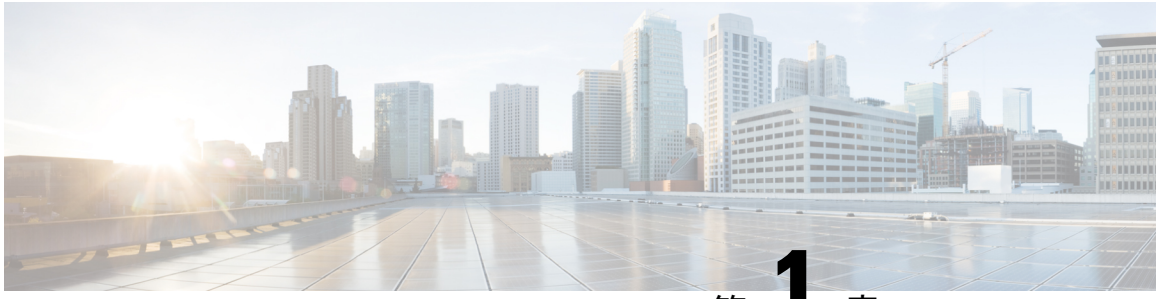
Cisco Secure Workload 移行ガイド

初版：2024 年 2 月 7 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次



第 1 章

このマニュアルについて

このマニュアルでは、オンプレミスのアプライアンス フォーム ファクタ（39RU、8RU）から Software-as-a-Service（SaaS）モデルへの移行など、導入モデル間で移行する際の Cisco Secure Workload のお客様向けのガイダンスを提供します。

このマニュアルは、各導入モデルに関連する利点と考慮事項を理解するのに役立つガイドとして機能します。たとえば、SaaS モデルには、柔軟な価格構成モデル、低い総所有コスト、および SaaS モデルを展開するためのハードウェアの物理的な設置が不要という利点があります（インフラストラクチャの所有と管理はシスコが行います）。したがって、提供されているさまざまな導入モデルを活用し、Cisco Secure Workload の導入について十分な情報に基づいて判断を下せます。

この章は、次の項で構成されています。

ユーザー構成の移行プロセスの概要

このマニュアルでは、導入モデル、移行パスの詳細、および実行し、移行が成功したことを確認するための移行プロセスについて説明します。このマニュアルには、Cisco Secure Workload の導入と管理に使用されるベストプラクティスも含まれています。

ユーザー構成の移行プロセスには、次のシナリオが含まれます。

- オンプレミスのアプライアンス フォーム ファクタ（39RU、8RU、および仮想）から SaaS モデルへの移行
- SaaS からオンプレミスのアプライアンス フォーム ファクタ（39RU、8RU、および仮想）への移行
- SaaS テナントから別の SaaS テナントへの移行
- オンプレミスのアプライアンス フォーム ファクタ（39RU、8RU）から別のオンプレミスのアプライアンス フォーム ファクタ（39RU、8RU）への移行

対象読者

このマニュアルは、Cisco Secure Workload 内でのテナント間の移行に関するワークフローの作成を支援する担当者を対象としています。

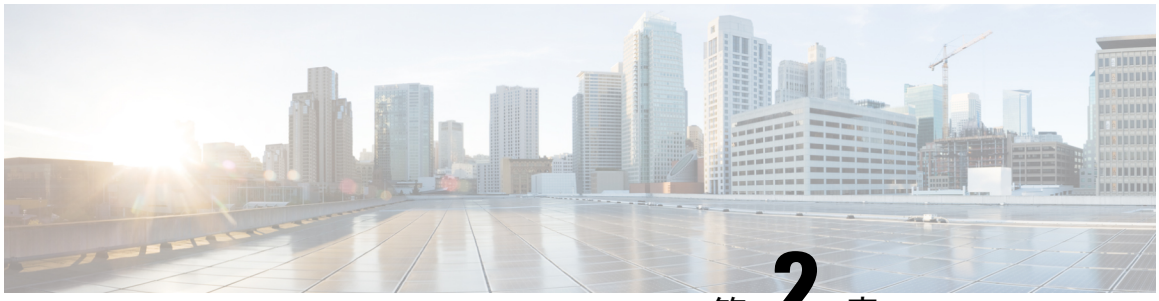
- チャネルパートナーとデリバリチーム
- シスコ顧客体験（CX）チーム
- シスコ テクニカル ソリューション アーキテクト
- Cisco Technical Assistance Center チーム

（注） シスコでは、個人およびチームが Cisco Secure Workload 環境内で必要な構成とアクションを特定して実装するために必要な知識とスキルを習得できるように、トレーニングプログラムとワークショップを提供しています。

新機能および変更された機能に関する情報

表 *1:* このマニュアルの変更点

変更内容	章	日付（**Date**）
オンプレミスクラスタから SaaS への移行マニュアルは、今後は Cisco Secure Workload 移行ガイド [英語] で維持されます。	Cisco Secure Workload オンプレミスクラスタから SaaS への移行	2024 年 2 月 7 日
初版発行。	Cisco Secure Workload クラスタ間の移行	2024 年 2 月 7 日



第 2 章

Cisco Secure Workload オンプレミスクラスタから SaaS への移行

この章では、Cisco Secure Workload SaaS 展開への Cisco Secure Workload オンプレミスクラスタの移行について重点的に説明します。このシナリオでは、各オンプレミス クラスタ テナントが SaaS 上の専用テナントに移行されます。オンプレミスのアプライアンスに複数のテナントがある場合は、各テナントを SaaS 上の対応する専用テナントに移行し、移行した新しい各 SaaS テナントに一意の URL を使用してアクセスできるようにします。

この章は、次の項で構成されています。

オンプレミスクラスタから SaaS 展開へのデータ移行の概要

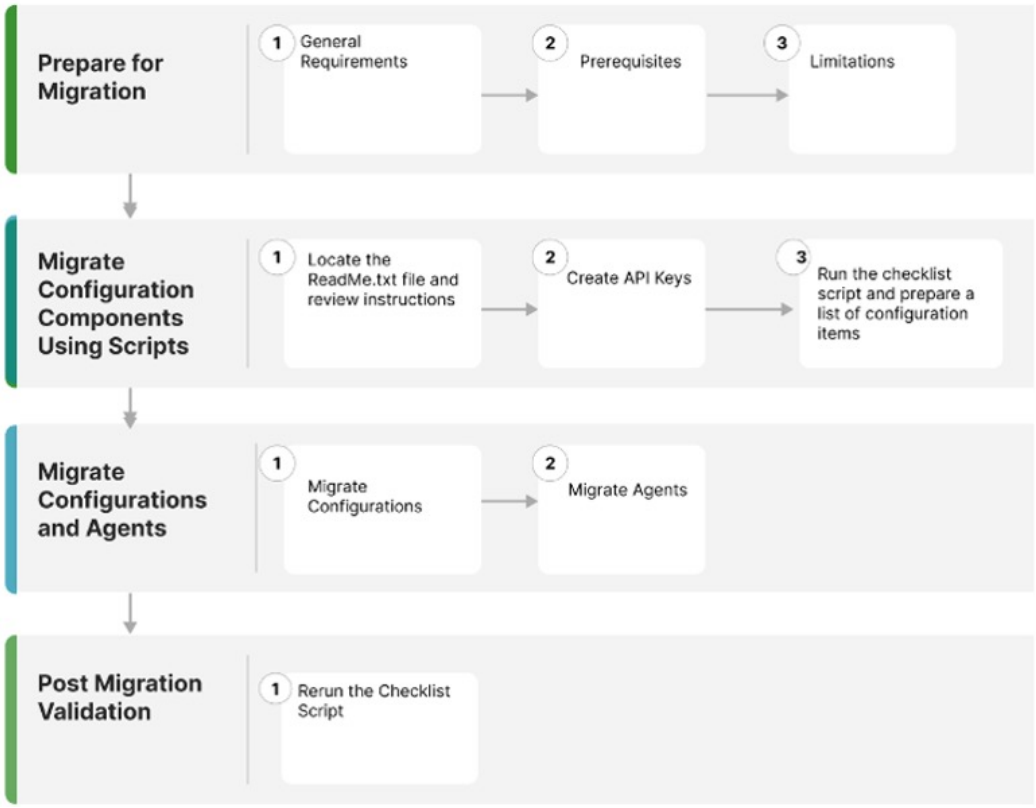
オンプレミスクラスタから Cisco Secure Workload の SaaS 展開にデータを移行する場合は、API を使用して移行プロセスを自動化します。ただし、オーケストレータ、コネクタ、仮想アプライアンス、およびユーザーアカウントの証明書とキーは手動で設定する必要があります。ユーザーは、ユーザーアカウントの移行中に、新しい Cisco Secure Workload インスタンスでパスワードをリセットする必要があります。

（注） 構成データ、フローデータ、監査ログ、会話、および ADM 履歴は、アカウントの移行には含まれません。

エンドツーエンドの移行ワークフロー

スムーズな移行を確保するには、オンプレミスアプライアンスから SaaS 展開にデータと構成を移行するために必要な手順の概要が示されている次のエンドツーエンドのワークフローに従います。移行アクティビティを最大化するには、各手順を順番に実行することが重要です。

図 *1*: 移行の準備



1	移行の準備	一般的な要件、前提条件、および制限事項を含む移行の準備。
2	スクリプトを使用した構成コンポーネントの移行	移行スクリプトをダウンロードしたら、ReadMe.txt ファイルを見つけて、テキストファイルの手順を確認します。クライアントマシンに Python 環境と移行スクリプトに必要なライブラリがインストールされていることを確認します。
3	構成とソフトウェアエージェントの移行	移行前チェックリストを作成したら、構成とソフトウェアエージェントの移行を続行します。
4	移行後の検証	自動構成項目と手動構成項目を移行したら、チェックリストスクリプトを再実行して移行状況を確認します。

前提条件

このマニュアルは、読者が Cisco Secure Workload ソリューションに精通していることを前提としており、移行プロセスに関するその他の前提条件を提供します。前提条件は次のとおりです。

- 移行プロセスに関与するオンプレミスクラスタがある場合は、単一のテナントが存在するか、オンプレミスクラスタの各テナントが専用の SaaS テナントに個別に移行されます。
- 適切なライセンスが移行先テナントで使用可能であり、SaaS への移行に管理者アクセスを使用できます。
- 移行期間中、オンプレミスクラスタ環境の構成は変更されません。
- 移行期間中、オンプレミスクラスタ環境での構成変更はフリーズします。
- オンプレミスのアプライアンスとサービスは期待どおりに動作し、正常です。
- オンプレミスのアプライアンスからの重大または警告レベルのアラートがないことを確認します。
- リリース 3.8 では、次の機能が廃止されています。
  - ハードウェアセンサーとユニバーサルエージェント。
  - データプラットフォーム：Tetration Lookout アプリケーション（**[編成（Organize）]** > **[Look Out]**）
  - [ダッシュボード（Dashboard）] : [フロー（Flows）]（**[Investigate]** > **[トラフィック ダッシュボード（Traffic Dashboard）]**）。
  - [パフォーマンス ダッシュボード（Performance Dashboard）]（**[Investigate]** > **[パフォーマンス ダッシュボード（Performance Dashboard）]**）。
  - ネイバーフッド アプリケーション（**[Investigate]** > **[ネイバーフッド（Neighborhood）]**）。
  - [ワークスペース（Workspace）] 内のポリシーコードビュー。

移行の準備

一般的な要件

- オンプレミスクラスタとソフトウェアエージェントは、バージョン 3.8 以降である必要があります。オンプレミスのアプライアンスで古いバージョンを実行している場合は、クラスタとソフトウェアエージェントを 3.8 バージョンにアップグレードしてから、移行を続行することを推奨します。

アップグレード方法の詳細については、『Cisco Secure Workload アップグレードガイド』を参照してください。

- Cisco Secure Workload プラットフォーム API と通信する外部システムのリストを作成します。移行が完了したら、新しい SaaS テナントで適切な Cisco Secure Workload API ログイン情報を作成し、新しいキーを使用して外部システムを更新してください。
- 移行中にエージェント適用の一時的な中断が予想されるため、メンテナンス期間を適宜計画してください。

前提条件

- 手動 API または自動化された API を使用して SaaS テナントを作成する場合は、ローカルユーザーをオンプレミス環境から SaaS テナントに移行します。

  外部認証には次の 2 つのタイプがあります。

  - Lightweight Directory Access Protocol（LDAP）：SaaS 環境でサポートされていないローカルユーザーを移行するには、最初にユーザーを ID プロバイダー（IdP）に移行する必要があります。ユーザーを IdP に移行するには、ユーザーとロールの手動移行の要求を SaaS プラットフォームで送信します。
  - シングルサインオン（SSO）：SSO の移行では、カスタマー IdP との**フェデレーション**を使用します。このタイプの外部認証では、SaaS プラットフォームと IdP 間の信頼関係を確立する必要があります。ユーザーとロールの手動移行の要求を SaaS プラットフォームで送信します。

- Cisco Secure Workload テナントにアクセスするための URL を変更します。
- CMDB エントリと保持の側面（オンプレミスと SaaS）を確認します。

  データの保持と削除の詳細については、「Cisco Secure Workload as a Service」を参照してください。

- オンプレミスから SaaS に移行する場合、オンプレミスアプライアンスの**[プラットフォーム（Platform）]** > **[トラブルシュート（Troubleshoot）]**セクションにある Cisco Secure Workload UI オプションは使用できません。また、SaaS 展開では外部インフラストラクチャのモニタリングは不要です。
  - SaaS 展開では、HTTP アウトバウンド/プロキシ構成は不要です。
  - [使用状況分析（Usage Analytics）] オプションは、SaaS 展開では使用できません。
- エンタープライズアウトバウンドファイアウォールルールで、Cisco Secure Workload SaaS の移行先へのアウトバウンドアクセスが許可されていることを確認します。SaaS のウェルカム電子メールには、許可リストに含める必要がある IP の詳細なリストがあります。
- 移行ワークフローの実行中に、検証の出力を文書化してください。
- 新機能の詳細については、リリースノートを参照してください。リリース 3.8 では、次の機能が廃止されています。

- ハードウェアセンサーとユニバーサルエージェント
- データプラットフォーム：Tetration Lookout アプリケーション（**[編成（Organize）]** > **[Look Out]**）
- [ダッシュボード（Dashboard）] : [フロー（Flows）]（**[Investigate]** > **[トラフィック ダッシュボード（Traffic Dashboard）]**）。
- [パフォーマンス ダッシュボード（Performance Dashboard）]（**[Investigate]** > **[パフォーマンス ダッシュボード（Performance Dashboard）]**）。
- ネイバーフッド アプリケーション（**[Investigate]** > **[ネイバーフッド（Neighborhood）]**）。
- ワークスペース内のポリシーコードビュー

制限事項

- 次のデータ項目は移行されません。
  - 履歴フローデータ
  - 変更ログ
  - API キー（再作成して外部システムに追加）
- ワークスペース内では、次のデータ項目は移行されません。
  - アクティビティログとポリシーバージョン履歴
  - ADM カンバセーションと ADM 結果の履歴と変更履歴
  - ポリシーの最新バージョンのみが移行されます。移行が完了したら、ポリシー分析を再度有効にします。
- 次のデータ項目は、SaaS 展開では使用できず、サポートされていません。
  - エージェントのリモート VRF 構成とインターフェイス構成のインテント
  - [ログイン（Login）] ページのメッセージと SSL 証明書のオプション
  - STIX-TAXII
  - [連携（Federation）]
- 移行中、SaaS 展開では以下の内容は使用できないか、または不要です。
  - オンプレミスのアプライアンスでは、GUI オプションの**[プラットフォーム（Platform）]** > **[トラブルシュート（Troubleshoot）]**は使用不可。
  - [使用状況分析（Usage Analytics）] オプションは使用不可。
  - 外部インフラストラクチャのモニタリングの回避。

• HTTP アウトバウンドまたはプロキシ構成の回避。

スクリプトを使用した構成コンポーネントの移行

ステップ 1 移行スクリプトをダウンロードしたら、ReadMe.txt ファイルを見つけて手順を確認し、Python 環境を作成し、移行スクリプトに必要なライブラリをクライアントマシンにインストールします。

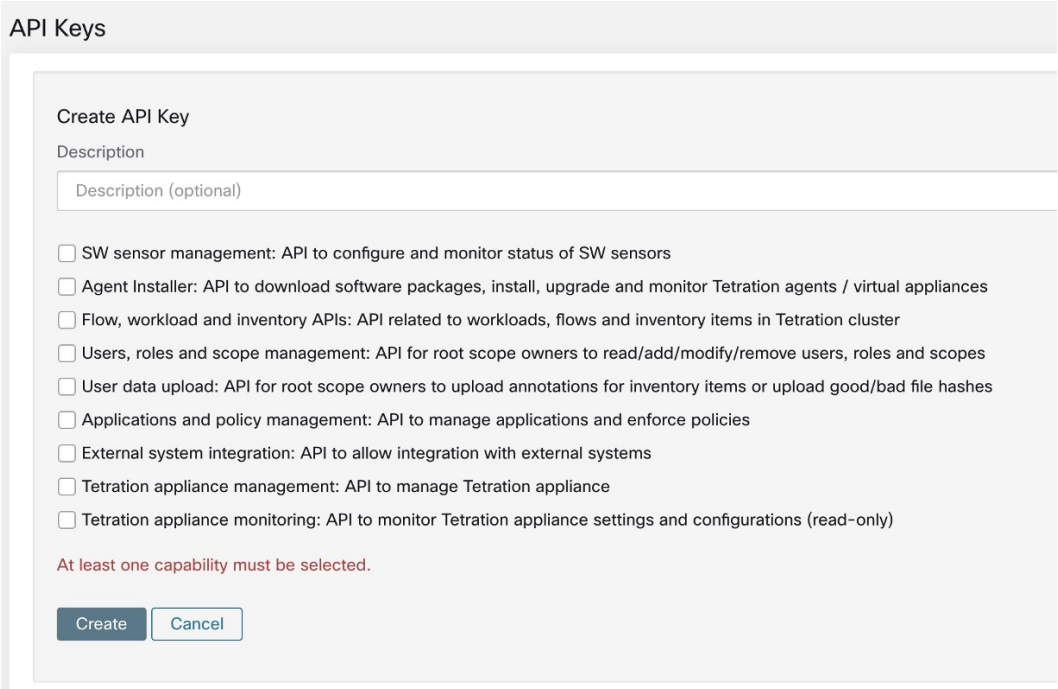
（注） TAC ケースをオープンし、オンプレミスから SaaS への移行スクリプトへのアクセスを要求します。実際のコマンドの使用方法と出力は、このマニュアルとは異なります。移行時に提供される詳細については、README マニュアルを参照してください。

ステップ 2 移行元と移行先の両方のクラスタテナントで、**サイト管理者**として Cisco Secure Workload テナントにログインします。

ステップ 3 Cisco Secure Workload UI で、**人間のアイコン** > **[APIキー（API Keys）]**の順に選択します。

ステップ 4 API キーを作成するには、[APIキーの作成（Create API Key）] を選択し、次のリストにある少なくとも 1 つの API 機能をオンにします。

図 *2 : API* キー機能

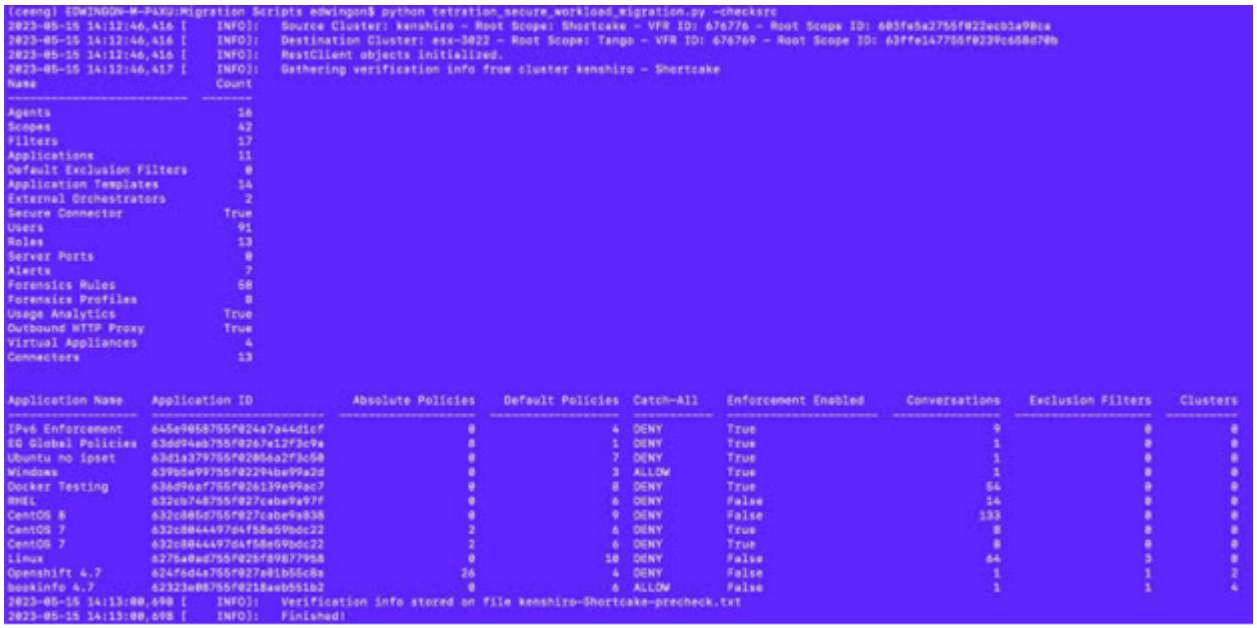


ステップ 5 API キーファイルをダウンロードし、移行スクリプトと同じ場所に保存します。

ステップ 6 オンプレミステナントでチェックリストスクリプトを実行して、移行する構成項目のリストを準備します。チェックリストスクリプトからの出力は必ず記録してください。

ステップ 7 移行のさまざまな段階で新しいSaaSテナントに対してチェックリストスクリプトを再実行して、すべての構成項目が適切に移行されるようにします。

図 *3*：チェックリストスクリプトの出力



```
(ceeng) EDWINGON-M-PAKU:Migration Scripts edwingon$ python tetration_secure_workload_migration.py -checksrc
2023-05-15 14:12:46,416 [    INFO]:   Source Cluster: kenshiro - Root Scope: Shortcake - VFR ID: 676776 - Root Scope ID: 603fe5a2755f022ec01a98ca
2023-05-15 14:12:46,416 [    INFO]:   Destination Cluster: esx-3022 - Root Scope: Tango - VFR ID: 676769 - Root Scope ID: 63ffe147755f0239c6580d70b
2023-05-15 14:12:46,416 [    INFO]:   RestClient objects initialized.
2023-05-15 14:12:46,417 [    INFO]:   Gathering verification info from cluster kenshiro - Shortcake
Name                        Count
--------------------------  -------
Agents                         16
Scopes                         42
Filters                        17
Applications                   11
Default Exclusion Filters       0
Application Templates          14
External Orchestrators          2
Secure Connector             True
Users                          91
Roles                          13
Server Ports                    0
Alerts                          7
Forensics Rules                68
Forensics Profiles              0
Usage Analytics              True
Outbound HTTP Proxy          True
Virtual Appliances              4
Connectors                     13

Application Name    Application ID            Absolute Policies    Default Policies  Catch-All    Enforcement Enabled    Conversations    Exclusion Filters    Clusters
------------------  -----------------------  -------------------  ------------------  -----------  ---------------------  ---------------  -------------------  ----------
IPv6 Enforcement    6445e90587555f024a7a44d1cf                   0                   4  DENY         True                               9                    0           0
EG Global Policies  636d94ab755f0267e12f3c9a                     0                   1  DENY         True                               1                    0           0
Ubuntu no ipset     63d1a379755f02054a2f3c68                     0                   7  DENY         True                               1                    0           0
Windows             6399b5e997555f02294be99a2d                   0                   3  ALLOW        True                               1                    0           0
Docker Testing      636d96af7555f026139e99ac7                    0                   8  DENY         True                              54                    0           0
RHEL                632cb748755f027cabe9a97f                     0                   6  DENY         False                             14                    0           0
CentOS 8            632c805d755f027cabe9a838                     0                   9  DENY         False                            133                    0           0
CentOS 7            632c8044497d4f58e59bdc22                     2                   6  DENY         True                               8                    0           0
CentOS 7            632c8044497d4f58e59bdc22                     2                   6  DENY         True                               8                    0           0
Linux               6275a0ad755f025f89877958                     0                  10  DENY         False                             64                    3           0
Openshift 4.7       624f6d4a7555f027e01b55c8a                   26                   4  DENY         False                              1                    1           2
bookinfo 4.7        62323e887555f0218aeb551b2                    0                   6  ALLOW        False                              1                    1           4
2023-05-15 14:13:00,698 [    INFO]:   Verification info stored on file kenshiro-Shortcake-precheck.txt
2023-05-15 14:13:00,698 [    INFO]:   Finished!
```

（注） 移行スクリプトを使用すると、一部の構成項目は自動化されますが、一部の項目は自動化されない可能性があります。現時点ではAPIがサポートされていないため、最後の一連の構成項目は手動で移行する必要があります。

次の表に、移行対象構成項目の完全なリストを示します。

表 *2*：移行対象構成コンポーネント

構成コンポーネント	移行方法
手動ラベル	[Automated]
スコープ	[Automated]
インベントリフィルタ	[Automated]
エージェントプロファイル	[Automated]
エージェントインテント	[Automated]
ワークスペース	[Automated]
ワークスペースポリシー（最新バージョン）	[Automated]
ワークスペースクラスタ	[Automated]
ロール	[Automated]

構成コンポーネント	移行方法
ユーザー	[Automated]
除外フィルタ：デフォルトおよびワークスペース	[Automated]
外部オーケストレータ	自動（ログイン情報が必要）
クライアントサーバーの構成（サーバーポート）	[Automated]
フォレンジック：プロファイルとインテント	[Automated]
ポリシーテンプレート（カスタムテンプレート）	手動（API 利用可能、未自動化）
収集ルール	[Automated]
デフォルトの ADM 構成	[Automated]
アラート設定/パブリッシャ	[Automated]
[セキュアコネクタ（Secure Connector）]	手動（API 利用不可）
仮想アプライアンス（Ingest または Edge）	手動（API 利用不可）
コネクタ	手動（API 利用可能、未自動化）
データタップの構成	手動（API 利用不可）

（注） **外部オーケストレータ**と**コネクタ**を使用している場合は、次の移行フェーズに進む前に、ログイン情報を用意してください。

構成とソフトウェアエージェントの移行

構成とエージェントを移行する最初のステップとして、移行前チェックリストを準備します。移行前チェックリストの準備ができたら、構成とエージェントの移行を開始します。依存関係のない一部の構成を並行して移行する場合は、エージェントの移行、移動、インストール、アンインストール、およびカットオーバーアクティビティの適用など、中断を伴うアクションのメンテナンス期間をスケジュールすることを推奨します。

顧客体験（CX）エンジニアとパートナーが、ご使用の環境と特定の要件を考慮した移行プロセス全体の詳細を記載した計画を作成します。

構成の移行

始める前に

仮想アプライアンス（Injest および Edge）とセキュアコネクタがすでに使用されている場合、移行を続行するにはそれらを再展開することを推奨します。

詳細については、『Cisco Secure Workload ユーザーガイド』の「Virtual Appliances for Connectors」を参照してください。

オンプレミスクラスタからのみ外部オーケストレータやコネクタにアクセスでき、SaaS テナントに移行する場合は、SaaS とオンプレミス インフラストラクチャ間の接続のために、オンプレミスのアプライアンスにセキュアコネクタを展開することを推奨します。

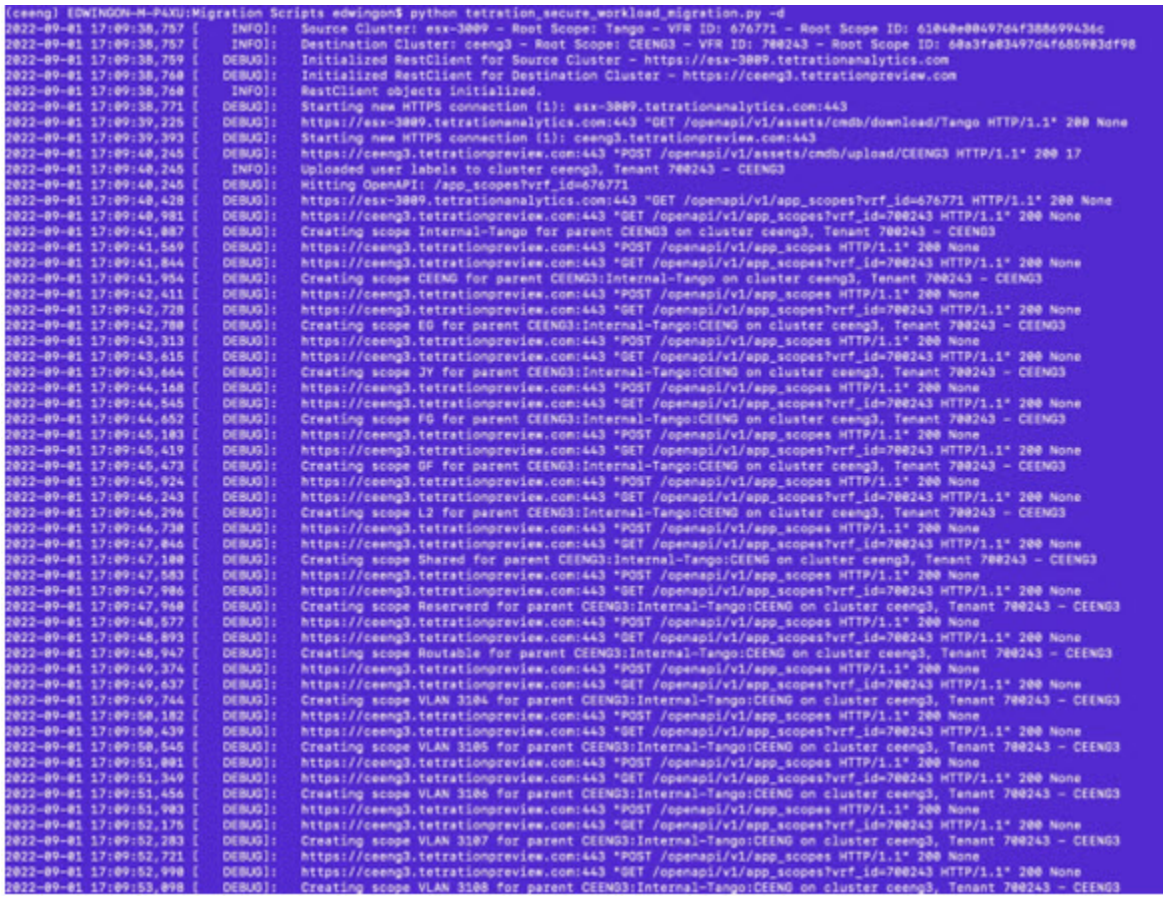
詳細については、『Cisco Secure Workload ユーザーガイド』の「Secure Connectors」を参照してください。

ステップ 1 移行スクリプトを実行して構成を移行します。

図 *4* : ラベルの移行

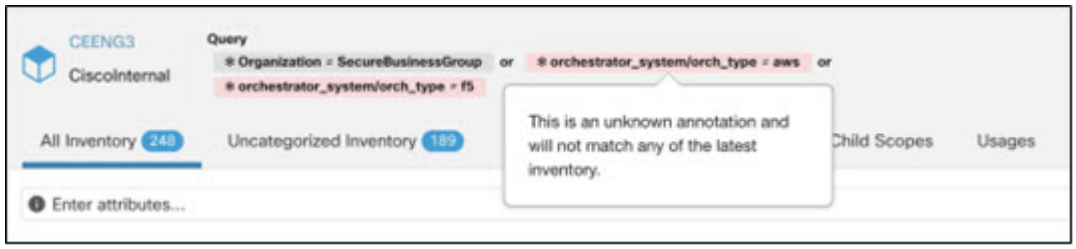
```
##########  Create CMDB (Labels) ##########

file_path = '{}-cmdb.csv'.format(src_vrf_id)
rc_src.download(file_path, '/assets/cmdb/download/%s' % src_root_scope_name)

req_payload = [tetpyclient.MultiPartOption(key='X-Tetration-Oper', val='add')]
rc_dst.upload(file_path, '/assets/cmdb/upload/%s' % dst_root_scope_name, req_payload)

print ("uploaded cmdb files to Tenant {}".format(dst_vrf_id))

uploaded cmdb files to Tenant 700243
```

図 *5*: 範囲ツリーの移行



（注） オーケストレータとコネクタ、またはエージェントのラベルに基づくフィルタ、範囲、およびインテントのクエリはすべて、新しいSaaSテナントに移行されますが、ステータスに「不明な注釈」と表示される場合があります。新しいSaaSテナントへのエージェント、コネクタ、およびオーケストレータの移行が完了すると、GUI に警告が表示されなくなります。

図 *6*: 不明な注釈



（注） 移行スクリプトは、SaaSテナント内のワークスペースの適用を無効にするため、エージェントの移行完了後に適用を再度手動で有効にする必要があります。

ステップ 2 サマリースクリプトオプションを実行して、各自動構成項目を移行前に記録された出力と比較します。特定の項目の不一致については、オンプレミスのテナント構成と SaaS テナント構成の比較を実行して、構成項目を特定します。

（注） TAC および SRE チームと協力して、移行の失敗原因をさらに調査します。

ステップ 3 共有自動化スクリプトを使用して**コネクタ**の移行は自動化できませんが、自動化された移行には API を使用できます。**コネクタ**の API キー、シークレット、またはログイン情報を再作成し、以降先 SaaS テナントの新しい構成に追加します。詳細については、『Cisco Secure Workload ユーザーガイド』の「Secure Connectors」を参照してください。

ソフトウェアエージェントの移行

始める前に

オンプレミスクラスタとソフトウェアエージェントが同じバージョン（Cisco Secure Workload 3.8.xx）で実行されていることを確認します。

移行プロセスを開始する前に、必要なアプリケーションに対する機能テストのリストを準備します。テストを実行し、期待どおりの結果が得られ、結果が記録されていることを確認します。

ステップ 1 移行のために選択した一連のエージェントの適用を無効にします。移行計画に応じて、すべてのエージェントを移行するための単一のアプローチまたは段階的なアプローチを選択します。

ステップ 2 ナビゲーションウィンドウで、**[管理（Manage）]** > **[エージェント（Agents）]**の順に選択し、[エージェントのリホーム（Agent Rehoming）] オプションを選択して、 エージェントのリホーム構成を追加します。

[範囲アクティベーションキー（Scope Activation Key）]：ナビゲーションウィンドウで、**[メニュー（Menu）]** > **[ワークロード（Workloads）]** > **[エージェント（Agents）]** > **[インストーラ（Installer）] タブ** > **[エージェント イメージ インストーラ（Agent Image Installer）]**の順に選択します。

[移行先センサーCA証明書（Destination Sensor CA Cert）]：移行先クラスタのナビゲーションウィンドウで、**[メニュー（Menu）]** > **[プラットフォーム（Platform）]** > **[クラスタ構成（Cluster Configuration）]**の順に選択します。

[移行先センサーVIP（Destination Sensor VIP）]：移行先クラスタのナビゲーションウィンドウで、**[メニュー（Menu）]** > **[プラットフォーム（Platform）]** > **[クラスタ構成（Cluster Configuration）]**の順に選択します。

（注） SaaS 展開の場合は、センサー VIP：「wss<cluster_name>.tetrationcloud.com」および「cluster_name」をエージェントインストーラスクリプト名から取得します。インストーラスクリプトのファイル名の形式は、tetration_installer_<tenant_name>_<agent_type>_<os>_<cluster_name> です。

図 *7:* エージェントのリホーム

ステップ 3 エージェントのリホームについては、すべてのエージェントまたは移行に必要な一連のエージェントのみを選択し、[エージェントのリホーム（Re-home Agents）] をクリックします。

ステップ 4 Cisco Secure Workload UI の**[管理（Manage）] > [エージェント（Agents）] > [エージェントリスト（Agent list）]**の下に各エージェントが正しく登録されていることを確認します。

（注） エージェントのステータスがアクティブと表示されるまで数時間かかります。

ステップ 5 エージェントを移行したら、関連するワークスペースでの適用を有効にします。

ステップ 6 ワークスペースでポリシーをプロビジョニングしていることを確認します。ナビゲーションウィンドウで、Cisco Secure Workload UI の**[防御（Defend）] > [適用ステータス（Enforcement status）]**の順に選択して、以下の点を確認します。

- [同期している具体的なポリシー（Concrete Policies in Sync）] ステータスが緑色で [はい（Yes）] と表示されている。
- [同期している具体的なポリシー（Concrete Policies in Sync）] ステータスが 赤色で [いいえ（No）] と表示されている。

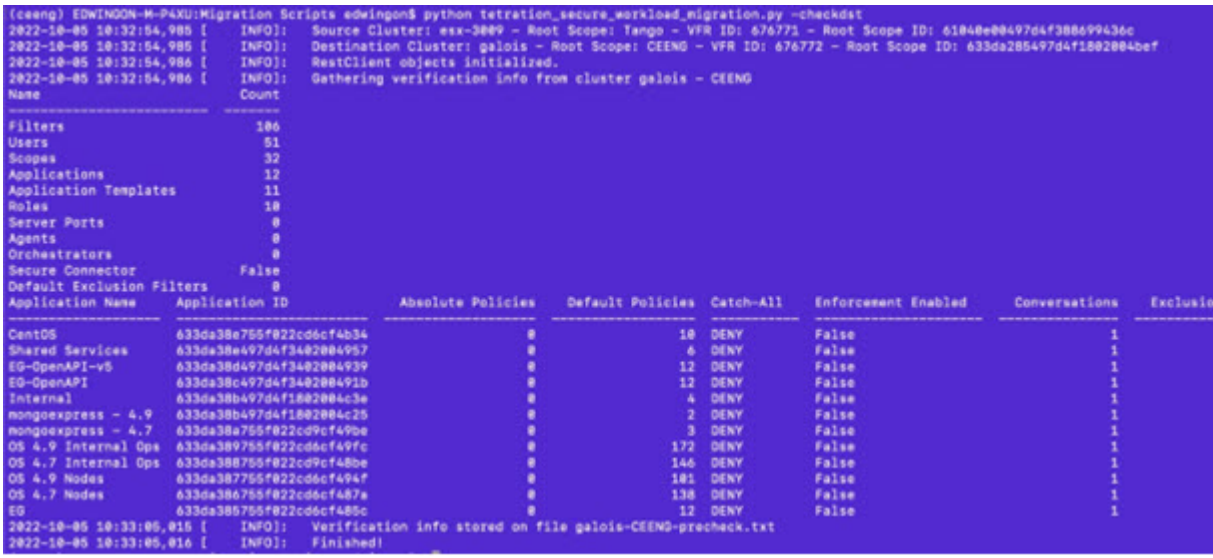
  ナビゲーションウィンドウで、指定されたワークロードの [ワークロードプロファイル（Workload profile）] を選択し、**[ログのダウンロード（Download logs）] > [ログ収集の開始（Initiate log collection）]** でエラーを探します。

（注） 必要なすべてのチェックを完了してから、検証チェックに進みます。

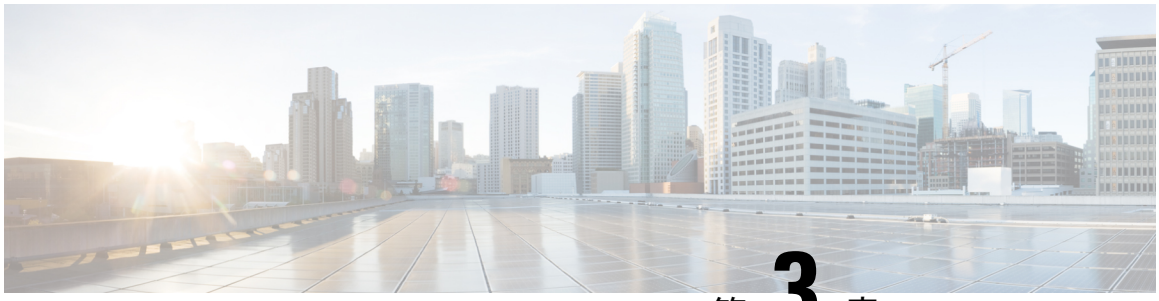
移行後の検証

自動構成と手動構成を移行したら、チェックリストスクリプトを再実行し、SaaSテナントの構成項目（エージェントの数を含む）がオンプレミステナントの項目と一致していることを確認します。

図 *8 :* 移行後の検証



```
(ceeng) EDWINGON-M-P4XU:Migration Scripts edwingon$ python tetration_secure_workload_migration.py -checkdst
2022-10-05 10:32:54,985 [    INFO]:   Source Cluster: esx-3089 - Root Scope: Tango - VFR ID: 676771 - Root Scope ID: 61040e00497d4f388699436c
2022-10-05 10:32:54,985 [    INFO]:   Destination Cluster: galois - Root Scope: CEENG - VFR ID: 676772 - Root Scope ID: 633da285497d4f1802004bef
2022-10-05 10:32:54,986 [    INFO]:   RestClient objects initialized.
2022-10-05 10:32:54,986 [    INFO]:   Gathering verification info from cluster galois - CEENG
Name                       Count
-------------------------  -------
Filters                      106
Users                         51
Scopes                        32
Applications                  12
Application Templates         11
Roles                         10
Server Ports                   0
Agents                         0
Orchestrators                  0
Secure Connector           False
Default Exclusion Filters      0
Application Name     Application ID            Absolute Policies    Default Policies  Catch-All    Enforcement Enabled      Conversations    Exclusio
-------------------  ------------------------  -------------------  ----------------  -----------  ---------------------  ---------------  ----------
CentOS               633da38e755f822cd6cf4b34                    0                10  DENY         False                              1
Shared Services      633da38e497d4f3402004957                    0                 6  DENY         False                              1
EG-OpenAPI-v5        633da38d497d4f3402004939                    0                12  DENY         False                              1
EG-OpenAPI           633da38c497d4f340200491b                    0                12  DENY         False                              1
Internal             633da38b497d4f1802004c3e                    0                 4  DENY         False                              1
mongoexpress - 4.9   633da38b497d4f1802004c25                    0                 2  DENY         False                              1
mongoexpress - 4.7   633da38a755f822cd9cf49de                    0                 3  DENY         False                              1
OS 4.9 Internal Ops  633da389755f822cd6cf49fc                    0               172  DENY         False                              1
OS 4.7 Internal Ops  633da388755f822cd9cf48be                    0               146  DENY         False                              1
OS 4.9 Nodes         633da387755f822cd6cf494f                    0               181  DENY         False                              1
OS 4.7 Nodes         633da386755f822cd6cf487e                    0               138  DENY         False                              1
EG                   633da385755f822cd6cf485c                    0                12  DENY         False                              1
2022-10-05 10:33:05,015 [    INFO]:   Verification info stored on file galois-CEENG-precheck.txt
2022-10-05 10:33:05,016 [    INFO]:   Finished!
```



第 3 章

Cisco Secure Workload クラスタ間の移行

この章では、移行パス、前提条件、制限事項、および移行を実行して成功を確認するためのワークフローガイダンスに関する段階的なプロセスの概要を示します。このプロセスでは、Cisco Secure Workload M4 または M5 クラスタから、39RU や 8RU などの一致するフォームファクタを持つ M6 クラスタにデータと構成を移行します。

この章は、次の項で構成されています。

クラスタ間の移行の概要

Cisco Secure Workload のプライマリクラスタからスタンバイクラスタにデータを転送する場合は、Data Backup and Restore（DBR）方式を使用することを推奨します。DBR を使用すると、プライマリクラスタから S3 互換ストレージにデータがコピーされ、同じデータがストレージからスタンバイクラスタに復元されます。特定の移行ニーズに応じて、「リーンモード」または「完全モード」のバックアップを選択できます。

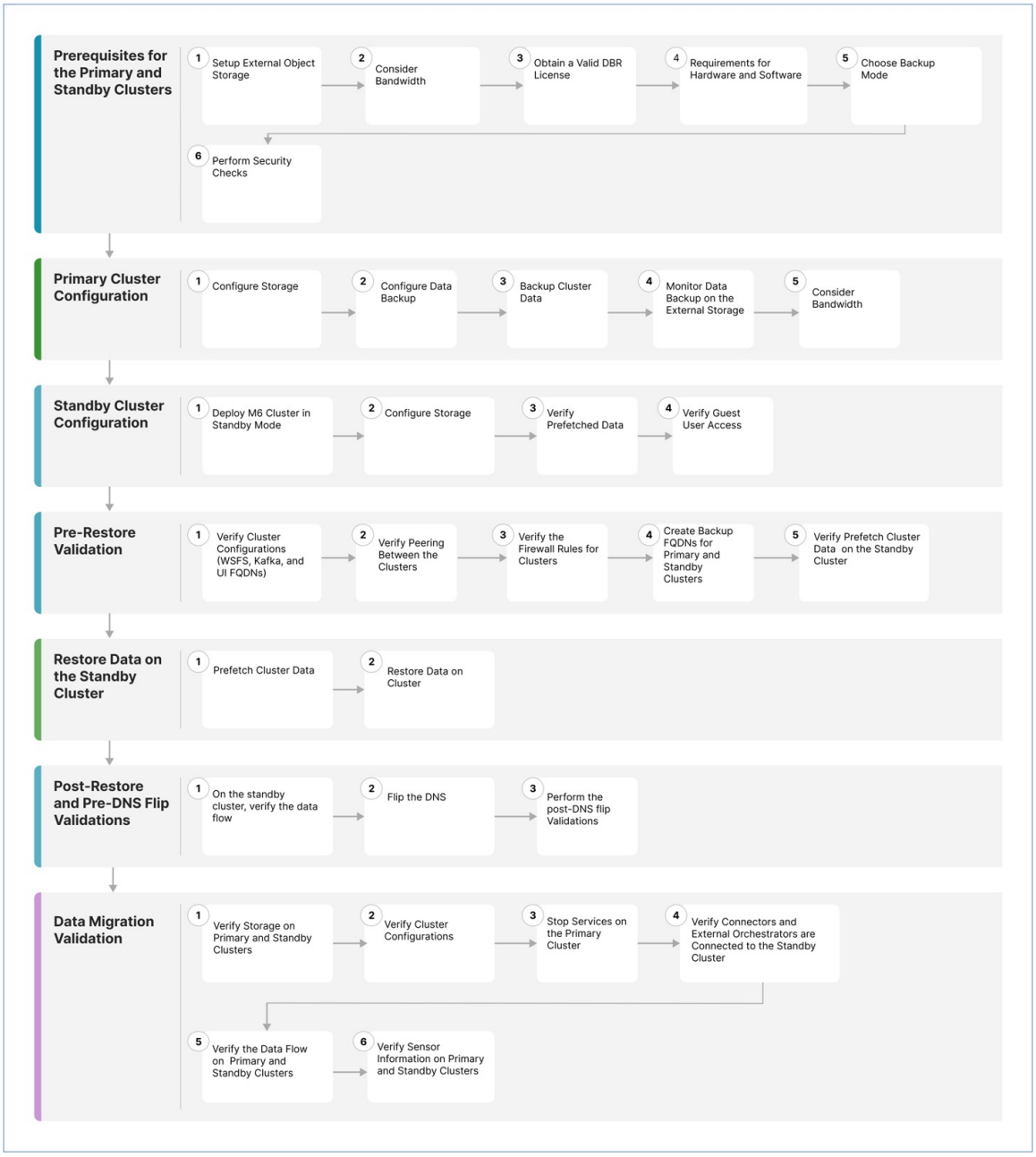
リーンバックアップモードまたは完全バックアップモードの詳細については、『Cisco Secure Workload ユーザーガイド』の「Data Backup and Restore (DBR)」の項を参照してください。

（注） このガイドでは、プライマリクラスタは M4 または M5 ですが、M6 はスタンバイクラスタとして参照されています。

エンドツーエンドの移行ワークフロー

Cisco Secure Workload では、クラスタ間の移行は複雑なプロセスです。スムーズな移行を確保するには、プライマリクラスタからスタンバイクラスタにデータを移行するために必要な手順の概要を示すエンドツーエンドのワークフローに従います。移行アクティビティを最大化するには、各手順を順番に実行することが重要です。

図 *9*: 移行の準備



1	プライマリクラスタとスタンバイクラスタの前提条件	プライマリクラスタとスタンバイクラスタの前提条件には、いくつかの手順と考慮事項が含まれています。
2	プライマリクラスタ構成（22 ページ）	プライマリクラスタ構成には、ストレージ、データバックアップ、クラスタデータのバックアップ、帯域幅、および WAN リンク管理の設定が含まれます。
3	スタンバイクラスタ構成	スタンバイクラスタの設定には、スタンバイモードでのスタンバイクラスタの展開、保管場所の設定、およびプリフェッチされたデータの確認が含まれます。
4	データ移行の検証	復元プロセスを開始する前に、スタンバイデータストレージ構成、プライマリとスタンバイのクラスタ構成、クラスタ間のピアリングを確認し、両方のクラスタのファイアウォールルールが同一であるか確認します。
5	スタンバイクラスタのクラスタデータ	スタンバイクラスタでデータを復元して、クラスタデータをプリフェッチし、クラスタデータを復元します。
6	復元後および DNS 反転前の検証	スタンバイクラスタでデータを復元したら、包括的な検証プロセスを実行します。このプロセスには、インベントリとラベルの確認、パイプラインのアクティブ化、サービスに関する緑色のステータスの検証、範囲ツリーの永続化、フローカウントがプライマリクラスタと一致することの確認が含まれます。
7	復元前の検証	スクリプトを使用して、復元プロセスの完了後にプライマリクラスタとスタンバイクラスタの両方に着信するフローデータを検証できます。

クラスタ間の移行の準備

Cisco Secure Workload のプライマリクラスタからスタンバイクラスタにデータを移行する場合は、Data Backup and Restore アプローチを使用することを推奨します。このアプローチには、プライマリクラスタから S3 互換ストレージへのデータのコピー、そのストレージからスタンバイクラスタへのデータの復元が含まれます。特定の移行要件に応じて、リーンモードまたは完全モードのバックアップを選択できます。

リーンモードまたは完全モードバックのアップの詳細については、『Cisco Secure Workload ユーザーガイド』の「Data Backup and Restore (DBR)」の項を参照してください。

プライマリクラスタとスタンバイクラスタの前提条件

ご使用の環境が次のハードウェアおよびソフトウェア要件を満たしていることを確認します。

外部オブジェクトストレージの設定

- S3v4 標準に準拠した外部オブジェクトストレージが使用可能であることを確認します。
- 39RU および 8RU クラスタの場合、完全バックアップの場合は 50TB のストレージ容量を推奨しますが、リーンバックアップの場合は最小の 1TB で十分です。詳細については、「Object Store Requirements」を参照してください。
- プライマリクラスタとスタンバイクラスタの組み合わせのリスト。

表 *3:* クラスタ *SKU*

プライマリクラスタ SKU	スタンバイクラスタ SKU
8RU-PROD	
8RU-M4 8RU-M5	8RU-M6
39RU-GEN1	
39RU-M4 39RU-M5	39RU-M6

有効な Data Backup Restore ライセンスの取得

有効な Data Backup Restore（DBR）ライセンスを取得するには、Cisco TAC にケースを送信します。ソフトウェア利用資格は、プライマリクラスタにのみ必要で、スタンバイクラスタには必要ありません。

帯域幅の考慮事項

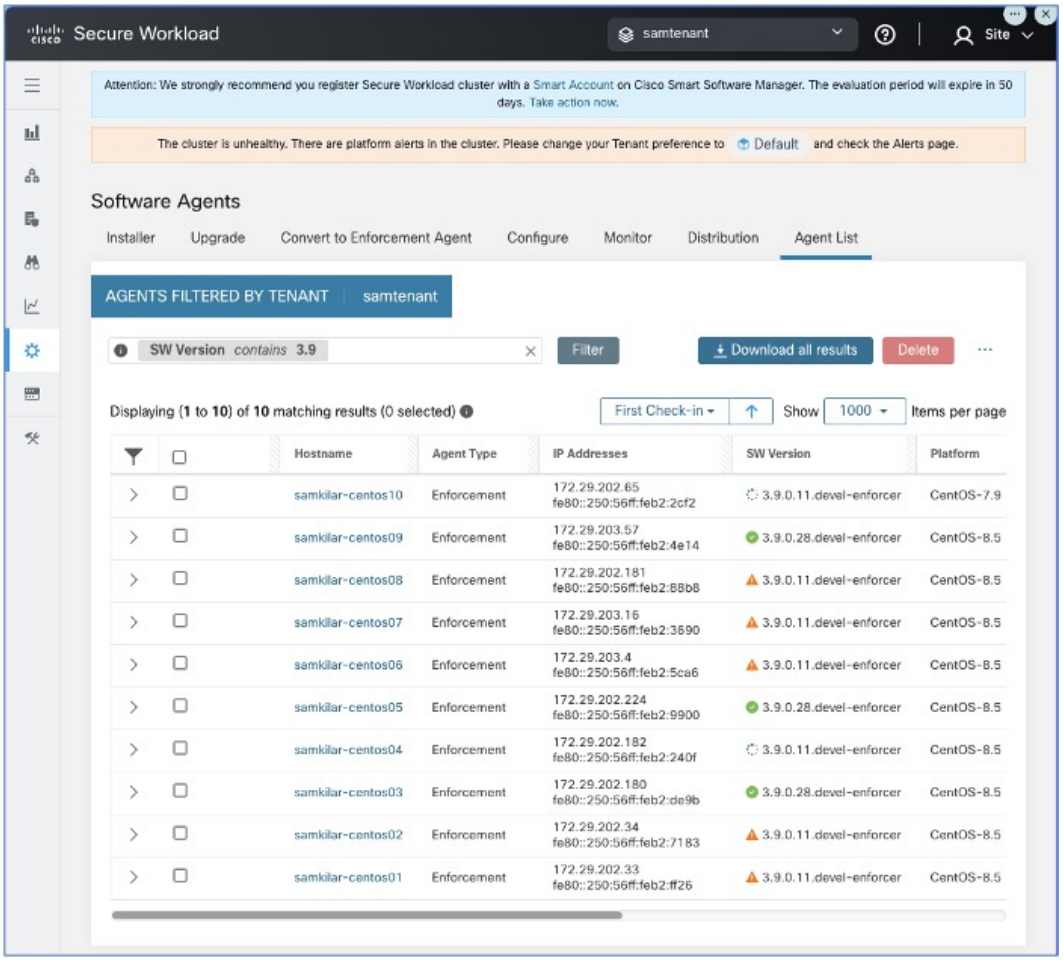
- プライマリクラスタから S3 サーバーにデータをバックアップし、スタンバイクラスタにデータを復元する場合は、10Mbps 以上の帯域幅を推奨します。
- オブジェクトストアがプライマリクラスタとスタンバイクラスタの両方に近い場所にあることを確認します。

ハードウェアおよびソフトウェアの要件

- 移行を開始する前に、プライマリクラスタとスタンバイクラスタが同じフォームファクタ（8RU または 39RU）であることを確認します。データ移行は、同じフォームファクタのクラスタ間でのみ実行されます。詳細については、『Cisco Secure Workload M6 クラスタ導入ガイド』を参照してください。

- プライマリクラスタを最新バージョンの Cisco Secure Workload 3.9 にアップグレードし、スタンバイクラスタに同じバージョンを展開していることを確認します。プライマリクラスタとスタンバイクラスタのソフトウェアエージェントのバージョンは同じである必要があります。詳細については、「Cisco Secure Workload リリース 3.9.1.1 へのアップグレード」を参照してください。
- Data Backup and Restore 機能を使用するには、ソフトウェアエージェントのバージョンが 3.3 以降であることを確認します。エージェントのバージョンを確認するには、ナビゲーションウィンドウで、**[管理（Manage）]** > **[ワークロード（Workloads）]** > **[エージェント（Agents）]** > **[エージェントリスト（Agent List）]**の順に選択します。

図 *10* : エージェントリスト



- Kafka と WSS の完全修飾ドメイン名（FQDN）の要件を確認して検証します。移行中のクラスタ間の通信を維持するために、Kafka 構成が FQDN 標準に準拠していることを確認します。詳細については、「Kafka FQDN Requirements」を参照してください。

バックアップモード

- **完全バックアップモード**
  - 構成、データ、サーバー設定、および履歴テレメトリを含む包括的なバックアップオプションを使用するには、[完全バックアップ（Full Backup）] モードを選択します。このモードでは、プライマリクラスタがスタンバイクラスタに完全に複製されます。完全バックアップモードでは、バックアップするフローデータの量に応じて、必要なストレージ容量は最大 50TB です。

- **リーンモード**
  - 構成データをバックアップするには、リーンモードを選択します。このモードは、履歴テレメトリなしでプライマリクラスタからスタンバイクラスタに重要な設定のみ複製されます。最小ストレージ要件は1TB です。データの冗長性が主な関心事ではない場合、移行は合理化されます。

（注） クラスタ間でデータを転送する場合、完全バックアップでは、リーンバックアップよりも多くの時間とストレージ容量が必要です。基本的な構成設定のみを含む迅速な移行の場合は、リーンモードを使用することを推奨します。プライマリクラスタの元のデータには引き続きアクセスでき、必要に応じて、データは完全バックアップモードを使用してスタンバイクラスタに転送されます。

セキュリティチェック

移行中にプライマリクラスタに関連するアラートや警告を確認するには、次の手順を実行します。

- ナビゲーションウィンドウで、**[概要（Overview）]**>**[セキュリティダッシュボード（Security Dashboard）]**の順に選択します。[セキュリティダッシュボード（Security Dashboard）] ページで、プライマリクラスタに関連するアラートや警告を確認します。

  詳細については、『Cisco Secure Workload ユーザーガイド』の「Cluster Status」の項を参照してください。

- ナビゲーションウィンドウで、**[プラットフォーム（Platform）]**>**[クラスタ構成（Cluster Configuration）]**の順に選択し、このページで、WSS および Kafka のプライマリクラスタの FQDN 構成がスタンバイクラスタ構成と一致することを確認します。

プライマリクラスタ構成

ステップ 1 ストレージの設定

1. 完全バックアップモード用に 50TB、リーンバックアップモード用に 1TB のストレージを設定するには、S3v4 準拠のオブジェクトストアに新しいバケットを作成します。一般的に使用される S3v4 ストレージデバイスは次のとおりです。
   - Amazon S3
   - Google Cloud Storage
   - Microsoft Azure Blob Storage
   - MinIO オブジェクトストレージ
2. 次の詳細を入力します。
   - ストレージの名前
   - ストレージに設定されている S3 準拠のバケット名
   - S3 準拠のストレージエンドポイントの URL
   - （特定のストレージのオプション）S3 準拠のストレージのリージョン。
   - ストレージのアクセスキー
   - ストレージの秘密鍵

   後で参照できるように、これらすべての詳細を正確に記録してください。
3. バケットのクラスタへの排他的な読み取り/書き込みアクセス権を付与します。
4. プライマリクラスタのナビゲーションウィンドウで、**[プラットフォーム（Platform）]** > **[データバックアップ（Data Backup）]**の順に選択します。**ステップ b** で収集した情報を入力します。
5. （任意）バックアップされたデータのマルチパートアップロードを使用する場合は、[マルチパートアップロードの使用（Use Multipart Upload）] を有効にします。
6. （オプション）必要に応じて、HTTP プロキシを有効にできます。
7. （任意）ストレージサーバーを認証するには、次の点を確認します。
   - CA 証明書の詳細の可用性。
   - [サーバーCA証明書の使用（Use Server CA Certificate）] の有効化。
8. [テスト（Test）] ボタンをクリックして確定します。

ステップ 2　データバックアップの設定

プライマリクラスタでデータバックアップを設定するには、『Cisco Secure Workload ユーザーガイド』の「Configure Data Backup」の項に記載されている手順を実行します。

ステップ 3　クラスタデータのバックアップ

プライマリクラスタでデータバックアップを設定すると、継続モードを無効にしていない限り、クラスタデータのバックアップは日中のスケジュールされた時刻に自動的にトリガーされます。プライマリクラス

タでは引き続きデータがバックアップされ、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。詳細については、『Cisco Secure Workload ユーザーガイド』の「Backup Status」を参照してください。

ステップ 4　外部ストレージでのデータバックアップのモニター

レプリケーションプロセスをモニターして、すべてのデータが正確に転送されていることを確認し、このフェーズで発生する可能性のある問題に迅速に対処します。

ステップ 5　帯域幅の推奨事項

クラスタと S3 互換ストレージ間で Backup and Restore システムを設定する場合は、それらを接続するリンクの帯域幅を考慮することが重要です。プライマリクラスタとスタンバイクラスタをストレージに接続して、データのバックアップと復元を容易にします。各移行では 1 秒ごとに特定の量の帯域幅が消費されるため、リンクの潜在的な飽和を評価し、適宜計画する必要があります。

ステップ 6　WAN リンク管理

WAN リンクが飽和状態になる可能性を考慮することが重要で、特に、移行トラフィックが多いピークの営業時間を考慮する必要があります。必要に応じて、中断を回避し、指定された移行期間内で移行を実行するようにデータ転送をスケジュールします。

スタンバイクラスタ構成

ステップ 1　バックアップされたデータを復元するには、スタンバイモードでスタンバイクラスタを展開します。詳細については、『Cisco Secure Workload ユーザーガイド』の「Deploying Cluster in Standby Mode」を参照してください。

1. スタンバイクラスタで、**[プラットフォーム（Platform）]** > **[データバックアップ（Data Backup）]**の順に選択します。
2. 次の詳細事項を入力します。
   - ストレージの名前
   - ストレージで設定されている S3 準拠のバケット名
   - S3 準拠のストレージエンドポイントの URL
   - （任意）特定のストレージに対する S3 準拠のストレージのリージョン
   - ストレージのアクセスキー
   - ストレージの秘密鍵
3. （オプション）必要に応じて、HTTP プロキシを有効にできます。
4. （任意）ストレージサーバーを認証するには、次の点を確認します。

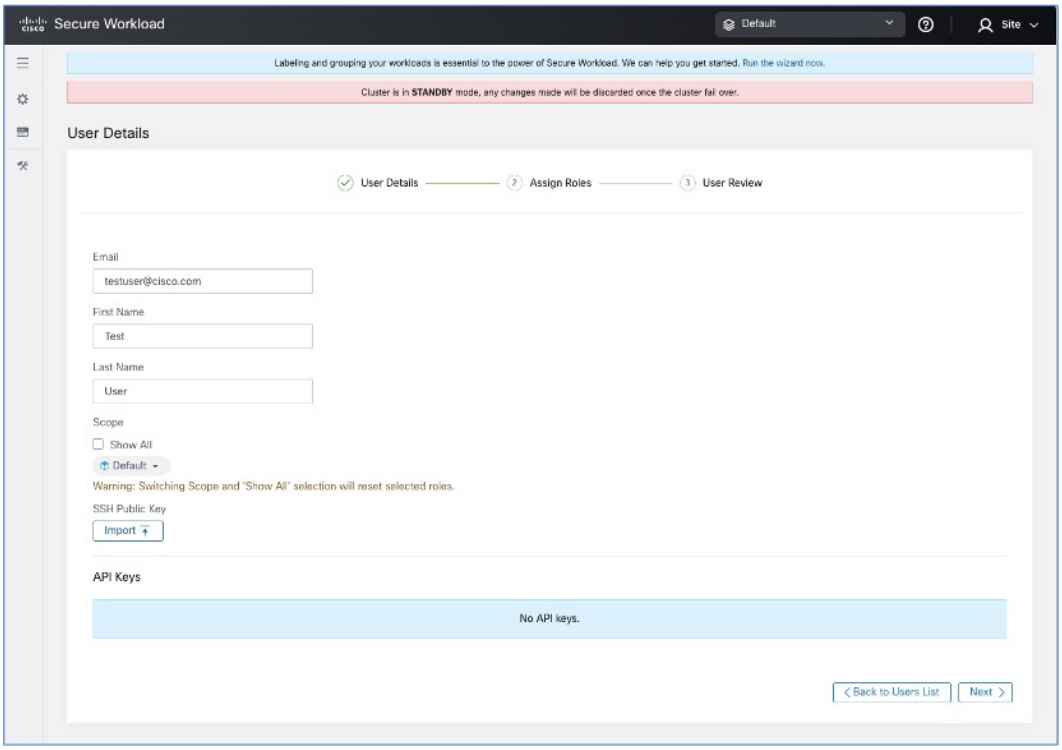
- CA 証明書の詳細の可用性。
- [サーバーCA証明書の使用（Use Server CA Certificate）] の有効化。

5. [テスト（Test）]ボタンをクリックし、S3テストが完了したことを確認します。エラーがある場合は、ストレージのアクセシビリティ、およびクラスタの権限を確認します。
6. テストが完了したら、[次へ（Next）] をクリックします。

バックアップデータが正しくプリフェッチされていることを確認し、バックアップのエラーをモニターします。詳細については、『Cisco Secure Workload ユーザーガイド』の「Data Restore」を参照してください。

ステップ 2 ta_guestユーザーがスタンバイクラスタにアクセスできるか確認するには、ユーザーの作成または編集時にSSHキーを追加します。ユーザーを追加または変更するには、ナビゲーションウィンドウで、**[ユーザーアクセス（User Access）]** > **[ユーザー（User）]**の順に選択します。

図 *11*：スタンバイクラスタのユーザーの詳細



復元前の検証

復元プロセスを開始する前に、次のデータがプライマリクラスタからスタンバイクラスタにプリフェッチされていることを確認します。

ステップ 1 スタンバイデータストレージ構成がプライマリデータストレージ構成と一致していることを確認するには、プライマリクラスタで[データバックアップ（Data Backup）]に移動し、スタンバイクラスタで[データ復元（Data Restore）]に移動します。両方のクラスタの WSFS、Kafka、および UI FQDN のクラスタ構成が同一であることを確認します。

ステップ 2 スタンバイクラスタのナビゲーションウィンドウで、**[プラットフォーム（Platform）]** > **[クラスタ構成（Cluster Configuration）]**の順に選択します。[プライマリクラスタサイト名（Primary Cluster Sitename）]フィールドに正しいプライマリクラスタ名が含まれていることを確認します。

ステップ 3 スタンバイクラスタと同じ方法で、すべてのエージェント、コネクタ、および外部オーケストレータからプライマリクラスタにアクセスできることを確認します。認証および認可の目的で LDAP または SSO を使用している場合は、LDAP および SSO に関連付けられたエンドポイントにアクセスできることを確認します。

ステップ 4 エージェントがプライマリクラスタと同じ方法でスタンバイクラスタと通信できるようにするには、両方のクラスタのファイアウォールルールが同じであることを確認します。対象には、ワークロード上のファイアウォールと、ワークロードとクラスタ間のネットワーク上のファイアウォールが含まれます。

ステップ 5 プライマリクラスタ UI への中断のないアクセスを確保するために、プライマリクラスタとスタンバイクラスタの両方にバックアップの完全修飾ドメイン名（FQDN）を作成することを推奨します。たとえば、プライマリクラスタのデータを復元し、DNS を反転すると、FQDN「cluster1.enterprise.com」と「cluster2.enterprise.com」の両方がスタンバイクラスタを指すようになります。その結果、cluster1.enterprise.com の GUI にアクセスできなくなりますが、プライマリクラスタと同じ IP アドレスを指す DNS サーバー「cluster1-backup.enterprise.com」に FQDN を作成することで、引き続き GUI にアクセスできます。データを復元して DNS を反転すると、「cluster1-backup.enterprise.com」と「cluster2-backup.enterprise.com」の両方がスタンバイクラスタを指し、「cluster1-backup.enterprise.com」は引き続きプライマリクラスタを指すようになります。

ステップ 6 スタンバイクラスタデータのプリフェッチが正しく機能していることを確認します。プリフェッチされたデータがプライマリクラスタのデータと一致することを検証するには、ナビゲーションウィンドウで、**[プラットフォーム（Platform）]** > **[データ復元（Data Restore）]**の順に選択します。

ステップ 7 ナビゲーションウィンドウで、**[トラブルシュート（Troubleshoot）]** > **[クラスタステータス（Cluster Status）]**の順に選択し、プライマリクラスタとスタンバイクラスタの両方の正常性ステータスを確認します。詳細については、『Cisco Secure Workload ユーザーガイド』の「Cluster Status」を参照してください。

ステップ 8 ナビゲーションウィンドウで、**[トラブルシュート（Troubleshoot）]** > **[スナップショット（Snapshot）]**の順に選択し、プライマリクラスタのスナップショットを作成します。このスナップショットは、移行中に発生した問題のトラブルシューティングに役立ちます。

スタンバイクラスタでプリフェッチされたバックアップデータが最新であることを確認します。

ステップ 9 ユーザー「ta_guest」がスタンバイクラスタにアクセスできるか確認します。このユーザーは、移行関連の問題が発生した場合に、トラブルシューティングの目的でスタンバイクラスタへのアクセスが許可されます。「ta_guest」ユーザーの詳細については、『Cisco Secure Workload ユーザーガイド』の「Users」を参照してください。

ステップ 10 クラスタ構成の検証を実行して、クラスタ構成情報を primary-config-data.txt に保存します。詳細については、『Cisco Secure Workload ユーザーガイド』の 「Cluster Configuration Validation」を参照してください。

ステップ 11 プライマリクラスタのコネクタおよび外部オーケストレータ機能からのデータを primary-ext-orch-data.txt に保存します。詳細については、『Cisco Secure Workload ユーザーガイド』の「Connector and External Orchestrator Functional Validation」を参照してください。

ステップ 12 プライマリクラスタでデータフローの検証ワークフローを実行して得たデータを、primary-flow-data.txt という名前のファイルに保存します。詳細については、『Cisco Secure Workload ユーザーガイド』の「Data Flow Validation」を参照してください。

スタンバイクラスタのクラスタデータ

クラスタデータは、次の 2 つのフェーズで復元できます。

- **必須フェーズ**：サービスの再起動に必要なデータを復元して、クラスタを使用できるようにします。必須フェーズにかかる時間は、構成、インストールされているソフトウェアエージェントの数、およびフローメタデータによって異なります。必須フェーズでは、構成の規模に応じて、GUI に 1 時間アクセスできないため、必須フェーズ中に TA ゲストキーをサポートに使用できることを確認してください。
- **遅延フェーズ**：バックグラウンドでクラスタのフローデータを復元している間、クラスタを引き続き使用して、GUI にアクセスできます。このフェーズ中、クラスタはデータパイプライン、フロー検索、およびエージェントからクラスタに送信される新しいデータの通常の機能で動作します。

詳細については、『Cisco Secure Workload ユーザーガイド』の「Cluster Restore」を参照してください。

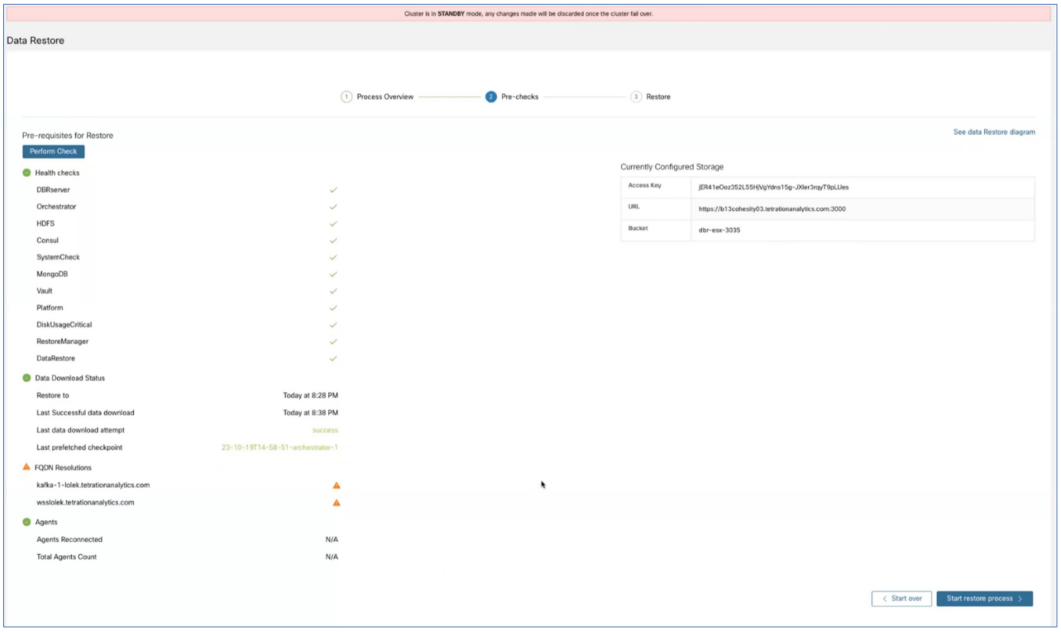
スタンバイクラスタでデータを復元するには、次の手順を実行します。

ストレージ構成を確認します。

ステップ 1 スタンバイクラスタのナビゲーションウィンドウで、**[プラットフォーム（Platform）]**>**[データ復元（Data Restore）]**の順に選択し、ストレージ構成が成功したことを確認します。ストレージを再設定することもできます。

ステップ 2 [チェックの実行（Perform Check）] をクリックして、クラスタの正常性を確認します。

図 *12 :* データ復元の前提条件

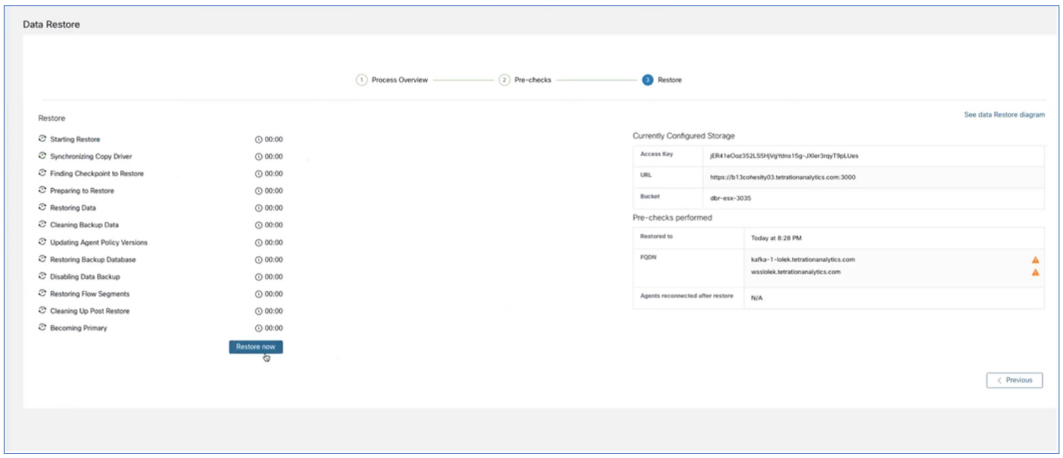


（注）
- 復元中に警告メッセージが表示された場合でも、復元プロセスを続行できます。
- ただし、エラーが発生した場合、[復元プロセスの開始（Start Restore Process）] ボタンは自動的に無効になります。エラーを修正してから、ステータスを確認することを推奨します。サービスの正常性ステータスを表示するには、ナビゲーションウィンドウで、**[トラブルシューティング（Troubleshooting）] > [サービスステータス（Service Status）]**の順に選択します。

ステップ 3 プライマリクラスタのバックアップスケジュールを停止する進行中のバックアップがないことを確認します。バックアップが進行中の場合は、そのバックアップが完了するのを待ってからスケジュールを非アクティブにします。

ステップ 4 復元プロセスを開始するには、[復元プロセスの開始（Start Restore Process）] をクリックします。次の図に示されているように、GUI で復元プロセスの段階を確認できます。

図 *13* : データ復元プロセスの段階



ステップ 5 [復元（Restore）] ページの下部にある [今すぐ復元（Restore Now）] ボタンをクリックします。

ステップ 6 [データ復元の確認（Confirmation Data Restore）] ウィンドウで、[確認（Confirm）] ボタンをクリックします。確認後、データ復元プロセスが順番に実行され、プロセスの最後に、スタンバイクラスタがプライマリになります。データ復元プロセスをモニターして、期待どおりに進行していることを確認します。

（注） **復元**の**準備**段階と**復元後のクリーンアップ**段階では、GUI にアクセスできないため、復元プロセスを開始する前に、必要なすべてのアクションが完了していることを確認してください。

クラスタデータのプリフェッチ

クラスタデータの復元を開始する前に、クラスタでデータをプリフェッチする必要があります。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チェックポイントデータをプリフェッチします。データをプリフェッチしてデータのステータスを確認するには、『Cisco Secure Workload ユーザーガイド』の「Prefetch Cluster Data」の項に記載されている手順を実行します。

スタンバイクラスタのクラスタデータ

クラスタデータは、次の 2 つのフェーズで復元できます。

- **必須フェーズ**：サービスの再起動に必要なデータを復元して、クラスタを使用できるようにします。必須フェーズにかかる時間は、構成、インストールされているソフトウェアエージェントの数、およびフローメタデータによって異なります。必須フェーズでは、構成の規模に応じて、GUI に 1 時間アクセスできないため、必須フェーズ中に TA ゲストキーをサポートに使用できることを確認してください。
- **遅延フェーズ**：バックグラウンドでクラスタのフローデータを復元している間、クラスタを引き続き使用して、GUIにアクセスできます。このフェーズ中、クラスタはデータパイ

プライン、フロー検索、およびエージェントからクラスタに送信される新しいデータの通常の機能で動作します。

詳細については、『Cisco Secure Workload ユーザーガイド』の「Cluster Restore」を参照してください。

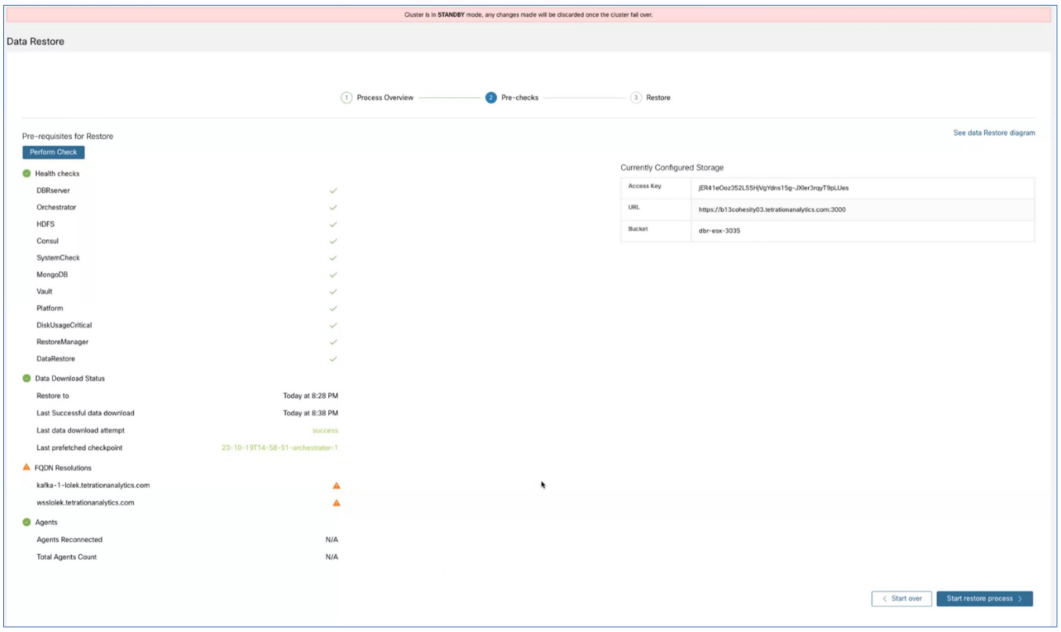
スタンバイクラスタでデータを復元するには、次の手順を実行します。

ストレージ構成を確認します。

ステップ 1 スタンバイクラスタのナビゲーションウィンドウで、**[プラットフォーム（Platform）]>[データ復元（Data Restore）]**の順に選択し、ストレージ構成が成功したことを確認します。ストレージを再設定することもできます。

ステップ 2 [チェックの実行（Perform Check）] をクリックして、クラスタの正常性を確認します。

図 *14*：データ復元の前提条件

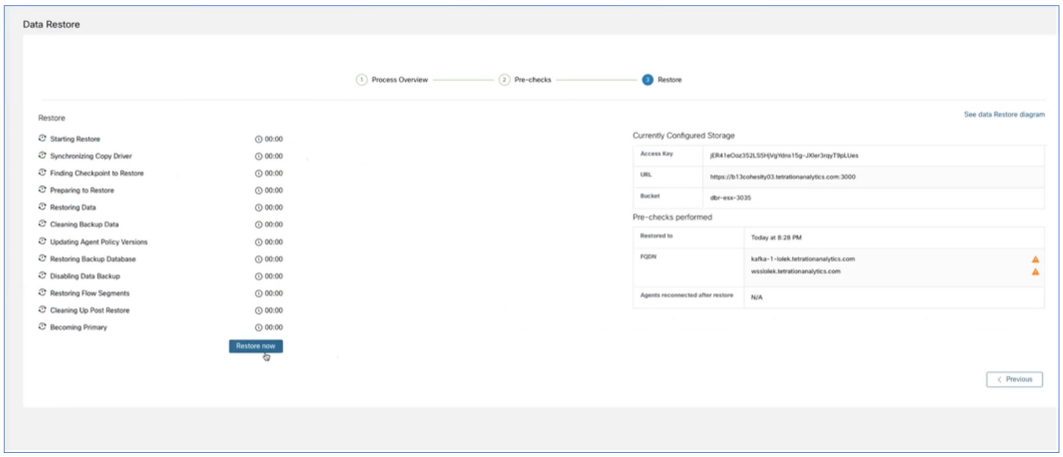


（注）
- 復元中に警告メッセージが表示された場合でも、復元プロセスを続行できます。
- ただし、エラーが発生した場合、[復元プロセスの開始（Start Restore Process）] ボタンは自動的に無効になります。エラーを修正してから、ステータスを確認することを推奨します。サービスの正常性ステータスを表示するには、ナビゲーションウィンドウで、**[トラブルシューティング（Troubleshooting）] > [サービスステータス（Service Status）]**の順に選択します。

ステップ 3 プライマリクラスタのバックアップスケジュールを停止する進行中のバックアップがないことを確認します。バックアップが進行中の場合は、そのバックアップが完了するのを待ってからスケジュールを非アクティブにします。

ステップ 4 復元プロセスを開始するには、[復元プロセスの開始（Start Restore Process）] をクリックします。次の図に示されているように、GUI で復元プロセスの段階を確認できます。

図 *15*：データ復元プロセスの段階



ステップ 5 [復元（Restore）] ページの下部にある [今すぐ復元（Restore Now）] ボタンをクリックします。

ステップ 6 [データ復元の確認（Confirmation Data Restore）] ウィンドウで、[確認（Confirm）] ボタンをクリックします。確認後、データ復元プロセスが順番に実行され、プロセスの最後に、スタンバイクラスタがプライマリになります。データ復元プロセスをモニターして、期待どおりに進行していることを確認します。

（注） **復元**の**準備**段階と**復元後のクリーンアップ**段階では、GUI にアクセスできないため、復元プロセスを開始する前に、必要なすべてのアクションが完了していることを確認してください。

復元後および DNS 反転前の検証

スタンバイクラスタインターフェイスがダウンしたら、クラスタへの接続を試行します。データ復元プロセスが完了したら、GUI にログインできます。

（注） データ復元プロセスが完了すると、複数のサービスが約 1 時間 [非正常（UNHEALTHY）] 状態になります。すべてのサービスが各データにアクセスできるようになると、ステータスが [正常（HEALTHY）] に変わります。

スタンバイクラスタのデータを復元したら、次の点を確認します。

ステップ 1 ライセンスのコピーを準備し、以前のバージョンと比較します。

ステップ 2 すべてのインベントリと注釈の可用性を確認し、[クラスタ構成（Cluster Configuration）] ページとサイト情報で IP アドレスを確認します。

ステップ 3 パイプラインは、データが取り込まれるまで、最初は [非正常（UNHEALTHY）] と表示されます。すべてのパイプラインがアクティブであることを確認します。

ステップ 4 すべてのサービスで緑色のステータスが表示されていることを確認します。一部のサービスのステータスは緑色になるまで、最大1時間かかる場合があります。パイプラインなどのフローデータを必要とするサービスは、データ復元プロセスが完了するまで待機するため、最も時間がかかる可能性があります。現在、データバックアップサービスに関する問題は無視しても問題ありません。

ステップ 5 重要なのは、クラスタ証明書が WSS と同じ CA に存在することを確認することです。確認するには、ナビゲーションウィンドウで、**[プラットフォーム（Platform）] > [クラスタ構成（Cluster Configuration）]**の順に選択します。センサー CA 証明書をダウンロードし、クラスタ証明書が WSS と同じ CA に存在しているか確認します。

ステップ 6 トラブルシューティングのためにスタンバイクラスタのスナップショットを取得して、範囲ツリーが保持されていることを確認します。

ステップ 7 **クラスタ構成の検証**を実行して、次の手順を実行します。

- スタンバイクラスタ構成情報を確認して確定します。
- プライマリクラスタとスタンバイクラスタの両方の構成を比較検証し、スタンバイクラスタのユーザーのリストを除き、構成が一致していることを確認します。

（注） スタンバイリストにはプライマリユーザーとスタンバイユーザーの両方が含まれるため、スタンバイ上のユーザーのリストはプライマリリストよりも多くなります。

ステップ 8 フローカウントがプライマリクラスタとスタンバイクラスタの間で一致していることを確認します。フローデータが大きい場合、スタンバイクラスタでの復元に時間がかかる場合があります。詳細については、「フロー入力データの検証方法」を参照してください。その後、スタンバイクラスタのデータをプライマリクラスタのデータと比較します。

（注） スタンバイクラスタには、次のようないくつかの依存関係があるため、プライマリクラスタよりもフローが少ない場合があります。

- プライマリクラスタの最後のバックアップのタイムスタンプ
- スタンバイクラスタで復元されたデータのタイムスタンプ
- エージェントからプライマリクラスタに送信されたデータ

（最後のバックアップ後に）エージェントからプライマリクラスタに送信されたデータは、転送中に失われるため、スタンバイクラスタには復元されないことに注意してください。

DNS の反転

DNS 反転は、プライマリクラスタの FQDN がスタンバイクラスタ VIP を指すように DNS サーバーレコードを変更するアクションです。このアクションにより、エージェント、外部オーケストレータ、およびコネクタがプライマリクラスタではなくスタンバイクラスタに接続できるようになります。

（注） ワークロードとクラスタを処理するように設定されている DNS サーバーにおいて、クラスタの外部で DNS 反転アクションを実行してください。

DNS を反転するには、次の手順を実行します。

ステップ 1 プライマリクラスタのサービスの停止

- エージェント、コネクタ、および外部オーケストレータと連携するプライマリクラスタ内のすべてのサービスを停止してから、スタンバイクラスタを指すようにドメインネームシステム（DNS）エントリを変更する必要があります。そうすることで、各コンポーネントはプライマリクラスタへの接続を失い、接続の再確立を試みます。
- DNS エントリを反転すると、エージェント、コネクタ、および外部オーケストレータは自動的にスタンバイクラスタに再接続します。プライマリクラスタのサービスを停止する段階的な手順については、「サービス停止ワークフロー」の項を参照してください。

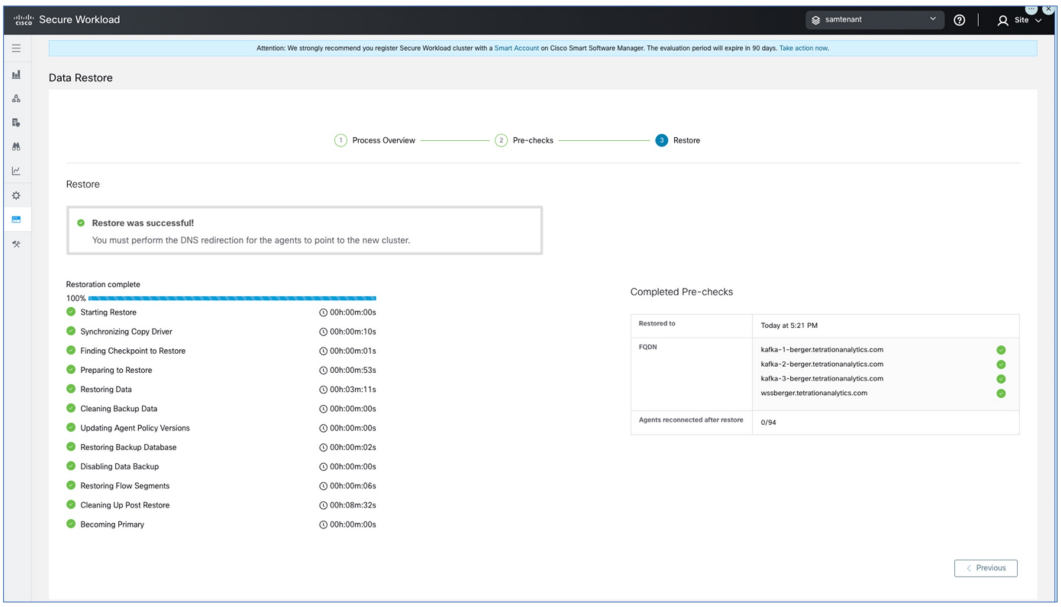
ステップ 2 FQDN の反転

次の FQDN を反転し、各 FQDN に関連付けられている IP アドレスがスタンバイクラスタに関連付けられている VIP を指していることを確認します。

- WSS FQDN
- ナビゲーションウィンドウで、**[プラットフォーム（Platform）] > [クラスタ構成（Cluster Configuration）]**の順に選択し、Kafka FQDN を確認します。最大 3 つの Kafka FQDN が存在する可能性があります。

クラスタ WSS と Kafka の DNS を反転すると、クラスタの [データ復元（Data Restore）] ページの FQDN チェックが緑色に変わります。

図 *16* : データ復元成功



DNS 反転後の検証

スタンバイクラスタの DNS を反転したら、次のシナリオを確認します。

ステップ 1 プライマリクラスタとスタンバイクラスタの両方のスナップショットを作成します。

ステップ 2 プロキシの有無にかかわらず、エージェントのすべてのバージョンが再接続されていることを確認します。

- スタンバイクラスタのデータを復元するには、ナビゲーションウィンドウで、**[プラットフォーム（Platform）] > [データ復元（Data Restore）]**の順に選択します。
- エージェントを再接続したら、プライマリクラスタと同じ数のエージェントがスタンバイクラスタに再接続されていることを確認します。エージェントの再接続時刻は異なる可能性があるため、検証には時間がかかる場合があります。プライマリクラスタのアクティブなエージェントの数をモニターし、同じ数のエージェントがスタンバイクラスタで再接続されていることを確認します。これは、[データ復元（Data Restore）] ページの [復元されたエージェント（Agents Restored）] データから確認できます。

  エージェントの詳細については、「センサーの検証」を参照してください。

ステップ 3 コネクタと外部オーケストレータが接続されていることを確認します。コネクタが接続されていない場合は、スタンバイクラスタからコネクタへのルートがあり、コネクタの接続を許可するようにファイアウォールルールが設定されていることを確認します。ナビゲーションウィンドウで、**[ワークロード（Workloads）]> [コネクタ（Connectors）]**の順に選択し、ログを確認して障害を特定します。段階的な検証手順については、「コネクタと外部オーケストレータ機能の検証」を参照してください。

ステップ 4 すべてのアラート通知、電子メール、および syslog データは転送できませんが、アラートはすべて再発行されます。

ステップ 5 パイプラインが適切に機能していることを確認し、必要に応じてプライマリクラスタの GUI FQDN をスタンバイクラスタに移行します。

ステップ 6 目的の結果を得るには、プライマリクラスタのクラスタ GUI FQDN を変更し、スタンバイクラスタの IP アドレスに置き換える必要があります。

この手順を完了後、ブラウザまたはクラスタ API を使用してプライマリクラスタの FQDN にアクセスすると、スタンバイクラスタにリダイレクトされます。

データ移行の検証

ここでは、プライマリクラスタからスタンバイクラスタへのデータ移行が成功したことを確認する手順の概要を示します。

ストレージの検証

プライマリクラスタとスタンバイクラスタでストレージを設定する前に、ストレージの検証を完了します。s3-test.py Python スクリプトを使用してストレージを検証します。このスクリプトには、Python 3 と、requirements.txt ファイルにリストされている特定のパッケージが必要です。

S3 ストレージ構成を検証するには、次の手順を実行します。

ステップ 1 s3-test.conf 構成ファイルにストレージの詳細を入力します。詳細には、ストレージ URL とポート番号、S3 アクセスキー、S3 秘密鍵、およびバケットの詳細が含まれます。

ステップ 2 次のオペレーティングシステムでスクリプトを実行します。

- **Linux および Mac の場合**：python s3-test.py
- **Windows の場合**：python s3-test.py

s3-test.py スクリプトは、バケットの検証、バケットからの読み取り/書き込み、およびバケットからのオブジェクトの一括削除を実行して、バケットへのアクセスをテストします。これらの基本テストにより、S3 互換ストレージ構成が正しいことを確認します。

スクリプトからは次の出力が生成されます。

図 *17* : 検証エラー

```
-> % python3 s3-test.py
Using Storage URL: https://b13cohesity03.tetrationanalytics.com:3000, Bucket: adtest-migration
Testing Write Objects...
Exception received: An error occurred (NoSuchBucket) when calling the PutObject operation: Unknown
Testing Read Objects One By One...
Exception received: An error occurred (NoSuchBucket) when calling the GetObject operation: Unknown
Testing Bulk Delete Objects...
Exception received: An error occurred (NoSuchBucket) when calling the DeleteObjects operation: Unknown


**********Test Results**********
Write Objects:  Fail
Read Objects:   Fail
Delete Objects: Fail
```

図 *18* : 検証成功

```
-> % python3 s3-test.py
Using Storage URL: https://b13cohesity03.tetrationanalytics.com:3000, Bucket: test-migration
Testing Write Objects...
Write Object Test Successful
Testing Read Objects One By One...
Read Object Test Successful
Testing Bulk Delete Objects...
Bulk Delete Objects Test Successful
Testing Read Objects One By One...
Read Object Test Successful


**********Test Results**********
Write Objects:  Success
Read Objects:   Success
Delete Objects: Success
```

図 *19* : ヘルプ画面

```
-> % python3 s3-test.py -h
usage: s3-test [-h] [-v] [-b]

Test S3 Configuration

options:
  -h, --help      show this help message and exit
  -v, --verbose   Print additional information
  -b, --botologs  Print S3 logs
```

クラスタ構成の検証

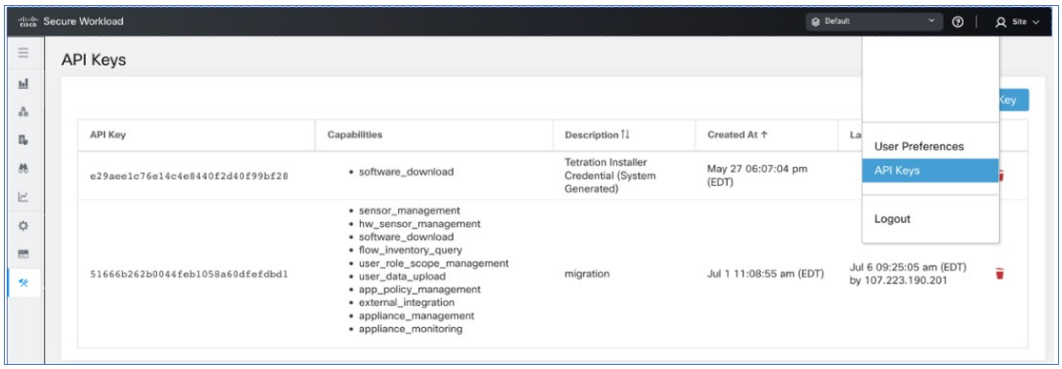
プライマリクラスタとスタンバイクラスタの両方から構成の概要をキャプチャします。移行プロセスが完了したら、両方のクラスタを比較して、構成が同一であることを確認します。次の点を確認してください。

- 復元プロセスの前にプライマリクラスタ構成をキャプチャします。
- 必須の復元フェーズが完了したら、スタンバイクラスタ構成をキャプチャします。この時点で、構成がスタンバイクラスタに移行されます。

ステップ 1 検証スクリプトでは OpenAPI が使用されます。API キーは、『Cisco Secure Workload ユーザーガイド』の「OpenAPI」の項に記載されている手順を使用して取得できます。

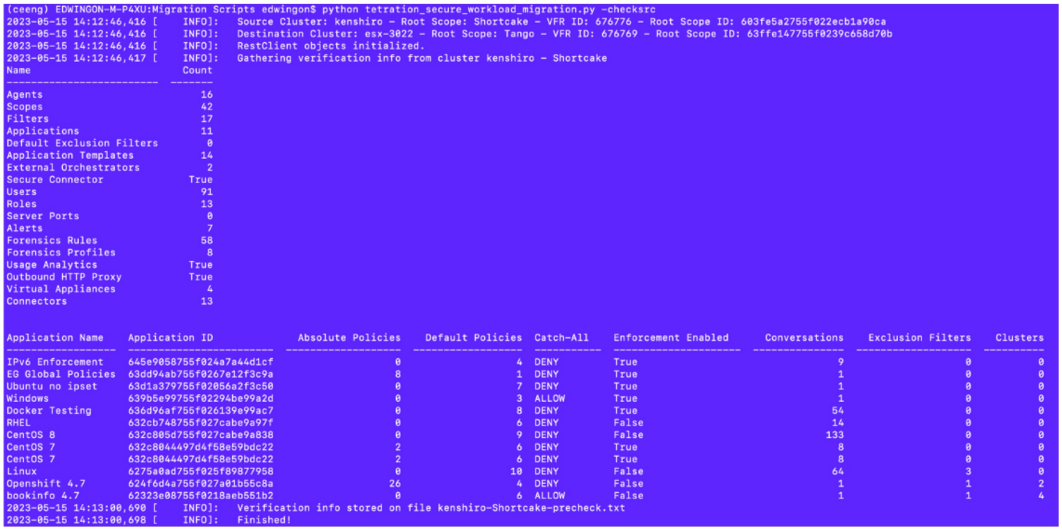
ステップ 2 すべての API キーの権限を選択し、API キーを含む JSON ファイルをダウンロードします。

図 *20 : API* キーを含む *JSON* ファイル



ステップ 3 プライマリクラスタでチェックリストスクリプトを実行して、検証する必要がある構成項目のリストを準備し、スクリプトの出力を記録します。このスクリプトでは、比較可能な両方のクラスタ構成に関する概要が表示されます。相違がある場合は、プライマリクラスタとスタンバイクラスタの完全な構成を比較して、不一致の有無を判断します。

図 *21 :* 出力例



```
(ceeng) EDWINGON-M-P4XU:Migration Scripts edwingon$ python tetration_secure_workload_migration.py -checksrc
2023-05-15 14:12:46,416 [    INFO]:   Source Cluster: kenshiro - Root Scope: Shortcake - VFR ID: 676776 - Root Scope ID: 603fe5a2755f022ecb1a90ca
2023-05-15 14:12:46,416 [    INFO]:   Destination Cluster: esx-3022 - Root Scope: Tango - VFR ID: 676769 - Root Scope ID: 63ffe147755f0239c658d70b
2023-05-15 14:12:46,416 [    INFO]:   RestClient objects initialized.
2023-05-15 14:12:46,417 [    INFO]:   Gathering verification info from cluster kenshiro - Shortcake
Name                      Count
------------------------  -------
Agents                       16
Scopes                       42
Filters                      17
Applications                 11
Default Exclusion Filters     0
Application Templates        14
External Orchestrators        2
Secure Connector           True
Users                        91
Roles                        13
Server Ports                  0
Alerts                        7
Forensics Rules              58
Forensics Profiles            8
Usage Analytics            True
Outbound HTTP Proxy        True
Virtual Appliances            4
Connectors                   13


Application Name    Application ID             Absolute Policies    Default Policies  Catch-All    Enforcement Enabled      Conversations    Exclusion Filters    Clusters
------------------  ------------------------  -------------------  ------------------  -----------  ---------------------  ---------------  -------------------  ----------
IPv6 Enforcement    645e9058755f024a7a44d1cf                    0                   4  DENY         True                                 9                    0           0
EG Global Policies  63dd94ab755f0267e12f3c9a                    8                   1  DENY         True                                 1                    0           0
Ubuntu no ipset     63d1a379755f02056a2f3c50                    0                   7  DENY         True                                 1                    0           0
Windows             639b5e99755f02294be99a2d                    0                   3  ALLOW        True                                 1                    0           0
Docker Testing      636d96af755f026139e99ac7                    0                   8  DENY         True                                54                    0           0
RHEL                632cb748755f027cabe9a97f                    0                   6  DENY         False                               14                    0           0
CentOS 8            632c805d755f027cabe9a838                    0                   9  DENY         False                              133                    0           0
CentOS 7            632c8044497d4f58e59bdc22                    2                   6  DENY         True                                 8                    0           0
CentOS 7            632c8044497d4f58e59bdc22                    2                   6  DENY         True                                 8                    0           0
Linux               6275a0ad755f025f89877958                    0                  10  DENY         False                               64                    3           0
Openshift 4.7       624f6d4a755f027a01b55c8a                   26                   4  DENY         False                                1                    1           2
bookinfo 4.7        62323e08755f0218aeb551b2                    0                   6  ALLOW        False                                1                    1           4
2023-05-15 14:13:00,690 [    INFO]:   Verification info stored on file kenshiro-Shortcake-precheck.txt
2023-05-15 14:13:00,698 [    INFO]:   Finished!
```

表 *4 :* 構成コンポーネントのリスト

構成コンポーネント	検証済み
手動ラベル	対応
範囲	対応
インベントリフィルタ	対応
エージェントプロファイル	対応
エージェントインテント	対応
ワークスペース	対応
ワークスペースポリシー（最新バージョン）	対応
ワークスペースクラスタ	対応
ロール	対応
ユーザー	対応
除外フィルタ：デフォルトおよびワークスペース	対応
外部オーケストレータ	対応
クライアントサーバーの構成（サーバーポート）	対応
フォレンジック：プロファイルとインテント	対応
ポリシーテンプレート（カスタムテンプレート）	×
収集ルール	対応

デフォルトの ADM 構成	対応
アラート設定/パブリッシャ	対応
セキュアコネクタ	対応
仮想アプライアンス（Ingest または Edge）	対応
コネクタ	対応
データタップの構成	対応

（注） すべての構成項目が適切に移行され、不一致がないことを確認するために、移行後にスタンバイクラスタに対してスクリプトが実行されます。

ステップ 4 すべてのクラスタ構成をダウンロードするモードでチェックリストスクリプトを実行します。download-src コマンドと download-dst コマンドを使用して、両方のクラスタから JSON 構成ファイルをダウンロードします。この構成が安全に保存されていることを確認します。

ステップ 5 データの復元プロセスが完了したら、スタンバイクラスタでステップ 2 ～ 7 を繰り返します。

ステップ 6 プライマリクラスタとスタンバイクラスタの構成の詳細を比較します。クラスタ構成に不一致がある場合は、構成の詳細をステップ 5 で収集したデータと比較して、違いを特定します。

プライマリクラスタのサービスの停止

このスクリプトを使用し、プライマリクラスタのサービスを停止して、エージェント、コネクタ、および外部オーケストレータを接続解除できます。

⚠

注意 プライマリクラスタでのみサービスを停止できます。スタンバイクラスタ上で、またはサービスを移行していない場合は、このスクリプトを実行しないでください。

サービス停止スクリプトを実行するには、次の手順を実行します。

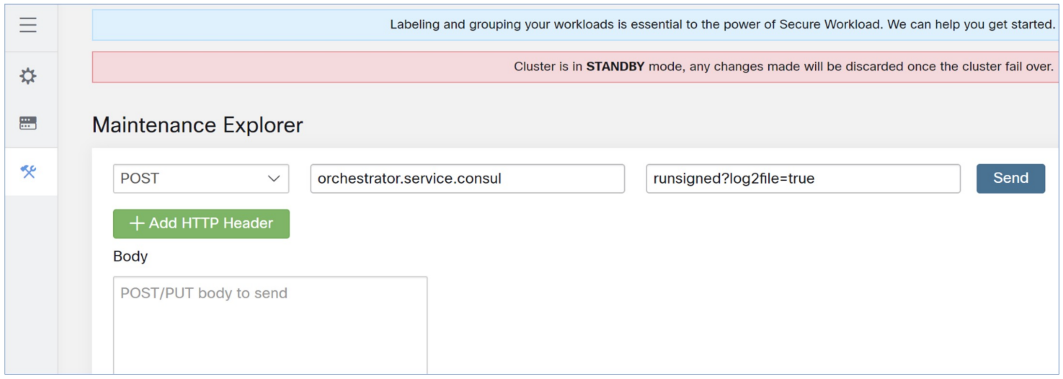
ステップ 1 ナビゲーションウィンドウで、**[トラブルシュート（Troubleshoot）] > [Maintenance Explorer]**の順に選択します。[アクション（Action）] として [POST] を選択します。

ステップ 2 [スナップショットホスト（Snapshot Host）] に *orchestrator.service.consul* と入力します。

ステップ 3 [本文（Body）] フィールドに、service_shutdown.sh.asc ファイルの詳細を入力します。

ステップ 4 [送信（Send）] をクリックします。

図 *22* : サービス停止スクリプトの実行



コネクタと外部オーケストレータ機能の検証

ここでは、移行後にスタンバイクラスタを使用してコネクタと外部オーケストレータ間の接続を確認する方法について説明します。

- プライマリクラスタで検証手順を実行し、データを収集します。
- 復元が完了したら、スタンバイサーバーで同じ手順を実行します。

  2 つのデータセットを比較して、同一であることを確認します。

GUI の [Maintenance Explorer] ページから、署名付きスクリプトとして検証スクリプトを実行します。詳細については、『Cisco Secure Workload ユーザーガイド』の「Explore/Snapshot Endpoints Overview」を参照してください。

（注） 検証スクリプトと生成される出力の詳細については、ext_appliances_health_README.md ファイルを参照してください。

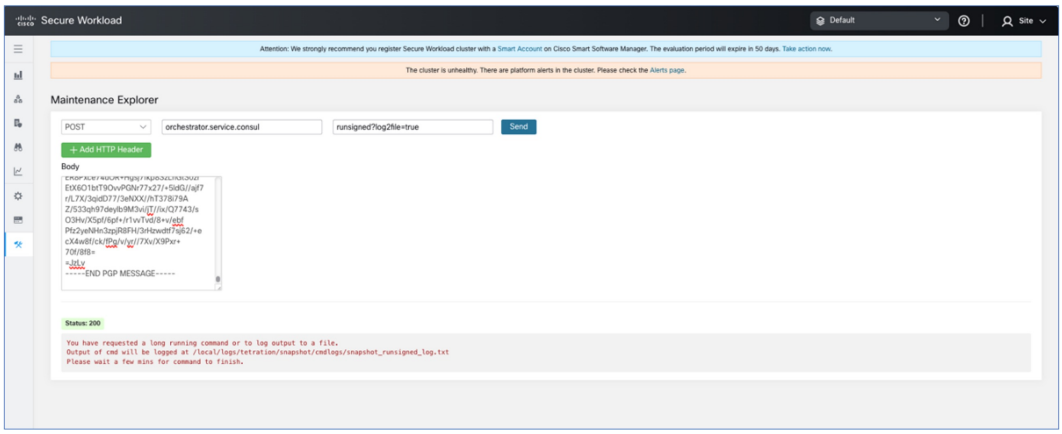
コネクタと外部オーケストレータ間の接続とログファイルの詳細を確認するには、次の手順を実行します。

ステップ 1 ナビゲーションウィンドウで、**[トラブルシュート（Troubleshoot）] > [Maintenance Explorer]**の順に選択します。

- [アクション（Action）] として [POST] を選択します。
- [スナップショットホスト（Snapshot Host）] に *orchestrator.service.consul* と入力します。
- [スナップショットパス（Snapshot Path）] に *runsigned?log2file=true* と入力します。
- [本文（Body）] フィールドに、ext_appliances_health.sh.asc ファイルの詳細を入力します。

- **[Send]** をクリックします。

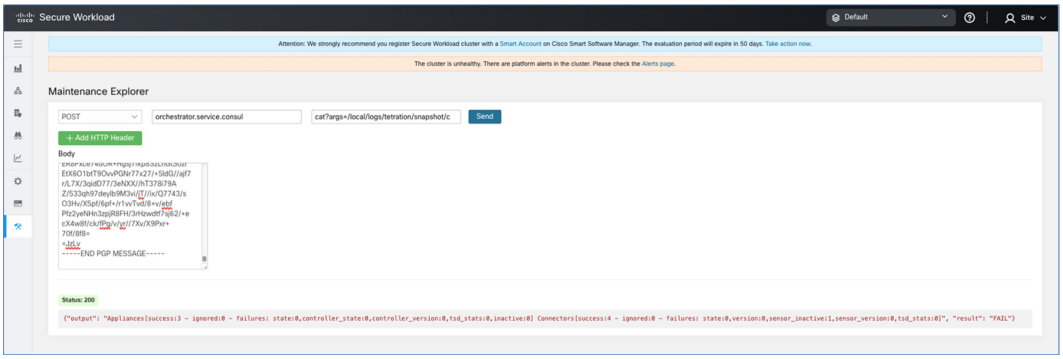
図 *23* : 出力例のログファイル



ステップ 2 ナビゲーションウィンドウで、**[トラブルシュート（Troubleshoot）] > [Maintenance Explorer]**の順に選択し、次の手順を実行します。

- [アクション（Action）] として [POST] を選択します。
- [スナップショットホスト（Snapshot Host）] に *orchestrator.service.consul* と入力します。
- [スナップショットパス（Snapshot Path）] に *cat?args=/local/logs/tetration/snapshot/cmdlogs/snapshot_runsigned_log.txt* と入力します。
- [送信（Send）] をクリックします。

図 *24* : 出力例のログファイル

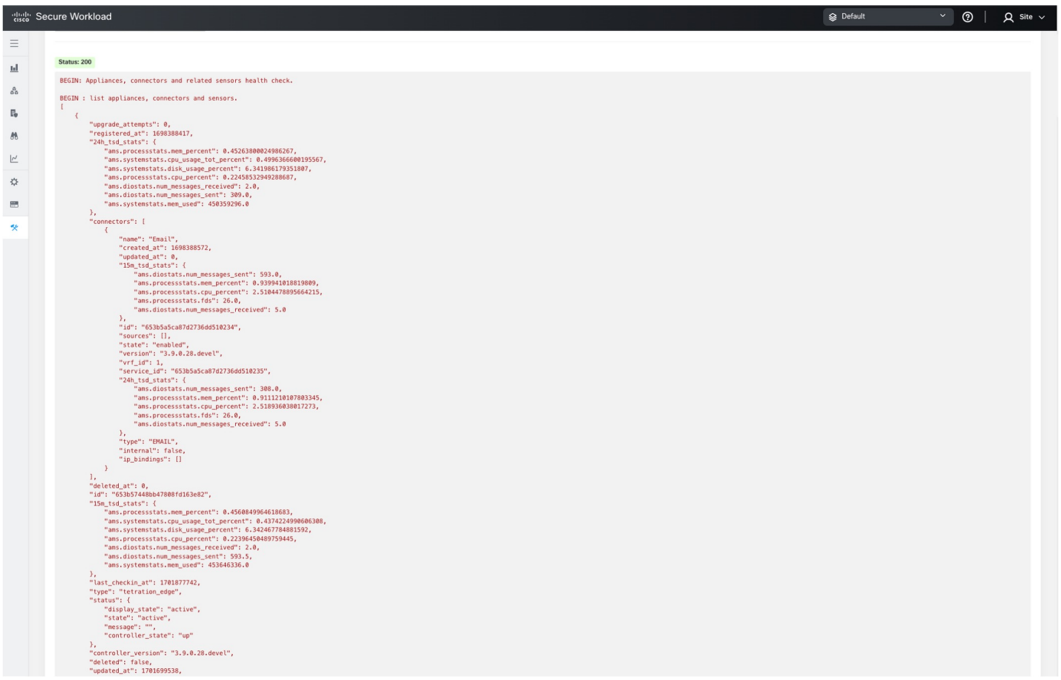


ステップ 3 出力には、コネクタと外部オーケストレータのステータスが表示され、結果が [失敗（FAIL）] または [合格（PASS）] として要約されます。結果が [失敗（FAIL）] の場合は、ナビゲーションウィンドウで、**[トラブルシュート（Troubleshoot）] > [Maintenance Explorer]**の順に選択し、次の手順を実行します。

- [アクション（Action）] として [POST] を選択します。
- [スナップショットホスト（Snapshot Host）] に *orchestrator.service.consul* と入力します。

- [スナップショットパス（Snapshot Path）] に *unsigned?log2file=true&args=--dry_run -d* と入力します。
- [送信（Send）] をクリックします。

コネクタと外部オーケストレータの詳細については、ログファイルを参照してください。移行ステータスが [失敗（FAIL）] である理由の詳細な説明は、すべてのコネクタと外部オーケストレータからの出力に表示されます。



データフローの検証

データ復元プロセス完了後、スクリプトを使用して、プライマリクラスタとスタンバイクラスタに着信するデータフローのデータを検証します。

ステップ 1 ナビゲーションウィンドウで、**[トラブルシュート（Troubleshoot）]** > **[Maintenance Explorer]**の順に選択し、次の手順を実行します。

- [アクション（Action）] として [POST] を選択します。
- [スナップショットホスト（Snapshot Host）] に *orchestrator.service.consul* と入力します。
- [スナップショットパス（Snapshot Path）] に *runsigned* と入力します。
- [本文（Body）] フィールドに dbr_druid_m6_migration.sh.asc ファイルの詳細を入力します。
- [送信（Send）] をクリックします。

ステップ 2 GUI に表示される flow_stats_primary.txt ファイルにデータを保存します。検証の出力には、次の 2 つの部分があります。

- 出力の上部には、データソースと各データソースのフローカウントが表示されます。また、各データソース内に含まれるフローのデータの比較が表示されます。
- 出力の下部は、情報の操作とプルに使用される JSON 出力です。

ステップ 3 復元プロセスが完了し、スタンバイクラスタが復元されたら（**遅延**復元を含む）、スタンバイクラスタに対してステップ 1 を繰り返し、結果を flow_stats_standby.txt に 保存します。

ステップ 4 プライマリクラスタとスタンバイクラスタの出力を比較します。出力は同一である必要があります。

図 *25 :* プライマリクラスタとスタンバイクラスタの出力の確認

センサー情報の検証

移行が完了したら、同じ手順を使用してスタンバイクラスタのセンサー情報を収集します。2つのクラスタの出力を比較して、エージェントが正しく移行されたことを確認します。移行前にプライマリクラスタのセンサー情報を収集するには、次の手順を実行します。

ステップ 1 ナビゲーションウィンドウで、**[トラブルシュート（Troubleshoot）] > [Maintenance Explorer]**の順に選択します。

- [アクション（Action）] として [POST] を選択します。
- [スナップショットホスト（Snapshot Host）] に *orchestrator.service.consul* と入力します。
- [スナップショットパス（Snapshot Path）] に *runsigned* と入力します。
- [本文（Body）] フィールドに、tenant_sensor_summary.sh.asc ファイルの詳細を入力します。
- [送信（Send）] をクリックします。

ステップ 2 センサー情報は CSV ファイルに書き込まれ、情報は GUI にも表示されます。CSV ファイルのデータは、データの分析に使用されます。

CSV ファイルからデータを取得するには、ナビゲーションウィンドウで、**[トラブルシュート（Troubleshoot）] > [Maintenance Explorer]**の順に選択します。

- [アクション（Action）] として [POST] を選択します。
- [スナップショットホスト（Snapshot Host）] に *orchestrator.service.consul* と入力します。
- [スナップショットパス（Snapshot Path）] に *cat?args=/tmp/summary.csv* と入力します。
- [本文（Body）] フィールドには詳細を入力しないでください。
- [送信（Send）] をクリックします。

データが画面に表示されます。CSV データをファイルに保存します。

トラブルシューティング：Data Backup and Restore

S3 構成チェックの失敗

ストレージテストが失敗した場合は、右側のペインに表示される障害シナリオを特定し、以下の点を確認します。

- S3 準拠のストレージの URL が正しい。

- ストレージのアクセスキーと秘密鍵が正しい。
- ストレージ上にバケットが存在し、正しいアクセス権限（読み取り/書き込み）が付与されている。
- プロキシが設定されている（ストレージに直接アクセスする必要がある場合）。
- マルチパート アップロード オプションが無効になっている（Cohesity を使用している場合）。

S3 構成チェックのエラーシナリオ

次の表は、一般的なエラーシナリオと解決策を示したものであり、すべてを網羅したものではありません。

表 *5: S3* 構成チェック中に表示されるエラーメッセージと解決策

エラー メッセージ	シナリオ	対処法
見つからない（Not found）	正しくないバケット名	ストレージに設定されているバケットの正しい名前を入力します。
SSL接続エラー（SSL connection error）	SSL 証明書の有効期限または検証のエラー	SSL 証明書を確認します
	無効な HTTPS URL	• ストレージの正しい HTTPS URL を再入力します。 • SSL 証明書の検証中に発生した障害を解決します。
接続がタイムアウトしました（Connection that is timed out）	S3 サーバーの IP アドレスに到達できません	クラスタと S3 サーバーの間のネットワーク接続を確認します
URLに接続できません（Unable to connect to URL）	正しくないバケットリージョン	正しいバケットのリージョンを入力します
	無効な URL	S3 ストレージエンドポイントの正しい URL を再入力します
Forbidden	無効な秘密鍵	ストレージの正しい秘密鍵を入力します
	無効なアクセスキー	ストレージの正しいアクセスキーを入力します

エラー メッセージ	シナリオ	対処法
S3設定を確認できません（Unable to verify S3 configuration）	その他の例外または一般的なエラー	しばらくしてからS3ストレージの設定を試みます

チェックポイントのエラーコード

次の表は、チェックポイントの一般的なエラーコードを示したものであり、すべてを網羅したものではありません。

表 *6:* チェックポイントのエラーコード

エラー コード	説明
E101：DBのチェックポイントの失敗（E101: DB checkpoint failure）	Mongodb oplog のスナップショットを取得できません
E102：フローデータのチェックポイントの失敗（E102: Flow data checkpoint failure）	Druidデータベースのスナップショットを取得できません
E103：DBスナップショットのアップロードの失敗（E103: DB snapshot upload failure）	Mongo DB スナップショットをアップロードできません
E201：DBのコピーの失敗（E201: DB copy failure）	Mongo スナップショットを HDFS にアップロードできません
E202：設定のコピーの失敗（E202: Config copy failure）	Consul-Vault スナップショットを HDFS にアップロードできません
E203：設定のチェックポイントの失敗（E203: Config checkpoint failure）	consul-vault データのチェックポイントを実行できません
E204：チェックポイント中の設定データの不一致（E204: Config data mismatch during checkpoint）	最大再試行回数後に consul/vault チェックポイントを生成できません
E301：バックアップデータのアップロードの失敗（E301: Backup data upload failure）	HDFS チェックポイントの失敗
E302：チェックポイントのアップロードの失敗（E302: Checkpoint upload failure）	Copydriver が S3 にデータをアップロードできませんでした

エラー コード	説明
E401：チェックポイント中のシステムアップグレード（E401: System upgrade during checkpoint）	このチェックポイント中にクラスタがアップグレードされました。チェックポイントは使用できません
E402：チェックポイント中のサービスの再起動（E402: Service restart during checkpoint）	Bkpdriver が作成状態で再起動しました。チェックポイントは使用できません
E403：前のチェックポイントの失敗（E403: Previous checkpoint failure）	前回の実行でチェックポイントが失敗しました
E404：別のチェックポイントが進行中（E404: Another checkpoint in progress）	別のチェックポイントが進行中です
E405：チェックポイントを作成できない（E405: Unable to create checkpoint）	チェックポイントのサブプロセスでエラーが発生しました
失敗：完了（Failed: Completed）	先行するチェックポイントの一部が失敗しました。同時に開始する複数のチェックポイントが重複している可能性があります

データ復元プロセス中のエラー

- ストレージ構成フェーズ：S3 ストレージ構成時のエラーのトラブルシューティングに推奨される解決策については、「*S3*構成チェックのエラーシナリオ」を参照してください。
- セカンダリクラスタの正常性を確認するための事前チェック：正常ではないサービスまたは警告があるサービスの場合は、[サービスステータス（Service Status）] ページに移動して、サービスを正常にレンダリングするための詳細情報を確認します。
- ストレージへの接続を確認するための事前チェック：

表 *7:* ストレージ接続の事前チェック中のエラー

エラーシナリオ	説明
構成された S3 ストレージからデータをダウンロードできない。	ネットワーク接続が原因で、S3 ストレージへのアクセスに失敗しました。接続が復元され、新しいチェックポイントが S3 ストレージからプリフェッチされるまで、エラーメッセージが表示されます。

エラーシナリオ	説明
セカンダリ（バックアップ）クラスタ SKU がプライマリクラスタと互換性がない。	39 RU から別の 39 RU クラスタにのみデータを復元していることを確認します。8 RU クラスタデータは 8 RU クラスタにのみ復元できます。
セカンダリ（バックアップ）クラスタのバージョンがプライマリと異なっている。	プライマリクラスタとセカンダリクラスタで同じバージョンが実行されていることを確認します。
MongoDB の復元に失敗する。	MongoDB メタデータを復元できません。この問題は、次のチェックポイントプリフェッチ時に修正されます。
DBRInfo マニュアルの形式が不明である。	S3 ストレージ内のチェックポイントメタデータが破損しているか、マニュアルが間違ったストレージにあります。S3 ストレージから dbrinfo.json ファイルをダウンロードし、確認のために Cisco TAC と共有します。
コピーサービスと同期できない。	データ復元マネージャと S3 コピーサービスの間で内部エラーが発生しました。問題のトラブルシューティングについては、Cisco TAC にお問い合わせください。

- FQDN 事前チェック：FQDN 事前チェックに対して警告サインが表示された場合、FQDN の DNS エントリがセカンダリクラスタを指していません。

  解決策：データを復元後、DNS エントリを変更して、ソフトウェアエージェントとセカンダリクラスタ間の接続を有効にします。

- データ復元フェーズ：データ復元の確認ダイアログボックスで、外部オーケストレータのチェックボックスに緑色のチェックマークが付いていない場合は、セカンダリクラスタと外部オーケストレータ間の接続を確認します。

（注） データが復元され、セカンダリクラスタがプライマリ状態になっても、[データ復元（Data Restore）] ページは引き続き使用でき、復元の所要時間と再接続したエージェントの数を確認できます。データが復元されないクラスタの場合、[データ復元（Data Restore）] ページは空白になります。

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。