



クラスタ

この章では、Threat Grid アプライアンスのクラスタリング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 アプライアンスのクラスタリングについて \(1 ページ\)](#)
- [クラスタの構築の概要 \(5 ページ\)](#)
- [Threat Grid アプライアンスのクラスタの開始 \(8 ページ\)](#)
- [Threat Grid アプライアンスのクラスタへの結合 \(17 ページ\)](#)
- [タイブレーカーノードの指定 \(22 ページ\)](#)
- [クラスタノードの削除 \(23 ページ\)](#)
- [クラスタのサイズ変更 \(23 ページ\)](#)
- [障害許容範囲 \(24 ページ\)](#)
- [障害の回復 \(25 ページ\)](#)
- [API/使用の特性 \(25 ページ\)](#)
- [運用/管理の特性 \(25 ページ\)](#)
- [サンプルの削除 \(25 ページ\)](#)

Threat Grid アプライアンスのクラスタリングについて

複数の Threat Grid アプライアンスをクラスタ化する機能は、v2.4.2 以降で使用できます。クラスタ内の各 Threat Grid アプライアンスは、共有ファイルシステムにデータを保存し、クラスタ内の他のノードと同じデータを保持します。

クラスタリングの主な目標は、複数の Threat Grid アプライアンスを1つのクラスタ (2～7 ノードで構成) に結合することによって、単一のシステムのキャパシティを増やすことです。さらにクラスタリングは、クラスタのサイズに応じて、クラスタ内の1つ以上のマシンが障害から回復するのをサポートする点でも役立ちます。

クラスタのインストールまたは再設定について不明な点がありましたら、データの破壊を避けるため、シスコサポートまでお問い合わせください。

クラスタリングの機能

Threat Grid アプライアンスのクラスタリングには、次の機能があります。

- **共有データ**：クラスタ内のすべてのThreatGridアプライアンスは、スタンドアロンであるかのように使用できます。それぞれが同じデータにアクセスして表示することができます。
- **サンプル送信処理**：送信されたサンプルは、いずれかのクラスタメンバーで処理され、他のメンバーは分析結果を確認できます。
- **レート制限**：各メンバーの送信レート制限を積算した値がクラスタの制限になります。
- **クラスタサイズ**：推奨されるクラスタのサイズは、3、5、または7メンバーです。2、4、6ノードのクラスタはサポートされますが、ノードが1つ多いものの機能が低下したクラスタ（1つ以上のノードが動作していないクラスタ）と同様の可用性になります。
- **タイブレーカー**：クラスタに偶数のノードを含めるように設定すると、タイブレーカーとして指定されたノードは、どのノードがプライマリデータベースを持つかを決定するイベントで二番手に位置付けられます。

クラスタ内の各ノードにはデータベースが含まれていますが、プライマリノードのデータベースのみが実際に使用されます。プライマリノードがダウンした場合、他のノードがその役割を引き継ぐ必要があります。条件を設定していると、ノードがちょうど半分失敗したとき、ただし、条件が失敗したノード上ではない場合のみ、クラスタがダウンするのを防止できます。

奇数クラスタには、関連付けられた投票はありません。奇数クラスタでは、（タイブレーカーではない）ノードがクラスタからドロップされた場合にのみ、タイブレーカーロールが関係することになります。その場合、クラスタは偶数クラスタになります。



(注) この機能は、2ノードのクラスタに対してのみ十分にテストされています。

クラスタリングの制限事項

Threat Grid アプライアンスのクラスタリングには、次の制限事項があります。

- 既存のスタンドアロンThreatGridアプライアンスのクラスタを構築する場合、最初のノード（初期ノード）のみがそのデータを保持できます。クラスタに既存のデータをマージすることは許可されないため、他のノードは手動でリセットする必要があります。

「バックアップ復元ターゲットとしてのThreatGridアプライアンスのリセット」に記載されているとおり、`destroy-data` コマンドを使用して既存のデータを削除します。



重要 シスコに返却してイメージを再作成しない限りアプライアンスが稼働しなくなるため、ワイプアプライアンス機能は使用しないでください。

- ノードを追加または削除すると、クラスタのサイズとメンバーノードのロールによって、短時間停止することがあります。
- M3 サーバのクラスタリングはサポートされていません。ご不明な点がございましたら、[Threat Grid サポート](#)までお問い合わせください。

クラスタリングの要件

Threat Grid アプライアンスをクラスタリングする場合、次の要件を満たす必要があります。

- **バージョン**：サポートされている設定でクラスタをセットアップするには、すべての Threat Grid アプライアンスが同じバージョンを実行している必要があります。常に使用可能な最新のバージョンにしておきます。
- **Clust インターフェイス**：各 Threat grid アプライアンスには、クラスタ内の他の Threat Grid アプライアンスへのダイレクトインターコネクトが必要です。クラスタ内の各 Threat Grid アプライアンスの Clust インターフェイススロットに SFP+ を設置する必要があります（スタンドアロン構成の場合には該当しません）。
ダイレクトインターコネクトとは、すべての Threat Grid アプライアンスが同じレイヤ 2 ネットワークセグメント上にあり、他のノードに到達するためのルーティングが不要で、大幅な遅延やジッターがないことを意味します。ノードが単一の物理ネットワークセグメント上にないネットワーク トポロジはサポートされていません。
- **エアギャップ展開の場合は非推奨**：デバッグの複雑さが増大するため、エアギャップ展開や、顧客がデバッグへの L3 サポートアクセスを提供できない、または提供を望まないシナリオでは、アプライアンスのクラスタリングは推奨されません。
- **データ**：Threat Grid アプライアンスは、データが含まれていない場合にのみクラスタに結合できます（初期ノードのみがデータを保持できます）。既存の Threat Grid アプライアンスをデータのない状態に移行するには、データベース リセット プロセスを使用する必要があります（v2.2.4 以降で使用可能）。



重要 破壊的なワイプアプライアンスプロセスを使用しないでください。このプロセスにより、すべてのデータが削除され、シスコに返却してイメージを再作成しない限りアプライアンスが稼働しなくなります。

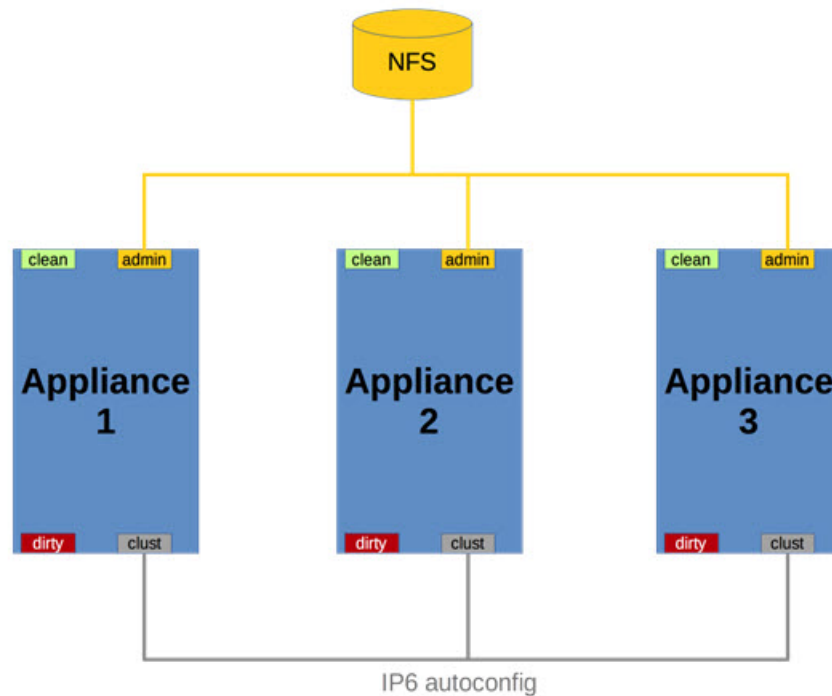
- **SSL 証明書** : 1つのクラスタノードにカスタム CA によって署名された SSL 証明書をインストールする場合、他のノードすべての証明書も同じ CA によって署名されている必要があります。

ネットワークと NFS ストレージ

Threat Grid アプライアンスをクラスタリングするには、ネットワークおよび NFS ストレージに関して次の点を考慮する必要があります。

- Threat Grid アプライアンスクラスタでは、NFS ストアを有効にして設定する必要があります。NFS ストアが管理インターフェイス経由で使用可能で、すべてのクラスタノードからアクセス可能になっている必要があります。
- 各クラスタは、キーが 1 つある 1 つの NFS ストアによってバックアップする必要があります。既存の Threat Grid アプライアンスのデータを使用して NFS ストアを初期化することはできますが、クラスタの動作中は、クラスタのメンバーではないシステムからアクセスすることはできません。
- NFS ストアはシングルポイント障害であり、そのロールに見合った、冗長性があり信頼性の高い機器を使用することが不可欠です。
- クラスタリングに使用される NFS ストアは、遅延を常に低い状態に保つ必要があります。

図 1: クラスタリングネットワーク構成図



クラスタの構築の概要

サポートされている方法でクラスタを構築するには、すべてのメンバーが同じバージョンである必要があります。バージョンは利用可能な範囲で常に最新のものにする必要があります。これは、すべてのメンバーが完全に更新されるように最初にスタンドアロンを構築する必要があることを意味します。

クラスタリングの前に Threat Grid アプライアンスがスタンドアロンマシンとして使用されている場合、最初のメンバーのデータのみを保持できます。その他は構築の一部としてリセットする必要があります。

最初のノードを使用して新しいクラスタを開始し、他の Threat Grid アプライアンスをそのクラスタに結合します。新しいクラスタを開始するために使用できる 2 つの異なるパスがあります。

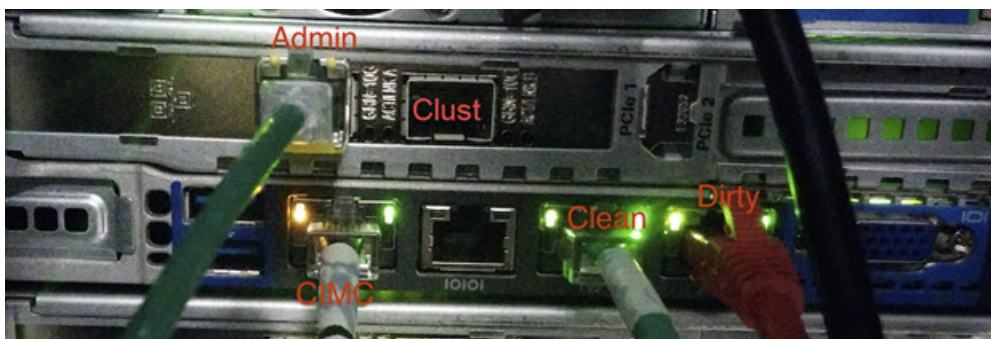
- 既存のスタンドアロン Threat Grid アプライアンスを使用して、新しいクラスタを開始します。
- 新しい Threat Grid アプライアンスを使用して、新しいクラスタを開始します。

Clust インターフェイスの設定

クラスタ内の各アプライアンスには、Clust インターフェイス用の SFP+ を追加する必要があります。

4 番目の (非管理) SFP ポートに SFP+ モジュールを取り付けます。

図 2: Cisco UCS M4 C220 の Clust インターフェイスの設定



クラスタリングの設定

クラスタは、[Clustering] ページ ([Configuration] > [Clustering]) の OpAdmin ポータルで設定および管理されます。このセクションでは、アクティブで正常なクラスタを理解するための [Clustering] ページのフィールドについて説明します (スクリーンショットには 3 つのノードを含むクラスタが示されます)。

図 3: アクティブクラスタのクラスタリング設定

Configure your Threat Grid Appliance to use Clustering.

Clustering Prerequisites Status

Installation Status	● Complete
Interface Status	✓ Available
NFS Status	✓ Active
Clustering Status	● Clustered

Start Cluster Join Cluster Make Tiebreaker

Clustering Components Status

ES	● replicated	PG	● replicated
----	--------------	----	--------------

Cluster Nodes Status

Appliance ID	Pulse	Ping	Consul	Tiebreaker	PG Master	Action
FCH1831V0F2	✓	✓	✓	✓	✓	✕
FCH1832V319	✓	✓	✓	●	●	✕
FCH1831V0JQ	✓	✓	✓	●	●	✕

Save

前提条件ステータスのクラスタリング

- **[Installation Status]** : Threat Grid アプライアンスのインストールステータス。ステータスが **[Complete]** になっている（完全にセットアップおよび設定されている）必要があります。
- **[Interface Status]** : Clust ネットワーク インターフェイスのステータス。
- **[NFS Status]** : NFS のステータス。ステータスが **[Available]** になっている必要があります。
- **[Clustering Status]** : Threat Grid アプライアンスがクラスタノードとスタンドアロンのどちらになっているかを示します。
 - **[Standalone (unsaved)]** : クラスタの一部として、またはスタンドアロンの Threat Grid アプライアンスとして明確に設定されていません。クラスタリングの前提条件が満たされている場合は、初期セットアップウィザードでこの選択を行います。
 - **[Standalone]** : スタンドアロンノードとして設定されています。リセットしないとクラスタの一部として設定できません。
 - **[Clustered]** : 1 つ以上の他の Threat Grid アプライアンスを含むクラスタに結合しています。

コンポーネントステータスのクラスタリング

- **[ES]** : Elasticsearch。検索機能を必要とするクエリに使用されるサービス。
- **[PG]** : PostgreSQL。最新の確定的なデータ（アカウントルックアップなど）が必要なクエリに使用されるサービス。

両方のサービスは、次のステータス値のいずれかで説明されます。

- **[Replicated]** : すべてが正常に動作しています。また、障害時に引き継ぎに必要なすべてのものも所定の位置にあります。アプライアンスは障害を許容して操作を続行できます。複製済みの状態は、障害発生時のダウンタイムがゼロになるという意味ではありません。むしろ、障害には、ゼロのデータ損失と制約ダウンタイムが伴います（通常の場合で1分未満、失敗した特定のクラスタ ノードでのアクティブな分析を除く）。

ノードがダウンするメンテナンス操作は、クラスタが複製された状態のときにのみ実行する必要があります。

完全に複製されたクラスタの場合、リカバリは自動的に行われ、通常のシナリオで完了するのに必要な時間は1分未満です。

- **[Available]** : すべてが正常に動作しており、参照サービスを使用できます（APIおよびユーザ要求を処理できます）が、複製されません。
- **[Unavailable]** : 非機能サービスとして知られています。

ステータスの色 :

- 緑色 : 複製済み
- 黄色 : 利用可能
- 赤色 : 利用不可
- 灰色 : 不明

詳細については、Cisco.com の「[Threat Grid Appliance Clustering FAQ](#)」を参照してください。

クラスタ ノードステータス

緑色のチェックマークは、ノードが稼働中で正常であることを示します。

赤色の X は、何かがまだ実行されていないか、正常でないことを示します。

- **[Pulse]** : （初期設定中ではなく、サービスを実行している間に）ノードがアクティブに接続されていて、NFS ストアを使用しているかどうかを示します。
- **[Ping]** : Clust インターフェイス上でクラスタノードを認識できるかどうかを示します。
- **[Consul]** : ノードがコンセンサスストアに参加しているかどうかを示します。参加には、Clust でのネットワーク接続と互換性のある暗号キーの両方が必要です。

- **[Tiebreaker]** : ノードをタイブレーカーに指定します。タイブレーカーは、クラスタのプライマリノードが選択される際に決定票を投じます。「[タイブレーカーノードの指定](#)」を参照してください。
- **[Keep Standalone]** : Threat Grid アプライアンスがクラスタ内のノードとして設定されていないことを示します。このオプションを選択すると、ユーザは、クラスタに結合していない Threat Grid アプライアンスの OpAdmin 設定ウィザードプロセスを完了できます。

Thread Grid アプライアンスのクラスタの開始

Threat Grid アプライアンスのクラスタを構築する場合、最初のノードが既存のスタンドアロン Threat Grid アプライアンスまたは新しいアプライアンスのいずれかであるクラスタを開始する必要があります。ご使用の環境に応じたクラスタの開始については、該当するセクションを参照してください。

既存のスタンドアロンアプライアンスを使用したクラスタの開始

既存のスタンドアロン Threat Grid アプライアンスからクラスタの構築を開始できます。この方法では、あるマシンの既存のデータを保存し、そのデータを使用して新しいクラスタを開始できます。クラスタが開始される NFS で、既存のバックアップが使用可能になっている必要があります。



- (注) クラスタに結合される他のすべてのノードから、結合前にデータを削除する必要があります。追加されるノードのデータをクラスタにマージすることはできません。



- (注) v2.4.3 よりも前のリリースで、NFS にバックアップされたデータを含むスタンドアロン Threat Grid アプライアンスの場合、新しいクラスタの初期ノードにするために、データベースのリセットとバックアップからの復元を行う必要がなくなりました。以前のバージョンの Threat Grid アプライアンスをお持ちの場合、新しいクラスタを開始する前に、v2.4.3 以降にアップグレードしてからリセット操作を実行することをお勧めします。

最初のノードを対象にクラスタを開始するには、次の手順を実行します。

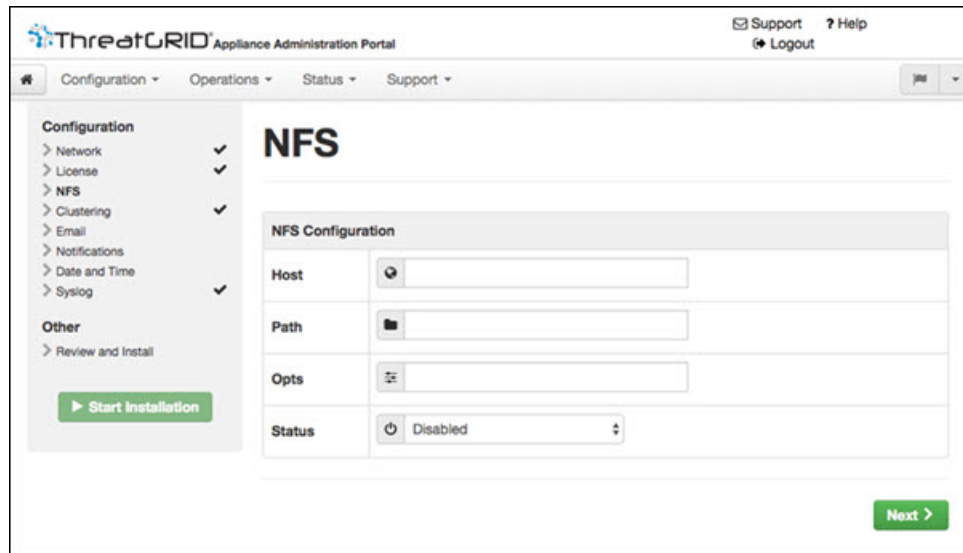
ステップ 1 Threat Grid アプライアンスを最新バージョンに完全に更新します。現在実行されているバージョンによっては、最新バージョンになるまでに複数の更新サイクルが必要になる場合があります。

ステップ 2 まだ実行していない場合は、NFS へのマシンのバックアップを設定します。

- (注) この手順では、デフォルト Linux NFS サーバの実装について説明します。サーバの設定によっては手順の調整が必要になる場合があります。

- a) OpAdmin ポータルで、[Configuration] > [NFS] をクリックして [NFS] ページを開きます。

図 4: NFS の設定



The screenshot shows the ThreatGRID Appliance Administration Portal. The top navigation bar includes 'Configuration', 'Operations', 'Status', and 'Support'. The left sidebar lists various configuration categories: Network, License, NFS, Clustering, Email, Notifications, Date and Time, Syslog, and Other. The main content area is titled 'NFS' and contains an 'NFS Configuration' section with the following fields:

NFS Configuration	
Host	<input type="text"/>
Path	<input type="text"/>
Opts	<input type="text"/>
Status	<input type="text" value="Disabled"/>

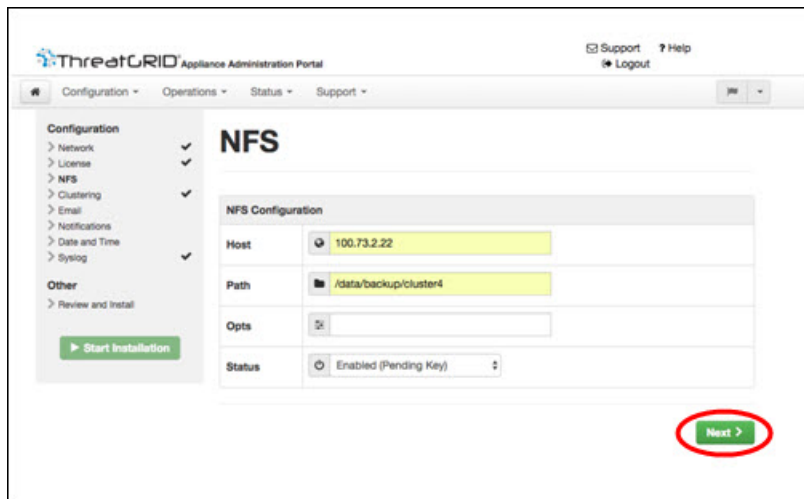
A 'Next >' button is located at the bottom right of the configuration area.

- b) 次のフィールドに入力します。

- **[Host]** : NFSv4 ホストサーバ。IP アドレスを使用することをお勧めします。
- **[Path]** : ファイルが保存される NFS ホストサーバ上の場所への絶対パス。これにはキー ID サフィックスは含まれません。自動的に追加されます。
- **[Oopts]** : このサーバで NFSv4 に対する標準 Linux のデフォルト値を変更する必要がある場合に使用される NFS マウントオプション。
- **[Status]** : ドロップダウンリストから **[Enabled (Pending Key)]** を選択します。

- c) [次へ (Next)] をクリックします。

図 5:有効化された NFS 設定（保留中のキー）



ページが更新され、[Generate] ボタンが使用可能になります。

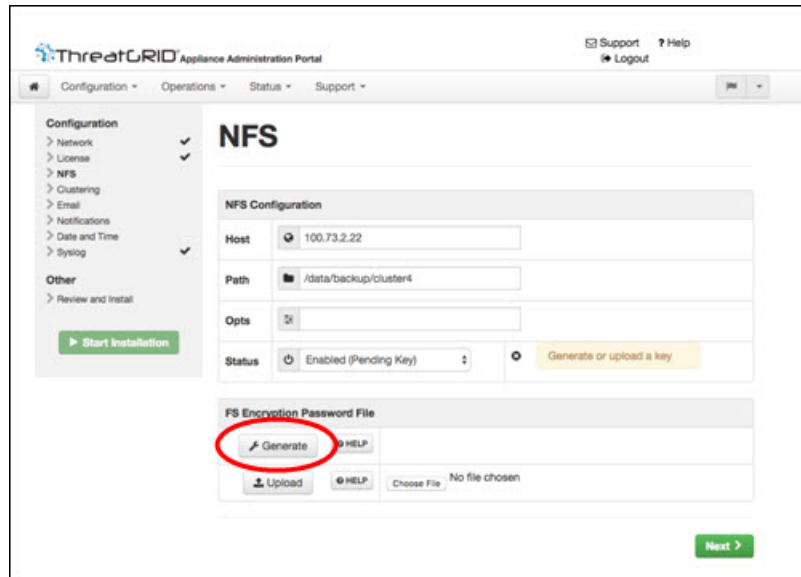
このページを初めて設定するときに、暗号キーの [Remove] ボタンと [Download] ボタンが表示されます。

[Upload] ボタンは、NFS が有効になっているものの、キーが作成されていない場合に使用できます。キーを作成すると、[Upload] ボタンが [Download] ボタンに変わります。キーを削除すると、[Download] ボタンが [Upload] ボタンに戻ります。

(注) 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、アップロード後に OpAdmin に表示される [Key ID] は、設定されたパス内の特定のディレクトリの名前と一致するはずで
 ず。暗号キーを使用せずにバックアップを復元することはできません。設定プロセスには、
 NFS ストアおよび暗号化データをマウントするプロセスと、NFS ストアのコンテンツからア
 プライアンスのローカル データストアを初期化するプロセスが含まれます。

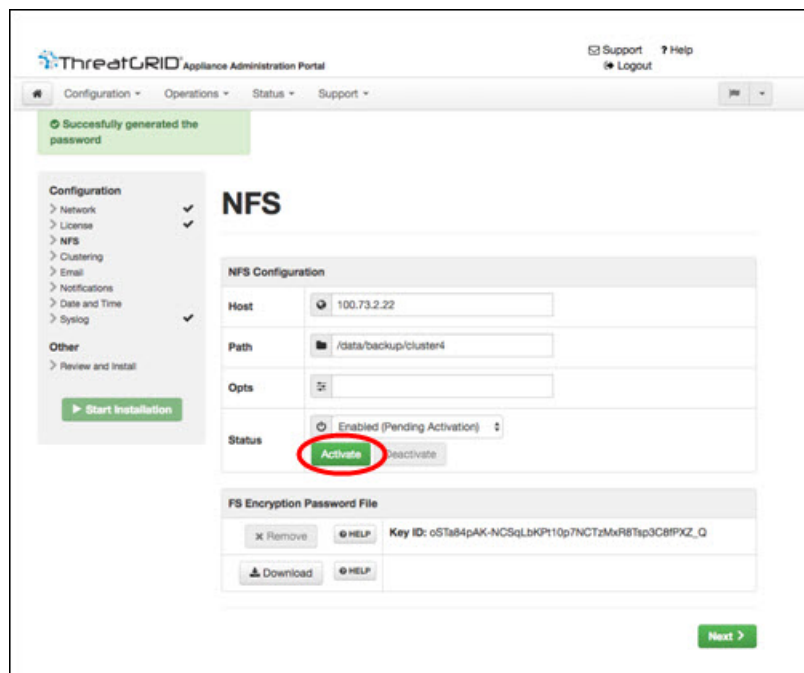
d) [生成 (Generate)] をクリックして、新しい NFS 暗号キーを作成します。

図 6:新しい NFS 暗号キーの生成



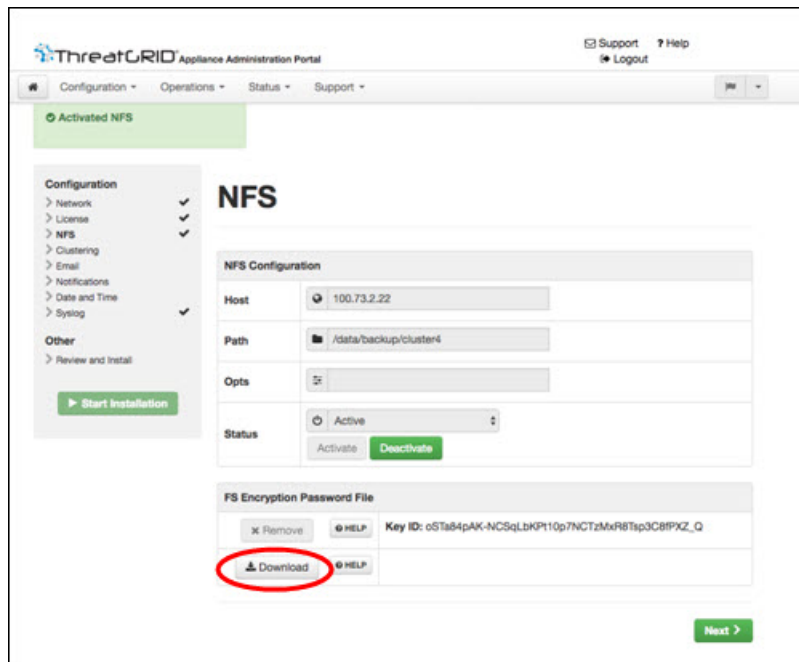
- e) [次へ (Next)]をクリックします。ページが更新されて [Key ID] が表示され、[Activate] ボタンと [Download] ボタンが使用可能になります。

図 7: NFS 設定のアクティブ化



- f) [Activate] をクリックします。アクティブ化には数秒かかります (ステータスインジケータは左下隅にあります)。[Status] が [Active] になります。

図 8: [Active]になった NFS



- g) **[Download]** をクリックして、バックアップの暗号キーをダウンロードします。安全な場所に生成したファイルを保存します。クラスタに追加のノードを結合するためのキーが必要です。

重要 この手順を実行しないと、次の手順ですべてのデータが失われます。

ステップ 3 必要に応じて設定を完了し、Threat Grid アプライアンスを再起動して、NFS バックアップ設定を適用します。

ステップ 4 バックアップを実行します。

- (注) 推奨どおりに、前もって少なくとも 48 時間バックアップを実行し、バックアップに問題が発生したことを示すサービス通知がなかった場合、次の手動による手順は不要です。

バックアップなどのサービス通知は、Threat Grid Portal UI の右上隅にあるアイコンで表示できます。「**There is no PostgreSQL backup yet (PostgreSQL バックアップがまだありません)**」というサービス通知が表示された場合は、手順を先に進めないでください。

再起動後に即座にバックアップを実行する場合は、完了していることを確認するために NFS に対するすべてのデータのバックアップを手動で開始する必要があります。手動バックアップコマンドの実行は、スタンドアロンボックスをクラスタに再構築する直前にバックアップを設定する場合にのみ必要です。

- a) **TGSH** を開き、次のコマンドを入力します。

```
service start tg-database-backup.service
service start freezer-backup-bulk.service
service start elasticsearch-backup.service
```

図 9: NFS に対する全データのバックアップの開始

```

:: [I]string([I]string("CONSOLE"))
Welcome to the ThreatGrid Shell.
For help, type "help" then enter.
>> help
COMMANDS:
  configure -- show|set: View or modify configuration variables
  conns     -- listening|open|all: Show open connections
  destroy-data -- Reset appliance to be a target for the restore process
  exit     -- Exit tgsh.
  halt    -- Halt appliance
  help    -- List available commands, or 'help COMMAND' for details.
  netctl  -- Configure the network
  netinfo -- routes|firewall|address|stats: Show network configuration and status
  opadmin -- import|check: Sync from, or validate, new configuration format
  passwd  -- Change password for this account
  ping    -- ping [-c count] [-I interface] host: ping a remote host
  poweroff -- Power off appliance
  queues  -- Show status of various application queues
  reboot  -- Reboot appliance
  service -- (status|start|stop|restart) [svc-name]: Toggle ThreatGRID services
  support-node -- status|start|stop|enable|disable: Toggle support node
  traceroute -- Determine the path used to a network location
  version -- Shows appliance version
>> service start tg-database-backup.service
>> service start freezer-backup-bulk.service
>> service start elasticsearch-backup.service
>>
    
```

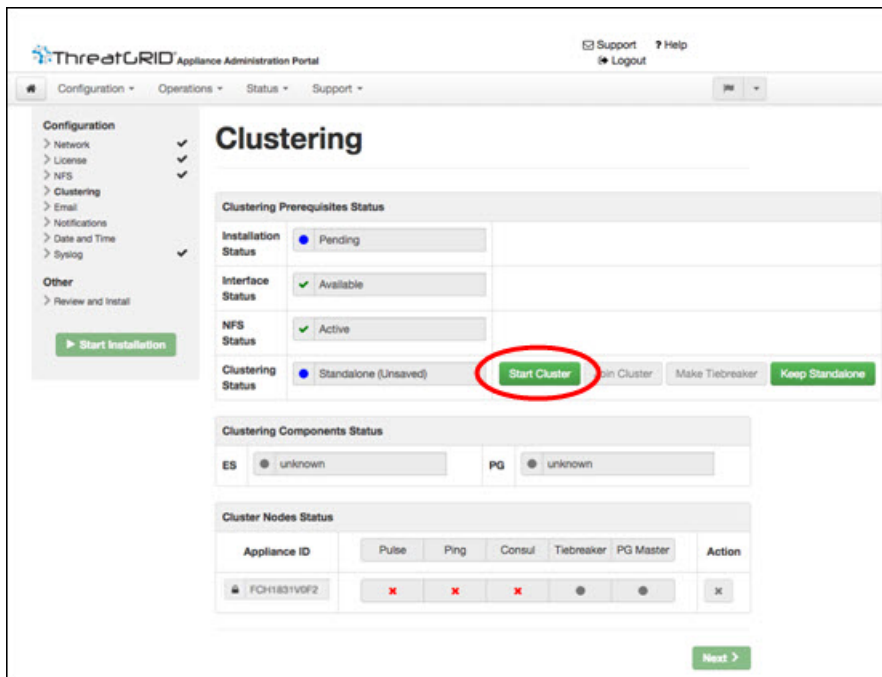
b) 最後のコマンドが返された後、約 5 分間待機します。

ステップ 5 Threat Grid Portal UI で、サービス通知を確認します。任意の通知に、PostgreSQL バックアップがまだありませんという警告などのバックアッププロセスの障害が示されている場合は、続行しないでください。

重要 上述のプロセスが正常に完了しない限り、手順を先に進めないでください。

ステップ 6 [Configuration] > [Clustering] に移動します。

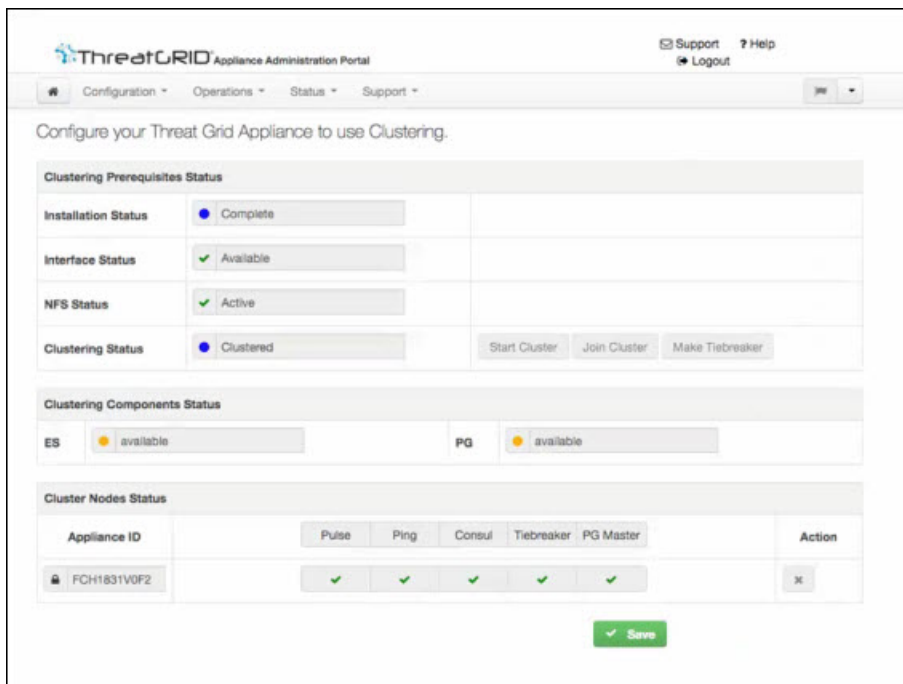
図 10: クラスタの開始



ステップ7 [Start Cluster] をクリックします。

ステップ8 確認ダイアログで、[OK] をクリックします。[Clustering Status] が [Clustered] に変わります。

図 11: [Clustering Status]: [Clustered]



データの復元が完了したら、[Clustering] ページに戻って、新しいクラスタの正常性を確認します。

ステップ9 インストールを終了します。この操作により、クラスタモードでデータの復元が開始されます。

次のタスク

「[Threat Grid アプライアンスのクラスタへの結合](#)」で説明されているように、他の Threat Grid アプライアンスの新しいクラスタへの結合を開始できます。

新しいアプライアンスを使用したクラスタの開始

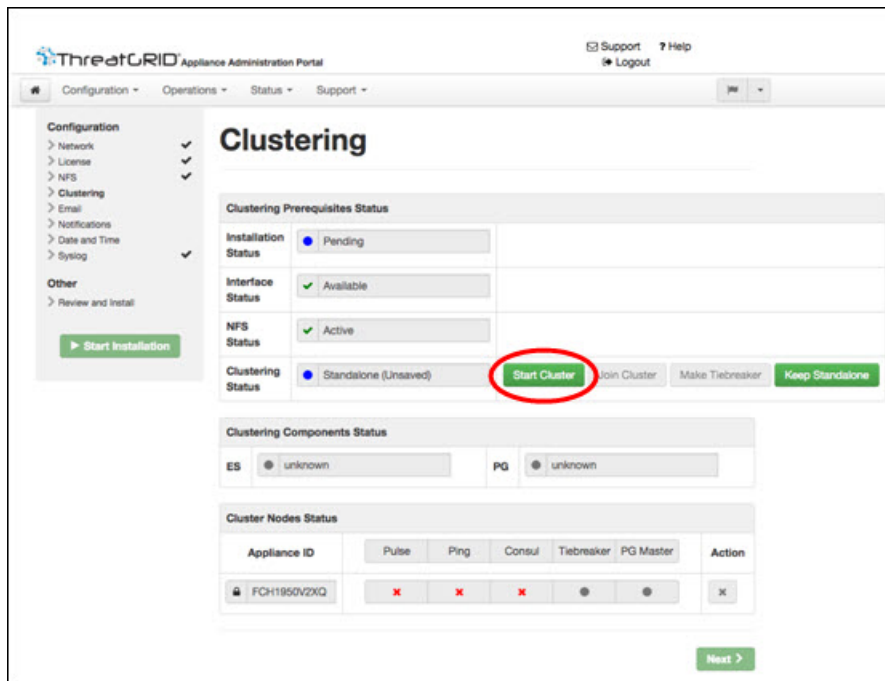
このクラスタ開始方法は、クラスタ対応バージョンのソフトウェアを搭載している新しい Threat Grid アプライアンスか、データをリセットした既存の Threat Grid アプライアンスに使用できます。



(注) 「[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](#)」に記載されているとおり、destroy-data コマンドを使用して既存のデータを削除します。アプライアンスのワイプ機能は使用しないでください。

-
- ステップ 1** 通常どおり OpAdmin 設定を設定および開始します。
- ステップ 2** OpAdmin で、**[Configuration] > [NFS]** をクリックします。
- (注) 「[既存のスタンドアロンアプライアンスを使用したクラスタの開始](#)」の図を参照してください。
- ステップ 3** **[Network]** と **[License]** を設定します。
- ステップ 4** NFS の設定ページで、次のフィールドに入力します。
- **[Host]** : NFSv4 ホストサーバ。IP アドレスを使用することをお勧めします。
 - **[Path]** : ファイルが保存される NFS ホストサーバ上の場所への絶対パス。これにはキー ID サフィックスは含まれません。自動的に追加されます。
 - **[Opots]** : このサーバで NFSv4 に対する標準 Linux のデフォルト値を変更する必要がある場合に使用される NFS マウントオプション。
 - **[Status]** : ドロップダウンリストから **[Enabled (Pending Key)]** を選択します。
- ステップ 5** **[次へ (Next)]** をクリックします。
- ページが更新されます。**[Generate]** ボタンと **[Activate]** ボタンが使用できるようになります。
- ステップ 6** **[生成 (Generate)]** をクリックして、新しい NFS 暗号キーを作成します。
- ステップ 7** **[Activate]** をクリックします。
- ステータスが **[アクティブ (Active)]** に変わります。
- ステップ 8** **[ダウンロード (Download)]** をクリックして、保管のために暗号キーのコピーをダウンロードします。クラスタに追加のノードを結合するためのキーが必要です。

図 12: クラスタリング設定ページ



- ステップ 9 [Clustering] ページで [Start Cluster] をクリックしてから、確認ダイアログで [OK] をクリックします。
[Clustering Status] が [Clustered] に変わります。
- ステップ 10 ウィザードの残りの手順を完了し、[Start Installation] をクリックします。この操作により、クラスタモードでデータの復元が開始されます。
- ステップ 11 [Clustering] ページを開き、新しいクラスタの正常性を確認します。

図 13: [Clustering Status]: [Clustered]

Clustering Prerequisites Status	
Installation Status	Complete
Interface Status	Available
NFS Status	Active
Clustering Status	Clustered

Clustering Components Status	
ES	available
PG	available

Cluster Nodes Status	
Appliance ID	Action
FCH1831V0F2	X

次のタスク

「[Threat Grid アプライアンスのクラスタへの結合](#)」に進みます。

Threat Grid アプライアンスのクラスタへの結合

このセクションでは、新規および既存の Threat Grid アプライアンスをクラスタに結合する方法について説明します。



(注) Threat Grid アプライアンスは、データが含まれていない場合にのみ、既存のクラスタに結合できます。データが含まれている可能性のある最初のアプライアンスの場合とは異なります。

また、クラスタに結合している Threat Grid アプライアンスに最新のソフトウェアバージョンがインストールされていることは非常に重要です（クラスタ内のすべてのノードが同じバージョンを実行している必要があります）。そのためには、Threat Grid アプライアンスの設定と更新が必要になる場合があります。その後、日付をリセットしてクラスタに結合することができます。

一度に1つのノードを追加するようにし、次のノードを追加する前に、Elasticsearch (ES) と Postgres (PG) が **[Replicated]** の状態になるまで待機します。**[Replicated]** のステータスは、2つ以上のノードを含むクラスタで想定されています。



(注) ES および PG の状態が **[Replicated]** に変更されるまでの待機時間は、単一ノードの場合には当てはまりません。バックアップから単一ノードクラスタを初期化する場合は、復元が完了し、アプリケーションが UI に表示されるのを待ってから、2番目のノードを追加する必要があります。

Threat Grid アプライアンスをクラスタに結合する場合、初期設定時に NFS とクラスタリングを設定する必要があります。

既存のアプライアンスのクラスタへの結合

既存の Threat Grid アプライアンスをクラスタに結合するには、次の手順を実行します。

ステップ1 Threat Grid アプライアンスを最新バージョンに更新します。この手順では、インストールされている現在のバージョンに応じて、複数の更新サイクルが必要になる場合があります。クラスタ内のすべてのノードを同じバージョンにする必要があります。

ステップ2 すべてのデータを削除するには、TGSU で **destroy-data** コマンドを実行します。既存の Threat Grid アプライアンスをクラスタに結合する際、クラスタにマージする前に、すべてのデータを削除する必要があります。「[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](#)」を参照してください。

既存の Threat Grid アプライアンスで `destroy-data` コマンドを実行した後、このアプライアンスは基本的に新しいノードになるため、クラスタに結合するには、新しい Threat Grid アプライアンスを結合する場合と同じ手順に従います。

次のタスク

「[新しいアプライアンスのクラスタへの結合](#)」に進みます。

新しいアプライアンスのクラスタへの結合

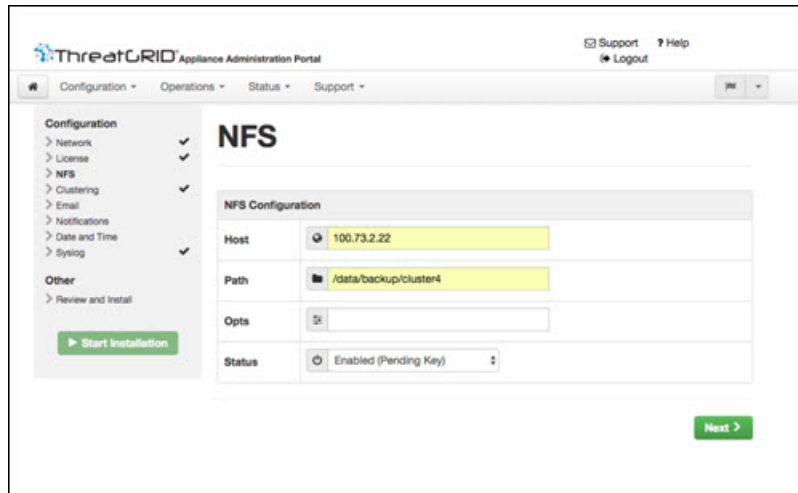
新しい Threat Grid アプライアンスをクラスタに結合するには、次の手順を実行します。

ステップ1 通常どおり OpAdmin 設定を設定および開始します。

ステップ2 OpAdmin で、**[Configuration]** > **[NFS]** をクリックし、クラスタ内の最初のノードで設定された内容と一致するホストとパスを指定します。

ステップ3 **[Status]** ドロップダウンリストで **[Enabled (Pending Key)]** を選択します。

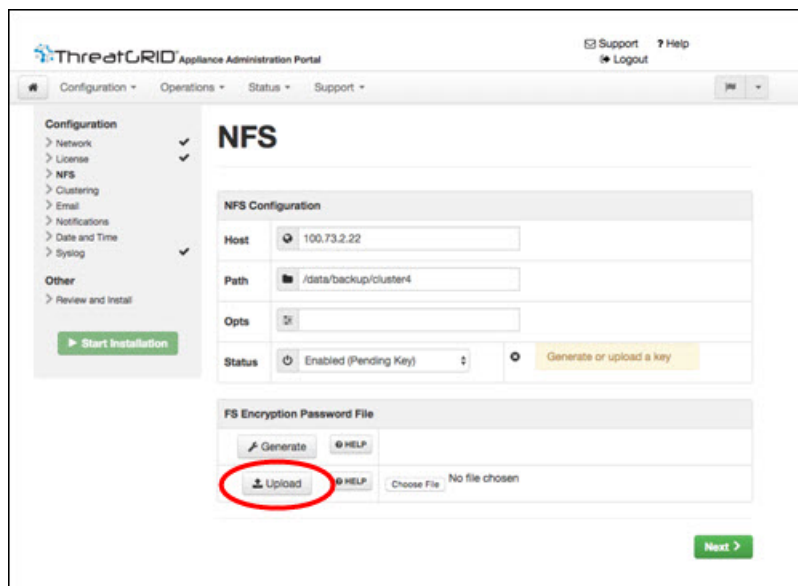
図 14: クラスタに結合するための NFS



ステップ 4 [次へ (Next)] をクリックします。ページが更新され、[Upload] ボタンが使用可能になります。

(注) 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、アップロード後に OpAdmin に表示される [Key ID] は、設定されたパス内の特定のディレクトリの名前と一致するはずですが、暗号キーを使用せずにバックアップを復元することはできません。設定プロセスには、NFS ストアおよび暗号化データをマウントするプロセスと、NFS ストアのコンテンツからアプライアンスのローカル データストアを初期化するプロセスが含まれます。

図 15: NFS 暗号キーのアップロード

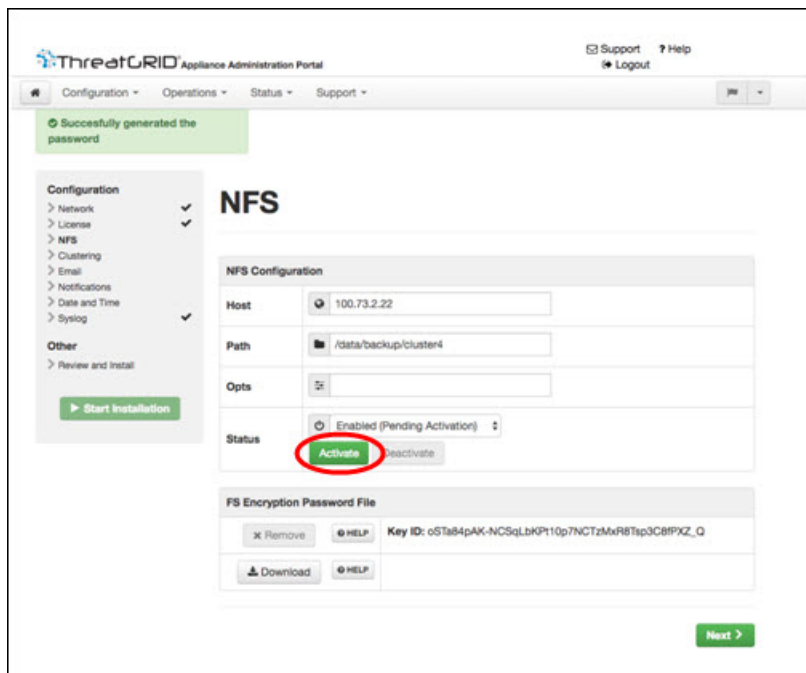


ステップ 5 [Upload] をクリックし、新しいクラスタを開始した際の最初のノードからダウンロードした NFS 暗号キーを選択します。

ステップ 6 [次へ (Next)] をクリックします。

ページが更新されます。[Key ID]が表示され、[Activate]ボタンが有効になります。

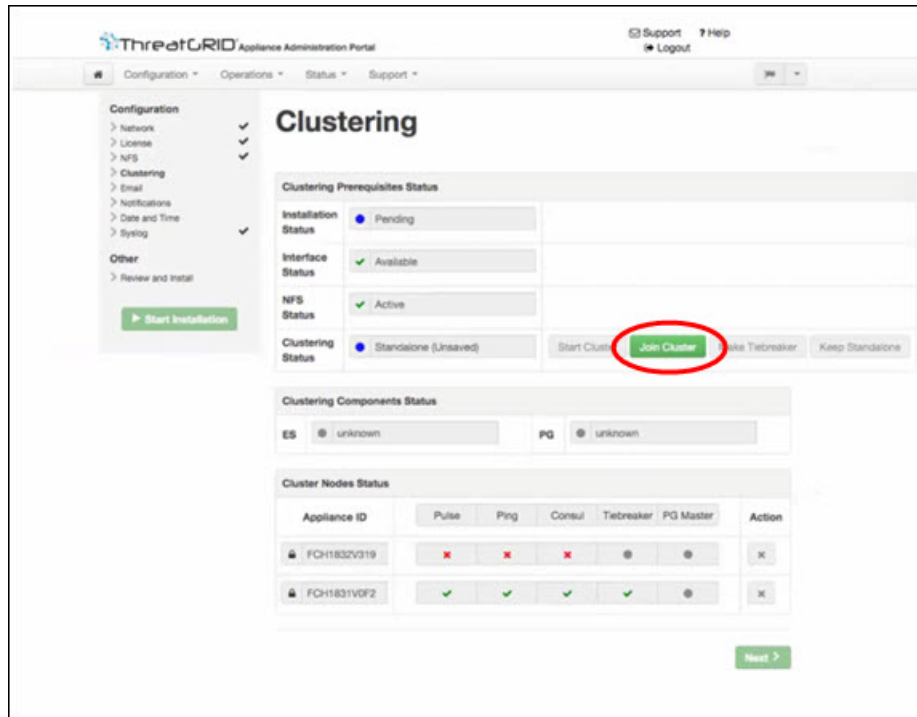
図 16: 結合するアプライアンスの NFS 暗号キーを有効にします。



ステップ 7 [Activate] をクリックします。数秒後に [Status] が [Active] に変わります (左下隅)。

ステップ 8 [Next] をクリックして、[Clustering] ページに進みます。

図 17: クラスタの結合

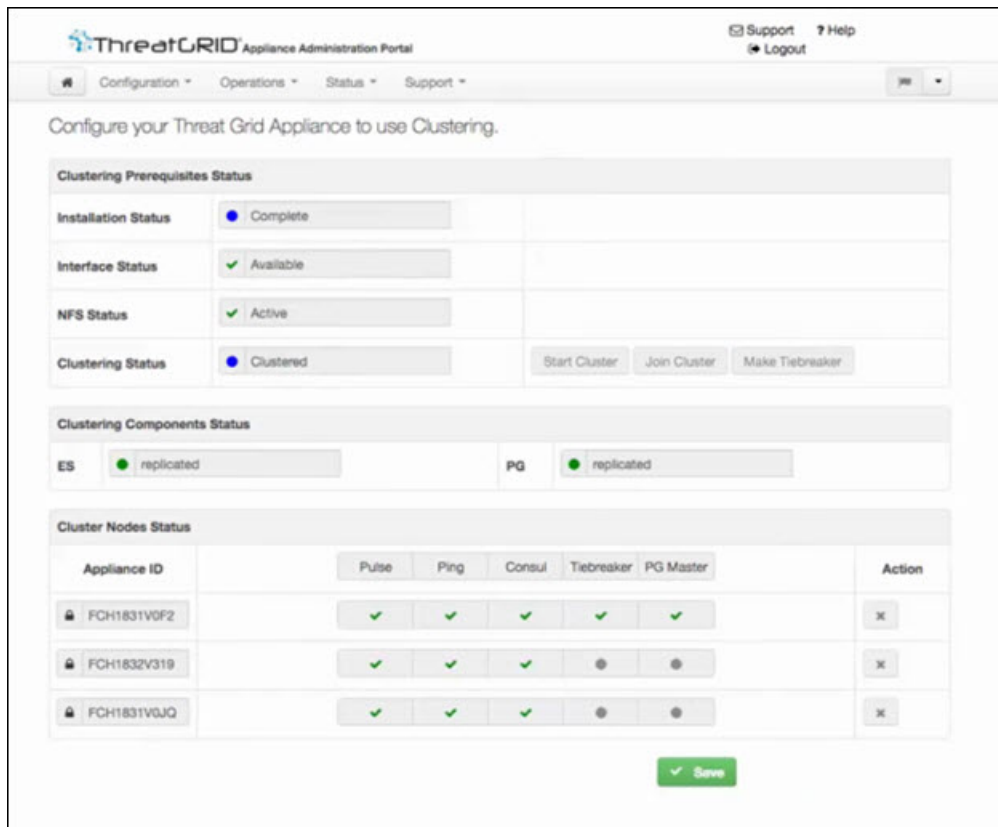


ステップ 9 [Join Cluster] をクリックしてから、確認ダイアログで [OK] をクリックします。

[Clustering Status] が [Clustered] に変わります。

ステップ 10 インストールを終了します。これにより、クラスタモードでデータの復元が開始されます。

図 18: アクティブかつ正常な 3 ノードクラスタ



ステップ 11 クラスタに結合するノードごとに、手順 1 ~ 手順 10 を繰り返します。

タイブレーカーノードの指定

クラスタに偶数のノードを含めるように設定すると、タイブレーカーとして指定されたノードは、どのノードがプライマリデータベースを持つかを決定するイベントで二番手に位置付けられます。

クラスタ内の各ノードにはデータベースが含まれていますが、プライマリノードのデータベースのみが実際に使用されます。プライマリノードがダウンした場合、他のノードがその役割を引き継ぐ必要があります。条件を設定していると、ノードがちょうど半分失敗したとき、ただし、条件が失敗したノード上ではない場合のみ、クラスタがダウンするのを防止できます。

クラスタには 3 つ、5 つ、または 7 つのノードを含めることを推奨します。タイブレーカーのサポートは、スタンドアロン Threat Grid アプライアンスから 2 ノードクラスタに移行する際の信頼性の喪失を軽減するための継続的な取り組みの一環です。

クラスタが完全に正常な状態で、現在のノードがタイブレーカーではない場合、[Clustering] ページの [Make Tiebreaker] ボタンがアクティブになります。

ノードをタイブレーカーに指定するには、**[MakeTiebreaker]** をクリックします。サービスが一時的に中断されます。その後現在のノードは障害の発生が許容されないノードになり、他のノードはクラスタを解除せずにシャットダウンできます。

前もってタイブレーカーの指定を変更できない状況で、タイブレーカーノードの恒久的な障害が発生した場合は、残るノードをリセットしてバックアップから復元するか、[Threat Grid サポート](#) に連絡して支援を求めてください。

クラスタノードの削除

クラスタからノードを削除するには、**[Clustering]** ページの **[Cluster Nodes Status]** ペインに表示される **[Action]** 列の **[Remove]** アイコン (X) をクリックします。

- クラスタからノードを削除するとは、ノードが一時的にダウンするというのではなく、クラスタの一部と見なされなくなることを意味します。Threat Grid アプライアンスは、使用を停止している間に削除する必要があります。削除されたアプライアンスは、別のハードウェアに置き換えられるか、データがリセットされた後にのみクラスタに再度結合されます。
- ノードの削除は、ノードを再度追加しないユーザーの意向をシステムに伝えることに相当します。再度追加しようとすると、ノードがリセットされます。
- ノードは、パルスがある (NFS にアクティブに書き込まれている) 場合、または **consul** (合意ストアの一部) でアクティブになっている場合、クラスタから完全に削除されたものとしてマークされません。

(7 ノード未満のクラスタ内の) ライブになっているノードを置き換えるには、新しいノードを追加し、クラスタが緑色になるのを待ってから、**[Remove]** ボタンを使用して古いノードをオフラインにします。この操作は、ノードを戻さない意向をシステムに伝えることに相当します。

ノードをオフラインにすると、クラスタのステータスは黄色に変わります。**[Remove]** をクリックすると、ステータスが緑色に戻ります (削除されたばかりのノードの存在が想定されなくなり、クラスタのサイズが変更されるため)。

クラスタのサイズ変更

[Remove] アイコンを使用してクラスタからノードが削除されると、クラスタのサイズが変更されます。その結果、許容される障害の数に影響が及ぶ場合があります。許容される障害の数 ([障害許容範囲](#) で定義) が変わるほど大きくクラスタのサイズが変更されると、Elasticsearch が強制的に再起動され、サービスが一時的に中断されます。

例外：上記には、再起動中か、一時的な障害が発生している PostgreSQL マスター以外のシステムは含まれません。中断は、そのノードをアクティブに使用したクライアントを除くケースで、またはサンプルを実行している場合は、最小限にする必要があります。

すでにクラスタの一部ではない Threat Grid アプライアンスを追加した場合や、[Remove] をクリックした場合は、クラスタサイズが変化して、許容される障害の数を変更されます。その後、クラスタの残りの部分が再設定されるため、短時間の中断が発生します。

障害許容範囲

障害が発生した場合、クラスタ化された Threat Grid アプライアンスは、障害が発生したノードによってアクティブに実行されている分析を除き、データを失うことはありません。また、サービスが中断される期間が最短（1分未満）のサービスをユーザの関与なしで回復します。

使用可能なノードの数が [Failure Tolerances] テーブルの [Nodes Required] 列に表示されている数以上である場合、ほとんどの障害は1分未満で回復します。または、使用可能なノードの数が増えて前述の数を満たすようになると回復します。この条件は、障害発生前にクラスタが正常な状態だった場合に当てはまります（[Clustering] ページで [Replicated] と表示されるサービスによって示される）。

特定のサイズのクラスタが許容すると想定される障害の数を次の表に示します。

表 1: 障害許容範囲

クラスタ サイズ	許容される障害	必要なノード
1	0	1
2	1*	1*
3	1	2
4	1	3
5	2	3
6	2	4
7	3	4

次の図は、最良のシナリオを表します。すべてのノードがアップするときにクラスタがボード上で緑色に表示されない場合、示された完全な障害の数を許容できない場合があります。

たとえば、2つの障害が許容される5ノードのクラスタサイズを使用しており、3つのノードが必要で、5台のアプライアンスすべてがアクティブにデータを処理しているときに、2つまでの障害が発生した場合、クラスタは自動的に再設定され、手動による管理アクションなしで動作を続行できます。

別の考慮事項として、5、6、または7ノードのクラスタの場合、許容される障害の数が1つ増えるごとに、障害が発生し得るノードの比率が高くなることを意味します。この事実は、ノードの数が障害発生率の乗数となるため、特に重要です。（2つのノードを使用していて、各々にハードウェア障害が10年ごとに発生している場合は、ハードウェアの障害発生率を5年間に1回に変更します）。

障害の回復

多くの場合、障害が発生しても自動的に回復します。回復しない場合は、Threat Grid サポート (support@threatgrid.com) に連絡するか、バックアップからデータを復元する必要があります。詳細については、「[バックアップコンテンツの復元](#)」を参照してください。

API/使用の特性

クラスタ内の任意のノードに送信されたサンプルのステータスは、クラスタ内の他のノードからクエリされることがあります。送信が行われる個々のノードを追跡する必要はありません。

1つのノードに行われたサンプル送信の処理は、クラスタ内のすべてのノード間で分割されます。クライアント側からアクティブに負荷分散する必要はありません。

運用/管理の特性

2つのノードがあるクラスタでは、一方のノードがタイブレーカーで、シングルポイント障害となります。ただし、他のノードは、（カットオーバー中に一時的な障害を超える）悪影響なく、クラスタから削除される可能性があります。2ノードクラスタが正常な（両方のノードが完全に動作している）場合、条件の指定はユーザによって変更され、シングルポイント障害であるノードを置換する可能性があります。

フェールオーバーが発生している間にサービスが一時的に中断される可能性があります。フェールオーバー中にアクティブに実行されているサンプルは自動的に再実行されません。

クラスタリングのコンテキストでは、キャパシティとは、ストレージではなくスループットを意味します。3つのノードを持つクラスタは、単一の Threat Grid アプライアンスと同じ最大ストレージレベルまでデータをプルーニングします。その結果、5000 サンプルアプライアンス3台を含むクラスタ（合計 15,000 サンプル/日のレート制限）は（フルキャパシティで使用されている場合）、Cisco.com の『[Threat Grid Appliance Data Retention Notes](#)』に記載されている 10,000 サンプル/日の想定よりも、最短保持期間が 33 % 短くなります。

サンプルの削除

Threat Grid アプライアンス（v2.5.0 以降）では、サンプルの削除がサポートされます。

- **[Delete]** オプションは、サンプルリストの **[Actions]** メニューにあります。
- **[Delete]** ボタンは、サンプル分析レポートの右上隅にあります。



-
- (注) 削除されたサンプルのバックアップコピーがすべてのノードから削除されるまでに、最大 24 時間かかる場合があります。
-

削除されたサンプルは、ただちに共有 NFS ストアから削除されます。削除要求を処理しているノードからはすぐに削除されますが、他のノードでは、夜間の `cron` ジョブが実行されるまで保留になります。クラスタモードでは、NFS ストアはサンプルのプライマリソースと見なされます。そのため、サンプルが他のノードから物理的に削除されていない場合でも、いずれのノードからも取得できなくなります。

Threat Grid アプライアンスバージョン 2.7 以降では、クラウド製品の動作に合わせて、サンプルの削除にアーティファクトが含まれるように拡張されています。