VMware vRealize Orchestrator のインストールおよび構成

vRealize Orchestrator 7.6

最新の技術ドキュメントは、 VMware の Web サイト （https://docs.vmware.com/jp/）

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

ヴイエムウェア株式会社
105-0013　東京都港区浜松町 1-30-5
浜松町スクエア 13F
www.vmware.com/jp

目次

VMware vRealize Orchestrator のインストールおよび構成

『VMware vRealize Orchestrator のインストールおよび構成』では、VMware® vRealize Orchestrator のインストール、アップグレード、構成に関する情報と手順について説明します。

対象読者

この情報は、vSphere 管理者としての経験があり、仮想マシン テクノロジーおよびデータセンターの運用に詳しい方を対象としています。

VMware vRealize Orchestrator の概要

1

VMware vRealize Orchestrator は、開発およびプロセス自動化のプラットフォームであり、VMware 製品およびサード パーティの技術を管理するための自動化された構成可能なプロセスを作成および実行できる拡張ワークフローのライブラリを提供します。

vRealize Orchestrator は、サービス デスク、変更管理システム、IT 資産管理システムなどの VMware およびサード パーティの両方のアプリケーションによる管理タスクおよび操作タスクを自動化します。

この章には、次のトピックが含まれています。

Orchestrator プラットフォームの主な機能

vRealize Orchestrator は、オーケストレーション ツールで必要な一般的な機能を提供するオーケストレーション プラットフォーム、サブシステムの制御を統合するプラグイン アーキテクチャ、およびワークフローのライブラリの 3 つの異なるレイヤーで構成されています。Orchestrator は、新しいプラグインやライブラリを使用して拡張でき、REST API によって大規模なアーキテクチャに統合できるオープン プラットフォームです。

Orchestrator には、ワークフローの実行と管理に役立ついくつかの重要な機能が含まれています。

永続性

プロセス、ワークフローの状態、および Orchestrator の構成などの関連情報の保存に、本番レベルのデータベースが使用されます。

集中管理

Orchestrator にはプロセスを集中的に管理する方法があります。全バージョンの履歴を持つアプリケーション サーバベースのプラットフォームでは、同じストレージ場所にスクリプトおよびプロセス関連のプリミティブを保存できます。このようにして、バージョニングおよび適切な変更制御のないスクリプトがサーバに置かれないようにできます。

チェックポイント処理

ワークフローの各ステップがデータベースに保存されるため、サーバを再起動する必要がある場合に、データの損失を防ぎます。この機能は特に、長時間の処理において役立ちます。

コントロール センター

Web ベースのポータルであるコントロール センターは、ランタイム動作、ワークフロー監視、統一されたログ アクセスおよび構成、ワークフロー実行とシステム リソース間の相関のための集中管理インターフェイスを提供することによって、vRealize Orchestrator インスタンスの管理効率を高めます。Orchestrator の ログ メカニズムは、Orchestrator エンジンのスループットのさまざまなパフォーマンス メトリックを収集する追加ログ ファイルによって最適化されています。

バージョニング

すべての Orchestrator プラットフォーム オブジェクトには、関連するバージョン履歴があります。バージョン履歴は、プロセスをプロジェクトのステージまたは場所に配布するときの基本的な変更管理に役立ちます。

スクリプト エンジン

Mozilla Rhino JavaScript エンジンには、Orchestrator プラットフォーム向けのビルディング ブロックを作成する方法が用意されています。このスクリプト エンジンは、基本バージョン管理、変数の型チェック、名前空間管理、および例外処理により強化されています。このエンジンは、次のビルディング ブロックで使用できます。

- アクション
- ワークフロー
- ポリシー

ワークフロー エンジン

ワークフロー エンジンを使用すると、ビジネス プロセスを自動化できます。この機能は、次のオブジェクトを使用して、ワークフローでの段階的なプロセスの自動化を作成します。

- Orchestrator が提供するワークフローおよびアクション
- ユーザーが作成するカスタム ビルディング ブロック
- プラグインが Orchestrator に追加するオブジェクト

ユーザー、他のワークフロー、スケジュール、またはポリシーがワークフローを開始できます。

ポリシー エンジン

ポリシー エンジンを使用すると、Orchestrator サーバまたはプラグイン テクノロジーでの変化する状態に反応して、イベントを監視および生成できます。ポリシーは、プラットフォームまたはプラグインからイベントを集計できるため、統合されたテクノロジーでの変化する状態の処理に役立ちます。

Orchestrator クライアント

vRealize Orchestrator Client を使用してワークフローを作成、実行、編集、および監視します。また、vRealize Orchestrator Client を使用して、アクション、構成、ポリシー、およびリソース要素を管理することもできます。詳細については、『vRealize Orchestrator クライアントの使用』を参照してください。

注： 廃止された Java ベースの Orchestrator レガシー クライアントの情報については、『VMware vRealize Orchestrator レガシー クライアントの使用』を参照してください。

開発とリソース

Orchestrator のトップページから、vRealize Orchestrator で使用する、独自のプラグインを開発するためのリソースにすばやくアクセスできます。Orchestrator REST API を使用して Orchestrator サーバに要求を送信する方法の詳細も確認できます。

セキュリティ

Orchestrator には、次の高度なセキュリティ機能があります。

- サーバ間でインポートおよびエクスポートされたコンテンツを署名して暗号化する公開鍵基盤 (PKI)。
- エクスポートされたコンテンツを表示、編集、および再配布する方法を制御するデジタル著作権管理 (DRM)。
- デスクトップ クライアントとサーバ間の暗号化通信および Web フロント エンドへの HTTPS アクセスを提供するセキュア ソケット レイヤ (SSL)。
- プロセスおよびこれらのプロセスによって操作されるオブジェクトへのアクセスを制御する、高度なアクセス権管理。

暗号化

vRealize Orchestrator は、文字列の暗号化用の 256 ビット暗号化キーを備えた FIPS 準拠の Advanced Encryption Standard (AES) を使用します。暗号化キーはランダムに生成され、クラスタの一部ではないアプリケーション全体にわたり一意となります。クラスタ内のすべてのノードが同じ暗号化キーを共有します。

Orchestrator のユーザーのタイプと関連責任

Orchestrator には、グローバル ユーザー ロールの特定の責任に基づいたさまざまなツールおよびインターフェイスがあります。Orchestrator では、管理者グループの一員である完全な権限を持つユーザー（管理者）と、管理者グループの一員ではない制限された権限を持つユーザー（エンド ユーザー）とを用意することができます。

完全な権限を持つユーザー

Orchestrator の管理者および開発者は同等の管理権限がありますが、責任の観点から分けられています。

管理者

このロールには、すべての Orchestrator プラットフォーム機能へのフル アクセス権があります。基本的な管理責任には次の項目が含まれます。

- Orchestrator のインストールおよび構成
- Orchestrator およびアプリケーションのアクセス権の管理

- パッケージのインポートおよびエクスポート
- ワークフローの実行とタスクのスケジュール設定
- インポートされた要素のバージョン管理
- 新しいワークフローおよびプラグインの作成

開発者

このユーザー タイプには、すべての Orchestrator プラットフォーム機能へのフル アクセス権があります。開発者には Orchestrator クライアント インターフェイスへのアクセス権が付与され、次の責任を持ちます。

- Orchestrator プラットフォーム機能を拡張するアプリケーションの作成
- 既存のワークフローのカスタマイズおよび新しいワークフローおよびプラグインの作成によるプロセスの自動化

制限された権限を持つユーザー

エンド ユーザー

エンド ユーザーは、管理者または開発者によって Orchestrator クライアントで利用できるようにされたワークフローおよびポリシーを実行およびスケジュール設定できます。

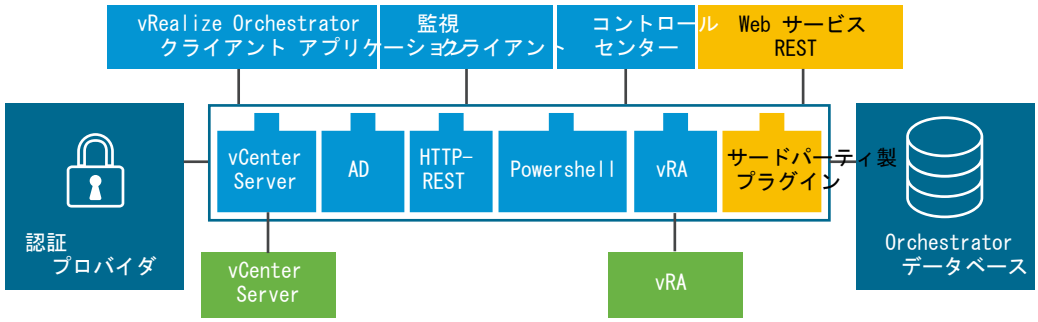
Orchestrator のアーキテクチャ

Orchestrator には、オーケストレーション プロセスを自動化するワークフローを作成および実行できる、ワークフロー ライブラリおよびワークフロー エンジンが含まれています。ワークフローは、Orchestrator が一連のプラグインを介してアクセスするさまざまなテクノロジーのオブジェクトに対して実行します。

Orchestrator には、vCenter Server および vRealize Automation 向けのプラグインを含む、プラグインの標準のセットが用意されており、プラグインが公開されているさまざまな環境においてタスクをオーケストレーションできます。

Orchestrator では、外部のサードパーティ製アプリケーションをオーケストレーション プラットフォームに接続するためのオープン アーキテクチャも提供されています。自身で定義したプラグイン テクノロジーのオブジェクトに対してワークフローを実行できます。Orchestrator は認証プロバイダに接続してユーザー アカウントを管理し、データベースに接続して実行するワークフローからの情報を保存します。Orchestrator、Orchestrator で公開するオブジェクト、および Orchestrator ワークフローに、Orchestrator クライアント インターフェイスまたは Web サービスを介してアクセスできます。Orchestrator ワークフローおよびサービスの監視と構成は、監視クライアントとコントロール センターを介して行われます。

図 1-1. VMware vRealize Orchestrator のアーキテクチャ



Orchestrator プラグイン

プラグインでは、Orchestrator を使用して外部のテクノロジーおよびアプリケーションにアクセスし、それらを制御できます。Orchestrator プラグインで外部テクノロジーを公開することで、外部テクノロジーのオブジェクトと関数にアクセスするワークフローにオブジェクトおよび関数を組み込むことができます。

プラグインを使用してアクセスできる外部テクノロジーには、仮想化管理ツール、E メール システム、データベース、ディレクトリ サービス、リモート制御インターフェイスなどがあります。

Orchestrator には、VMware vCenter Server API および E メール機能などのテクノロジーをワークフローに組み込むために使用できる一連の標準プラグインが用意されています。プラグインを使用することで、新しい IT サービスの提供を自動化したり、既存の vRealize Automation インフラストラクチャおよびアプリケーション サービスの機能を適用したりできます。また、Orchestrator オープン プラグイン アーキテクチャを使用し、他のアプリケーションにアクセスするためのプラグインを開発できます。

VMware が開発する Orchestrator プラグインは、`.vmoapp` ファイルとして配布されます。VMware が開発して配布する Orchestrator プラグインの詳細は、vRealize Orchestrator 外部プラグインを参照してください。サードパーティの Orchestrator プラグインの詳細は、VMware Solution Exchange を参照してください。

Orchestrator のシステム要件

2

システムは Orchestrator が適切に機能するうえで必要な技術要件を満たしている必要があります。

vCenter Server、vSphere Web Client、vRealize Automation、および他の VMware ソリューションのサポートされているバージョン、および互換性のあるデータベース バージョンのリストについては、VMware 製品の相互運用性マトリックスを参照してください。

この章には、次のトピックが含まれています。

- Orchestrator Appliance のハードウェア要件
- vRealize Orchestrator でサポートされるブラウザ
- Orchestrator のデータベース要件
- Orchestrator Appliance に含まれるソフトウェア
- 国際化サポートのレベル
- vRealize Orchestrator ネットワーク ポート

Orchestrator Appliance のハードウェア要件

Orchestrator Appliance は、事前構成された Linux ベースの仮想マシンです。アプライアンスを導入する前に、システムがハードウェアの最小要件を満たしていることを確認します。

Orchestrator Appliance には、次のハードウェア要件があります。

- 2 個の CPU
- 6 GB のメモリ
- 17 GB のハード ディスク

Orchestrator サーバには 2 GB 以上の空きメモリが必要なため、デフォルトのメモリ サイズを減らさないでください。

vRealize Orchestrator でサポートされるブラウザ

ブラウザで vRealize Orchestrator がサポートされていることを確認します。

vRealize Orchestrator Client およびコントロール センターにアクセスするには、次のブラウザのいずれかを使用する必要があります。

- Microsoft Edge
- Mozilla Firefox
- Google Chrome

Orchestrator のデータベース要件

Orchestrator サーバには、稼動準備ができている事前構成済みの PostgreSQL データベースが含まれています。

vRealize Orchestrator 7.5 以降、外部データベースの統合はサポートされません。事前構成された PostgreSQL データベースのみを使用できます。

Orchestrator Appliance に含まれるソフトウェア

Orchestrator Appliance は事前構成された仮想マシンで、Orchestrator の実行用に最適化されています。このアプライアンスは、事前インストール済みソフトウェアを使用して配布されます。

Orchestrator Appliance パッケージには、次のソフトウェアが含まれています。

- VMware 用 SUSE Linux Enterprise Server 11 Update 3（64 ビット エディション）
- PostgreSQL
- Orchestrator

Orchestrator Appliance のデフォルトのデータベース構成は動作準備済みです。

注： Orchestrator Appliance を本番環境で使用するには、vRealize Automation または vSphere で認証する Orchestrator サーバを構成する必要があります。認証プロバイダの構成の詳細については、スタンドアロン Orchestrator サーバの構成を参照してください。

国際化サポートのレベル

Orchestrator コントロール センターには、スペイン語、フランス語、ドイツ語、繁体字中国語、簡体字中国語、韓国語、日本語のロケールが含まれています。Orchestrator クライアントは国際化レベル 1 をサポートします。

Orchestrator がサポートする ASCII 以外の文字

Orchestrator クライアントはローカライズされていませんが、英語以外のオペレーティング システムで動作し、ASCII 以外の文字をサポートします。

表 2-1. Orchestrator GUI がサポートする ASCII 以外の文字

	ASCII 以外の文字のサポート			
Orchestrator の項目	**説明フィールド**	**名前フィールド**	**入力および出力パラメータ**	**属性**
アクション	はい	いいえ	いいえ	いいえ
フォルダ	はい	はい	-	-
構成要素	はい	はい	-	いいえ
パッケージ	はい	はい	-	-
ポリシー	はい	はい	-	-
ポリシー テンプレート	はい	はい	-	-
リソース要素	はい	はい	-	-
ワークフロー	はい	はい	いいえ	いいえ
ワークフローのプレゼンテーションの表示グループと入力手順	はい	はい	-	-

vRealize Orchestrator ネットワーク ポート

vRealize Orchestrator は他のシステムとの通信に特定のポートを使用します。これらのポートは、変更できないデフォルト値で設定されます。

デフォルト構成ポート

vRealize Orchestrator サービスを提供するには、デフォルト ポートを設定し、受信 TCP 接続を許可するようにファイアウォールを構成する必要があります。

注： カスタム プラグインを使用する場合には、他のポートが必要になる場合があります。

表 2-2. VMware vRealize Orchestrator のデフォルト構成ポート

ポート	番号	プロトコル	ソース	ターゲット	説明
仮想アプライアンス管理インターフェイス	5480	TCP			アプライアンス システム設定インターフェイスへのアクセス ポート。
vRealize Orchestrator アプライアンス	5488 5489	TCP			更新のために vRealize Orchestrator アプライアンスによって内部で使用されるポート。
HTTP サーバ ポート	80	TCP	エンド ユーザーの Web ブラウザ	vRealize Orchestrator サーバ	任意。vRealize Orchestrator のデフォルトの HTTP Web ポート 80 に送信されたリクエストは、デフォルトの HTTPS Web ポート 8281 にリダイレクトされます。
HTTP サーバ ポート	8280	TCP	エンド ユーザーの Web ブラウザ	vRealize Orchestrator サーバ	Orchestrator のデフォルトの HTTP Web ポート 8280 に送信されたリクエストは、デフォルトの HTTPS Web ポート 8281 にリダイレクトされます。

表 2-2. VMware vRealize Orchestrator のデフォルト構成ポート （続き）

ポート	番号	プロトコル	ソース	ターゲット	説明
HTTPS サーバ ポート	8281	TCP	エンド ユーザーの Web ブラウザ	vRealize Orchestrator サーバ	vRealize Orchestrator ホーム ページ用のアクセス ポート。
Web 構成 HTTPS アクセス ポート	8283	TCP	エンド ユーザーの Web ブラウザ	vRealize Orchestrator 構成	vRealize Orchestrator クライアントの SSL アクセス ポート。

外部通信ポート

vRealize Orchestrator を外部サービスと通信させるために、送信接続を許可するようにファイアウォールを構成する必要があります。

表 2-3. VMware vRealize Orchestrator の外部通信ポート

ポート番号	プロトコル	ソース	ターゲット	説明
123	UDP	vRealize Orchestrator サーバ	NTP サーバ	ホスト時刻を使用する代わりに直接 NTP に接続するためのデフォルト ポート。
25	TCP	vRealize Orchestrator サーバ	SMTP サーバ	電子メール通知に使用されるポート。
443	TCP	vRealize Orchestrator サーバ	vCenter Server API	オーケストレーションされた vCenter Server インスタンスから仮想インフラストラクチャおよび仮想マシンの情報を取得するために vRealize Orchestrator に使用される vCenter Server API 通信ポート。
4,000	UDP	vRealize Orchestrator サーバ	SNMP サーバ	SNMP プラグインで SNMP トラップをリッスンするためのデフォルト ポート。
514	UDP	vRealize Orchestrator サーバ	Syslog サーバ	Syslog イベント メッセージを送信するためのポート。
5432	TCP	vRealize Orchestrator サーバ	PostgreSQL サーバ	vRealize Orchestrator データベースとして構成される PostgreSQL サーバとの通信に使用されるポート。
5434	TCP	vRealize Orchestrator サーバ	PostgreSQL サーバ	PostgreSQL マネージャ サービスがデータベース フォールト トレランスに使用するポート。

vRealize Orchestrator コンポーネントの設定

3

vRealize Orchestrator Appliance をダウンロードして展開すると、vRealize Orchestrator サーバが事前構成されます。展開されると、サービスは自動的に開始されます。

vRealize Orchestrator 設定の可用性とスケーラビリティを強化するには、以下のガイドラインに従います。

- 認証プロバイダをインストールして構成し、このプロバイダと連携して使用できるように vRealize Orchestrator を構成します。
- クラスタ化された vRealize Orchestrator 環境では、ロード バランシング サーバをインストールして構成することにより、複数の vRealize Orchestrator サーバ間でワークロードを分散します。

この章には、次のトピックが含まれています。

vCenter Server の設定

Orchestrator の設定で vCenter Server インスタンスの数が増加すると、Orchestrator で管理するセッションが増えます。vCenter Server の接続が 10 回を超えると、アクティブなセッションが多すぎるために Orchestrator の操作がタイムアウトになる可能性があります。

vCenter Server でサポートされるバージョンのリストについては、VMware 製品の相互運用性マトリックスを参照してください。

注： ネットワークに十分なバンド幅と待機時間がある場合は、Orchestrator の設定時に異なる仮想マシンで複数の vCenter Server インスタンスを実行できます。LAN を使用して Orchestrator と vCenter Server の間の通信を向上する場合、100 Mb は必須です。

認証方法

ユーザー権限を認証し、管理するには、Orchestrator で vRealize Automation または vSphere サーバ インスタンスのいずれかに接続する必要があります。

Orchestrator Appliance をダウンロードおよび導入する場合は、vRealize Automation または vSphere との接続を設定する必要があります。

vRealize Orchestrator のインストール

4

vRealize Orchestrator は、サーバ コンポーネントとクライアント コンポーネントから構成されています。

vRealize Orchestrator を使用するには、vRealize Orchestrator Appliance を展開し、vRealize Orchestrator サーバを構成する必要があります。

デフォルトの vRealize Orchestrator 設定を変更するには、vRealize Orchestrator コントロール センターを使用します。

この章には、次のトピックが含まれています。

vRealize Orchestrator Appliance のダウンロードと展開

テンプレートから vRealize Orchestrator Appliance を展開して、ダウンロードし、インストールします。

前提条件

- vCenter Server がインストールされて実行されていることを確認します。
- vRealize Orchestrator Appliance を展開する先のホストが、ハードウェアの最小要件を満たしていることを確認します。詳細については、Orchestrator Appliance のハードウェア要件を参照してください。
- システムが分離されておりインターネットにアクセスできない場合は、VMware Web サイトからアプライアンスの `.ova` ファイルをダウンロードする必要があります。

手順

1. 管理者として vSphere Web Client にログインします。
2. vSphere Web Client で、仮想マシンの有効な親オブジェクトであるインベントリ オブジェクト（データセンター、フォルダ、クラスタ、リソース プール、ホストなど）を選択します。
3. [アクション] - [OVF テンプレートのデプロイ] の順に選択します。
4. `.ova` ファイルの URL のパスを入力し、[次へ] をクリックします。
5. 展開された vRealize Orchestrator Appliance の名前と場所を入力し、[次へ] をクリックします。
6. アプライアンスの実行対象としてホスト、クラスタ、リソース プール、または vApp を選択し、[次へ] をクリックします。

7 展開の詳細を確認し、[次へ] をクリックします。

8 使用許諾契約書の条項に同意して、[次へ] をクリックします。

9 展開された vRealize Orchestrator Appliance に使用するストレージ フォーマットを選択します。

フォーマット	説明
シック プロビジョニング (Lazy Zeroed)	仮想ディスクをデフォルトのシック形式で作成します。仮想ディスクの作成時に、仮想ディスクに必要な容量が割り当てられます。物理デバイスにデータが残っている場合は、そのデータは仮想ディスク作成中に消去されませんが、後で仮想マシンから初めて書き込むときにオン デマンドで消去できます。
シック プロビジョニング (Eager Zeroed)	フォルト トレランスなどのクラスタ機能をサポートします。仮想ディスクの作成時に、仮想ディスクに必要な容量が割り当てられます。物理デバイスにデータが残っている場合は、そのデータは仮想ディスクの作成時に消去されます。この形式でのディスクの作成には、他の形式でのディスク作成時と比較すると、はるかに長い時間を要することがあります。
シン プロビジョニング形式	ハード ディスク容量を節約します。シン ディスクの場合、選択したディスク サイズの値に応じて、ディスクに必要な容量と同じデータストア容量をプロビジョニングします。シン ディスクは最初は小さく、初期処理に必要なデータストア容量のみを使用します。

10 [次へ] をクリックします。

11 （オプション） ネットワーク設定を入力し、[次へ] をクリックします。

デフォルトでは、vRealize Orchestrator Appliance は DHCP を使用します。この設定は変更でき、アプライアンスの Web コンソールから固定 IP アドレスを割り当てることができます。

12 有効にするオプションを選択し、root ユーザー アカウントの初期パスワードを設定します。

初期パスワードは 8 文字以上である必要があります。

重要： Orchestrator Appliance の root アカウントのパスワードの有効期限は 365 日です。Orchestrator Appliance に root としてログインし、`passwd –x number_of_days name_of_account` を実行することによって、アカウントの有効期限を延長できます。Orchestrator Appliance の root パスワードの有効期限を無期限にする場合は、`passwd –x 99999 root` を実行します。

13 [設定の確認] 画面の内容を確認して [終了] をクリックします。

結果

vRealize Orchestrator Appliance が正常に展開されました。

vRealize Orchestrator Appliance をパワーオンし、ホームページを開く

vRealize Orchestrator Appliance を使用するには、まずパワーオンし、仮想アプライアンスの IP アドレスを取得する必要があります。

手順

1 vSphere Web Client に管理者としてログインします。

2 vRealize Orchestrator Appliance を右クリックし、[電源] - [パワーオン] の順に選択します。

3 アプライアンスがパワーオンしたら、[サマリ] タブを選択して vRealize Orchestrator Appliance の IP アドレスを表示します。

4 Web ブラウザで、vRealize Orchestrator Appliance 仮想マシンのホスト アドレスに移動します。

https://*your_orchestrator_hostname*/vco

root パスワードの変更

セキュリティ上の理由により、vRealize Orchestrator Appliance の root パスワードを変更できます。

デフォルトでは、vRealize Orchestrator Appliance の root アカウントのパスワードの有効期限は 365 日です。SSH クライアントを使用して vRealize Orchestrator Appliance にログインし、`passwd –x` *`number_of_days name_of_account`* を実行することにより、root アカウントの有効期限を延長できます。vRealize Orchestrator Appliance のルート パスワードの有効期限を無期限にする場合は、`passwd –x 99999 root` を実行します。

前提条件

- vRealize Orchestrator Appliance をダウンロードして展開します。
- vRealize Orchestrator Appliance が稼動し、実行されていることを確認します。

手順

1 vRealize Orchestrator VAMI に **root** としてログインします。

https://*your_orchestrator_hostname*:5480 の VAMI にアクセスします。

2 [管理者] タブを選択します。

3 [現在の管理者パスワード] テキスト ボックスで、現在のパスワードを入力します。

4 [新規の管理者パスワード] テキスト ボックスと [新規の管理者パスワードの再入力] テキスト ボックスに新しいパスワードを入力します。

5 [設定の保存] をクリックします。

結果

vRealize Orchestrator Appliance の root Linux ユーザーのパスワードが変更されました。

vRealize Orchestrator アプライアンスの SSH 管理者ログインの有効化または無効化

SSH による vRealize Orchestrator Appliance へのアクセスを有効または無効にすることができます。

前提条件

- vRealize Orchestrator Appliance をダウンロードして展開します。
- vRealize Orchestrator Appliance が稼動し、実行されていることを確認します。

手順

1 vRealize Orchestrator VAMI に **root** としてログインします。

https://*your_orchestrator_hostname*:5480 の VAMI にアクセスします。

2 [管理者] タブで、[SSH サービス有効] をクリックして vRealize Orchestrator SSH サービスを有効または無効にします。

3 （オプション）[管理者の SSH ログイン有効] をクリックして、vRealize Orchestrator Appliance への SSH を使用した root アクセスを有効または無効にします。

4 [設定の保存] をクリックします。

結果

有効にすると、[SSH ステータス] が *実行中* と表示されます。無効にすると、[SSH ステータス] が *停止* と表示されます。

vRealize Orchestrator Appliance 用ネットワークの構成

固定 IP アドレスを割り当て、プロキシ設定を定義するように vRealize Orchestrator Appliance のネットワークを構成します。

前提条件

- vRealize Orchestrator Appliance をダウンロードして展開します。
- vRealize Orchestrator Appliance が稼動し、実行されていることを確認します。

手順

1 vRealize Orchestrator VAMI に **root** としてログインします。

https://*your_orchestrator_hostname*:5480 の VAMI にアクセスします。

2 [ネットワーク] タブで、[アドレス] をクリックします。

3 vRealize Orchestrator Appliance が IP アドレス設定を取得する方法を選択します。

オプション	説明
DHCP	DHCP サーバから IP アドレス設定を取得します。これがデフォルトの設定です。
Static	固定 IP アドレス設定を使用します。このオプションを選択すると、IP アドレス、ネットマスク（IPv4 の場合）、プリフィックス（IPv6 の場合）、およびゲートウェイ情報を入力するように求められます。

ネットワーク設定によっては、IPv4 および IPv6 アドレス タイプの選択が必要になる場合もあります。

4 [設定の保存] をクリックします。

5 （オプション） プロキシ サーバを構成するには、[プロキシ] タブを選択します。

6 （オプション） プロキシを設定したら、[設定の保存] をクリックします。

初期構成

5

vRealize Orchestrator を使用してタスクの自動化とシステムおよびアプリケーションの管理を開始する前に、vRealize Orchestrator コントロール センターを使用して外部の認証プロバイダを設定する必要があります。また、vRealize Orchestrator コントロール センターを使用して、ライセンスおよび証明書の情報の管理、プラグインのインストール、vRealize Orchestrator ログの監視および構成などの追加の設定タスクを実行できます。

この章には、次のトピックが含まれています。

スタンドアロン Orchestrator サーバの構成

Orchestrator Appliance は事前構成された Linux ベースの仮想マシンですが、Orchestrator コントロール センターにアクセスする前に、構成ウィザードを実行する必要があります。

vRealize Automation 認証でのスタンドアロン Orchestrator サーバの構成

Orchestrator Appliance を使用できるようにするには、ホストの設定および認証プロバイダを構成する必要があります。vRealize Automation コンポーネント レジストリを通じて認証を行うように Orchestrator を構成することができます。

前提条件

- vRealize Orchestrator アプライアンスの最新バージョンをダウンロードして導入します。vRealize Orchestrator Appliance のダウンロードと展開を参照してください。
- vRealize Automation をインストールおよび構成し、vRealize Automation サーバが実行されていることを確認します。vRealize Automation のドキュメントを参照してください。

クラスタを作成するには、次の操作を実行します。

- vRealize Orchestrator の複数のインスタンス間でトラフィックを分散するロード バランサを設定します。詳細については、vRealize Orchestrator ロード バランシングのドキュメントを参照してください。

手順

1 コントロール センターにアクセスして、構成ウィザードを開始します。

   a https://*your_orchestrator_server_IP_or_DNS_name*:8283/vco-controlcenter に移動します。

   b OVA の展開時に入力したパスワードを使用して **root** としてログインします。

2 [変更] をクリックしてコントロール センターからアクセスできるホスト名を設定します。

   注： Orchestrator クラスタを構成する場合は、ロード バランサの仮想サーバのホスト名を入力します。

3 認証プロバイダを構成します。

   a [認証プロバイダを設定] ページで、[認証モード] ドロップダウン メニューから [vRealize Automation] を選択します。

   b [ホスト アドレス] テキスト ボックスに vRealize Automation のホスト アドレスを入力し、[接続] をクリックします。

   c [証明書を承諾] をクリックします。

   d [ユーザー名] および [パスワード] テキスト ボックスに、vRealize Automation で SSO 接続用に設定されたユーザー アカウントの認証情報を入力します。[登録] をクリックします。

   デフォルトでは、SSO アカウントは **administrator**、デフォルト テナント名は **vsphere.local** です。

   e [管理グループ] テキスト ボックスに管理者グループの名前を入力し、[検索] をクリックします。

   例：**vsphere.local\vcoadmins**

   f グループのリストで、グループの名前をクリックして選択します。

   g [変更を保存] をクリックします。

   設定が正常に保存されたことを示すメッセージが表示されます。

結果

これで、コントロール センターの構成が正常に完了しました。

次のステップ

- [VRA] が [ライセンス] ページで構成されたライセンス プロバイダであることを確認します。
- [設定を検証] ページで、ノードが正しく構成されていることを確認します。

注： 認証プロバイダの構成に従って、Orchestrator サーバは 2 分後に自動的に再起動します。プロセス完了直後に構成を確認すると、無効な構成ステータスが返される可能性があります。

vSphere 認証を使用したスタンドアロン Orchestrator サーバの構成

vSphere 認証モードを使用して、Orchestrator サーバを vCenter Single Sign-On サーバに登録します。vCenter Single Sign-On 認証は vCenter Server 6.0 以降で使用します。

前提条件

- vRealize Orchestrator アプライアンスの最新バージョンをダウンロードして導入します。vRealize Orchestrator Appliance のダウンロードと展開を参照してください。
- vCenter Single Sign-On の実行中に vCenter Server をインストールし、構成します。詳細については、vSphere のドキュメントを参照してください。

クラスタを作成するには、次の操作を実行します。

- vRealize Orchestrator の複数のインスタンス間でトラフィックを分散するロード バランサを設定します。詳細については、vRealize Orchestrator ロード バランシングのドキュメントを参照してください。

手順

1 コントロール センターにアクセスして、構成ウィザードを開始します。

   a https://*your_orchestrator_server_IP_or_DNS_name*:8283/vco-controlcenter に移動します。

   b OVA の展開時に入力したパスワードを使用して **root** としてログインします。

2 [変更] をクリックしてコントロール センターからアクセスできるホスト名を設定します。

   注： Orchestrator クラスタを構成する場合は、ロード バランサの仮想サーバのホスト名を入力します。

3 認証プロバイダを構成します。

   a [認証プロバイダを設定] ページで、[認証モード] ドロップダウン メニューから [vSphere] を選択します。

   b [ホスト アドレス] テキスト ボックスに、vCenter Single Sign-On を含む Platform Services Controller インスタンスの完全修飾ドメイン名または IP アドレスを入力し、[接続] をクリックします。

   注： 外部の Platform Services Controller を使用する場合、またはロード バランサの背後で複数の Platform Services Controller インスタンスを使用する場合は、同一の vCenter Single Sign-On ドメインを共有するすべての Platform Services Controller の証明書を手動でインポートする必要があります。

   注： 構成済みの vRealize Orchestrator 環境と異なる vSphere Client を統合するには、Orchestrator に登録されているのと同じ Platform Services Controller を使用するように vSphere を構成する必要があります。高可用性 Orchestrator 環境では、Orchestrator ロード バランサ サーバの背後に Platform Services Controller (PCS) インスタンスをレプリケートする必要があります。

   c [証明書を承諾] をクリックします。

   d [ユーザー名] テキスト ボックスおよび [パスワード] テキスト ボックスに、vCenter Single Sign-On ドメインのローカル管理者アカウントの認証情報を入力します。[登録] をクリックします。

   デフォルトでは、このアカウントは **administrator@vsphere.local**、デフォルト テナント名は **vsphere.local** です。

e [管理グループ] テキスト ボックスに管理者グループの名前を入力し、[検索] をクリックします。

例：**vsphere.local\vcoadmins**

f グループのリストで、グループの名前をクリックして選択します。

g [変更を保存] をクリックします。

設定が正常に保存されたことを示すメッセージが表示されます。

結果

これで、コントロール センターの構成が正常に完了しました。

次のステップ

- [CIS] が [ライセンス] ページで構成されたライセンス プロバイダであることを確認します。
- [設定を検証] ページで、ノードが正しく構成されていることを確認します。

注： 認証プロバイダの構成に従って、Orchestrator サーバは 2 分後に自動的に再起動します。プロセス完了直後に構成を確認すると、無効な構成ステータスが返される可能性があります。

vRealize Orchestrator ネットワーク ポート

vRealize Orchestrator は他のシステムとの通信に特定のポートを使用します。これらのポートは、変更できないデフォルト値で設定されます。

デフォルト構成ポート

vRealize Orchestrator サービスを提供するには、デフォルト ポートを設定し、受信 TCP 接続を許可するようにファイアウォールを構成する必要があります。

注： カスタム プラグインを使用する場合には、他のポートが必要になる場合があります。

表 5-1. VMware vRealize Orchestrator のデフォルト構成ポート

ポート	番号	プロトコル	ソース	ターゲット	説明
仮想アプライアンス管理インターフェイス	5480	TCP			アプライアンス システム設定インターフェイスへのアクセス ポート。
vRealize Orchestrator アプライアンス	5488 5489	TCP			更新のために vRealize Orchestrator アプライアンスによって内部で使用されるポート。
HTTP サーバ ポート	80	TCP	エンド ユーザーの Web ブラウザ	vRealize Orchestrator サーバ	任意。vRealize Orchestrator のデフォルトの HTTP Web ポート 80 に送信されたリクエストは、デフォルトの HTTPS Web ポート 8281 にリダイレクトされます。
HTTP サーバ ポート	8280	TCP	エンド ユーザーの Web ブラウザ	vRealize Orchestrator サーバ	Orchestrator のデフォルトの HTTP Web ポート 8280 に送信されたリクエストは、デフォルトの HTTPS Web ポート 8281 にリダイレクトされます。

表 5-1. VMware vRealize Orchestrator のデフォルト構成ポート （続き）

ポート	番号	プロトコル	ソース	ターゲット	説明
HTTPS サーバ ポート	8281	TCP	エンド ユーザーの Web ブラウザ	vRealize Orchestrator サーバ	vRealize Orchestrator ホーム ページ用のアクセス ポート。
Web 構成 HTTPS アクセス ポート	8283	TCP	エンド ユーザーの Web ブラウザ	vRealize Orchestrator 構成	vRealize Orchestrator クライアントの SSL アクセス ポート。

外部通信ポート

vRealize Orchestrator を外部サービスと通信させるために、送信接続を許可するようにファイアウォールを構成する必要があります。

表 5-2. VMware vRealize Orchestrator の外部通信ポート

ポート番号	プロトコル	ソース	ターゲット	説明
123	UDP	vRealize Orchestrator サーバ	NTP サーバ	ホスト時刻を使用する代わりに直接 NTP に接続するためのデフォルト ポート。
25	TCP	vRealize Orchestrator サーバ	SMTP サーバ	電子メール通知に使用されるポート。
443	TCP	vRealize Orchestrator サーバ	vCenter Server API	オーケストレーションされた vCenter Server インスタンスから仮想インフラストラクチャおよび仮想マシンの情報を取得するために vRealize Orchestrator に使用される vCenter Server API 通信ポート。
4,000	UDP	vRealize Orchestrator サーバ	SNMP サーバ	SNMP プラグインで SNMP トラップをリッスンするためのデフォルト ポート。
514	UDP	vRealize Orchestrator サーバ	Syslog サーバ	Syslog イベント メッセージを送信するためのポート。
5432	TCP	vRealize Orchestrator サーバ	PostgreSQL サーバ	vRealize Orchestrator データベースとして構成される PostgreSQL サーバとの通信に使用されるポート。
5434	TCP	vRealize Orchestrator サーバ	PostgreSQL サーバ	PostgreSQL マネージャ サービスがデータベース フォールト トレランスに使用するポート。

Orchestrator データベース接続

Orchestrator サーバには、データを保存するためのデータベースが必要です。

Orchestrator Appliance をダウンロードして展開すると、アプライアンスに事前インストールされている PostgreSQL データベースと連携するように Orchestrator サーバが構成されます。

事前構成された Orchestrator PostgreSQL データベースは、稼動準備済みです。Orchestrator PostgreSQL のすべてのトランザクションは、VAMI インターフェイスを介して自動的に処理されます。

注： vRealize Orchestrator 7.5 以降、Oracle および Microsoft SQL などの外部データベースはサポートされません。

証明書の管理

証明書は特定のサーバ用に発行され、そのサーバのパブリック キーに関する情報を含んでいるため、これを使用すると、vRealize Orchestrator で作成されたすべての要素に署名し、その正当性を保証できます。クライアントは、サーバから要素（通常はパッケージ）を受信すると、そのアイデンティティを検証してその署名を信頼するかどうかを判断します。

- Orchestrator の証明書の管理

  Orchestrator の証明書の管理は、コントロール センターの [証明書] ページで行うことも、「構成」ワークフロー カテゴリの「SSL トラスト マネージャ」ワークフローを使用して Orchestrator クライアント経由で行うこともできます。

Orchestrator の証明書の管理

Orchestrator の証明書の管理は、コントロール センターの [証明書] ページで行うことも、「構成」ワークフロー カテゴリの「SSL トラスト マネージャ」ワークフローを使用して Orchestrator クライアント経由で行うこともできます。

Orchestrator トラスト ストアへの証明書のインポート

コントロール センターは安全な接続を使用して vCenter Server、リレーショナル データベース管理システム (RDBMS)、LDAP、Single Sign-On など、各種サーバと通信します。必要な SSL 証明書は、URL からインポートするか、PEM でエンコードされたファイルからインポートすることができます。SSL 接続を使用してサーバ インスタンスに接続するたびに、[証明書] ページの [信頼された証明書] タブから対応する証明書をインポートし、さらに対応する SSL 証明書をインポートする必要があります。

Orchestrator の SSL 証明書は、URL アドレスからロードするか、PEM でエンコードされたファイルからロードできます。

オプション	説明
[URL またはプロキシ URL からインポート]	リモート サーバの URL： **`https://`*`your_server_IP_address`*** または ***`your_server_IP_address:port`***
[ファイルからインポート]	PEM でエンコードされた証明書ファイルのパス。 PEM エンコード証明書ファイルのインポートの詳細については、コントロール センターからの信頼された証明書のインポートを参照してください。

自己署名付きサーバ証明書の生成

Orchestrator Appliance には、アプライアンスのネットワーク設定に基づいて自動的に生成される自己署名付き証明書が含まれています。アプライアンスのネットワーク設定が変更された場合は、新しい自己署名付き証明書を手動で生成する必要があります。自己署名付き証明書を作成すると、暗号化された通信を確保して、パッケージに署名を追加できます。ただし、受信者は、自己署名付きパッケージがサードパーティからではなく署名者のサーバから実際に発行されているのかどうかを確認することができません。サーバの ID を証明するには、認証局が署名した証明書を使用します。

自己署名付き証明書は、コントロール センターの [証明書] ページにある [Orchestrator サーバ SSL 証明書] タブで生成できます。

オプション	説明
[署名アルゴリズム]	デジタル署名を生成するための暗号化アルゴリズム。
[共通名]	Orchestrator サーバのホスト名。
[組織]	組織の名前。例：**VMware**
[組織単位]	組織単位の名前。例：**R&D**
[国コード]	国コードの省略形。例：**US**

Orchestrator は環境に対して一意のサーバ証明書を生成します。証明書のパブリック キーの詳細は、[Orchestrator サーバ SSL 証明書] タブに表示されます。プライベート キーは、Orchestrator データベースの `vmo_keystore` テーブルに保存されます。

Orchestrator サーバ SSL 証明書のインポート

vRealize Orchestrator は安全な通信を行うため、クライアントやリモート サーバに対して SSL 証明書を使用して ID を証明します。Orchestrator にはデフォルトで、アプライアンスのネットワーク設定に基づいて自動的に生成される自己署名付き SSL 証明書が含まれています。認証局が署名している SSL 証明書をインポートすることにより、証明書の信頼性に関するエラーを回避できます。

認証局が署名した証明書は、PEM でエンコードされたファイルとしてインポートする必要があります。また、このファイルにはパブリック キーとプライベート キーが含まれている必要があります。

注： SSL サーバ証明書を生成またはインポートした後、[Orchestrator サーバ SSL 証明書] タブを更新して、新しい証明書の詳細を表示します。Orchestrator Configurator サービスも再起動する必要があります。

```
service vco-configurator restart
```

パッケージ署名証明書

Orchestrator サーバからエクスポートされたパッケージはデジタル署名されています。パッケージの署名に使用する新しい証明書は、インポート、エクスポート、生成できます。パッケージ署名証明書のフォームはデジタル ID です。これは暗号化された通信や Orchestrator パッケージの署名に使用されます。

Orchestrator Appliance には、アプライアンスのネットワーク設定に基づいて自動的に生成されるパッケージ署名証明書が含まれています。アプライアンスのネットワーク設定が変更された場合は、新しいパッケージ署名証明書を手動で生成する必要があります。

注： Orchestrator Appliance には、Orchestrator の初期構成時に自動的に生成される自己署名付きパッケージ署名証明書が含まれています。パッケージ署名証明書は変更できます。変更すると、その後にエクスポートされるすべてのパッケージは、新しい証明書を使用して署名されます。

コントロール センターからの信頼された証明書のインポート

他のサーバと安全に通信するには、Orchestrator サーバがその ID を確認できる必要があります。この目的で、リモート エンティティの SSL 証明書を、Orchestrator トラスト ストアにインポートすることが必要になる場合があります。特定の URL への接続を確立してトラスト ストアにインポートする方法、または PEM エンコード ファイルとしてトラスト ストアに直接インポートする方法のいずれかが使用できます。

前提条件

SSL 経由で Orchestrator を接続するサーバの完全修飾ドメイン名を検索します。

手順

1. SSH を使用して Orchestrator Appliance に **root** としてログインします。
2. リモート サーバの証明書を取得するためのコマンドを実行します。

   ```
   openssl s_client –connect host_or_dns_name:secure_port
   ```

   a. 暗号化されていないポートを使用する場合は、`starttls` と必要なプロトコルを、`openssl` コマンドとともに使用します。

   ```
   openssl s_client –connect host_or_dns_name:port –starttls smtp
   ```

3. `–––––BEGIN CERTIFICATE–––––` タグから `–––––END CERTIFICATE–––––` タグまでのテキストをテキスト エディタにコピーし、それをファイルとして保存します。
4. コントロール センターに **root** としてログインします。
5. [証明書] ページに移動します。
6. [信頼された証明書] タブで、[インポート] をクリックし、 [PEM エンコード ファイルからインポート] オプションを選択します。
7. 証明書ファイルを参照して、[インポート] をクリックします。

結果

リモート サーバ証明書は Orchestrator トラスト ストアに正常にインポートされました。

vRealize Orchestrator プラグインの構成

デフォルトの vRealize Orchestrator プラグインは、vRealize Orchestrator Client でプラグイン固有のワークフローを実行することによって構成されます。

vRealize Orchestrator Appliance では、デフォルトのプラグインの事前インストール済みライブラリへのアクセスが用意されています。これらのデフォルトのプラグインは、vRealize Orchestrator Client から固有のワークフローを実行することによって構成できます。

たとえば、ワークフロー ライブラリの検索テキスト ボックスに、*タグ AMQP* および *Configuration* を入力すると、AMQP ブローカーとサブスクリプションを管理するために使用されるワークフローが得られます。

vRealize Orchestrator プラグインの管理

vRealize Orchestrator コントロール センターの [プラグインを管理] 画面で、vRealize Orchestrator にインストールされているすべてのプラグインのリストを表示して、基本的な管理アクションを実行できます。

プラグインのログ レベルの変更

vRealize Orchestrator のログ レベルを変更する代わりに、特定のプラグインのみに合わせて変更することができます。

新しいプラグインのインストールまたはアップグレード

vRealize Orchestrator プラグインでは、vRealize Orchestrator サーバは他のソフトウェア製品と統合することができます。vRealize Orchestrator Appliance には、事前インストールされたプラグインのセットが含まれています。また、カスタムのプラグインをインストールして、vRealize Orchestrator プラットフォームの機能をさらに拡張することもできます。

プラグインのインストールまたはアップグレードは、vRealize Orchestrator の [プラグインを管理] 画面から実行できます。使用できるファイルの拡張子は、`.vmoapp` および `.dar` です。`.vmoapp` ファイルは複数の `.dar` ファイルを含むことができ、また、アプリケーションとしてインストールできます。1 つのプラグインに関連付けられているすべてのリソースを 1 つの `.dar` ファイルに含めることができます。

注： vRealize Orchestrator プラグインの推奨されるファイル形式は *.vmoapp* です。

vRealize Orchestrator プラグインのインストールまたはアップグレードの詳細については、vRealize Orchestrator プラグインのインストールまたはアップデートを参照してください。

プラグインの無効化

プラグインの名前の横にある [有効] チェック ボックスをオフにすると、プラグインを無効にすることができます。

このアクションでは、プラグイン ファイルは削除されません。Orchestrator のプラグインのアンインストールについては、プラグインのアンインストールを参照してください。

vRealize Orchestrator プラグインのインストールまたはアップデート

vRealize Orchestrator コントロール センターを使用して、サードパーティ プラグインをインストールまたはアップデートできます。

前提条件

プラグインの *.dar* ファイルまたは *.vmoapp* ファイルをダウンロードします。

注： vRealize Orchestrator プラグインの推奨されるファイル形式は *.vmoapp* です。

手順

1 コントロール センターに root としてログインします。

2 [プラグインを管理] 画面を選択します。

3 [参照] をクリックし、インストールまたはアップデートするプラグインの *.dar* ファイルまたは *.vmoapp* ファイルを選択します。

4 [アップロード] をクリックします。

5 プラグイン情報を確認します。該当する場合は、エンドユーザー使用許諾契約書に同意し、[インストール] をクリックします。

プラグインがインストールまたは更新され、vRealize Orchestrator サーバ サービスが再起動されます。

次のステップ

正しいプラグイン情報が [プラグインを管理] 画面に一覧表示されていることを確認します。

プラグインのアンインストール

vRealize Orchestrator コントロール センターを使用して、サードパーティ製プラグインを削除できます。コントロール センターからプラグインを削除した後は、関連付けられたパッケージを vRealize Orchestrator クライアントから削除する必要があります。

手順

1 コントロール センターに **root** としてログインします。

2 [プラグインの管理] を選択します。

3 アンインストールするプラグインを選択し、右側の削除アイコンをクリックします。

4 プラグインを削除することを確認し、[削除] をクリックします。

5 vRealize Orchestrator クライアントに管理者としてログインします。

6 [資産] - [パッケージ] の順に選択します。

7 削除したプラグインに関連付けられているパッケージを参照し、[削除] をクリックします。

注： 関連するパッケージを検索するには、[検索] テキスト ボックスにプラグイン固有のタグを入力します。たとえば、Site Recovery Manager プラグイン パッケージは、**SRM** タグを入力することによって確認できます。

8 [パッケージとコンテンツを削除して、共有アイテムは保持] を選択して、[削除] をクリックします。

9 Orchestrator レガシー クライアントに管理者としてログインします。

10 右上隅にある [ツール] メニューから、[ユーザー環境設定] を選択します。

11 [全般] ページで、[許可される空でないフォルダを削除] チェック ボックスを選択します。

12 [保存して閉じる] をクリックします。

フォルダ全体を、そのサブフォルダとワークフローを含め、1 回のクリックで削除できるようになりました。

13 [ワークフロー] タブをクリックします。

14 アンインストールするプラグインが含まれているフォルダを削除します。

15 [アクション] タブをクリックします。

16 アンインストールするプラグインのアクション モジュールを削除します。

17 vRealize Orchestrator サービスを再起動します。

結果

プラグインに関連するカスタム ワークフロー、アクション、ポリシー、構成、設定、リソースがすべて削除されました。

Orchestrator の可用性とスケーラビリティ

Orchestrator サービスの可用性を高めるには、共有データベースを使用してクラスタ内の複数の Orchestrator サーバ インスタンスを起動します。vRealize Orchestrator はクラスタの一部として動作するように構成されるまで、単一のインスタンスとして動作します。

Orchestrator クラスタ

サーバおよびプラグインの構成が同じである複数の Orchestrator サーバ インスタンスは、クラスタ内で一緒に動作して 1 つのデータベースを共有できます。

すべての Orchestrator サーバ インスタンスはハートビートを交換して相互に通信します。個々のハートビートは、ノードによってクラスタの共有データベースに一定の間隔で書き込まれるタイムスタンプです。ネットワーク問題、データベース サーバが応答しない問題、またはオーバーロードの問題が発生すると、Orchestrator クラスタ ノードは応答を停止する場合があります。アクティブな Orchestrator サーバ インスタンスが、フェイルオーバーのタイムアウト期間内にハートビートを送信しなかった場合は、応答していないとみなされます。フェイルオーバーのタイムアウト期間は、ハートビート間隔をフェイルオーバー ハートビートの数で乗じた値と等しくなります。これによって信頼性の低いノードを特定できます。また、フェイルオーバーのタイムアウト期間は、使用可能なリソースや本番環境の負荷に応じてカスタマイズすることができます。

Orchestrator ノードはデータベース接続が失われると、データベース接続がリストアされるまでスタンバイ モードになります。クラスタ内の他のノードがアクティブな操作を制御し、中断されているすべてのワークフローを未完了の操作（スクリプト化可能なタスク、ワークフローの呼び出しなど）から再開します。

Orchestrator は、クラスタのステータスを監視してフェイルオーバーの通知を送信する組み込みツールは提供していません。クラスタの状態は、ロード バランサなどの外部コンポーネントを使用して監視できます。ノードが実行されているかどうかを確認するには、https://*your_orchestrator_server_IP_or_DNS_name*:8281/vco/api/healthstatu で REST API サービスの健全性ステータスを使用するか、https://*your_orchestrator_server_IP_or_DNS_name*:8283/vco-controlcenter/docs/ でコントロール センターのステータスを監視して、ノードのステータスを確認します。

VAMI での vRealize Orchestrator インスタンスのクラスタの構成

vRealize Orchestrator 7.5 以降、すべてのクラスタリング操作は Orchestrator Appliance の VAMI インターフェイスを介して行われます。

Orchestrator クラスタは、1 つのデータベースを共有する複数の Orchestrator インスタンスで構成されます。新しい Orchestrator クラスタを構成するか、または Orchestrator VAMI インターフェイスから既存のクラスタに新しいノードを追加します。Orchestrator クラスタには 3 つの種類のノードがあります。

ノード タイプ	定義
プライマリ ノード	各 Orchestrator クラスタには 1 台のプライマリ ノードがあります。クラスタ内のすべてのノードは、プライマリ ノードの PostgreSQL データベースを共有します。プライマリ データベースは、非同期と同期のどちらのモードでも実行できます。クラスタが機能するには、プライマリ ノードが健全な状態でなければなりません。
レプリカ ノード	レプリカ ノードは、プライマリの Orchestrator ノードに参加している Orchestrator インスタンスです。
同期されたレプリカ ノード	同期モードを有効にすると、レプリカ ノードが同期されたレプリカ ノードの状態にプロモートされます。同期されたレプリカの状態になると、プライマリ ノードの自動フェイルオーバーが有効になります。

前提条件

- 少なくとも 2 つのスタンドアローン サーバ ノードを構成します。詳細については、スタンドアロン Orchestrator サーバの構成を参照してください。
- Orchestrator インスタンスがインストールされている仮想マシンのクロックを同期します。
- Orchestrator の複数のインスタンス間でトラフィックを分散するロード バランサを設定します。

手順

1 **root** として VAMI インターフェイスにログインします。

https://*your_orchestrator_server_ip_or_DNS_name*: 5480 のアドレスで、VAMI インターフェイスにアクセスします。

2 [クラスタ] タブを選択し、クラスタのプライマリ ノードになる Orchestrator ノードの認証情報を入力します。

既存のクラスタ化された Orchestrator 環境の場合、Orchestrator クラスタのプライマリ ノードの認証情報を入力します。

3 [クラスタに参加] をクリックします。

4 ノードの証明書情報を確認して、[OK] をクリックします。

5 クラスタリング操作により、Orchestrator ノードのコンテンツが同期され、レプリカ ノードがプライマリ ノードの PostgreSQL データベースに参加します。

次のステップ

Orchestrator コントロール センターの [設定を検証] ページで、クラスタが正しく構成されていることを確認します。

注： クラスタ ノードの構成に従って、Orchestrator サーバは 2 分後に自動的に再起動します。プロセス終了直後に構成を確認すると、無効なクラスタ ステータスが返される可能性があります。

Orchestrator クラスタの監視

クラスタを作成した後、クラスタ ノードの状態を監視できます。

コントロール センターの [Orchestrator クラスタ管理] ページから、クラスタに参加している Orchestrator インスタンスの構成の同期状態を監視できます。

設定同期状態	説明
実行時間	Orchestrator サービスが使用可能になり、要求を受け入れることができます。
スタンバイ	Orchestrator サービスは、次のことが原因で要求を処理できません。 ■ ノードは、高可用性 (HA) クラスタの一部であり、プライマリ ノードに障害が発生するまでスタンバイ モードのままになります。 ■ データベース、認証プロバイダ、および Orchestrator インスタンスのライセンスへの有効な接続など、構成の前提条件をサービスでは確認できません。
サービスの健全性ステータスの取得に失敗しました。	Orchestrator サーバ サービスが停止しているか、またはネットワークの問題が存在するため、接続できません。
保留中の再起動	コントロール センターによって構成変更が検出され、Orchestrator サーバが自動的に再起動します。

Orchestrator クラスタの同期モードの有効化

Orchestrator データベース クラスタを同期モードで実行するように構成できます。

同期モードでは、プライマリの Orchestrator データベースの自動フェイルオーバーが有効になります。このプロセスにより、レプリカ ノードの 1 つが [同期されたレプリカ] の状態にプロモートされます。現在のプライマリ ノードに障害が起きると、同期されたレプリカが自動的にプライマリ ノードにプロモートされます。同期されたレプリカは、プライマリ ノードのデータベースから終了したすべてのトランザクションを受け取ります。

前提条件

少なくとも 3 つの Orchestrator ノードで構成される Orchestrator クラスタを構成します。

手順

1 **root** として VAMI インターフェイスにログインします。

https://*your_orchestrator_server_ip_or_DNS_name*: 5480 のアドレスで、VAMI インターフェイスにアクセスします。

2 [クラスタ] タブを選択します。

3 [同期モード] をクリックします。

4 クラスタのノードの 1 つが [同期されたレプリカ] の状態にプロモートされます。

同期操作が正常に実行されたことを確認するには、[クラスタ] タブのレプリケーション モードの状態が [データベースは同期モードです] となっていることを確認します。

Orchestrator レプリカ ノードのプライマリ ノードへのプロモート

レプリカ ノードをプライマリ ノードにプロモートすることにより、Orchestrator クラスタを再構成できます。

非同期モードと同期モードの両方で Orchestrator ノードをプロモートすることができます。

注： 同期モードの Orchestrator クラスタには自動フェイルオーバー機能があるため、現在のプライマリ ノードに障害が起きると、同期されたレプリカ ノードが自動的に新しいプライマリ ノードになります。

前提条件

少なくとも 2 つの Orchestrator インスタンスで構成される Orchestrator クラスタを構成します。

手順

1. **root** として VAMI インターフェイスにログインします。

   https://*your_orchestrator_server_ip_or_DNS_name*: 5480 のアドレスで、VAMI インターフェイスにアクセスします。

2. [クラスタ] タブを選択します。
3. 新しいプライマリ ノードの状態にプロモートするレプリカ ノードの横にある [プロモート] をクリックします。
4. [新しいプライマリ ノードに正常にプロモートしました] というメッセージが VAMI ユーザー インターフェイスの左上に表示され、ノードの状態が [プライマリ] に変わります。

Orchestrator クラスタ ノードの削除

Orchestrator レプリカ ノードを Orchestrator クラスタから削除して、レプリカ ノードを交換したり、容量を削減したりすることができます。

レプリカ ノードのみクラスタから削除できます。プライマリ ノードを削除するには、最初にレプリカ ノードをプロモートして交換する必要があります。詳細については、Orchestrator レプリカ ノードのプライマリ ノードへのプロモートを参照してください。

手順

1. **root** として VAMI インターフェイスにログインします。

   https://*your_orchestrator_server_ip_or_DNS_name*: 5480 のアドレスで、VAMI インターフェイスにアクセスします。

2. [クラスタ] タブを選択します。
3. レプリカ ノードの横にある [削除] コマンドを選択します。
4. レプリカ ノードをクラスタから削除することを確認して、[OK] をクリックします。

   注： 削除されたレプリカ ノードのホスト名をロード バランサ サーバから削除する必要があります。

5. Orchestrator ノードがクラスタから削除され、ユーザー インターフェイスの上部に [ノードが正常に削除されました] というメッセージが表示されます。

カスタマ エクスペリエンス改善プログラムの設定

カスタマ エクスペリエンス改善プログラム (CEIP) に参加すると、VMware 製品とサービスの品質、信頼性、および機能を向上させるための匿名の情報が VMware に送られます。

VMware が受信する情報の種類

カスタマ エクスペリエンス向上プログラム (CEIP) では、VMware 製品とサービスの改善や問題点の修正に役立つ情報を VMware に提供します。

CEIP を通して収集されるデータおよび VMware のその使用目的に関する詳細は、Trust & Assurance センター (http://www.vmware.com/trustvmware/ceip.html) に記載されています。この製品の CEIP への参加または参加終了については、「カスタマ エクスペリエンス改善プログラムに参加」を参照してください。

カスタマ エクスペリエンス改善プログラムに参加

コントロール センターからカスタマ エクスペリエンス改善プログラムに参加します。

手順

1. コントロール センターに **root** としてログインし、[カスタマー エクスペリエンス向上プログラム] 画面を開きます。
2. [カスタマー エクスペリエンス向上プログラムに参加] チェック ボックスをオンにして CEIP を有効にするか、またはチェック ボックスをオフにしてプログラムを無効にしてから、[保存] をクリックします。
3. （オプション） プロキシ ホストを手動で追加する場合は、[プロキシ自動検出] チェック ボックスをオフにします。

API サービスの使用

6

コントロール センターを使用して Orchestrator を構成できるだけでなく、Orchestrator REST API、コントロール センターの REST API、またはコマンド ライン ユーティリティを使用して、アプライアンスに保存されている Orchestrator サーバの構成を変更することもできます。

構成プラグインはデフォルトで、Orchestrator パッケージに含まれています。構成プラグイン ワークフローには、Orchestrator ワークフロー ライブラリまたは Orchestrator REST API からアクセスできます。これらのワークフローを使用すると、Orchestrator サーバの信頼された証明書およびキーストアの設定を変更できます。使用可能なすべての Orchestrator REST API サービス呼び出しについては、https://*orchestrator_server_IP_or_DNS_name*:8281/vco/api/docs にある『Orchestrator REST API リファレンス』を参照してください。

- REST API を使用した SSL 証明書とキーストアの管理

  コントロール センターを使用すると、SSL 証明書を管理できるだけでなく、構成プラグインや REST API を使用してワークフローを実行する際に、信頼された証明書とキーストアを管理することができます。

- コントロール センター REST API を使用した Orchestrator 構成の自動化

  コントロール センターの REST API から、Orchestrator サーバを構成するためのリソースにアクセスできます。サードパーティ システムでコントロール センターの REST API を使用して、Orchestrator 構成を自動化できます。

REST API を使用した SSL 証明書とキーストアの管理

コントロール センターを使用すると、SSL 証明書を管理できるだけでなく、構成プラグインや REST API を使用してワークフローを実行する際に、信頼された証明書とキーストアを管理することができます。

構成プラグインには SSL 証明書とキーストアをインポートおよび削除するためのワークフローが含まれています。これらのワークフローにアクセスするには、Orchestrator クライアントのワークフロー ビューで [ライブラリ] - [構成] - [SSL トラスト マネージャ] に移動するか、[ライブラリ] - [構成] - [キーストア] に移動します。これらのワークフローは Orchestrator REST API を使用して実行することもできます。

REST API を使用した SSL 証明書の削除

SSL 証明書を削除するには、構成プラグインの「信頼された証明書の削除」ワークフローを実行するか、REST API を使用します。

手順

1 「信頼された証明書の削除」ワークフローのワークフロー サービスの URL で以下の GET 要求を作成します。

```
GET https://{orchestrator_host}:{port}/vco/api/workflows?conditions=name=Delete trusted
certificate
```

2 「信頼された証明書の削除」ワークフローの定義の URL で以下の GET 要求を作成して、ワークフローの定義を取得します。

```
GET https://{orchestrator_host}:{port}/vco/api/workflows/8a70a326-ffd7-4fef-97e0-2002ac49f5bd
```

3 「信頼された証明書」ワークフローの実行オブジェクトが存在する URL で以下の POST 要求を作成します。

```
POST https://{orchestrator_host}:{port}/vco/api/workflows/8a70a326-ffd7-4fef-97e0-2002ac49f5bd/
executions/
```

4 要求本文の実行コンテキスト要素で「信頼された証明書の削除」ワークフローの入力パラメータとして、削除する証明書の名前を指定します。

REST API を使用した SSL 証明書のインポート

SSL 証明書をインポートするには、構成プラグインからワークフローを実行するか、REST API を使用します。

信頼された証明書をファイルまたは URL からインポートできます。コントロール センターを使用した Orchestrator の証明書のインポートについては、Orchestrator の証明書の管理を参照してください。

手順

1 ワークフロー サービスの URL で以下の GET 要求を作成します。

オプション	説明
信頼された証明書をファイルからインポート	信頼された証明書をファイルからインポートします。
信頼された証明書を URL からインポート	信頼された証明書を URL アドレスからインポートします。
プロキシ サーバを使用して信頼された証明書を URL からインポート	プロキシ サーバを使用して、信頼された証明書を URL アドレスからインポートします。
証明書別名を持つ信頼された証明書を URL からインポート	証明書別名を持つ信頼された証明書を URL アドレスからインポートします。

信頼された証明書をファイルからインポートするには、以下の GET 要求を作成します。

```
GET https://{orchestrator_host}:{port}/vco/api/workflows?conditions=name=Import
                trusted certificate from a file
```

2 ワークフローの定義の URL で GET 要求を作成して、ワークフローの定義を取得します。

「信頼された証明書をファイルからインポート」ワークフローの定義を取得するには、以下の GET 要求を作成します。

```
GET https://{orchestrator_host}:{port}/vco/api/workflows/93a7bb21-0255-4750-9293-2437abe9d2e5
```

3 ワークフローの実行オブジェクトが存在する URL で POST 要求を作成します。

「信頼された証明書をファイルからインポート」ワークフローの場合は、以下の POST 要求を作成します。

```
POST https://{orchestrator_host}:{port}/vco/api/workflows/93a7bb21-0255-4750-9293-2437abe9d2e5/
executions
```

4 要求本文内の実行コンテキスト要素で、ワークフローの入力パラメータの値を指定します。

パラメータ	説明
cer	SSL 証明書をインポートする元の CER ファイル。 このパラメータは、「信頼された証明書をファイルからインポート」ワークフローの場合に適用可能です。
url	SSL 証明書をインポートする元の URL。非 HTTPS サービスの場合、サポートされる形式は *IP_address_or_DNS_name:port* です。 このパラメータは、「信頼された証明書を URL からインポート」ワークフローの場合に適用可能です。

REST API を使用したキーストアの作成

キーストアを作成するには、構成プラグインの「キーストアの作成」ワークフローを実行するか、REST API を使用します。

手順

1 「キーストアの作成」ワークフローのワークフロー サービスの URL で以下の GET 要求を作成します。

```
GET https://{orchestrator_host}:{port}/vco/api/workflows?conditions=name=Create a keystore
```

2 「キーストアの作成」ワークフローの定義の URL で以下の GET 要求を作成して、ワークフローの定義を取得します。

```
GET https://{orchestrator_host}:{port}/vco/api/workflows/6c301bff-e8fe-4ae0-ad08-5318178594b3/
```

3 「キーストアの作成」ワークフローの実行オブジェクトが存在する URL で以下の POST 要求を作成します。

```
POST https://{orchestrator_host}:{port}/vco/api/workflows/6c301bff-e8fe-4ae0-ad08-5318178594b3/
executions/
```

4 要求本文の実行コンテキスト要素で「キーストアの作成」ワークフローの入力パラメータとして、作成するキーストアの名前を指定します。

REST API を使用したキーストアの削除

キーストアを削除するには、構成プラグインの「キーストアの削除」ワークフローを実行するか、REST API を使用します。

手順

1 「キーストアの削除」ワークフローのワークフロー サービスの URL で以下の GET 要求を作成します。

```
GET https://{orchestrator_host}:{port}/vco/api/workflows?conditions=name=Delete a keystore
```

2 「キーストアの削除」ワークフローの定義の URL で以下の GET 要求を作成して、ワークフローの定義を取得します。

```
GET https://{orchestrator_host}:{port}/vco/api/workflows/7a3389eb-1fab-4d77-860b-81b66bb45b86/
```

3 「キーストアの削除」ワークフローの実行オブジェクトが存在する URL で以下の POST 要求を作成します。

```
POST https://{orchestrator_host}:{port}/vco/api/workflows/7a3389eb-1fab-4d77-860b-81b66bb45b86/
executions/
```

4 要求本文の実行コンテキスト要素で「キーストアの削除」ワークフローの入力パラメータとして、削除するキーストアの名前を指定します。

REST API を使用したキーの追加

キーを追加するには、構成プラグインの「キーの追加」ワークフローを実行するか、REST API を使用します。

手順

1 「キーの追加」ワークフローのワークフロー サービスの URL で以下の GET 要求を作成します。

```
GET https://{orchestrator_host}:{port}/vco/api/workflows?conditions=name=Add key
```

2 「キーの追加」ワークフローの定義の URL で以下の GET 要求を作成して、定義を取得します。

```
GET https://{orchestrator_host}:{port}/vco/api/workflows/6c301bff-e8fe-4ae0-ad08-5318178594b3/
```

3 「キーの追加」ワークフローの実行オブジェクトが存在する URL で以下の POST 要求を作成します。

```
POST https://{orchestrator_host}:{port}/vco/api/workflows/6c301bff-e8fe-4ae0-ad08-5318178594b3/
executions/
```

4 要求本文の実行コンテキスト要素で「キーの追加」ワークフローの入力パラメータとしてキーストア、キー エイリアス、PEM エンコード キー、証明書チェーン、およびキー パスワードを指定します。

コントロール センター REST API を使用した Orchestrator 構成の自動化

コントロール センターの REST API から、Orchestrator サーバを構成するためのリソースにアクセスできます。サードパーティ システムでコントロール センターの REST API を使用して、Orchestrator 構成を自動化できます。

コントロール センターの REST API の root エンドポイントは、https://*orchestrator_server_IP_or_DNS_name*:8283/vco-controlcenter/api です。コントロール センターの REST API に対して発行できるすべてのサービス呼び出しについては、https://*orchestrator_server_IP_or_DNS_name*:8283/vco-controlcenter/docs にある『コントロール センター REST API リファレンス』を参照してください。

コマンドライン ユーティリティ

Orchestrator コマンドライン ユーティリティを使用して、Orchestrator 構成を自動化できます。

コマンドライン ユーティリティにアクセスするには、SSH を使用して Orchestrator Appliance に root としてログインします。ユーティリティは `/var/lib/vco/tools/configuration-cli/bin` にあります。使用可能な構成オプションを確認するには、`./vro-configure.sh --help` を実行します。

その他の構成オプション 7

Orchestrator のデフォルトの動作を変更するには、コントロール センターを使用します。

この章には、次のトピックが含まれています。

認証の再構成

コントロール センターの初期構成時に認証方法を設定すると、その後はいつでも、認証プロバイダや構成済みのパラメータを変更できます。

認証プロバイダの変更

認証モードまたは認証プロバイダの接続設定を変更するには、まず既存の認証プロバイダを登録解除する必要があります。

前提条件

手順

1 コントロール センターに **root** としてログインします。

2 [認証プロバイダを設定] ページで、ホスト アドレスのテキスト ボックスの横にある [登録解除] ボタンをクリックして、使用中の認証プロバイダを登録解除します。

3 [ID サービス] セクションで [登録解除] をクリックして、サーバの認証情報を削除します。

結果

これで、認証プロバイダを正常に登録解除できました。

次のステップ

コントロール センターの認証を再設定します。詳細については、 vRealize Automation 認証でのスタンドアロン Orchestrator サーバの構成または vSphere 認証を使用したスタンドアロン Orchestrator サーバの構成を参照してください。

認証パラメータの変更

vRealize Automation をコントロール センターの認証プロバイダとして使用する場合、Orchestrator 管理者グループのデフォルト テナントの変更が必要になる場合があります。vSphere 認証を使用すると、管理者グループを変更できます。

前提条件

- コントロール センターに **root** としてログインします。
- 認証モードを選択して、認証プロバイダの接続設定を行います。

手順

1 デフォルト テナントを変更します。

注： vRealize Automation 認証モードを使用する場合にのみ、デフォルト テナントを変更できます。

a コントロール センターの [認証プロバイダを設定] ページで、[デフォルト テナント] テキスト ボックスの横にある [変更] ボタンをクリックします。

b テキスト ボックスで、既存のデフォルト テナント名を使用する名前に置き換えます。

c [管理グループ] テキスト ボックスの横にある [変更] ボタンをクリックします。

注： 管理者グループを再設定しないと、このグループは空のままになりコントロール センターにアクセスできなくなります。

d 管理者グループの名前を入力し、[検索] をクリックします。

e グループのリストで、グループの名前をダブルクリックして選択します。

f [変更を保存] をクリックします。

コントロール センターからログアウトすると、シングル サインオンのログイン画面にリダイレクトされます。

2 管理者グループを変更します。

a [管理グループ] テキスト ボックスの横にある [変更] ボタンをクリックします。

b 管理者グループの名前を入力し、[検索] をクリックします。

c グループのリストで、グループの名前をダブルクリックして選択します。

d [変更を保存] をクリックします。

コントロール センターからログアウトすると、シングル サインオンのログイン画面にリダイレクトされます。

Orchestrator 構成のエクスポート

コントロール センターには、Orchestrator 構成設定をローカル ファイルにエクスポートするメカニズムがあります。このメカニズムを使用して、システム構成のスナップショットをあらゆる時点で作成し、この構成を新しい Orchestrator インスタンスにインポートできます。

構成設定のエクスポートと保存は、特に構成の変更や保守タスクの実行、あるいはシステムのアップグレードを行う場合に定期的に実行する必要があります。

重要： エクスポートされた構成を含むファイルには機密性の高い管理情報が含まれているため、セキュリティが確保された安全な場所に保管してください。

手順

1 コントロール センターに **root** としてログインします。

2 [設定をエクスポート/インポート] をクリックします。

3 エクスポートするファイルのタイプを選択します。

注： [プラグイン設定をエクスポート] を選択し、プラグイン設定に暗号化プロパティが含まれている場合は、インポートするときにデータを正しく復号化するために [サーバ設定をエクスポート] も選択する必要があります。

4 （オプション） 構成ファイルを保護するためのパスワードを入力します。

構成を後でインポートするときは、同じパスワードを使用します。

5 [エクスポート] をクリックします。

結果

Orchestrator によって、`orchestrator-config-export-`*`hostname-dateReference`*`.zip` ファイルが作成され、これがローカル マシンにダウンロードされます。このファイルを使用すると、システムのクローンを作成したり、システムをリストアしたりすることができます。

Orchestrator 構成のインポート

Orchestrator を再インストールした後、またはシステム障害が発生した場合に、以前にエクスポートしたシステム構成をリストアできます。

インポート手順を使用して Orchestrator 構成のクローンを作成した場合、新しい vCenter Server プラグイン ID が生成されるため、vCenter Server プラグイン構成は無効になって機能しません。

手順

1 コントロール センターに **root** としてログインします。

2 [設定をエクスポート/インポート] をクリックして、[設定をインポート] タブに移動します。

3 以前のインストールでエクスポートした `.zip` ファイルを参照して選択します。

注： エクスポートした構成ファイルのデフォルトの構文は、`orchestrator-config-export-`*`hostname-dateofexport_timeofexport`*`.zip` です。

4 （オプション） 構成をエクスポートするときに使用したパスワードを入力します。

パスワードを指定して構成をエクスポートしなかった場合はこのステップは必要ありません。

5 インポート タイプを選択します。

オプション	説明
組み込み	vRealize Automation に組み込まれている Orchestrator インスタンスに移行します。
外部	外部の Orchestrator に移行します。
レプリカ	同一の Orchestrator インスタンスをレプリケートします。

6 [インポート] をクリックします。

結果

新しいシステムでは、選択したインポート タイプに基づき、古い構成がレプリケートされます。Orchestrator サーバ サービスが自動的に再起動されます。

次のステップ

コントロール センターの [設定を検証] ページで、Orchestrator が正しく設定されていることを確認します。

ワークフローの実行のプロパティの設定

デフォルトではノードあたり最大 300 個のワークフローを実行できます。実行中のワークフローが最大数に達した場合は、最大 10,000 個のワークフローをキューに入れることができます。

Orchestrator ノードで 300 個を超える同時ワークフローを実行する必要がある場合、保留中のワークフローの実行はキューに入れられます。アクティブなワークフローの実行が完了すると、キュー内にある次のワークフローの実行が開始されます。キュー内のワークフローが最大数に達すると、保留中のいずれかのワークフローの実行が開始されるまで、次のワークフローの実行は失敗します。

コントロール センターの [詳細オプション] ページで、ワークフローの実行のプロパティを設定できます。

オプション	説明
[セーフ モードを有効化]	セーフ モードが有効になっている場合、すべての実行中のワークフローはキャンセルされ、次回の Orchestrator ノード起動時に再開されません。
[同時実行中のワークフローの数]	同時に実行される同時実行 Orchestrator ノード ワークフローの最大数。
[キュー内の実行中のワークフローの最大数]	Orchestrator ノードが受け付け可能なワークフローの実行要求の数。
[ワークフローごとに保持される実行の最大数]	クラスタ内のワークフローごとに履歴として保持される終了済みのワークフローの実行の最大数。最大数を超えると最も古いワークフローの実行が削除されます。
[ログ イベントの有効期間 (日)]	クラスタのログ イベントがデータベースから消去されるまでの日数。
[すべてのワークフロー実行をプロファイル]	ワークフローの自動プロファイルを有効または無効にします。有効な場合は、ワークフローのプロファイルにより、すべてのワークフロー実行でメトリック データが生成されます。
[ワークフロー プロファイラの統計情報を配布する間隔]	プロファイラの統計情報が環境内のすべての Orchestrator インスタンスに配布される間隔。

Orchestrator のログ ファイル

VMware テクニカル サポートでは、通常、サポート要求が送信されると診断情報を要求します。診断情報には、製品固有のログや、製品を実行しているホストの構成ファイルが含まれます。

Orchestrator の構成ファイルとログ ファイルが含まれている ZIP バンドルは、コントロール センターの [ログをエクスポート] メニューからダウンロードできます。

表 7-1. Orchestrator のログ ファイル リスト

ファイル名	場所	説明
`scripting.log`	`/var/log/vco/app-server`	ワークフローおよびアクションのスクリプト ログ メッセージを示します。`scripting.log` ファイルを使用すると、ワークフローの実行およびアクションの実行を通常の Orchestrator 操作から分離できます。この情報は `server.log` ファイルにも記載されます。
`server.log`	`/var/log/vco/app-server`	Orchestrator サーバ上のすべてのアクティビティに関する情報を示します。Orchestrator をデバッグする際か、Orchestrator で実行しているアプリケーションをデバッグする際に `server.log` ファイルを使用して分析します。
`metrics.log`	`/var/log/vco/app-server`	サーバのランタイム情報が記載されます。このログ ファイルには情報が 5 分ごとに追加されます。
`localhost_access_log.txt`	`/var/log/vco/app-server`	サーバの HTTP 要求のログが記載されます。
`localhost_access_log.`*`date`*`.txt`	`/var/log/vco/configuration`	コントロール センター サービスの HTTP 要求のログが記載されます。
`controlcenter.log`	`/var/log/vco/configuration`	コントロール センター サービスのログ ファイルです。

ログのパーシステンス

任意の種類の Orchestrator スクリプト（ワークフロー、ポリシー、アクションなど）の情報を使用してログを作成することができます。この情報にはタイプとレベルが用意されています。タイプはパーシステントと非パーシステントのどちらかになります。レベルは DEBUG、INFO、WARN、ERROR、TRACE、FATAL のいずれかになります。

表 7-2. パーシステント ログと非パーシステント ログの作成

ログ レベル	パーシステント タイプ	非パーシステント タイプ
DEBUG	Server.debug("short text", "long text");	System.debug("text")
INFO	Server.log("short text", "long text");	System.log("text");
WARN	Server.warn("short text", "long text");	System.warn("text");
ERROR	Server.error("short text", "long text");	System.error("text");

パーシステント ログ

パーシステント ログ（サーバ ログ）は過去のワークフローの実行ログを追跡し、Orchestrator データベースに保存します。サーバ ログを表示するには、ワークフロー、完了しているワークフローの実行、またはポリシーを選択し、Orchestrator クライアントの [イベント] タブをクリックします。

非パーシステント ログ

非パーシステント ログ（システム ログ）を使用してスクリプトを作成する場合、Orchestrator サーバはすべての実行中の Orchestrator アプリケーションにこのログを通知しますが、この情報はデータベースに保存されません。アプリケーションが再起動されるとログ情報は失われます。非パーシステント ログはデバッグ時に最新情報として使用されます。システム ログを表示するには、Orchestrator クライアントで完了しているワークフローの実行を選択し、[スキーマ] タブの [ログ] をクリックします。

Orchestrator ログの設定

コントロール センターの [ログを設定] ページで、必要なサーバ ログとスクリプト ログのレベルを設定できますどちらかのログが 1 日に複数回生成されると、問題の原因を特定するのが困難になります。

サーバ ログとスクリプト ログのデフォルトのログ レベルは INFO です。ログ レベルを変更すると、サーバによってログに記録されるすべての新しいメッセージと、データベースへのアクティブな接続の数に影響が及びます。ログの詳細レベルは降順で低くなります。

注意： DEBUG または ALL のログ レベルは、問題をデバッグする場合にのみ設定してください。パフォーマンスを大幅に低下させる可能性があるため、これらのログ レベルは本番環境に設定しないでください。

ログのローテーション設定

サーバ ログが大きくなりすぎるのを回避するには、[最大ファイル数] および [最大ファイル サイズ (MB)] テキスト ボックスの値を変更し、サーバ ログの最大ファイル数と最大ファイル サイズを設定します。

Orchestrator ログ ファイルのエクスポート

コントロール センターの [ログをエクスポート] ページから、構成、サーバ、ラッパー、およびインストール ログ ファイルなど、トラブルシューティング情報の ZIP アーカイブを生成できます。

ログ情報は `vco-logs-date_hour.zip` という名前の ZIP アーカイブに保存されます。

注： クラスタ内に Orchestrator インスタンスが複数ある場合は、ZIP アーカイブにクラスタのすべての Orchestrator インスタンスからのログが含まれます。

Orchestrator ログのフィルタリング

特定のワークフローを実行するために Orchestrator サーバ ログのフィルタリングを行って、ワークフローの実行に関する診断データを収集できます。

Orchestrator ログには、リアルタイムで監視できる有用な情報が多く含まれています。同じワークフローの複数のインスタンスを同時に実行している場合は、Orchestrator ライブ ログ ストリームで実行されている各ワークフローに関する診断データをフィルタリングして、異なるワークフローの実行を追跡できます。

注： クラスタ内に Orchestrator インスタンスが複数ある場合、ライブ ログ ストリームにはローカルの Orchestrator ノードのログのみが表示されます。

手順

1. コントロール センターに **root** としてログインします。
2. [ライブ ログ ストリーム] をクリックします。
3. 検索バーに検索パラメータを入力します。

   たとえば、ユーザー名、ワークフロー名、ワークフロー ID、トークン ID でログをフィルタリングできます。
4. （オプション） 検索結果をさらに絞り込むには、[大文字と小文字を区別する] および [フィルタ (grep)] を選択します。

   [フィルタ (grep)] を選択すると、ライブ ストリームには検索パラメータに一致する行のみが表示されます。

結果

Orchestrator ライブ ログ ストリームは、検索パラメータに従ってフィルタリングされます。

次のステップ

コントロール センターの [ライブ ログ ストリーム] ページからアクセスできない古いログをフィルタリングする場合は、サードパーティ製のログ分析ツールを使用できます。

リモート サーバでのログ統合の構成

vRealize Log Insight やその他の Syslog サーバなどのリモート ログ システムにログを送信するように Orchestrator を構成できます。

手順

1. コントロール センターに **root** としてログインします。

2 [ログ統合] メニューに移動します。

3 [リモート ログ サーバへのログ記録を有効化] を有効にします。

4 ログ統合オプションを設定します。

a ログ システム タイプを選択します。

b リモート ログ サーバのホスト名とポート値を入力します。

c リモート ログ サーバにログ イベントを送信するために使用されるプロトコルを選択します。

5 リモート サーバへのログ統合の構成を完了するには、[保存] をクリックします。

ネットワーク インターフェイス コントローラの追加

vRealize Orchestrator では、複数のネットワーク インターフェイス コントローラ (NIC) がサポートされています。インストール後に、NIC を Orchestrator Appliance に追加できます。

前提条件

vRealize Orchestrator を vCenter Server 環境に完全にインストールします。

手順

1 vCenter Server で、各 vRealize Orchestrator Appliance に NIC を追加します。

a アプライアンスを右クリックして、[設定の編集] を選択します。

b VMXNET3 NIC を追加します。

c パワーオンされている場合、アプライアンスを再起動します。

2 vRealize Orchestrator Appliance 管理インターフェイスに root としてログインします。

https://*orchestrator-appliance-IP*:5480

3 [ネットワーク] を選択して、複数の NIC が使用できることを確認します。

4 [アドレス] を選択して、NIC の IP アドレスを設定します。

表 7-3. NIC 設定の例

設定	値
IPv4 アドレス タイプ	Static
IPv4 アドレス	172.22.0.2
ネットマスク	255.255.255.0

5 [設定の保存] をクリックします。

スタティック ルートの設定

NIC を vRealize Orchestrator インストール環境に追加する際に、スタティック ルートが必要な場合、コマンド プロンプト セッションを開いて設定します。

前提条件

vRealize Orchestrator Appliance に複数の NIC を追加します。

手順

1 vRealize Orchestrator Appliance のコマンド ラインに root としてログインします。

2 テキスト エディタでルート ファイルを開きます。

`/etc/sysconfig/network/routes`

3 デフォルト ゲートウェイの `default` 行を特定します。ここでは変更しないでください。

注： デフォルト ゲートウェイを変更する必要がある場合は、代わりに vRealize Orchestrator 管理インターフェイスを使用します。

4 `default` 行の下にスタティック ルートの新しい行を追加します。例：

```
default 10.10.10.1 - -
172.30.30.0 192.168.100.1 255.255.255.0 eth0
192.168.210.0 192.168.230.1 255.255.255.0 eth2
```

5 ルート ファイルを保存して閉じます。

6 アプライアンスを再起動します。

7 HA クラスタで、各アプライアンスに対してこのプロセスを繰り返します。

OpenTracing と Wavefront 拡張機能の有効化

vRealize Orchestrator の Opentracing および Wavefront 拡張機能には、vRealize Orchestrator 環境に関するデータを収集するためのツールが用意されています。このデータを使用して、vRealize Orchestrator システムおよびワークフローのトラブルシューティングを行うことができます。

vRealize Orchestrator Appliance で OpenTracing および Wavefront 拡張機能を使用するように構成するには、vRealize Orchestrator でそれらを有効にする必要があります。

前提条件

vRealize Orchestrator Appliance SSH サービスが有効であることを確認します。vRealize Orchestrator VAMI の [管理者] タブで、SSH サービスのステータスを確認できます。

手順

1 SSH クライアントを使用して、**root** として vRealize Orchestrator Appliance にログインします。

https://*your_orchestrator_hostname*:5480 の vRealize Orchestrator Appliance にアクセスします。

2 拡張機能のディレクトリに移動します。

`cd /var/lib/vco/app-server/extensions`

3 `ls` コマンドを実行して、使用可能なすべての vRealize Orchestrator 拡張機能を一覧表示します。

4 Wavefront および OpenTracing 拡張機能 を有効にします。

```
mv opentracing-7.6.0.jar.inactive opentracing-7.6.0.jar
mv wavefront-7.6.0.jar.inactive wavefront-7.6.0.jar
```

5 `ls` コマンドを再度実行して、拡張機能が `.inactive` で終わらないことを確認します。

次のステップ

コントロール センターの [拡張機能プロパティ] 画面で、OpenTracing および Wavefront と vRealize Orchestrator の連携を構成します。詳細については、OpenTracing 拡張機能の構成および Wavefront 拡張機能の構成を参照してください。

OpenTracing 拡張機能の構成

OpenTracing 拡張機能は、ワークフローの実行に関するデータを Jaeger サーバに送信します。データには、ワークフローのステータス、入出力パラメータ、ワークフローの実行を開始したユーザー、およびワークフロー ID データが含まれます。

前提条件

- Orchestrator アプリケーションで Orchestrator Appliance が有効になっていることを確認してください。詳細については、OpenTracing と Wavefront 拡張機能の有効化を参照してください。
- Orchestrator OpenTracing 拡張機能で使用する Jaeger サーバをデプロイします。詳細については、Jaeger スタート ガイド ドキュメントを参照してください。

手順

1 Orchestrator コントロール センターに **root** としてログインします。

2 [拡張機能プロパティ] 画面に移動します。

3 OpenTracing 拡張機能を選択します。

4 Jaeger サーバ ホストのアドレスおよびポートを入力します。

> **注：** サーバ アドレスを入力する前に、2 つのスラッシュ (//) を挿入します。

5 [保存] をクリックします。

結果

Orchestrator OpenTracing 拡張機能が構成されました。

次のステップ

- OpenTracing 拡張機能によって収集されたデータを含む Jaeger ユーザー インターフェイスにアクセスするには、構成時に入力したホストのアドレスにアクセスします。
- [サービス] オプションで、[ワークフロー] を選択します。
- 表示するデータを指定するには、[タグ] オプションを使用します。たとえば、失敗したワークフローに関するデータを表示するには、**status=failed** と入力します。

Wavefront 拡張機能の構成

Wavefront 拡張機能を使用して、Orchestrator システムとワークフローに関するメトリック データを収集します。

前提条件

1 Orchestrator Appliance で Wavefront が有効であることを確認します。詳細については、OpenTracing と Wavefront 拡張機能の有効化を参照してください。

2 Wavefront 証明書を次のようにインポートします。

   a Orchestrator コントロール センターに **root** としてログインします。

   b [証明書] 画面に移動します。

   c [インポート] ドロップダウン メニューをクリックして、[URL からのインポート] を選択します。

   d Wavefront URL を入力し、[インポート] をクリックします。

3 Wavefront プロキシを構成します。詳細については、Wavefront プロキシの構成を参照してください。

手順

1 Orchestrator コントロール センターに **root** としてログインします。

2 [拡張機能プロパティ] 画面に移動します。

3 Wavefront 拡張機能を選択します。

4 Wavefront プロパティを設定します。

オプション	説明
プロキシ	Wavefront プロキシ アドレス。
ホスト	任意。Wavefront ホスト アドレス。
トークン	任意。Wavefront API トークン。Wavefront API トークンの生成の詳細については、API トークンの生成を参照してください。
プリフィックス	Wavefront に送信されたメトリックごとにプリフィックス ラベルを追加します。プリフィックス ラベルは、ドット記号で区切ります。

5 （オプション）[次の開始時にデフォルトのダッシュボードを送信する] を選択します。

6 [保存] をクリックします。

結果

Orchestrator Wavefront 拡張機能が構成されました。

次のステップ

- Wavefront によって収集されたメトリックにアクセスするには、構成時に入力したアドレスでダッシュボードにアクセスします。

- Orchestrator 環境内の特定のイベントに関する通知を取得するには、Wavefront アラートを使用できます。詳細については、Wavefront アラートのドキュメントを参照してください。

構成の使用事例とトラブルシューティング

8

Orchestrator サーバを vCenter Server アプライアンスと連携するように構成できます。また、Orchestrator からプラグインをアンインストールしたり、自己署名の証明書を変更したりすることもできます。

構成の使用事例では、Orchestrator サーバの特定の構成要件に適合させるために実行できるタスク フローを紹介します。また、トラブルシューティングのトピックでは、問題を理解し、回避策がある場合の対処方法について説明します。

この章には、次のトピックが含まれています。

vSphere Web Client の vRealize Orchestrator プラグインの構成

vSphere Web Client に対して vRealize Orchestrator プラグインを使用するには、vRealize Orchestrator を vCenter Server の拡張機能として登録する必要があります。

vRealize Orchestrator サーバを vCenter Single Sign-On に登録し、vCenter Server と連携するように構成したら、vRealize Orchestrator を vCenter Server の拡張機能として登録する必要があります。

前提条件

管理対象 vCenter Server の認証に使用されるものと同じ Platform Services Controller に、vSphere 認証を使用して vRealize Orchestrator を登録する必要があります。

手順

1. vRealize Orchestrator Client にログインします。
2. [ライブラリ] - [ワークフロー] の順に移動します。
3. [vCenter Orchestrator を vCenter Server エクステンションとして登録] ワークフローを見つけ、[実行] をクリックします。
4. vRealize Orchestrator を登録する vCenter Server インスタンスを選択します。
5. （オプション） https://*your_orchestrator_hostname*:8281 を入力するか、要求を vRealize Orchestrator サーバ ノードにリダイレクトするロード バランサのサービス URL を入力します。
6. [実行] をクリックします。

Orchestrator 認証の登録解除

シングル サインオン ソリューションとして使用している Orchestrator を登録解除するには、コントロール センターの [認証プロバイダを設定] ページを使用します。

Orchestrator vCenter Single Sign-On 認証または vRealize Automation 認証を再設定する場合は、まず Orchestrator 認証を登録解除する必要があります。

手順

1. コントロール センターに **root** としてログインします。
2. [認証プロバイダを設定] をクリックします。
3. [登録解除] をクリックします。
4. （オプション） 登録データを ID サーバから削除するには、認証情報を入力します。
5. [ID サービス] セクションで [登録解除] をクリックします。

結果

Orchestrator サーバ インスタンスが正常に登録解除されました。

SSL 証明書の変更

デフォルトでは、Orchestrator サーバは自己署名の SSL 証明書を使用して、Orchestrator クライアントとリモートで通信します。たとえば、会社のセキュリティ ポリシーにより SSL 証明書を使用する必要がある場合に、SSL 証明書を変更できます。

信頼されている SSL インターネット接続経由で Orchestrator を使用し、Web ブラウザでコントロール センターを開こうとすると、Mozilla Firefox を使用している場合は、接続が信頼されていないことを示す警告が出され、Internet Explorer を使用している場合は、Web サイトのセキュリティ証明書でその問題が検出されたことを示す警告が出されます。

[このサイトの閲覧を続行する（推奨されません）] をクリックすると、トラスト ストアに SSL 証明書をインポートした場合でも、Web ブラウザのアドレス バーに証明書エラー通知が赤で表示され続けます。Orchestrator は Web ブラウザで操作することもできますが、HTTPS 経由で API にアクセスしようとすると、サードパーティ システムが正常に機能しない可能性があります。

また、Orchestrator クライアントを起動して、SSL 接続経由で Orchestrator サーバに接続しようとした場合も、証明書の警告が出されることがあります。

この問題を解決するには、商用認証局 (CA) によって署名された証明書をインストールします。Orchestrator クライアントから出される証明書の警告を停止するには、Orchestrator クライアントがインストールされているマシン上の Orchestrator キーストアにルート CA 証明書を追加します。

ローカル ストアへの証明書の追加

認証局 (CA) から証明書を受け取ったら、コントロール センターを操作する際に証明書の警告やエラー メッセージが出ないようにするために、その証明書をローカル ストレージに追加しておく必要があります。

このワークフローでは、Internet Explorer を使用して証明書をローカル ストレージに追加する操作について説明します。

1 Internet Explorer を開き、https://*orchestrator_server_IP_or_DNS_name*:8283/ にアクセスします。

2 [このサイトの閲覧を続行する（推奨されません）] が表示されたら、これをクリックします。

Internet Explorer のアドレス バーの右側に証明書エラーが表示されます。

3 [証明書エラー] をクリックし、[証明書の表示] を選択します。

4 [証明書をインストール] をクリックします。

5 [証明書インポート ウィザード] の [ようこそ] ページで、[次へ] をクリックします。

6 [証明書ストア] ウィンドウで [証明書をすべて次のストアに配置する] を選択します。

7 [信頼されたルート証明書機関] を参照して選択します。

8 ウィザードを完了し、Internet Explorer を再起動します。

9 SSL 接続経由で Orchestrator サーバに移動します。

警告も、アドレス バーの証明書エラーも表示されなくなりました。

VMware Service Manager などのその他のアプリケーションおよびシステムは、SSL 接続で Orchestrator REST API にアクセスできる必要があります。

Orchestrator Appliance 管理サイトの証明書の変更

Orchestrator Appliance は、Light HTTPd を使用してその管理サイトを稼動させます。たとえば、会社のセキュリティ ポリシーにより SSL 証明書を使用する必要がある場合に、Orchestrator Appliance 管理サイトの SSL 証明書を変更できます。

前提条件

デフォルトでは、Orchestrator Appliance SSL 証明書とプライベート キーは、/opt/vmware/etc/lighttpd/server.pem にある PEM ファイルに保存されます。新しい証明書をインストールするには、必ず Java キーストアから PEM ファイルへ新しい SSL 証明書とプライベート キーをエクスポートしてください。

手順

1 Orchestrator Appliance Linux コンソールに root としてログインします。

2 /opt/vmware/etc/lighttpd/lighttpd.conf ファイルを見つけ出して、エディタで開きます。

3 次の行を検索します。

```
#### SSL engine
ssl.engine = "enable"
ssl.pemfile = "/opt/vmware/etc/lighttpd/server.pem"
```

4 新しい SSL 証明書とプライベート キーが含まれている PEM ファイルを指すように、ssl.pemfile 属性を変更します。

5 lighttpd.conf ファイルを保存します。

6 次のコマンドを実行して、light-httpd サーバを再起動します。

```
service vami-lighttp restart
```

結果

Orchestrator Appliance 管理サイトの証明書が正常に変更されました。

実行中のワークフローのキャンセル

コントロール センターを使用すると、適切に終了しなかったワークフローをキャンセルできます。

手順

1 コントロール センターに **root** としてログインします。

2 [トラブルシューティング] をクリックします。

3 実行中のワークフローをキャンセルします。

オプション	説明
すべてのワークフローの実行をキャンセル	ワークフロー ID を入力し、そのワークフローのすべてのトークンをキャンセルします。
ID を使用してワークフローの実行をキャンセル	キャンセルするすべてのトークン ID を入力します。ID はコンマで区切ります。
すべての実行中のワークフローをキャンセル	サーバ上で実行中のすべてのワークフローをキャンセルします。

注： 実行中のスレッドをすぐにキャンセルできる確実な方法がないため、ID を使用してワークフローをキャンセルする操作は正常に完了しない可能性があります。

結果

次回のサーバ起動時に、ワークフローはキャンセルされた状態に設定されます。

次のステップ

コントロール センターの [ワークフローの確認] ページから、ワークフローがキャンセルされたことを確認してください。

Orchestrator サーバのデバッグの有効化

プラグインの開発時に問題をデバッグするには、Orchestrator サーバをデバッグ モードで起動します。

手順

1 コントロール センターに **root** としてログインします。

2 [Orchestrator のデバッグ] をクリックします。

3 [デバッグを有効化] をクリックします。

4 （オプション） デフォルト ポート以外の任意のポートを入力します。

5 （オプション） [中断] をクリックします。

このオプションを選択して、Orchestrator サーバの起動前にデバッガを接続する必要があります。

6 [保存] をクリックします。

7 コントロール センターの [起動オプション] ページを開き、[再起動] をクリックします。

結果

リモート Java デバッガを定義済みのポートに接続するまで、Orchestrator サーバの起動は中断されます。

Orchestrator の構成および要素のバックアップ

カスタムの Orchestrator サーバの構成およびワークフロー要素をバックアップし、他の Orchestrator インスタンスが再利用できるようにしてください。

任意の標準ワークフロー、アクション、ポリシー、または構成要素を編集した後で、バージョン番号の新しい Orchestrator と同じ要素が含まれているパッケージをインポートすると、各要素に対して行った変更内容が失われます。Orchestrator インスタンスを移行する前にエクスポートすることで、カスタマイズされたワークフローおよびその他の要素の損失を防ぐことができます。

各 Orchestrator サーバ インスタンスには一意の証明書が含まれ、各 vCenter Server プラグイン インスタンスには一意の ID が含まれています。証明書および一意の ID によって、Orchestrator サーバの ID と vCenter Server プラグインを定義します。Orchestrator 要素のバックアップまたはバックアップを目的とした Orchestrator 構成のエクスポートを実行しない場合は、これらの ID を必ず変更してください。

前提条件

新しい Orchestrator サーバ インスタンスを展開して、構成します。スタンドアロン Orchestrator サーバの構成を参照してください。

手順

1 Orchestrator 構成をエクスポートします。

a コントロール センターに **root** としてログインします。

b [設定をエクスポート/インポート] をクリックします。

c エクスポートするファイルのタイプを選択します。

d （オプション） パスワードを入力して、構成ファイルを保護します。

構成をインポートするときは同一のパスワードを使用します。

e [エクスポート] をクリックします。

2 Orchestrator のクライアント アプリケーションにログインします。

3 作成または編集したすべての Orchestrator 要素を含むパッケージを作成します。

a [管理者] ビューで、[パッケージ] タブをクリックします。

b [パッケージ] リストのタイトル バーにあるメニュー ボタンをクリックし、[パッケージの追加] を選択します。

c 新しいパッケージの名前を入力して [OK] をクリックします。

パッケージ名の構文は *domain.your_company.folder.package_name* になります。

たとえば、`com.vmware.myfolder.mypackage` という名前を付けます。

d パッケージを右クリックして [編集] を選択します。

e [全般] タブでパッケージの説明を追加します。

f [ワークフロー] タブでワークフローをパッケージに追加します。

g （オプション） ポリシー テンプレート、アクション、構成要素、リソース要素、アクセス権、およびプラグインをパッケージに追加します。

h [保存して閉じる] をクリックします。

4 パッケージをエクスポートします。

a エクスポートするパッケージを右クリックして、[パッケージをエクスポート] を選択します。

b パッケージを保存する場所を参照して選択します。

c （オプション） 対応する証明書を使用してパッケージに署名します。

d （オプション） エクスポートしたパッケージに制限を適用します。

e （オプション） エクスポートしたパッケージのコンテンツに制限を適用するには、必要に応じてオプションを選択解除します。

オプション	説明
[バージョン履歴をエクスポート]	オフにすると、パッケージのバージョン履歴はエクスポートされません。
[構成設定の値をエクスポート]	オフにすると、パッケージ内の構成要素の属性値はエクスポートされません。
[グローバル タグをエクスポート]	オフにすると、パッケージ内のグローバル タグはエクスポートされません。

注： [SecureString 構成設定の値をエクスポート] オプションは、デフォルトで選択解除されています。これらの構成設定をエクスポートすると、セキュリティ上の問題が発生する可能性があります。慎重に使用してください。

f [保存] をクリックします。

5 先ほどエクスポートした Orchestrator 構成を、新しい Orchestrator サーバ インスタンスにインポートします。

a Orchestrator インスタンスのコントロール センターに **root** としてログインします。

b [設定をエクスポート/インポート] をクリックして、[設定をインポート] タブに移動します。

c 以前のインストールでエクスポートした .zip ファイルを参照して選択します。

d 構成をエクスポートしたときに使用したパスワードを入力します。

パスワードを指定していなかった場合はこのステップは必要ありません。

e インポート タイプを選択します。

f [インポート] をクリックします。

6 新しい Orchestrator インスタンスにエクスポートしたパッケージをインポートします。

a 新しい Orchestrator インスタンスの Orchestrator クライアント アプリケーションにログインします。

b Orchestrator クライアントのドロップダウン メニューから、[管理者] を選択します。

c [パッケージ] タブをクリックします。

d [パッケージ] リストのタイトル バーにあるメニュー ボタンをクリックし、[パッケージのインポート] を選択します。

e インポートするパッケージを参照して選択し、[開く] をクリックします。

エクスポータの証明書情報が表示されます。

f パッケージのインポートに関する詳細を確認し、[インポート] または [インポートしてプロバイダを信頼] を選択します。

[パッケージのインポート] ビューが表示されます。インポートされたパッケージ要素のバージョンがサーバ上のバージョンより新しい場合は、インポート対象の要素が自動的に選択されます。

g インポートする要素を選択します。

注： カスタム要素に新しいバージョンがある場合は、選択解除します。

h （オプション） パッケージから構成要素の属性値をインポートしない場合は、[構成の値をインポートする] チェック ボックスをオフにします。

i ドロップダウン メニューから、パッケージに含まれるタグをインポートするかどうかを選択します。

オプション	説明
[タグをインポートするが既存の値を保持]	既存のタグ値を上書きせずに、パッケージからタグをインポートします。
[タグをインポートして既存の値を上書き]	パッケージからタグをインポートして、値を上書きします。
[タグをインポートしない]	パッケージからタグをインポートしません。

j [選択した要素のインポート] をクリックします。

結果

これで、Orchestrator の構成および要素のバックアップが正常に完了しました。

vRealize Orchestrator のバックアップとリストア

vSphere Data Protection を使用すると、vRealize Orchestrator インスタンスが含まれている仮想マシン (VM) をバックアップおよびリストアできます。

vSphere Data Protection は、vSphere 環境向けに設計された VMware ディスク ベースのバックアップおよびリカバリ ソリューションです。vSphere Data Protection は vCenter Server に完全に統合されています。vSphere Data Protection を使用すると、バックアップ ジョブを管理でき、重複解除したストレージ先にバックアップを保存できます。vSphere Data Protection を導入して構成した後、vSphere Web Client インターフェイスを使用して vSphere Data Protection にアクセスすると、仮想マシンのバックアップとリカバリを選択、スケジュール、設定、および管理できます。vSphere Data Protection はバックアップ中に仮想マシンの静止スナップショットを作成します。バックアップ操作を行うたびに重複解除が自動的に実行されます。

vSphere Data Protection を導入および設定する方法については、『vSphere Data Protection 管理ガイド』を参照してください。

vRealize Orchestrator のバックアップ

vRealize Orchestrator インスタンスは仮想マシンとしてバックアップできます。

単一製品内で 1 台の仮想マシンのすべてのコンポーネントをまとめてバックアップするには、vRealize Orchestrator 環境の仮想マシンを単一の vCenter Server フォルダに保存し、そのフォルダ用のバックアップ ポリシー ジョブを作成します。

前提条件

- vSphere Data Protection アプライアンスが導入および構成されていることを確認します。vSphere Data Protection を導入および構成する方法については、『vSphere Data Protection 管理ガイド』を参照してください。

- vSphere Web Client を使用して、環境を管理している vCenter Server インスタンスにログインします。vSphere Data Protection の構成中に使用した管理者権限を持つユーザーとしてログインします。

手順

1. vSphere Web Client のホーム ページで、[vSphere Data Protection] をクリックします。
2. [VDP アプライアンス] ドロップダウン メニューで vSphere Data Protection アプライアンスを選択し、[接続] をクリックします。
3. [はじめに] タブで、[バックアップ ジョブの作成] をクリックします。
4. [ゲスト イメージ] をクリックして vRealize Orchestrator インスタンスをバックアップし、[次へ] をクリックします。
5. [完全なイメージ] を選択して仮想マシン全体をバックアップし、[次へ] をクリックします。
6. [仮想マシン] ツリーを展開し、vRealize Orchestrator 仮想マシンのチェック ボックスをオンにします。
7. 表示される指示に従ってバックアップ スケジュール、保持ポリシー、バックアップ ジョブ名を設定します。

   仮想マシンをバックアップおよびリストアする方法については、『vSphere Data Protection 管理ガイド』を参照してください。

   バックアップ ジョブは [バックアップ] タブのバックアップ ジョブ リストに表示されます。
8. （オプション）[バックアップ] タブを開いてバックアップ ジョブを選択し、[今すぐバックアップ] をクリックして vRealize Orchestrator をバックアップします。

   注： 設定しているスケジュールに従ってバックアップが自動的に開始されるのを待機することもできます。

   バックアップ プロセスは [最近のタスク] ページに表示されます。

結果

仮想マシンのイメージは [リストア] タブのバックアップ リストに表示されます。

次のステップ

[リストア] タブを開いて、仮想マシンのイメージがバックアップ リストに表示されていることを確認します。

vRealize Orchestrator インスタンスのリストア

同じ vCenter Server の元の場所または別の場所にある vRealize Orchestrator インスタンスはリストアできます。

前提条件

- vSphere Data Protection アプライアンスが導入および構成されていることを確認します。vSphere Data Protection を導入および構成する方法については、『vSphere Data Protection 管理ガイド』を参照してください。
- vRealize Orchestrator インスタンスをバックアップします。 vRealize Orchestrator のバックアップを参照してください。

- vSphere Web Client を使用して、環境を管理している vCenter Server インスタンスにログインします。vSphere Data Protection の構成中に使用した管理者権限を持つユーザーとしてログインします。

手順

1. vSphere Web Client のホーム ページで、[vSphere Data Protection] をクリックします。
2. [VDP アプライアンス] ドロップダウン メニューで vSphere Data Protection アプライアンスを選択し、[接続] をクリックします。
3. [リストア] タブを開きます。
4. バックアップ ジョブ リストで、リストアする vRealize Orchestrator バックアップを選択します。

   注： 仮想マシンが複数存在する場合は、仮想マシンが同期されるように複数同時にリストアする必要があります。

5. 同じ vCenter Server に存在する vRealize Orchestrator インスタンスをリストアするには、[リストア] アイコンをクリックし、プロンプトの指示に従って、vRealize Orchestrator のリストア先となる vCenter Server の場所を設定します。

   アプライアンスは最後にパワーオンする必要があるため、[パワーオン] は選択しないでください。仮想マシンをバックアップおよびリストアする方法については、『vSphere Data Protection 管理ガイド』を参照してください。

   リストアが正常に開始されたことを示すメッセージが表示されます。
6. （オプション）外部データベース ホストを使用している場合は、データベース ホストをパワーオンして、ロードバランサ構成をリストアします。
7. vRealize Orchestrator Appliance をパワーオンします。

結果

リストアされた vRealize Orchestrator 仮想マシンが vCenter Server インベントリに表示されます。

次のステップ

コントロール センターの [設定を検証] ページで vRealize Orchestrator が正しく設定されていることを確認します。

Site Recovery Manager を使用した Orchestrator のディザスタ リカバリ

vRealize Orchestrator を保護するように Site Recovery Manager を構成する必要があります。Site Recovery Manager の一般的な構成タスクを実行して保護します。

環境の準備

Site Recovery Manager の構成を開始する前に、以下の前提条件を満たしておく必要があります。

- 保護されたサイトとリカバリ サイトに vSphere 5.5 がインストールされていることを確認します。

- Site Recovery Manager 5.8 を使用していることを確認します。
- vRealize Orchestrator が構成されていることを確認します。

vSphere Replication のための仮想マシンの構成

Site Recovery Manager を使用するためには、vSphere Replication またはアレイ ベースのレプリケーションに対応するように仮想マシンを構成する必要があります。

必要な仮想マシンで vSphere Replication を有効にするには、次の手順を実行します。

手順

1. vSphere Web Client で vSphere Replication を有効にする仮想マシンを選択し、[アクション] - [vSphere Replication のすべてのアクション] - [レプリケーションの構成] の順にクリックします。
2. [レプリケーション タイプ] ウィンドウで [vCenter Server にレプリケート] を選択し、[次へ] をクリックします。
3. [ターゲット サイト] ウィンドウでリカバリ サイトの vCenter を選択し、[次へ] をクリックします。
4. [レプリケーション サーバ] ウィンドウで vSphere Replication サーバを選択し、[次へ] をクリックします。
5. [ターゲットの場所] ウィンドウで [編集] をクリックし、レプリケートしたファイルを保存する先のターゲット データストアを選択し、[次へ] をクリックします。
6. [レプリケーション オプション] ウィンドウでデフォルト設定をそのまま保持し、[次へ] をクリックします。
7. [リカバリ設定] ウィンドウで、[リカバリ ポイント目標 (RPO)] と [ポイント イン タイム インスタンス] の時間を入力し、[次へ] をクリックします。
8. [設定内容の確認] ウィンドウで設定を確認し、[完了] をクリックします。
9. vSphere Replication を有効にする必要があるすべての仮想マシンについて、上記の手順を繰り返します。

保護グループの作成

Site Recovery Manager が仮想マシンを保護できるようにするには、保護グループを作成します。

保護グループを作成する場合、この処理が想定どおりに完了するまで待機します。Site Recovery Manager が保護グループを作成すること、およびグループ内の仮想マシンが正常に保護されていることを確認します。

前提条件

次のいずれかのタスクを実行したことを確認します。

- アレイ ベースのレプリケーションを構成するデータストアに仮想マシンを含めていること
- 仮想マシンで vSphere Replication を構成したこと
- 両方の組み合わせを実行したこと

手順

1. vSphere Web Client で、[サイト リカバリ] > [保護グループ] の順に選択します。
2. [オブジェクト] タブで、保護グループを作成するためのアイコンをクリックします。

3 [保護グループ タイプ] ページで保護サイトを選択し、レプリケーション タイプを選択して、[次へ] をクリックします。

オプション	アクション
アレイ ベースのレプリケーション グループ	[アレイ ベースのレプリケーション (ABR)] を選択し、アレイのペアを選択します。
vSphere Replication 保護グループ	[vSphere Replication] を選択します。

4 保護グループに追加するデータストア グループまたは仮想マシンを選択します。

オプション	アクション
アレイ ベースのレプリケーションの保護グループ	データストア グループを選択し、[次へ] をクリックします。
vSphere Replication 保護グループ	リストから仮想マシンを選択し、[次へ] をクリックします。

vSphere Replication 保護グループを作成すると、vSphere Replication 用に構成した仮想マシンのうち、まだ保護グループに含まれていないもののみが、リストに表示されます。

5 設定を確認し、[完了] をクリックします。

保護グループ作成の進捗状況は、[保護グループ] の [オブジェクト] タブで監視できます。

結果

- Site Recovery Manager が保護された仮想マシンにインベントリ マッピングを正常に適用した場合は、保護グループの保護ステータスが [OK] になります。
- Site Recovery Manager が、ストレージ ポリシーに関連付けられているすべての仮想マシンを正常に保護した場合は、保護グループの保護ステータスが [OK] になります。

リカバリ プランの作成

リカバリ プランを作成して、Site Recovery Manager による仮想マシンのリカバリ方法を確立します。

手順

1 vSphere Web Client で、[サイト リカバリ] > [リカバリ プラン] の順に選択します。

2 [オブジェクト] タブで、リカバリ プランを作成するためのアイコンをクリックします。

3 プランの名前と説明を入力し、フォルダを選択して、[次へ] をクリックします。

4 リカバリ サイトを選択して、[次へ] をクリックします。

5 メニューからグループ タイプを選択します。

オプション	説明
仮想マシンの保護グループ	アレイ ベースのレプリケーションと vSphere Replication 保護グループが含まれているリカバリ プランを作成するには、このオプションを選択します。
ストレージ ポリシーの保護グループ	ストレージ ポリシーの保護グループが含まれているリカバリ プランを作成するには、このオプションを選択します。

デフォルトは [仮想マシンの保護グループ] です。

注： ストレッチ ストレージを使用している場合は、グループ タイプとして [仮想マシンの保護グループ] を選択します。

6 このプランで復旧する保護グループを 1 つ以上選択し、[次へ] をクリックします。

7 [テスト ネットワーク] の値をクリックし、リカバリ テスト中に使用するネットワークを選択して、[次へ] をクリックします。

デフォルト オプションでは、隔離されたネットワークが自動的に作成されます。

8 概要情報を確認し、[終了] をクリックして、リカバリ プランを作成します。

リカバリ プランのフォルダの整理

リカバリ プランを整理するためのフォルダを作成することができます。

リカバリ プランが多数存在する場合は、フォルダを使用してリカバリ プランを整理すると便利です。リカバリ プランへのアクセスを制限するには、リカバリ プランをフォルダに入れて、フォルダに対する権限をユーザーまたはグループごとに割り当てます。

手順

1 vSphere Web Client のホーム ビューで、[サイト リカバリ] をクリックします。

2 [インベントリ ツリー] を展開し、[リカバリ プラン] をクリックします。

3 [関連オブジェクト] タブを選択し、[フォルダ] をクリックします。

4 [フォルダの作成] アイコンをクリックし、作成するフォルダの名前を入力して、[OK] をクリックします。

5 新規または既存のリカバリ プランをフォルダに追加します。

オプション	説明
新しいリカバリ プランの作成	フォルダを右クリックし、[リカバリ プランの作成] を選択します。
既存のリカバリ プランの追加	リカバリ プランをインベントリ ツリーからフォルダにドラッグ アンド ドロップします。

6 （オプション） フォルダを名前変更または削除するには、フォルダを右クリックして [フォルダ名の変更] または [フォルダの削除] を選択します。

フォルダは空の場合にのみ削除できます。

リカバリ プランの編集

リカバリ プランを編集して、そのリカバリ プランの作成時に指定したプロパティを変更することができます。リカバリ プランは、保護サイトまたはリカバリ サイトから編集できます。

手順

1 vSphere Web Client で、[サイト リカバリ] > [リカバリ プラン] の順に選択します。

2 リカバリ プランを右クリックし、[プランを編集] を選択します。

リカバリ プランの編集は、[監視] タブの [リカバリ手順] ビューで [リカバリ プランを編集] アイコンをクリックして行うこともできます。

3 （オプション） [リカバリ プラン名] テキスト ボックスでプランの名前または説明を変更し、[次へ] をクリックします。

4 [リカバリ サイト] ページで、[次へ] をクリックします。

リカバリ サイトは変更できません。

5 （オプション） プランに追加するかプランから削除する保護グループを 1 つ以上選択または選択解除し、[次へ] をクリックします。

6 （オプション） テスト ネットワークをクリックしてリカバリ サイト上の異なるテスト ネットワークを選択し、[次へ] をクリックします。

7 概要情報を確認して [終了] をクリックし、指定した変更をリカバリ プランに加えます。

プランの更新は [最近のタスク] ビューで監視できます。

システム プロパティの設定

9

システム プロパティを設定することにより、Orchestrator のデフォルトの動作を変更することができます。

この章には、次のトピックが含まれています。

管理者以外による Orchestrator クライアントへのアクセスの無効化

Orchestrator 管理者グループのメンバーでないすべてのユーザーが Orchestrator クライアントにアクセスするのを拒否するように、Orchestrator サーバを設定できます。

デフォルトでは、実行権限が付与されたすべてのユーザーが、Orchestrator クライアントにアクセスできます。ただし、Orchestrator 構成システム プロパティを設定することによって、Orchestrator 管理者のみが Orchestrator クライアントにアクセスできるように制限できます。

重要： プロパティが構成されていない場合、またはプロパティが false に設定されている場合は、すべてのユーザーによる Orchestrator クライアントへのアクセスが許可されます。

手順

1 コントロール センターに **root** としてログインします。

2 [システム プロパティ] をクリックします。

3 [追加] アイコン（ + ）をクリックします。

4 [キー] テキスト ボックスに **com.vmware.o11n.smart-client-disabled** と入力します。

5 [値] テキスト ボックスに **true** と入力します。

6 （オプション） [説明] テキスト ボックスに、**Orchestrator クライアント接続の無効化**と入力します。

7 [追加] をクリックします。

8 ポップアップ メニューから [変更を保存] をクリックします。

正常に保存されたことを示すメッセージが表示されます。

9 Orchestrator サーバを再起動します。

結果

Orchestrator 管理者グループのメンバー以外のすべてのユーザーによる Orchestrator クライアントへのアクセスが無効になりました。

ワークフローとアクションからサーバ ファイル システムにアクセスするための設定

Orchestrator では、ワークフローとアクションからの特定のファイル システム ディレクトリへのアクセスが制限されます。`js-io-rights.conf` Orchestrator 構成ファイルを変更することにより、アクセス範囲を拡大して、サーバ ファイル システムの他の場所にアクセスすることができます。

Orchestrator システムへの書き込みアクセスを許可する、js-io-rights.conf ファイル内のルール

`js-io-rights.conf` ファイルには、サーバ ファイル システム内の定義されたディレクトリに対する書き込みアクセスを許可するルールが含まれています。

重要： `js-io-rights.conf` ファイルを変更する前に、vRealize Orchestrator コントロール センター サービスを停止する必要があります。そうしないと、`js-io-rights.conf` ファイルはデフォルト構成に戻ります。ワークフローとアクションからサーバ ファイル システムにアクセスするための設定を参照してください。

js-io-rights.conf ファイルの必須の内容

`js-io-rights.conf` ファイルの各行には、次の情報を含める必要があります。

- 権限を許可するのか、それとも拒否するのかを示すプラス (+) またはマイナス (-) の記号
- 権限に対する読み取り (r)、書き込み (w)、および実行 (x) のレベル
- 権限を適用するパス

js-io-rights.conf ファイルのデフォルトの内容

Orchestrator Appliance の `js-io-rights.conf` 構成ファイルのデフォルトの内容は、次のとおりです。

```
-rwx /
+rwx /var/run/vco
-rwx /etc/vco/app-server/security/
+rx /etc/vco
+rx /var/log/vco/
```

デフォルトの js-io-rights.conf 構成ファイルの先頭の 2 行は、次のアクセス権を許可します。

-rwx /

ファイル システムへのすべてのアクセスは拒否されます。

+rwx /var/run/vco

/var/run/vco ディレクトリでの読み取り、書き込み、実行のアクセスは許可されます。

js-io-rights.conf ファイル内のルール

Orchestrator は、js-i/o-rights.conf ファイルに記述されている順序でアクセス権を解決します。各行は前の行をオーバーライドできます。

重要： ファイル システムのすべての部分へのアクセスを許可するには、js-i/o-rights.conf ファイルで +rwx / を設定します。ただし、これを行うとセキュリティ リスクが増加します。

ワークフローとアクションからサーバ ファイル システムにアクセスするための設定

ワークフローと vRealize Orchestrator API がアクセスできるサーバ ファイル システムの場所を変更するには、js-io-rights.conf 構成ファイルを変更します。js-io-rights.conf ファイルは、ワークフローが vRealize Orchestrator サーバ ファイル システムへのアクセスを試みる際に作成されます。

手順

1. vRealize Orchestrator Appliance Linux コンソールに root ユーザーとしてログインします。
2. vRealize Orchestrator コントロール センター サービスを停止します。

   ```
   service vco-configurator stop
   ```

3. /etc/vco/app-server に移動します。
4. js-io-rights.conf 構成ファイルをテキスト エディタで開きます。
5. js-io-rights.conf ファイルに必要な行を追加します。

   たとえば、以下の行は */path_to_folder*/noexec ディレクトリ内に対する実行権限を拒否します。

   ```
   -x /path_to_folder/noexec
   ```

   /path_to_folder/noexec に対する実行権限は保持されますが、*/path_to_folder*/noexec/bar に対しては保持されません。どちらのディレクトリも読み取りと書き込みは引き続き可能です。
6. 変更を適用するには、次のコマンドを実行します。

   ```
   /var/lib/vco/tools/configuration-cli/bin/vro-configure.sh sync-local
   ```

7. vRealize Orchestrator コントロール センター サービスを開始します。

   ```
   service vco-configurator start
   ```

結果

ワークフローと vRealize Orchestrator API のファイル システムへのアクセス権が変更されました。

ワークフローとアクションからオペレーティング システム コマンドにアクセスするための設定

Orchestrator API には、Orchestrator サーバ ホストのオペレーティング システム上で各種のコマンドを実行するための Command というスクリプト クラスが用意されています。Orchestrator サーバ ホストに対する無許可のアクセスを防ぐため、デフォルトで、Orchestrator アプリケーションには Command クラスを実行するための権限が設定されていません。ホストのオペレーティング システム上でコマンドを実行するための権限が Orchestrator アプリケーションに必要な場合は、Command スクリプト クラスを有効にします。

Command クラスを使用する権限を付与するには、Orchestrator 構成のシステム プロパティを設定します。

手順

1 コントロール センターに **root** としてログインします。

2 [システム プロパティ] をクリックします。

3 [追加] アイコン（ + ）をクリックします。

4 [キー] テキスト ボックスに **com.vmware.js.allow-local-process** と入力します。

5 [値] テキスト ボックスに **true** と入力します。

6 [説明] テキスト ボックスにシステム プロパティの説明を入力します。

7 [追加] をクリックします。

8 ポップアップ メニューから [変更を保存] をクリックします。

正常に保存されたことを示すメッセージが表示されます。

9 Orchestrator サーバを再起動します。

結果

Orchestrator サーバ ホストのオペレーティング システムでローカル コマンドを実行する権限が Orchestrator アプリケーションに付与されました。

注： com.vmware.js.allow-local-process システム プロパティを true に設定すると、Command スクリプト クラスでファイル システムのすべての場所での書き込みが許可されます。このプロパティは、js-io-rights.conf ファイルで Command スクリプト クラスにのみ設定しているファイル システム アクセス権限より優先されます。Command を除くすべてのスクリプト クラスでは、js-io-rights.conf ファイルで設定しているファイル システム アクセス権限は引き続き適用されます。

JavaScript から Java クラスにアクセスするための設定

デフォルトでは、Orchestrator の JavaScript からアクセスできる Java クラスのセットは制限されています。JavaScript からさまざまな Java クラスにアクセスするには、そのための Orchestrator システム プロパティを設定する必要があります。

JavaScript エンジンに Java 仮想マシン（JVM）へのフル アクセスを許可すると、セキュリティ上の問題が発生することがあります。不正な形式のスクリプトや悪意のあるスクリプトが、Orchestrator サーバを実行するユーザーがアクセスできるすべてのシステム コンポーネントへのアクセス権を取得する可能性があります。そのため、デフォルトでは、Orchestrator JavaScript エンジンは `java.util.*` パッケージ内のクラスにのみアクセスできます。

JavaScript が `java.util.*` パッケージの外部にあるクラスにアクセスする必要がある場合は、JavaScript からアクセスできるようにする Java パッケージのリストを構成ファイル内に記載できます。その後、このファイルを指すように `com.vmware.scripting.rhino-class-shutter-file` システム プロパティを設定します。

手順

1 JavaScript からアクセスできるようにする Java パッケージのリストを格納するためのテキスト構成ファイルを作成します。

たとえば、JavaScript から `java.net` パッケージ内のすべてのクラスと `java.lang.Object` クラスにアクセスできるようにするには、このファイルに次の内容を追加します。

```
java.net.*
java.lang.Object
```

2 この構成ファイルを適切な名前で、適切な場所に保存します。

3 コントロール センターに **root** としてログインします。

4 [システム プロパティ] をクリックします。

5 [追加] アイコン（  ）をクリックします。

6 [キー] テキスト ボックスに **com.vmware.scripting.rhino-class-shutter-file** と入力します。

7 [値] テキスト ボックスに構成ファイルへのパスを入力します。

8 [説明] テキスト ボックスにシステム プロパティの説明を入力します。

9 [追加] をクリックします。

10 ポップアップ メニューから [変更を保存] をクリックします。

正常に保存されたことを示すメッセージが表示されます。

11 Orchestrator サーバを再起動します。

結果

JavaScript エンジンが指定された Java クラスにアクセスできるようになりました。

カスタム タイムアウト プロパティの設定

vCenter Server でオーバーロードが発生すると、Orchestrator サーバに応答を返す時間がデフォルトで設定されている 20,000 ミリ秒より長くなります。このような状況を回避するには、Orchestrator 構成ファイルを変更してデフォルトのタイムアウト期間を長くする必要があります。

特定の操作が完了する前にデフォルトのタイムアウト期間が切れると、Orchestrator サーバ ログにエラーが記録されます。

```
Operation 'getPropertyContent' total time : '5742228' for 1823 calls, mean time :
'3149.0', min time : '0', max time : '32313' Timeout, unable to get property 'info'
com.vmware.vmo.plugin.vi4.model.TimeoutException
```

手順

1 コントロール センターに **root** としてログインします。

2 [システム プロパティ] をクリックします。

3 [追加] アイコン（ + ）をクリックします。

4 [キー] テキスト ボックスに **com.vmware.vmo.plugin.vi4.waitUpdatesTimeout** と入力します。

5 [値] テキスト ボックスに新しいタイムアウト期間をミリ秒単位で入力します。

6 （オプション） [説明] テキスト ボックスにシステム プロパティの説明を入力します。

7 [追加] をクリックします。

8 ポップアップ メニューから [変更を保存] をクリックします。

正常に保存されたことを示すメッセージが表示されます。

9 Orchestrator サーバを再起動します。

結果

設定した値により、デフォルトのタイムアウト設定である 20,000 ミリ秒はオーバーライドされます。

次の手順

10

vRealize Orchestrator をインストールして構成すると、仮想環境を管理する際に頻繁に繰り返されるプロセスを Orchestrator を使用して自動化できます。

- Orchestrator クライアントにログインし、vCenter Server のインベントリ オブジェクトに対して、または Orchestrator がプラグインを介してアクセスする他のオブジェクトに対して、ワークフローの実行およびスケジュール設定を行います。『VMware vRealize Orchestrator クライアントの使用』を参照してください。
- Orchestrator の標準ワークフローを複製または変更し、独自のアクションやワークフローを作成して、vCenter Server での操作を自動化します。
- プラグインや Web サービスを作成し、Orchestrator プラットフォームを拡張します。
- vSphere Web Client を使用して、vSphere インベントリ オブジェクトに対してワークフローを実行します。

この章には、次のトピックが含まれています。

Orchestrator Appliance の Web コンソールから Orchestrator レガシー クライアントへのログイン

一般的な管理タスクの実行またはワークフローの編集と作成を行うには、Orchestrator レガシー クライアントのインターフェイスにログインする必要があります。

Orchestrator レガシー クライアント インターフェイスは、ワークフロー、アクション、およびその他のカスタム要素を開発するための管理権限を持つ開発者向けに設計されています。

重要： Orchestrator Appliance と Orchestrator レガシー クライアント コンピュータの間でクロックが同期されていることを確認します。

前提条件

- Orchestrator Appliance をダウンロードおよび展開します。
- アプライアンスが稼動し、実行されていることを確認します。

- Orchestrator レガシー クライアントを実行する Workstation に、64 ビットの Java をインストールします。

  注： 32 ビットの Java はサポートされていません。

手順

1. Web ブラウザで、Orchestrator Appliance 仮想マシンの IP アドレスに移動します。

   http://*orchestrator_appliance_ip*

2. [Orchestrator クライアントの起動] をクリックします。
3. [ホスト名]テキスト ボックスに Orchestrator Appliance の IP アドレスまたはドメイン名を入力します。

   デフォルトで Orchestrator Appliance の IP アドレスが表示されます。

4. Orchestrator レガシー クライアントのユーザー名とパスワードを使用してログインします。

   認証プロバイダとして vRealize Automation と vSphere のどちらを使用しているかに応じて、Orchestrator レガシー クライアントにログインするそれぞれの認証情報を入力します。

   Orchestrator 環境でマルチテナントが有効である場合は、それぞれのシステム管理者またはテナント管理者のユーザー名、パスワード、およびテナント ID を入力します。

5. [セキュリティ警告]ウィンドウで、証明書の警告を処理するためのオプションを選択します。

   Orchestrator レガシー クライアントは、SSL 証明書を使用して Orchestrator サーバと通信します。信頼性のある CA が、インストール中に証明書に署名することはありません。Orchestrator サーバに接続するたびに、証明書の警告を受信します。

オプション	説明
無視	現在の SSL 証明書を使用して続行します。 同じ Orchestrator サーバに再接続した場合、またはリモート Orchestrator サーバを使用してワークフローを同期しようとした場合は、警告メッセージが再度表示されます。
キャンセル	ウィンドウを閉じて、ログイン プロセスを停止します。
この証明書をインストールし、セキュリティ警告をこれ以上表示しない。	証明書をインストールし、セキュリティ警告が表示されないようにするには、このチェック ボックスを選択し、[無視] をクリックします。

   デフォルトの SSL 証明書を CA により署名された証明書に変更できます。SSL 証明書の変更の詳細については、『VMware vRealize Orchestrator のインストールおよび構成』を参照してください。

次のステップ

システムでパッケージのインポート、ワークフローの開始、または root アクセス権限の設定を行うことができます。