vRealize Orchestrator のマルチテナント

vRealize Orchestrator 7.6

vmware®

VMware Web サイトで最新の技術ドキュメントをご確認いただけます。
https://docs.vmware.com/jp/
VMware の Web サイトでは、最新の製品アップデートを提供しています。
本書に関するご意見、ご要望をお寄せください。フィードバック送信先：
docfeedback@vmware.com

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

内容

VMware vRealize Orchestrator のマルチテナント

1

「VMware vRealize Orchestrator のマルチテナント」には、 VMware® vRealize Orchestrator 7.4 で導入されたマルチテナント アーキテクチャに関する全般的な情報を掲載しています。

対象者

この情報は、 vRealize Automation システム管理者、テナント管理者、および Orchestrator の管理者を対象としています。

vRealize Orchestrator のマルチテナントの概要

vRealize Orchestrator 7.4 では、マルチテナント アーキテクチャが導入され、複数の vRealize Automation テナントが 1 つの外部または組み込みの vRealize Automation インスタンスを共有できようになりました。

テナントは、vRealize Automation 環境の組織単位です。vRealize Orchestrator 7.4 では、マルチテナント アーキテクチャが導入され、複数の vRealize Automation テナントが 1 つの外部または組み込みの vRealize Orchectration インスタンスを共有できようになりました。これは、Orchestrator によって認証プロバイダとして使用される vRealize Automation インスタンスです。vRealize Automation のマルチ テナントの詳細については、『vRealize Automation でのサービス ブループリントの準備と使用』の「テナントとユーザー ロール」を参照してください。

vRealize Automation のマルチテナント機能は、後方互換性を維持するためにデフォルトで無効になっています。これは、この機能を有効にすると製品のユーザー エクスペリエンスに大きな変化が生じるためです。vRealize Orchestrator のマルチテナントを有効にした場合、後から安全に無効にすることはできません。

注: マルチテナントを有効にした場合、vRealize Automation 認証のみがサポートされます。

vRealize Orchestrator のマルチテナントの有効化

2

認証プロバイダとして vRealize Automation を使用するように Orchestrator が構成されている場合にのみ、マルチテナントを有効にできます。マルチテナントは、デフォルトでは無効です。

vRealize Orchestrator マルチテナントの有効化

新しい vRealize Orchestrator のインストール環境は、シングルテナント モードで実行するように構成されます。Orchestrator をマルチ テナント モードで実行するには、明示的に有効にする必要があります。

注: マルチテナントを有効にすると、その変更を元に戻すことはできません。この機能の目的を認識していない場合は、有効にしないでください。

手順

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

2 Orchestrator サーバ サービスとコントロール センター サービスを停止します。

```
service vco-server stop && service vco-configurator stop
```

3 `/var/lib/vco/tools/configuration-cli/bin` ディレクトリに移動します。

```
cd /var/lib/vco/tools/configuration-cli/bin
```

4 マルチテナント機能を有効にするには、`vro-configure.sh` スクリプトを実行します。

```
./vro-configure.sh enable-multi-tenancy
```

5 Orchestrator サーバ サービスとコントロール センター サービスを開始します。

```
service vco-server start && service vco-configurator start
```

これで、vRealize Orchestrator マルチテナント機能が正常に有効になりました。

vRealize Orchestrator のテナントの分離

3

Orchestrator のマルチテナント機能は、テナント間で特定のレベルの分離を実現します。

マルチテナントを有効にすると、Orchestrator が管理するオブジェクトは、システム スコープとテナント固有のスコープに分割されます。これらのオブジェクトには、ワークフロー、アクション、パッケージ、構成、カテゴリ、ポリシー、ポリシー テンプレート、タスク、ワークフローの実行などがあります。

システム スコープ

システム スコープは、すべてのテナント間で共有されるすべての Orchestrator コンテンツを保持するセマンティック領域です。システム コンテンツには、次の項目が含まれます。

- すべてのオブジェクトがデフォルトの Orchestrator プラグインに含まれています。
- マルチテナント機能を有効にする前に作成されたカスタム オブジェクト。
- vRealize Automation のシステム管理者によって作成されたオブジェクト。
- システム テナントによって管理され、すべての非システム テナントによって読み取りおよび呼び出しできる事前定義済み自動化コンテンツ（ワークフロー、アクションなど）。

テナントには、このコンテンツに対する読み取り専用アクセス権があります。また、テナントがシステム スコープ オブジェクトを作成、変更、または削除することはできません。

テナント固有のスコープ

テナント固有のオブジェクトは、そのオブジェクトを作成したテナントに関連付けられます。これらのオブジェクトには、ワークフロー、アクション、ポリシー、ポリシー テンプレート、リソースなどがあります。テナントは、自身で作成したコンテンツを編集または削除できます。テナントは、システム コンテンツと自身のテナント固有のコンテンツを実行および表示できます。

テナントは、システム スコープ オブジェクトまたはその他のテナントによって作成されたオブジェクトを表示、編集、または削除することはできません。

マルチテナント環境の Orchestrator プラグイン

vRealize Orchestrator 7.4 は、Orchestrator プラグインとプラグインのインベントリ オブジェクトのマルチテナントをサポートしていません。プラグインインベントリに属するオブジェクトは、システム スコープの一部です。

注: プラグインのライブラリからワークフローを実行して作成したエンドポイントやインベントリ項目などのオブジェクトは、すべてのテナントが表示およびアクセスできます。

リソース割り当て

CPU、メモリ、ストレージ、ネットワーク バンド幅、データベース領域、ワークフローの実行の最大数、スレッド プールなどの Orchestrator サーバ リソースは、すべてのテナント間で共有されます。テナントのいずれかが、割り当てられたリソースの上限に達すると、同一の Orchestrator インスタンスを使用する、その他のすべてのテナントに影響します。

セキュリティ

vRealize Orchestrator 7.4 のテナント間のセキュリティ分離では、システム管理者およびテナント管理者ユーザー ロールが使用され、これらのロールは、vRealize Automation で定義されます。vRealize Automation のユーザー ロールの詳細については、『vRealize Automation でのサービス ブループリントの準備と使用』の「ユーザー ロールの概要」を参照してください。

注: vRealize Automation のシステム管理者は、コントロール センターで認証プロバイダを構成するときに、[管理者グループ] テキスト ボックスに入力した Orchestrator 管理者グループのメンバーである必要があります。

Orchestrator クライアントから設定可能なユーザー権限は、vRealize Automation ユーザー ロールに対応していません。特定のユーザーまたはグループについて、権限を明示的に設定する必要があります。ユーザー権限の設定の詳細については、『VMware vRealize Orchestrator クライアントの使用』を参照してください。

マルチテナントの Orchestrator 環境でのアクセス権限の分離

マルチテナントが有効な場合、システム管理者とテナント ユーザーは、Orchestrator のオブジェクトを操作する異なる権限を持ちます。これらの権限は、オブジェクトがシステム スコープとテナント固有のスコープのどちらに属しているのかによって異なります。

表 3-1. テナント間の分離

ロール	システム コンテンツ	テナント A コンテンツ	テナント B コンテンツ
システム管理者	■ システム スコープ オブジェクトを作成、表示、編集、削除、およびリストアする ■ システム ワークフローを実行する ■ システム管理者が開始したワークフローの実行を監視する	注: システム管理者として指定されているアカウントが既存のいずれかのテナントの管理者でない限り、そのシステム管理者は、テナント固有のコンテンツへのアクセスや操作を行うことはできません。	
テナント A 管理者	■ システム コンテンツを表示する ■ システム ワークフローを実行する ■ 任意のテナント A ユーザーによって開始されたシステム ワークフローを監視する	■ テナント A に属するオブジェクトを作成、表示、編集、削除、およびリストアする ■ テナント A ワークフローを実行する ■ 任意のテナント A ユーザーによって開始されたテナント A ワークフローの実行を監視する	テナント A からのユーザーは、テナント B ユーザーによって作成されるどのオブジェクトにもアクセスできない。ただし、テナント B ユーザーがプラグイン ライブラリからワークフローを実行して作成したリソースは除く。
テナント B 管理者	■ システム コンテンツを表示する ■ システム ワークフローを実行する ■ 任意のテナント B ユーザーによって開始されたシステム ワークフローを監視する	テナント B からのユーザーは、テナント A ユーザーによって作成されるどのオブジェクトにもアクセスできない。ただし、テナント A ユーザーがプラグイン ライブラリからワークフローを実行して作成したリソースは除く。	■ テナント B に属するオブジェクトを作成、表示、編集、削除、およびリストアする ■ テナント B ワークフローを実行する ■ 任意のテナント B ユーザーによって開始されたテナント B ワークフローの実行を監視する
ソリューション ユーザー	■ システム スコープ オブジェクトを作成、表示、編集、削除、およびリストアする ■ システム ワークフローを実行する	■ テナント A に属するオブジェクトを作成、表示、編集、削除、およびリストアする ■ テナント A ワークフローを実行する	■ テナント B に属するオブジェクトを作成、表示、編集、削除、およびリストアする ■ テナント B ワークフローを実行する

シングルテナントとマルチテナントの Orchestrator 展開の比較

4

7.4 バージョン以降、ビジネスのニーズや要件に応じて、Orchestrator はシングルテナント モードとマルチテナント モードで動作できるようになりました。

シングルテナントの展開

マルチテナント機能が有効な場合以外は、Orchestrator はシングルテナント モードで動作します。これは、Orchestrator のコンテンツおよびランタイムを形成するすべてのオブジェクトがすべてのユーザー間で共有されることを意味します。あるオブジェクトに対してさまざまなユーザーまたはユーザー グループが持つことのできるアクセス権を制限するために、そのオブジェクトに対して異なる権限のレベルを設定します。ユーザー権限の設定の詳細については、『VMware vRealize Orchestrator クライアントの使用』を参照してください。

マルチテナントの展開

マルチテナント機能を有効にすると、Orchestrator のテナント固有のオブジェクトが vRealize Automation テナント間およびシステムスコープ オブジェクトから分離されます。テナント ユーザーは、ユーザー名、パスワード、およびテナント ID を使用して Orchestrator クライアントにログインし、テナント固有のコンテンツを表示できます。

注: プラグイン インベントリのオブジェクトは、マルチテナントではありません。これらのオブジェクトは、システム スコープの一部です。

5 レガシー カスタム コンテンツの管理

vRealize Orchestrator のマルチ テナント機能を有効にすると、すべての既存のオブジェクトはシステムスコープ オブジェクトになります。

Orchestrator プラットフォームに含まれ、あらかじめ用意されているオブジェクトやリソースと同様に、マルチテナントを有効にする前に作成したカスタム オブジェクトは、読み取り専用モードですべてのテナント間で共有されます。また、それらのオブジェクトは、システム管理者のみが変更または削除できます。

レガシー カスタム コンテンツの分離

カスタム コンテンツをシステムスコープ コンテンツにしない場合は、カスタム オブジェクトおよびリソースをパッケージとしてエクスポートし、マルチテナント機能を有効にする前に、Orchestrator サーバから削除します。マルチテナントを有効にした後で、特定のテナント（複数も可）にこれらのオブジェクトをインポートできます。

注: 同一のパッケージを、複数のテナントに個別にインポートできます。システム スコープに配置されているパッケージは、テナントにインポートできません。また、テナント固有のコンテンツとして配置されているパッケージは、システム スコープにインポートできません。

前提条件

マルチテナントが、vRealize Orchestrator 7.4 で有効になっていないことを確認します。

手順

1 Orchestrator クライアントに管理者としてログインします。

2 エクスポート用パッケージを作成します。

「パッケージの作成」を参照してください。

3 パッケージをエクスポートします。

「パッケージのエクスポート」を参照してください。

4 Orchestrator サーバからエクスポートされたパッケージを削除します。

「パッケージの削除」を参照してください。

5 マルチテナントを有効にします。

「vRealize Orchestrator マルチテナントの有効化」を参照してください。

6 特定のテナントにパッケージをインポートするテナント管理者として、Orchestrator クライアントにログインします。

7 パッケージをインポートします。

「パッケージのインポート」を参照してください。