# メンテナンス

表示されるメンテナンスオプションは、ユーザーロールによって異なります。

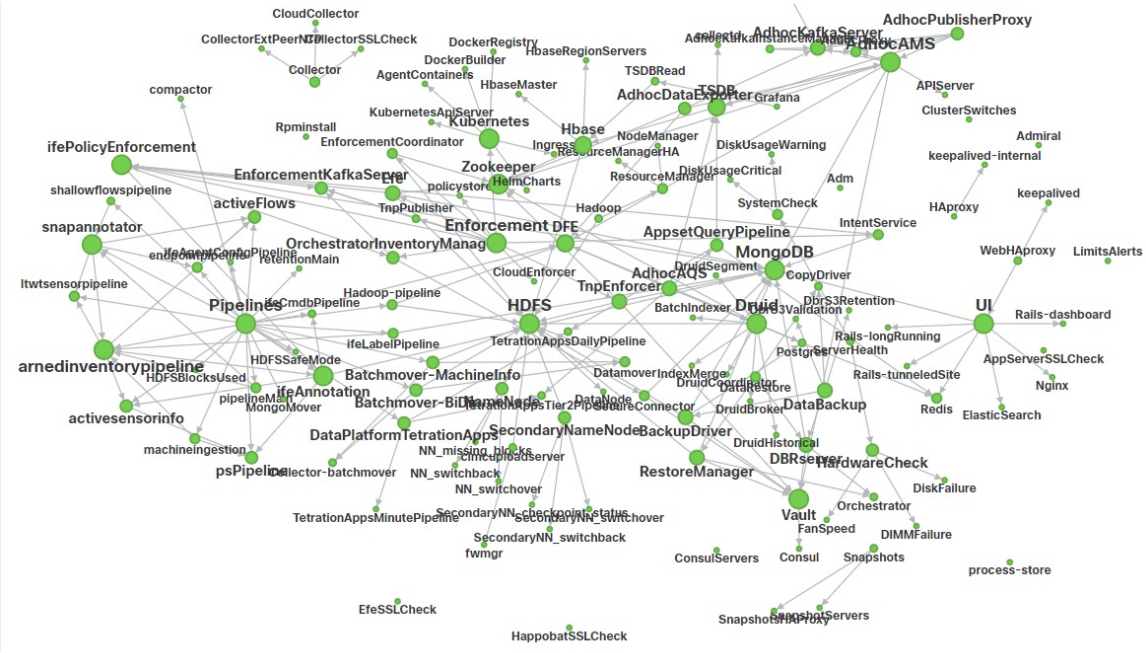


# サービスのステータス

左側のナビゲーションバーの [トラブルシュート（Troubleshoot）] メニューの下にある [サービスステータス（Service Status）] ページには、Cisco Secure Workload クラスタで使用されている全サービスの正常性と、サービスの依存関係が表示されます。

グラフビューにはサービスの正常性が表示されます。グラフの各ノードにはサービスの正常性が表示され、エッジは他のサービスへの依存関係を表します。異常なサービスは、サービスが利用できない場合は赤色、サービスが低下しているが利用可能な場合はオレンジ色で示されます。緑色のノードは、サービスが正常であることを示します。ノードに関する詳細なデバッグ情報を確認する場合は、[すべて展開（Expand All）] ボタンがあるツリービューを使用して、依存関係ツリー内のすべての子ノードを表示します。「ダウン」はサービスが機能していないことを示し、「異常」はサービスが完全には機能していないことを示します。

図 *1 : [*サービスステータス（***Service Status***）*]* ページ




# アドミラルアラート

アドミラルは、統合されたアラートシステムです。サービスのステータスによって報告されたサービスの正常性に基づいてアラートを処理します。そのため、統一された方法でユーザーはサービス/クラスタの健全性を判断することができます。サービスステータスは、サービスの現在（特定の時点）の状態を示します。サービスステータスが赤色と報告された場合、サービスは停止していると見なされ、それ以外の場合は稼働していると見なされます。稼働時間は、サービスが稼働していると報告される時間です。アドミラルは、一定期間にわたるサービスステータスによって報告されたサービスの正常性を評価し、サービスの稼働時間の割合が特定のしきい値を下回った場合にアラートを生成します。一定期間にわたってこの評価を行うことで、誤検知を減らし、本当のサービス停止時にのみ警告を発することが保証されます。

サービスによってアラートのニーズは異なるため、この割合と時間間隔は、サービスごとに異なる方法で固定されています。

顧客は、アドミラル通知を使用して、これらのイベントの通知を受けることができます。これらのイベントは、プラットフォームタイプの **[調査（Investigate）]**>**[アラート（Alerts）]** ページにも表示されます。

（注） アドミラルアラートは、選択したサービスのサブセットのみに関連付けられます。サービスが上記のサブセットに含まれていない場合、サービスがダウンしてもアドミラルアラートは発生しません。このサービスのサブセットで設定されているアドミラルアラートとそのアラートしきい値の割合と時間間隔は固定であり、ユーザーは設定できません。

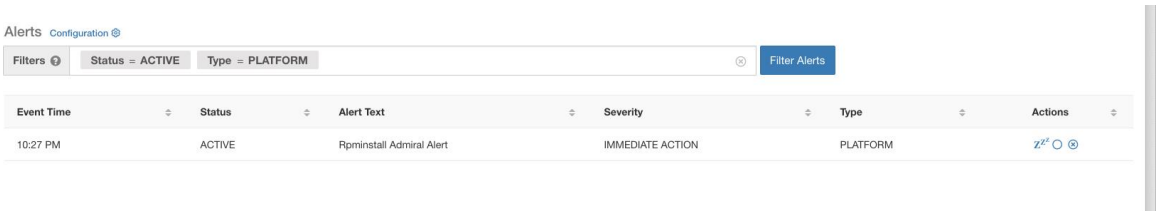
次のセクションでは、アドミラルアラートと通知について詳しく説明します。

# アドミラルアラートのライフサイクル

アドミラルは、サービスステータスでサービスの稼働時間をチェックします。この稼働時間があらかじめ設定されたアラート用のしきい値を下回ると、アラートが発生します。

たとえば、RPminstall は、展開、アップグレード、パッチなどの際に rpm をインストールするために使用されるサービスです。1 時間以上の稼働時間が 80% 未満の場合、アドミラルアラートを生成するように設定されています。Rpminstall サービスが上で指定されたしきい値よりも長い期間ダウンした場合、RPminstall のアドミラルアラートが生成され、ステータスが ACTIVE になります。

**図 *2:* アクティブなアドミラルアラート**




サービスが回復すると、稼働時間の割合が増加し始めます。稼働時間がしきい値を超えると、アラートは自動的にクローズし、ステータスは CLOSED に移行します。上記の Rpminstall の例では、稼働時間が 1 時間で 80% を超えると、Rpminstall アドミラルアラートは自動的にクローズします。

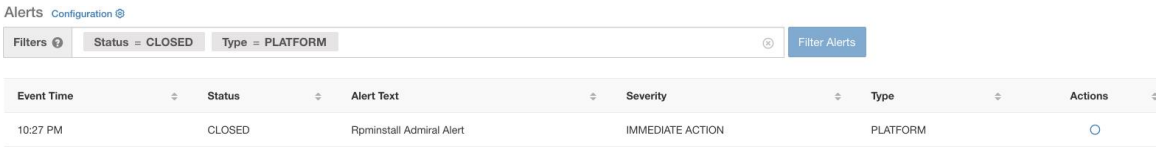
（注） アラートのクローズにより、サービスは常に正常に戻るのが遅れます。これは、アドミラルが一定期間サービス正常性を監視するためです。上記の例では、RPminstall アラートのしきい値が 1 時間の稼働時間の 80% に設定されているため、アラートがクローズするまでに少なくとも 48 分間（1 時間の 80%）稼働している必要があります。

アラートをクローズするために必要なユーザーのアクションはありません。アクティブなアドミラルアラートは、注意が必要な現在の根本的な問題を示すようになります。

（注） アラートがクローズしても、専用の通知は生成されません。

アラートが CLOSED に移動すると、ACTIVE アラートの下に表示されなくなります。クローズされたアラートは、次に示すように、フィルタの Status=CLOSED を使用して、UI に引き続き表示されます。

**図 *3:* サービス回復時に自動的にクローズするアドミラルアラート**



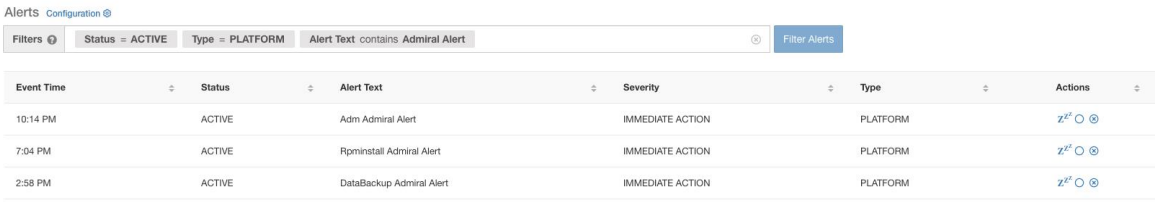

アドミラルアラートには次の 2 種類があります。

1. 個別のアドミラルアラート
2. サマリーのアドミラルアラート

# 個別のアドミラルアラート

上記で説明したアラート、個々のサービスに対して発生したアラートは、このカテゴリに分類されます。これらのアラートのアラートテキストには常に <Service Name> Admiral Alert が含まれています。これにより、個々のアラートをサービスまたは「Admiral Alert」サフィックスで簡単にフィルタリングできます。

**図 *4:* 個別のアドミラルアラートのアラートテキストフィルタ**



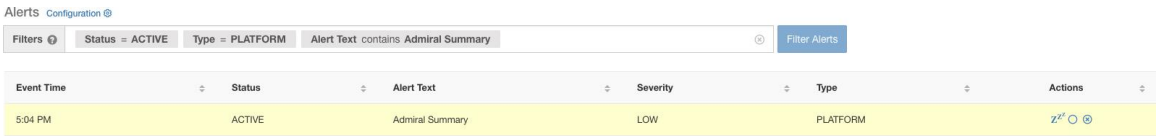

このサービスのその他の属性については、_admiral_indiv_details-label で説明しています。

# サマリーのアドミラルアラート

アドミラルは、UTC の午前 0 時に毎日サマリーアラートを生成します。サマリーアラートには、現在アクティブなアラートと、過去1日以内にクローズされたすべてのアラートのリストが含まれているため、ユーザーは、アドミラルによって報告された全体的なクラスタの正常性を1か所で確認できます。これは、専用の通知を生成しないクローズされたアラートを表示する場合にも役立ちます。クラスタが正常で、過去1日以内にクローズされたアラートがない場合、その日のサマリー通知は生成されません。これは、不要な通知とノイズを減らすために行われます。

この場合のアラートテキストは常に「アドミラルサマリー」なので、以下に示すように、サマリーアラートを簡単にフィルタ処理できます。

**図 *5:* アドミラル サマリー テキスト フィルタ**



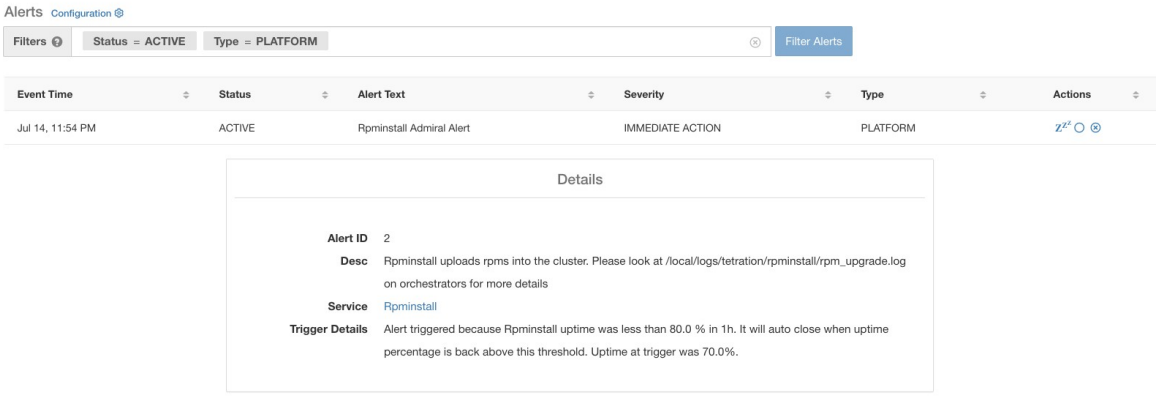

このサービスのその他の属性については、_admiral_summary_dets-label を参照してください。

# アラート詳細

## 個別のアラート

個別のアドミラルアラートのアラートをクリックすると、アラートが展開され、アラートのデバッグと分析に役立つフィールドが表示されます。

**図 *6:* アラート詳細**




以下の表で各フィールドについて説明します。

| フィールド | バージョン情報 |
|---|---|
| アラートID（Alert ID） | 各アラートには、アラート ID と呼ばれる一意の ID があります。この ID は、特定のサービスダウン発生を一意に把握するのに役立ちます。前述のように、アラートによってレポートされているサービスの基本的な稼働時間が正常になると、アラートは自動的に閉じます。その後、同じサービスが再びダウンすると、別のアラート ID を持つ新しいアラートが生成されます。このように、アラート ID は、発生したアラートの各インシデントを一意に把握するのに役立ちます。 |
| Desc | 説明フィールドには、アラートの原因となっているサービスの問題についての追加情報が含まれています。 |

| フィールド | バージョン情報 |
|---|---|
| サービス | このフィールドには、ユーザーがサービスの現在のステータスを確認できるサービスステータスページへのリンクが含まれています。ユーザーは、サービスステータスページでサービスがダウンとマークされている理由の詳細を把握することもできます。 |
| トリガーの詳細情報 | このフィールドには、サービスのトリガーしきい値に関する詳細情報が含まれます。ユーザーは、これらのしきい値を確認することで、基本的なサービスが復旧した後にアラートが閉じるタイミングを把握できます。例：Rpminstallのしきい値は、1時間で80%の稼働時間と記されています。したがって、アラートが自動的に閉じる前に、Rpminstallサービスは少なくとも48分間（1時間の80%）稼働している必要があります。ここには、アラートが発生した時点でサービスに表示された稼働時間の値も示されています。 |

JSON Kafka出力の例は次のとおりです。

```
{
"severity": "IMMEDIATE_ACTION",
"tenant_id": 0,
"alert_time": 1595630519423,
"alert_text": "Rpminstall Admiral Alert",
"key_id": "ADMIRAL_ALERT_5",
"alert_id": "/Alerts/5efcfdf5497d4f474f1707c2/DataSource{location_type='TETRATION',
‹→location_name='platform', location_grain='MIN', root_scope_id=
‹→'5efcfdf5497d4f474f1707c2'}/
‹→66eb975f5f987fe9eaefa81cee757c8b6dac5facc26554182d8112a98b35c4ab",
"root_scope_id": "5efcfdf5497d4f474f1707c2",
"type": "PLATFORM",
"event_time": 1595630511858,
"alert_details": "{\"Alert ID\":5,\"Service\":\"Rpminstall\",\"Desc\":\"Rpminstall
‹→uploads rpms into the cluster. Please look at /local/logs/tetration/rpminstall/rpm_
‹→upgrade.log on orchestrators for more details\",\"Trigger Details\":\"Alert
‹→triggered because Rpminstall uptime was less than 80.0 % in 1h. It will auto close
‹→when uptime percentage is back above this threshold. Uptime at trigger was 65.0%. \
‹→"}"
}
```

個別のアラートはすべて、上記の形式に従います。アドミラルモニタリングの対象となる（サービスステータスからの）サービスのリストを表に示します。

| サービス | トリガー条件 | 重大度 |
|---|---|---|
| KubernetesApiServer | 過去15分間でサービスの稼働時間が90%を下回っている。 | 即時対応（IMMEDIATE ACTION） |

| サービス | トリガー条件 | 重大度 |
|---|---|---|
| Adm | 過去1時間でサービスの稼働時間が90%を下回っている。 | 即時対応（IMMEDIATE ACTION） |
| DataBackup | 過去6時間でサービスの稼働時間が90%を下回っている。 | 即時対応（IMMEDIATE ACTION） |
| DiskUsageCritical | 過去1時間でサービスの稼働時間が80%を下回っている。 | 即時対応（IMMEDIATE ACTION） |
| RebootRequired | 過去1時間でサービスの稼働時間が90%を下回っている。 | 即時対応（IMMEDIATE ACTION） |
| Rpminstall | 過去1時間でサービスの稼働時間が80%を下回っている。 | 即時対応（IMMEDIATE ACTION） |
| SecondaryNN_checkpoint_status | 過去1時間でサービスの稼働時間が90%を下回っている。 | 即時対応（IMMEDIATE ACTION） |

8RU/39 RU 物理クラスタの場合、次のサービスが追加でモニタリングされます。

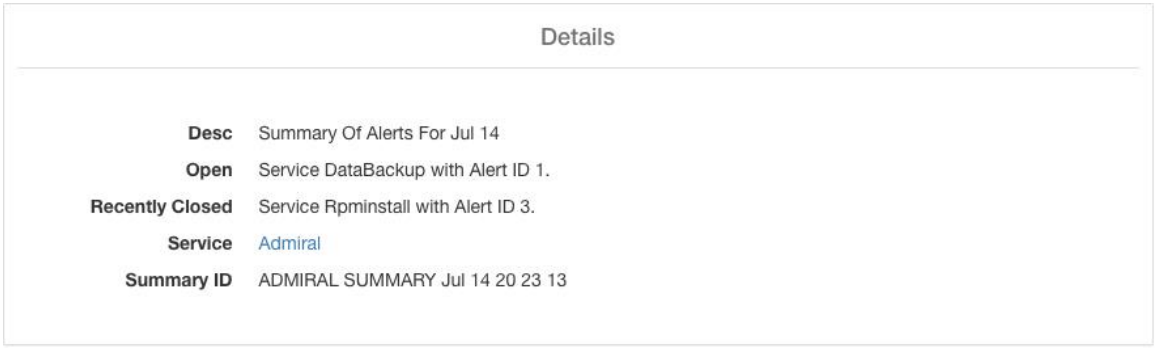
| サービス | トリガー条件 | 重大度 |
|---|---|---|
| DIMMFailure | 過去 1 時間でサービスの稼働時間が 80% を下回っている。 | 即時対応（IMMEDIATE ACTION） |
| DiskFailure | 過去 1 時間でサービスの稼働時間が 80% を下回っている。 | 即時対応（IMMEDIATE ACTION） |
| FanSpeed | 過去 1 時間でサービスの稼働時間が 80% を下回っている。 | 即時対応（IMMEDIATE ACTION） |
| ClusterSwitches | 過去 1 時間でサービスの稼働時間が 80% を下回っている。 | 即時対応（IMMEDIATE ACTION） |

（注） Admiral は、サービスステータスによって生成された処理メトリックに依存してアラートを生成します。メトリックの取得が長期間不可能な場合（たとえば、サービスステータスが停止している場合）、アラート（TSDBOracleConnectivity）が発生し、クラスタでサービスベースのアラート処理がオフになっていることを通知します。

### サマリーアラート

サマリーアラートは本質的に情報提供であり、優先順位は常に LOW に設定されます。アドミラルサマリーアラートをクリックすると、アドミラルアラートに関する概要情報を含む複数のフィールドが展開されて表示されます。

**図 *7:* アドミラルサマリーアラートの詳細**




| フィールド | バージョン情報 |
|---|---|
| Desc | 説明フィールドには、日次概要の日付が含まれています。 |
| オープン（Open） | オープンアラートは、概要が生成された時点でアクティブだったアラートを示しています<br><br>。 |
| [最近閉じたアラート（Recently Closed）] | このフィールドには、過去24時間以内、つまり概要が生成された日に閉じたアラートが表示されます。各アラートのIDも含まれます。アラートは自動的に閉じるため、特定のサービスがダウンしてアラートが作成された後、正常になり、アラートが自動的に閉じる場合があります。アラートが閉じるケースが 1 日に複数回発生した場合、各インシデントとその固有のアラートIDが一覧表示されます。ただし、アラートが閉じる前に各サービスがしきい値時間の間稼働状態になっている必要があることを考えると、こうした状況が頻繁に発生することは想定されていません。ユーザーは、Status＝CLOSEDでフィルタリングして、各インシデントに関する詳細情報を取得できます。 |

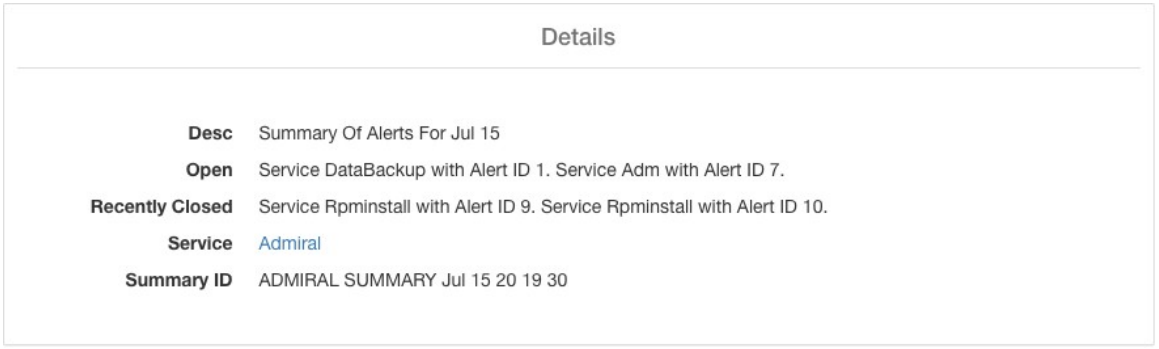
| フィールド | バージョン情報 |
|---|---|
| サービス | サービスを処理し、日次概要を生成する Admiral のサービスステータスリンク。 |
| [サマリーID（Summary ID）] | サマリーアラートの ID。 |

JSON Kafka 出力の例は次のとおりです。

```
{
"severity": "LOW",
"tenant_id": 0,
"alert_time": 1595721914808,
"alert_text": "Admiral Summary",
"key_id": "ADMIRAL_SUMMARY_Jul-26-20-00-04",
"alert_id": "/Alerts/5efcfdf5497d4f474f1707c2/DataSource{location_type='TETRATION',
‹→location_name='platform', location_grain='MIN', root_scope_id=
‹→'5efcfdf5497d4f474f1707c2'}/
‹→e95da4521012a4789048f72a791fb58ab233bbff63e6cbc421525d4272d469aa",
"root_scope_id": "5efcfdf5497d4f474f1707c2",
"type": "PLATFORM",
"event_time": 1595721856303,
"alert_details": "{\"Desc\":\"Summary of alerts for Jul-26\",\"Recently Closed\":\
‹→"None\",\"Open\":\" Service Rpminstall with Alert ID 5.\",\"Service\":\"Admiral\",\
‹→"Summary ID\":\"ADMIRAL_SUMMARY_Jul-26-20-00-04\"}"
}
```

1 日に複数のアラートを発生させるサービスを含むサマリーアラートの例を以下に示します。

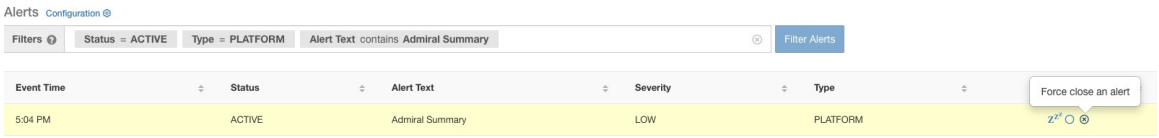
**図 *8*：複数のアラート**




# ユーザのアクション

アドミラルアラートはアラートごとに1回だけ個別の通知を生成するため、特定のアラートを含めたり除外したり、スヌーズしたりする必要はありません。上述のとおり、しきい値である稼働時間の間サービスが正常に動作すると、アラートが自動的に閉じます。アラートを強制的に閉じるための強制終了オプションがあります。個々のアラートは自動的に閉じるため、通常、このオプションの使用は、UI からサマリーアラートを削除する場合に限る必要があります。

図 *9:* アラートの強制終了

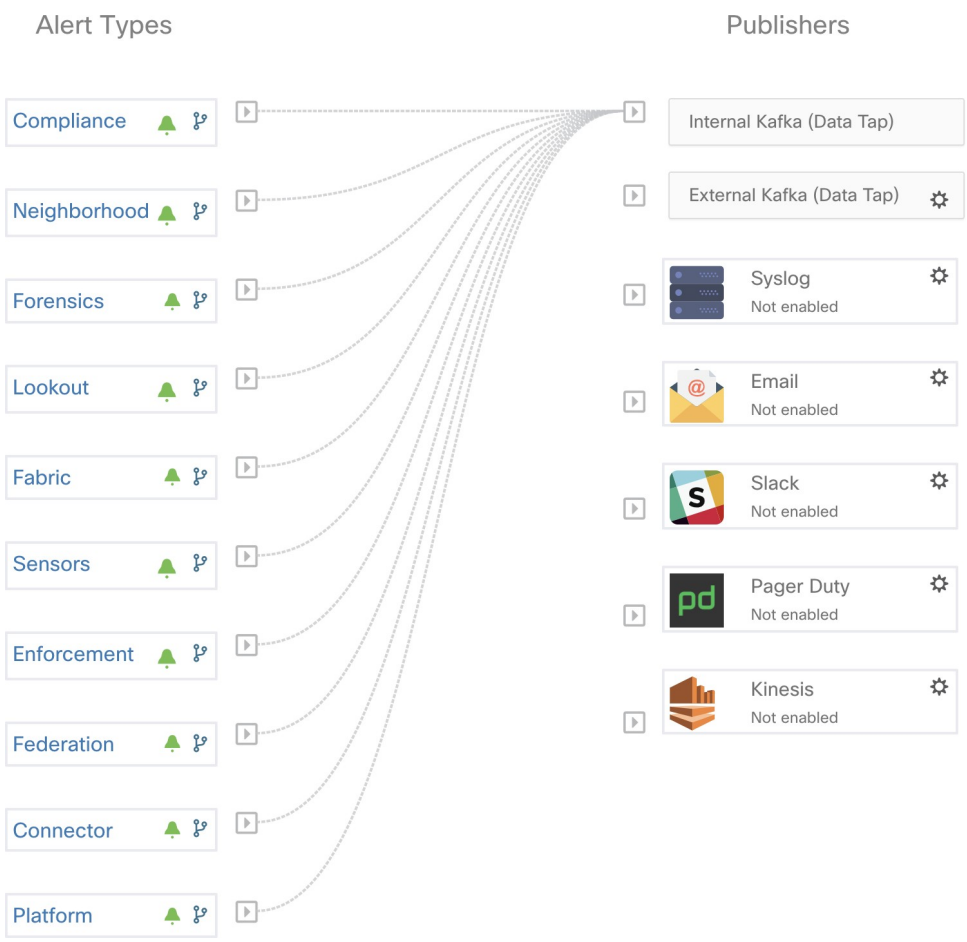



**警告** 個々のアラートを強制終了しないでください。基礎となるサービスがまだダウンしているか、稼働時間が予想されるしきい値を下回っているときに強制終了すると、次のアドミラル処理の反復で同じサービスに対して別のアラートが発生します。

# アドミラル通知

アドミラルアラートのタイプは PLATFORM です。したがって、これらのアラートは、設定ページでの設定によるプラットフォームアラートへの適切な接続によって、さまざまなパブリッシャに送信されるように設定できます。利便性を考慮し、プラットフォームアラートと内部 Kafka 間の接続はデフォルトでオンになっています。これにより、アドミラルアラートが [現在のアラート（Current Alerts）] ページ（**[調査（Investigate）]** > **[アラート（Alerts）]** に移動）に表示されます。手動で設定する必要はありません。

図 *10* : プラットフォームアラートの設定




アドミラルアラートは、**[プラットフォーム（Platform）]** > **[クラスタの設定（Cluster Configuration）]** > **[アドミラルアラートメール（Admiral Alert Email）]** で設定された電子メールアドレスにも送信されます。

図 *11* : アドミラルメールのサンプル

There is a new admiral platform alert on your tetration cluster.
**Service:** Rpminstall
**Start Time:** 2020-07-14 23:09 UTC
**Alert ID:** 3
**Description:** Rpminstall uploads rpms into the cluster. Please look at /local/logs/tetration/rpminstall/rpm_upgrade.log for more details

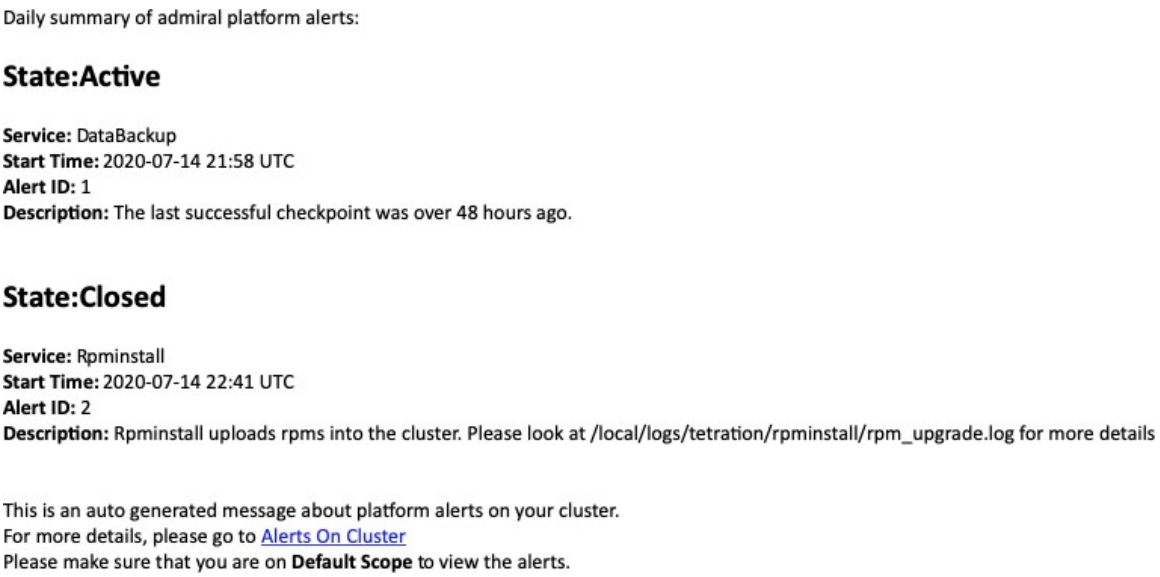
This is an auto generated message about platform alerts on your cluster.
For more details, please go to Alerts On Cluster
Please make sure that you are on **Default Scope** to view the alerts.

そのため、ユーザーは TAN エッジアプライアンスをセットアップしていなくても、アドミラル通知を受け取ることができます。この動作は、以前のリリースの Bosun の動作に似ています。

図 *12 :* アドミラルメール


これらの電子メール通知は、[現在のアラート（Current Alerts）] ページと同じトリガーに基づいて生成されます。したがって、電子メール通知はアラートの作成時に送信され、UTC の午前 0 時に日次概要メールが送信されます。日次概要メールには、すべてのアクティブなアラートと過去 24 時間以内に閉じられたアラートが一覧表示されます。

図 *13 :* 概要アドミラルメールのサンプル

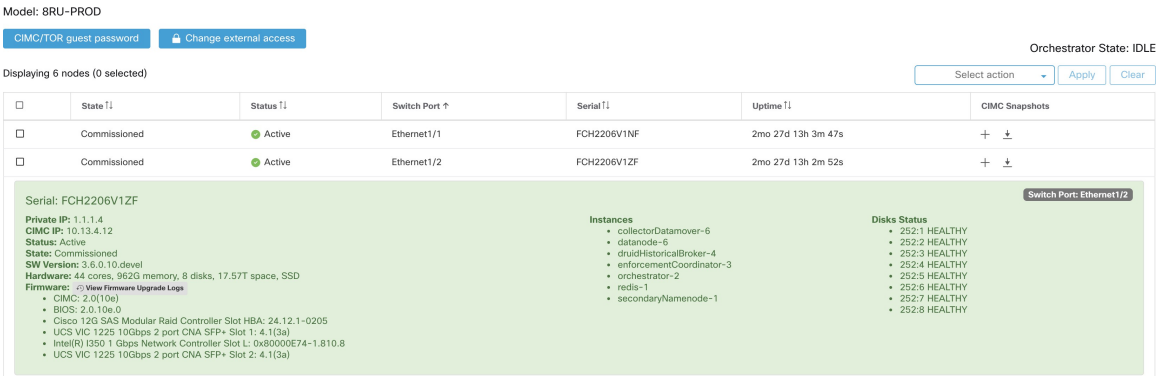



アクティブなアラートがなく、過去 24 時間以内に閉じられたアラートもない場合、電子メールノイズを減らすために概要メールはスキップされます。

# クラスタのステータス

左側のナビゲーションバーの [トラブルシュート（Troubleshoot）] メニューにある [クラスタのステータス（Cluster Status）] ページには、**サイト管理者**ユーザーがアクセスできますが、アクションを実行できるのは**カスタマーサポート**ユーザーのみです。Cisco Secure Workload ラック内にあるすべての物理サーバーのステータスが表示されます。テーブルの各行は、ハードウェアとファームウェアの構成、CIMC IP アドレス（割り当てられている場合）などの詳細が設定された物理ノードを表します。行をクリックすると、ノードの詳細ビューを表示できます。このページでは、ノードの CIMC パスワードを変更し、ノードへの外部アクセスを有効/無効にすることもできます。 [クラスタのステータス（Cluster Status）] ページにはオーケストレータの状態も表示され、カスタマーサポートにコンテキストを提供できます。

**図 *14* : クラスタのステータス**




## すべてのノードに影響するアクション

CIMC パスワードの変更と外部 CIMC アクセスの有効化/無効化は、[CIMC/TOR ゲストパスワード（CIMC/TOR guest password）] ボタンおよび [外部アクセスの変更（Change external access）] ボタンを使用して行うことができます。これらのアクションはクラスタ内のすべてのノードに影響します。

## 外部 CIMC アクセスの詳細

[外部アクセスの変更（Change external access）] ボタンをクリックするとポップアップが開き、外部 CIMC アクセスのステータスが表示され、CIMC への外部アクセスを有効化、更新、または無効化できます。

[有効化（Enable）] ボタンをクリックすると、クラスタがバックグラウンドで構成され、外部 CIMC アクセスが有効になります。これらのタスクが完了し、外部 CIMC アクセスが完全に有効になるまでに最大 60 秒かかる場合があります。外部 CIMC アクセスが有効になっており、アクセスの自動期限切が設定されている場合、ポップアップが表示され、[有効（Enable）] ボタンが [更新（Renew）] に変わり、外部 CIMC アクセスを更新できることが反映されます。外部 CIMC アクセスを更新すると、有効期限が現在の時刻から 2 時間先になります。

外部 CIMC アクセスが有効になっている場合、ノードの詳細（ノードの行をクリックして表示可能）の CIMC IP アドレスは、CIMC WebUI に直接アクセスできるクリック可能なリンクになります。このリンクを表示するには、[クラスタのステータス（Cluster Status）] ページのリロードが必要になる場合あります。

**図 *15* : 外部 *CIMC* アクセスノードの詳細**


CIMC WebUI には通常、自己署名証明書があり、CIMC WebUI にアクセスすると、証明書が無効であることを示すエラーがブラウザに表示される可能性があります。Google Chrome を使用

している場合、証明書チェックをバイパスしてCIMC WebUIにアクセスするためには、無効な証明書エラーが Google Chrome に表示されたときに、引用符なしで「thisisunsafe」と入力する必要があります。

CIMC WebUI では、CIMC バージョンが 4.1(1g) 以降の場合にのみ、KVM アクセスが機能します。外部 CIMC アクセスが有効になると、アクセスを更新または無効にしない限り、2 時間後に自動的に無効になります。

外部CIMCアクセスを無効にすると、クラスタがバックグラウンドで構成され、外部CIMCアクセスが無効になります。これらのタスクが完了し、外部CIMCアクセスが完全に無効になるまでに最大 60 秒かかる場合があります。

**表 *1*: 物理ノードの詳細**

| フィールド | 説明 |
|---|---|
| [Status（ステータス）] | [ステータス（Status）] フィールドは、ノードの電源ステータスを示します。値は以下のとおりです。<br>- [アクティブ（Active）]：ノードの電源がオンになっています。<br>[非アクティブ（Inactive）]：ノードの電源が入っていないか、接続されていません。 |

| フィールド | 説明 |
|---|---|
| [状態（State）] | [状態（State）] フィールドは、ノードのクラスタメンバーシップの状態を示します。値は以下のとおりです。<br>[新規（New）] : ノードはまだクラスタの一部ではありません。<br>[初期化済み（Initialized）] : ノードはクラスタの一部です。ただし、Cisco Secure Workload ソフトウェアはまだ完全にはノードにインストールされていません。<br>[稼働済み（Commissioned）] : ノードは Cisco Secure Workload ソフトウェアを使用して稼働しています。<br>[SW バージョン（SW Version）] フィールドも表示され、個々のノードのバージョンがクラスタ全体と同じでない場合は赤に変わります。<br>[稼働停止（Decommissioned）] : ノードはクラスタから削除されています（RMA の目的で）。ノードを新しいハードウェアと交換する必要があります。ノードは、デコミッションアクションにより稼働を停止できます。下記のアクションを参照してください。 |
| [スイッチポート（Switch Port）] | 物理ノードが接続されている 2 つのスイッチのスイッチポートを指します。 |
| [稼働時間（Uptime）] | ノードが再起動またはシャットダウンせずに稼働していた時間を示します。 |
| [CIMCスナップショット（CIMC Snapshots）] | CIMC テクニカルサポートデータの収集を開始して、ダウンロードするために使用できます。 |

**表 *2:* アクション**

| アクション | 説明 |
|---|---|
| [コミッション（Commission）] | このアクションを選択すると、新しいノードがクラスタに組み込まれます。このアクションについては、状態が [新規（New）] のノードのみを選択できます。 |

| アクション | 説明 |
|---|---|
| [デコミッション（Decommission）] | 現在クラスタに属しているノードを削除するには、このアクションを選択します。このアクションについては、状態が [稼働済み（Commissioned）] または [初期化済み（Initialized）] のノードのみを選択できます。 |
| [再イメージ化（Reimage）] | このアクションを選択すると、ボックス内に Secure Workload ソフトウェアが再インストールされます。これにより、ボックス内のファイルがすべて消去されます。ベアメタル オペレーティング システムを旧バージョンから新バージョンにアップグレードする際に特に便利です。この手順は、ベアメタルが稼働停止になった後に必要になります。 |
| [ファームウェアのアップグレード（Firmware upgrade）] | ファームウェア情報は、CIMC IP に到達可能なノードで利用できます。このアクションは、旧バージョンのノードのファームウェアをアップグレードするのに役立ちます。 |
| [電源オフ（Power off）] | ノードの電源を切るには、このアクションを選択します。ステータスが [非アクティブ（Inactive）] で**シャットダウン中**のノードの電源を切ることはできないので注意してください。 |

# ファームウェア アップグレードの詳細

Secure Workload 物理アプライアンスには、ユニファイドコンピューティング システム（UCS）Cisco Integrated Management Controller（CIMC）ホストアップグレードユーティリティ（HUU）の ISO イメージがバンドルされています。[クラスタのステータス（Cluster Status）] ページでファームウェア アップグレード オプションを使用して、物理ベアメタルを Secure Workload RPM ファイルにバンドルされている HUU ISO に含まれる UCS ファームウェアのバージョンに更新できます。

ベアメタルホストは、ステータスが [アクティブ（Active）] または [非アクティブ（Inactive）] で、ベアメタルのステータスが [初期化（Initialized）] または [SKU不一致（SKU Mismatch）] でない場合に、ファームウェアの更新を開始できます。UCS ファームウェアを一度に更新できるベアメタルは 1 つだけです。ファームウェアの更新を開始するには、Secure Workload オーケストレータの状態が [アイドル（Idle）] である必要があります。UCS ファームウェアの更新が開始されると、Consul リーダー、アクティブなオーケストレータ、またはアクティブなファームウェアマネージャ（fwmgr）を他のホストに切り替える必要がある場合、[クラスタのステータス（Cluster Status）] ページに固有の UI 機能の一部が一時的に影響を受けることがあります。これらのスイッチオーバーは自動的に行われます。ファームウェアの更新中は、更新中のベアメタルホストのファームウェアの詳細は表示されません。更新が完了した後、[クラスタのステータス（Cluster Status）] ページにファームウェアの詳細が再度表示されるまで最大 15 分か

かることがあります。ファームウェアの更新を開始する前に、[サービスのステータス（Service Status）] ページですべてのサービスが正常であることを確認してください。

ベアメタルでファームウェアの更新を開始すると、fwmgr では更新が続行できることを確認し、必要に応じてベアメタルを正常にパワーダウンし、ベアメタルの CIMC にログインして HUU ベースのファームウェアの更新を開始します。この HUU ベースのファームウェアの更新プロセスには、HUU ISO でベアメタルを起動させ、更新を実行し、CIMC を再起動して新しいファームウェアをアクティブ化し、その後 HUU ISO でベアメタルを再起動して、更新が完了したことを確認することが含まれます。全体的な更新プロセスには、G1 ベアメタルの場合は 2 時間以上、G2 ベアメタルの場合は 1 時間以上かかる場合があります。ファームウェアの更新プロセスが開始されると、ベアメタルと、そのベアメタルで実行されているすべての仮想マシンがクラスタ内でアクティブでなくなるため、[サービスのステータス（Service Status）] ページに、一部のサービスが正常でないと示される場合があります。ファームウェアの更新が完了すると、ベアメタルがクラスタ内で再びアクティブになるまでにさらに 30 分かかり、すべてのサービスが再び正常になるまでにさらに時間がかかる場合があります。ファームウェアの更新後 2 時間以内にサービスが回復しない場合は、シスコテクニカルサポートにお問い合わせください。

[クラスタのステータス（Cluster Status）] ページで、ベアメタルノードをクリックして、ベアメタルに関する詳細を展開できます。ファームウェアの更新が開始されたら、[ファームウェアのアップグレードログを表示（View Firmware Upgrade Logs）] ボタンをクリックして、ファームウェア更新のステータスを表示できます。このログには、ファームウェア更新の全体的なステータスが一番上に表示されます。内容は次のいずれかです。

- [ファームウェアの更新がトリガーされました（Firmware update has been triggered）]：ファームウェアの更新が要求されましたが、まだ開始されていません。このステータス中に、fwmgr では、ファームウェアの更新に必要なサービスが機能していること、および CIMC がそれらのサービスに到達できることが確認されます。
- [ファームウェアの更新を実行中です（Firmware update is running）]：ファームウェアの更新が開始されました。ファームウェアの更新がこの状態に達すると、CIMC と HUU で更新が制御され、Secure Workload クラスタでは CIMC から取得した更新に関するステータスが報告されます。
- [ファームウェアの更新がタイムアウトしました（Firmware update has timed out）]：ファームウェアの更新の一部のプロセスが、完了予測時間を超えたことを示します。[ファームウェアの更新を実行中です（Firmware update is running）] のフェーズに入ると、ファームウェアの更新プロセス全体の制限時間は 240 分になります。ファームウェアの更新中に、新しいバージョンでリブートすると CIMC が到達不能になることがあります。この到達不能状態のタイムアウトは、ファームウェアの更新が「タイムアウト」と宣言されるまでの 40 分間です。ファームウェアの更新が開始されると、その更新のモニタリングは 120 分後にタイムアウトします。
- [ファームウェアの更新がエラーのため失敗しました（Firmware update has failed with an error）]：エラーが発生し、ファームウェアの更新が失敗したことを示します。通常、CIMC では成功または失敗は示されません。そのため、この状態は通常、ファームウェアの更新が実際に実行される前にエラーが発生したことを示しています。

- [ファームウェアの更新が終了しました（Firmware update has finished）]：ファームウェアの更新は、エラーやタイムアウトが発生することなく終了しました。通常、CIMC では成功または失敗は示されないため、[クラスタのステータス（Cluster Status）] ページでこれらの詳細が確認できるようになった後に、UCS ファームウェアバージョンが更新されているか確認することをお勧めします。詳細が確認できるようになるまで最大 15 分かかります。

[ファームウェアのアップグレードログを表示（View Firmware Upgrade Logs）] ポップアップウィンドウの全体的なステータスの下にある [更新の進行状況（Update progress）] セクションには、ファームウェア更新の進行状況を示すタイムスタンプ付きのログメッセージが含まれます。これらのログメッセージに [ホストの再起動が進行中です（Rebooting Host In Progress）] ステータスが表示されると、CIMC で更新が制御され、クラスタがその更新をモニターします。後続のほとんどのログメッセージはCIMCから直接送信され、更新のステータスが変更された場合にのみログメッセージのリストに追加されます。

CIMC で個々のコンポーネント更新ステータスの提供が開始されると、[ファームウェアのアップグレードログを表示（View Firmware Upgrade Logs）] ポップアップの [更新の進行状況（Update progress）] セクションの下に、[コンポーネントの更新ステータス（Component update status）] セクションが表示されます。このセクションでは、ベアメタル上のさまざまな UCS コンポーネントの更新のステータスがすぐに把握できます。

# Data Backup And Restore（DBR）

データのバックアップと復元のオプションは、左側のナビゲーションバーの [プラットフォーム（Platform）] メニューにあります。

データのバックアップと復元では、Secure Workload クラスタ、コネクタ、および外部オーケストレータからオフサイトストレージに特定のデータがコピーされます。障害が発生した場合は、このオフサイトストレージから同じフォームファクタの任意のクラスタにデータを復元できます。

1. データのバックアップと復元は、物理クラスタ（8RU と 39RU の両方）でサポートされています。
2. データは、S3V4 API と互換性のある任意の外部オブジェクトストアにバックアップできます。任意のオブジェクトストアを使用できますが、Secure Workload にはデータをバックアップするために十分な帯域幅とストレージが必要になります。
3. バックアップには少なくとも 200TB のストレージが推奨されます。容量が不足すると、バックアップが失敗します。
4. データは互換性のあるフォームファクタのクラスタにのみ復元できます。たとえば、8RU クラスタからのデータは別の 8RU にのみ復元できます。

# データ バックアップ

バックアップは、ユーザー設定に基づいて、スケジュールされた時刻に1日1回トリガーされます。バックアップの成功は、チェックポイントと呼ばれます。チェックポイントは、クラスタのプライマリデータストアのポイントインタイムスナップショットです。フローデータベース、ADM、および適用エージェントの復元に必要なデータのみがバックアップされます。成功したチェックポイントを使用して、データを別のクラスタまたは同じクラスタに復元できます。

Mongo、Consul、およびVaultのデータは、すべてのチェックポイントで常に完全にバックアップされます。HDFS と Druid では、バックアップされるデータが大量になるため、増分変更のみがバックアップされます。必要に応じて、すべてのデータソースに対して完全バックアップをスケジュールすることもオンデマンドでトリガーすることもできます。完全バックアップでは、チェックポイント内のすべてのオブジェクトがコピーされます。オブジェクトが変更されていない場合でもコピーされます。これにより、クラスタ、オブジェクトストア間のネットワーク、およびオブジェクトストア自体にかなりの負荷がかかる可能性があります。完全バックアップをスケジュールせず、必要に応じてオンデマンドワークフローを使用することを推奨します。オブジェクトが破損している場合、またはオブジェクトストアに回復不能なハードウェア障害がある場合は、完全バックアップが必要になることがあります。さらに、バックアップ用に提供されたバケットが変更された場合、完全バックアップが自動的に実行されます。

# 前提条件

1. Data Backup and Restore（DBR）機能のアクティベーションキーを取得するには、taentitlement@cisco.com に電子メールを送信して DBR アクティベーションキーを要求します。電子メールにはクラスタ ID ファイルも添付します。
2. オブジェクトストアのアクセスキーと秘密鍵が必要です。DBRは、オブジェクトストアの事前認証されたリンクでは機能しません。
3. Secure Workloadアプライアンスがオブジェクトストアに使用する帯域幅を調整するポリシングを設定します。
4. FQDN を設定し、センサーホストが FQDN を解決できることを確認します。

（注） DBR を有効にすると、現在および将来のソフトウェア エージェント バージョンのみをインストールおよびアップグレードに使用できます。現在のクラスタバージョンより古いソフトウェア エージェント バージョンは、互換性がないため非表示のままです。

### センサー/Kafka FQDN の要件

センサーは、IP アドレスを使用して Secure Workload アプライアンスから制御情報を取得します。DBRを有効にして、災害後のシームレスなフェイルオーバーを可能にするため、センサーを FQDN の使用に切り替える必要があります。このスイッチでは、Secure Workload クラスタ

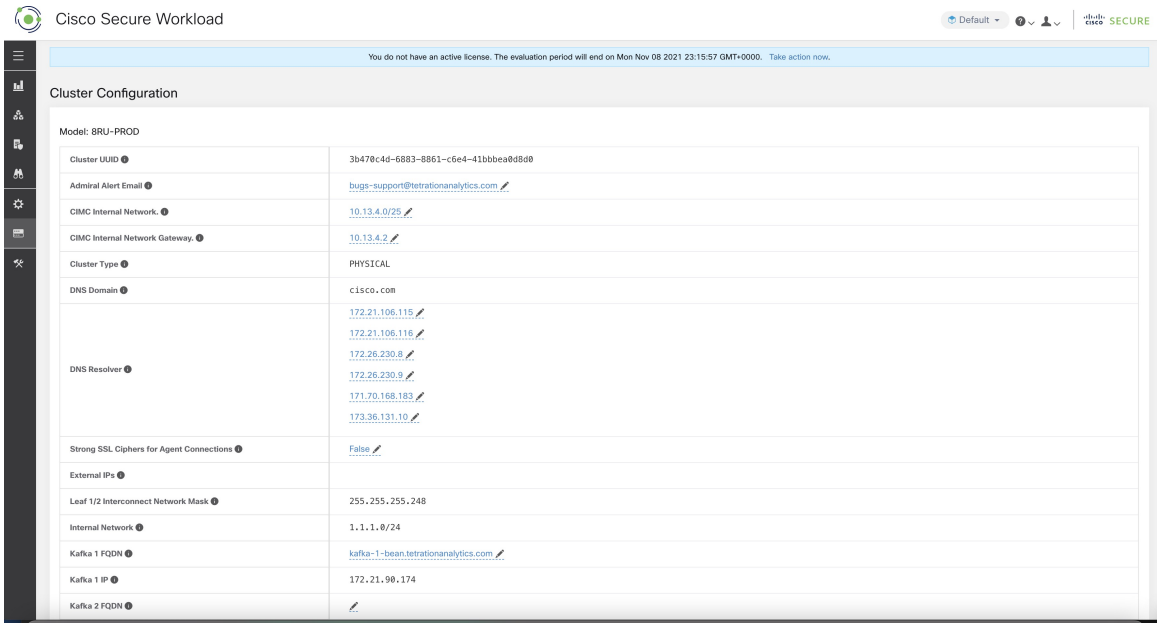
のアップグレードだけでは不十分です。センサーは、リリース 3.3 以降で FQDN の使用をサポートします。そのため、センサーのフェイルオーバーを有効にして DBR 対応にするには、センサーがリリース 3.3 にアップグレードされていることを確認してください。

FQDN が設定されていない場合、デフォルトの FQDN は次のとおりです。

| IP タイプ（IP Type） | デフォルトの FQDN |
|---|---|
| センサー VIP | wss{{cluster_ui_fqdn}} |
| Kafka 1 | kafka-1-{{cluster_ui_fqdn}} |
| Kafka 2 | kafka-2-{{cluster_ui_fqdn}} |
| Kafka 3 | kafka-3-{{cluster_ui_fqdn}} |

FQDN は、**[プラットフォーム（Platform）]** > **[クラスタ設定（Cluster Configuration）]** ページで変更できます。

**図 *16 : [クラスタ設定（Cluster Configuration）]* ページの *DBR* 用 *FQDN/IP***




これらの FQDN の DNS レコードを、同じページで提供される IP で更新します。IP と FQDN のマッピングは次のとおりです。

| フィールド名 | 対応する IP フィールド | 説明 |
|---|---|---|
| センサー VIP FQDN | センサー VIP | FQDN を更新してクラスタ コントロール プレーンに接続する |
| Kafka 1 FQDN | Kafka 1 IP | アドホック Kafka ノード 1 IP |

| フィールド名 | 対応する IP フィールド | 説明 |
|---|---|---|
| Kafka 2 FQDN | Kafka 2 IP | アドホック Kafka ノード 2 IP |
| Kafka 3 FQDN | Kafka 3 IP | アドホック Kafka ノード 3 IP |

（注） 注：センサー VIP および kafka ホストの FQDN は、DBR が構成される前にのみ変更できます。DBR が設定されると、FQDN は変更できません。

# オブジェクトストアの要件

オブジェクトストアは、S3V4 準拠のインターフェイスを提供する必要があります。

**Bucket**

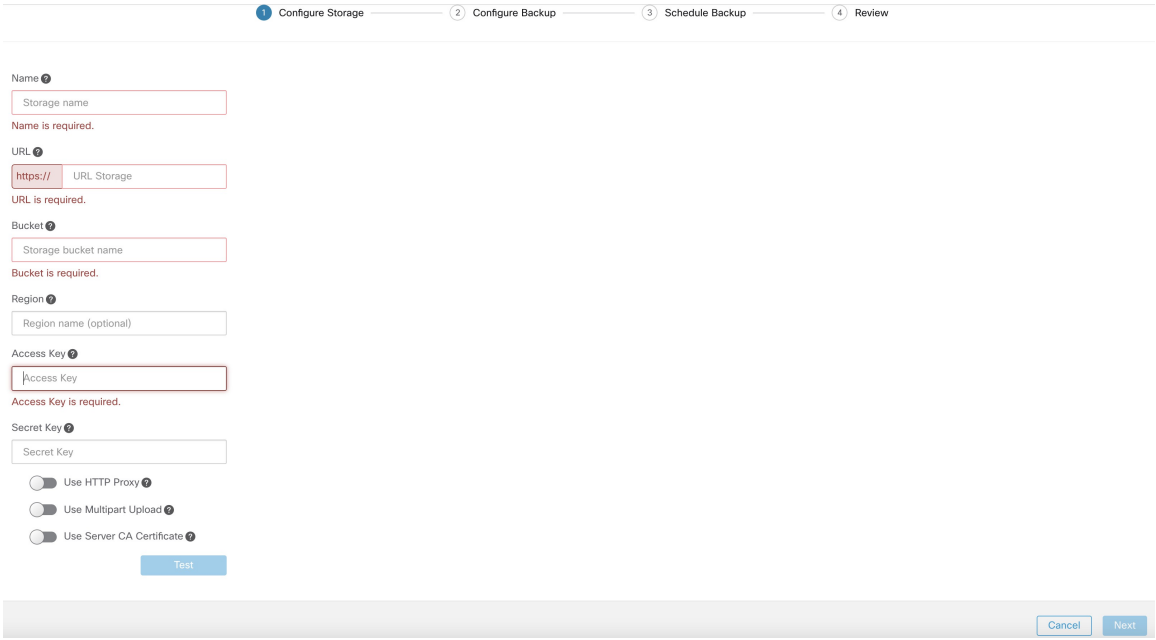
オブジェクトストアの Secure Workload に、専用の新しいバケットを作成します。このバケットへの書き込みアクセス権を持つのは Secure Workload クラスタのみです。Secure Workload クラスタはオブジェクトを書き込み、バケットの保持を管理します。バケット用に少なくとも 200 TB のストレージをプロビジョニングし、バケットのアクセスと秘密鍵を取得します。Secure Workload は事前認証されたリンクでは機能しません。

オブジェクトストアとして Cohesity が使用されている場合は、スケジュール時にマルチパートアップロードを無効にします。

**HTTPS**

Secure Workload のデータバックアップは、オブジェクトストアでの https インターフェイスのみをサポートします。オブジェクトストアへ転送中のデータが暗号化され、安全であることを保証するためです。ストレージ SSL/TSL 証明書が信頼できるサードパーティ CA によって署名されている場合、クラスタはその証明書を使用してオブジェクトストアを認証します。オブジェクトストアが自己署名証明書を使用している場合は、[サーバーCA証明書を使用（Use Server CA Certificate）] オプションを選択して、公開キーまたは CA をアップロードできます。

図 *17*: 自己署名証明書を提供するサーバー *CA* 証明書オプション




### サーバー側の暗号化

Secure Workload に提供されるバケットのサーバー側の暗号化をオンにすることも強く推奨します。Secure Workload クラスタは、HTTPS を使用してデータをオブジェクトストアに転送します。ただし、オブジェクトストアはオブジェクトを暗号化して、保存されたデータの安全性を確保する必要があります。

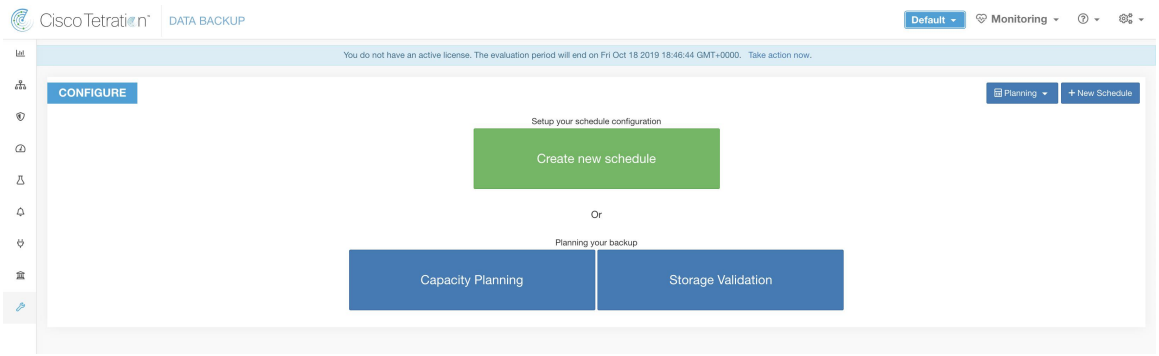
# データのバックアップの設定

### ステップ 1 - 計画

バックアップでは、プランナーを使用して、オブジェクトストアへのアクセスをテストし、ストレージ要件と、各日に必要なバックアップ期間を決定することができます。これは、実際にスケジュールを設定する前の試験に使用できます。

DBR 計算ツールを使用するには、**[プラットフォーム（Platform）]>[データバックアップ（Data Backup）]** に移動します。DBR が設定されていない場合は、データバックアップのランディングページに移動します。

**図 *18* : バック アップランディング ページ**



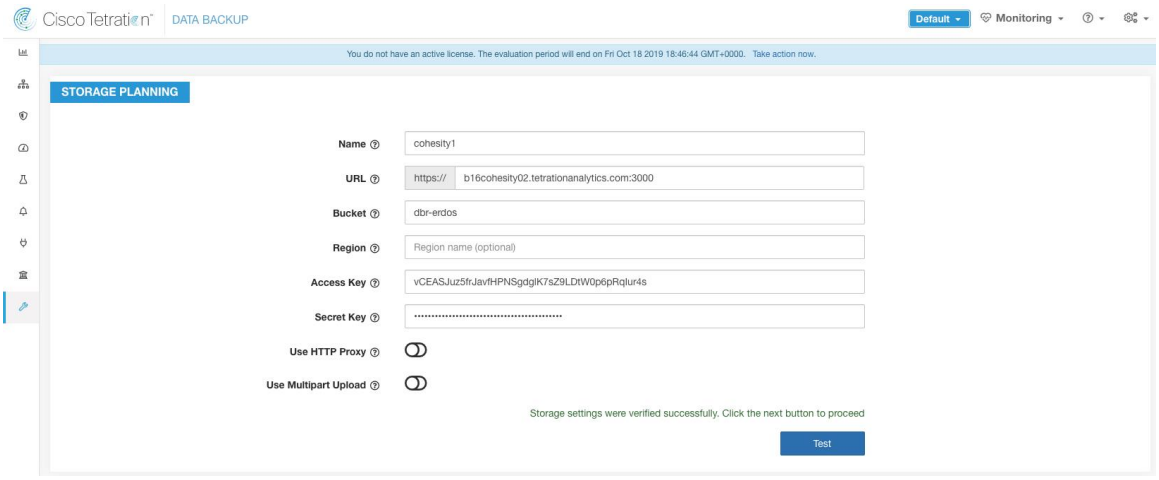

（注） **[メンテナンス（Maintenance）]に[データバックアップ（Data Backup）]オプションがない場合は、DBR を有効にするライセンスがあることを確認してください。**

ストレージと Secure Workload の互換性を確保するため、[ストレージプランニング（Storage Planning）] オプションを使用します。[ストレージプランニング（Storage Planning）] をクリックして、ストレージ設定を入力します。検証では次のことがテストされます。

- オブジェクトストアとバケットにアクセスし認証します。
- 設定されたバケットにアップロードし、そのバケットからダウンロードします。
- 帯域幅をチェックします。

完了までに 5 分ほどかかる場合があります。

**図 *19* : バックアップの *[ストレージプランニング（Storage Planning）]* ページ**



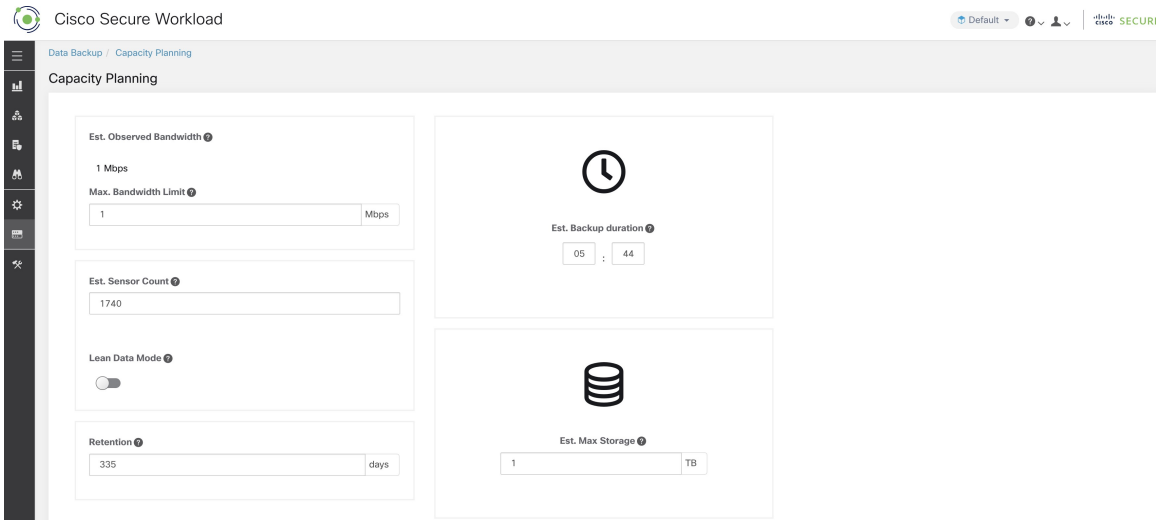

テストが完了すると、ステータスメッセージが表示されます。テストに失敗した場合は、次を確認してください。

1. URL は正しいかどうか。

2. アクセス/秘密鍵は正しいかどうか。
3. バケットが存在するかどうか。
4. ストレージに直接アクセスする必要がある場合は、プロキシを設定します。
5. Cohesity を使用している場合は、マルチパートアップロードを無効にします。

Capacity Planner を使用して、想定されるストレージサイズとバックアップ時間を計画できます。

**図 *20* : バックアップ キャパシティ プラン**



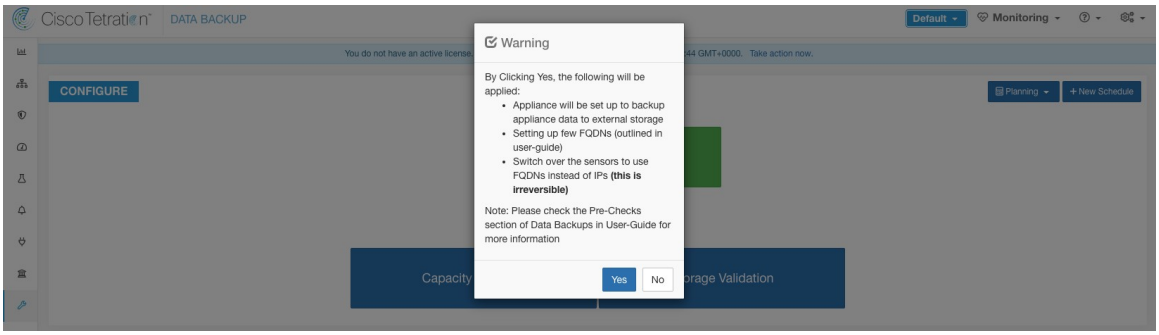

- [最大帯域幅制限（Max Bandwidth Limit）]：データのバックアップ中に使用できる最大帯域幅。この帯域幅は、オブジェクトストアへのデータをスロットリングするポリサー設定の値以下である必要があります。
- [推定センサー数（Est. Sensor Count）]：この値はデフォルトで既存の登録済みセンサーの数に設定されますが、予測に基づいて変更できます。
- [保持（Retention）]：オブジェクトストアでの保持の想定日数。
- [推定バックアップ時間（Est. Backup Duration）]：1 日分のデータをバックアップするのに必要な時間。この値は、上記で設定した一般的なセンサー負荷、推定センサー数、および最大帯域幅に基づく推定値です。
- [推定最大ストレージ（Est. Max Storage）]：この値は、指定された保持期間と推定センサー数のサポートに Secure Workload が必要とする最大ストレージの推定値です。

### ステップ 2 - 設定

Secure Workload は、設定された時間枠でのみ、データをオブジェクトストアにコピーします。バックアップ設定ウィザードは、プランナーと同様に、ストレージ/時間枠の設定手順を順次示します。

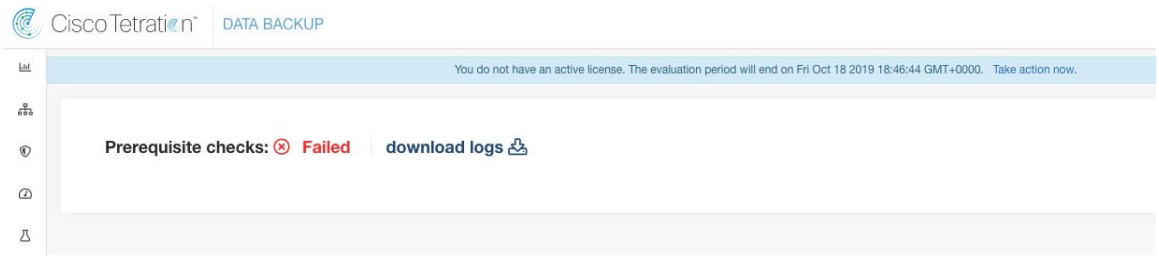
バックアップを設定するには、データバックアップのランディングページで[新しいスケジュールの作成（Create new schedule）] をクリックします。バックアップを初めて設定するときに、事前チェックが実行され、FQDN が解決可能であり、正しい IP に解決されることを確認します。それが検証されると、クラスタに現在登録されているすべてのセンサーに更新がプッシュされ、FQDN の使用に切り替わります。FQDN がないと、センサーはディザスタイベント後に別のクラスタにフェイルオーバーできません。FQDN の使用をサポートするには、クラスタでサポートされている最新バージョンにセンサーをアップグレードする必要があり、すべてのセンサーがセンサー VIP FQDN を解決できる必要があります。リリース 3.3 の時点では、詳細可視性センサーと適用センサーのみが DBR をサポートしており、FQDN の使用に切り替えます。残りのセンサーは引き続き IP を使用します。

**図 *21* : バックアップの警告 - *FQDN* が設定されていることを確認します。**



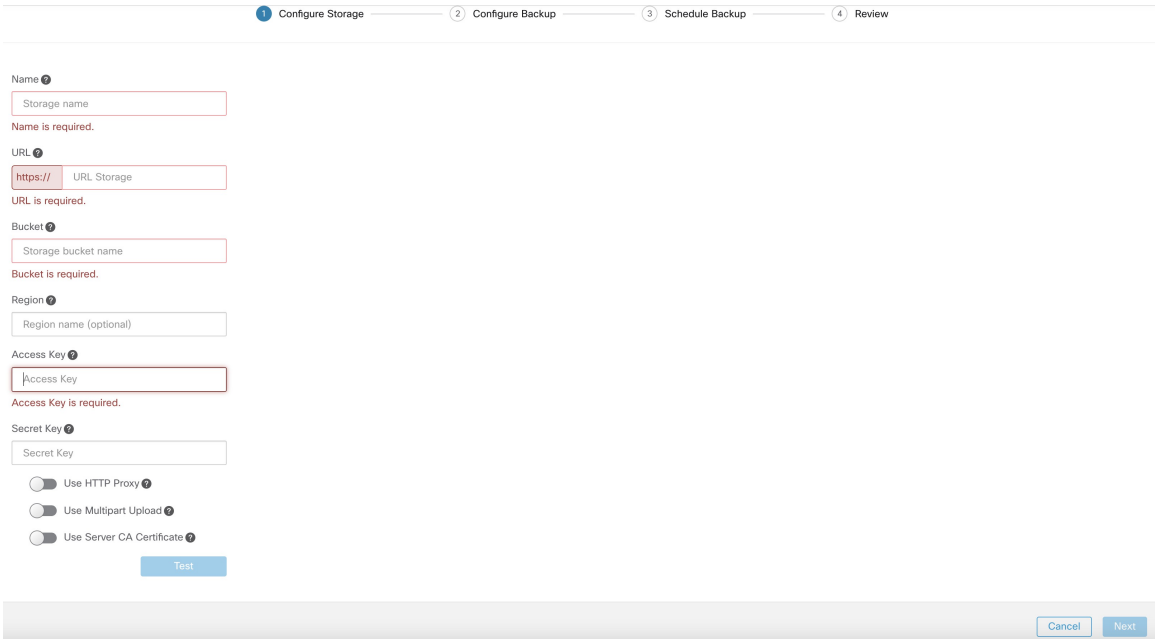

警告ボックスで [はい（Yes）] をクリックして、前提条件チェックを続行します。前提条件チェックでエラーが発生した場合、詳細ログにステータスが「Failed」と表示されます。

**図 *22* : 失敗した事前要件チェック**



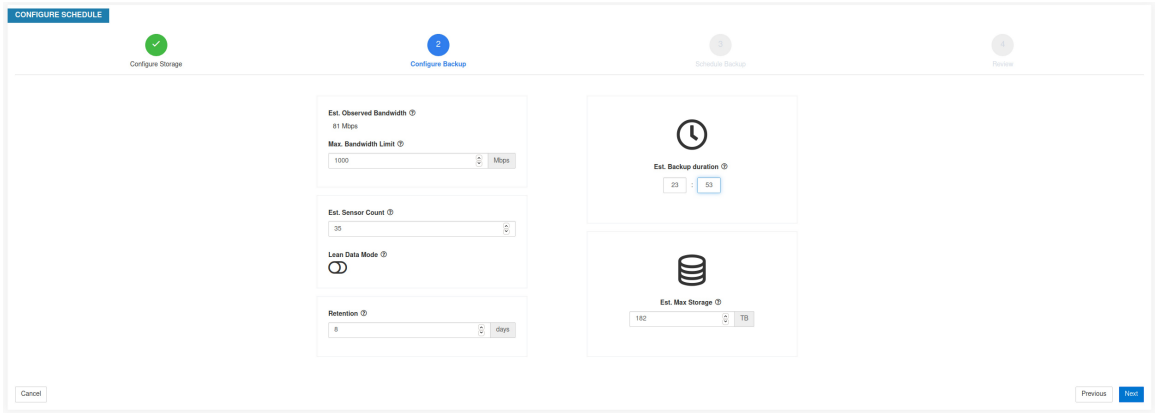

すべての事前要件チェックに合格したら、ストレージ情報の入力に進みます。

**図 *23* : ストレージの設定**




ストレージの検証後、[次へ（Next）]をクリックしてキャパシティのプランニングに移行します。

**図 *24* : キャパシティ プランニング**

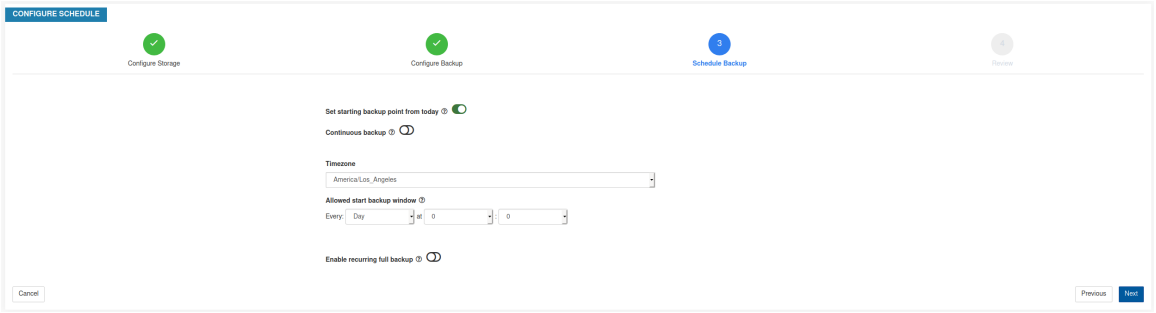



これら2つの手順は、プランニングフェーズとまったく同じです。リーンデータモードが選択されている場合、フローデータはバックアップされません。このモードは、バックアップストレージが限られている場合に便利です。[次へ]をクリックして、スケジュールの設定に移行します。

- [バックアップの開始点を今日からに設定（Set starting backup point from today）]：（デフォルトで有効）このオプションでは、設定日の午前0時（UTC）より前に作成されたすべてのファイルが無視されます。一定の期間稼働しているクラスタでは、初日にバックアップされるデータが大量に存在する場合があり、クラスタ、ネットワーク、およびオブジェク

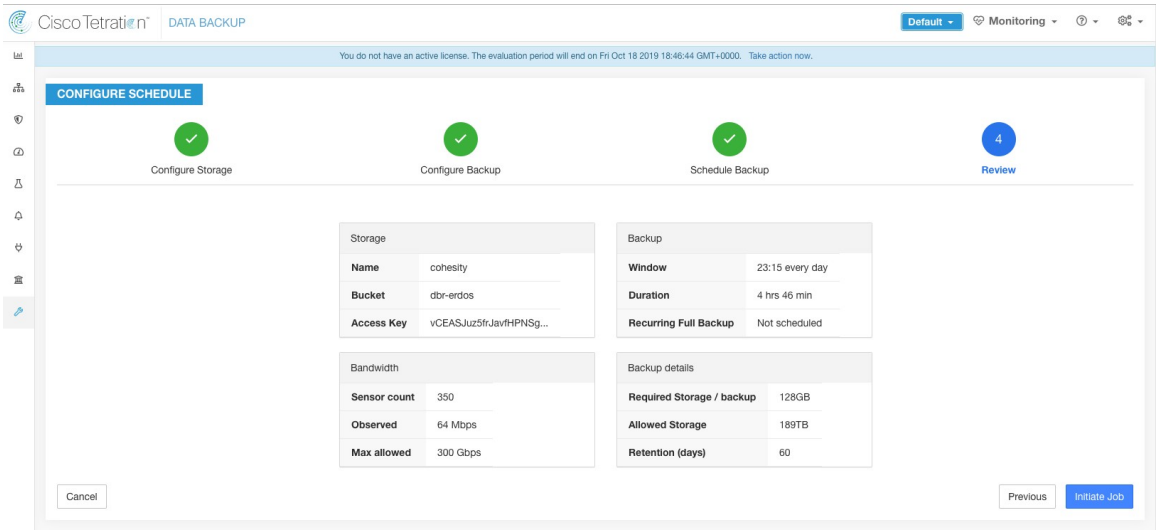
トストアに過剰な負荷がかかる可能性があります。このオプションに関係なく、すべての設定が引き続きバックアップされます。

- [タイムゾーン（Tmezone）]：デフォルトはブラウザのタイムゾーンです。
- [許可されるバックアップ開始時間（Allowed Start backup window）]：バックアップが開始される時間/分（24 時間形式）。
- [定期的な完全バックアップの有効化（Enable recurring full backup）]（デフォルトでは無効）：オンにすると、完全バックアップのスケジュールを選択するオプションが表示されます。完全バックアップのスケジュールを使用しないようにお勧めします。
- [継続的バックアップ（Continuous backup）]：このオプションを選択すると、バックアップが可能な限り頻繁に実行されます。




最後の手順は、バックアップジョブを確認して開始することです。

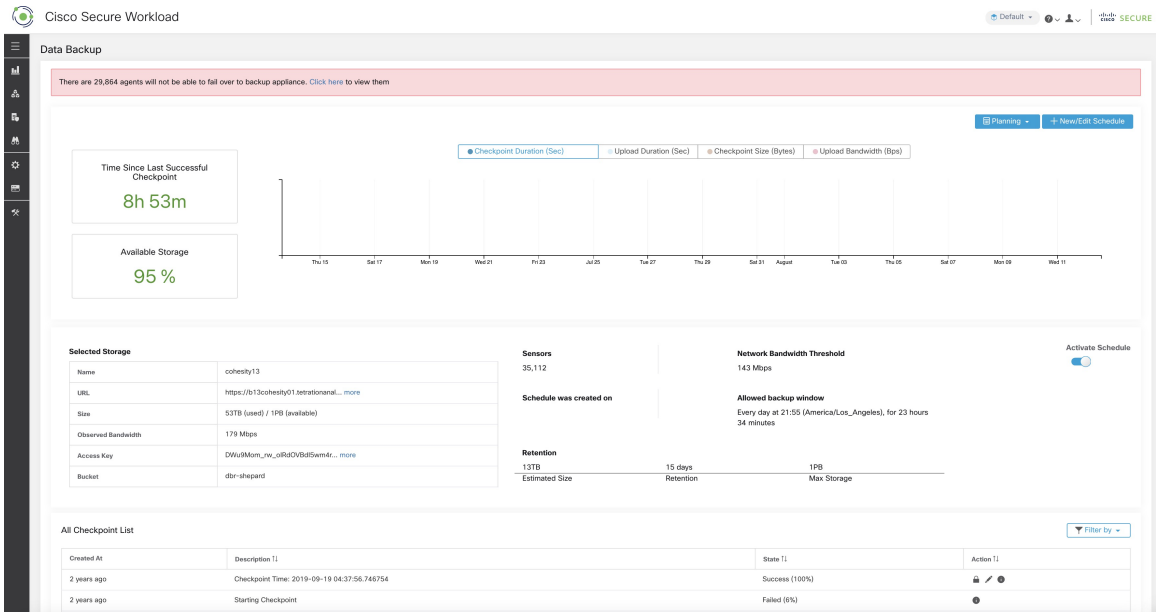
**図 *25*：バックアップ設定のレビュー**



# バックアップステータス

設定後、スケジュールされた時刻に毎日バックアップがトリガーされます。バックアップのステータスは、[データバックアップ（Data Backup）] ダッシュボード（**[プラットフォーム（Platform）] > [データバックアップ（Data Backup）]**）で確認できます。

**図 *26* : バックアップ/チェックポイントの状態**




最後に成功したチェックポイントからの経過時間は、チェックポイントにかかる時間と 24 時間を足した時間未満である必要があります。チェックポイントとバックアップに約 6 時間かかる場合、最後に成功したチェックポイントからの経過時間は 30 時間未満である必要があります。

ダッシュボードには、チェックポイントとバックアップに関する他のグラフがいくつかあります。

この表は、すべてのチェックポイントを示しています。チェックポイントラベルは編集可能で、復元中にチェックポイントを選択するときにラベルを使用できます。ラベルは、チェックポイントの [アクション（Action）] の下にある [編集（Edit）] オプションをクリックして編集できます。

チェックポイントは複数の段階を経て次のステータスとなる場合があります。

- 作成済み/保留中（created/pending）：チェックポイントは作成済みで、コピーされるのを待機しています。
- 実行中（running）：データは外部ストレージにアクティブにバックアップされています。
- 成功（success）：チェックポイントが完了し、成功しました。復元に使用できます。
- 失敗（failed）：チェックポイントは完了しましたが失敗しました。復元には使用できません。

• 削除中/削除済み（deleting/deleted）：期限切れのチェックポイントを削除中です。

スケジュールまたはバケットを変更するには、[新規スケジュール/スケジュールの編集（New/Edit Schedule）] をクリックします。バックアップの設定に使用したものと同じウィザードが表示されます。

## バックアップスケジュールの非アクティブ化

[スケジュールをアクティブ化（Activate Schedule）] ボタンを無効にすることで、バックアップを非アクティブ化できます。スケジュールを変更する前に、バックアップスケジュールを非アクティブ化することをお勧めします。スケジュールを無効にするのは、進行中のチェックポイントがない場合のみにしてください。チェックポイントの進行中にテストを実行したり、スケジュールを無効にすると、進行中のチェックポイントが失敗する可能性があります。

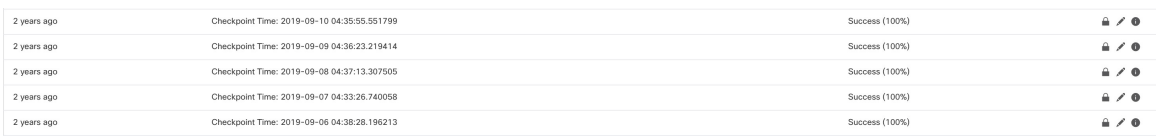
# オブジェクトストアの保持

Secure Workload クラスタは、バケット内のオブジェクトのライフサイクルを管理します。ユーザーがバケットのオブジェクトを削除または追加してはなりません。これを行うと、不整合が発生し、正常なチェックポイントが破損する可能性があります。設定ウィザードで、使用する最大ストレージを指定します。Secure Workload は、バケットの使用量がこの制限内にとどまるようにします。オブジェクトをエージアウトしてバケットから削除するストレージ保持サービスがあります。ストレージ使用量は設定された最大ストレージと受信データレートに基づいて計算されます。保持サービスは、使用量がしきい値に達するとすぐに、使用量を T1 に減らすために、保存されていないチェックポイントを削除しようとします。また、保持サービスでは、常に最低2つの成功したチェックポイントと、保存されたすべてのチェックポイント（いずれか多い方）が維持されます。保持サービスでチェックポイントを削除して容量を空けることができない場合、チェックポイントでエラーが発生し始めます。

# チェックポイントの保持

新しいチェックポイントが作成されると、古いチェックポイントはエージアウトになり、削除されます。ただし、チェックポイントを保持することができ、保持設定により削除されることがなくなります。保持されたチェックポイントは削除されません。保持されたチェックポイントが複数ある場合、ある時点で新しいオブジェクト用のストレージがなくなりますが、エージアウトしたチェックポイントは保持されているため削除されません。ベストプラクティスとして、必要に応じて保持を使用し、参照用としてラベルにその理由と妥当性を含めてチェックポイントを更新します。チェックポイントを保持するには、右側のロックアイコンをクリックします。

**図 *27 :* チェックポイントの保持**



# データの復元

データの復元操作は、左側のナビゲーションバーの [プラットフォーム（Platform）] メニューで実行できます。

バックアップデータを使用してクラスタを復元するには、クラスタが DBR スタンバイ モードになっている必要があります。現在、クラスタは展開時にのみスタンバイモードに設定できます。

次の組み合わせが可能です。

| プライマリクラスタ SKU | スタンバイクラスタ SKU |
|---|---|
| 8RU-PROD | 8RU-PROD、8RU-M5 |
| 8RU-M5 | 8RU-PROD、8RU-M5 |
| 39RU-GEN1 | 39RU-GEN1、39RU-M5 |
| 39RU-M5 | 39RU-GEN1、39RU-M5 |
| OCI | OCI |

## スタンバイモードの展開

### スタンバイモードの展開

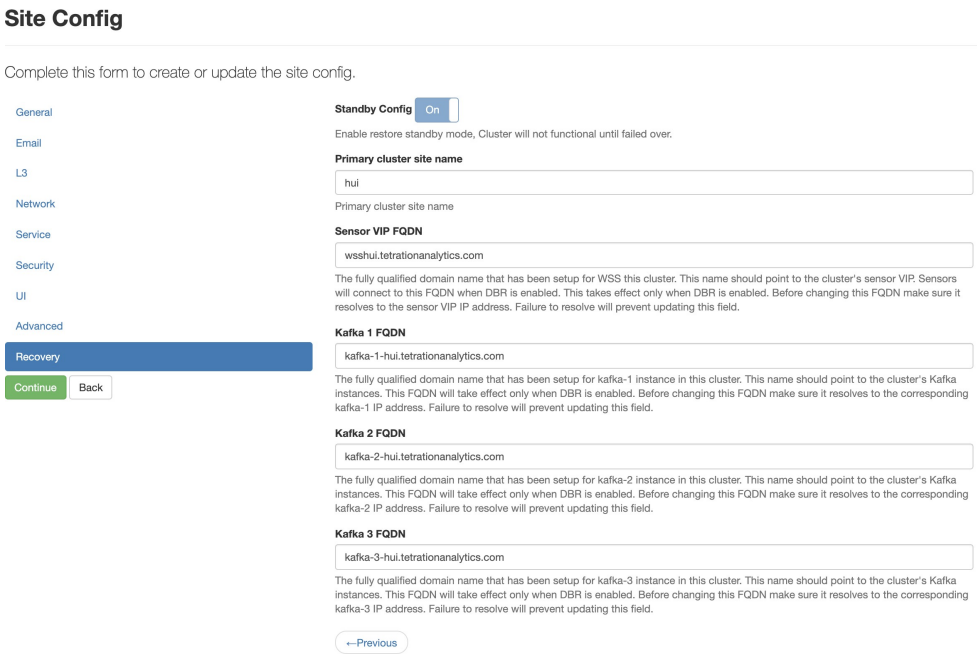
データの復元を開始するには、シスコに連絡してください。

サイト情報でリカバリオプションを設定することにより、クラスタをスタンバイモードで展開できます。展開中にサイト情報を設定するときに、[リカバリ（Recovery）] タブで復元の詳細を設定します。

クラスタをスタンバイモードで展開するには、[リカバリ（Recovery）] タブで次のように設定します。

1. [スタンバイ設定（Standby Config）] を [オン（On）] に設定します。
2. プライマリクラスタ名と FQDN を設定します。

展開の残りの部分は、通常の展開とまったく同じです。




展開後にプライマリクラスタ名とFQDNを再設定して、スタンバイクラスタが別のクラスタを追跡できるようにすることができます。この設定は、[クラスタ設定（Cluster Configuration）]ページからフェイルオーバーがトリガーされる前に、後で再設定できます。

DBR スタンバイモードのクラスタには、スタンバイモードバナーが表示されます。

**図 *28 :* スタンバイバナー**

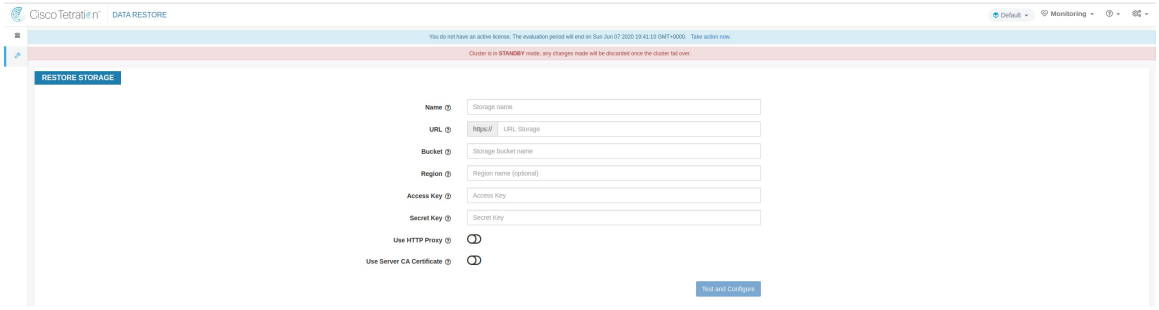

[DBRの復元（DBR Restore）]ページに移動するには、Secure Workload Web インターフェイスの左側にあるナビゲーションバーから**[プラットフォーム（Platform）]>[データの復元（Data Restore）]**を選択します。

## データのプリフェッチ

クラスタを復元する前に、データをプリフェッチする必要があります。データは、データのバックアップに使用されるのと同じストレージバケットからプリフェッチされます。バックアップサービスがストレージからダウンロードできるようにするには、ログイン情報を提供する必要があります。ストレージがプリフェッチ用に設定されていない場合、ユーザーは[データの復元（Data Restore）]タブからセットアップウィザードに直接移動されます。

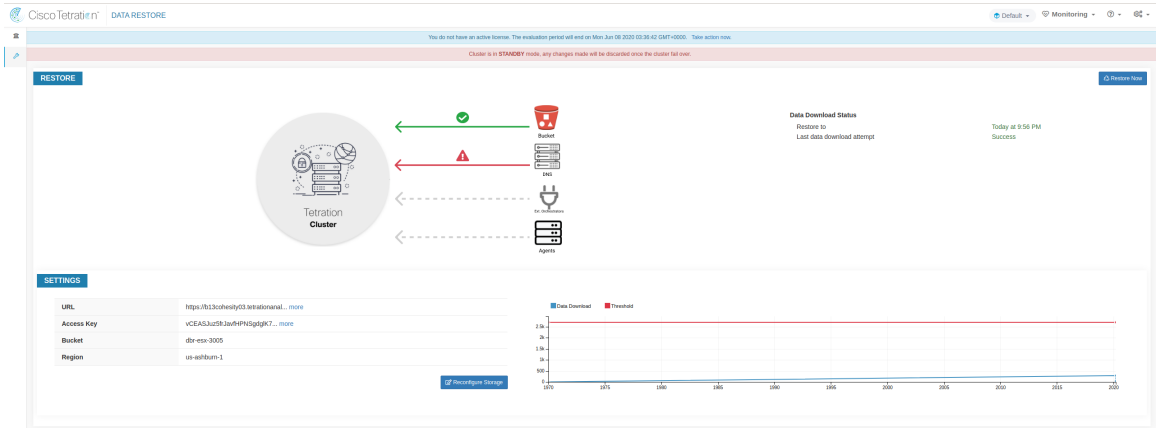
**スタンバイクラスタは、S3 ストレージとのみ対話します。プライマリクラスタのバックアップを更新して別のストレージ/バケットを使用する場合、スタンバイクラスタのストレージを更新する必要があります。**

図 *29 : ストレージのセットアップウィザード*




情報がテストされると、ストレージはプリフェッチ用に自動設定されます。[DBRの復元（DBR Restore）] タブにプリフェッチステータスが表示されるようになるはずです。

図 *30 : DBR プリフェッチステータス*




[ステータス（Status）] ページは、ユーザーにさまざまなデータを提供します。

**ステップ 1** 左上の部分には、復元を開始するためのさまざまなコンポーネントの準備ができていることを示す図があります。データを確認するには、コンポーネントにカーソルを合わせてください。関連するデータが右上の部分に表示されます。

[バケット（Bucket）] : プリフェッチの状態を示します。最新のデータが 45 分以上前のものである場合、赤で表示されます。

[DNS] : スタンバイクラスタ IP に関する Kafka および WSS FQDN 解決を示します。復元中に、FQDN がスタンバイクラスタ IP に更新されない場合、センサーは接続できません。FQDN がスタンバイクラスタへの解決を開始すると、緑色に変わります。

[外部オーケストレータ（Ext. Orchestrators）] : スタンバイクラスタから外部オーケストレータへの接続を示しています。

[エージェント（Agents）] : スタンバイクラスタに正常に切り替えられたエージェントの数を示しています。これは復元がトリガーされた後にのみ関係します。

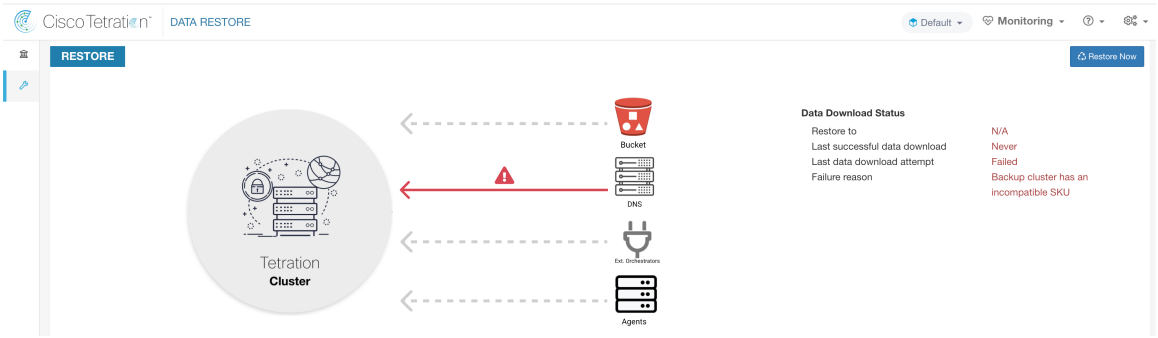
**ステップ 2** 右上の部分には、左上の部分で選択した図に関連する情報が表示されます。右上隅にある [今すぐ復元（Restore Now）] をクリックすると、復元プロセスが開始されます。

**ステップ 3** 左下の部分は、使用中のプリフェッチストレージ設定を示しています。

**ステップ 4** 右下の部分は、プリフェッチ遅延のグラフを示しています。

データのプリフェッチは、迅速な復元を確実にするために、いくつかの必要なコンポーネントを更新します。データのプリフェッチが失敗した場合、ステータスページに理由が表示されます。

**図 *31 : DBR* プリフェッチのエラー事例**




プリフェッチの失敗原因となる一般的なエラーを次に示します。

S3 アクセスエラー：この場合、ストレージからのデータを正常にダウンロードできませんでした。これは、無効なログイン情報、ストレージポリシーの変更、または一時的なネットワークの問題が原因で発生する可能性があります。

互換性のないクラスタバージョン：復元が行えるのは、バックアップクラスタと同じ Secure Workload バージョンを実行しているクラスタに対してのみです。これは、アップグレード中にクラスタの 1 つだけが展開されている場合に発生することがあります。または、展開中に、別のバージョンが展開に使用されている場合です。クラスタを共通バージョンにアップグレードすると、この問題が解消されます。

互換性のない SKU バージョン：プライマリクラスタを踏まえて、スタンバイクラスタで許可されている SKU に注意してください。プライマリクラスタの SKU の復元には、特定の SKU のみが許可されます。

## クラスタの復元

クラスタの復元は、[復元ステータス（Restore Status）] ページの右上隅にある [今すぐ復元（Restore Now）] ボタンをクリックしてトリガーできます。復元アクションがトリガーされる前に、確認を求められます。

クラスタデータは 2 つのフェーズで復元されます。

**必須フェーズ**：サービスを再開するために必要なデータが最初に復元されます。このデータはすでにプリフェッチされています。必須フェーズにかかる時間は、インストールされているセンサーの数、バックアップされるデータの量などによって異なります。必須フェーズ中は、UI にアクセスできません。**必須フェーズに UI にアクセスする必要が生じた場合、サポートを受けるにはワーキング TA ゲストキーが必要です。**

**レイジーフェーズ**：クラスタデータ（druid のフロー DB など）はバックグラウンドで復元され、クラスタの展開はブロックされません。また、クラスタ UI にアクセスでき、復元の進行中にバナーが表示されます。このフェーズ中、クラスタは動作可能であり、データパイプラインは正常に機能しています。

## アップグレード（DBR あり）

クラスタで **DBR** が有効になっている場合は、アップグレードを開始する前にスケジュールを非アクティブ化することを推奨します（「バックアップスケジュールの非アクティブ化」を参照）。これにより、アップグレードが開始される前に正常なバックアップが存在し、新しいバックアップがアップロードされないことが保証されます。チェックポイントのエラーを回避するため、スケジュールの非アクティブ化は、チェックポイントが進行中でないときにのみ実行してください。

# VM の情報

[トラブルシューティング（Troubleshoot）] メニューの [仮想マシン（Virtual Machine）] ページには、Cisco Secure Workload クラスタの一部であるすべての仮想マシンが表示されます。クラスタの起動またはアップグレード（あれば）中の展開ステータス、さらにパブリック IP も表示されます。クラスタ内のすべての VM はパブリックネットワークの一部ではないため、パブリック IP を持たない場合があることに注意してください。

# クラスタのアップグレード

アップグレードオプションにアクセスするには、左側のナビゲーションバーで[プラットフォーム（Platform）] > [アップグレード/再起動/シャットダウン（Upgrade/Reboot/Shutdown）] をクリックします。

アップグレードには2種類があります。ここでは、「フル」アップグレードプロセスについて説明します。このアップグレード中に、Orchestrator-VM を除くクラスタ内のすべての VM がシャットダウンされ、新しい VM が展開され、サービスが再プロビジョニングされます。クラスタ内のすべてのデータは、このアップグレード中に保持されます。ただし、このアップグレード中に発生する約 2 時間のダウンタイムを除きます。

## アップグレードの開始

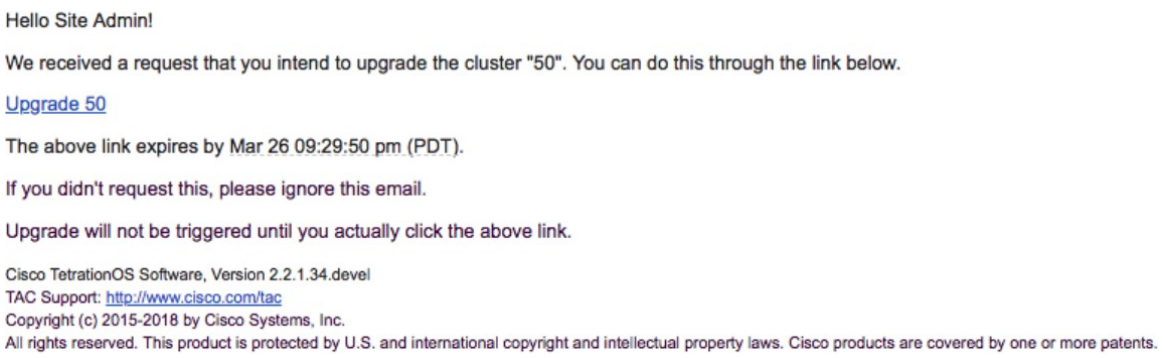
アップグレードを開始するには、左側のナビゲーションバーで[プラットフォーム（Platform）] > [アップグレード/再起動/シャットダウン（Upgrade/Reboot/Shutdown）] をクリックします。

アップグレードページには、クラスタのアップグレード/パッチアップグレード/シャットダウン/再起動オプションがあります。

フルアップグレードを開始するには、[アップグレードリンクの送信（Send Upgrade Link）] をクリックします。フルアップグレードを実行すると、オーケストレータ VM 以外のすべての

VM がシャットダウンされ、それらすべてがアップグレードおよび再展開されます。このため、2 時間以上のクラスタのダウンタイムが発生します。パッチアップグレードを実行するとダウンタイムは最小限に抑えられますが、パッチの適用が必要なサービスが更新されるだけで、VM は再起動されません。ダウンタイムは通常、数分程度です。パッチアップグレードを開始するには、[パッチアップグレードリンクの送信（Send Patch Upgrade Link）] をクリックします。電源を切った後にクラスタの再起動を開始するには、[再起動リンクの送信（Send Reboot Link）] を使用します。これらのリンクのいずれかをクリックすると、リンクを含む電子メールが生成され、アップグレードを開始したユーザーに送信されます。

**図 *32 :* フルアップグレードの開始**


Hello Site Admin!

We received a request that you intend to upgrade the cluster "50". You can do this through the link below.

Upgrade 50

The above link expires by Mar 26 09:29:50 pm (PDT).

If you didn't request this, please ignore this email.

Upgrade will not be triggered until you actually click the above link.

Cisco TetrationOS Software, Version 2.2.1.34.devel
TAC Support: http://www.cisco.com/tac
Copyright (c) 2015-2018 by Cisco Systems, Inc.
All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. Cisco products are covered by one or more patents.

オーケストレータは電子メールを送信する前に、いくつかの検証チェックを実行して、クラスタがアップグレード可能であることを確認します。検証チェックの内容は次のとおりです。

1. 稼働停止中のノードがないことを確認します。
2. 各ベアメタルをチェックして、ハードウェア障害がないことを確認します。ハードウェア障害には以下が含まれます。
    1. ドライブの障害
    2. ドライブの予測可能な障害
    3. ドライブの欠落
    4. StorCLI の障害
    5. MCE ログエラー
3. すべての BM が稼働状態であることを確認します。39RU の場合はサーバーが 36 台以上、8RU の場合は 6 台以上であることを確認します。

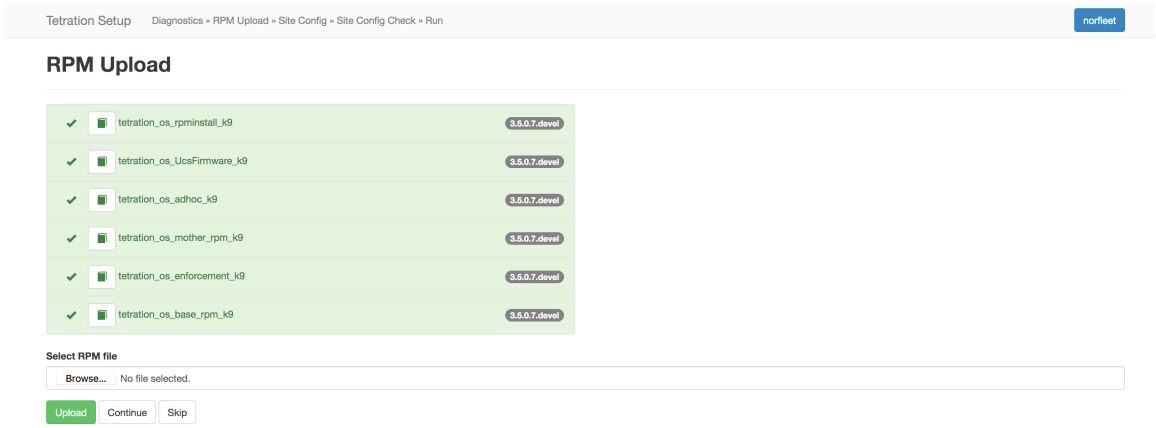
いずれかの障害がある場合は、アップグレードリンクは送信されません。HW エラーやホスト欠落などの情報を含む 500 エラーが表示されるため、オーケストレータログで詳細を確認します。このシナリオでは、ホストの orchestrator.service.consul にある /local/logs/tetration/orchestrator/orchestrator.log で、最後の 100 個のエラーメッセージを確認できます。ここで、3 つのチェックポイントのどれが障害の原因であるかに関する詳細情報が提供されます。このとき、通常はハードウェアの修正とノードの再稼働が必要になります。それが

完了したら、[アップグレードリンクの送信（Send Upgrade Link）] をクリックしてアップグレードを再開できます。

# RPM アップロード

電子メールのリンクをクリックすると、クラスタのセットアップ UI に接続します。セットアップ UI は、クラスタの展開とアップグレードで使用する操作 UI です。最初のページには、現在クラスタにインストールされている RPM のリストが表示されます。このページは、すべての RPM をアップロードするためのアップロードページでもあります。

**図 *33 : RPM* アップロード**




セットアップ UI に表示される順序で RPM をアップロードします。順序は次のとおりです。

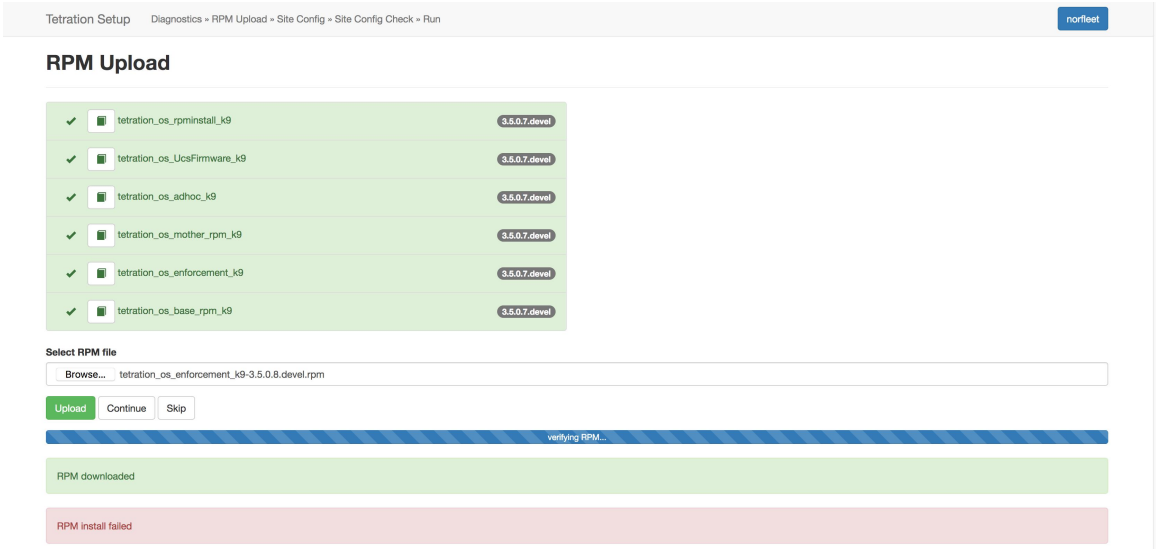
1. tetration_os_rpminstall_k9
2. tetration_os_UcsFirmware_k9
3. tetration_os_adhoc_k9
4. tetration_os_mother_rpm_k9
5. tetration_os_enforcement_k9
6. tetration_os_base_rpm_k9

（注） vSphere に展開された Secure Workload 仮想クラスタの場合は、必ず tetration_os_ova_k9 RPM もアップグレードしてください。tetration_os_base_rpm_k9 はアップグレードしないでください。

これ以外の順序でアップロードすると、アップロードが失敗します。すべての RPM が正しい順序でアップロードされるまで、[続行（Continue）] ボタンは無効になります。

各アップロードのログは、それぞれの RPM の左側にあるログ記号をクリックして表示できます。また、失敗したアップロードは赤色でマークされます。

図 *34 : RPM* アップロードログ




# サイト情報

次のステップは、サイト情報を更新することです。すべてのサイト情報フィールドが更新可能というわけではありません。次のフィールドのみを更新できます。

1. SSH 公開キー
2. Sentinel アラート電子メール（Bosun 用）
3. CIMC 内部ネットワーク
4. CIMC 内部ネットワークゲートウェイ
5. 外部ネットワーク。注：既存の外部ネットワークは変更しないでください。既存のネットワークに付加することで、さらにネットワークを追加できます。既存のネットワークを変更または削除すると、クラスタが使用できなくなります。
6. DNS リゾルバ
7. DNS ドメイン
8. NTP サーバ
9. SMTP サーバー（SMTP Server）
10. SMTP ポート（SMTP Port）
11. SMTP ユーザー名（オプション）
12. SMTP パスワード（オプション）
13. Syslog サーバー（オプション）

14. Syslog ポート（オプション）
15. Syslog シビラティ（重大度）（オプション）

（注） Syslogサーバーのシビラティ（重大度）は、クリティカルから情報提供までの範囲です。Bosunアラートのシビラティ（重大度）は、警告以上（情報提供）に設定する必要があります。

（注） バージョン 3.1 以降、セットアップ UI を介した外部 syslog はサポートされていません。ユーザーは、syslog にデータをエクスポートするように TAN アプライアンスを設定する必要があります。詳細については、「TAN に移行する外部 syslog トンネリング」を参照してください。

（注） Secure Workload は、STARTTLS コマンドを介した SSL/TLS 通信を行うメールサーバーとの安全なSMTP通信をサポートします。安全なトラフィックをサポートするサーバーの標準ポートは、通常は 587/TCP ですが、多くのサーバーは標準の 25/TCP ポートでも安全な通信を受け入れます。

**Secure Workload は、外部メールサーバーと通信するための SMTPS プロトコルをサポートしていません。**

残りのフィールドは更新できません。変更がない場合は、[続行（Continue）] をクリックしてアップグレード前のチェックをトリガーします。変更がある場合は、フィールドを更新して [続行（Continue）] をクリックします。

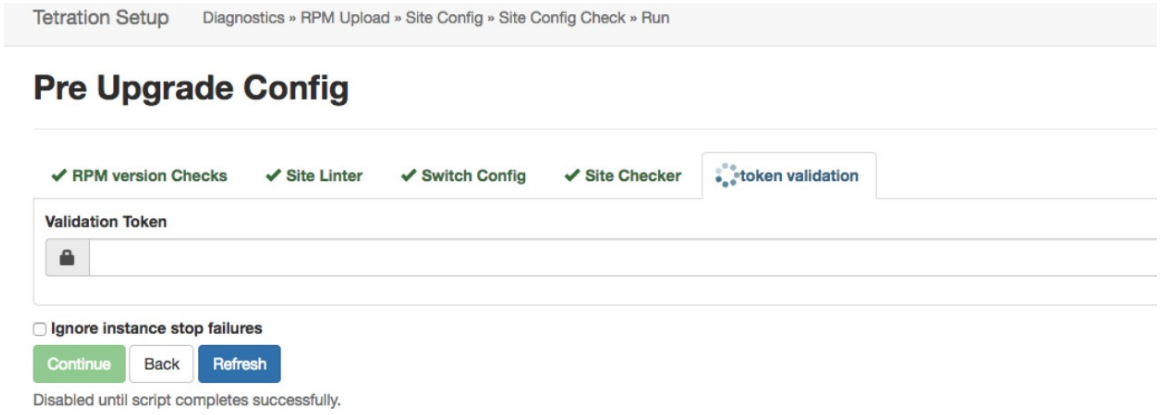
# アップグレードの事前チェック

アップグレードを開始する前に、クラスタでいくつかのチェックを行い、アップグレードを開始する前に問題がないことを確認します。

1. RPM バージョンチェック：すべての RPM がアップロードされ、バージョンが正しいことを確認します。状態が正しいかどうかを確認するのではなく、アップロードされたかどうかを確認するだけです。状態チェックは、アップロード自体の一部として実行されます。
2. サイトリンター：サイト情報のリンティングを行います。
3. スイッチ構成：リーフ/スパインスイッチを構成します。
4. サイトチェッカー：DNS、NTP、および SMTP サーバーのチェックを行います。最後にトークン付きの電子メールを送信します。このメールは、プライマリサイトの管理者アカウントに送信されます。DNS、NTP、または SMTP のいずれかのサービスが使用できない場合、この手順は失敗します。

5. トークンの検証：電子メールで送信されたトークンを入力し、[続行（Continue）]をクリックします。

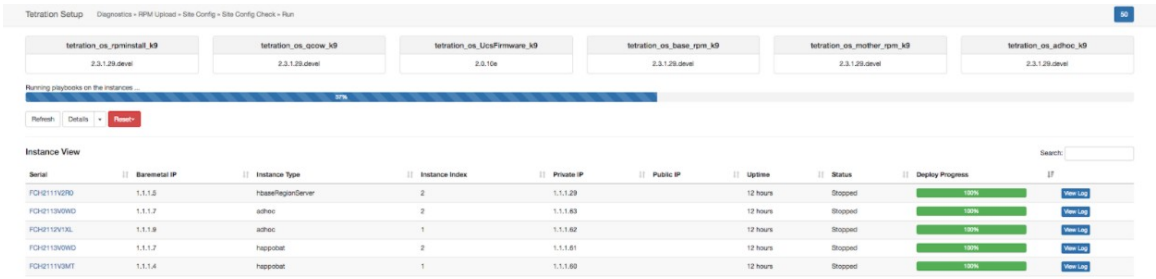
**図 *35*：アップグレードの事前チェック**




# クラスタのアップグレード

アップグレード前の手順が完了したら、「トークンの確認メール」で受け取ったトークンを入力した後に、[続行（Continue）]をクリックすると、アップグレードを開始できます。[障害時に停止を無視（Ignore Stop Failures）] という追加オプションがありますが、このオプションをオンにしてはいけません。これは、特定のサービスがシャットダウンせず、アップグレードが失敗した場合の回復オプションです。このオプションを使用すると、VM が強制的にシャットダウンされ、サービスの再稼働時に障害が発生する可能性があります。このオプションは、エンジニアの監督下で使用してください。

**図 *36*：クラスタのアップグレード**




[続行（Continue）] をクリックすると、アップグレードが開始されます。

**ステップ 1** 右上のクラスタ名をクリックすると、使用されているサイト情報が表示されます。

**ステップ 2** その下には、すべての Tetration_os RPM とそのバージョンがあります。

**ステップ 3** グローバルアップグレードバーには、アップグレードの進行状況が表示されます。進行中は青色、完了時は緑色、失敗時は赤色になります。進行状況バーのすぐ上に、アップグレードの現在のステータスが表示されます。

**ステップ 4** また、次の 3 つのボタンがあります。

a) [更新（Refresh）] : ページを更新します
b) [詳細]（Details）] : クリックすると、このアップグレード中に完了したすべてのステップが表示されます。ステップの横にある矢印をクリックすると、利用可能なすべてのログが表示されます。詳細については別途記します。
c) [リセット（Reset）] : オーケストレータの状態をリセットするオプションです。このオプションを選択すると、アップグレードがキャンセルされて、最初に戻ります。アップグレードに失敗した場合を除き、このボタンを使用しないでください。また、アップグレードが失敗した後、アップグレード再開前にすべてのプロセスが完了するまで数分かかります。
d) [再開（Resume）] : アップグレードに失敗すると、失敗した段階に応じて、再開オプションが表示されます。[再開（Resume）] をクリックすると、前回の安定していた部分からアップグレードが再開されます。

**ステップ 5** 次に、インスタンスビューが表示されます。個々の VM の展開ステータスがすべて追跡されます。インスタンスビューは次の列で構成されます。

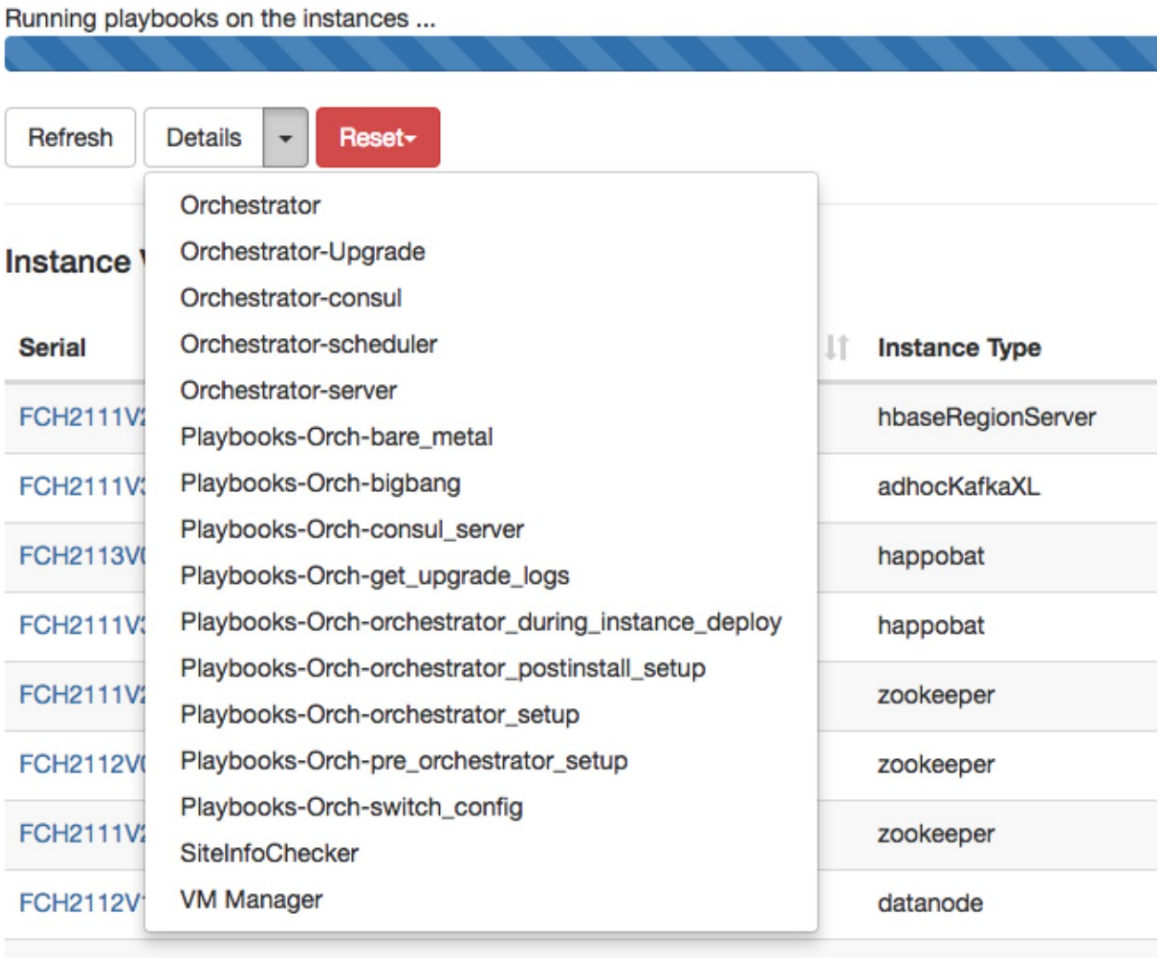
a) [シリアル（Serial）] : この VM をホストするベアメタルのシリアル番号
b) [ベアメタルIP（Baremetal IP）] : このベアメタルに割り当てられた内部 IP
c) [インスタンスタイプ（Instance Type）] : VM のタイプ
d) [インスタンスインデックス（Instance Index）] : VM のインデックス - 高可用性向けに同じタイプの VM が複数あります。
e) [プライベートIP（Private IP）] : この VM に割り当てられた内部 IP
f) [パブリックIP（Pubic IP）] : この VM に割り当てられたルーティング可能な IP - すべての VM にあるわけではありません。
g) [稼働時間（Uptime）] : VM の稼働時間
h) [ステータス（Status）] : [停止（Stopped）]、[展開（展開済み）]、[失敗（Failed）]、[未開始（未開始）]、[進行中（In Progress）] のいずれかです。
i) [展開の進行状況（Deploy Progress）] : 展開が完了した割合
j) [ログの表示（View Log ）] : VM の展開ステータスを表示するためのボタン

# ログ

ログには 2 つのタイプがあります。

1. VM 展開ログ：これらのログは、[ログの表示（View Log）] ボタンをクリックして表示できます。
2. オーケストレーションログ。詳細ボタンの横にある矢印をクリックすると、これらが表示されます。次のように表示されます。

図 *37* : ログ




各リンクはログを指します。

**ステップ 1** [Orchestrator] - オーケストレータログ：これは進行状況を追跡する最初の場所です。エラーが発生すると、別のログを指して参照します。

**ステップ 2** [Orchestrator-Upgrade] - 2.3 の NOP

**ステップ 3** [Orchestrator-consul]：プライマリオーケストレータで実行される consul ログ

**ステップ 4** [Orchestrator-Scheduler] - VM スケジューラログ：どの VM がどのベアメタルに配置されたかを示すログと、スケジューリングログ

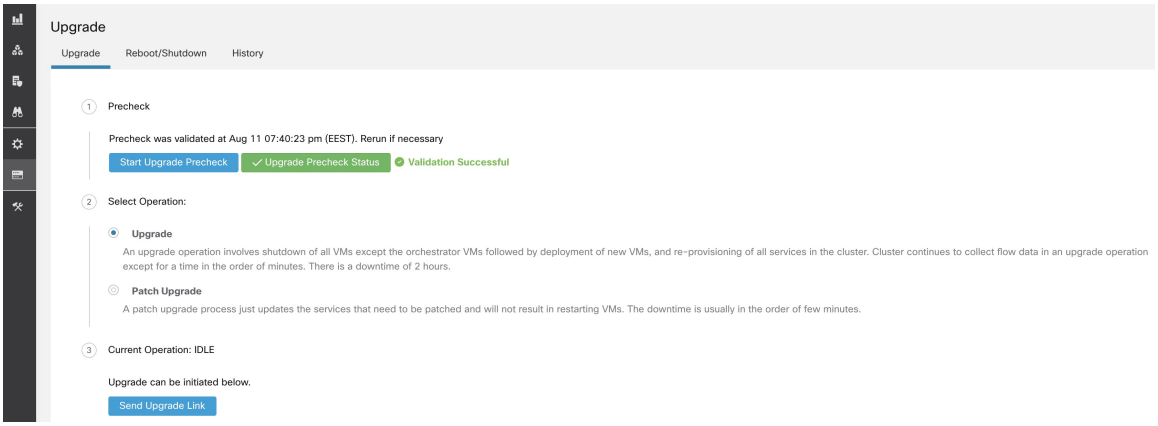
**ステップ 5** [Orchestrator-server]：オーケストレータからの HTTP サーバーログ

**ステップ 6** [Playbooks-*]：オーケストレータで実行されるすべての playbook ログ。

# アップグレードの事前チェックをいつでも実行

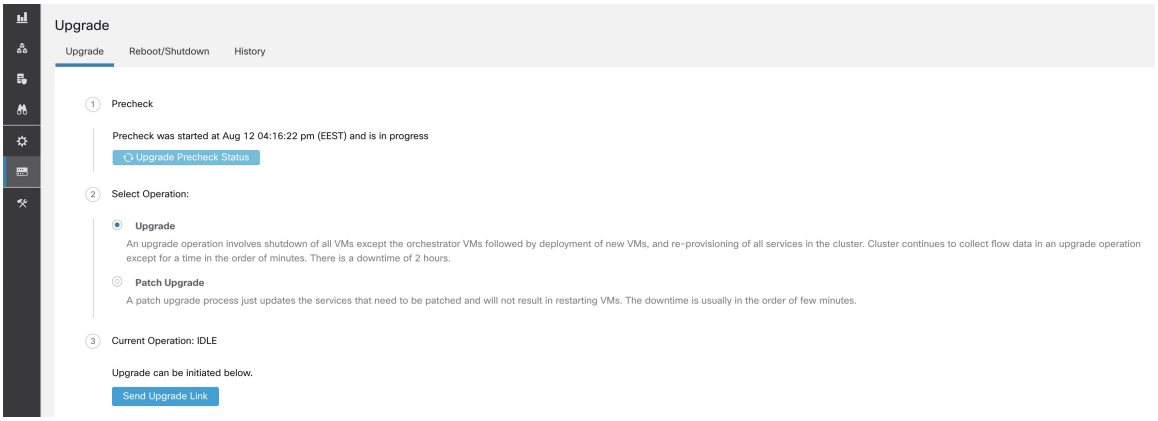
場合によっては、アップグレードをスケジュールした後、アップグレードを開始しているときに、ハードウェア障害が発生するか、クラスタをアップグレードする準備ができていないことがあります。アップグレードを続行する前に、これを修正する必要があります。アップグレードウィンドウまで待つ代わりに、アップグレードの事前チェックをいつでも開始できます。これらのチェックは、アップグレード/パッチ/再起動の開始時を除き、いつでも何度でも実行できます。アップグレードの事前チェックを任意のタイミングで実行するには、[アップグレード（Upgrade）] ページに移動します。

**図 *38* : アップグレードの事前チェックをいつでも実行する手順**



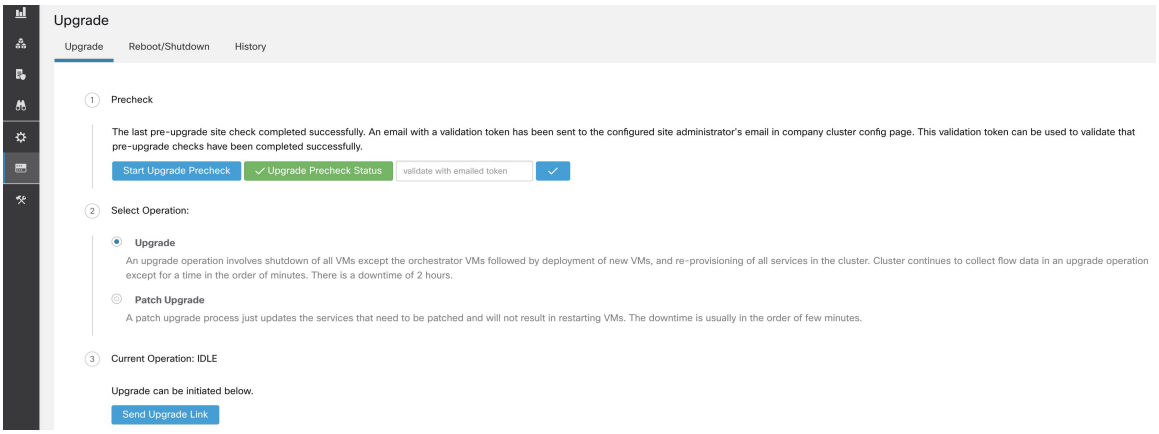

[アップグレードの事前チェックの開始（Start Upgrade Precheck）] をクリックします。これにより、アップグレードの事前チェックが開始され、実行状態に移行します。

**図 *39* : アップグレードの事前チェックをいつでも実行する手順**



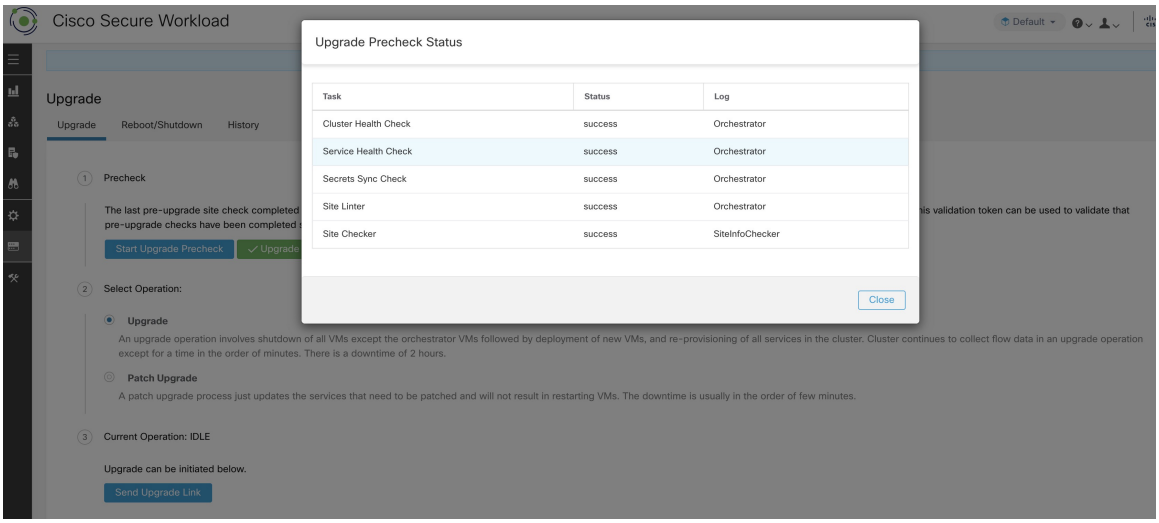

この間、オーケストレータはすべてのアップグレードの事前チェックを実行します。すべてのチェックに合格すると、チェックを開始したユーザーに、電子メールトークンが記載された電子メールが送信されます。トークンを入力して、アップグレードの事前チェックを完了します。

図 *40* : アップグレードの事前チェックをいつでも実行する手順




アップグレードの事前チェック中にエラーが発生した場合、失敗状態に移行し、失敗したタスクが表示されます。ステータスはいつでも確認でき、新しいダイアログボックスに表示されます。

図 *41* : アップグレードの事前チェックをいつでも実行する手順




# Data Backup and Restore（DBR）

クラスタで **DBR** が有効になっている場合は、「アップグレード（DBR あり）」も参照してください。

# スナップショット

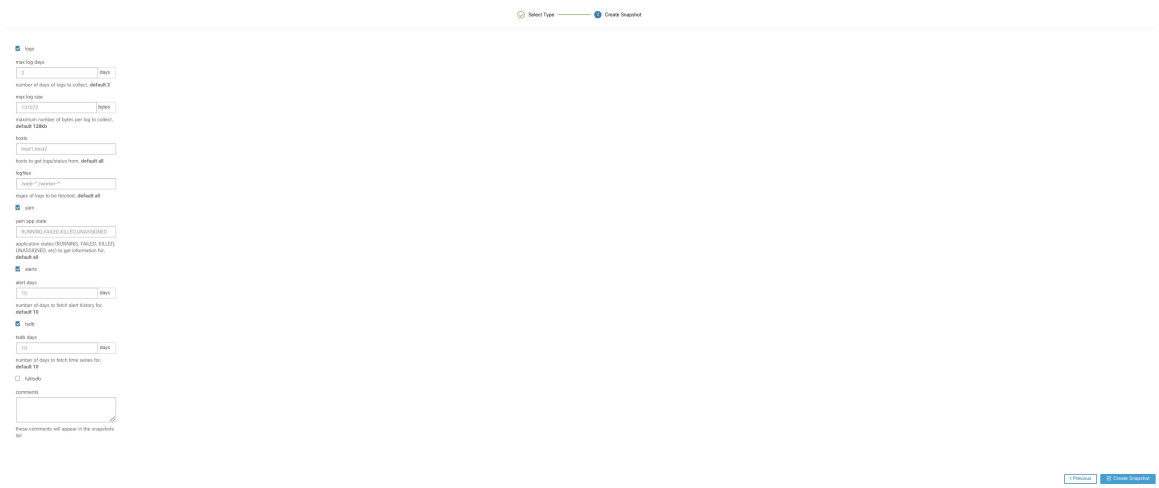
## スナップショット作成ユーザーインターフェイスへのアクセス

**カスタマーサポートロール**を持つユーザーは、ウィンドウの左側にあるナビゲーションバーから **[トラブルシューティング（Troubleshoot）]** > **[スナップショット（Snapshots）]** を選択して、スナップショットツールにアクセスできます。

スナップショットツールを使用して、クラシックスナップショットまたは Cisco Integrated Management Controller（CIMC）テクニカルサポートバンドルを作成できます。スナップショット ファイル リスト ページで [スナップショットの作成（Create Snapshot）] ボタンをクリックすると、クラシックスナップショットまたはCIMC スナップショット（テクニカルサポートバンドル）を選択するページがロードされます。CIMC スナップショットを選択するオプションは、Secure Workload ソフトウェアのみ（ESXi）および Secure Workload SaaS では無効になっています。

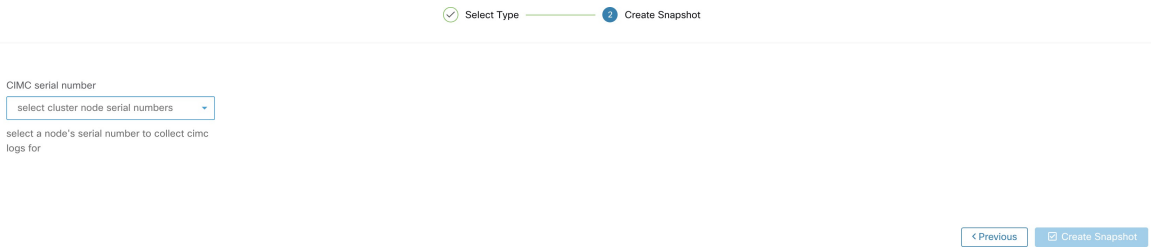
[クラシックスナップショット（Classic Snapshot）] ボタンをクリックすると、スナップショットツールを実行するためのユーザーインターフェイスがロードされます。

**図 *42 :* スナップショットツールの実行**




[CIMC スナップショット（CIMC Snapshot）] ボタンをクリックすると、CIMC テクニカルサポートツールを実行するためのユーザーインターフェイスがロードされます。

図 *43 : CIMC* テクニカルサポートの実行




# スナップショットの作成

[スナップショットの作成（Create Snapshot）] でデフォルトのオプションを選択すると、スナップショットツールは次の情報を収集します。

- ログ
- Hadoop/YARN アプリケーションの状態とログ
- アラート履歴
- さまざまな TSDB 統計情報

デフォルトをオーバーライドして、特定のオプションを指定することができます。

- ログオプション
  - 最大ログ日数（max log days）：収集するログの日数、デフォルトは 2。
  - 最大ログサイズ（max log size ）：収集するログごとの最大バイト数、デフォルトは 128 KB。
  - ホスト（hosts）：ログ/ステータスを取得するホスト、デフォルトは [すべて（all）]。
  - ログファイル（logfiles）：取得するログの正規表現、デフォルトは [すべて（all）]。
- yarn オプション
  - yarn アプリの状態（yarn app state）：情報を取得するアプリケーションの状態（[実行中（RUNNING）]、[失敗（FAILED）]、[強制終了（KILLED）]、[未割り当て（UNASSIGNED）] など）。デフォルトは all。
- アラートオプション
  - アラート日数（alert days）：アラートデータを収集する日数。
- tsdb オプション
  - tsdb 日数（tsdb days）：tsdb データを収集する日数。この値を増やすと、非常に大規模なスナップショットが作成される可能性があります。

- fulltsdb オプション
  - fulltsdb：startTime、endTime fullDumpPath、localDumpFile、nameFilterIncludeRegex を指定し、収集するメトリックを制限するために使用できる JSON オブジェクト。
- コメント（comments）：スナップショットを収集する理由や収集するユーザーを記載するために追加できます。

[スナップショットの作成（Create Snapshot）] を選択すると、スナップショット ファイル リストページの上部にスナップショットの進行状況バーが表示されます。スナップショットが完了したら、スナップショット ファイル リスト ページの [ダウンロード（Download）] ボタンを使用してダウンロードできます。一度に収集できるスナップショットは 1 つだけです。

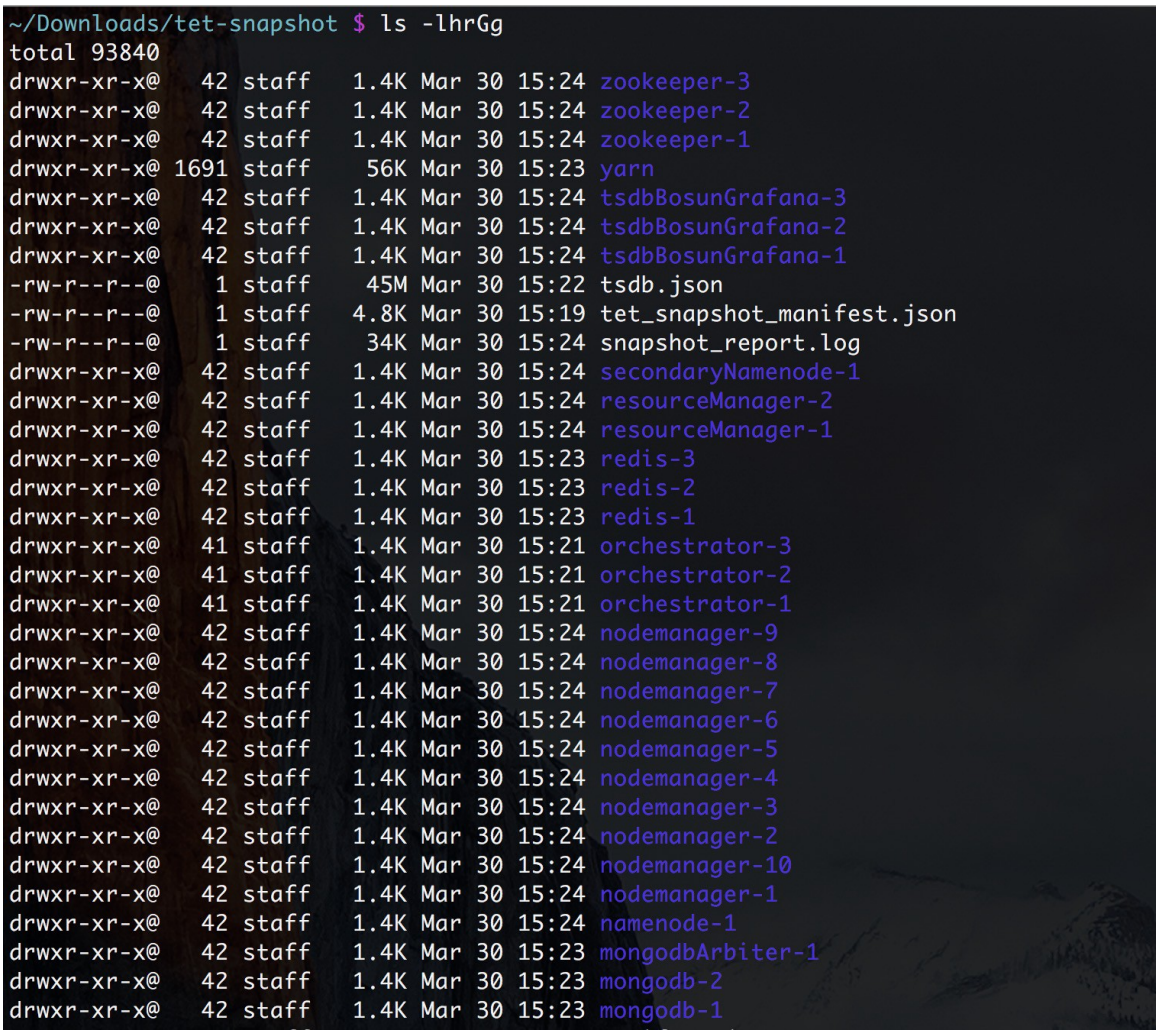
# CIMC テクニカルサポートバンドルの作成

CIMC スナップショット（テクニカルサポートバンドル）ページで、CIMC テクニカルサポートバンドルを作成するノードのシリアル番号を選択し、[スナップショットの作成（Create Snapshot）] ボタンをクリックします。CIMC テクニカルサポートバンドル収集の進捗バーがスナップショット ファイル リスト ページに表示され、コメントセクションには CIMC テクニカルサポートバンドル収集がトリガーされたことが反映されます。CIMC テクニカルサポートバンドルの収集が完了すると、スナップショット ファイル リスト ページからファイルをダウンロードできます。

# スナップショットの使用

スナップショットを解凍すると、各マシンのログを含む ./clustername_snapshot ディレクトリが作成されます。ログは、マシンのいくつかのディレクトリのデータを含むテキストファイルとして保存されます。スナップショットは、JSON 形式でキャプチャされたすべての Hadoop/TSDB データも保存します。

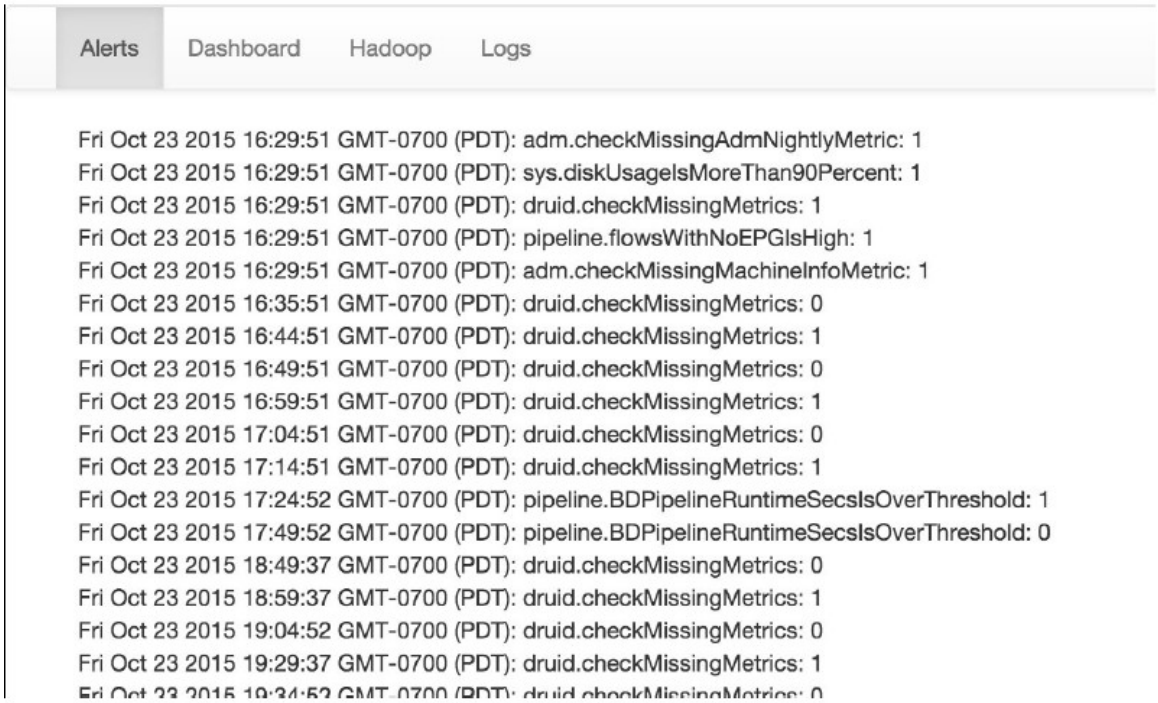
図 *44 :* スナップショットの使用




パッケージ化された index.html をブラウザで開くと、次のタブが表示されます。

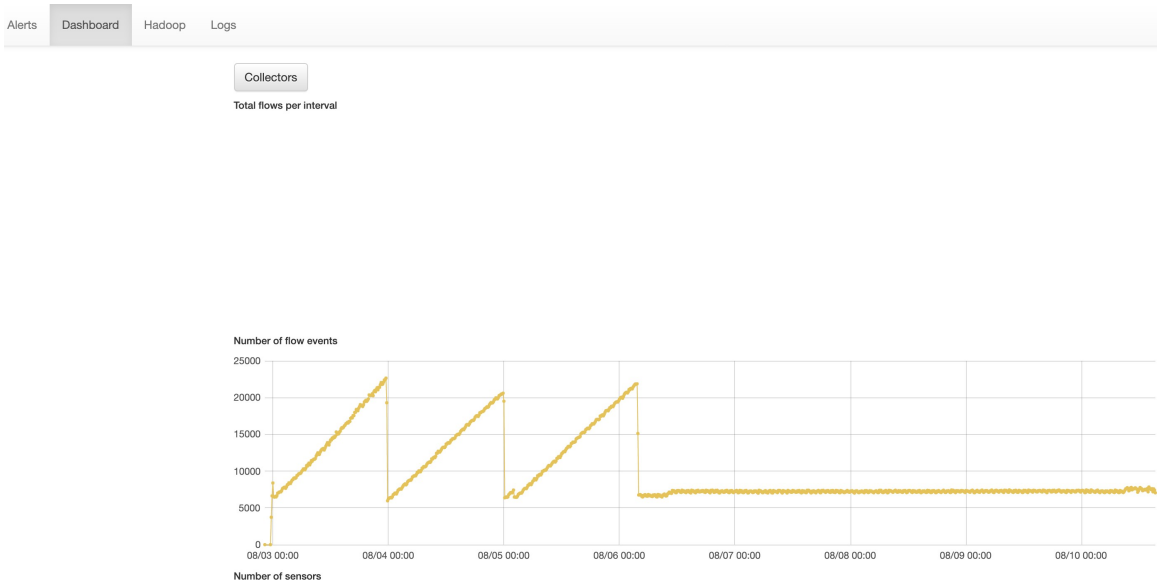
- アラート状態の変化についての簡潔なリスト。

図 *45 :* アラート状態の変化についての簡潔なリスト



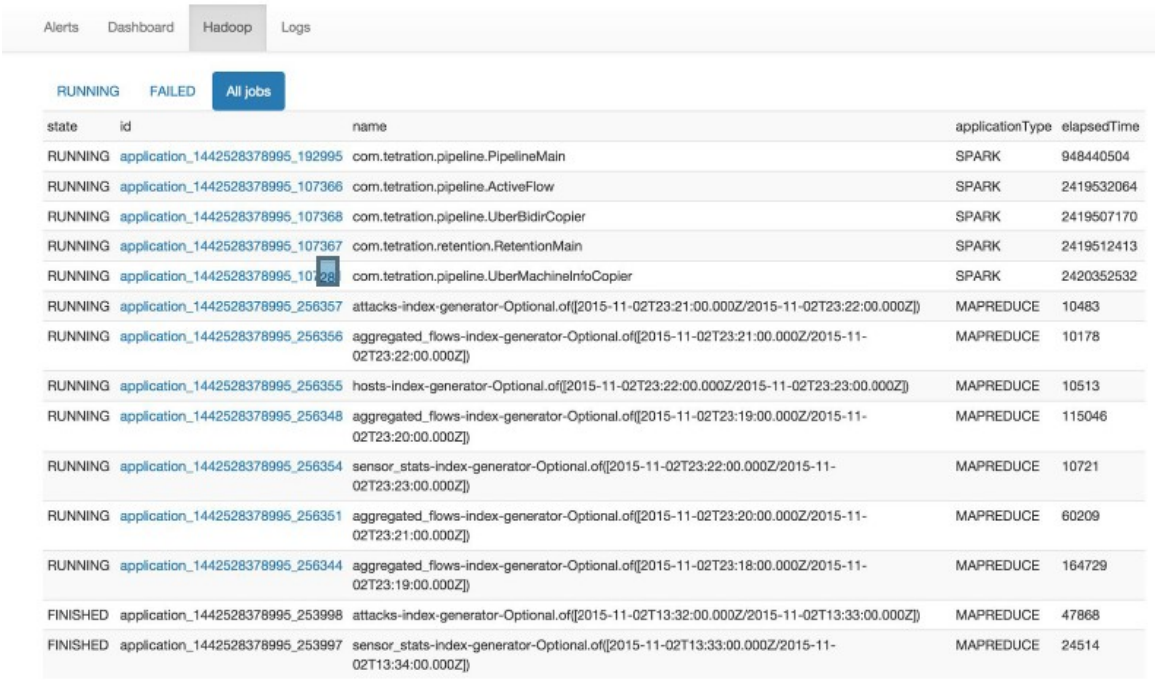

- grafana ダッシュボードの複製。

図 *46 : grafana* ダッシュボードの複製




- ジョブとその状態を含む Hadoop Resource Manager のフロントエンドの複製。ジョブを選択すると、そのジョブのログが表示されます。

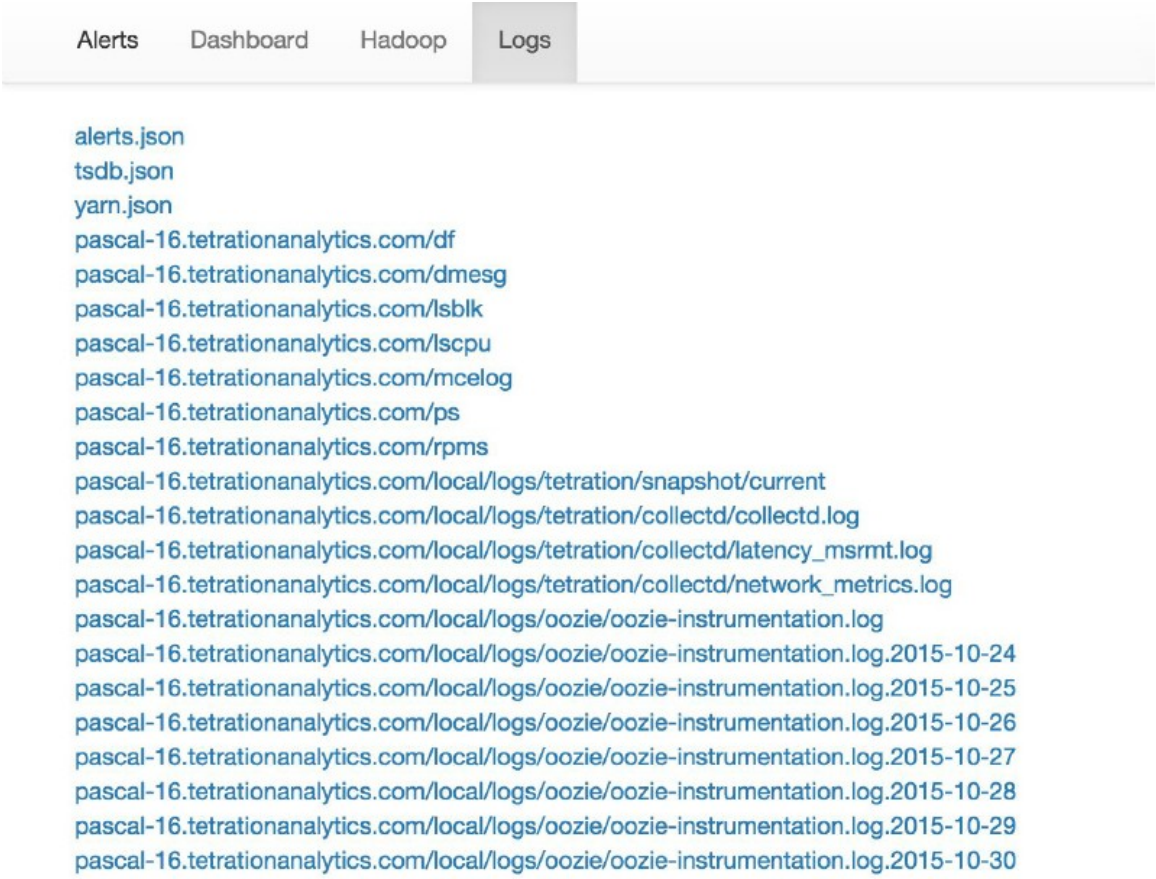
図 *47 : Hadoop Resource Manager* の複製




| state | id | name | applicationType | elapsedTime |
|---|---|---|---|---|
| RUNNING | application_1442528378995_192995 | com.tetration.pipeline.PipelineMain | SPARK | 948440504 |
| RUNNING | application_1442528378995_107366 | com.tetration.pipeline.ActiveFlow | SPARK | 2419532064 |
| RUNNING | application_1442528378995_107368 | com.tetration.pipeline.UberBidirCopier | SPARK | 2419507170 |
| RUNNING | application_1442528378995_107367 | com.tetration.retention.RetentionMain | SPARK | 2419512413 |
| RUNNING | application_1442528378995_10728 | com.tetration.pipeline.UberMachineInfoCopier | SPARK | 2420352532 |
| RUNNING | application_1442528378995_256357 | attacks-index-generator-Optional.of([2015-11-02T23:21:00.000Z/2015-11-02T23:22:00.000Z]) | MAPREDUCE | 10483 |
| RUNNING | application_1442528378995_256356 | aggregated_flows-index-generator-Optional.of([2015-11-02T23:21:00.000Z/2015-11-02T23:22:00.000Z]) | MAPREDUCE | 10178 |
| RUNNING | application_1442528378995_256355 | hosts-index-generator-Optional.of([2015-11-02T23:22:00.000Z/2015-11-02T23:23:00.000Z]) | MAPREDUCE | 10513 |
| RUNNING | application_1442528378995_256348 | aggregated_flows-index-generator-Optional.of([2015-11-02T23:19:00.000Z/2015-11-02T23:20:00.000Z]) | MAPREDUCE | 115046 |
| RUNNING | application_1442528378995_256354 | sensor_stats-index-generator-Optional.of([2015-11-02T23:22:00.000Z/2015-11-02T23:23:00.000Z]) | MAPREDUCE | 10721 |
| RUNNING | application_1442528378995_256351 | aggregated_flows-index-generator-Optional.of([2015-11-02T23:20:00.000Z/2015-11-02T23:21:00.000Z]) | MAPREDUCE | 60209 |
| RUNNING | application_1442528378995_256344 | aggregated_flows-index-generator-Optional.of([2015-11-02T23:18:00.000Z/2015-11-02T23:19:00.000Z]) | MAPREDUCE | 164729 |
| FINISHED | application_1442528378995_253998 | attacks-index-generator-Optional.of([2015-11-02T13:32:00.000Z/2015-11-02T13:33:00.000Z]) | MAPREDUCE | 47868 |
| FINISHED | application_1442528378995_253997 | sensor_stats-index-generator-Optional.of([2015-11-02T13:33:00.000Z/2015-11-02T13:34:00.000Z]) | MAPREDUCE | 24514 |

- 収集されたすべてのログのリスト

図 *48* : 収集されたすべてのログのリスト

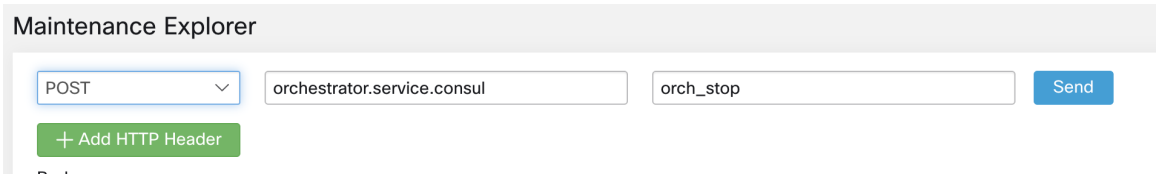



# デバッグとメンテナンスにスナップショットサービスを使用

スナップショットサービスを使用してサービスコマンドを実行できますが、これにはカスタマーサポート権限が必要です。

Explore ツール （**[トラブルシュート（Troubleshoot）] > [メンテナンスエクスプローラ（Maintenance Explorer)]**）を使用すると、クラスタ内の任意の URI に到達できます。

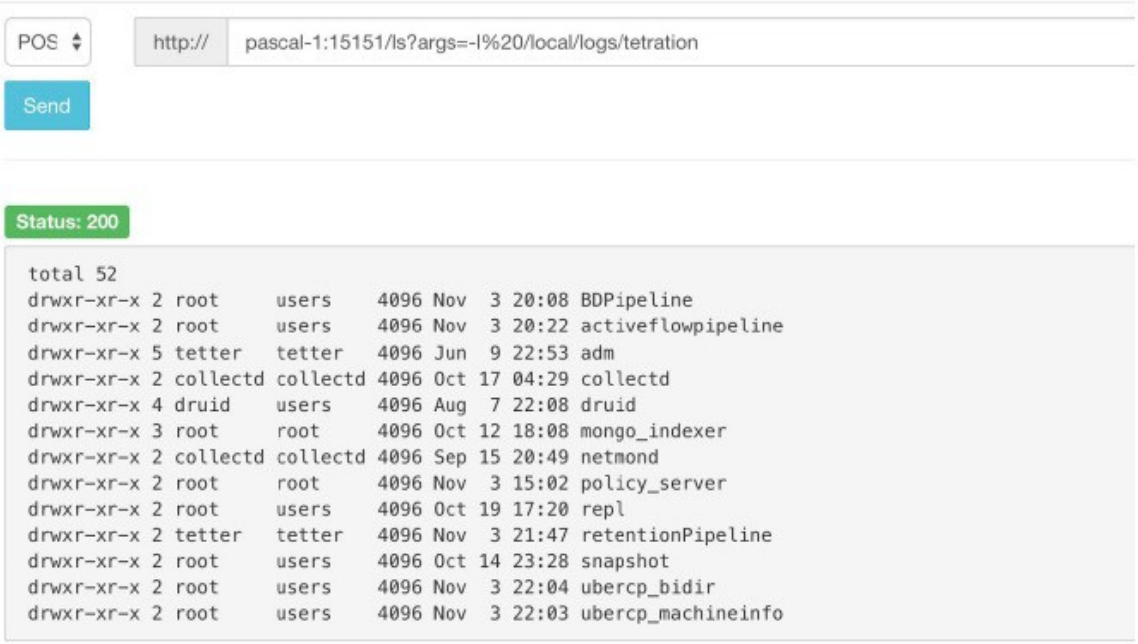
図 *49* : デバッグとメンテナンスにスナップショットサービスを使用する例




Explore ツールは、カスタマーサポートの権限を持つユーザーのみに表示されます。

スナップショットサービスは、すべてのノードのポート 15151 で実行されます。内部ネットワークのみでリッスンし（外部には公開されません）、さまざまなコマンド用の POST エンドポイントがあります。

**図 *50* : デバッグとメンテナンスにスナップショットサービスを使用する例**




到達する必要がある URI は **POST** http://<hostname>:15151/<cmd>?args=<args> です。ここで args はスペースで区切られ、URI はエンコードされます。この URI によってシェルでコマンドが実行されることはありません。これにより、何かが実行されることを回避できます。

**スナップショットのエンドポイントは、次に対して定義されています。**

- **snapshot 0.2.5**

  –ls

  –**svstatus、svrestart - sv status、sv restart を実行** 例：1.1.11.15:15151/svrestart?args=snapshot

  –hadoopls - hadoop fs -ls <args> を実行

  –hadoopdu - hadoop fs -du <args> を実行

  –**ps** 例：1.1.11.31:15151/ps?args=eafux

  –du

  –ambari - ambari_service.py を実行

  –monit

  –MegaCli64（/usr/bin/MegaCli64）

  –service

  –hadoopfsck - hadoop -fsck を実行

- **snapshot 0.2.6**

  −makecurrent - make -C /local/deploy-ansible current を実行

  −netstat

- **snapshot 0.2.7（uid “nobody” として実行）**

  −cat

  −head

  −tail

  −grep

  −ip -6 neighbor

  −ip address

  −ip neighbor

別のエンドポイント POST /runsigned があります。これは、Secure Workload により署名されたシェルスクリプトを実行します。これは、POST されたデータ上で gpg -d を実行します。署名に対して検証できる場合は、暗号化されたテキストをシェルで実行します。これは、Ansible セットアップの一部として各サーバーに公開鍵をインポートすること、および秘密鍵を安全に保つ必要があることを意味します。

# ランブック

カスタマーサポートの権限を持つユーザーは、ウィンドウの左側にあるナビゲーションバーから **[トラブルシューティング（Troubleshoot）]** > **[メンテナンスエクスプローラ（Maintenance Explorer）]** を選択して、ランブックを使用できます。ドロップダウンメニューから **[POST]** を選択します。（そうしないと、コマンドの実行時に Page Not Found エラーが発生します。）

**スナップショット REST エンドポイントを使用してサービスを再起動します。**

- **druid: 1.1.11.17:15151/service?args=supervisord%20restart**

  — druid ホストは、すべて .17 から .24 までの IP です。.17、.18 はコーディネータ、.19 はインデクサ、.20 ～ .24 はブローカです。

- **hadoop パイプラインランチャ**：

  −1.1.11.25:15151/svrestart?args=activeflowpipeline

  −1.1.11.25:15151/svrestart?args=adm

  −1.1.11.25:15151/svrestart?args=batchmover_bidir

  −1.1.11.25:15151/svrestart?args=batchmover_machineinfo

  −1.1.11.25:15151/svrestart?args=BDPipeline

  −1.1.11.25:15151/svrestart?args=mongo_indexer

  −1.1.11.25:15151/svrestart?args=retentionPipeline

- **ポリシー エンジン**

−1.1.11.25:15151/svrestart?args=policy_server

- **wss**

−1.1.11.47:15151/svrestart?args=wss

# Explore / スナップショットのエンドポイントの概要

エンドポイントを実行するには、ウィンドウの左側にあるナビゲーションバーから **[トラブルシューティング（Troubleshoot）] > [メンテナンスエクスプローラ（Maintenance Explorer）]** ページに移動する必要があります。

また、**<end- point>?usage=true** のように任意のホストで **POST** コマンドを実行して、エクスプローラページで各エンドポイントの概要を表示することもできます。

例：**makecurrent?usage=true**

## GET コマンド

| エンドポイント | 説明 |
|---|---|
| **bm_details** | • ベアメタル情報を表示します。 |
| **endpoints** | • ホスト上のすべてのエンドポイントを一覧表示します。 |
| **メンバー** | • consul メンバーの現在のリストとそのステータスを表示します。 |
| **port2cimc** | • ポートの接続先 IP を一覧表示します。<br>• **オーケストレータホスト**でのみ実行する必要があります。 |
| **status** | • ホスト上のスナップショットサービスのステータスを表示します。 |
| **vm_info** | • ロケーションの VM 情報を表示します。<br>• **ベアメタルホストのみ**で実行する必要があります。<br>• エンドポイントを **vm_info?args=<vmname>** として実行します。 |

# POST コマンド

| エンドポイント | 説明 |
|---|---|
| **bm_shutdown_or_reboot** | • 最初にそのホスト上のすべての仮想マシンをシャットダウンしてから、シャットダウンまたは再起動コマンドをベアメタルに発行することにより、ベアメタルホストのグレースフルシャットダウンまたはリブートを実行します。このエンドポイントを使用して、シャットダウンまたはリブートのステータスを取得することもできます。<br>• 任意のノードのシャットダウンまたはリブートステータスを取得するには、コマンド `bm_shutdown_or_reboot? query=serial=FCH2308V0FH` を使用します。<br>• ベアメタルのグレースフルシャットダウンを開始するには、`bm_shutdown_or_reboot? method=POST` を使用して、本文をホストのシリアル番号を表す JSON オブジェクトに設定します。例：`{"serial": "FCH2308V0FH"}`<br>• ベアメタルのグレースフルリブートを開始するには、`bm_shutdown_or_reboot? method=POST` を使用して、本文をホストのシリアル番号を表す JSON オブジェクトに設定し、「true」に設定したリブートキーを含めます。例：`{"serial": "FCH2308V0FH", "reboot": true}` |
| **cat** | • UNIX 「cat」コマンドのラッパーコマンド |
| **cimc_password_random** | • CIMC パスワードをランダム化します。<br>• **オーケストレータホスト**でのみ実行する必要があります。 |
| **cleancmdlogs** | • /lo- cal/logs/tetration/snapshot/cmdlogs/snapshot_cleancmdlogs_log 内のログをクリアします。 |

| エンドポイント | 説明 |
| --- | --- |
| **clear_sel** | • システムイベントログをクリアします。<br>• **ベアメタルホストのみ**で実行する必要があります。 |
| **cluster_fw_upgrade** | • これは**ベータ**機能です。<br>• クラスタ全体でUCSファームウェアアップグレードを実行します。<br>• これが正常に完了したら、各ベアメタルを再起動して、BIOSおよびその他のコンポーネント ファームウェアをアクティブ化する必要があります。<br>• **cluster_fw_upgrade** のように実行します。<br>• このエンドポイントは、ファームウェアのアップグレードを開始して監視し、アップグレードの段階が開始または完了したときにログファイルを更新します。<br>• 完全なアップグレードのステータスを取得するには、**cluster_fw_upgrade_status** エンドポイントを使用してください。 |
| **cluster_fw_upgrade_status** | • これは**ベータ**機能です。<br>• 完全なクラスタUCSファームウェアアップグレードのステータスを取得します。<br>• **cluster_fw_upgrade_status** のように実行します。 |
| **cluster_powerdown** | • クラスタの電源をオフにします。<br>• クラスタがダウンするため、注意して使用してください。<br>• エンドポイントを **cluster_powerdown?args=–start** のように実行します。 |
| **collector_status** | • コレクタのステータスを表示します。<br>• **コレクタホストでのみ**実行する必要があります。 |

| エンドポイント | 説明 |
|---|---|
| **consul_kv_export** | • consul からの k-v ペアを JSON 形式で表示します。<br>• **オーケストレータホスト**でのみ実行する必要があります。 |
| **consul_kv_recurse** | • consul からの k-v ペアを表形式で表示します。<br>• **オーケストレータホスト**でのみ実行する必要があります。 |
| **df** | • UNIX「df」コマンドのラッパーコマンド |
| **dig** | • UNIX「dig」コマンドのラッパーコマンド |
| **dmesg** | • UNIX「dmesg」コマンドのラッパーコマンド |
| **dmidecode** | • UNIX「dmidecode」コマンドのラッパーコマンド |
| **druid_coordinator_v1** | • DRUID のステータスを表示します。 |
| **du** | • UNIX「du」コマンドのラッパーコマンド |
| **dusorted** | • UNIX「dusorted」コマンドのラッパーコマンド |
| **externalize_change_tunnel** | • CIMC UI をトンネリングするために使用されるコレクタ IP を変更します。<br>• **externalize_change_tunnel?method=POST** として実行します。<br>• 本文に **{“collector_ip” : “<IP>”}** を渡します。<br>• **オーケストレータホスト**でのみ実行する必要があります。 |

| エンドポイント | 説明 |
| --- | --- |
| **externalize_mgmt** | • 各サーバーの CIMC UI の外部化の現在のステータスを表示します。<br>• 外部化のアドレスと残り時間を表示します。<br>• **オーケストレータホスト**でのみ実行する必要があります。 |
| **externalize_mgmt_read_only_password** | • スイッチと CIMC UI の両方の読み取り専用パスワード（ta_guest）を変更します。<br>• 変更は、外部化された場合にのみ行われます。<br>• **externalize_mgmt_read_only_password?method=POST** のように実行します。<br>• **{"password" : "<password>"}** を本文に渡します。<br>• **オーケストレータホスト**でのみ実行する必要があります。 |
| **fsck** | • UNIX「fsck」コマンドのラッパーコマンド<br>• **ベアメタルホストのみ**で実行する必要があります。 |
| **get_cimc_techsupport** | • BM の内部 IP アドレスを**入力**します。<br>• CIMCテクニカルサポートを取得します。<br>• 完了すると、UI のスナップショットページからダウンロードできるようになります。<br>• これは、クラスタ上の任意のホストから実行でき、引数としてベアメタルの内部 IP アドレスが必要です。<br>• 例：**get_cimc_techsupport?args=1.1.0.9** |

| エンドポイント | 説明 |
| --- | --- |
| **syslog_endpoints** | • 1 つ以上の UCS サーバーの syslog 構成を制御します。<br>• **パラメータの完全なリストを取得するには、-h を使用してコマンドを実行します。** |
| **grep** | • UNIX「grep」コマンドのラッパーコマンド |
| **hadoopbalancer** | • HDFS データをすべてのノードに均一に分散します。<br>• launcherhost などの **hdfs を持つホスト**で実行する必要があります。 |
| **hadoopdu** | • hdfs のディレクトリ使用率を出力します。<br>• launcherhost などの **hdfs を持つホスト**で実行する必要があります。 |
| **hadoopfsck** | • hadoop fsck を実行し、提供された hdfs ファイルシステムの状態を報告します。<br>• また、破損または欠落しているブロックをクリアする引数として「-delete」を使用します。<br>• 削除する前に、すべての DataNodes が起動していることを確認してください。そうしないと、データが失われる可能性があります。<br>• **ランチャホストでのみ**実行する必要があります。<br>• 状態をレポートするには、**hadoopfsck?args=/raw** のように実行します。<br>• 破損したファイルを削除するには、**hadoopfsck?args=/raw -delete** のように実行します。 |

| エンドポイント | 説明 |
| --- | --- |
| **hadoopls** | • Hadoop ファイルシステムを一覧表示します。<br>• launcherhost などの **hdfs を持つホスト**で実行する必要があります。 |
| **hbasehbck** | • 整合性およびテーブルの完全性の問題をチェックし、破損した HBase を修復します。<br>• **HBase ホストでのみ**実行する必要があります。<br>• 不整合を特定するには、**hbasehbck?args=-details** のように実行します。<br>• 破損した HBase を修復するには、**hbasehbck?args=-repair** のように実行します。<br>• **出力先 : /var/log/active/snapshot/cmdlogs/snpsht_hbasehbck_log.txt**<br>• **修復は、慎重に行ってください。** |
| **hdfs_safe_state_recover** | • HDFS を安全な状態から削除します。<br>• 容量に空きがなくスペースがクリアされているために HDFS が READ_ONLY_STATE の場合は必須です。<br>• **ランチャホストでのみ**実行する必要があります。<br>• **hadoopfs-rm'{{ hdfs_safe_state_marker_location }}/HDFS_READ_ONLY'** のように実行します。 |
| **initctl** | • UNIX「initctl」コマンドのラッパーコマンド |
| **head** | • UNIX「head」コマンドのラッパーコマンド |

| エンドポイント | 説明 |
| --- | --- |
| **internal_haproxy_status** | • 内部 haproxy のステータスと統計を出力します。<br>• **オーケストレータホスト**でのみ実行する必要があります。 |
| **ip** | • UNIX「ip」コマンドのラッパーコマンド |
| **ipmifru** | • Field Replaceable Unit（FRU、現場交換可能ユニット）の情報を出力します。<br>• **ベアメタルホストのみ**で実行する必要があります。 |
| **ipmilan** | • LAN 構成を出力します。<br>• **ベアメタルホストのみ**で実行する必要があります。 |
| **ipmisel** | • システムイベントログ（SEL）エントリを出力します。<br>• **ベアメタルホストのみ**で実行する必要があります。 |
| **ipmisensorlist** | • IPMI センサー情報を出力します。<br>• **ベアメタルホストのみ**で実行する必要があります。 |
| **jstack** | • 指定された Java プロセスまたはコアファイルの Java スレッドの Java スタックトレースを出力します。 |
| **ls** | • UNIX「ls」コマンドのラッパー コマンド |
| **lshw** | • 「lshw」コマンドのラッパーコマンド |
| **lsof** | • UNIX「lsof」コマンドのラッパーコマンド |
| **lvdisplay** | • UNIX「lvdisplay」コマンドのラッパーコマンド |

| エンドポイント | 説明 |
| --- | --- |
| **lvs** | • UNIX「lvs」コマンドのラッパーコマンド |
| **lvscan** | • 「lvscan」コマンドのラッパーコマンド |
| **makecurrent** | • マーカーを現在のタイムスタンプに処理しているパイプラインをリセット/早送りします。<br>• **オーケストレータノードのみ**で実行する必要があります。<br>• エンドポイントを、**makecurrent?args=–start** のように実行します。 |
| **mongo_rs_status** | • Mongo のレプリケーションステータスを表示します。<br>• **mongodb または enforcementpolicystore ホスト**のいずれかで実行する必要があります。 |
| **mongo_stats** | • Mongo の統計情報を表示します。<br>• **mongodb または enforcementpolicystore ホスト**のいずれかで実行する必要があります。 |
| **mongodump** | • データベースからコレクションをダンプします。<br>• **mongodb または enforcementpolicystore ホスト**のいずれかで実行する必要があります。<br>• mongodump?args=<collection>[–db DB] のように実行します。 |
| **monit** | • UNIX「monit」コマンドのラッパーコマンド |
| **namenode_jmx** | • プライマリ namenode jmx メトリックを表示します。 |

| エンドポイント | 説明 |
| --- | --- |
| **ndisc6** | • UNIX「ndisc6」コマンドのラッパーコマンド |
| **netstat** | • UNIX「netstat」コマンドのラッパーコマンド |
| **ntpq** | • UNIX「ntpq」コマンドのラッパーコマンド |
| **orch_reset** | • オーケストレータの状態をアイドルにリセットします。<br>• コミッショニングまたはデコミッショニングの失敗後に実行します。<br>• **orchestrator.service.consul ホストのみ**で実行する必要があります。<br>• **このコマンドを使用するときは、必ずカスタマーサポートに相談してください。** |
| **orch_stop** | • オーケストレータのプライマリを停止し、スイッチオーバーをトリガーします。<br>• **orchestrator.service.consul ホストのみ**で実行する必要があります。<br>• **慎重に使用してください。** |
| **ping** | • UNIX「ping」コマンドのラッパーコマンド |
| **ping6** | • UNIX「ping6」コマンドのラッパーコマンド |
| **ps** | • UNIX「ps」コマンドのラッパーコマンド |
| **pv** | • UNIX「pv」コマンドのラッパーコマンド |
| **pvs** | • UNIX「pvs」コマンドのラッパーコマンド |
| **pvdisplay** | • UNIX「pvdisplay」コマンドのラッパーコマンド |

| エンドポイント | 説明 |
| --- | --- |
| **rdisc6** | • UNIX「rdisc6」コマンドのラッパーコマンド |
| **rebootnode** | • ノードをリブートします。<br>• **ベアメタルホストのみ**で実行する必要があります。 |
| **recover_rpmdb** | • ノード上の破損した RPMDB を回復します。<br>• ベアメタルまたは VM で実行可能です。 |
| **recoverhbase** | • Hbase および TSDB サービスを回復します。<br>• **オーケストレータホスト**でのみ実行する必要があります。<br>• HDFS が正常なときに実行する必要があります。 |
| **recovervm** | • stop/fsck/start を介して VM の回復を試みます。<br>• **オーケストレータホスト**でのみ実行する必要があります。<br>• エンドポイントを **recovervm?args=<vmname>** のように実行します。 |
| **restartservices** | • すべての非UIサービスを停止して開始します。<br>• **orchestrator.service.consul ホストのみ**で実行する必要があります。<br>• **慎重に使用してください。**<br>• エンドポイントを **restartservices?args=–start** のように実行します。 |

| エンドポイント | 説明 |
| --- | --- |
| **runsigned** | • シスコが提供する署名付きスクリプトを実行します。<br>• **スクリプトガイドラインに記載されている手順に従ってください。** |
| **service** | • UNIX「service」コマンドのラッパーコマンド |
| **smartctl** | • smartctl 実行可能ファイルを実行します。<br>• ベアメタルノードのみで実行する必要があります。 |
| **storcli** | • UNIX「storcli」コマンドのラッパーコマンド |
| **sudocat** | • /var/log または /local/logs でのみ機能する「cat」コマンドのラッパー |
| **sudogrep** | • /var/log または /local/logs のみで機能する「grep」コマンドのラッパー |
| **sudohead** | • /var/log または /local/logs のみで機能する「head」コマンドのラッパー |
| **sudols** | • 以下でのみ機能する「ls」コマンドのラッパー<br><br>/var/log または /local/logs |
| **sudotail** | • 以下でのみ機能する「tail」コマンドのラッパー<br><br>/var/log または /local/logs |
| **sudozgrep** | • /var/log または /local/logs のみで機能する「zgrep」コマンドのラッパー |
| **sudozcat** | • /var/log または /local/logs のみで機能する「zcat」コマンドのラッパー |

| エンドポイント | 説明 |
| --- | --- |
| **svrestart** | • 指定したサービスを再起動します。**svrestart?args=<servicename>** のようにコマンドを実行します。 |
| **svstatus** | • 指定したサービスのステータスを出力します。**svstatus?args=<servicename>** のように実行します。 |
| **switchinfo** | • クラスタスイッチに関する情報を取得します。 |
| **switch_namenode** | • プライマリまたはセカンダリから namenode を手動でフェールオーバーします。<br>• **orchestrator.service.consul** ホストのみで実行する必要があります。<br>• namenode ホストのリコミッションまたはデコミッション中に実行します。<br>• エンドポイントを **switch_namenode?args=–start** のように実行します。 |
| **switch_secondarynamenode** | • secondarynamenode をセカンダリからプライマリに手動でフェールオーバーします。<br>• **orchestrator.service.consul** ホストのみで実行する必要があります。<br>• namenode ホストのリコミッションまたはデコミッション中に実行します。<br>• エンドポイントを **switch_secondarynamenode?args=–start** のように実行します。 |

| エンドポイント | 説明 |
| --- | --- |
| **switch_yarn** | • resourcemanager をプライマリからセカンダリへ、またはその逆に手動でフェールオーバーします。<br>• **orchestrator.service.consul ホストのみ**で実行する必要があります。<br>• sourcemanager ホストのリコミッションまたはデコミッション中に実行します。<br>• エンドポイントを **switch_yarn?args=–start** のように実行します。 |
| **tail** | • UNIX「tail」コマンドのラッパーコマンド |
| **toggle_chassis_locator** | • ノードのシリアル番号で指定された物理ベアメタル上のシャーシロケータを切り替えます。<br>• 任意のノードから **toggle_chassis_locator?method=POST** のように実行します。<br>• 本文を、ホストのシリアル番号を記述する JSON オブジェクトに設定します（同時にサポートされるシリアル番号は 1 つだけです）。例：**{“serials”: [“FCH2308V0FH”]}** |
| **tnp_agent_logs** | • 外部オーケストレータとして登録されたロードバランサエージェントによって提供されるすべてのログ ファイルを使用してスナップショットを作成します。<br>• launcherhost ホストで実行する必要があります。 |

| エンドポイント | 説明 |
| --- | --- |
| **tnp_datastream** | • 外部オーケストレータとして登録されたロードバランサポリシー適用エージェントによって消費されるポリシーストリームデータを使用してスナップショットを作成します。<br>• オーケストレータホストで実行する必要があります。<br>• ポリシー ステータス ストリーム データをダウンロードするには、エンドポイントを **tnp_datastream?args=–ds_type datasink** のように実行します。 |
| **ui_haproxy_status** | • 外部 haproxy の haproxy 統計情報とステータスを出力します。 |
| **uptime** | • UNIX「uptime」コマンドのラッパーコマンド |
| **userapps_kill** | • 実行中のすべてのユーザーアプリケーションを強制終了します。<br>• **launcherhost ホストのみ**で実行する必要があります。 |
| **vgdisplay** | • UNIX「vgdisplay」コマンドのラッパーコマンド |
| **vgs** | • UNIX「vgs」コマンドのラッパーコマンド |
| **vmfs** | • VM 上のファイルシステムを一覧表示します。<br>• **ベアメタルホストのみ**で実行する必要があります。<br>• エンドポイントを **vmfs?args=<vmname>** のように実行します。 |

| エンドポイント | 説明 |
| --- | --- |
| **vminfo** | • VM 情報を出力します。<br>• **ベアメタルホストのみ**で実行する必要があります。<br>• エンドポイントを **vminfo?args=<vmname>** のように実行します。 |
| **vmlist** | • ベアメタル上のすべての VM を一覧表示します。<br>• **ベアメタルホストのみ**で実行する必要があります。<br>• エンドポイントを **vmlist?args=<vmname>** のように実行します。 |
| **vmreboot** | • VM を再起動します。<br>• **ベアメタルホストのみ**で実行する必要があります。<br>• エンドポイントを **vmreboot?args=<vmname>** のように実行します。 |
| **vmshutdown** | • VM のグレースフルシャットダウンを行います。<br>• **ベアメタルホストのみ**で実行する必要があります。<br>• エンドポイントを **vmshutdown?args=<vmname>** のように実行します。 |
| **vmstart** | • VM を起動します。<br>• **ベアメタルホストのみ**で実行する必要があります。<br>• エンドポイントを **vmstart?args=<vmname>** のように実行します。 |

| エンドポイント | 説明 |
|---|---|
| **vmstop** | • VM を強制的にシャットダウンします。<br>• **ベアメタルホストのみ**で実行する必要があります。<br>• エンドポイントを **vmstop?args=<vmname>** のように実行します。 |
| **yarnkill** | • 実行中の Yarn アプリケーションを強制終了します。<br>• **launcherhost ホストのみ**で実行する必要があります。<br>• エンドポイントを **yarnkill?args=<application id>** のように実行します。<br>• すべてのアプリケーションを強制終了するには、**yarnkill?args=ALL** のように実行します。 |
| **yarnlogs** | • Yarn アプリケーションログの最後の 500 MB をダンプします。<br>• **launcherhost ホストのみ**で実行する必要があります。<br>• エンドポイントを **yarnlogs?args=<application id> <job user>** のように実行します。 |
| **zcat** | • UNIX「zcat」コマンドのラッパーコマンド |
| **zgrep** | • UNIX「zgrep」コマンドのラッパーコマンド |

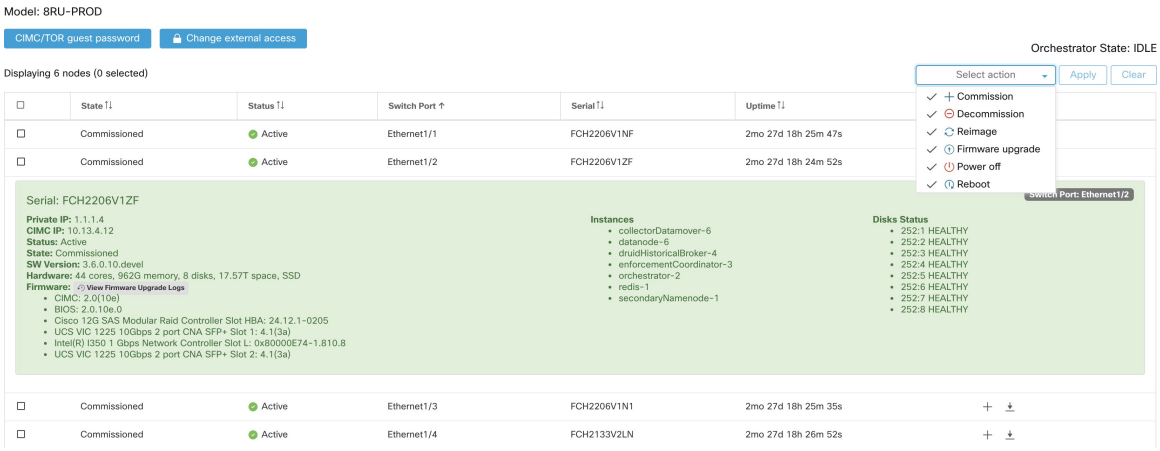
# サーバーのメンテナンス

サーバーのメンテナンスには、故障したサーバーコンポーネント（ハードディスク、メモリなど）の交換、またはサーバー自体の交換が含まれます。

（注） クラスタ上にメンテナンスが必要なサーバーが複数ある場合は、一度に1つずつサーバーのメンテナンスを実行します。複数のサーバーを同時にデコミッションすると、データが失われる可能性があります。

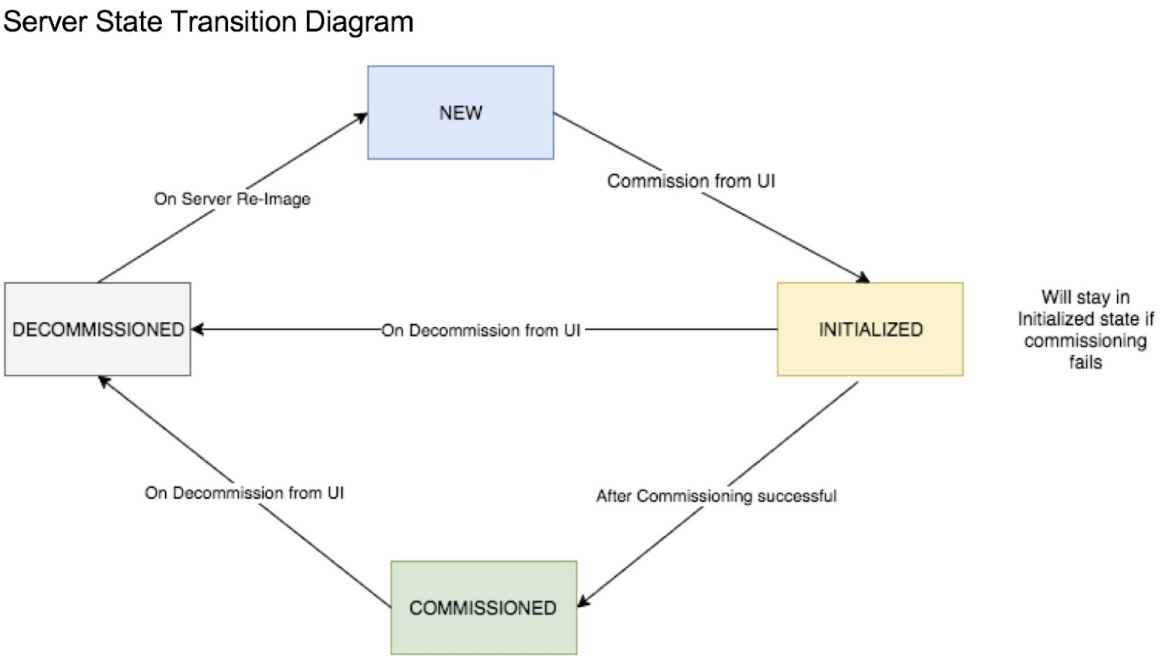
[クラスタステータス（Cluster Status）]ページ（左側のナビゲーションバーの[トラブルシュート（Troubleshoot）]メニューからアクセス）を使用して、サーバーのメンテナンスに関連するすべての手順を実行します。このページにはすべてのユーザーがアクセスできますが、アクションを実行できるのは**カスタマーサポート**ユーザーのみです。このページには、Cisco Secure Workload ラック内のすべての物理サーバーのステータスが表示されます。

**図 *51* : サーバーのメンテナンス**



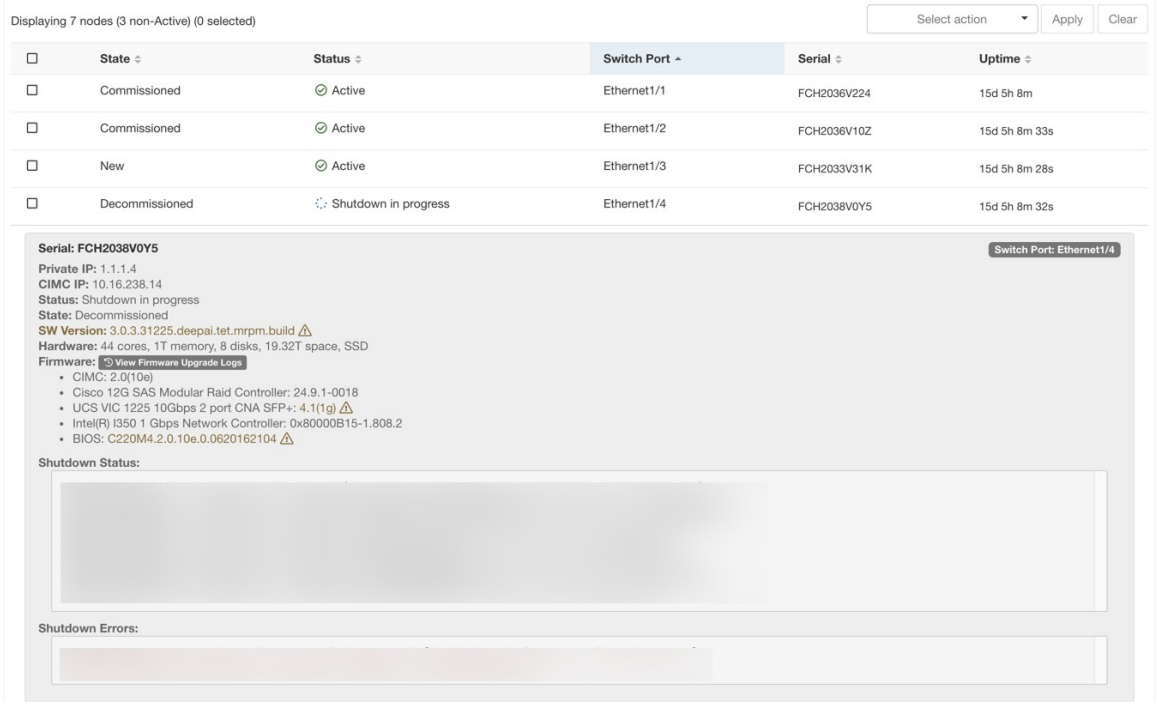

## サーバーまたはコンポーネントの交換に関連する手順

図 *52* : サーバーのメンテナンス手順




1. **メンテナンスが必要なサーバーの判断**：[クラスタステータス（Cluster Status）]ページで、サーバーの [シリアル（Serial）] 番号またはサーバーが接続されている [スイッチポート（Switchport）] を使用して判断します。交換するサーバーの CIMC IP を書き留めます。CIMC IP は、[クラスタステータス（Cluster Status ）] ページのサーバーボックスに表示されます。
2. **特別な VM のアクションの確認**：サーバーボックスから、サーバーに存在する VM またはインスタンスを見つけ、それらの VM に対して特別なアクションを実行する必要があるか確認します。次のセクションに、サーバーメンテナンス中の VM のアクションが一覧表示されています。
3. **サーバーのデコミッション**：デコミッション前のアクションが実行されたら、[クラスタステータス（Cluster Status）]ページを使用してサーバーをデコミッションします。サーバーに障害が発生し、ページに [非アクティブ（Inactive）] と表示された場合でも、サーバーのメンテナンス手順をすべて実行する必要があります。サーバーの電源がオフの場合でも、デコミッション手順を実行できます。

図 *53* : サーバーのメンテナンス手順

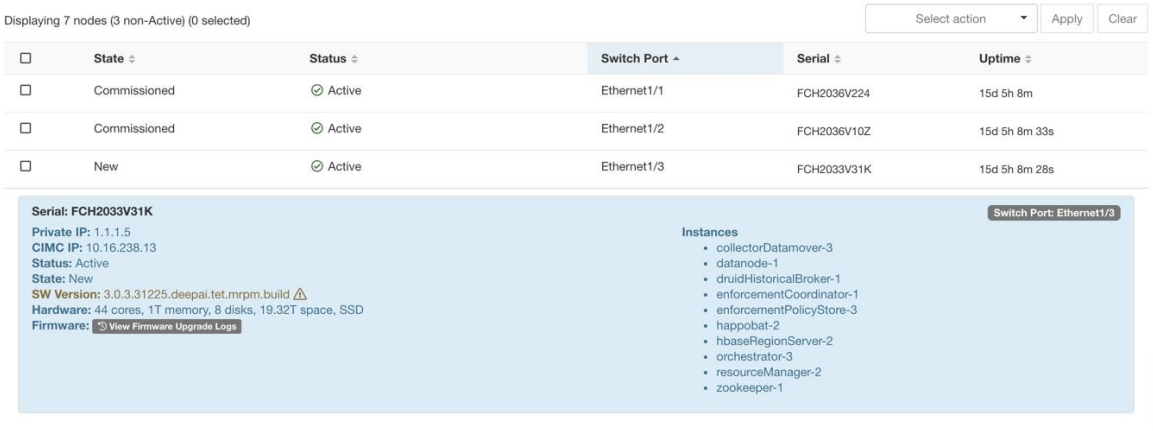



4. **サーバーのメンテナンスの実行**：[クラスタステータス（Cluster Status）] ページでノードが [デコミッション済み（Decommissioned）] とマークされたら、VM に対してデコミッション後の特別なアクションを実行します。これで、コンポーネントまたはサーバーを交換できます。サーバー全体を交換する場合は、新しいサーバーの CIMC IP を、交換したサーバーと同じ CIMC IP に変更します。各サーバーの CIMC IP は、[クラスタステータス（Cluster Status）] ページで確認できます。

5. **コンポーネント交換後の再イメージ化**：[クラスタステータス（Cluster Status）] ページを使用して、コンポーネント交換後にサーバーを再イメージ化します。再イメージ化には約 30 分かかり、サーバーへの CIMC アクセスが必要です。再イメージ化が完了したサーバーは [新規（NEW）] とマークされます。

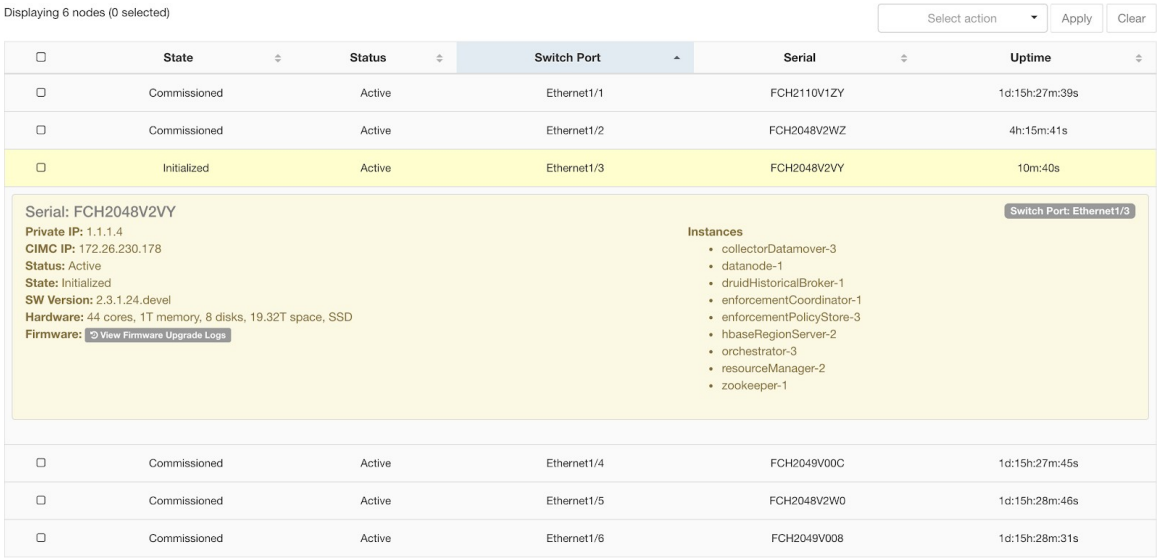
6. **サーバー全体の交換**：サーバー全体を交換した場合、そのサーバーは [クラスタステータス（Cluster Status）] ページに [新規（NEW）] 状態で表示されます。サーバーのソフトウェアバージョンは、同じページで確認できます。ソフトウェアバージョンがクラスタのソフトウェアバージョンと異なる場合は、サーバーを再イメージ化します。

図 *54* : サーバーのメンテナンス手順




7. **サーバーのコミッション**：サーバーが [新規（NEW）] とマークされたら、[クラスタステータス（Cluster Status）] ページからノードのコミッショニングを開始できます。この手順により、サーバー上に VM がプロビジョニングされます。サーバーのコミッショニングには約 45 分かかります。コミッショニングが完了すると、サーバーは [コミッション済み（Commissioned）] とマークされます。

図 *55* : サーバーのメンテナンス手順



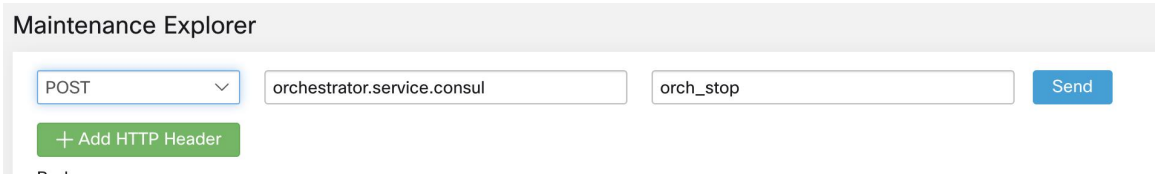

### サーバーメンテナンス中の VM のアクション

一部の VM では、サーバーのメンテナンス手順中に特別なアクションを実行する必要があります。それらのアクションは、デコミッション前、デコミッション後、またはコミッション後に実行できます。

1. **オーケストレータのプライマリ**：これはデコミッション前のアクションです。メンテナンス中のサーバーにプライマリオーケストレータがある場合は、デコミッションする前に探

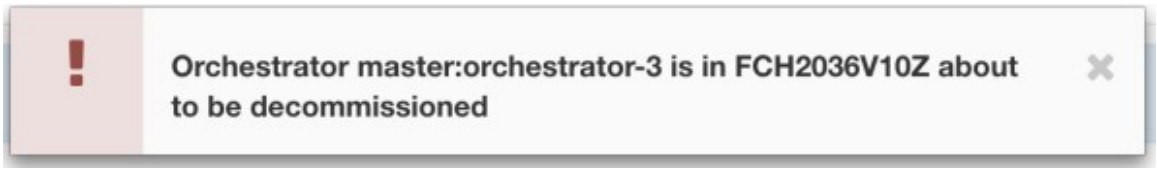
索ページから orchestrator.service.consul に orch_stop コマンドを POST します。これで、プライマリオーケストレータが切り替わります。

**図 *56*：サーバーのメンテナンス手順**




プライマリオーケストレータでサーバーをデコミッションしようとすると、次のエラーが表示されます。

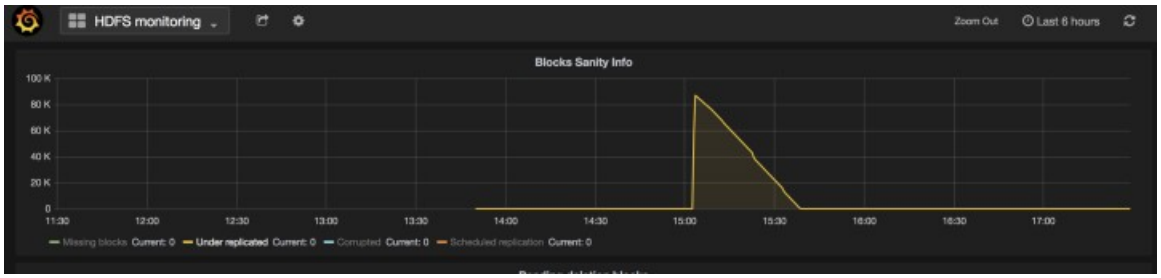
**図 *57*：サーバーのメンテナンス手順**




オーケストレータのプライマリを特定するには、任意のホストで explore コマンド「primaryorchestrator」を実行します。

2. **NameNode**：メンテナンス中のサーバーに NameNode VM がある場合は、デコミッション後に探索ページから orchestrator.service.consul に switch_namenode を POST し、コミッション後に orchestrator.service.consul に switch_namenode を POST します。これらは、デコミッション後とコミッション後のアクションです。
3. **セカンダリ NameNode**：メンテナンス中のサーバーにセカンダリ NameNode VM がある場合、デコミッション後に探索ページから orchestrator.service.consul に switch_secondarynamenode を POST し、コミッション後に orchestrator.service.consul に switch_secondarynamenode を POST します。これらは、デコミッション後とコミッション後のアクションです。
4. **Resource Manager プライマリ**：メンテナンス中のサーバーに Resource Manager プライマリがある場合、探索ページから orchestrator.service.consul に switch_yarn を POST します。これらは、デコミッション後とコミッション後のアクションです。
5. **DataNode**：クラスタは、一度に 1 つの DataNode 障害のみを許容します。DataNode VM を持つ複数のサーバーにメンテナンスが必要な場合は、一度に 1 つずつサーバーのメンテナンスを実行します。各サーバーのメンテナンス後、[モニタリング（Monitoring）] | [hawkeye] | [hdfs-monitoring] | [健全性情報のブロック（Block Sanity Info）] の下に表示されるチャートの [欠落ブロック数（Missing blocks）] および [レプリケーション中（Under replicated）] の数が 0 になるのを待ちます。

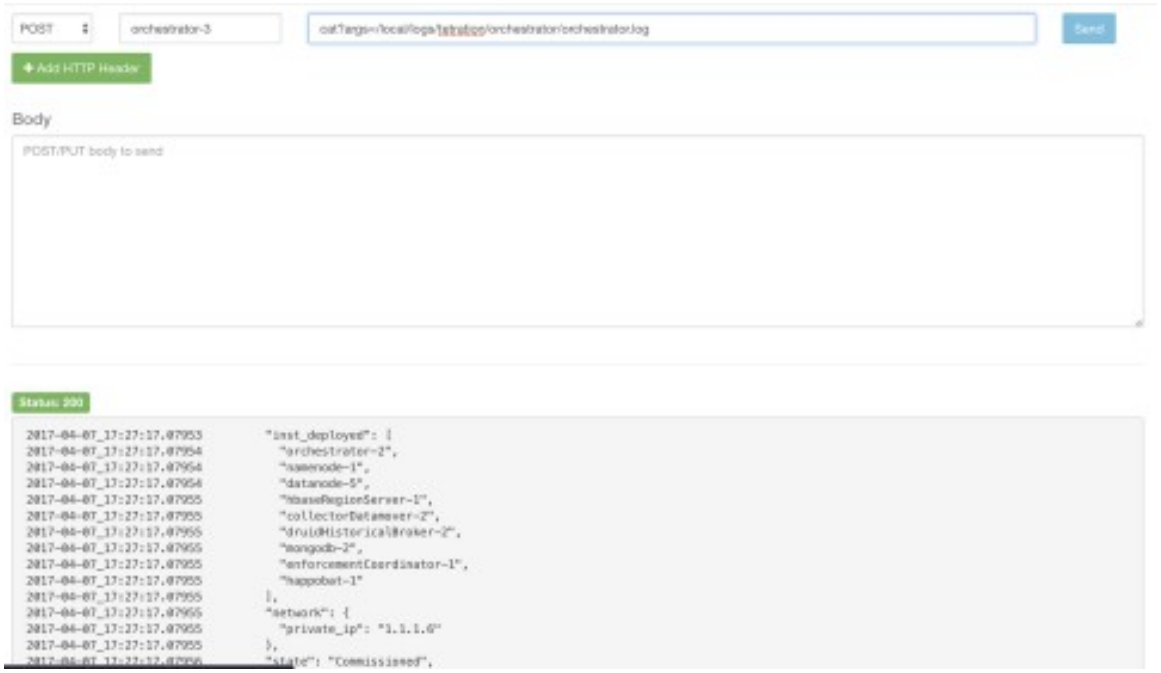
図 *58* : サーバーのメンテナンス手順




## サーバーメンテナンスのトラブルシューティング

1. **ログ**：サーバーのメンテナンスログはすべて、オーケストレータログの一部で、orchestrator.service.consul の /local/logs/tetration/orchestrator/orchestrator.log にあります。

   図 *59* : サーバーのメンテナンスログ




2. **デコミッション**：
   1. この手順により、サーバー上の VM またはインスタンスが削除されます。
   2. 次に、バックエンド consul テーブル内にある削除されたインスタンスのエントリが削除されます。
   3. この手順は約 5 分かかります。
   4. 完了すると、サーバーは[デコミッション済み（Decommissioned）] とマークされます。

（注） デコミッションされても、サーバーの電源がオフになるわけではありません。デコミッションでは、サーバー上の Secure Workload コンテンツのみ削除されます。

5. 電源がオフになっているサーバーは[非アクティブ（Inactive）]とマークされます。このサーバーのデコミッションは、[クラスタステータス（Cluster Status）]ページから引き続き実行できます。ただし、サーバーの電源がオフになっているため、VM の削除手順は実行されないため、このサーバーがデコミッション状態でクラスタに再び参加しないようにしてください。サーバーは再イメージ化してクラスタに追加し直す必要があります。

3. **再イメージ化**：

1. この手順では、サーバーに Secure Workload ベース OS またはハイパーバイザ OS をインストールします。
2. また、ハードドライブをフォーマットし、サーバーにいくつかの Secure Workload ライブラリをインストールします。
3. 再イメージ化では、**mjolnir** というスクリプトを実行して、サーバーのイメージングが開始されます。mjolnir の実行には約 5 分かかり、その後、実際のイメージングが開始されます。イメージングには約30分かかります。イメージング中のログは、再イメージ化されているサーバーのコンソールでのみ確認できます。ユーザーは、ta_dev キーを使用して、再イメージ化に関する追加情報を確認できます。PXE ブート時の /var/log/nginx ログ、DHCP IP および PXE ブート構成を確認するための /var/log/messages などがあります。
4. 再イメージ化には、オーケストレータからの CIMC 接続が必要です。CIMC の接続を確認する最も簡単な方法は、探索ページを使用するか、orchestrator.service.consul から ping?args=<cimc ip> を POST する方法です。サーバーを交換した場合は、CIMC IP を変更し、CIMC パスワードをデフォルトのパスワードに設定することを**忘れないでください**。
5. また、スイッチが正しいルートで設定されるように、クラスタの展開時に CIMC ネットワークがサイト情報に設定されている必要があります。クラスタ CIMC 接続が正しく設定されていない場合、オーケストレータログに次の結果が表示されます。

4. **コミッション**：

1. コミッショニングでは、サーバー上の VM がスケジュールされ、VM でプレイブックを実行して Secure Workload ソフトウェアがインストールされます。
2. コミッショニングが完了するまでに約 45 分かかります。
3. ワークフローは、展開またはアップグレードのワークフローと同様です。
4. ログには、コミッショニング中の障害が示されます。

5. [クラスタステータス（Cluster Status）] ページのサーバーは、コミッショニング中は [初期化済み（Initialized）] としてマークされ、手順完了後にのみ [コミッション済み（Commissioned）] としてマークされます。

# ベアメタル除外

電源シャットダウン後のクラスタの再起動時にハードウェア障害が検出された場合、現在のところ、サービスを安定させるための再起動ワークフローの実行も、コミッションワークフローの実行もできない（サービスが停止するとコミッションが失敗するため）状態でクラスタがスタックします。この機能は、このようなシナリオで役立つことが期待されており、ユーザーは障害のあるハードウェアで再起動（アップグレード）でき、その後、失敗したベアメタルの通常の RMA プロセスを実行できます。

ユーザーは、POST を使用して、除外するベアメタルのシリアルでエンドポイントを探索する必要があります。

1. アクション：POST
2. ホスト：orchestrator.service.consul
3. エンドポイント：exclude_bms?method=POST
4. 本文：{“baremetal”：[“BMSERIAL”]}

オーケストレータは、除外が実行可能か判断するためにいくつかのチェックを実行します。この場合、オーケストレータはいくつかの consul キーをセットアップし、次の再起動またはアップグレードワークフローで除外されるベアメタルと VM を示す成功メッセージを返します。ベアメタルに特定の VM が含まれている場合、それらの VM は除外できません（以下の「制限事項」セクションを参照）。探索エンドポイントは、除外できない理由を示すメッセージで応答します。探索エンドポイントでの POST が成功すると、ユーザーはメイン UI から再起動またはアップグレードを開始し、通常どおり再起動を続行できます。アップグレードの最後に、除外 BM リストを削除します。BM を除外してアップグレードまたは再起動を再度実行する必要がある場合、ユーザーは bmexclude 探索エンドポイントに再度 POST する必要があります。

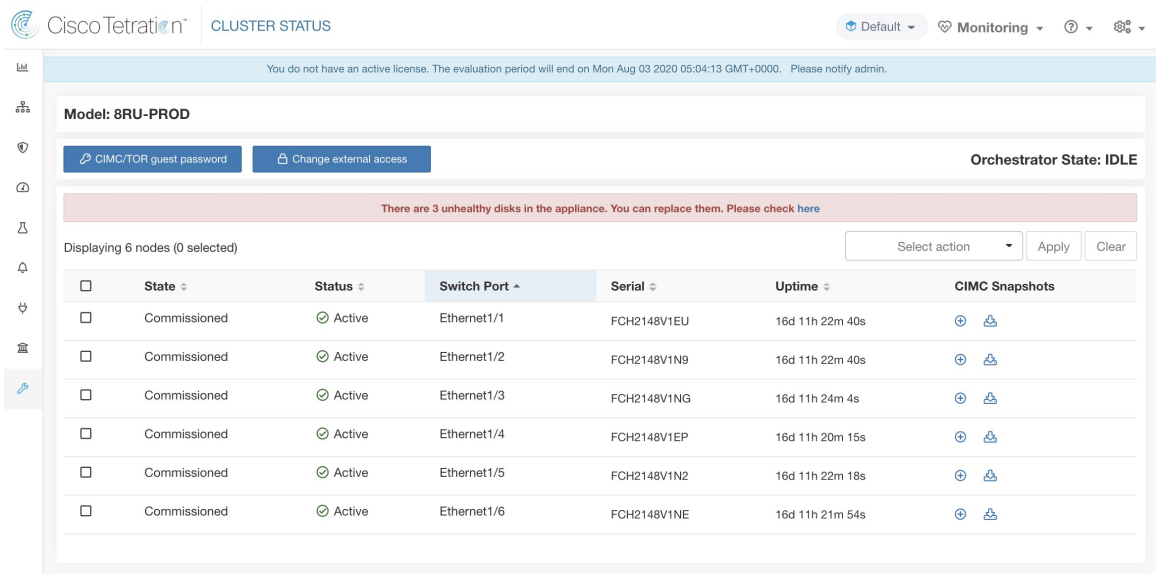
**制限事項**：現在、次の VM は除外できません。1. namenode 2. secondaryNamenode 3. mon- godb 4. mongodbArbiter

# ディスク メンテナンス

ディスクメンテナンスには、サーバーから障害のあるハードディスクを交換することが含まれます。オーケストレータは、クラスタ内のすべてのサーバーで bmmgr によって報告されるディスクの状態を監視します。障害のあるディスクが検出された場合、[クラスタステータス（Cluster Status）] ページ（左側のナビゲーションバーの [トラブルシューティング（Troubleshoot）] メニューからアクセスできます）のバナーにそれが示されます。このバナーには、異常（UNHEALTHY）状態のディスクの数が表示されます。そのバナーでこちらをクリックすると、ディスク交換ウィザードが表示され、ディスクメンテナンスのすべての手順を実行するこ

とができます。[クラスタステータス（Cluster Status）] ページと同様に、ディスク交換ページにはすべてのユーザーがアクセスできますが、アクションを実行できるのはカスタマーサポート ユーザーのみです。

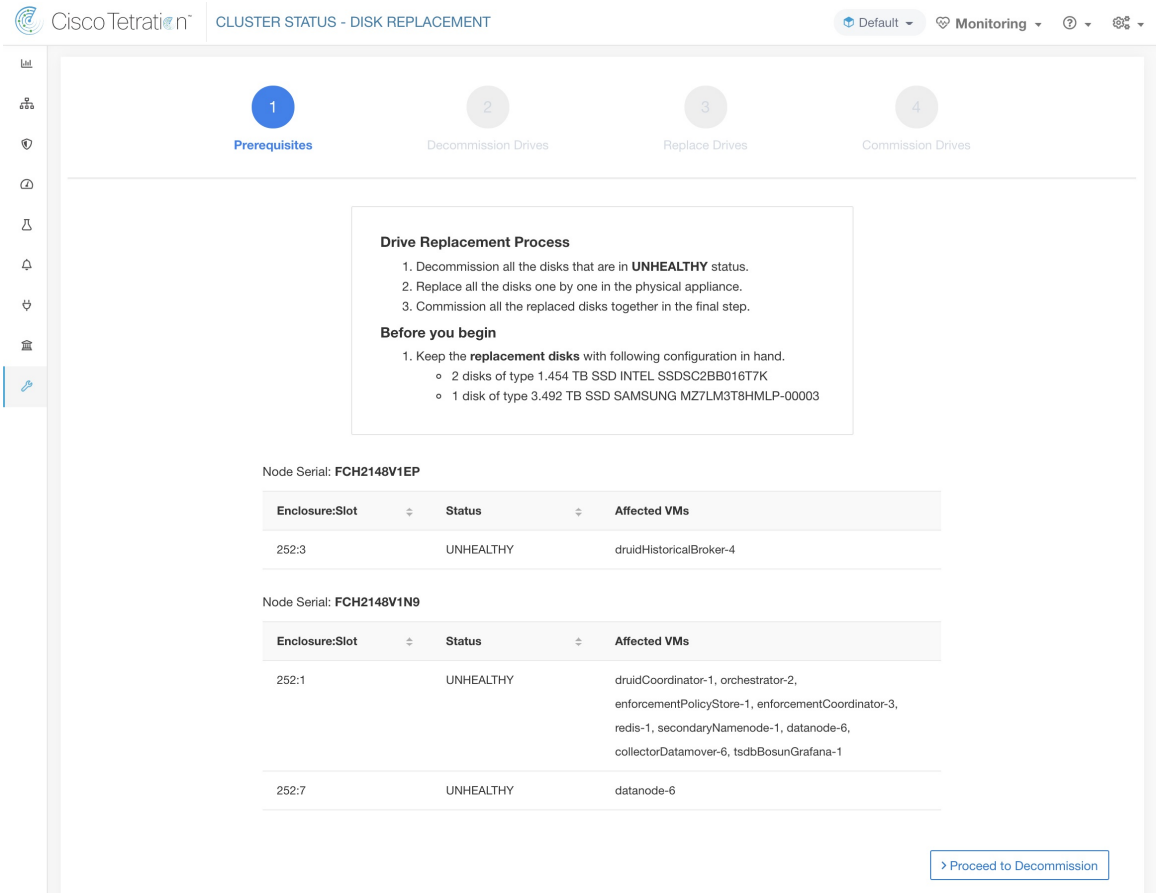
**図 *60* : 障害のあるディスクのバナー**




## ディスク交換ウィザード

ディスク交換ウィザードのランディングページには、障害が発生したディスクの詳細が表示されます。これらの詳細には、交換が必要なすべてのディスクのサイズ、タイプ、製造元、およびモデルが含まれます。また、スロット ID も表示され、これらの各ディスクを使用するすべての VM が一覧表示されます。交換プロセスを開始する前に、交換用ディスクを用意しておく必要があります。

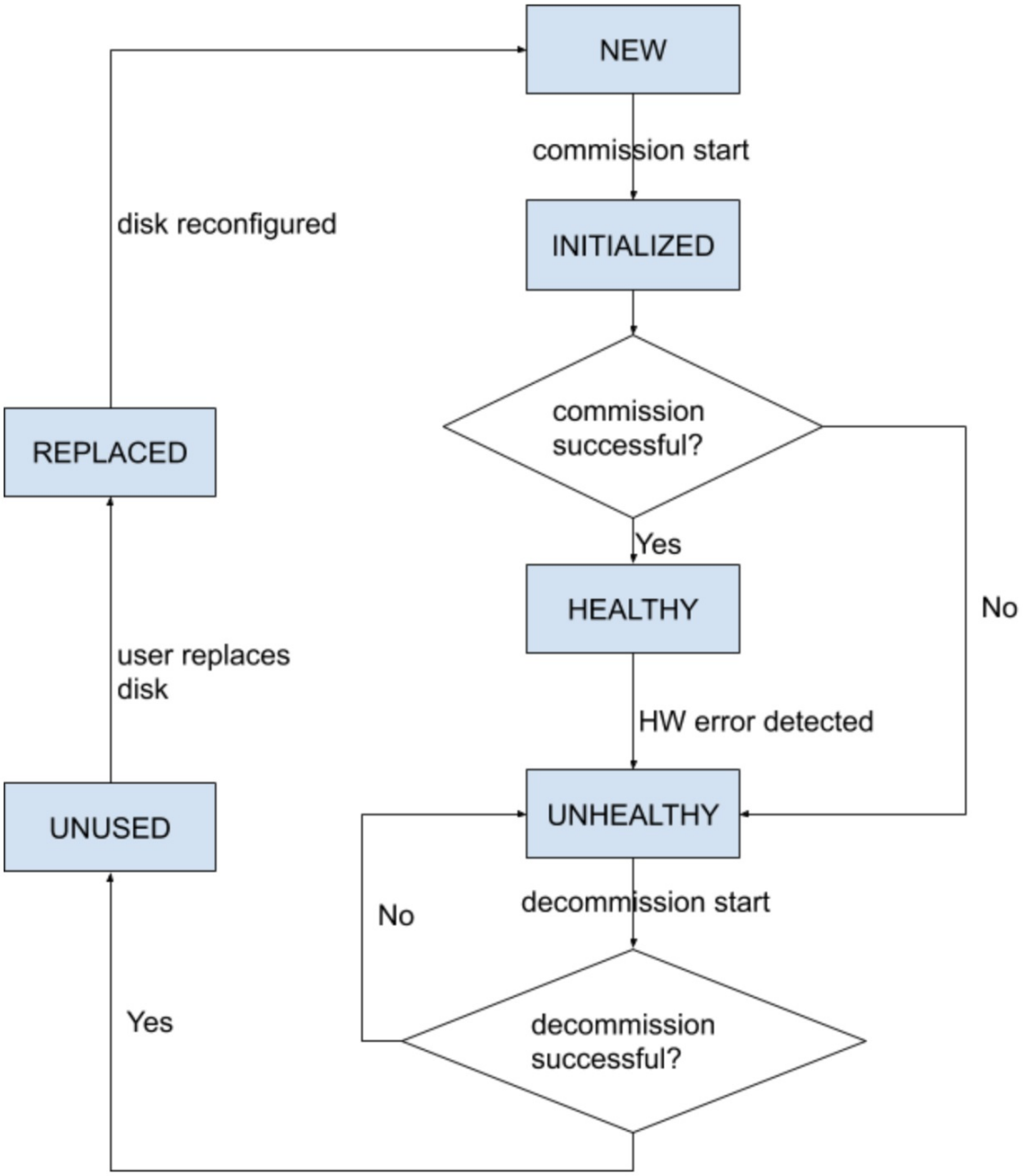
**図 *61* : ディスク交換ウィザード**




## ディスクのステータス遷移

クラスタでは、ハードディスクには次の 6 つの状態があります。正常（HEALTHY）、異常（UNHEALTHY）、未使用（UNUSED）、交換済み（REPLACED）、新規（NEW）、初期化済み（INITIALIZED）。展開/アップグレード後のクラスタ内のすべてのディスクのステータスは正常（HEALTHY）です。さまざまなエラーが検出され、1 つ以上のディスクのステータスが異常（UNHEALTHY）になることがあります。

図 *62 :* ディスクのステータス遷移




ディスク交換プロセスの最初のステップは、デコミッションです。この手順では、これらのディスクを使用するすべての仮想マシンをクラスタから削除します。デコミッションされたディスクのステータスは未使用（UNUSED）になります。デコミッション後、交換用ディスクを適切なスロットに挿入する必要があります。ディスクが交換されたことをユーザーが確認します。これは、新しくインストールされたディスクを再設定するためのバックエンド信号になります。するとステータスが交換済み（REPLACED）に変わり、次のハードウェアスキャン後

に、これらの交換されたディスクのステータスが新規（NEW）に変わります。この移行には 2 ～ 3 分かかることがあります。

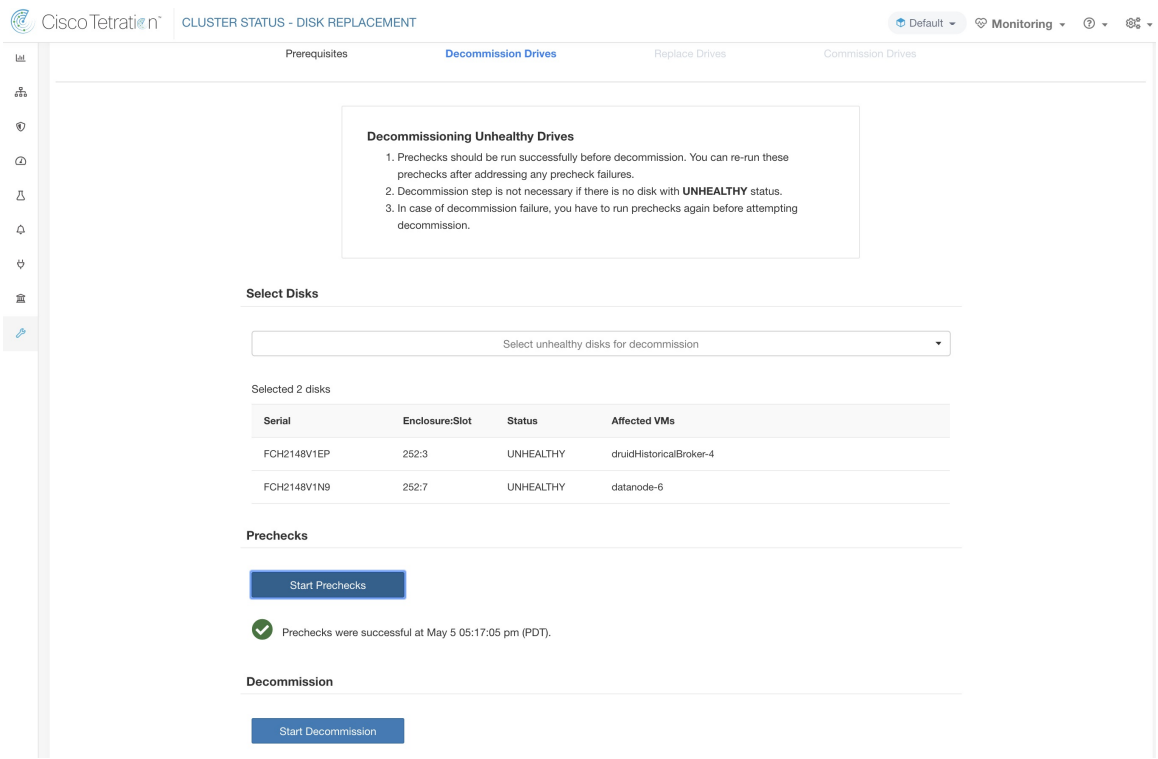
すべてのディスクを交換して再設定したら、コミッショニングに進み、デコミッションプロセスの一部として削除されたすべての VM を展開します。コミッションが開始されると、ディスクのステータスが初期化済み（INITIALIZED）に変わります。コミッションが成功すると、すべてのディスクのステータスが正常（HEALTHY）になります。このステップで失敗すると、ステータスは再び異常（UNHEALTHY）になり、デコミッションからの回復を再度開始することになります。

### 要件の事前チェック

デコミッションまたはコミッションの手順を実行する前に、要件の事前チェックを実行する必要があります。バックエンドでさまざまなチェックが実行されますが、ユーザーがデコミッションまたはコミッションのステップに進む前に、これらのチェックすべてに合格する必要があります。失敗したチェックは、失敗の詳細と推奨される修正処置とともにディスク交換ウィザードで報告されます。必要な手順を続行する前にこれらの修正処置を実行する必要があります。

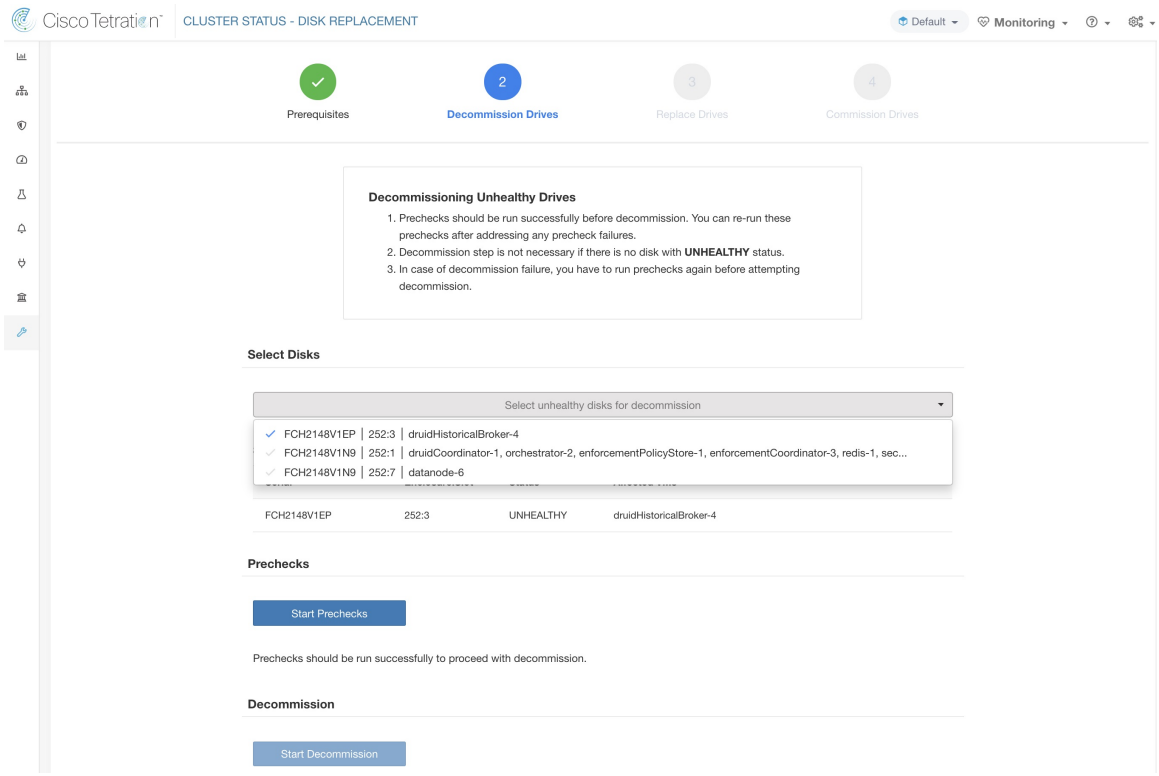
こうした事前チェックの例は次のとおりです。namenode と secondaryNamenode を一緒にデコミッションすることはできません。一度にデコミッションできるデータノードは 1 つだけです。 namenode はコミッション前に正常でなければなりません。

**図 *63* : ディスク交換の事前チェック**



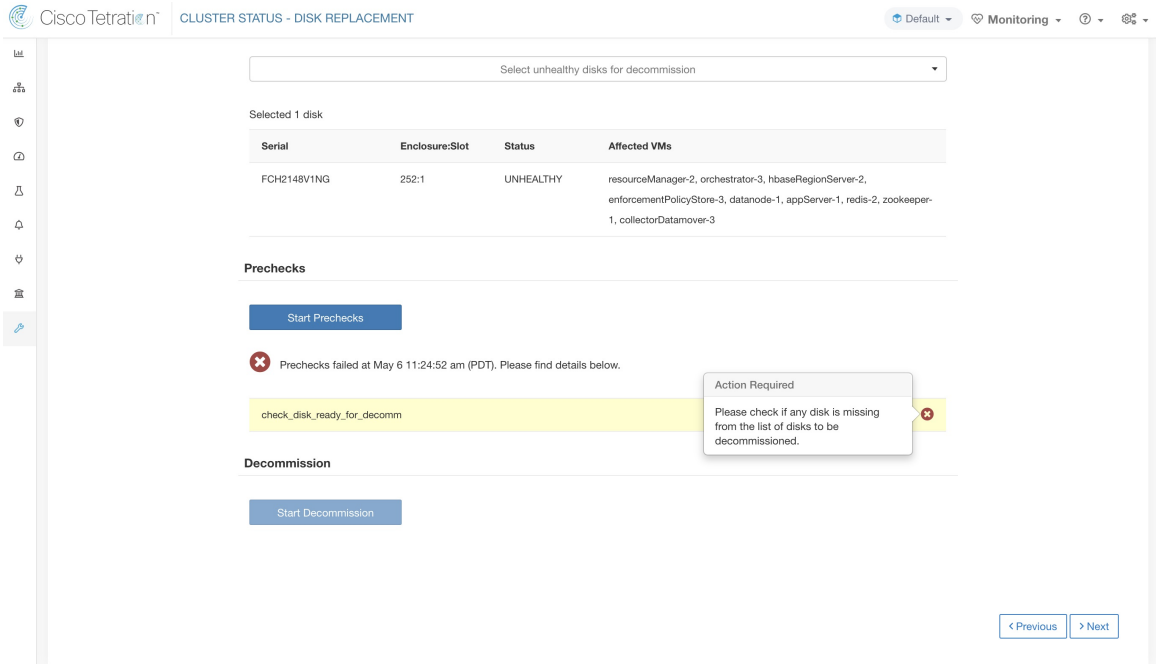
ユーザーは、障害が発生したディスクの任意のセットをまとめてデコミッションするために選択し、デコミッションの事前チェックを開始できます。障害が発生したディスクのセットを変更するには、事前チェックを再実行する必要があります。タスク（デコミッション/コミッション）を開始する前に、同じ事前チェックを再度行って、最後の事前チェックの実行からデコミッションタスクの開始までの間に新しい事前チェックの失敗がないことを確認します。

**図 *64 : デコミッションする 1 つまたはすべての異常（UNHEALTHY）ディスクの選択***




事前チェックが失敗した場合、失敗メッセージをクリックすると詳細メッセージが表示され、ポインターを赤い十字ボタンの上に置くと、推奨される処置がポップオーバーに表示されます。

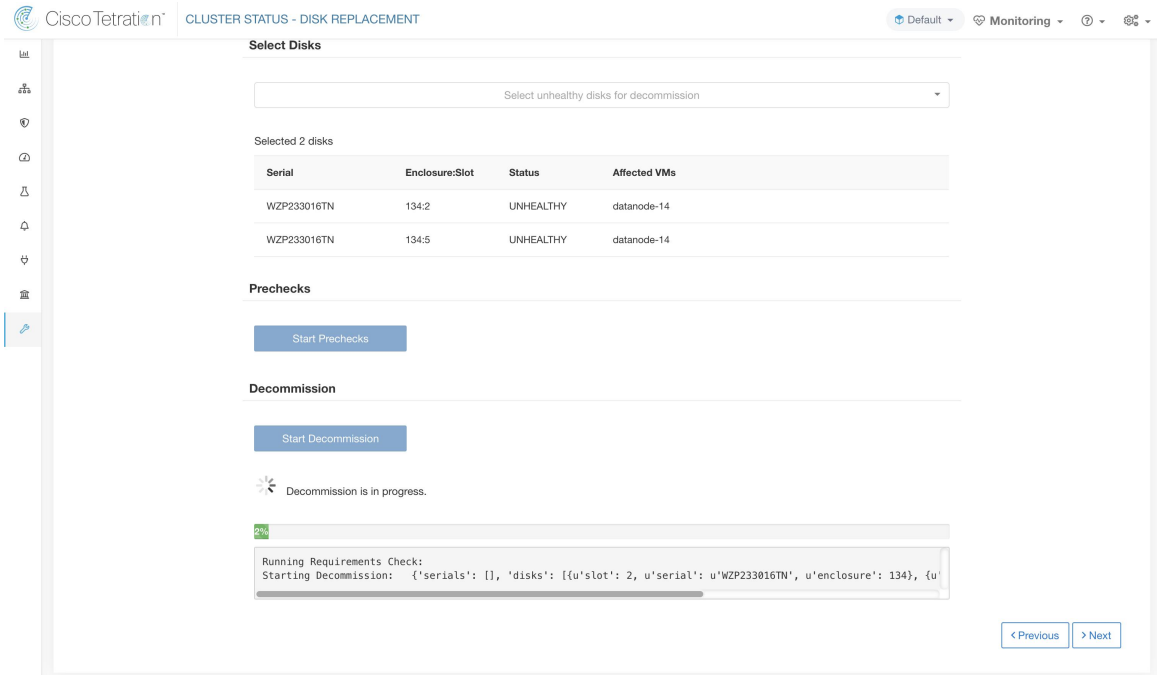
図 *65* : 事前チェックに失敗した場合にポップオーバーで表示される推奨処置




## デスクのデコミッション

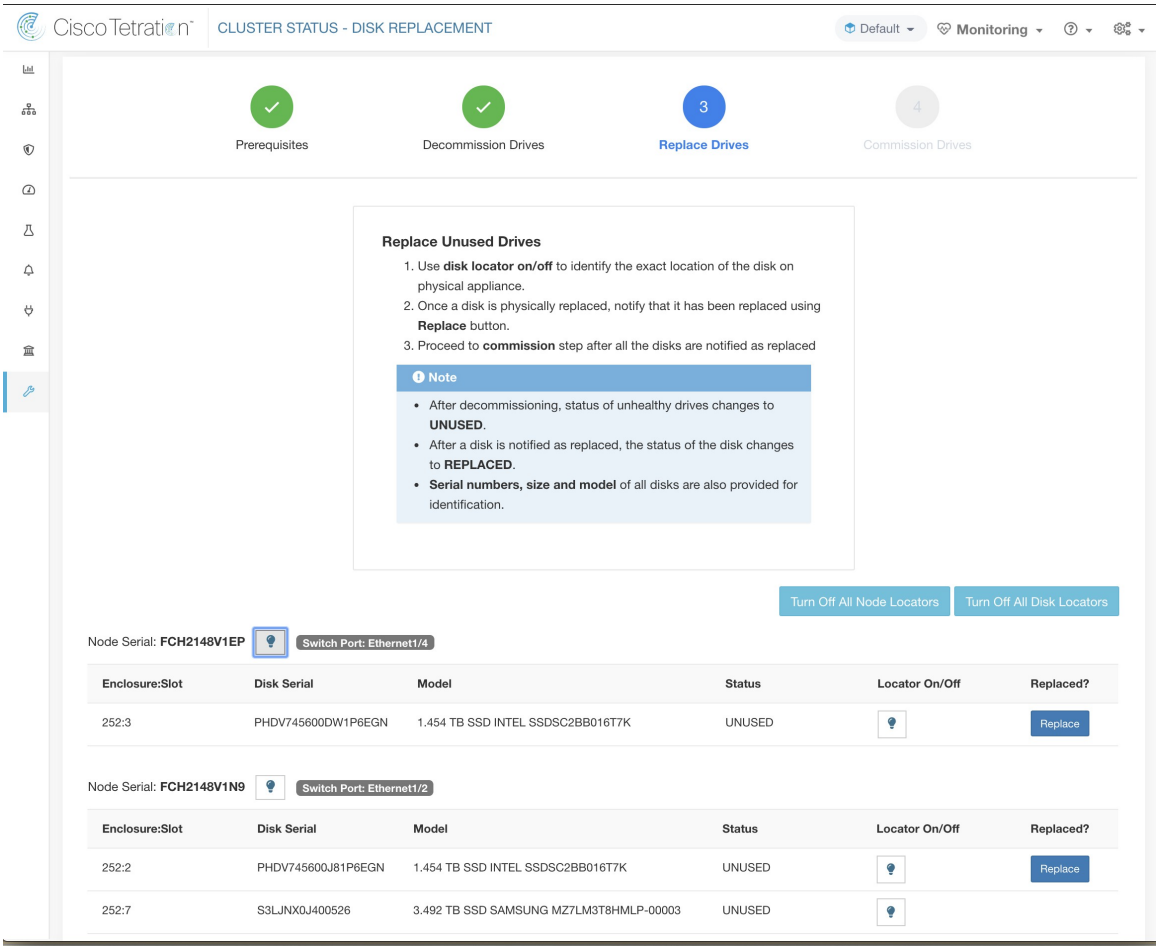
事前チェックに合格すると、ユーザーはディスクのデコミッションに進むことができます。デコミッションの進行状況は、ディスク交換ウィザードに表示されます。デコミッションの進行状況が 100% に達すると、デコミッションされたすべてのディスクのステータスが未使用（UNUSED）に変わります。

図 *66 :* ディスクのデコミッションの進行状況の監視



## ディスクの交換

**図 *67* : 新しく追加されたディスクの再設定**



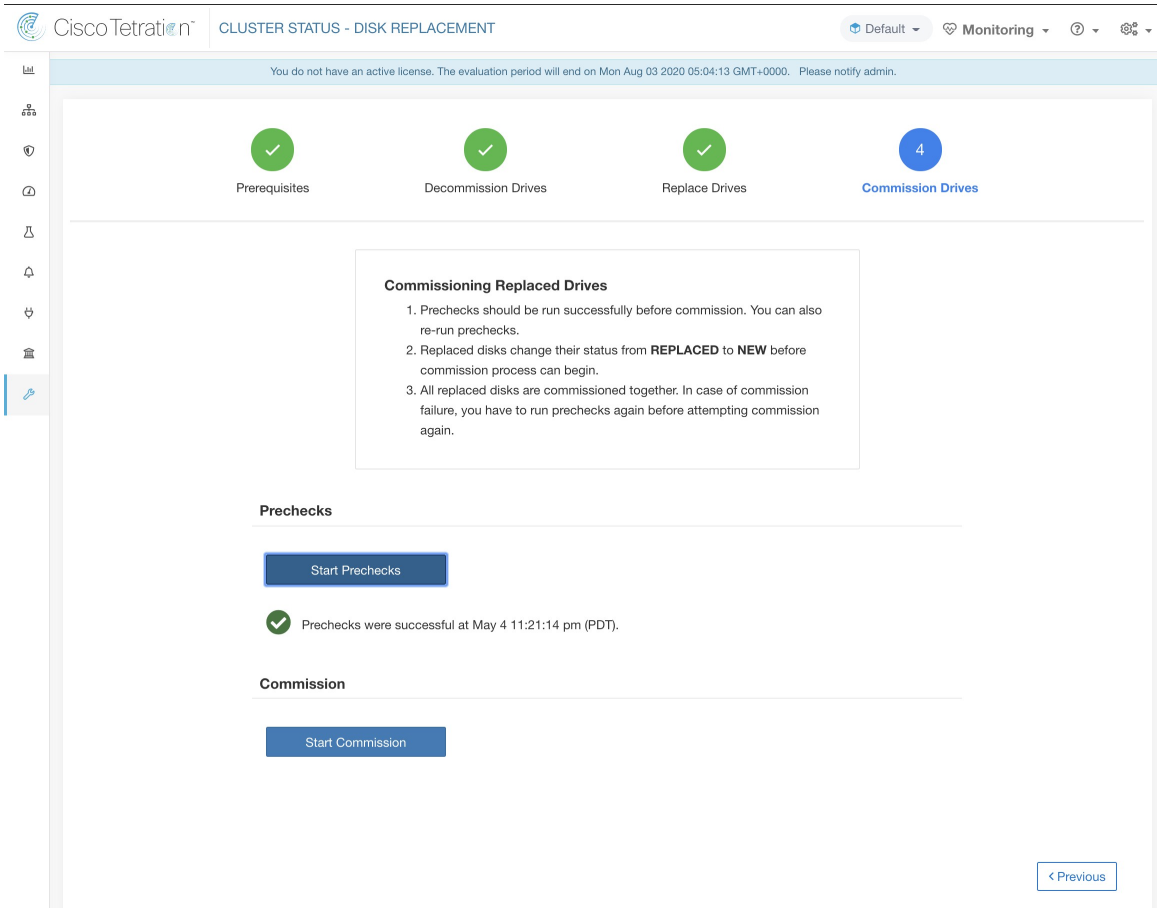

ディスクのデコミッション後、ユーザーはディスクを物理的に交換する必要があります。このプロセスを支援するために、交換ページにディスクとサーバーのロケーター LED へのアクセス機能を追加しました。サーバーとディスクのロケーター LED をすべてオフにするボタンがあるので、他のプロセスでロケーターがオンのままになっている可能性に対処することができます。

ディスクの物理的な交換は任意の順序で行えますが、再設定は特定のサーバーの最小スロット番号から最大スロット番号の順序で行う必要があります。この順序は、UI とバックエンドの両方に適用されます。UI では、ステータスが未使用（UNUSED）で、スロット番号が最も小さいディスクの交換ボタンがアクティブになります。

### デスクのコミッショニング

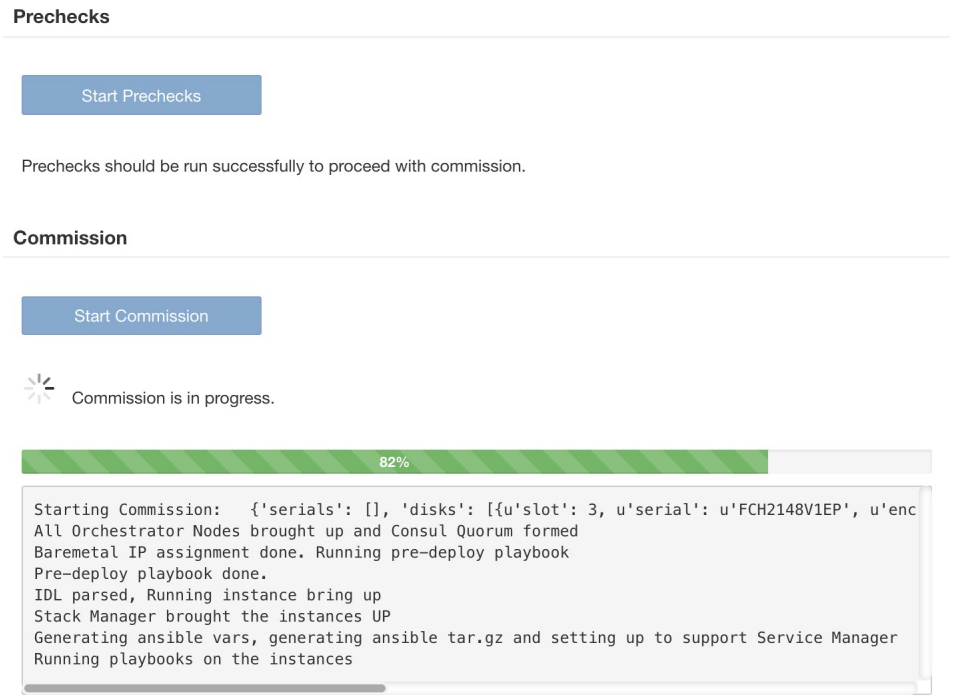
すべてのディスクを交換したら、コミッションに進みます。デコミッションと同様に、コミッション転を続行する前に一連の事前チェックを実行する必要があります。

**図 *68 :* コミッション前の事前チェック**




コミッションの進行状況は、ディスクコミッションページで監視します。コミッションが正常に終了すると、すべてのディスクのステータスが正常（HEALTHY）に変わります。

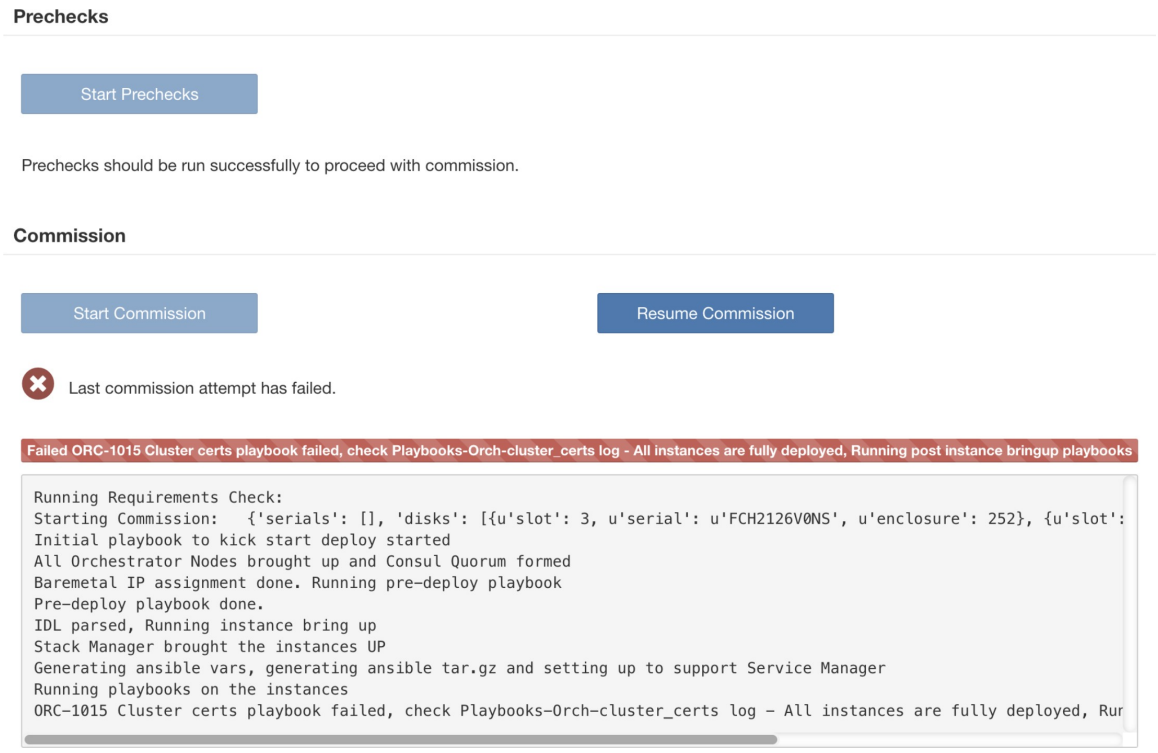
図 *69* : コミッションの進行状況




## コミッション中の障害からの復旧

VM が再展開された後に障害が発生した場合は、再開（Resume）機能で回復できます。このようなエラーが発生した場合、[コミッションの再開（Resume Commission）] ボタンがディスクコミッションページに表示されます。このボタンをクリックすると、展開後のプレイブックを再起動してコミッションを続行できます。

図 *70 :* コミッションの再開




VM が再展開される前に障害が発生した場合、コミッション中だったディスクのステータスは異常（UNHEALTHY）に変更されます。そのため、交換プロセスは異常（UNHEALTHY）ディスクのデコミッションから再開する必要があります。

### コミッション中の追加のディスク障害

ディスクのコミッションの進行中に交換対象のディスク以外のディスクに障害が発生した場合、進行中のコミッションプロセスが成功または失敗した後に、ディスク交換ウィザードにこの障害に関する通知が表示されます。

再開可能な障害が発生した場合、ユーザーは次のステップについて2つのオプションから選択することができます。

1. 現在のコミッションを再開および完了してから、新しい障害に対するディスク交換プロセスの実行を試みます。
2. または、新しく故障したディスクのデコミッションを開始し、すべてのディスクのコミッションをまとめて実行します。

この2番目の方法は、再開不可能な障害が発生した場合に使用できる唯一の方法です。新しく障害が発生したディスクが原因で展開後に障害が発生した場合、再開ボタンは使用できますが、その場合でも 2 番目の方法が唯一の対処方法になります。

### トラブルシューティング

### ログ

1. すべてのディスクコミッション/デコミッションログは、オーケストレータログの一部です。デバッグの開始ポイントは、orchestrator.service.consul の /local/logs/tetration/orchestrator/orchestrator.log である必要があります。
2. ディスクの交換/再設定アクション中に発生した障害の詳細は、対象のサーバーの bmmgr ログで探すことができます。サーバー上のログの場所は、/local/logs/tetration/bmmgr/bmmgr.log になります。

### 制限事項

1. サーバーのルートボリュームを含むディスクは、この手順では交換できません。このようなディスク障害は、サーバーメンテナンスプロセスを使用して修正する必要があります。
2. ディスクのコミッションは、すべてのサーバーがアクティブで、コミッション済みの状態にある場合にのみ実行できます。ディスクとサーバーの交換を組み合わせることが必要な場合の対応方法については、以下の特別な対処方法のセクションを参照してください。

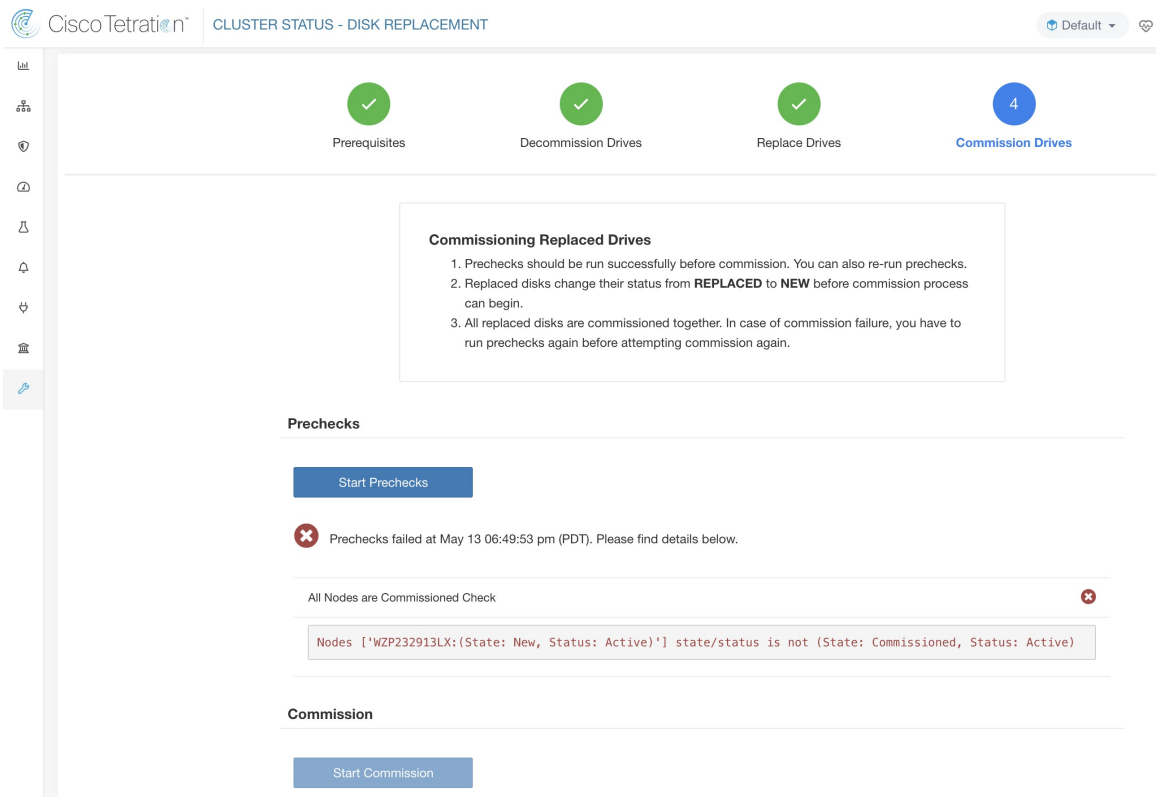
### 特別な対処方法

#### ディスクとサーバーをまとめて交換する

ディスクとサーバーを同時にコミッションする必要がある障害シナリオでは、ユーザーは、デコミッション可能なすべてのディスクをデコミッションして交換する必要があります。事前チェックで以下ことが確認されるため、これらのディスクをコミッションすることはできません。

1. すべての正常でないディスクのステータスが新規（NEW）であること。
2. すべてのサーバーのステータスがアクティブで、コミッション済みの状態であること。

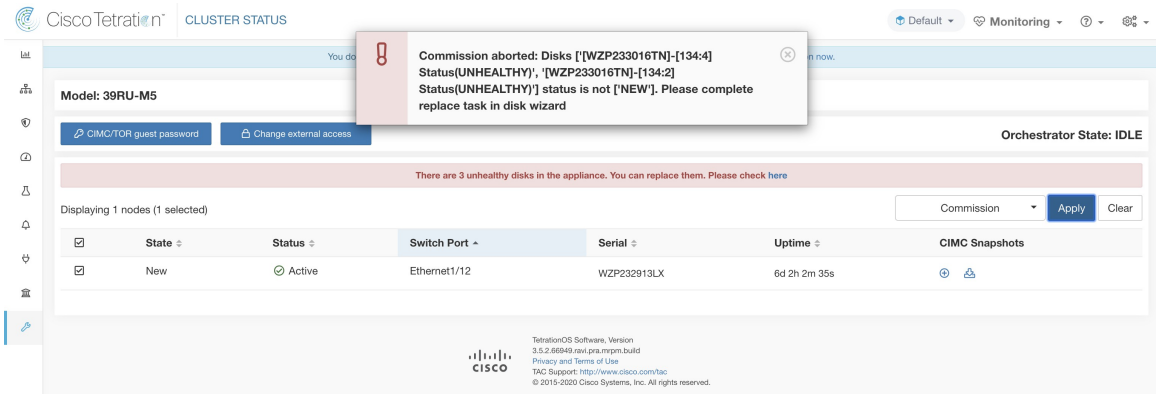
**図 *71*：ディスクのコミッションの前に、すべてのサーバーがコミッション済みでアクティブであることを確認します**




すべての異常（UNHEALTHY）ディスクが新規（NEW）状態になると、障害の発生したサーバーは、サーバーメンテナンス手順を使用してデコミッション/再イメージ化/再コミッションさせることが期待されます。

これで、ステータスが正常（HEALTHY）または新規（NEW）でないディスクがある場合、サーバーのコミッションが防止されます。サーバーのコミッションが成功すると、すべてのディスクのステータスも正常（HEALTHY）になります。

**図 *72*：サーバーをコミッションする前に、障害のあるすべてのディスクが新規（*NEW*）状態であることを確認します**



# クラスタのメンテナンス：クラスタのシャットダウンと再起動

このセクションでは、クラスタ全体に影響を及ぼす2つのメンテナンス操作について説明します。

1. クラスターのシャットダウン
2. クラスターの再起動

## クラスタのシャットダウン

クラスタのシャットダウンでは、実行中のすべてのSecure Workloadプロセスを停止させ、個々のノードの電源をすべてダウンさせます。以下の手順でシャットダウンを実行してください。

### シャットダウンの開始

**ステップ1** ウィンドウの左側にあるナビゲーションバーから、**[プラットフォーム（Platform）]** > **[アップグレード/再起動/シャットダウン（Upgrade/Reboot/Shutdown）]** をクリックします。

**ステップ2** [再起動/シャットダウン（Reboot/Shutdown）] タブをクリックします。

**ステップ3** [シャットダウン（Shutdown）]オプションボタンを選択し、[シャットダウンリンクの送信（Send Shutdown Link）]をクリックします。クリックすると、以下に示すように、電子メールでシャットダウンリンクが送信されます。シャットダウンリンクは、リンクを要求しているユーザーの電子メールアドレスに配信されます。

**図 *73:* シャットダウンメール**

Hello Site Admin!

We received a request that you intend to shutdown the cluster "98". You can do this through the link below.

Shutdown 98 (For best results, please use Google Chrome)

The above link expires by Jul 22 08:34:30 pm (PDT).

If you didn't request this, please ignore this email.

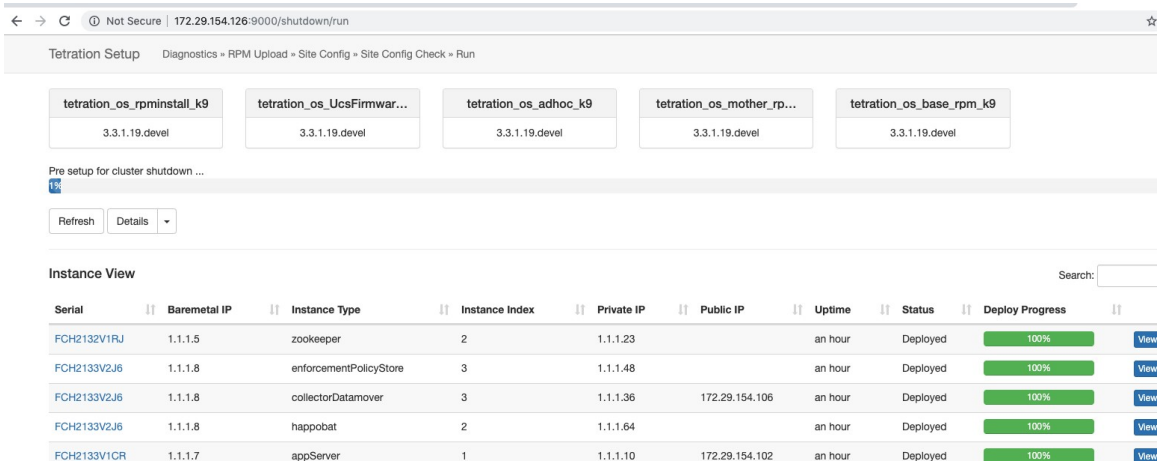
Shutdown will not be triggered until you actually click the above link.

**ステップ4** [クラスタシャットダウン（Cluster Shutdown）] ページの赤い [シャットダウン（Shutdown）] ボタンをクリックして、シャットダウンを開始します。**重要：このボタンをクリックした後にシャットダウンをキャンセルすることはできません。**

# シャットダウンの進捗状況

シャットダウンが開始されると、シャットダウンの進行状況を追跡する進行状況バーがページに表示されます。

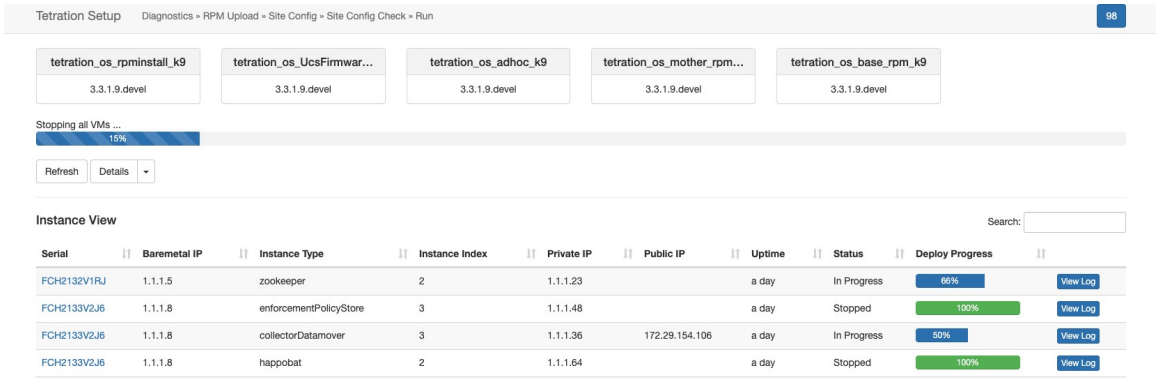
**図 *74 :* シャットダウンの進捗状況**




最初のシャットダウンの事前チェックでエラーが発生した場合、進行状況バーが赤くなり、エラーの修正後にクリックしてシャットダウンを再開できる再開ボタンが表示されます。

事前チェックが完了すると、VMが停止します。VMが徐々に停止する間、その進行状況がページの下部に表示されます。このページは、アップグレード中の VM 停止のページに似ています。表示されている各フィールドの詳細については、アップグレードのセクションを参照してください。VM の停止には最大 30 分かかる場合があることに注意してください。

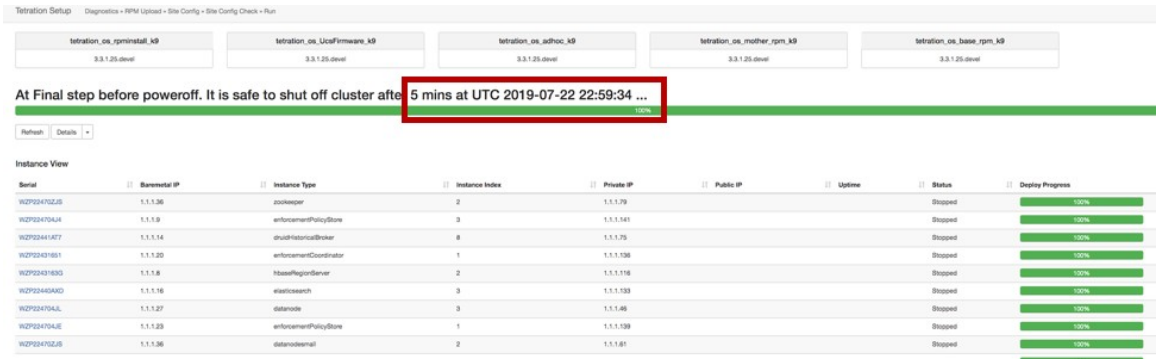
**図 *75 : VM* 停止**




最終的に、クラスタを完全にシャットダウンする準備が整うと、進行状況バーが 100% になり、クラスタの電源の安全な切断が可能になる時刻が示されます。その時刻は、以下のスクリーンショットで強調表示されています。

（注） 進行状況バーに表示される時刻を過ぎるまで、クラスタの電源を切らないでください。

図 *76 :* シャットダウン *100%*




# クラスタの再起動

シャットダウン後にクラスタを回復するには、ベアメタルの電源をオンにします。個々のベアメタルがすべて起動すると、UI に再びアクセスできるようになります。クラスタにログインした後、クラスタを再起動して、クラスタを再び完全に動作可能な状態にする必要があります。

（注） クラスタを再び完全に動作可能な状態にするには、シャットダウン後にクラスタを再起動する必要があります。

## 再起動の開始

**ステップ 1** ウィンドウの左側にあるナビゲーションバーから、**[プラットフォーム（Platform）] > [アップグレード/再起動/シャットダウン（Upgrade/Reboot/Shutdown）]**をクリックします。

**ステップ 2** [再起動/シャットダウン（Reboot/Shutdown）] タブをクリックします。

**ステップ 3** [再起動（Reboot）] ラジオボタンを選択し、[再起動リンクを送信（Send Reboot Link）] をクリックします。

再起動リンクは、リンクを要求しているユーザーの電子メールアドレスに送信されます。

Secure Workload サービスの再起動は、制限付きのアップグレード操作を実行します。電子メールの再起動リンクをクリックすると、再起動を開始できるセットアップ UI に移動します。

ここから先の手順はアップグレードと同じです。詳細については、アップグレードセクションを参照してください。

## シャットダウンと再起動の履歴

シャットダウンと再起動の履歴は、[アップグレード（Upgrade）] ページの [履歴（History）] タブに表示されます（左側のナビゲーションバーから**[プラットフォーム（Platform）]**>**[アップグレード/再起動/シャットダウン（Upgrade/Reboot/Shutdown）]**からアクセスします）。

# [データタップ管理者（Data Tap Admin）]：データのタップ

1. データタップ
2. 管理対象データタップ

### データタップ

（注） Cisco Secure Workload は現在、データタップ用に Kafka Broker 0.9.x、0.10.x、1.0.x、1.1.x への書き込みをサポートしています。

Secure Workload クラスタからアラートをプッシュするには、ユーザーは設定済みのデータタップを使用する必要があります。データタップ管理ユーザーは、新規または既存のデータタップを設定およびアクティブ化できる唯一のユーザーです。ユーザーは、自分の[テナント（Tenant）] に属するデータタップのみを表示できます。

**図 77：利用可能なデータタップ**


データタップを管理するには、ウィンドウの左側にあるナビゲーションバーで **[管理（Manage）]** > **[データタップ管理者（Data Tap Admin）]** をクリックします。

### 推奨される Kafka 設定

Kafka クラスタを設定する際は、Secure Workload では 9092、9093 または 9094 以降のポートの使用が推奨されます。これらのポートは Secure Workload が Kafka の発信トラフィック用に開くポートであるためです。Kafka Broker の推奨設定は次のとおりです。

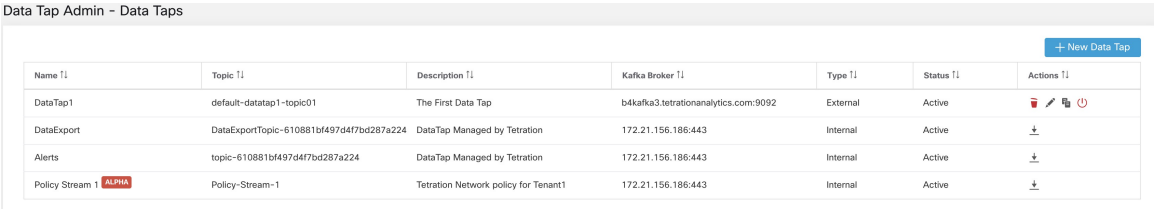
```
broker.id=<incremental number based on the size of the cluster>
auto.create.topics.enable=true
delete.topic.enable=true
listeners=PLAINTEXT://:9092
port=9092
default.replication.factor=2
host.name=<your_host_name>
advertised.host.name=<your_adversited_hostname>
num.network.threads=12
```

```
num.io.threads=12
socket.send.buffer.bytes=102400
socket.receive.buffer.bytes=102400
socket.request.max.bytes=104857600
log.dirs=<directory where logs can be written, ensure that there is sufficient space to
 hold the kafka num.partitions=72
num.recovery.threads.per.data.dir=1
log.retention.hours=24
log.segment.bytes=1073741824
log.retention.check.interval.ms=300000
log.cleaner.enable=false
zookeeper.connect=<address of zookeeper ensemble>
zookeeper.connection.timeout.ms=18000
```

### データタップ管理セクション

[データタップ管理者（Data Tap Admins）]は、**[管理（Manage）]**>**[データタップ管理者（Data Tap Admin）]**>**[データタップ（Data Taps）]**ページに移動して、利用可能なすべてのデータタップを表示および設定できます。データタップは [テナント（Tenant）] ごとに設定されます。

**図 *78*：利用可能なすべてのデータタップ**

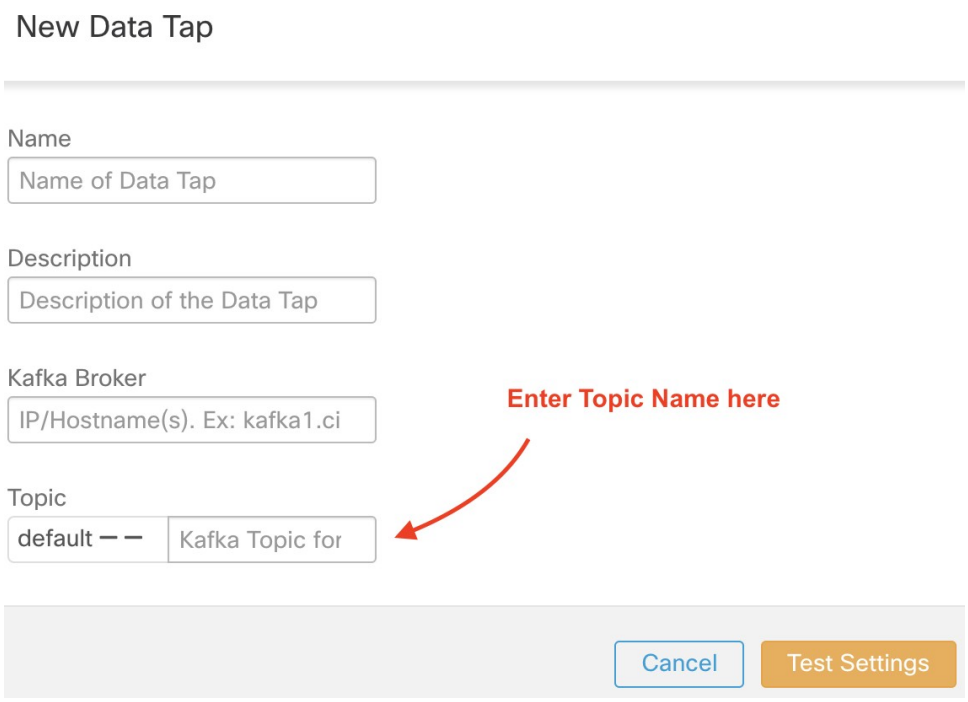



### 新しいデータタップの追加

データタップ管理者は、 

をクリックして新しいデータタップを追加できます

図 *79*：新しいデータタップの追加

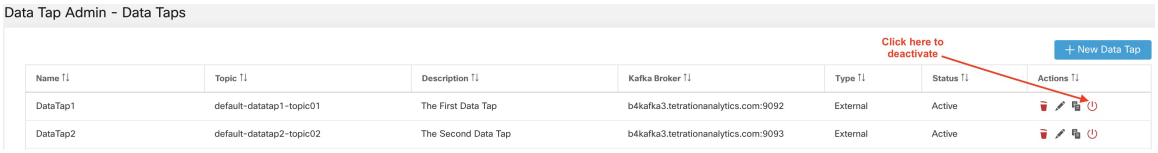



（注） データタップの値を変更するには、設定を検証する必要があります。

### データタップの非アクティブ化

データ管理者は、一時的にSecure Workloadからメッセージが送信されないように、データタップを非アクティブ化できます。そのデータタップへのメッセージは送信されません。データタップはいつでも再開できます。

図 *80*：データタップの非アクティブ化




### データタップの削除

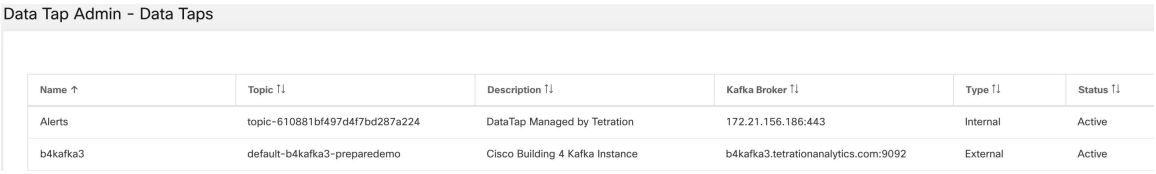
データタップを削除すると、そのアプリケーションに依存するすべてのSecure Workloadアプリケーションインスタンスが削除されます。たとえば、ユーザーがコンプライアンスアラートを（Secure Workloadアプリケーションアラートで）データタップAに送信するように指定し、管理者がデータタップAを削除した場合、アラートアプリケーションはデータタップAをアラート出力対象にしなくなります。

## 管理対象データタップ

管理対象データタップ（MDT）は、Secure Workload クラスタ内でホストされるデータタップです。認証、暗号化、承認に関しては十分に安全です。MDT との間でメッセージを送受信するには、クライアントを認証する必要があり、ネットワーク経由で送信されるデータは暗号化され、承認されたユーザーのみが Secure Workload MDT との間でメッセージを読み書きできます。 Secure Workload は、UI からダウンロードされるクライアント証明書を提供します。 Secure Workload は Apache Kafka 1.1.0 をメッセージブローカとして使用し、クライアントに同じバージョンと互換性のある安全なクライアントの使用を推奨します。

MDT はルート範囲の作成時に自動的に作成されます。すべてのルート範囲には、作成されたアラート MDT があります。ユーザーは Secure Workload クラスタからアラートを引き出すためにアラート MDT を使用する必要があります。証明書をダウンロードできるのはデータタップ管理ユーザーのみです。ユーザーは、[ルート範囲（root scope）] に属する MDT のみを表示できます。

**図 *81*：設定されたデータタップのリスト**




すべての Secure Workload アプリケーションアラートはデフォルトで MDT に送信されますが、別のデータタップに変更できます。証明書をダウンロードするには、2 つの選択肢があります。

1. JKS（Jave キーストア形式）。JKS 形式は Java クライアント向きです。
2. Certs。通常の証明書は、Go クライアントで簡単に使用できます。

**図 *82*：ダウンロード（*Download*）**

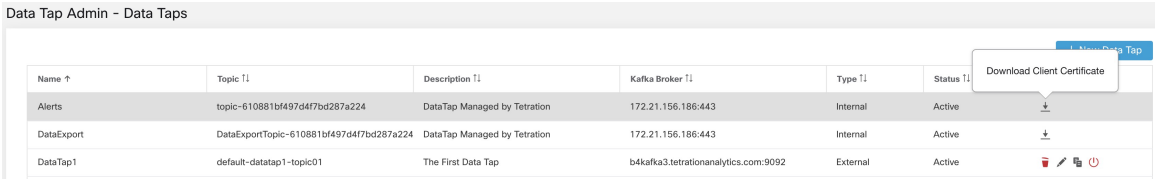
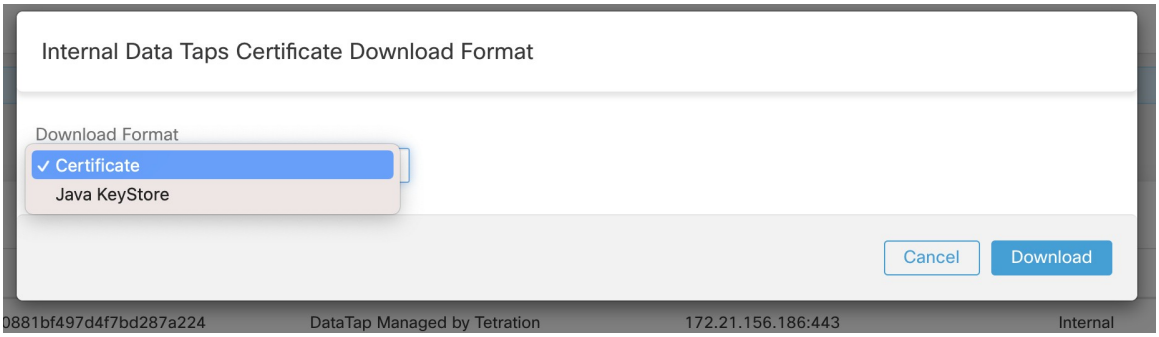



**図 *83*：証明書の種類**



### Java キーストア

Alerts.jks.tar.gz をダウンロードすると、Secure Workload MDT に接続してメッセージを受信するための情報を含む次のファイルが表示されます。

1. kafkaBrokerIps.txt：このファイルには、Kafka クライアントが Secure Workload MDT への接続に使用する必要がある IP アドレス文字列が含まれています。
2. topic.txt：このファイルには、このクライアントによるメッセージの読み取りが可能なトピックが含まれています。トピックは <root_scope_id> のトピック形式です。この root_scope_id は、後で Java クライアントで他のプロパティを設定するときに使用できます。
3. keystore.jks：Kafka クライアントが以下に示す接続設定で使用するキーストアです。
4. truststore.jks：Kafka クライアントが以下に示す接続設定で使用するトラストストアです。
5. passphrase.txt：このファイルには、#3 と #4 で使用するパスワードが含まれています。

キーストアとトラストストアを使用する Consumer.properties（Java クライアント）を設定する際には、次の Kafka 設定を使用する必要があります。

```
security.protocol=SSL
ssl.truststore.location=<location_of_truststore_downloaded>
ssl.truststore.password=<passphrase_mentioned_in_passphrase.txt>
ssl.keystore.location=<location_of_truststore_downloaded>
ssl.keystore.password=<passphrase_mentioned_in_passphrase.txt>
ssl.key.password=<passphrase_mentioned_in_passphrase.txt>
```

Java コードで Kafka コンシューマを設定する際には、次の一連のプロパティを使用する必要があります。

```
Properties props = new Properties();
props.put("bootstrap.servers", brokerList);
props.put("group.id", ConsumerGroup-<root_scope_id>); // root_scope_id is same as
‹→mentioned above
props.put("key.deserializer", "org.apache.kafka.common.serialization.
‹→StringDeserializer");
props.put("value.deserializer", "org.apache.kafka.common.serialization.
‹→StringDeserializer");
props.put("enable.auto.commit", "true");
props.put("auto.commit.interval.ms", "1000");
props.put("session.timeout.ms", "30000");
props.put("security.protocol", "SSL");
props.put("ssl.truststore.location", "<filepath_to_truststore.jks>");
props.put("ssl.truststore.password", passphrase);
props.put("ssl.keystore.location", <filepath_to_keystore.jks>);
props.put("ssl.keystore.password", passphrase);
props.put("ssl.key.password", passphrase);
props.put("zookeeper.session.timeout.ms", "500");
props.put("zookeeper.sync.time.ms", "250");
props.put("auto.offset.reset", "earliest");
```

### 証明書

エンドユーザーが証明書を使用する場合は、Sarama Kafka ライブラリを使用している Go クライアントを使用して Secure Workload MDT に接続できます。Alerts.cert.tar.gz をダウンロードすると、次のファイルが表示されます。

1. kafkaBrokerIps.txt：このファイルには、Kafka クライアントが Secure Workload MDT への接続に使用する必要がある IP アドレス文字列が含まれています。
2. topic：このファイルには、このクライアントによるメッセージの読み取りが可能なトピックが含まれています。トピックは<root_scope_id>のトピック形式です。この root_scope_id は、後で Java クライアントで他のプロパティを設定するときに使用できます。
3. KafkaConsumerCA.cert：このファイルには、Kafka コンシューマの証明書が含まれています。
4. KafkaConsumerPrivateKey.key：このファイルには、Kafka コンシューマの秘密鍵が含まれています。
5. KafkaCA.cert：このファイルは、Go クライアントの root CA 証明書リストで使用する必要があります。

Secure Workload MDT に接続する Go クライアントの次の例を参照してください。（サンプル Go コードを添付）MDT からのアラートを使用するサンプル Go クライアント

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。