システムの強化
StorageGRID software

NetApp
December 03, 2025

目次

システムの強化

システム強化に関する一般的な考慮事項

システム強化は、 StorageGRIDシステムから可能な限り多くのセキュリティ リスクを排除するプロセスです。

StorageGRIDをインストールして構成するときには、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満たすために、これらのガイドラインを使用してください。

システム強化については、すでに業界標準のベスト プラクティスを使用しているはずです。たとえば、StorageGRIDには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します。

StorageGRIDは "NetApp脆弱性対応ポリシー"。報告された脆弱性は、製品のセキュリティ インシデント対応プロセスに従って検証され、対処されます。

StorageGRIDシステムを強化する場合は、次の点を考慮してください。

- **3** つの**StorageGRID**ネットワークのうちどれを実装しましたか。すべてのStorageGRIDシステムはグリッド 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システム内の個々のノードに使用する プラットフォームの種類。 StorageGRIDノードは、VMware 仮想マシン、Linux ホスト上のコンテナ エンジン内、または専用のハードウェア アプライアンスとして展開できます。各タイプのプラットフォームには、独自の強化ベスト プラクティスがあります。
- テナント アカウントの信頼性。信頼されていないテナント アカウントを持つサービス プロバイダーの場合、信頼できる社内テナントのみを使用する場合とは異なるセキュリティ上の懸念が生じます。
- 組織が従うセキュリティ要件と規則。特定の規制または企業の要件に準拠する必要がある場合があります。

ソフトウェアアップグレードの強化ガイドライン

攻撃から身を守るには、 StorageGRIDシステムと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

可能な限り、 StorageGRIDソフトウェアを最新のメジャー 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っている時間を短縮し、全体的な攻撃対象領域を減らすことができます。さらに、 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かった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。

ご相談ください "NetApp Interoperability Matrix Tool"(IMT) を使用して、使用する必要があるStorageGRIDソフトウェアのバージョンを決定します。ホットフィックスが必要になった場合、NetAppは最新リリースに対するアップデートの作成を優先します。一部のパッチは以前のリリースと互換性がない可能性があります。

- 最新のStorageGRIDリリースとホットフィックスをダウンロードするには、 "NetAppのダウンロード

：StorageGRID" 。

- StorageGRIDソフトウェアをアップグレードするには、"アップグレード手順" 。
- 修正プログラムを適用するには、"StorageGRIDホットフィックス手順" 。

外部サービスへのアップグレード

外部サービスには、 StorageGRID に間接的に影響を及ぼす脆弱性が存在する可能性があります。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する必要があります。これらのサービスには、LDAP、KMS (または KMIP サーバー)、DNS、NTP が含まれます。

サポートされているバージョンのリストについては、 "NetApp Interoperability Matrix Tool" 。

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上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リストについては、 "NetApp Interoperability Matrix Tool" 。

Linuxノードへのアップグレード

StorageGRIDノードが 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。さらに、ファームウェアのアップデートが利用可能になったら、脆弱なハードウェアにアップデート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リストについては、 "NetApp Interoperability Matrix Tool" 。

StorageGRIDネットワークの強化ガイドライン

StorageGRIDシステムは、グリッド ノードごとに最大 3 つのネットワーク インターフェイスをサポートしているため、セキュリティとアクセスの要件に合わせて各グリッド ノードのネットワークを構成できます。

StorageGRIDネットワークの詳細については、"StorageGRIDネットワークの種類" 。

グリッドネットワークのガイドライン

すべての内部StorageGRIDトラフィックに対してグリッド ネットワークを構成する必要があります。すべてのグリッド ノードはグリッド ネットワーク上に存在し、他のすべてのノードと通信できる必要があります。

グリッド ネットワークを構成するときは、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使用してください。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追加のファイアウォール制限があります。外部クライアント トラフィックにグリッド ネットワークを使用することはサポートされていますが、この使用方法では保護層が少なくなります。

- StorageGRID の展開が複数のデータ センターにまたがる場合は、グリッド ネットワーク上で仮想プライベート ネットワーク (VPN) または同等のものを使用して、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 ノード間のポート 22 でのセキュア シェル (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。

管理者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 (グリッド マネージャーまたは SSH を使用する信頼できる従業員) や、LDAP、DNS、NTP、KMS (または KMIP サーバー) などの他の信頼できるサービスとの通信に使用されます。ただし、 StorageGRID は内部的にこの使用法を強制しません。

管理ネットワークを使用している場合は、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。参照"内部ポートのリスト"。
- 信頼でき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を使用して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、テナント用、および CloudMirror レプリケーション サービスや他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 は内部的にこの使用法を強制しません。

クライアント ネットワークを使用している場合は、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。参照"内部ポートのリスト"。
- 明示的に構成されたエンドポイントでのみ、受信クライアント トラフィックを受け入れます。に関する情報を見る"ファイアウォール制御の管理"。

StorageGRIDノードの強化ガイドライン

StorageGRIDノードは、VMware 仮想マシン、Linux ホスト上のコンテナ エンジン内、または専用のハードウェア アプライアンスとして展開できます。各タイプのプラットフォームと各タイプのノードには、独自の強化ベスト プラクティス セットがあります。

BMCへのリモートIPMIアクセスを制御する

BMCを含むすべてのアプライアンスに対してリモート IPMI アクセスを有効または無効にすることができます。リモート IPMI インターフェイスを使用すると、 BMCアカウントとパスワードを持つすべてのユーザーがStorageGRIDアプライアンスに低レベルのハードウェア アクセスできるようになります。BMCへのリモート IPMI アクセスが必要ない場合は、このオプションを無効にします。

- Grid Manager でBMCへのリモート IPMI アクセスを制御するには、[構成] > [セキュリティ] > [セキュリティ設定] > [アプライアンス] に移動します。
  - BMCへの IPMI アクセスを無効にするには、[リモート IPMI アクセスを有効にする] チェックボックスをオフにします。

- BMCへの IPMI アクセスを有効にするには、[リモート IPMI アクセスを有効にする] チェックボックスをオンにします。

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構成を確認し、厳密に必要な IP アドレスとポートからのトラフィックのみが受け入れられるように変更する必要があります。

StorageGRID には各ノードに内部ファイアウォールが含まれており、ノードへのネットワーク アクセスを制御できるため、グリッドのセキュリティが強化されます。あなたがすべき"内部ファイアウォール制御を管理する"特定のグリッド展開に必要なポートを除くすべてのポートでのネットワーク アクセスを防止します。ファイアウォール制御ページで行った構成の変更は、各ノードに展開されます。

具体的には、次の領域を管理できます。

- 特権アドレス: 選択した IP アドレスまたはサブネットが、[外部アクセスの管理] タブの設定によって閉じられているポートにアクセスできるようにすることができます。
- 外部アクセスの管理: デフォルトで開いているポートを閉じたり、以前に閉じたポートを再度開いたりすることができます。
- 信頼できないクライアント ネットワーク: 信頼できないクライアント ネットワークが構成されている場合に、ノードがクライアント ネットワークからの受信トラフィックを信頼するかどうか、および開く追加のポートを指定できます。

この内部ファイアウォールは、いくつかの一般的な脅威に対する追加の保護層を提供しますが、外部ファイアウォールの必要性を排除するものではありません。

StorageGRIDで使用されるすべての内部ポートと外部ポートのリストについては、"ネットワークポートリファレンス" 。

使用していないサービスを無効にする

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にするかブロックする必要があります。たとえば、DHCP を使用する予定がない場合は、グリッド マネージャーを使用してポート 68 を閉じます。構成 > ファイアウォール制御 > 外部アクセスの管理*を選択します。次に、ポート **68** のステータス トグルを ***Open** から **Closed** に変更します。

仮想化、コンテナ、共有ハードウェア

すべてのStorageGRIDノードでは、信頼でき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、ハイパーバイザ保護によってマルウェアがStorageGRIDで保護されたデータにアクセスするのを防止できると想定しないでください。たとえば、Meltdown 攻撃や Spectre 攻撃では、最新のプロセッサの重大な脆弱性が悪用され、プログラムが同じコンピューター上のメモリ内のデータを盗むことが可能になります。

インストール中にノードを保護する

ノードのインストール中は、信頼できないユーザーが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安全ではありません。

管理ノードのガイドライン

管理ノードは、システム構成、監視、ログ記録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システム内の管理ノードを保護するには、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すべての管理ノードを保護します。信頼できないクライアントがグリッド ネットワーク、管理ネットワーク、またはクライアント ネットワーク上の管理ノードにアクセスできないようにします。
- StorageGRIDグループは、Grid Manager および Tenant Manager 機能へのアクセスを制御します。各ユーザー グループに、そのロールに必要な最小限の権限を付与し、読み取り専用アクセス モードを使用して、ユーザーが構成を変更できないようにします。
- StorageGRIDロード バランサ エンドポイントを使用する場合は、信頼できないクライアント トラフィックに対して管理ノードではなくゲートウェイ ノードを使用します。
- 信頼できないテナントがある場合は、テナント マネージャーまたはテナント管理 API への直接アクセスを許可しないでください。代わりに、信頼できないテナントには、テナント管理 API と対話するテナント ポータルまたは外部テナント管理システムを使用するようにします。
- オプションで、管理プロキシを使用して、管理ノードからNetAppサポートへのAutoSupport通信をより詳細に制御できます。手順については、"管理プロキシの作成" 。
- 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。追加の保護のために、共有ポート 443 をブロックし、テナント要求をポート 9443 に制限します。
- 必要に応じて、グリッド管理者とテナント ユーザーごとに個別の管理ノードを使用します。

詳細については、"StorageGRIDの管理" 。

ストレージノードのガイドライン

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保存します。 StorageGRIDシステム内のストレージ ノードを保護するには、次のガイドラインに従ってください。

- 信頼できないクライアントがストレージ ノードに直接接続することを許可しません。ゲートウェイ ノードまたはサードパーティのロード バランサーによって提供されるロード バランサー エンドポイントを使用します。
- 信頼されていないテナントに対して送信サービスを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 ID ソースを使用することや、プラットフォーム サービスを使用することを許可しないでください。手順については、"テナントアカウントの作成" 。
- 信頼できないクライアント 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。サードパーティの負荷分散により、より高度な制御と、攻撃に対する追加の保護レイヤーが提供されます。
- 必要に応じて、ストレージ プロキシを使用して、ストレージ ノードから外部サービスへのクラウド ストレージ プールとプラットフォーム サービス通信をより詳細に制御します。手順については、"ストレージプロキシの作成" 。
- 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、構成 > セキュリティ > ファイアウォール制御 > 信頼されていないクライアント ネットワーク 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 ネットワーク上の着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

送信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に接続するために使用できるオプションの負荷分散インターフェイスを提供します。 StorageGRIDシステム内のゲートウェイ ノードを保護するには、次のガイドラインに従ってください。

- ロード バランサーのエンドポイントを構成して使用します。見る"負荷分散に関する考慮事項" 。
- 信頼できないクライアント トラフィックの場合は、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。サードパーティの負荷分散により、より高度な制御と、攻撃に対する追加の保護レイヤーが提供されます。サードパーティのロード バランサを使用する場合でも、ネットワーク トラフィックをオプションで構成して、内部ロード バランサのエンドポイントを通過するか、ストレージ ノードに直接送信するかを選択できます。
- ロード バランサー エンドポイントを使用している場合は、オプションでクライアントをクライアント ネットワーク経由で接続します。次に、[構成] > [セキュリティ] > [ファイアウォール制御] > [信頼されていないクライアント ネットワーク] 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 バランサーのエンドポイントとして明示的に構成されたポート上の受信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システムで使用するために特別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たり、完全に設計された全アプライアンス グリッドを展開したりできます。

StorageGRIDシステム内のハードウェア アプライアンス ノードを保護するには、次のガイドラインに従ってください。

- アプライアンスがストレージ コントローラの管理にSANtricity System Manager を使用する場合は、信頼できないクライアントが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。
- アプライアンスにベースボード管理コントローラ (BMC) が搭載されている場合は、 BMC管理ポートによって低レベルのハードウェア アクセスが許可される場合があるので注意してください。BMC管理ポートは、安全で信頼できる内部管理ネットワークにのみ接続してください。このようなネットワークが利用できない場合は、テクニカル サポートからBMC接続が要求されない限り、 BMC管理ポートを未接続またはブロックされたままにしておきます。
- アプライアンスがインテリジェント プラットフォーム管理インターフェイス (IPMI) 標準を使用してイーサネット経由でコントローラ ハードウェアのリモート管理をサポートしている場合は、ポート 623 上の信頼できないトラフィックをブロックします。

> BMCを含むすべてのアプライアンスに対してリモート IPMI アクセスを有効または無効にすることができます。リモート IPMI インターフェイスを使用すると、 BMCアカウントとパスワードを持つすべてのユーザーがStorageGRIDアプライアンスに低レベルのハードウェア アクセスできるようになります。BMCへのリモート IPMI アクセスが必要ない場合は、次のいずれかの方法でこのオプションを無効にします。+ Grid Manager で、構成 > セキュリティ > セキュリティ設定 > アプライアンス に移動し、リモート **IPMI** アクセスを有効にする チェックボックスをオフにします。+ グリッド管理 API では、プライベート エンドポイントを使用します。 `PUT /private/bmc` 。

- SANtricity System Managerで管理するSED、FDE、またはFIPS NL-SASドライブを搭載したアプライアンスモデルの場合、 "SANtricityドライブセキュリティを有効にして構成する" 。
- StorageGRIDアプライアンスインストーラおよびグリッドマネージャを使用して管理するSEDまたはFIPS NVMe SSDを搭載したアプライアンスモデルの場合、 "StorageGRIDドライブ暗号化を有効にして構成する" 。
- SED、FDE、またはFIPSドライブを搭載していないアプライアンスの場合は、 StorageGRIDソフトウェアノード暗号化を有効にして構成します。 "キー管理サーバー（KMS）を使用する" 。

TLSとSSHの強化ガイドライン

インストール中に作成されたデフォルトの証明書を置き換え、TLS および SSH 接続に適切なセキュリティ ポリシーを選択する必要があります。

証明書の強化ガイドライン

インストール中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。実稼働システムでは、 StorageGRID の認証に使用する CA 署名付き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の代わりにカスタム サーバー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証明書: グリッド マネージャー、テナント マネージャー、グリッド管理 API、およびテナント管理 API へのアクセスを保護するために使用されます。
- **S3 API** 証明書: S3 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するストレージ ノードとゲートウェイ ノードへのアクセスを保護するために使用されます。

見る"セキュリティ証明書を管理する"詳細と手順についてはこちらをご覧ください。

> StorageGRID は、ロード バランサのエンドポイントに使用される証明書を個別に管理します。ロードバランサ証明書を構成するには、"ロードバランサのエンドポイントを構成する" 。

カスタム サーバー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 `*subjectAltName*`StorageGRIDの DNS エントリに一致します。詳細については、セクション4.2.1.6「サブジェクト代替名」を参照してください。 "RFC 5280: PKIX証明書とCRLプロファイル" 。
- 可能な場合は、ワイルドカード証明書の使用は避けてください。このガイドラインの例外は、S3 仮想ホスト スタイルのエンドポイントの証明書です。バケット名が事前にわかっていない場合、ワイルドカードを使用する必要があります。
- 証明書で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。ワイルドカードパターンを使用する例： `*.s3.example.com` 、そして、 `s3.example.com`他のアプリケーション用のサフィックス。このパターンは、次のようなパススタイルの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（たとえば 2 か月）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の場合に特に重要です。

さらに、クライアントはStorageGRIDと通信するときに厳密なホスト名チェックを使用する必要があります。

TLS および SSH ポリシーの強化ガイドライン

セキュリティ ポリシーを選択して、クライアント アプリケーションとの安全な TLS 接続と内部StorageGRIDサービスへの安全な SSH 接続を確立するために使用されるプロトコルと暗号を決定できます。

セキュリティ ポリシーは、TLS と SSH が移動中のデータを暗号化する方法を制御します。ベストプラクティスとして、アプリケーションの互換性に必要のない暗号化オプションを無効にする必要があります。システムが Common Criteria に準拠している必要がある場合、または他の暗号を使用する必要がない限り、デフォルトのモダン ポリシーを使用します。

見る"TLSおよびSSHポリシーを管理する"詳細と手順についてはこちらをご覧ください。

その他の強化ガイドライン

StorageGRIDネットワークとノードの強化ガイドラインに従うことに加えて、StorageGRIDシステムの他の領域の強化ガイドラインにも従う必要があります。

一時インストールパスワード

インストール中にStorageGRIDシステムを保護するには、 StorageGRIDインストール UI またはインストール API の一時インストーラ パスワード ページでパスワードを設定します。このパスワードを設定すると、ユーザーインターフェイス、インストールAPI、およびStorageGRIDのインストールのすべての方法に適用されます。 `configure-storagegrid.py`スクリプト。

詳細については、以下を参照してください。

- "Red Hat Enterprise LinuxにStorageGRIDをインストールする"
- "UbuntuまたはDebianにStorageGRIDをインストールする"
- "VMwareにStorageGRIDをインストールする"
- "StorageGRIDアプライアンスをインストールする"

ログと監査メッセージ

StorageGRIDログと監査メッセージ出力を常に安全に保護します。 StorageGRIDログと監査メッセージは、サポートとシステムの可用性の観点から貴重な情報を提供します。さらに、 StorageGRIDログおよび監査メッセージ出力に含まれる情報と詳細は、通常、機密性の高いものです。

セキュリティ イベントを外部 Syslog サーバーに送信するようにStorageGRIDを構成します。 Syslog エクスポートを使用する場合は、トランスポート プロトコルとして TLS と RELP/TLS を選択します。

参照"ログファイルリファレンス"StorageGRIDログの詳細については、こちらをご覧ください。見る"監査メッセージ"StorageGRID監査メッセージの詳細については、こちらをご覧ください。

NetApp AutoSupport

StorageGRIDのAutoSupport機能を使用すると、システムの健全性をプロアクティブに監視し、パッケージをNetAppサポート サイト、組織の内部サポート チーム、またはサポート パートナーに自動的に送信できま

す。デフォルトでは、 StorageGRIDが初めて構成されるときに、 AutoSupportパッケージのNetAppへの送信が有効になります。

AutoSupport機能は無効にすることもできます。ただし、 StorageGRIDシステムで問題が発生した場合、AutoSupportによって問題の特定と解決が迅速化されるため、 NetAppこれを有効にすることを推奨しています。

AutoSupportは、転送プロトコルとしてHTTPS、HTTP、およびSMTPをサポートします。AutoSupportパッケージは機密情報であるため、 NetApp、 AutoSupportパッケージをNetAppに送信する際のデフォルトのトランスポート 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。

クロスオリジンリソース共有（CORS）

S3 バケットとそのバケット内のオブジェクトを他のドメインの Web アプリケーションからアクセスできるようにする場合は、S3 バケットに対してクロスオリジン リソース共有 (CORS) を設定できます。一般に、必要な場合を除き、CORS を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。

手順については、"クロスオリジンリソース共有（CORS）の設定" 。

外部セキュリティデバイス

完全な強化ソリューションでは、 StorageGRID外部のセキュリティ メカニズムに対処する必要があります。追加のインフラストラクチャ デバイスを使用してStorageGRIDへのアクセスをフィルタリングおよび制限することは、厳格なセキュリティ体制を確立して維持するための効果的な方法です。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、侵入防止システム (IPS)、その他のセキュリティ デバイスが含まれます。

信頼できないクライアント トラフィックには、サードパーティのロード バランサの使用をお勧めします。サードパーティの負荷分散により、より高度な制御と、攻撃に対する追加の保護レイヤーが提供されます。

ランサムウェア対策

ランサムウェア攻撃からオブジェクトデータを保護するために、以下の推奨事項に従ってください。"StorageGRIDによるランサムウェア防御" 。

著作権に関する情報

商標に関する情報