バックアップ

この章では、Threat Gridアプライアンスの要件、予想される成果、データ保持ポリシー、およびバックアップと復元の手順について説明します。説明する項目は次のとおりです。

Threat Grid アプライアンスのバックアップ

Threat Grid アプライアンス（v2.2.4 以降）は、NFS 対応ストレージへの暗号化されたバックアップ、NFS 対応ストレージからのデータの初期化、さらに、データベースを空の状態にリセットして前述のバックアップのロードを可能にする機能をサポートしています。

（注） リセットは、アプライアンスのワイププロセスとは異なっており、アプライアンスが情報漏えいなしで顧客構内に出荷されるようにするために使用され、バックアップ準備のためにも使用されます。その目的に適したワイププロセスは、リカバリブートローダーにすでに存在していますが、バックアップを復元するためのシステムの準備には適していません。

コンテンツは、サードパーティ製オープンソース製品である gocryptfs を使用して暗号化されます。

（注） パフォーマンス上の理由から、ファイル名の暗号化は無効になっています。Threat Grid 内のサンプルとその他のコンテンツは、どのような状況でも元の名前では保存されないため、顧客の所有データが漏洩することはありません。

ご使用の前に、ドキュメントをよくお読みいただくことを強くお勧めします。バックアップの機能に関する詳細ドキュメントを入手できます。使用する前によくお読みいただくことを強くお勧めします。追加の技術情報と手順については、Cisco.com で『*Threat Grid Appliance Backup Notes and FAQ*』と『*Cisco Threat Grid Appliance Setup and Configuration Guide*』を参照してください。

NFS 要件

NFS バックアップストレージへの暗号化されたバックアップを実現するには、次の NFS 要件を満たす必要があります。

- Threat Grid アプライアンス管理インターフェイスからアクセス可能な TCP 経由の NFSv4 プロトコルを実行している必要があります。
- 設定されているディレクトリは、nfsnobody（UID 65534）で書き込み可能である必要があります。
- NFSv4 サーバは、10 GB 管理インターフェイス経由でアクセス可能である必要があります。
- 十分なストレージが使用可能である必要があります（「バックアップストレージ要件」を参照）。
- 次のマウントパラメータが無条件で使用されます。`rw`、`sync`、`nfsvers=4`、`nofail`

  （注） これらのパラメータを手動で入力する必要はありません。これらと競合するパラメータを手動で入力することがサポートされないのは明白で、未定義の動作が発生する可能性があります。

- 無効な NFS 設定（または、誤って設定されている NFS サーバでのサービスを示している設定）をすると、通常、設定を適用するプロセスが失敗します。OpAdmin でのこの設定を修正して再適用すると成功します。
- **nfsnobody** による書き込みへのファイルの公開は安全です。**nfsnobody** または **nfsnobody** として実行されている Threat Grid アプライアンスでの唯一のプロセスは、データの暗号化に関するプロセスです。プレーンテキストデータは、最小権限の原則に基づいて、さまざまなサブツリーの個別のユーザアカウントで公開されます。アプライアンス上の PostgreSQL サービスは、Elasticsearch データやフリーザにアクセスできません。Elasticsearch サービスは、PostgreSQL やフリーザデータにアクセスできません。

- **nfsnobody**アカウントを使用すると、設定が簡素化され、カスタマーサイトごとに**idmap.conf**を構築する必要がなくなり、ローカルとリモートのアカウント名が一緒にマッピングされます。

ファイル システム

Threat Grid アプライアンス（v2.7 以降）では、プライマリファイルシステムとして XFS が使用されます。リセットされていない古いアプライアンスで使用されていたZFSファイルシステムは使用されません。この変更は、特に記載されている場合を除き、既存のアプライアンスには影響しません（「データリセットプロセス」を参照）。

バックアップ ストレージ要件

バックアップストアに合計で 5.6 TB を超えるストレージは必要ありません。バックアップ ストアは、次のコンポーネントで構成されています。

- **オブジェクトストア**：通常、使用されるストレージの大部分を占めています。バックアップストアの一括コンポーネントでのデータ保持は、使用中のThreat Gridアプライアンスリリース向けに文書化されたものと同じポリシーと制限に従っており、このコンポーネントの最大ストレージ使用量は 4.1 TB です。『Threat Grid Appliance Data Retention Notes』を参照してください。
- **PostgreSQL データベースストア**：PostgreSQL ストアの 2 つの完全バックアップと、保持されている完全バックアップのうち一番古いものから再生するのに十分な一連の WAL ログが含まれます。合計 500 GB 未満にする必要があります。
- **Elasticsearch スナップショットストア**：合計 1 TB 未満にする必要があります。

バックアップで予想される成果

次のバックアップで予想される成果を考慮する必要があります。

バックアップに含まれるもの

Threat Gridアプライアンスのバックアッププロセスの初回リリースには、お客様所有の次のバルクデータが含まれます。

- Samples
- 分析結果、アーティファクト、フラグ付き
- アプリケーション層の（OpAdmin ではない）組織およびユーザ アカウントのデータ。
- データベース（ユーザおよび組織を含む）

- Face または Mask ポータルの UI 内で行われた設定

バックアップに含まれないもの

次のものは、Threat Grid アプライアンスのバックアッププロセスの初回リリースに含まれません。

- [System logs]
- 以前にダウンロードおよびインストールした更新
- SSL キーと CA 証明書を含む、アプライアンス OpAdmin インターフェイスでの設定

その他の予想される成果

バックアッププロセスに関するその他の考慮事項は次のとおりです。

- PostgreSQL ベースバックアップは 24 時間サイクルで実行されます。データベースのバックアップの復元はできません。少なくとも 1 回正常に完了するまで警告が表示されます。
- Elasticsearch バックアップは 5 分ごとに段階的に行われます。
- Freezer バックアップは、進行中のバックアップから失われたオブジェクトを処理するために、24 時間ごとに後続のジョブを使用して継続的に実行されます。
- 新しいキーを生成すると、新しい独立したバックアップストアが作成されます。オリジナルのように、この新しいストアは、24 時間サイクルのベース バックアップが行われるまで有効になりません。

バックアップ データの保持

バックアップの際、次のようにデータが保持されます。

- **PostgreSQL**：最後の 2 つの正常なバックアップと、それらのバックアップ以降のすべての WAL セグメントが保持されます。
- **Elasticsearch**：最新の 5 分ごとのスナップショット 2 回分が保持されます。
- **バルクストレージ**：単一の Threat Grid アプライアンス向けに使用され文書化されるものと同じ保持ポリシーが、共有ストアに対して使用されます。

長期間にわたって履歴データを保持する場合は、ファイルシステムレイヤまたはブロックレイヤのスナップショットをサポートする NFS サーバを使用することを強くお勧めします。

データベースのベースバックアップは、新しいベースバックアップが正常に作成されるまで保持されます。

（注） バルクストレージでの障害発生後のリセット時に使用するため、仮想マシンイメージのバックアップコピーが RAID-1 ストレージアレイ上に作成されます。初期の Cisco Threat Grid アプライアンスモデル（UCS C220-M3 プラットフォームをベースとする）は、後のモデルよりもストレージが小さく、Threat Grid アプライアンス v2.9 のインストール後に、他のユニットが使用できる空き容量が、RAID-1 ファイルシステムのディスク容量の 25 % 未満になる可能性が高くなります。その場合、サービス通知がトリガーされます。

後のモデルのハードウェアで、v2.9 リリースのインストール後に、RAID-1 アレイの空きストレージが 25 % 未満になる場合、これは正常な状態ではないため、カスタマーサポートに問い合わせる必要があります。

保持期限の厳密な適用

TGSH（v2.6 以降）の **strict_retention** オプションを使用すると、分析済みのアーティファクトを 15 日間を超えて保存しないことにより、保持期間の制限を厳密に適用することができます。このオプションを有効にすると、最初の夜間プルーニングの際に、15 日間を超えて保存されているファイルが削除されます。

（注） 15 日の期間を設定または変更することはできません。

アーティファクトとは、サンプル自体と、サンプルから生成されたその他のものを意味します。アーティファクトには分析レポートの HTML が含まれていません。分析レポートの HTML は、別途記載されているとおり、最初から制限の対象となります。アーティファクトには、データベースエントリや検索インデックスも含まれません。

strict_retention オプションは、デフォルトでは無効（false）になっています。15 日後のアーティファクトのハードプルーニングを有効にするには、**TGSH** でこのオプションを true に設定します。

configure set strict_retention true

バックアップ プロセスの概要

Threat Grid アプライアンスのバックアッププロセスは、次の手順で構成されます。

ステップ 1 「NFS 要件」に従って、バックアップのターゲットディレクトリを作成します。

ステップ 2 『*Cisco Threat Grid Appliance Setup and Configuration Guide*』の説明に従って、OpAdmin の [**NFS**] ページ（**[Configuration] > [NFS]**）に入力します。

ステップ 3 NFS の設定が完了したら、生成された暗号キーをダウンロードします。バックアップデータを復元するには、このキーが必要です。

重要 お客様には、暗号キーをバックアップして安全に保管する責任があります。Threat Grid にはコピーが保持されません。このキーを使用せずにバックアップを完了することはできません。

ステップ 4 「バックアップ復元ターゲットとしての Threat Grid アプライアンスのリセット」の説明に従って、バックアップ復元ターゲットをリセットします。

ステップ 5 バックアップコンテンツの復元 （9 ページ） の説明に従って、バックアップデータを復元します。

バックアップ頻度

データのバックアップ頻度は次のとおりです。

- サンプル、アーティファクト、レポートのバルクストレージの場合、コンテンツは継続的にバックアップされます。さらに、パスが実行されると、24時間サイクルで不足しているコンテンツが検索されて転送されます。
- PostgreSQL データベースの場合、ベースバックアップが 24 時間サイクルで作成され、その後は、新たに書き込まれたデータベースコンテンツが 16 MB のしきい値に達するごとに、または 5 分ごとに、増分コンテンツが継続的に追加されます。
- Elasticsearch データベースの場合、コンテンツはバックアップ ストアに 5 分間サイクルで段階的に追加されます。

バックアップの頻度を制御または調整することはできません。頻度を変更すると、ストレージ使用率、復元の処理時間、パフォーマンスのオーバーヘッドに関する想定が無効になるためです。

バックアップ復元ターゲットとしての Threat Grid アプライアンスのリセット

アプライアンスを復元ターゲットとして使用する前に、事前設定された状態にする必要があります。アプライアンスは、この状態で出荷されます。ただし、設定した後に事前設定された状態に戻すには、明示的な管理操作が必要になります。

⚠

注意 このプロセスを実行すると、お客様が所有するデータが破棄されます。タスクを実行する前にすべてのマニュアルを読み、慎重に作業を続行してください。.

（注） リセットは、リカバリモードで使用できるセキュアワイプと同じものではありません。DLP再イメージ化センターに発送する前に、お客様が所有するデータをマシンから完全に削除するのに適しているのは、リカバリモードでのセキュアワイプのみです。ただし、リカバリモードでのセキュアワイプは、リセットに代わるものではありません。セキュアワイプでは、再イメージ化されるまで使用できなくなるアプライアンスが処理され、リセットでは、アプライアンスがバックアップを復元する準備が行われます。

データリセットプロセス

データリセットプロセスが Threat Grid アプライアンス v2.7 以降で更新され、さらに包括的になりました。すべての顧客関連データの確実な破壊を保証するため、（リカバリ ブートローダー メニューの）ワイププロセスは依然として必要ですが、リセットプロセスにより、オペレーティングシステムのログや、そのまま残されていた他の状態がクリアされるようになりました。

Threat Grid アプライアンスが正常にリセットされると、新しいランダム生成のパスワードがコンソールに表示されるようになりました（新規インストール時の動作と同じです）。この改善されたプロセスでは、複数回再起動するようになっています。また、リカバリモードからの起動が可能になりました（以前のプロセスでは、通常の操作で起動した場合にのみ正常に起動することが可能でした）。

Threat Grid アプライアンスのデータがリセットされると、データストアは、ZFS ファイルシステムから XFS ファイルシステムに変更されます。これにより、前方互換性が向上し、サービス単位の I/O 使用率のモニタリングに OS レベルのサポートが提供されるようになります。

また、更新されたデータリセットプロセスでは、システム SDD への新規インストールに必要なすべてのコンテンツを格納するのに十分なストレージが必要です。既存のデータは、このコンテンツの存在と有効性が確認された後にのみ削除されます。長期間にわたって使用されているシステム（特に第 1 世代のハードウェア）の場合、すぐに使用できる十分な空き容量がない可能性があります。その場合は、必要に応じてカスタマーサポートの支援を受けることができます。

ターゲットアプライアンスを事前設定された状態に戻す

メーカーから届いたばかりのシステムで復元するわけではない場合、既存のデータと NFS 関連の設定をシステムから消去することによって、復元のターゲットアプライアンスを事前設定された状態に戻す必要があります。

ステップ 1 Threat Grid アプライアンス TTY または SSH を使用して TGSH ダイアログにアクセスします。

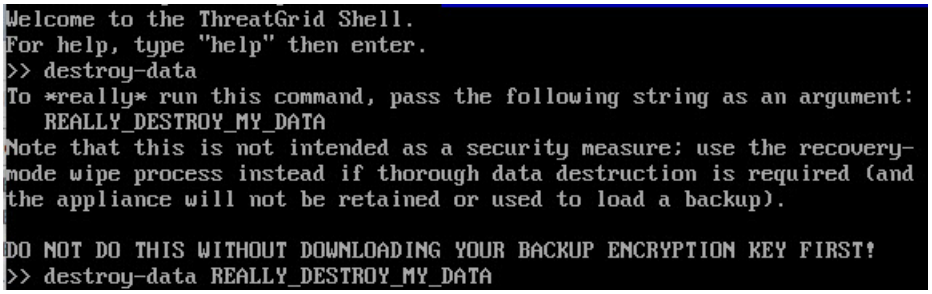
ステップ 2 [**CONSOLE**] オプションを選択して「**tgsh**」と入力します。

（注） リカバリモードによる「**tgsh**」の入力は、この使用例には適していません。

ステップ 3 **tgsh** プロンプトで、コマンド `destroy-data` を入力します。プロンプトをよく読んで、指示に従ってください。

注意 このコマンドを実行すると、元に戻すことはできません。すべてのデータが破棄されます。

図 *1 : destroy-data REALLY_DESTROY_MY_DATA* コマンドと引数



次のデータが破棄されます。

- Samples
- 分析結果、アーティファクト、フラグ付き
- アプリケーションレイヤ（OpAdmin ではない）の組織およびユーザアカウントのデータ
- データベース（ユーザおよび組織を含む）
- Face または Mask ポータルの UI 内で行われた設定
- NFS の設定とログイン情報
- NFS に使用される暗号キーのローカルコピー

復元中のバックアップにアクティブに書き込んでいるアプライアンス

別のシステムまたは Threat Grid アプライアンスが、復元中のバックアップにアクティブに書き込みを行っている場合（実稼働でアクティブに使用されている第 2 マスター Threat Grid アプライアンスが書き込んでいるコンテンツのテスト復元など）、その Threat Grid アプライアンスを事前設定された状態に戻します。

ステップ 1 データストアの一貫した書き込み可能なコピーを生成します。

ステップ 2 テスト復元を実行している Threat Grid アプライアンスを、継続的に書き込まれているストアではなく、書き込み可能なコピーにポイントします。

Threat Grid アプライアンスが事前設定された状態の場合は、「バックアップコンテンツの復元」で説明されているとおり、バックアップストアのターゲットとして機能します。

バックアップコンテンツの復元

重要 復元プロセスの間、システムをサンプル送信に使用することはできません。

バックアップコンテンツを復元するには、次の手順を実行します。

ステップ 1 OpAdmin ポータルで、**[Configuration] > [NFS]** をクリックして [**NFS**] ページを開きます。

ステップ 2 [**Upload**] をクリックして、バックアップが作成されたサーバの設定時に生成されたバックアップキーを取得します。

このキーがバックアップの作成に使用されたキーと正確に一致する場合、OpAdmin ポータルに表示される **キー ID** は、設定されたパス内のディレクトリ名と一致している必要があります。インストールウィザードによってバックアップキーと一致するディレクトリが検索され、そのディレクトリが検出されると、検出された場所へのデータの復元が開始されます。

（注） 経過表示バーは表示されません。データの復元に必要な時間は、バックアップのサイズや他の要因によって異なります。テストによると、1.2 GB の復元は迅速ですが、1.2 TB の復元には 16 時間以上かかります。大規模な復元の場合、インストールがハングしているように見えることがありますが、しばらくお待ちください。OpAdmin に復元が成功したと表示され、アプライアンスが起動します。

ステップ 3 復元されたデータが元のデータと同じであることを確認します。

バックアップおよび復元に関する注意事項

- 復元プロセス中にサンプル送信を使用することはできません。
- バックアップは、セットアップ ウィザードからのみ復元できます。
- 以前に使用したものと同じ NFS ストアと暗号キーを、最初のプロセスと同じプロセスで設定します。
- 以前の NFS ストアと暗号キーを使用して Threat Grid アプライアンスを設定すると、復元がトリガーされます。
- プライマリ Threat Grid アプライアンスの動作中に別の Threat Grid アプライアンスで復元プロセスをテストするには、バックアップストアの一貫したスナップショットのコピーを作成し、（アップロードされた暗号化キーを使用して）新しい Threat Grid アプライアンスをポイントします。

重要 特定のアクティブなバックアップストアのデータを使用して一度に実行できるのは、1台のサーバのみです。

バックアップに関連するサービスの通知

バックアッププロセス中に、次のサービス通知が表示される場合があります。

- 「**Network storage not mounted（ネットワークストレージがマウントされていません）**」：バックエンドとして使用されているネットワーク ファイル システムが完全に動作していることを確認して、OpAdmin で設定を再適用するか、アプライアンスを再起動します。
- 「**Network storage not working（ネットワークストレージが動作していません）**」：バックエンドとして使用されているネットワーク ファイル システムが完全に動作していることを確認します。システムが NFS サーバの問題の修正から 15 分以内に回復しない場合は、アプライアンスを再起動してください。
- 「**Backup file system access failure（バックアップ ファイル システムのアクセスに失敗しました）**」：カスタマーサポートまでお問い合わせください。
- **PostgreSQL のバックアップが見つかりません**：これは、バックアップ ストアが設定された時間内のポイントと（自動的に24時間サイクルで実行される）最初のベースバックアップが行われる時間内のポイント間で正常な状態です。これが完了するまで、バックアップ完了とは見なされず、復元することはできません。このメッセージが 48 時間を超えて続く場合または続く場合に限り、カスタマー サポートに連絡してください。
- 「**Newest PostgreSQL base backup more than two days old（最新の PostgreSQL ベース バックアップは 3 日以上前です）**」：システムが PostgreSQL の新しいベースバックアップの生成に成功していないことを示します。修正されない場合、（古くなりつつあるバックアップポイントから復元するために必要な書き込みの完全なチェーンを保持するための）バックアップストアでの使用が制限されなくなり、行われる復元に必要な処理時間が許容できる長さを超えます。カスタマー サポートに連絡してください。
- 「**Backup Creation Messages（バックアップ作成メッセージ）**」：バックアップの開始またはトリガーの際に検出されたエラーを反映しています。
- **非アクティブの ES バックアップ（作成）**：Elasticsearch が開始して、バックアップ ストアが使用不可能であることを示します。この状態は、アプライアンスを再起動するか、（NFS と暗号化サービスが機能している場合）**TGSH** にログインして `restart elasticsearch.service` コマンドを実行することで改善できます。
- 「**Backup Maintenance Messages（バックアップ メンテナンス メッセージ）**」：以前に作成されたバックアップのステータスを確認する際に検出されたエラーを反映しています。
- 「**ES Backup (Maintenance) snapshot (...) status FAILED（ES バックアップ（メンテナンス）スナップショット（...）のステータスが [FAILED] になっています）**」：Elasticsearch データベースのバックアップの最近の更新で、インデックスが正常に書き込まれなかった

ことを示します。NFS サーバが機能していて空き領域があることを確認します。問題を特定できず、解決しない場合は、カスタマー サポートにお問い合わせください。

- 「**ES Backup (Maintenance) snapshot (...) status INCOMPATIBLE（ES バックアップ（メンテナンス）スナップショット（...）のステータスが [INCOMPATIBLE] になっています）**」：アプライアンスのアップグレードで新しいバージョンの Elasticsearch がインストールされた直後にのみ発生します。バックアップストアがアップグレードされて、新しいリリースとの互換性を持つようになるまで表示されます。この状態の間に障害が発生した場合、互換性のないバックアップからの復元には、カスタマーサービスの支援が必要になることがあります。
- 「**ES Backup (Maintenance) snapshot (...) status PARTIAL（ES バックアップ（メンテナンス）スナップショット（...）のステータスが [PARTIAL] になっています）**」：本文に次の 2 つのメッセージのうちのいずれかが含まれています。「No prior successful backups seen, so retaining（以前に成功したバックアップが見つからないため、そのまま保持します）」（バックアップは存在するものの部分的でしかない場合）。または「Prior successful backups exist, so removing（以前に成功したバックアップが存在するため、削除します）」（後で再試行するために部分的なバックアップを破棄しようとしている場合）。
- 「**ES Backup (Maintenance) - Backup required (...) ms（ES バックアップ（メンテナンス）：バックアップに（...）分間かかります）**」：バックアップに 60 秒を超える時間が必要な場合に発生します。これは必ずしもエラーとは限りません。Elasticsearch では定期的なメンテナンスを実行し、これがアイドル状態のシステムにも重要な書き込み負荷を発生させることがあります。ただし、これが負荷が少ない期間で一貫して発生する場合は、ストレージ パフォーマンスを調査するか、サポートが必要な場合はカスタマー サービスに連絡してください。
- 「**ES Backup (Maintenance) - Unable to query Elasticsearch snapshot status（ES バックアップ（メンテナンス）：Elasticsearch スナップショット ステータスのクエリを実行できませんでした）**」：Elasticsearch に接続できませんでした。この障害は、バックアップの作成が正常に開始された後に発生します。一般に、他のアプライアンスの障害と同時に発生するため、それらの問題の修復に重点を置く必要があります。アプライアンスが他の点では完全に機能しているときにこのエラーが発生し、自分では解決できない場合は、カスタマー サポートに問い合わせてください。