Systemhärtung

StorageGRID

NetApp
October 03, 2025

Inhalt

Systemhärtung

Informieren Sie sich über Systemeinstellungen, Best Practices und Empfehlungen zum Schutz eines StorageGRID-Systems vor Sicherheitsbedrohungen.

- "Sicherung eines StorageGRID Systems"
- "Hardening-Richtlinien für Software Upgrades"
- "Hardening Guidelines for StorageGRID Networks"
- "Hardening-Richtlinien für StorageGRID-Knoten"
- "Härtungsrichtlinien für Serverzertifikate"
- "Andere Hinweise zur Verhärtung"]

Sicherung eines StorageGRID Systems

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 *NetApp Richtlinie zur Handhabung von Schwachstellen*. Gemeldete Schwachstellen werden gemäß dem Prozess der Reaktion auf Produktsicherheitsvorfälle überprüft und behoben.

Allgemeine Überlegungen zur Erhöhung der Sicherheit eines StorageGRID-Systems

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 eines Docker Containers 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.

Verwandte Informationen

"Richtlinie Zum Umgang Mit Schwachstellen"

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 Versionen von StorageGRID oft Funktionen zur Erhöhung der Sicherheit, die in früheren Versionen nicht enthalten sind.

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 auf der StorageGRID Software Download-Seite herunterladen. Schritt-für-Schritt-Anleitungen zum Aktualisieren der StorageGRID-Software finden Sie in den Anweisungen zum Aktualisieren von StorageGRID. Anweisungen zum Anwenden eines Hotfix finden Sie in den Anweisungen zur Wiederherstellung und Wartung.

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.

Mit dem NetApp Interoperabilitäts-Matrix-Tool können Sie eine Liste der unterstützten Versionen abrufen.

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.

Mit dem NetApp Interoperabilitäts-Matrix-Tool können Sie eine Liste der unterstützten Versionen abrufen.

Upgrade 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.

Mit dem NetApp Interoperabilitäts-Matrix-Tool können Sie eine Liste der unterstützten Versionen abrufen.

Verwandte Informationen

"NetApp Downloads: StorageGRID"

"Software-Upgrade"

"Verwalten Sie erholen"

"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.

Richtlinien für das Grid-Netzwerk

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 das Admin-Netzwerk

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. Informationen zu Ihrer Plattform finden Sie in der Liste der internen Ports im Installationshandbuch.
- 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 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. Informationen zu Ihrer Plattform finden Sie in

der Liste der internen Ports im Installationshandbuch.

- Eingehende Clientdatenverkehr nur an explizit konfigurierten Endpunkten akzeptieren. Informationen zum Verwalten von nicht vertrauenswürdigen Clientnetzwerken finden Sie in den Anweisungen zur Verwaltung von StorageGRID.

Verwandte Informationen

"Netzwerkrichtlinien"

"Gittergrundierung"

"StorageGRID verwalten"

"Installieren Sie Red hat Enterprise Linux oder CentOS"

"Installieren Sie Ubuntu oder Debian"

"VMware installieren"

Hardening-Richtlinien für StorageGRID-Knoten

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

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.

Bei Nodes, die auf VMware Plattformen und StorageGRID Appliances ausgeführt werden, kommt eine interne Firewall zum Einsatz, die automatisch gemanagt wird. Diese interne Firewall bietet zwar eine zusätzliche Schutzschicht gegen häufig vorgängige Bedrohungen, sie macht aber keine externe Firewall erforderlich.

Eine Liste aller von StorageGRID verwendeten internen und externen Ports finden Sie im Installationsleitfaden für Ihre Plattform.

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. Gehen Sie nicht davon aus, dass der Hypervisor-Schutz Malware den Zugriff auf StorageGRID geschützte Daten verhindert, wenn sowohl StorageGRID als auch die Malware auf derselben physischen Hardware vorhanden sind. So nutzen beispielsweise die Meltdown- und Specter-Angriffe kritische Schwachstellen in modernen Prozessoren und ermöglichen Programmen, Daten im Arbeitsspeicher auf demselben Computer zu stehlen.

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 Client-Zugriff auf die Audit-Shares für CIFS oder NFS zu konfigurieren, blockieren oder deaktivieren Sie den Zugriff auf diese Dienste.

Schutz von Nodes während der Installation

Erlauben Sie nicht, nicht vertrauenswürdigen Benutzern über das Netzwerk auf StorageGRID-Knoten zuzugreifen, wenn die Knoten installiert werden. Nodes sind erst dann vollständig gesichert, 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 Mandanten nicht vertrauenswürdig sind, dürfen sie keinen direkten Zugriff auf den Mandantenmanager oder die Mandantenmanagement-API haben. Verwenden Sie stattdessen ein Mandantenportal oder ein externes Mandantenmanagement-System, das mit der Mandantenmanagement-API interagiert.
- Optional können Sie einen Admin-Proxy verwenden, um mehr Kontrolle über die AutoSupport Kommunikation von Admin Nodes zur NetApp Unterstützung zu erhalten. Lesen Sie die Schritte zum Erstellen eines Admin-Proxys in den Anweisungen zur Administration von StorageGRID.
- 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 zum Verwalten 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.

- Aktivieren Sie keine Outbound-Services für nicht vertrauenswürdige Mandanten. Wenn Sie beispielsweise das Konto für einen nicht vertrauenswürdigen Mandanten erstellen, dürfen Sie dem Mandanten nicht erlauben, seine eigene Identitätsquelle zu verwenden, und lassen Sie die Nutzung von Plattformdiensten nicht zu. Informationen zum Erstellen eines Mandantenkontos finden Sie in den Anweisungen für die Administration von StorageGRID.
- Verwenden Sie einen Drittanbieter-Load-Balancer für nicht vertrauenswürdigen Client-Datenverkehr. Der Lastausgleich von Drittanbietern bietet mehr Kontrolle und zusätzlichen Schutz vor Angriffen.
- Optional können Sie einen Storage Proxy verwenden, um mehr Kontrolle über Cloud Storage Pools und die Kommunikation von Plattform-Services von Storage Nodes zu externen Services zu erhalten. Lesen

Sie die Schritte zum Erstellen eines Speicher-Proxy in den Anweisungen für die Administration von StorageGRID.

- Optional können Sie über das Client-Netzwerk eine Verbindung zu externen Diensten herstellen. Wählen Sie dann **Konfiguration** > **Netzwerkeinstellungen** > **nicht vertrauenswürdiges Clientnetzwerk** aus, und geben Sie an, dass das Client-Netzwerk auf dem Speicherknoten 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 anstatt den CLB-Service auf Gateway-Nodes zu verwenden. Lesen Sie in den Anweisungen zur Administration von StorageGRID die Schritte zum Verwalten des Lastausgleichs.

  Der CLB-Service ist veraltet.

- 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 **Konfiguration** > **Netzwerkeinstellungen** > **nicht vertrauenswürdiges Clientnetzwerk** aus, und geben Sie an, dass das Client-Netzwerk auf dem Gateway-Knoten 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.

- Wenn der Storage Controller in der Appliance Laufwerke mit FDE- oder FIPS-Laufwerken umfasst und die Laufwerkssicherheitsfunktion aktiviert ist, konfigurieren Sie die Schlüssel zur Laufwerksicherheit mithilfe von SANtricity.
- Bei Appliances ohne FDE- oder FIPS-Laufwerke ermöglicht die Node-Verschlüsselung mithilfe eines Key Management Servers (KMS).

Hinweise zur Installation und Wartung Ihrer StorageGRID Hardware-Appliance finden Sie in der Installations- und Wartungsanleitung.

Verwandte Informationen

"Installieren Sie Red hat Enterprise Linux oder CentOS"

"Installieren Sie Ubuntu oder Debian"

"VMware installieren"

"StorageGRID verwalten"

"Verwenden Sie ein Mandantenkonto"

"SG100 SG1000 Services-Appliances"

"SG5600 Storage Appliances"

"SG5700 Storage-Appliances"

"SG6000 Storage-Appliances"

Härtungsrichtlinien für Serverzertifikate

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:

- **Management Interface Server Certificate**: Wird verwendet, um den Zugriff auf den Grid Manager, den Tenant Manager, die Grid Management API und die Tenant Management API zu sichern.
- **Object Storage API Service Endpoints Serverzertifikat**: Wird verwendet, um den Zugriff auf Storage-Nodes und Gateway-Nodes zu sichern, die S3- und Swift-Client-Anwendungen zum Hochladen und Herunterladen von Objektdaten verwenden.

> StorageGRID managt die für Load Balancer-Endpunkte verwendeten Zertifikate separat. Informationen zum Konfigurieren von Load Balancer-Zertifikaten finden Sie in den Schritten zum Konfigurieren von Load Balancer-Endpunkten in den Anweisungen zur Verwaltung von StorageGRID.

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, „SAlternative Name des Subject“ in "RFC 5280: PKIX-Zertifikat und CRL-Profil".
- Wenn möglich, vermeiden Sie die Verwendung von Platzhalterzertifikaten. Eine Ausnahme von dieser Richtlinie ist das Zertifikat für einen virtualisierten S3-Endpunkt im gehosteten Stil. Dazu ist die Verwendung eines Platzhalters erforderlich, wenn Bucket-Namen vorab nicht 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.

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.

Weitere Informationen zu StorageGRID-Protokollen finden Sie in den Anweisungen zum Monitoring und zur Fehlerbehebung. Weitere Informationen zu StorageGRID-Audit-Meldungen finden Sie in den Anweisungen für Audit-Meldungen.

NetApp AutoSupport

Mit der AutoSupport Funktion von StorageGRID können Sie proaktiv den Systemzustand überwachen und automatisch Nachrichten und Details an den technischen Support von NetApp, das interne Support-Team Ihres Unternehmens oder einen Support-Partner senden. Standardmäßig sind AutoSupport Meldungen an den technischen Support von NetApp aktiviert, wenn StorageGRID zum ersten Mal konfiguriert ist.

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 sensible Natur von AutoSupport Meldungen empfiehlt NetApp dringend, HTTPS als Standard-Transportprotokoll für das Senden von AutoSupport Meldungen an die NetApp Unterstützung zu verwenden.

Optional können Sie einen Admin-Proxy für mehr Kontrolle über die AutoSupport Kommunikation von Admin Nodes zum technischen Support von NetApp konfigurieren. Lesen Sie die Schritte zum Erstellen eines Admin-Proxys in den Anweisungen zur Administration von StorageGRID.

Cross-Origin Resource Sharing (CORS)

Die Cross-Origin Resource Sharing (CORS) kann für einen S3-Bucket konfiguriert werden, wenn für Web-Applikationen in anderen Domänen auf diesen Bucket und Objekte in diesem Bucket zugegriffen werden soll. Aktivieren Sie CORS im Allgemeinen nur, wenn dies erforderlich ist. Wenn CORS erforderlich ist, beschränken Sie es auf vertrauenswürdige Herkunft.

Lesen Sie die Schritte zum Konfigurieren der Cross-Origin Resource Sharing (CORS) in der Anleitung zur Verwendung von Mandantenkonten.

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.

Verwandte Informationen

"Monitor Fehlerbehebung"

"Prüfung von Audit-Protokollen"

"Verwenden Sie ein Mandantenkonto"

"StorageGRID verwalten"