システムの保護対策
StorageGRID 11.5

NetApp
April 11, 2024

目次

システムの保護対策 . . . 1
StorageGRID システムのセキュリティ強化 . . . 1
ソフトウェアアップグレードの強化に関するガイドライン . . . 2
StorageGRID ネットワークのセキュリティ強化のガイドライン . . . 3
StorageGRID ノードの保護対策のガイドライン . . . 4
サーバ証明書のセキュリティ強化ガイドライン . . . 7
その他のセキュリティ強化に関するガイドライン . . . 8

システムの保護対策

StorageGRID システムをセキュリティの脅威から保護するためのシステム設定、ベストプラクティス、および推奨事項について説明します。

- "StorageGRID システムのセキュリティ強化"
- "ソフトウェアアップグレードの強化に関するガイドライン"
- "StorageGRID ネットワークのセキュリティ強化のガイドライン"
- "StorageGRID ノードの保護対策のガイドライン"
- "サーバ証明書のセキュリティ強化ガイドライン"
- "その他のセキュリティ強化に関するガイドライン"]

StorageGRID システムのセキュリティ強化

システムのセキュリティ強化とは、 StorageGRID システムからできるだけ多くのセキュリティリスクを排除するプロセスです。

このドキュメントでは、 StorageGRID 固有の強化ガイドラインの概要を説明します。これらのガイドラインは、システム強化に関する業界標準のベストプラクティスを補足するものです。たとえば、次のガイドラインでは、 StorageGRID に強力なパスワードを使用し、 HTTP ではなく HTTPS を使用し、可能な場合は証明書ベースの認証を有効にすることを前提としています。

StorageGRID をインストールして構成する際に、これらのガイドラインを使用して、情報システムの機密性、整合性、可用性に関する規定のセキュリティ目標を達成できます。

StorageGRID は、 _NetApp 脆弱性処理ポリシー _ に従います。報告された脆弱性は、製品セキュリティインシデント対応プロセスに従って検証および解決されます。

StorageGRID システムを強化するための一般的な考慮事項

StorageGRID システムを強化する際は、次の点を考慮する必要があります。

- 実装した 3 つの StorageGRID ネットワークのうち、どれですか。すべての StorageGRID システムでグリッドネットワークを使用する必要がありますが、管理ネットワーク、クライアントネットワーク、またはその両方を使用することもできます。ネットワークごとにセキュリティに関する考慮事項が異なります。
- StorageGRID システムの個々のノードで使用するプラットフォームのタイプ。StorageGRID ノードは、VMware仮想マシン、Linuxホスト上のDockerコンテナ内に導入できるほか、専用のハードウェアアプライアンスとして導入することもできます。プラットフォームのタイプごとに、強化に関するベストプラクティスがあります。
- テナントアカウントが信頼されている方法。テナントアカウントを信頼しないサービスプロバイダである場合は、信頼できる社内テナントのみを使用した場合とはセキュリティ上の問題が異なります。
- どのセキュリティ要件および規則に準拠しているか。特定の規制や企業の要件に準拠しなければならない場合があります。

関連情報

"脆弱性対策ポリシー"

ソフトウェアアップグレードの強化に関するガイドライン

攻撃を防御するには、 StorageGRID システムおよび関連サービスを最新の状態に保つ必要があります。

StorageGRID ソフトウェアへのアップグレード

StorageGRID ソフトウェアは、可能なかぎり、最新のメジャーリリースまたは以前のメジャーリリースにアップグレードする必要があります。StorageGRID を最新の状態に保つことで、既知の脆弱性がアクティブになる時間を短縮し、攻撃対象領域全体を削減できます。また、 StorageGRID の最新リリースには、以前のリリースには含まれていないセキュリティ強化機能が含まれていることがよくあります。

ホットフィックスが必要になったときに、ネットアップは最新リリースの更新プログラムの作成に優先順位を付けます。一部のパッチは、以前のリリースと互換性がない場合があります。

StorageGRID の最新のリリースやホットフィックスをダウンロードするには、 StorageGRID のソフトウェアダウンロードページにアクセスします。StorageGRID ソフトウェアのアップグレード手順については、StorageGRID のアップグレード手順を参照してください。ホットフィックスの適用手順については、リカバリとメンテナンスの手順を参照してください。

外部サービスへのアップグレード

外部サービスには、 StorageGRID に間接的に影響する脆弱性が存在する場合がありますStorageGRID が依存するサービスが最新の状態に保たれていることを確認してください。LDAP 、 KMS （ KMIP サーバ）、 DNS 、 NTP などのサービスを利用できます。

サポートされているバージョンの一覧については、 NetApp Interoperability Matrix Tool を参照してください。

ハイパーバイザーのアップグレード

StorageGRID ノードが VMware または別のハイパーバイザーで実行されている場合は、ハイパーバイザーのソフトウェアとファームウェアが最新であることを確認する必要があります。

サポートされているバージョンの一覧については、 NetApp Interoperability Matrix Tool を参照してください。

* Linuxノードへのアップグレード*

StorageGRID ノードで Linux ホストプラットフォームを使用している場合は、セキュリティ更新とカーネル更新がホスト OS に適用されていることを確認する必要があります。また、これらの更新プログラムが利用可能になった場合は、脆弱なハードウェアにファームウェアの更新プログラムを適用する必要があります。

サポートされているバージョンの一覧については、 NetApp Interoperability Matrix Tool を参照してください。

関連情報

"ネットアップのダウンロード： StorageGRID"

"ソフトウェアをアップグレードする"

""

"NetApp Interoperability Matrix Tool で確認できます"

StorageGRID ネットワークのセキュリティ強化のガイドライン

StorageGRID システムでは、グリッドノードあたり最大 3 つのネットワークインターフェイスがサポートされ、各グリッドノードのネットワークをセキュリティやアクセスの要件に応じて設定することができます。

グリッドネットワークのガイドライン

グリッドネットワークはすべての内部 StorageGRID トラフィック用に設定する必要があります。グリッドネットワークのグリッドノードは、いずれも他のすべてのノードと通信できなければなりません。

グリッドネットワークを設定する際は、次のガイドラインに従ってください。

- オープンインターネット上のクライアントなど、信頼できないクライアントからネットワークが保護されていることを確認します。
- 可能な場合は、グリッドネットワークを内部トラフィック専用にします。管理ネットワークとクライアントネットワークの両方に、内部サービスへの外部トラフィックをブロックするファイアウォール制限が追加されています。グリッドネットワークを使用した外部クライアントトラフィックの処理はサポートされていますが、この使用によって保護レイヤが少なくなります。
- StorageGRID 環境が複数のデータセンターにまたがっている場合は、仮想プライベートネットワーク（ VPN ）またはグリッドネットワーク上で同等の機能を使用して、内部トラフィックをさらに保護します。
- 一部のメンテナンス手順では、プライマリ管理ノードと他のすべてのグリッドノードの間のポート 22 で Secure Shell （ SSH ）アクセスが必要です。外部ファイアウォールを使用して、信頼できるクライアントへの SSH アクセスを制限します。

管理ネットワークのガイドライン

管理ネットワークは、通常、管理タスク（ Grid Manager または SSH を使用する信頼できる従業員）および LDAP 、 DNS 、 NTP 、 KMS （ KMIP サーバ）などの信頼された他のサービスとの通信に使用します。ただし、 StorageGRID ではこの使用が内部的に適用されることはありません。

管理ネットワークを使用する場合は、次のガイドラインに従ってください。

- 管理ネットワーク上のすべての内部トラフィックポートをブロックします。使用するプラットフォームに対応したインストールガイドの内部ポートの一覧を参照してください。
- 信頼されていないクライアントが管理ネットワークにアクセスできる場合は、外部ファイアウォールで管理ネットワーク上の StorageGRID へのアクセスをブロックします。

クライアントネットワークのガイドライン

クライアントネットワークは、通常、テナント、および CloudMirror レプリケーションサービスや別のプラットフォームサービスなどの外部サービスとの通信に使用されます。ただし、 StorageGRID ではこの使用が内部的に適用されることはありません。

クライアントネットワークを使用する場合は、次のガイドラインに従ってください。

- クライアントネットワーク上のすべての内部トラフィックポートをブロックします。使用するプラットフォームに対応したインストールガイドの内部ポートの一覧を参照してください。
- 明示的に設定されたエンドポイントでのみ、インバウンドクライアントトラフィックを受け入れます。StorageGRID の管理手順の信頼されていないクライアントネットワークの管理に関する情報を参照してください。

関連情報

"ネットワークガイドライン"

"グリッド入門"

"StorageGRID の管理"

"Red Hat Enterprise Linux または CentOS をインストールします"

"Ubuntu または Debian をインストールします"

"VMware をインストールする"

StorageGRID ノードの保護対策のガイドライン

StorageGRID ノードは、VMware仮想マシン、Linuxホスト上のDockerコンテナ内に導入できるほか、専用のハードウェアアプライアンスとして導入することもできます。プラットフォームのタイプとノードのタイプにはそれぞれ、強化に関するベストプラクティスがあります。

ファイアウォールの設定

システム強化プロセスの一環として、外部ファイアウォールの設定を確認し、 IP アドレスとそれが厳密に必要なポートからのみトラフィックが許可されるように変更する必要があります。

VMwareプラットフォームおよびStorageGRID アプライアンスで実行されるノードは、自動的に管理される内部ファイアウォールを使用します。この内部ファイアウォールは、一部の一般的な脅威に対する追加の保護レイヤを提供しますが、外部ファイアウォールの必要性は排除されません。

StorageGRID で使用されるすべての内部ポートと外部ポートの一覧については、ご使用のプラットフォームのインストールガイドを参照してください。

仮想化、コンテナ、共有ハードウェア

すべての StorageGRID ノードで、信頼されていないソフトウェアと同じ物理ハードウェア上で StorageGRID を実行しないでください。StorageGRID とマルウェアの両方が同じ物理ハードウェア上に存在する場合、ハイパーバイザーによる保護によって、 StorageGRID で保護されたデータへのマルウェアのアクセスが防止されるとは限りません。たとえば、 Meltdown と Specter 攻撃は、最新のプロセッサに存在する重要な脆弱性を悪用し、プログラムが同じコンピュータ上のメモリにデータを盗むことを可能にします。

未使用のサービスを無効にします

すべての StorageGRID ノードについて、未使用のサービスへのアクセスを無効化またはブロックする必要が

あります。たとえば、 CIFS または NFS 用の監査共有へのクライアントアクセスを設定しない場合は、これらのサービスへのアクセスをブロックするか無効にします。

インストール中にノードを保護

信頼されていないユーザが、ノードのインストール時にネットワーク経由で StorageGRID ノードにアクセスすることを許可しないでください。ノードは、グリッドに参加するまで完全にはセキュアではありません。

管理ノードのガイドライン

管理ノードは、システムの設定、監視、ロギングなどの管理サービスを提供します。Grid Manager または Tenant Manager にサインインすると、管理ノードに接続されます。

StorageGRID システムで管理ノードを保護するには、次のガイドラインに従います。

- 開いているインターネット上の管理ノードなど、信頼されていないクライアントからすべての管理ノードを保護します。グリッドネットワーク上、管理ネットワーク上、またはクライアントネットワーク上のどの管理ノードにも、信頼されていないクライアントがアクセスできないようにします。
- StorageGRID グループは Grid Manager とテナントマネージャの機能へのアクセスを制御します。各ユーザグループにロールに最低限必要な権限を付与し、読み取り専用アクセスモードを使用してユーザによる設定変更を防止します。
- StorageGRID ロードバランサエンドポイントを使用する場合は、信頼されないクライアントトラフィックに管理ノードの代わりにゲートウェイノードを使用します。
- 信頼されていないテナントがある場合は、テナントマネージャやテナント管理 API に直接アクセスすることを許可しないでください。代わりに、信頼されていないテナントがテナントポータルまたはテナント管理 API と連動する外部テナント管理システムを使用するようにします。
- 必要に応じて、管理ノードからネットアップサポートへの AutoSupport 通信をより細かく制御するために管理プロキシを使用します。StorageGRID の管理手順の管理プロキシの作成手順を参照してください。
- 必要に応じて、制限された 8443 ポートと 9443 ポートを使用して Grid Manager と Tenant Manager の通信を分離します。共有ポート 443 をブロックして、テナント要求をポート 9443 に制限して追加の保護を確保します。
- 必要に応じて、グリッド管理者とテナントユーザには別々の管理ノードを使用します。

詳細については、 StorageGRID の管理手順を参照してください。

ストレージノードに関するガイドライン

ストレージノードは、オブジェクトデータとメタデータを管理および格納します。StorageGRID システムでストレージノードを保護するには、次のガイドラインに従います。

- 信頼されていないテナントのアウトバウンドサービスは有効にしないでください。たとえば、信頼されていないテナントのアカウントを作成する場合は、テナントが独自のアイデンティティソースを使用することを許可せず、プラットフォームサービスの使用も許可しないでください。StorageGRID の管理手順に従って、テナントアカウントを作成する手順を参照してください。
- 信頼されないクライアントトラフィックには、サードパーティのロードバランサを使用します。サードパーティ製のロードバランシングにより、攻撃に対する制御性が向上し、追加の保護レイヤが提供されます。
- 必要に応じて、ストレージプロキシを使用して、クラウドストレージプールとプラットフォームサービス

のストレージノードから外部サービスへの通信をより細かく制御します。StorageGRID の管理手順のストレージプロキシの作成手順を参照してください。

- 必要に応じて、クライアントネットワークを使用して外部サービスに接続します。次に、「* Configuration > Network Settings > Untrusted Client Network *」を選択し、ストレージノード上のクライアントネットワークが信頼されていないことを示します。ストレージノードはクライアントネットワーク上の受信トラフィックを受け入れなくなりますが、プラットフォームサービスへのアウトバウンド要求は引き続き許可します。

ゲートウェイノードのガイドライン

ゲートウェイノードは、クライアントアプリケーションが StorageGRID への接続に使用できるオプションのロードバランシングインターフェイスです。StorageGRID システムにゲートウェイノードを保護するには、次のガイドラインに従います。

- ゲートウェイノード上の CLB サービスを使用する代わりに、ロードバランサエンドポイントを設定して使用する。StorageGRID の管理手順のロードバランシングの管理手順を参照してください。

  CLB サービスは廃止されました。

- クライアントとゲートウェイノードまたはストレージノードの間で、信頼されていないクライアントトラフィックにサードパーティのロードバランサを使用します。サードパーティ製のロードバランシングにより、攻撃に対する制御性が向上し、追加の保護レイヤが提供されます。サードパーティのロードバランサを使用する場合でも、内部のロードバランサエンドポイントを経由するようにネットワークトラフィックを設定したり、ストレージノードに直接送信したりすることができます。
- ロードバランサエンドポイントを使用している場合は、必要に応じてクライアントネットワーク経由で接続します。次に、「* Configuration > Network Settings > Untrusted Client Network *」を選択し、ゲートウェイノード上のクライアントネットワークが信頼されていないことを示します。ゲートウェイノードは、ロードバランサエンドポイントとして明示的に設定されたポートのインバウンドトラフィックのみを受け入れます。

ハードウェアアプライアンスノードのガイドライン

StorageGRID ハードウェアアプライアンスは、 StorageGRID システム専用に設計されています。一部のアプライアンスはストレージノードとして使用できます。その他のアプライアンスは、管理ノードまたはゲートウェイノードとして使用できます。アプライアンスノードをソフトウェアベースのノードと組み合わせることも、自社開発の全アプライアンスグリッドを導入することもできます。

StorageGRID システムにハードウェアアプライアンスノードを固定するには、次のガイドラインに従います。

- アプライアンスでストレージコントローラの管理に SANtricity System Manager を使用している場合は、信頼されていないクライアントからネットワーク経由で SANtricity System Manager にアクセスできないようにします。
- アプライアンスに Baseboard Management Controller （ BMC ；ベースボード管理コントローラ）が搭載されている場合は、 BMC 管理ポートで下位レベルのハードウェアアクセスが許可されることに注意してください。BMC 管理ポートは、信頼されているセキュアな内部管理ネットワークにのみ接続してください。該当するネットワークがない場合は、テクニカルサポートから BMC 接続の要請があった場合を除き、 BMC 管理ポートを接続しないか、またはブロックしたままにしてください。
- アプライアンスが Intelligent Platform Management Interface （ IPMI ）標準を使用したイーサネット経由でのコントローラハードウェアのリモート管理をサポートする場合は、ポート 623 での信頼されていない

トラフィックをブロックします。

- アプライアンスのストレージコントローラに FDE または FIPS ドライブが搭載されていて、ドライブセキュリティ機能が有効になっている場合は、 SANtricity を使用してドライブセキュリティキーを設定します。
- FDE または FIPS ドライブが搭載されていないアプライアンスの場合は、 Key Management Server （ KMS ）を使用してノード暗号化を有効にします。

使用している StorageGRID ハードウェアアプライアンスのインストールとメンテナンスの手順を参照してください。

関連情報

"Red Hat Enterprise Linux または CentOS をインストールします"

"Ubuntu または Debian をインストールします"

"VMware をインストールする"

"StorageGRID の管理"

"テナントアカウントを使用する"

"SG100 SG1000サービスアプライアンス"

"SG5600 ストレージアプライアンス"

"SG5700 ストレージアプライアンス"

"SG6000 ストレージアプライアンス"

サーバ証明書のセキュリティ強化ガイドライン

インストール時に作成されたデフォルトの証明書を独自のカスタム証明書に置き換える必要があります。

多くの組織では、 StorageGRID Web アクセス用の自己署名デジタル証明書が、情報セキュリティポリシーに準拠していません。本番用システムでは、 StorageGRID の認証に使用する CA 署名デジタル証明書をインストールする必要があります。

具体的には、次のデフォルト証明書ではなくカスタムサーバ証明書を使用する必要があります。

- 管理インターフェイスのサーバ証明書：Grid Manager、テナントマネージャ、Grid管理API、テナント管理APIへのアクセスを保護するために使用されます。
- * Object Storage API Service Endpoints Server Certificate *：ストレージノードおよびゲートウェイノードへのアクセスを保護するために使用します。これらのノードは、S3およびSwiftクライアントアプリケーションがオブジェクトデータをアップロードおよびダウンロードするために使用します。

> StorageGRID では、ロードバランサエンドポイントに使用する証明書は別に管理されます。ロードバランサ証明書を設定するには、 StorageGRID の管理手順でロードバランサエンドポイントの設定手順を参照してください。

カスタムサーバ証明書を使用する場合は、次のガイドラインに従ってください。

- 証明書にはが必要です *subjectAltName* StorageGRID のDNSエントリと同じです。詳細については、のセクション 4.2.1.6 「 Subject Alternative Name 」を参照してください "RFC 5280: PKIX 証明書と CRL プロファイル"。
- 可能であれば、ワイルドカード証明書は使用しないでください。このガイドラインの例外は、 S3 仮想ホスト形式のエンドポイントの証明書です。バケット名が事前に不明な場合は、ワイルドカードを使用する必要があります。
- 証明書にワイルドカードを使用する必要がある場合は、リスクを軽減するために追加の手順を実行する必要があります。などのワイルドカードパターンを使用します `*.s3.example.com`を使用せずに、を使用してください `s3.example.com` その他のアプリケーションのサフィックス。このパターンは、などのパス形式のS3アクセスでも機能します `dc1-s1.s3.example.com/mybucket`。
- 証明書の有効期限を短く（ 2 カ月など）設定し、グリッド管理 API を使用して証明書のローテーションを自動化します。これは、ワイルドカード証明書で特に重要です。

また、クライアントは StorageGRID との通信に厳密なホスト名チェックを使用する必要があります。

その他のセキュリティ強化に関するガイドライン

StorageGRID ネットワークおよびノードに対する強化ガイドラインに加えて、StorageGRID システムの他の領域に対する強化ガイドラインに従う必要があります。

ログと監査メッセージ

StorageGRID ログおよび監査メッセージ出力は必ず安全な方法で保護してください。StorageGRID のログと監査メッセージは、サポートやシステム可用性の観点から非常に重要な情報を提供します。また、StorageGRID のログおよび監査メッセージの出力に含まれる情報や詳細情報は、一般に機密性が高いため、

StorageGRID ログの詳細については、監視とトラブルシューティングの手順を参照してください。StorageGRID 監査メッセージの詳細については、監査メッセージに関する手順を参照してください。

NetApp AutoSupport

StorageGRID の AutoSupport 機能を使用すると、システムの状態をプロアクティブに監視し、ネットアップテクニカルサポート、組織の社内サポートチーム、またはサポートパートナーにメッセージと詳細を自動的に送信できます。デフォルトでは、 StorageGRID を初めて設定した場合、ネットアップテクニカルサポートへの AutoSupport メッセージが有効になります。

AutoSupport 機能は無効にすることができます。ただし、 StorageGRID システムで問題 に障害が発生した場合には、 AutoSupport を使用して迅速に問題を識別し解決できるため、ネットアップではこの機能を有効にすることを推奨してい

AutoSupport は、転送プロトコルとして HTTPS 、 HTTP 、 SMTP をサポートしています。AutoSupport メッセージは機密性が高いため、ネットアップでは、 AutoSupport メッセージをネットアップサポートに送信する際のデフォルト転送プロトコルとして HTTPS を使用することを強く推奨しています。

必要に応じて、管理ノードからネットアップテクニカルサポートへの AutoSupport 通信をより細かく制御するための管理プロキシを設定できます。StorageGRID の管理手順の管理プロキシの作成手順を参照してください。

Cross-Origin Resource Sharing （ CORS ）

S3 バケットとバケット内のオブジェクトに他のドメインにある Web アプリケーションからアクセスできるようにする必要がある場合は、そのバケットに Cross-Origin Resource Sharing （ CORS ）を設定できます。一般に、 CORS は必要でないかぎり有効にしないでください。CORS が必要な場合は、信頼できるオリジンに制限します。

テナントアカウントの使用手順の Cross-Origin Resource Sharing （ CORS ）の設定手順を参照してください。

外部セキュリティデバイス

完全なセキュリティ強化解決策 は、 StorageGRID 以外のセキュリティメカニズムに対応する必要があります。StorageGRID へのアクセスをフィルタリングおよび制限するために追加のインフラデバイスを使用すると、厳格なセキュリティ体制を確立し、維持するための効果的な方法となります。これらの外部セキュリティデバイスには、ファイアウォール、 Intrusion Prevention System （ IPS ；侵入防御システム）、およびその他のセキュリティデバイスが含まれます。

信頼されないクライアントトラフィックには、サードパーティのロードバランサを使用することを推奨します。サードパーティ製のロードバランシングにより、攻撃に対する制御性が向上し、追加の保護レイヤが提供されます。

関連情報

"トラブルシューティングを監視します"

"監査ログを確認します"

"テナントアカウントを使用する"

"StorageGRID の管理"

著作権に関する情報

商標に関する情報