

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 (1ページ)
- ・エンドツーエンドの移行ワークフロー (2ページ)
- ・クラスタ間の移行の準備(3ページ)
- 復元前の検証 (9ページ)
- •スタンバイクラスタのクラスタデータ (11ページ)
- 復元後および DNS 反転前の検証 (15 ページ)
- ・データ移行の検証(19ページ)
- トラブルシューティング: Data Backup and Restore (29 ページ)

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 1:移行の準備

the Primary and Standby Clusters	Setup External Object Storage Perform Security Checks	Consider Bandwidth	 Obtain a Valid DBR License 	Requirements for Hardware and Software	Choose Backup Mode
Primary Cluster Configuration	1 Configure Storage	2 Configure Data Backup	3 Backup Cluster Data	4 Monitor Data Backup on the Executed the generation	Consider Bandwidth
Ţ					
Standby Cluster Configuration	1 Deploy M6 Cluster in Standby Mode	2 Configure Storage	3 Verify Prefetched Data	4 Verify Guest User Access	
\downarrow					
Pre-Restore Validation	1 Verify Cluster Configurations (WSFS, Kafka, and UI FQDNs)	2 Verify Peering Between the Clusters	3 Verify the Firewall Rules for Clusters	4 Create Backup FQDNs for Primary and Standby Clusters	Verify Prefetch Cluster Data on the Standby Cluster
Ļ					
Restore Data on the Standby Cluster	1 Prefetch Cluster Data	2 Restore Data on Cluster			
Ţ					
Post-Restore and Pre-DNS Flip Validations	1 On the standby cluster, verify the data flow	2 Flip the DNS	3 Perform the post-DNS flip Validations		
Ļ					
Data Migration Validation	1 Verify Storage on Primary and Standby Clusters	2 Verify Cluster Configurations	3 Stop Services on the Primary Cluster	4 Verify Connectors and External Orchestrators an Connected to the Standt Cluster	e y
	5 Verify the Data Flow on Primary and Standby Clusters	6 Verify Sensor Information on Primary and Standby Clusters			

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 (6 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 1: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-M6
8RU-M5	
39RU-GEN1	
39RU-M4	39RU-M6
39RU-M5	

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。

secure vv	orkload			😪 samtenant	~ Ø	Q Site		
Attention:	We strongly re	commend you register Secure Wo	rkload cluster with a days. T	Smart Account on Cisco Smart Software action now.	ware Manager. The evaluation pe	riod will expire in 50		
The cluster is unhealthy. There are platform alerts in the cluster. Please change your Tenant preference to Tenant preference to Default and check the Alerts page								
Softwar	re Agents							
Installer	Upgrad	e Convert to Enforceme	nt Agent Cont	igure Monitor Distrib	ution Agent List			
AGENT	'S FILTERED	BY TENANT samtena	ant					
0 5	SW Version of	contains 3.9	×	Filter +	Download all results	Delete		
Display	ing (1 to 10)	of 10 matching results (0 sel	ected)	First Check-in -	↑ Show 1000 -	Items per page		
T		Hostname	Agent Type	IP Addresses	SW Version	Platform		
>		samkilar-centos10	Enforcement	172.29.202.65 fe80::250:56ff:feb2:2cf2	© 3.9.0.11.devel-enforcer	CentOS-7.9		
>		samkilar-centos09	Enforcement	172.29.203.57 fe80::250:56ff:feb2:4e14	3.9.0.28.devel-enforcer	CentOS-8.5		
>		samkilar-centos08	Enforcement	172.29.202.181 fe80::250:56ff:feb2:88b8	A 3.9.0.11.devel-enforcer	CentOS-8.5		
>		samkilar-centos07	Enforcement	172.29.203.16 fe80::250:56ff:feb2:3690	A 3.9.0.11.devel-enforcer	CentOS-8.5		
>		samkilar-centos06	Enforcement	172.29.203.4 fe80::250:56ff:feb2:5ca6	A 3.9.0.11.devel-enforcer	CentOS-8.5		
>		samkilar-centos05	Enforcement	172.29.202.224 fe80::250:56ff:feb2:9900	3.9.0.28.devel-enforcer	CentOS-8.5		
>	0	samkilar-centos04	Enforcement	172.29.202.182 fe80::250:56ff:feb2:240f	③ 3.9.0.11.devel-enforcer	CentOS-8.5		
>		samkilar-centos03	Enforcement	172.29.202.180 fe80::250:56ff:feb2:de9b	3.9.0.28.devel-enforcer	CentOS-8.5		
>		samkilar-centos02	Enforcement	172.29.202.34 fe80::250:56ff;feb2:7183	A 3.9.0.11.devel-enforcer	CentOS-8.5		
>		samkilar-centos01	Enforcement	172.29.202.33 fe80::250:56ff:feb2:ff26	A 3.9.0.11.devel-enforcer	CentOS-8.5		
	Attention: Softwar Installer Display Y > > > > > > > > > > > > >	Attention: We strongly re The cluster is u Software Agents Installer Upgrad AGENTS FILTERED Displaying (1 to 10) 4 P Displaying (1 to 10) 4 P Displaying (1 to 10) 4 P Displaying (1 to 10) 4 P Displaying (1 to 10) 4 P D D D D D D D D D D D D D	Attention: We strongly recommend you register Secure We The cluster is unhealthy. There are platform alert Software Agents Installer Upgrade Convert to Enforceme AGENTS FILTERED BY TENANT samtene SW Version contains 3.9 Displaying (1 to 10) of 10 matching results (0 seld P Hostname Samkilar-centos01 Samkilar-centos02 Samkilar-centos04 Samkilar-centos02 Samkilar-centos02 Samkilar-centos02 Samkilar-centos01	Attention: We strongly recommend you register Secure Workload cluster with a 3 days. To The cluster is unhealthy. There are platform alerts in the cluster. Please Software Agents Installer Upgrade Convert to Enforcement Agent Conf AGENTS FILTERED BY TENANT samtenant SW Version contains 3.9 × Displaying (1 to 10) of 10 matching results (0 selected) ① Upgrade Samkilar-centos09 Enforcement Samkilar-centos03 Enforcement Samkilar-centos05 Enforcement Samkilar-centos05 Enforcement Samkilar-centos05 Enforcement Samkilar-centos05 Enforcement Samkilar-centos05 Enforcement Samkilar-centos05 Enforcement Samkilar-centos04 Enforcement Samkilar-centos02 Enforcement Samkilar-centos03 Enforcement	Attention: We strongly recommend you register Secure Workload cluster with a Smart Account on Cisco Smart Soft days. Take action now. The cluster is unhealthy. There are platform alerts in the cluster. Please change your Tenant preference to Software Agents Installer Upgrade Convert to Enforcement Agent Configure Monitor Displaying (1 to 10) of 10 matching results (0 selected) • First Check-in • • Box Version Enforcement • Hostname Agent Type IP Addresses • Samkilar-centos09 Enforcement 172.29.203.65 • samkilar-centos08 Enforcement 172.29.203.16 • samkilar-centos08 Enforcement 172.29.203.16 • samkilar-centos05 Enforcement 172.29.203.16 • samkilar-centos05 Enforcement 172.29.203.16 • samkilar-centos05 Enforcement 172.29.203.24 • samkilar-centos05 Enforcement 172.29.203.18 • samkilar-centos05 Enforcement 172.29.203.24 • samkilar-centos05 Enforcement 172.29.203.34 • samkil	Attendor: We strongly recommend you register Secure Workload cluster with a Smart Account on Clico Smart Software Manager. The evaluation per days. Take action now. The cluster is unhealthy. There are platform alerts in the cluster. Please change you? Terrant preference to ◆ Default and check the A Software Agents Installer Upgrade Convert to Enforcement Agent Configure Monitor Distribution Agent List ACENTS FILTERED BY TENANT samtemant SW Version contains 3.9 × Filter Download all results I Displaying (1 to 10) of 10 matching results (0 selected) First Check-in + ↑ Show 1000 + Y Hostname Agent Type IP Addresses SW Version > samkilar-centos09 Enforcement 172.29.202.65 3.9.0.28.devel-enforcer > samkilar-centos08 Enforcement 172.29.202.65 3.9.0.28.devel-enforcer > samkilar-centos08 Enforcement 172.29.202.65 3.9.0.28.devel-enforcer > samkilar-centos08 Enforcement 172.29.202.65 3.9.0.11.devel-enforcer > samkilar-centos05		

図 **2**: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

- 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。
- 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3:スタンバイクラスタのユーザーの詳細

cisco	Secure Workload			😂 Default	~ (9	Q Site √
Ξ	Labeling a	nd grouping your workloads is essential to	o the power of Secure Workload. We o	an help you get started. Run the wizard no	w.	
¢		Cluster is in STANDBY mode, a	any changes made will be discarded o	nce the cluster fail over.		
	User Details					
*		⊘ User Details ———	— 🕗 Assign Roles ———	(3) User Review		
	Email					
	testuser@cisco.com					
	First Name					
	Test					
	Last Name					
	User					
	Scope					
	Default - Warning: Switching Scorp and "Show All" sales	tion will must selected roles				
	SSH Public Key	aun wiil loabt abiecteu ruisa.				
	API Keys					
			No API keys.			
					✓ Back to Users List	t Next >

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 4: データ復元の前提条件

		Cluster is in STANDBY mode, any changes made will be discarded once the clust	er fail over.		
Data Restore					
	1) Process Over	View View	3 Hestore		
Pre-requisites for Restore					See data Restore diagram
Perform Check					
Health checks		c	urrently Configure	d Storage	
DBRserver	~		Access Key	jER41eOoz352L55HjVgYdns15g-JXler3rqyT9pLUes	
Orchestrator	~		URL	https://b13cohesity03.tetrationanalytics.com:3000	
HDFS	~		Bucket	dbr-esx-3035	
Consul	~				
SystemCheck	~				
MongoLits Vavit					
Platform					
DiskUsageCritical	~				
RestoreManager	~				
DataRestore	~				
Data Download Status					
Restore to	Today at 8:28 PM				
Last Successful data download	Today at 8:38 PM				
Last data download attempt	success				
Last prefetched checkpoint	23-10-19T14-58-51-orchestrator-1				
FQDN Resolutions					
kalka-1-lolek.tetrationanalytics.com	^	•			
wsslolek.tetrationanalytics.com	· •				
Agents					
Agents Reconnected	N/A				
Total Agents Count	N/A				
					< Start over Start restore process >

(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 5: データ復元プロセスの段階

		Process Overview 2 Pre-checks	3 Restore			
						See data Restore
esure	0.000		Currently Config	ared Storage		
Starting Hestore	0 00:00		Access Key	FRA1eOn	3521 SSH0/wWiss 15a	
Finding Checkpoint to Restore	0 00:00		185			
Preparing to Restore	() 00:00			https://b1	conestry03.tetrationanarytics.com:3000	
Restoring Data	() 00:00		Bucket	dbr-esx-3	235	
Cleaning Backup Data	() 00:00		Pre-checks perfe	ormed		
Updating Agent Policy Versions	O 00:00		Restored to		Today at 8:28 PM	
Restoring Backup Database	() 00:00		FQDN		kafka-1-lolek.tetrationanalytics.com	
Disabling Data Backup	() 00:00				wssiolek.tetrationanalytics.com	
Restoring Flow Segments	O 00:00		Agents reconnection	ed after restore	N/A	
Cleaning Up Post Restore	© 00:00					
Becoming Primary	() 00:00					
	Restore now					
	0					
						< Pre

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。

		Chuster is in STANDBY mode new character and	he discarded once the st	ater fail come			
		owner oin oranger mode, any changes hade will	or outerbea once the ciu	over red OVEC			
Data Restore							
	1 Proce	ss Overview 2 Pre-checks		3 Restore			
Pre-requisites for Restore						See data Resto	re diagram
Perform Check							
Health checks				Currently Configures	d Storage		
DBRserver	~			Access Key	jER41eOoz352LS5H/VgYdns15g-JXler3rgyT9pLUes		
Orchestrator	J			URL	https://b13cohesity03.tetrationanalytics.com:3000		
HDFS	~			Bucket	dbr-esx-3035		
Consul	~						
SystemCheck	~						
MongoDB	~						
Vault	~						
Platform	~						
DiskUsageCritical	~						
RestoreManager	~						
DataMestore	~						
Data Download Status							
Restore to	Today at 8:28 PM						
Last Successful data download	Today at 8:38 PM						
Last data download attempt							
Last pretetched checkpoint	23-10-19114-58-51-orchestrator-1						
FQDN Resolutions							
kafka-1-lolek.tetrationanalytics.com	^						
wsslolek.tetrationanalytics.com	^						
Ø Agents							
Agents Reconnected	N/A						
Total Agents Count	N/A						
						< Start over Start restore proc	iess >

(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。

図 6: データ復元の前提条件

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 7: データ復元プロセスの段階

		1 Process Overview	2 Pre-checks	3 Restore			
Restore							See data Restore dia
C Starting Restore	0 00:00			Currently Configure	red Storage		
C Synchronizing Copy Driver	() 00:00			Access Key	jER41eOo	352L55H[VgYdns15g-JXler3rqyT9pLUes	
P Finding Checkpoint to Restore	() 00:00			URL	https://b1	Icohesity03.tetrationanalytics.com: 3000	
D Preparing to Restore	() 00:00			Backet	Ac. 411-3	1	
C Restoring Data	() 00:00				der-esk-3		
Cleaning Backup Data	O 00:00			Pre-checks perfor	rmed		
D Updating Agent Policy Versions	⊙ 00:00			Restored to		Today at 8:28 PM	
C Restoring Backup Database	() 00:00			FQDN		kafka-1-lolek.tetrationanalytics.com	
Disabling Data Backup	O 00:00					wssiolek.tetrationanalytics.com	
C Restoring Flow Segments	O 00:00			Agents reconnected	d after restore	N/A	
Cleaning Up Post Restore	O 00:00						
Becoming Primary	() 00:00						
	Restore now						
	Ø						
							< Previ

- 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1 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8:データ復元成功

cisc	5 Secure Workload			😝 samtenant	~ 0	Q Site
Ξ		Attention: We strongly recommend you register Secure Workload cluster with a Smart Account on Cis	co Smart Software Manager. The evaluation period will expire in	90 days. Take action now.		
ы	Data Restore					
å 80						
E,						
88		1 Process Overview 2 Pre-checks	3 Restore			
~						
~	Restore					
*						
-	Restore was successful! You must perform the DNS redirection for	r the agente to point to the new eluster				
*	fou must perform the DNS redirection to	the agents to point to the new closter.				
	Destaution complete					
	100%		Completed Pre-checks			
	Starting Restore	③ 00h:00m:00s	Destand to			
	Synchronizing Copy Driver	③ 00h:00m:10s	Resored to	Today at 5:21 PM		
	Finding Checkpoint to Restore	③ 00h:00m:01s	FQDN	kafka-1-berger.tetrationanalytics.com		0
	Preparing to Restore	() 00h:00m:53s		kafka-2-berger.tetrationanalytics.com		
	Restoring Data	() 00h:03m:11s		wssberger.tetrationanalytics.com		
	Cleaning Backup Data	() 00h:00m:00s				
	Updating Agent Policy Versions	() 00h:00m:00s	Agents reconnected after restore	0/94		
	Restoring Backup Database	() 00h:00m:02s				
	Disabling Data Backup	() 00h:00m:00s				
	Restoring Flow Segments	() 00h:00m:06s				
	Cleaning Up Post Restore	() 00h:08m:32s				
	Becoming Primary	© 00h:00m:00s				
					< Pre	wious
-						

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GUIFQDN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 9:検証エラー

-> % python3 <u>s3-test.py</u>
Using Storage UKL: https://Disconesity03.tetrationanalytics.com:3000, Bucket: aatest-migration
lesting write ubjects
Exception received: An error occurred (NoSuchBucket) when calling the PutUbject 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

White Objects: Eail
Mile Objects. Fail

図 10: 検証成功



図 11:ヘルプ画面

```
-> % python3 <u>s3-test.py</u> -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。

altade. CISCO	Secure Workload			₽ De	ault	~ 0 I	A site ∨
≡	API Keys						
<u>네</u> 슈							Key
E.	API Key	Capabilities	Description 1	Created At ↑	La	User Preferences	
88. 12	e29aee1c76e14c4e8440f2d40f99bf28	software_download	Tetration Installer Credential (System Generated)	May 27 06:07:04 pm (EDT)		API Keys	
⊂ ■ *	51666b262b0044feb1058a60dfefdbd1	sensor, management tww_sensor_management software_download flow_inventiony_query user_role_scope_management user_data_upload app_policy_management external_integration appliance_management appliance_monitoring	migration	Jul 1 11:08:55 am (EDT)	Ju by	Logout I 6 09:25:05 am (EDT) 107.223.190.201	•

図 12: 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。

I

図 *13* :出力例

2023-05-15 14:12:46	,416 [INFO]: Source	e Cluster: kenshiro - R	on_secure_workload_m oot Scope: Shortcake	- VFR ID: 6	-checksrc 76776 - Root Scope ID: 6	03fe5a2755f022ecb1	a90ca	
2023-05-15 14:12:46	,416 [INFO]: Desti	nation Cluster: esx-302	2 - Root Scope: Tang	o - VFR ID:	676769 - Root Scope ID:	63ffe147755f0239c6	58d70b	
2023-05-15 14:12:46	416 [INFO]: RestC	lient objects initializ	ed.					
2023-05-15 14:12:46	,417 [INFO]: Gathe:	ring verification info	from cluster kenshir	o - Shortcak				
Name	Count							
Agents	16							
Scopes								
Filters								
Applications								
Default Exclusion F:	ilters 0							
Application Template	es 14							
External Orchestrate	ors 2							
Secure Connector	True							
Users	91							
Roles								
Server Ports	θ							
Alerts								
Forensics Rules	58							
Forensics Profiles	8							
Usage Analytics	True							
Outbound HTTP Proxy	True							
Virtual Appliances								
Connectors								
Application Name	Application ID	Absolute Policies	Default Policies	Catch-All	Enforcement Enabled	Conversations	Exclusion Filters	Clusters
IPv6 Enforcement	645e9058755f024a7a44d1c	f 0	4	DENY	True	9	0	0
EG Global Policies	63dd94ab755f0267e12f3c9			DENY	True			0
Ubuntu no ipset	63d1a379755f02056a2f3c5	9 0		DENY	True			0
Windows	639b5e99755f02294be99a2	d O		ALLOW	True		9	0
Docker Testing	636d96af755f026139e99ac	7 0	8	DENY	True		9	0
RHEL	632cb748755f027cabe9a97	f e		DENY	False		9	0
CentOS 8	632c805d755f027cabe9a83	в е		DENY	False	133	9	0
CentOS 7	632c8044497d4f58e59bdc2	2 2		DENY	True			0
CentOS 7	632c8044497d4f58e59bdc2	2 2		DENY	True	8	9	0
Linux	6275a0ad755f025f8987795	8 0	10	DENY	False	64		0
Openshift 4.7	624f6d4a755f027a01b55c8	a 26		DENY	False			2
bookinfo 4.7	62323e08755f0218aeb551b	2 0		ALLOW	False			4
2023-05-15 14:13:00	,690 [INFO]: Verif	ication info stored on	file kenshiro-Shorto	ake-precheck	.txt			
2023-05-15 14:13:00	.698 INFO]: Finis	hed!						

表2: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 ²¹
	97
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。

 Λ

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14:サービス停止スクリプトの実行

Ξ	Labeling and grouping your workloads is essential to the power of Secure Workload. We can help you get started.			
⇔	Cluster is in STANDBY mode, any changes made will be discarded once the cluster fail over.			
	Maintenance Explorer			
*	POST v orchestrator.service.consul runsigned?log2file=true Send			
	+ Add HTTP Header			
	Body			
	POST/PUT body to send			

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 **15**:出力例のログファイル

-141-141- CISCO	Q Default ✓ Ø Q site ✓				
≡	American: We attorney's recommend you register Secure Workload cluster with a Smark Account on Cloco Smark Software Manager. The availation period will expire in 50 days. Take action now.				
ы	The cluster is unhealthy. There are platform alerts in the cluster. Plasse check the Alerts page.				
\$	Maintenance Explorer				
E ₀	POST V erchestrator.service.consul nunsigned?tog2tile=true Secol				
88	+ Add HTTP Header				
2	Body				
0	EXXXD1b170xx470k72721/s0401437 1172/540201737040011137874 225324970491498NAV0[11027741] 028440592[1011111]				
-					
*	Pt2;p4846ctzp1041/1045ced1710421+e CXAeff12(Hz)/pf17Kx03197#+				
	7/0/318+ 				
	en rup reconcerne				
	State: 200				
	You have requested a long running command or to log output to a file. Detect of red will be logged in flact/logitress/maphdreconflag/rangeber_runnipred_log.txt				

- **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 **16**:出力例のログファイル

-ili-ili- cisco	that Secure Workload 🔹 🕥 🗛 see 🗸				
Ξ	Attention, We strongly recommend you register Secure Workload cluster with a Smart Account on Class Smart Software Manager. The evaluation periods will register in 50 days, Table action non.				
ы	The cluster is unbeating. There are platform alerts is the cluster. Please clust it have a long spin.				
۵	Maintenance Explorer				
E ₀	POST v exhestrato:service.consul car/hega-flocal/loga/hetaflov/inega/social				
8	+ Add HTTP Header				
≥ © *	Body Construct wavering in substantiation ExtX01115730xP401772.01%8001007 Construct wavering in substantiation ExtX01115730xP401772.01%800 Construct wavering in substantiation P22298142000000000000000000000000000000000000				
	584xx200				
	("suppr": "Appliance (access) - ippered = failures: statest, controller_statest, controller_statest, instand, instand in the statest of the stat				

- 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。

I

データフローの検証

図 17: 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。

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	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
URL)	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

表 3: 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
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 4: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 5: 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	ネットワーク接続が原因で、S3 ストレージ
ンロードできない。	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。