Protezione avanzata del sistema

StorageGRID

NetApp
September 04, 2024

Sommario

Protezione avanzata del sistema

Protezione avanzata del sistema: Panoramica

La protezione avanzata del sistema è il processo che consente di eliminare il maggior numero possibile di rischi per la sicurezza da un sistema StorageGRID.

Questo documento fornisce una panoramica delle linee guida per la protezione avanzata specifiche di StorageGRID. Queste linee guida integrano le Best practice standard di settore per la protezione avanzata dei sistemi. Ad esempio, queste linee guida presuppongono l'utilizzo di password complesse per StorageGRID, l'utilizzo di HTTPS invece di HTTP e l'attivazione dell'autenticazione basata su certificato, se disponibile.

Durante l'installazione e la configurazione di StorageGRID, è possibile utilizzare queste linee guida per soddisfare qualsiasi obiettivo di sicurezza prescritto in termini di riservatezza, integrità e disponibilità del sistema informativo.

StorageGRID segue la *policy NetApp per la gestione delle vulnerabilità*. Le vulnerabilità segnalate vengono verificate e risolte in base al processo di risposta agli incidenti di sicurezza del prodotto.

Considerazioni generali per la protezione avanzata dei sistemi StorageGRID

Quando si esegue la protezione avanzata di un sistema StorageGRID, è necessario considerare quanto segue:

- Quale delle tre reti StorageGRID è stata implementata? Tutti i sistemi StorageGRID devono utilizzare la rete griglia, ma è possibile utilizzare anche la rete di amministrazione, la rete client o entrambi. Ogni rete ha considerazioni di sicurezza diverse.
- Il tipo di piattaforme utilizzate per i singoli nodi nel sistema StorageGRID. I nodi StorageGRID possono essere implementati su macchine virtuali VMware, all'interno di un motore di container su host Linux o come appliance hardware dedicate. Ogni tipo di piattaforma dispone di un proprio set di Best practice per la protezione avanzata.
- Quanto sono affidabili gli account tenant. Se sei un provider di servizi con account tenant non attendibili, avrai problemi di sicurezza diversi rispetto all'utilizzo di tenant interni affidabili.
- Quali requisiti e convenzioni di sicurezza sono seguiti dalla tua organizzazione. Potrebbe essere necessario rispettare requisiti normativi o aziendali specifici.

Informazioni correlate

"Policy per la gestione delle vulnerabilità"

Linee guida per la protezione avanzata degli aggiornamenti software

Per difenderti dagli attacchi, devi tenere aggiornato il tuo sistema StorageGRID e i servizi correlati.

Aggiornamenti al software StorageGRID

Se possibile, è necessario aggiornare il software StorageGRID alla versione principale più recente o alla versione principale precedente. Mantenere aggiornato StorageGRID aiuta a ridurre il tempo di attivazione delle

vulnerabilità note e l'area complessiva della superficie di attacco. Inoltre, le versioni più recenti di StorageGRID contengono spesso funzionalità di protezione avanzata che non sono incluse nelle versioni precedenti.

Quando è necessaria una correzione rapida, NetApp assegna la priorità alla creazione di aggiornamenti per le release più recenti. Alcune patch potrebbero non essere compatibili con le release precedenti.

Per scaricare le versioni più recenti di StorageGRID e gli aggiornamenti rapidi, accedere alla pagina di download del software StorageGRID. Per istruzioni dettagliate sull'aggiornamento del software StorageGRID, consultare le istruzioni per l'aggiornamento di StorageGRID. Per istruzioni sull'applicazione di una correzione rapida, consultare le istruzioni di ripristino e manutenzione.

Aggiornamenti a servizi esterni

I servizi esterni possono presentare vulnerabilità che influiscono indirettamente su StorageGRID. Devi assicurarti che i servizi da cui dipende StorageGRID siano sempre aggiornati. Questi servizi includono LDAP, KMS (o server KMIP), DNS e NTP.

Utilizza NetApp Interoperability Matrix Tool per ottenere un elenco delle versioni supportate.

Aggiornamenti agli hypervisor

Se i nodi StorageGRID sono in esecuzione su VMware o su un altro hypervisor, è necessario assicurarsi che il software e il firmware dell'hypervisor siano aggiornati.

Utilizza NetApp Interoperability Matrix Tool per ottenere un elenco delle versioni supportate.

Upgrade a nodi Linux

Se i nodi StorageGRID utilizzano piattaforme host Linux, è necessario assicurarsi che gli aggiornamenti di sicurezza e del kernel siano applicati al sistema operativo host. Inoltre, è necessario applicare gli aggiornamenti del firmware all'hardware vulnerabile quando questi aggiornamenti diventano disponibili.

Utilizza NetApp Interoperability Matrix Tool per ottenere un elenco delle versioni supportate.

Informazioni correlate

"Download NetApp: StorageGRID"

Aggiornare il software

Ripristino e manutenzione

"Tool di matrice di interoperabilità NetApp"

Linee guida per la protezione avanzata delle reti StorageGRID

Il sistema StorageGRID supporta fino a tre interfacce di rete per nodo di rete, consentendo di configurare la rete per ogni singolo nodo di rete in modo che corrisponda ai requisiti di sicurezza e accesso.

Linee guida per Grid Network

È necessario configurare una rete griglia per tutto il traffico StorageGRID interno. Tutti i nodi Grid si trovano sulla rete Grid e devono essere in grado di comunicare con tutti gli altri nodi.

Durante la configurazione della rete Grid, attenersi alle seguenti linee guida:

- Assicurarsi che la rete sia protetta da client non attendibili, ad esempio quelli su Internet aperto.
- Se possibile, utilizzare Grid Network esclusivamente per il traffico interno. Sia la rete di amministrazione che la rete client presentano ulteriori restrizioni firewall che bloccano il traffico esterno verso i servizi interni. È supportato l'utilizzo di Grid Network per il traffico client esterno, ma questo tipo di utilizzo offre meno livelli di protezione.
- Se l'implementazione di StorageGRID si estende su più data center, utilizzare una rete privata virtuale (VPN) o equivalente sulla rete grid per fornire una protezione aggiuntiva per il traffico interno.
- Alcune procedure di manutenzione richiedono l'accesso Secure shell (SSH) sulla porta 22 tra il nodo di amministrazione primario e tutti gli altri nodi della griglia. Utilizzare un firewall esterno per limitare l'accesso SSH ai client attendibili.

Linee guida per la rete amministrativa

La rete di amministrazione viene generalmente utilizzata per le attività amministrative (dipendenti attendibili che utilizzano Grid Manager o SSH) e per la comunicazione con altri servizi attendibili come LDAP, DNS, NTP o KMS (o server KMIP). Tuttavia, StorageGRID non applica questo utilizzo internamente.

Se si utilizza la rete di amministrazione, attenersi alle seguenti linee guida:

- Bloccare tutte le porte di traffico interne sulla rete di amministrazione. Consultare l'elenco delle porte interne nella guida all'installazione della piattaforma in uso.
- Se i client non attendibili possono accedere alla rete di amministrazione, bloccare l'accesso a StorageGRID sulla rete di amministrazione con un firewall esterno.

Linee guida per la rete client

La rete client viene generalmente utilizzata per i tenant e per le comunicazioni con servizi esterni, come il servizio di replica CloudMirror o un altro servizio della piattaforma. Tuttavia, StorageGRID non applica questo utilizzo internamente.

Se si utilizza la rete client, attenersi alle seguenti linee guida:

- Bloccare tutte le porte di traffico interne sulla rete client. Consultare l'elenco delle porte interne nella guida all'installazione della piattaforma in uso.
- Accettare il traffico client in entrata solo su endpoint configurati esplicitamente. Vedere Gestione di reti client non attendibili.

Informazioni correlate

Linee guida per il networking

Primer griglia

Amministrare StorageGRID

Installare Red Hat Enterprise Linux o CentOS

Installare Ubuntu o Debian

Installare VMware

Linee guida per la protezione avanzata dei nodi StorageGRID

I nodi StorageGRID possono essere implementati su macchine virtuali VMware, all'interno di un motore di container su host Linux o come appliance hardware dedicate. Ogni tipo di piattaforma e ogni tipo di nodo dispone di un proprio set di Best practice per la protezione avanzata.

Configurazione del firewall

Nell'ambito del processo di protezione avanzata del sistema, è necessario rivedere le configurazioni dei firewall esterni e modificarle in modo che il traffico venga accettato solo dagli indirizzi IP e dalle porte da cui è strettamente necessario.

StorageGRID utilizza un firewall interno che viene gestito automaticamente. Sebbene questo firewall interno offra un ulteriore livello di protezione contro alcune minacce comuni, non elimina la necessità di un firewall esterno.

Per un elenco di tutte le porte interne ed esterne utilizzate da StorageGRID, consultare la guida all'installazione della piattaforma.

Virtualizzazione, container e hardware condiviso

Per tutti i nodi StorageGRID, evitare di eseguire StorageGRID sullo stesso hardware fisico del software non attendibile. Non presupporre che le protezioni dell'hypervisor impediscano al malware di accedere ai dati protetti da StorageGRID se StorageGRID e il malware esistono sullo stesso hardware fisico. Ad esempio, gli attacchi Meltdown e Spectre sfruttano le vulnerabilità critiche dei processori moderni e consentono ai programmi di rubare dati in memoria sullo stesso computer.

Disattivare i servizi inutilizzati

Per tutti i nodi StorageGRID, è necessario disattivare o bloccare l'accesso ai servizi inutilizzati. Ad esempio, se non si intende configurare l'accesso client alle condivisioni di controllo per CIFS o NFS, bloccare o disattivare l'accesso a questi servizi.

Proteggere i nodi durante l'installazione

Non consentire agli utenti non attendibili di accedere ai nodi StorageGRID sulla rete durante l'installazione dei nodi. I nodi non sono completamente sicuri fino a quando non si sono Uniti alla griglia.

Linee guida per i nodi di amministrazione

I nodi di amministrazione forniscono servizi di gestione quali configurazione, monitoraggio e registrazione del sistema. Quando si accede a Grid Manager o al tenant Manager, si sta effettuando la connessione a un nodo amministratore.

Seguire queste linee guida per proteggere i nodi di amministrazione nel sistema StorageGRID:

- Proteggere tutti i nodi di amministrazione da client non attendibili, ad esempio quelli su Internet aperto. Assicurarsi che nessun client non attendibile possa accedere a qualsiasi nodo Admin sulla rete Grid, sulla rete amministrativa o sulla rete client.
- I gruppi StorageGRID controllano l'accesso alle funzioni di gestione griglia e di gestione tenant. Concedere a ciascun gruppo di utenti le autorizzazioni minime richieste per il proprio ruolo e utilizzare la modalità di accesso in sola lettura per impedire agli utenti di modificare la configurazione.
- Quando si utilizzano gli endpoint del bilanciamento del carico StorageGRID, utilizzare i nodi gateway invece dei nodi di amministrazione per il traffico client non attendibile.
- Se si dispone di tenant non attendibili, non consentire loro di accedere direttamente al tenant Manager o all'API di gestione del tenant. I tenant non attendibili devono invece utilizzare un portale tenant o un sistema di gestione tenant esterno, che interagisce con l'API di gestione tenant.
- Se lo si desidera, utilizzare un proxy amministratore per un maggiore controllo sulle comunicazioni AutoSupport dai nodi di amministrazione al supporto NetApp. Consultare la procedura per la creazione di un proxy amministratore nelle istruzioni per l'amministrazione di StorageGRID.
- Facoltativamente, utilizzare le porte limitate 8443 e 9443 per separare le comunicazioni di Grid Manager e Tenant Manager. Bloccare la porta condivisa 443 e limitare le richieste del tenant alla porta 9443 per una protezione aggiuntiva.
- Facoltativamente, utilizzare nodi di amministrazione separati per gli amministratori di grid e gli utenti del tenant.

Per ulteriori informazioni, consultare le istruzioni per l'amministrazione di StorageGRID.

Linee guida per i nodi di storage

I nodi di storage gestiscono e memorizzano i dati e i metadati degli oggetti. Seguire queste linee guida per proteggere i nodi di storage nel sistema StorageGRID.

- Non consentire ai client non attendibili di connettersi direttamente ai nodi di storage. Utilizzare un endpoint di bilanciamento del carico servito da un nodo gateway o da un bilanciamento del carico di terze parti.
- Non abilitare i servizi in uscita per tenant non attendibili. Ad esempio, quando si crea l'account per un tenant non attendibile, non consentire al tenant di utilizzare la propria origine di identità e non consentire l'utilizzo dei servizi della piattaforma. Consultare la procedura per la creazione di un account tenant nelle istruzioni per l'amministrazione di StorageGRID.
- Utilizzare un bilanciamento del carico di terze parti per il traffico client non attendibile. Il bilanciamento del carico di terze parti offre un maggiore controllo e ulteriori livelli di protezione dagli attacchi.
- Se lo si desidera, utilizzare un proxy dello storage per un maggiore controllo sui pool di storage cloud e sulle comunicazioni dei servizi della piattaforma dai nodi di storage ai servizi esterni. Consultare la procedura per la creazione di un proxy di storage nelle istruzioni per l'amministrazione di StorageGRID.
- Se lo si desidera, connettersi a servizi esterni utilizzando la rete client. Quindi, selezionare **CONFIGURATION** > **Network** > **Untrusted Client Networks** e indicare che la rete client sul nodo di storage non è attendibile. Il nodo di storage non accetta più alcun traffico in entrata sulla rete client, ma continua a consentire le richieste in uscita per Platform Services.

Linee guida per i nodi gateway

I nodi gateway forniscono un'interfaccia opzionale per il bilanciamento del carico che le applicazioni client possono utilizzare per connettersi a StorageGRID. Attenersi alle seguenti linee guida per proteggere i nodi gateway nel sistema StorageGRID:

- Configurare e utilizzare gli endpoint del bilanciamento del carico invece di utilizzare il servizio CLB sui nodi gateway. Consultare la procedura per la gestione del bilanciamento del carico nelle istruzioni per l'amministrazione di StorageGRID.

  Il servizio CLB è obsoleto.

- Utilizzare un bilanciamento del carico di terze parti tra il client e il nodo gateway o i nodi di storage per il traffico client non attendibile. Il bilanciamento del carico di terze parti offre un maggiore controllo e ulteriori livelli di protezione dagli attacchi. Se si utilizza un bilanciamento del carico di terze parti, il traffico di rete può comunque essere configurato in modo opzionale per passare attraverso un endpoint interno di bilanciamento del carico o essere inviato direttamente ai nodi di storage.
- Se si utilizzano endpoint di bilanciamento del carico, è possibile che i client si connettano tramite la rete client. Quindi, selezionare **CONFIGURATION** > **Network** > **Untrusted Client Networks** e indicare che la rete client sul nodo gateway non è attendibile. Il nodo gateway accetta solo il traffico in entrata sulle porte esplicitamente configurate come endpoint del bilanciamento del carico.

Linee guida per i nodi dell'appliance hardware

Le appliance hardware StorageGRID sono progettate appositamente per l'utilizzo in un sistema StorageGRID. Alcune appliance possono essere utilizzate come nodi di storage. Altri appliance possono essere utilizzati come nodi di amministrazione o nodi gateway. È possibile combinare nodi appliance con nodi basati su software o implementare grid all-appliance completamente progettati.

Segui queste linee guida per proteggere i nodi dell'appliance hardware nel tuo sistema StorageGRID:

- Se l'appliance utilizza Gestione di sistema di SANtricity per la gestione del controller di storage, impedire ai client non attendibili di accedere a Gestione di sistema di SANtricity tramite la rete.
- Se l'appliance dispone di un BMC (Baseboard Management Controller), tenere presente che la porta di gestione BMC consente un accesso hardware di basso livello. Collegare la porta di gestione BMC solo a una rete di gestione interna sicura e affidabile. Se tale rete non è disponibile, lasciare la porta di gestione BMC disconnessa o bloccata, a meno che non venga richiesta una connessione BMC dal supporto tecnico.
- Se l'appliance supporta la gestione remota dell'hardware del controller su Ethernet utilizzando lo standard IPMI (Intelligent Platform Management Interface), bloccare il traffico non attendibile sulla porta 623.
- Se lo storage controller dell'appliance include dischi FDE o FIPS e la funzione di protezione del disco è attivata, utilizzare SANtricity per configurare le chiavi di protezione del disco.
- Per le appliance senza dischi FDE o FIPS, abilitare la crittografia dei nodi utilizzando un server di gestione delle chiavi (KMS).

Consultare le istruzioni di installazione e manutenzione dell'appliance hardware StorageGRID.

Informazioni correlate

- Installare Red Hat Enterprise Linux o CentOS
- Installare Ubuntu o Debian
- Installare VMware
- Amministrare StorageGRID
- Utilizzare un account tenant
- Appliance di servizi SG100 e SG1000

- Appliance di storage SG5600
- Appliance di storage SG5700
- Appliance di storage SG6000

Linee guida per la protezione avanzata dei certificati server

È necessario sostituire i certificati predefiniti creati durante l'installazione con certificati personalizzati.

Per molte organizzazioni, il certificato digitale autofirmato per l'accesso Web a StorageGRID non è conforme alle policy di sicurezza delle informazioni. Nei sistemi di produzione, è necessario installare un certificato digitale con firma CA da utilizzare per l'autenticazione di StorageGRID.

In particolare, è necessario utilizzare certificati server personalizzati anziché i seguenti certificati predefiniti:

- **Certificato dell'interfaccia di gestione**: Utilizzato per proteggere l'accesso a Grid Manager, Tenant Manager, Grid Management API e Tenant Management API.
- **Certificato API S3 e Swift**: Utilizzato per proteggere l'accesso ai nodi di storage e ai nodi gateway, utilizzati dalle applicazioni client S3 e Swift per caricare e scaricare i dati degli oggetti.

> StorageGRID gestisce separatamente i certificati utilizzati per gli endpoint del bilanciamento del carico. Per configurare i certificati di bilanciamento del carico, vedere i passaggi per la configurazione degli endpoint di bilanciamento del carico nelle istruzioni per l'amministrazione di StorageGRID.

Quando si utilizzano certificati server personalizzati, attenersi alle seguenti linee guida:

- I certificati devono avere un *`subjectAltName`* Che corrisponde alle voci DNS per StorageGRID. Per ulteriori informazioni, vedere la sezione 4.2.1.6, "Subject alternative Name," in "RFC 5280: Certificato PKIX e profilo CRL".
- Se possibile, evitare l'utilizzo di certificati con caratteri jolly. Un'eccezione a questa linea guida è il certificato per un endpoint di stile host virtuale S3, che richiede l'utilizzo di un carattere jolly se i nomi dei bucket non sono noti in anticipo.
- Quando è necessario utilizzare i caratteri jolly nei certificati, è necessario adottare ulteriori misure per ridurre i rischi. Utilizzare un modello con caratteri jolly come `*.s3.example.com`e non utilizzare `s3.example.com` suffisso per altre applicazioni. Questo modello funziona anche con l'accesso S3 di tipo path, ad esempio `dc1-s1.s3.example.com/mybucket`.
- Impostare i tempi di scadenza del certificato su brevi (ad esempio, 2 mesi) e utilizzare l'API Grid Management per automatizzare la rotazione del certificato. Ciò è particolarmente importante per i certificati con caratteri jolly.

Inoltre, i client devono utilizzare un rigoroso controllo del nome host quando comunicano con StorageGRID.

Altre linee guida per la protezione avanzata

Oltre a seguire le linee guida per la protezione avanzata per reti e nodi StorageGRID, è necessario seguire le linee guida per la protezione avanzata per altre aree del sistema StorageGRID.

Registri e messaggi di audit

Proteggere sempre i log StorageGRID e l'output dei messaggi di controllo in modo sicuro. I registri e i messaggi di audit di StorageGRID forniscono informazioni preziose dal punto di vista del supporto e della disponibilità del sistema. Inoltre, le informazioni e i dettagli contenuti nei registri StorageGRID e nell'output dei messaggi di audit sono generalmente di natura sensibile.

Configurare StorageGRID per inviare eventi di sicurezza a un server syslog esterno. Se si utilizza l'esportazione syslog, selezionare TLS e RELP/TLS per i protocolli di trasporto.

Per ulteriori informazioni sui registri StorageGRID, consultare le istruzioni per il monitoraggio e la risoluzione dei problemi. Per ulteriori informazioni sui messaggi di audit di StorageGRID, consultare le istruzioni per i messaggi di audit.

NetApp AutoSupport

La funzione AutoSupport di StorageGRID consente di monitorare in modo proattivo lo stato di salute del sistema e di inviare automaticamente messaggi e dettagli al supporto tecnico NetApp, al team di supporto interno della tua organizzazione o a un partner di supporto. Per impostazione predefinita, i messaggi AutoSupport al supporto tecnico NetApp vengono attivati quando si configura StorageGRID per la prima volta.

La funzione AutoSupport può essere disattivata. Tuttavia, NetApp consiglia di abilitare l'IT perché AutoSupport aiuta a velocizzare l'identificazione e la risoluzione dei problemi in caso di problemi nel sistema StorageGRID.

AutoSupport supporta HTTPS, HTTP e SMTP per i protocolli di trasporto. A causa della natura sensibile dei messaggi AutoSupport, NetApp consiglia vivamente di utilizzare HTTPS come protocollo di trasporto predefinito per l'invio di messaggi AutoSupport al supporto NetApp.

Facoltativamente, è possibile configurare un proxy amministratore per un maggiore controllo sulle comunicazioni AutoSupport dai nodi di amministrazione al supporto tecnico NetApp. Consultare la procedura per la creazione di un proxy amministratore nelle istruzioni per l'amministrazione di StorageGRID.

Cross-Origin Resource Sharing (CORS)

È possibile configurare Cross-Origin Resource Sharing (CORS) per un bucket S3 se si desidera che quel bucket e gli oggetti in quel bucket siano accessibili alle applicazioni web in altri domini. In generale, non abilitare il CORS a meno che non sia necessario. Se è richiesto un CORS, limitarlo alle origini attendibili.

Consultare la procedura per la configurazione di Cross-Origin Resource Sharing (CORS) nelle istruzioni per l'utilizzo degli account tenant.

Dispositivi di sicurezza esterni

Una soluzione di protezione avanzata completa deve affrontare i meccanismi di sicurezza esterni a StorageGRID. L'utilizzo di ulteriori dispositivi di infrastruttura per il filtraggio e la limitazione dell'accesso a StorageGRID è un metodo efficace per stabilire e mantenere una posizione di sicurezza rigorosa. Questi dispositivi di sicurezza esterni includono firewall, sistemi di prevenzione delle intrusioni (IPS) e altri dispositivi di sicurezza.

Per il traffico client non attendibile, si consiglia un bilanciamento del carico di terze parti. Il bilanciamento del carico di terze parti offre un maggiore controllo e ulteriori livelli di protezione dagli attacchi.

Informazioni correlate

Monitorare e risolvere i problemi

Esaminare i registri di audit

USA account tenant

Amministrare StorageGRID