Clients sollte keine direkte Verbindung zu Storage Nodes ermöglicht werden. Ein Load Balancer Endpoint, der von einem Gateway Node oder einem Third Party Load Balancer bereitgestellt wird, ist zu verwenden.
- Keine ausgehenden Dienste für nicht vertrauenswürdige Mandanten aktivieren. Beispielsweise sollte beim Erstellen eines Kontos für einen nicht vertrauenswürdigen Mandanten nicht erlaubt werden, dass dieser seine eigene Identitätsquelle verwendet oder Plattformdienste nutzt. Die Schritte für "Erstellen eines Mandantenkontos" sind zu beachten.
- Ein Load Balancer eines Drittanbieters kann für den Datenverkehr nicht vertrauenswürdiger Clients eingesetzt werden. Load Balancing durch Drittanbieter bietet mehr Kontrolle und zusätzliche Schutzebenen gegen Angriffe.
- Optional kann ein Speicherproxy verwendet werden, um mehr Kontrolle über die Kommunikation von Cloud Storage Pools und Plattformdiensten von Storage Nodes zu externen Diensten zu erhalten. Siehe die Schritte für "Erstellen eines Speicherproxys".
- Optional kann über das Clientnetzwerk eine Verbindung zu externen Diensten hergestellt werden. Dann **Konfiguration** > **Sicherheit** > **Firewall control** > **Untrusted Client Networks** auswählen und angeben, dass das Clientnetzwerk auf dem Storage Node nicht vertrauenswürdig ist. Der Storage Node akzeptiert keinen eingehenden Datenverkehr mehr über das Clientnetzwerk, erlaubt jedoch weiterhin ausgehende Anfragen an Platform Services.

Richtlinien für Gateway-Knoten

Gateway Nodes bieten eine optionale Load-Balancing-Schnittstelle, die von Clientanwendungen zur Verbindung mit StorageGRID genutzt werden kann. Die folgenden Richtlinien dienen der Absicherung aller Gateway Nodes im StorageGRID System:

- Load Balancer-Endpunkte konfigurieren und verwenden. Siehe "Überlegungen zum Lastausgleich".
- Ein Load Balancer eines Drittanbieters sollte zwischen dem Client und dem Gateway Node oder den Storage Nodes für nicht vertrauenswürdigen Client-Datenverkehr eingesetzt werden. Ein Load Balancer eines Drittanbieters bietet mehr Kontrolle und zusätzliche Schutzebenen gegen Angriffe. Wenn ein Load Balancer eines Drittanbieters verwendet wird, kann der Netzwerkverkehr optional weiterhin so konfiguriert werden, dass er über einen internen Load Balancer-Endpunkt geleitet oder direkt an die Storage Nodes gesendet wird.
- Wenn Sie Load-Balancer-Endpunkte verwenden, können Clients optional über das Client-Netzwerk eine Verbindung herstellen. Anschließend **Konfiguration** > **Sicherheit** > **Firewall control** > **Nicht vertrauenswürdige Client-Netzwerke** auswählen und angeben, dass das Client-Netzwerk auf dem Gateway-Knoten nicht vertrauenswürdig ist. Der Gateway-Knoten akzeptiert eingehenden Datenverkehr nur auf den Ports, die explizit als Load-Balancer-Endpunkte konfiguriert sind.

Richtlinien für Hardware Appliance-Knoten

StorageGRID Hardware Appliances sind speziell für den Einsatz in einem StorageGRID System konzipiert. Einige Appliances können als Storage Nodes verwendet werden. Andere Appliances können als Admin Nodes oder Gateway Nodes verwendet werden. Es besteht die Möglichkeit, Appliance Nodes mit softwarebasierten Nodes zu kombinieren oder vollständig entwickelte, ausschließlich aus Appliances bestehende Grids bereitzustellen.

Diese Richtlinien dienen der Absicherung aller Hardware Appliance-Knoten in Ihrem StorageGRID System:

- Wenn das Gerät SANtricity System Manager für die Verwaltung des Speichercontrollers verwendet, sollte verhindert werden, dass nicht vertrauenswürdige Clients über das Netzwerk auf SANtricity System Manager zugreifen.

- Verfügt das Gerät über einen Baseboard Management Controller (BMC), ist zu beachten, dass der BMC Management Port den Zugriff auf die Hardware auf niedriger Ebene ermöglicht. Der BMC Management Port sollte ausschließlich mit einem sicheren, vertrauenswürdigen internen Management-Netzwerk verbunden werden.

  Sie können ein VLAN einrichten, um BMC-Netzwerkverbindungen zu isolieren und den Internetzugang von BMC auf vertrauenswürdige Netzwerke zu beschränken. Weitere Informationen zur Durchsetzung der VLAN-Trennung enthält das "Baseboard Management Controller härten" Informationsblatt zur Cybersicherheit von "National Security Agency (NSA)" und "Cybersecurity and Infrastructure Security Agency (CISA)".

  Wenn kein sicheres, vertrauenswürdiges internes Managementnetzwerk verfügbar ist, sollte der BMC Managementport unverbunden oder blockiert bleiben. Der technische Support könnte während eines Supportfalls temporären Zugriff anfordern.

- Wenn das Gerät die Fernverwaltung der Controller-Hardware über Ethernet unter Verwendung des Intelligent Platform Management Interface (IPMI)-Standards unterstützt, sollte nicht vertrauenswürdiger Datenverkehr auf Port 623 blockiert werden.

> ⓘ Sie können den Remote-IPMI-Zugriff für alle Appliances mit einem BMC aktivieren oder deaktivieren. Die Remote-IPMI-Schnittstelle ermöglicht jedem Benutzer mit einem BMC-Konto und -Passwort einen Low-Level-Hardwarezugriff auf Ihre StorageGRID Appliances. Wenn kein Remote-IPMI-Zugriff auf den BMC benötigt wird, kann diese Option mit einer der folgenden Methoden deaktiviert werden: + Im Grid Manager unter **Konfiguration** > **Sicherheit** > **Sicherheitseinstellungen** > **Appliances** das Kontrollkästchen **Remote-IPMI-Zugriff aktivieren** deaktivieren. + In der Grid-Management-API den privaten Endpunkt verwenden: `PUT /private/bmc`.

+ Sie können auch Remote IPMI-Zugriff deaktivieren.

- Für Appliance-Modelle mit SED, FDE oder FIPS NL-SAS-Laufwerken, die Sie mit SANtricity System Manager verwalten, "SANtricity Drive Security aktivieren und konfigurieren".
- Für Appliance-Modelle mit SED- oder FIPS-NVMe-SSDs, die mit dem StorageGRID Appliance Installer und Grid Manager verwaltet werden "StorageGRID Laufwerkverschlüsselung aktivieren und konfigurieren".
- Für Appliances ohne SED-, FDE- oder FIPS-Laufwerke kann ein Key Management Server (KMS) verwendet werden, um "StorageGRID Softwareknotenverschlüsselung aktivieren und konfigurieren".

Verwandte Informationen

"Erfahren Sie mehr über die Laufwerkssicherheit im SANtricity System Manager"

Härtungsrichtlinien für TLS und SSH in StorageGRID

Sie sollten den SSH-Zugriff kontrollieren, die Standard-TLS-Zertifikate ersetzen und die geeignete Sicherheitsrichtlinie für TLS- und SSH-Verbindungen auswählen.

Härtungsrichtlinien für Zertifikate

Die während der Installation erstellten Standardzertifikate sollten durch eigene benutzerdefinierte Zertifikate ersetzt werden.

Für viele Organisationen entspricht das selbstsignierte digitale Zertifikat für den StorageGRID-Webzugriff nicht ihren Informationssicherheitsrichtlinien. Auf Produktivsystemen ist ein von einer Zertifizierungsstelle signiertes

digitales Zertifikat zur Authentifizierung von StorageGRID zu installieren.

Insbesondere sollten benutzerdefinierte Serverzertifikate anstelle dieser Standardzertifikate verwendet werden:

- **Management Interface-Zertifikat**: Dient zur Absicherung des Zugriffs auf den Grid Manager, den Tenant Manager, die Grid Management API und die Tenant Management API.
- **S3 API-Zertifikat**: Dient zur Sicherung des Zugriffs auf Storage Nodes und Gateway Nodes, die von S3-Clientanwendungen zum Hoch- und Herunterladen von Objektdaten verwendet werden.

Weitere Details und Anweisungen sind unter "Sicherheitszertifikate verwalten" zu finden.

> StorageGRID verwaltet die für Load-Balancer-Endpunkte verwendeten Zertifikate separat. Zur Konfiguration von Load-Balancer-Zertifikaten siehe "Load Balancer-Endpunkte konfigurieren".

Bei der Verwendung benutzerdefinierter Serverzertifikate gelten folgende Richtlinien:

- Zertifikate sollten ein *`subjectAltName`* enthalten, das mit den DNS-Einträgen für StorageGRID übereinstimmt. Einzelheiten finden sich in Abschnitt 4.2.1.6, „Subject Alternative Name“, in "RFC 5280: PKIX-Zertifikat und CRL-Profil".
- Wenn möglich, sollte auf die Verwendung von Wildcard-Zertifikaten verzichtet werden. Eine Ausnahme von dieser Richtlinie ist das Zertifikat für einen S3 Virtual Hosted Style Endpoint, bei dem die Verwendung eines Wildcard-Zertifikats erforderlich ist, wenn die Bucket-Namen nicht im Voraus bekannt sind.
- Wenn in Zertifikaten Wildcards verwendet werden müssen, sollten zusätzliche Maßnahmen ergriffen werden, um die Risiken zu minimieren. Ein Wildcard-Muster wie `*.s3.example.com` sollte verwendet werden, und das `s3.example.com` Suffix sollte für andere Anwendungen nicht verwendet werden. Dieses Muster funktioniert auch mit pfadbasierendem S3-Zugriff, wie `dc1-s1.s3.example.com/mybucket`.
- Die Gültigkeitsdauer der Zertifikate sollte kurz sein (zum Beispiel 2 Monate), und die Grid Management API kann zur Automatisierung der Zertifikatsrotation verwendet werden. Dies ist besonders wichtig für Wildcard-Zertifikate.

Darüber hinaus wird empfohlen, dass Clients bei der Kommunikation mit StorageGRID eine strikte Hostnamenprüfung verwenden.

Härtungsrichtlinien für TLS- und SSH-Richtlinien

Sie können eine Sicherheitsrichtlinie auswählen, um festzulegen, welche Protokolle und Verschlüsselungsverfahren 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 während der Übertragung verschlüsseln. Als bewährte Methode sollten Verschlüsselungsoptionen deaktiviert werden, die für die Anwendungskompatibilität nicht erforderlich sind. Die Standardrichtlinie Modern sollte verwendet werden, es sei denn, das System muss Common Criteria-konform, FIPS 140-2-konform sein oder es müssen andere Verschlüsselungsverfahren verwendet werden.

Siehe "TLS- und SSH-Richtlinie verwalten" für Details und Anweisungen.

Externen SSH-Zugriff verwalten

Zur Erhöhung der Systemsicherheit ist der externe SSH-Zugriff standardmäßig blockiert. SSH-Zugriff sollte nur aktiviert werden, wenn Aufgaben ausgeführt werden müssen, die einen eingehenden SSH-Zugriff erfordern, wie beispielsweise zur Fehlerbehebung. Weitere Informationen und Anweisungen sind unter "Externen SSH-

Zugriff verwalten" zu finden.

Härtungsrichtlinien für Protokolle, Passwörter und Prüfmeldungen in StorageGRID

Zusätzlich zur Einhaltung der Härtungsrichtlinien für StorageGRID Netzwerke und StorageGRID Knoten sollten auch die Härtungsrichtlinien für andere Bereiche des StorageGRID Systems berücksichtigt werden.

Temporäres Installationspasswort

Um das StorageGRID System während der Installation zu schützen, kann auf der Seite für temporäre Installationspasswörter in der StorageGRID Installations-UI oder in der Installations-API ein Passwort festgelegt werden. Ist dieses Passwort gesetzt, gilt es für alle Methoden zur Installation von StorageGRID, einschließlich der Benutzeroberfläche, der Installations-API und `configure-storagegrid.py` Skript.

Weitere Informationen sind unter folgendem Link verfügbar:

- "StorageGRID auf softwarebasierten Knoten installieren"
- "StorageGRID Appliance installieren"

Protokolle und Prüfmeldungen

StorageGRID-Protokolle und Audit-Meldungen sollten stets auf sichere Weise geschützt werden. StorageGRID-Protokolle und Audit-Meldungen liefern aus Sicht von Support und Systemverfügbarkeit unschätzbare Informationen. Zudem sind die in StorageGRID-Protokollen und Audit-Meldungen enthaltenen Informationen und Details in der Regel sensibler Natur.

StorageGRID so konfigurieren, dass Sicherheitsereignisse an einen externen Syslog-Server gesendet werden. Bei Verwendung des Syslog-Exports sollten TLS und RELP/TLS als Transportprotokolle ausgewählt werden.

Weitere Informationen zu StorageGRID-Protokollen sind in "Referenz zu Protokolldateien" zu finden. Weitere Informationen zu StorageGRID Auditmeldungen sind in "Audit-Meldungen" zu finden.

NetApp AutoSupport

Die AutoSupport-Funktion von StorageGRID ermöglicht die proaktive Überwachung des Systemzustands und das automatische Senden von Paketen an die NetApp Support Site, das interne Support-Team Ihres Unternehmens oder einen Support-Partner. Standardmäßig ist das Senden von AutoSupport-Paketen an NetApp aktiviert, wenn StorageGRID zum ersten Mal konfiguriert wird.

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

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

Cross-Origin Resource Sharing (CORS)

Es besteht die Möglichkeit, Cross-Origin Resource Sharing (CORS) für einen S3-Bucket zu konfigurieren, wenn dieser Bucket und die darin enthaltenen Objekte für Webanwendungen in anderen Domänen zugänglich sein sollen. Im Allgemeinen sollte CORS nur aktiviert werden, wenn es erforderlich ist. Wenn CORS erforderlich ist, sollte die Nutzung auf vertrauenswürdige Ursprünge beschränkt werden.

Siehe die Schritte für "CORS-Konfiguration für Buckets und Objekte".

Externe Sicherheitsgeräte

Eine umfassende Hardening-Lösung muss Sicherheitsmechanismen außerhalb von StorageGRID berücksichtigen. Der Einsatz zusätzlicher Infrastrukturgeräte zur Filterung und Begrenzung des Zugriffs auf StorageGRID ist eine effektive Methode, um eine strenge Sicherheitsposition zu etablieren und aufrechtzuerhalten. Zu diesen externen Sicherheitsgeräten gehören Firewalls, Intrusion Prevention Systeme (IPSs) und andere Sicherheitsgeräte.

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

Ransomware-Abwehr

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