



OpenShift Container Platform 4.9

Windows Container Support for OpenShift

Red Hat OpenShift for Windows Containers ガイド

OpenShift Container Platform 4.9 Windows Container Support for OpenShift

Red Hat OpenShift for Windows Containers ガイド

法律上の通知

Copyright © 2023 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux[®] is the registered trademark of Linus Torvalds in the United States and other countries.

Java[®] is a registered trademark of Oracle and/or its affiliates.

XFS[®] is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL[®] is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js[®] is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack[®] Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

概要

Red Hat OpenShift for Windows Containers は、OpenShift Container Platform で Microsoft Windows Server コンテナを実行するための組み込みサポートを提供します。本書では、すべての詳細情報を提供します。

目次

第1章 RED HAT OPENSIFT SUPPORT FOR WINDOWS CONTAINERS の概要	3
第2章 WINDOWS CONTAINER SUPPORT FOR RED HAT OPENSIFT リリースノート	4
2.1. WINDOWS CONTAINER SUPPORT FOR RED HAT OPENSIFT について	4
2.2. サポート	4
2.3. RED HAT WINDOWS MACHINE CONFIG OPERATOR 4.0.2 リリースノート	4
2.4. RED HAT WINDOWS MACHINE CONFIG OPERATOR 4.0.1 リリースノート	5
2.5. RED HAT WINDOWS MACHINE CONFIG OPERATOR 4.0.0 リリースノート	5
2.6. WINDOWS MACHINE CONFIG OPERATOR の前提条件	7
2.7. 既知の制限	9
第3章 WINDOWS コンテナワークロードについて	11
3.1. WINDOWS MACHINE CONFIG OPERATOR の前提条件	11
3.2. WINDOWS ワークロード管理	13
3.3. WINDOWS ノードサービス	15
3.4. 既知の制限	16
第4章 WINDOWS コンテナワークロードの有効化	18
前提条件	18
4.1. WINDOWS MACHINE CONFIG OPERATOR のインストール	18
4.2. WINDOWS MACHINE CONFIG OPERATOR のシークレットの設定	21
4.3. 関連情報	22
第5章 WINDOWS MACHINESSET オブジェクトの作成	23
5.1. AWS での WINDOWS MACHINESSET オブジェクトの作成	23
5.2. AZURE での WINDOWS MACHINESSET オブジェクトの作成	28
5.3. VSPHERE での WINDOWS MACHINESSET オブジェクトの作成	33
第6章 WINDOWS コンテナワークロードのスケジューリング	44
前提条件	44
6.1. WINDOWS POD の配置	44
6.2. スケジューリングメカニズムをカプセル化するための RUNTIMECLASS オブジェクトの作成	45
6.3. WINDOWS コンテナワークロードのデプロイメント例	46
6.4. マシンセットの手動によるスケーリング	47
第7章 WINDOWS ノードのアップグレード	49
7.1. WINDOWS MACHINE CONFIG OPERATOR のアップグレード	49
第8章 BYOH (BRING-YOUR-OWN-HOST) WINDOWS インスタンスをノードとして使用	50
8.1. BYOH WINDOWS インスタンスの設定	50
8.2. BYOH WINDOWS インスタンスの削除	51
第9章 WINDOWS ノードの削除	52
9.1. 特定マシンの削除	52
第10章 WINDOWS コンテナワークロードの無効化	53
10.1. WINDOWS MACHINE CONFIG OPERATOR のアンインストール	53
10.2. WINDOWS MACHINE CONFIG OPERATOR NAMESPACE の削除	53

第1章 RED HAT OPENSIFT SUPPORT FOR WINDOWS CONTAINERS の概要

Red Hat OpenShift support for Windows Containers は、OpenShift Container Platform クラスターで Windows コンピュートノードを実行する機能を提供します。これは、Red Hat Windows Machine Config Operator (WMCO) を使用して Windows ノードをインストールし、管理することで実行できます。Red Hat Subscription を使用すると、OpenShift Container Platform での Windows ワークロードの実行をサポートできます。詳細は [リリースノート](#) を参照してください。

Linux と Windows の両方を含むワークロードの場合、OpenShift Container Platform を使用すると、Windows Server コンテナで実行される Windows ワークロードをデプロイすると同時に、Red Hat Enterprise Linux CoreOS (RHCOS) または Red Hat Enterprise Linux (RHEL) でホストされる従来の Linux ワークロードを提供できます。詳細については、[getting started with Windows container workloads](#) を参照してください。

クラスターで Windows ワークロードを実行するには、WMCO が必要です。WMCO は、クラスター上で Windows ワークロードをデプロイし、管理するプロセスをオーケストレーションします。詳細については、[how to enable Windows container workloads](#) を参照してください。

Windows **MachineSet** オブジェクトを作成して、インフラストラクチャー Windows マシンセットおよび関連マシンを作成し、サポートされている Windows ワークロードを新しい Windows マシンに移動できます。複数のプラットフォームで Windows **MachineSet** オブジェクトを作成できます。

Windows コンピュートノードに [Windows ワークロードをスケジュール](#) することができます。

[Windows Machine Config Operator のアップグレードを実行](#) して、Windows ノードに最新の更新が適用されていることを確認できます。

特定のマシンを削除することで、[Windows ノードを削除](#) できます。

[Bring-Your-Own-Host \(BYOH\) Windows インスタンスを使用](#) して、Windows Server VM を再利用し、OpenShift Container Platform に移動できます。BYOH Windows インスタンスは、Windows サーバーがオフラインになった場合に、主要な中断を軽減するのに役立ちます。BYOH Windows インスタンスは、OpenShift Container Platform 4.8 以降のバージョンのノードとして使用できます。

次の手順を実行して、[Windows コンテナのワークロードを無効](#) にできます。

- Windows Machine Config Operator のアンインストール
- Windows Machine Config Operator namespace の削除

第2章 WINDOWS CONTAINER SUPPORT FOR RED HAT OPENSIFT リリースノート

2.1. WINDOWS CONTAINER SUPPORT FOR RED HAT OPENSIFT について

Red Hat OpenShift support for Windows Containers は、OpenShift Container Platform クラスターでの Windows コンピュータノードの実行を可能にします。Windows ワークロードは、Red Hat Windows Machine Config Operator (WMCO) を使用して Windows ノードをインストールし、管理することで実行できます。Windows ノードが利用可能になると、Windows コンテナワークロードを OpenShift Container Platform で実行できます。

Red Hat OpenShift support for Windows Containers のリリースノートでは、OpenShift Container Platform にすべての Windows コンテナワークロード機能を提供する WMCO の開発の進展を追跡できます。

2.2. サポート

Red Hat OpenShift support for Windows Containers は、オプションのインストール可能なコンポーネントとして提供されており、その使用が可能です。Red Hat OpenShift support for Windows Containers は OpenShift Container Platform サブスクリプションの一部ではありません。追加の Red Hat サブスクリプションが必要で、[対象範囲](#) および [サービスレベルアグリーメント](#) に従ってサポートされます。

Red Hat OpenShift support for Windows Containers のサポートを受けるには、別のこのサブスクリプションが必要です。この追加の Red Hat サブスクリプションがないと、実稼働クラスターへの Windows コンテナワークロードのデプロイはサポートされません。[Red Hat カスタマーポータル](#) からサポートをリクエストできます。

詳細は、[Red Hat OpenShift support for Windows Containers](#) の Red Hat OpenShift Container Platform ライフサイクルポリシーのドキュメントを参照してください。

この追加の Red Hat サブスクリプションがない場合は、正式なサポートのないディストリビューションである Community Windows Machine Config Operator を使用できます。

2.3. RED HAT WINDOWS MACHINE CONFIG OPERATOR 4.0.2 リリースノート

発行日：2023-3-28

WMCO 4.0.2 がバグ修正およびセキュリティ更新と共に利用できるようになりました。WMCO のコンポーネントは [RHBA-2023:1488](#) でリリースされました。

2.3.1. バグ修正

- 以前は、Windows ノード上のコンテナには、デフォルトのサブネットに基づいてハードコーディングされた DNS サーバー IP アドレス (172.30.0.10 など) が割り当てられていました。これにより、特定の状況で DNS 解決が失敗しました。今回の修正により、ハードコーディングされた DNS アドレスが削除され、Windows コンテナには、クラスター DNS 設定に基づく有効な DNS サーバー IP アドレスが割り当てられるようになりました。その結果、DNS 解決は Windows コンテナでは期待どおりに機能します。([BZ#2020350](#))

2.4. RED HAT WINDOWS MACHINE CONFIG OPERATOR 4.0.1 リリースノート

発行日: 2021-12-13

WMCO 4.0.1 がバグ修正およびセキュリティー更新と共に利用できるようになりました。WMCO のコンポーネントは [RHBA-2021:4757](#) でリリースされました。

2.4.1. バグ修正

- 以前は、**windows-exporter** メトリックエンドポイントオブジェクトに、削除されたマシンへの参照が含まれていました。この誤った参照により、WMCO は無効な IP アドレスを持つマシンの削除されたイベントを無視していました。このバグ修正により、マシンオブジェクトの検証がイベントフィルタリングから削除され、マシンがまだ **Deleting** フェーズにあるときに、**windows-exporter** メトリックエンドポイントオブジェクトが正しく更新されるようになります。(BZ#2008992)
- 以前は、Windows **Machine** オブジェクトに関連付けられたノードを削除すると、Operator の再起動時に調整エラーが発生していました。このバグ修正は、**実行** 状態の Windows マシンによって参照されるノードがクラスター内に見つからない場合に反応または調整しないことを選択し、エラーループを防ぎ、Linux マシンオブジェクトの機能を標準化します。(BZ#2009474)
- 以前は、Windows VM で WMCO によって実行されている特定のコマンドは、PowerShell によって正しく解析されませんでした。これにより、PowerShell をデフォルトの SSH シェルとして使用している Windows VM は、ノードとしてクラスターに参加できなくなりました。WMCO は、Windows VM のデフォルトの SSH シェルを識別し、それに応じて関連するコマンドを実行します。この新機能により、PowerShell をデフォルトの SSH シェルとして使用する WindowsVM をクラスター内のノードとして設定できます。(BZ#2014707)
- 以前は、暗号化されたユーザー名が追加のタグで生成されていたため、正しく表示されませんでした。このバグ修正により、余分なタグが削除され、暗号化されたユーザー名が正しく表示されるようになります。(BZ#2016712)
- 以前は、VM が DNS オブジェクトで指定されている場合、WMCO は BYOH Windows VM を **Node** オブジェクトに適切に関連付けませんでした。これにより、WMCO はすでに完全に設定されている VM の設定を試みました。WMCO は、関連付けられたノードを探すときに DNS アドレスで指定された VM を正しく解決するようになりました。(BZ#2020648)

2.5. RED HAT WINDOWS MACHINE CONFIG OPERATOR 4.0.0 リリースノート

本 WMCO リリースノートは、Windows コンピュートノードを OpenShift Container Platform クラスターで実行するためのバグ修正を提供します。WMCO 4.0.0 のコンポーネントは [RHBA-2021:3702](#) でリリースされています。

2.5.1. バグ修正

- 以前のバージョンでは、WMCO は Bring-Your-Own-Host (BYOH) Windows ノードの作成時に、ユーザーが指定するインスタンスアドレスを使用していました。これにより、BYOH Windows インスタンスが OpenShift Container Platform クラスターに加わりませんでした。今回のバグ修正により、ユーザーによって提供される DNS 名が有効な IPv4 アドレスに解決され、BYOH Windows インスタンスの作成時に解決された値が使用されるようになりました。BYOH インスタンスは異なるホスト名で、DNS アドレスは Windows ノードとして設定できません。(BZ#1995684)

- 以前のバージョンでは、WMCO はインスタンス/ノード間の関連付けを特定する際に、未解決のインスタンスアドレスを使用した直接比較が実行されました。これにより、OpenShift Container Platform クラスターに参加するように設定された BYOH Windows インスタンスが削除されました。今回のバグ修正により、**Windows インスタンス** 設定マップに追加されるエントリーの DNS 検索を実行して DNS アドレスを検証します。WMCO は、設定されたインスタンス間の関係を適切に特定できるようになりました。これにより、BYOH ノードの削除ができなくなりました。(BZ#2005126)

2.5.2. 既知の問題

- Windows ノードについては、Web コンソールで利用可能なファイルシステムのグラフは表示されません。この問題は、ファイルシステムクエリーの変更によって生じます。これは、WMCO の今後のリリースで修正されます。(BZ#1930347)
- VMware vSphere にインストールされているクラスターの場合、WMCO は **Deleting** フェーズ通知イベントを無視し、正しくないノード情報を **windows-exporter** メトリクスエンドポイントに残します。これにより、Prometheus メトリクスエンドポイントに無効なマッピングが生じました。このバグは修正されています。WMCO は **Deleting** phase 通知イベントを認識し、Prometheus メトリクスエンドポイントを適切にマップするようになりました。(BZ#1995341)

- RunAsUser** パーミッションが Linux ベースの Pod のセキュリティコンテキストに設定されている場合、Projected ファイルには、コンテナユーザー所有権を含む適切なパーミッションが設定されます。ただし、Windows の同等の **RunAsUsername** パーミッションが Windows Pod に設定されている場合、kubelet は Projected ボリュームのファイルに正しい所有権を設定できなくなります。この問題は、ベストプラクティスに従わない **hostPath ボリューム** と組み合わせて使用すると悪化する可能性があります。たとえば、Pod に **C:\var\lib\kubelet\pods** フォルダへのアクセス権限を付与すると、Pod が他の Pod からサービスアカウントトークンにアクセスできるようになります。

デフォルトでは、この例では Windows の Projected ボリュームファイルに示されるように、projected ファイルに以下の所有者が設定されます。

```
Path :
Microsoft.PowerShell.Core\FileSystem::C:\var\run\secrets\kubernetes.io\serviceaccount\..2021_
08_31_22_22_18.318230061\ca.crt
Owner : BUILTIN\Administrators
Group : NT AUTHORITY\SYSTEM
Access : NT AUTHORITY\SYSTEM Allow FullControl
        BUILTIN\Administrators Allow FullControl
        BUILTIN\Users Allow ReadAndExecute, Synchronize
Audit :
Sddl : O:BAG:SYD:AI(A;ID;FA;;;SY)(A;ID;FA;;;BA)(A;ID;0x1200a9;;;BU)
```

これは、**ContainerAdministrator** ロールを持つユーザーなどのすべての管理者ユーザーに対して読み取り、書き込み、実行アクセスがある一方で、管理者以外のユーザーが読み取りおよび実行アクセスを持っていることを示しています。



重要

OpenShift Container Platform は、オペレーティングシステムに関係なく、**RunAsUser** セキュリティコンテキストをすべての Pod に適用します。これは、Windows Pod の **RunAsUser** パーミッションがセキュリティコンテキストに自動的に適用されることを意味します。

さらに、Windows Pod がデフォルトの **RunAsUser** パーミッションセットで Projected ボリュームで作成される場合、Pod は **ContainerCreating** フェーズで停止します。

これらの問題に対応するため、OpenShift Container Platform は Pod のセキュリティーコンテキストで設定される Projected サービスアカウントボリュームでのファイルパーミッションの処理を Windows の projected ボリュームに反映しないように強制します (BZ#1971745)。Windows Pod のこの動作は、OpenShift Container Platform 4.7 より前のすべての Pod タイプでどのように機能するかについて使用されるファイルパーミッションの処理であることに注意してください。

2.6. WINDOWS MACHINE CONFIG OPERATOR の前提条件

以下では、Windows Machine Config Operator のサポート対象のプラットフォームバージョン、Windows Server バージョン、およびネットワーク設定について詳しく説明します。対象のプラットフォームのみに関連する情報については、vSphere のドキュメントを参照してください。

2.6.1. OpenShift Container Platform および WMCO バージョンをベースとするサポートされるプラットフォーム

プラットフォーム	サポート対象の Red Hat OpenShift Container Platform バージョン	サポート対象の WMCO バージョン	インストーラーでプロビジョニングされるインフラストラクチャーのインストールサポート	ユーザーによってプロビジョニングされるインフラストラクチャーのインストールサポート
Amazon Web Services (AWS)	4.6+	WMCO 1.0+	GA	
Microsoft Azure	4.6+	WMCO 1.0+	GA	
VMware vSphere	4.7+	WMCO 2.0+	GA	

2.6.2. OpenShift Container Platform および WMCO バージョンをベースとした BYOH (Bring-Your-Own-Host) インスタンスでサポートされるプラットフォーム

プラットフォーム	サポート対象の Red Hat OpenShift Container Platform バージョン	サポート対象の WMCO バージョン	インストーラーでプロビジョニングされるインフラストラクチャーのインストールサポート用の BYOH	ユーザーによってプロビジョニングされるインフラストラクチャーのインストールサポート用の BYOH
Amazon Web Services (AWS)	4.8 以降	WMCO 3.1+	GA	
Microsoft Azure	4.8 以降	WMCO 3.1+	GA	
VMware vSphere	4.8 以降	WMCO 3.1+	GA	

プラットフォーム	サポート対象の Red Hat OpenShift Container Platform バージョン	サポート対象の WMCO バージョン	インストーラーでプロビジョニングされるインフラストラクチャーのインストールサポート用の BYOH	ユーザーによってプロビジョニングされるインフラストラクチャーのインストールサポート用 BYOH
プロバイダーに依存しない (プラットフォーム: なし)	4.8 以降	WMCO 3.1+		GA

2.6.3. サポート対象の Windows Server バージョン

以下の表は、適用可能なプラットフォームを基にした、サポート対象の [Windows Server バージョン](#) の一覧です。リストに含まれない Windows Server バージョンはサポートされず、エラーを引き起こします。これらのエラーを回避するには、使用中のプラットフォームに合わせて適切なバージョンのみを使用します。

プラットフォーム	サポート対象の Windows Server バージョン
Amazon Web Services (AWS)	Windows Server 長期サービスチャネル (Long-Term Servicing Channel, LTSC): Windows Server 2019
Microsoft Azure	Windows Server 長期サービスチャネル (Long-Term Servicing Channel, LTSC): Windows Server 2019
VMware vSphere	Windows Server 長期サービスチャネル (LTSC): Windows Server 2022 (OS ビルド 20348.681 以降)
ベアメタル	Windows Server 長期サービスチャネル (Long-Term Servicing Channel, LTSC): Windows Server 2019

2.6.4. サポート対象のネットワーク

サポート対象のネットワーク設定は、OVN-Kubernetes を使用したハイブリッドネットワークのみです。この機能の詳細は、以下の追加リソースを参照してください。以下の表は、プラットフォームで使用するネットワーク設定の種類と Windows Server バージョンの概要を示しています。クラスタのインストール時にネットワーク設定を指定する必要があります。OpenShift SDN ネットワークは OpenShift Container Platform クラスタのデフォルトのネットワークであることに注意してください。ただし、OpenShift SDN は WMCO ではサポートされません。

表2.1 プラットフォームネットワークングサポート

プラットフォーム	サポート対象のネットワーク
Amazon Web Services (AWS)	OVN-Kubernetes を使用したハイブリッドネットワーク

プラットフォーム	サポート対象のネットワーク
Microsoft Azure	OVN-Kubernetes を使用したハイブリッドネットワーク
VMware vSphere	カスタム VXLAN ポートを備えた OVN-Kubernetes でのハイブリッドネットワーク
ベアメタル	OVN-Kubernetes を使用したハイブリッドネットワーク

表2.2 ハイブリッド OVN-Kubernetes Windows Server のサポート

OVN-Kubernetes を使用したハイブリッドネットワーク	サポート対象の Windows Server バージョン
デフォルトの VXLAN ポート	Windows Server 長期サービスチャネル (Long-Term Servicing Channel, LTSC): Windows Server 2019
カスタム VXLAN ポート	Windows Server 長期サービスチャネル (LTSC): Windows Server 2022 (OS ビルド 20348.681 以降)

**重要**

Windows コンテナワークロードの実行は、ネットワークが制限された環境または非接続環境のクラスターではサポートされません。

WMCO のバージョン 4.x は OpenShift Container Platform 4.9 とのみ互換性があります。

2.7. 既知の制限

WMCO によって管理される Windows ノード (Windows ノード) を使用する場合は、次の制限に注意してください。

- 以下の OpenShift Container Platform 機能は、Windows ノードではサポートされていません。
 - Red Hat OpenShift Developer CLI (odo)
 - イメージビルド
 - OpenShift Pipeline
 - OpenShift Service Mesh
 - ユーザー定義プロジェクトの OpenShift モニターリング
 - OpenShift Serverless
 - Horizontal Pod Autoscaling
 - Vertical Pod Autoscaling

- 次の Red Hat 機能は、Windows ノードではサポートされていません。
 - [Red Hat のコスト管理](#)
 - [Red Hat OpenShift Local](#)
- Windows ノードは、プライベートレジストリーからのコンテナイメージのプルをサポートしていません。パブリックレジストリーのイメージを使用するか、イメージを事前にプルすることができます。
- Windows ノードは、デプロイ設定を使用して作成されたワークロードをサポートしていません。デプロイまたはその他の方法を使用して、ワークロードをデプロイできます。
- Windows ノードは、クラスター全体のプロキシを使用するクラスターではサポートされていません。これは、WMCO がワークロードのプロキシ接続を介してトラフィックをルーティングできないためです。
- Windows ノードは、切断された環境にあるクラスターではサポートされていません。
- Red Hat OpenShift による Windows コンテナのサポートでは、トランクポートを介したクラスターへの Windows ノードの追加はサポートされていません。Windows ノードを追加するためにサポートされている唯一のネットワーク設定は、VLAN のトラフィックを伝送するアクセスポート経由です。
- Windows コンテナの Red Hat OpenShift サポートは、すべてのクラウドプロバイダーのツリー内ストレージドライバーのみをサポートします。
- Kubernetes は、次の [ノード機能の制限](#) を特定しました。
 - Windows コンテナでは Huge Page はサポートされていません。
 - 特権コンテナは、Windows コンテナではサポートされていません。
 - Pod 終了の猶予期間では、containerd コンテナランタイムを Windows ノードにインストールする必要があります。
- Kubernetes は、[いくつかの API 互換性の問題](#) を特定しました。

第3章 WINDOWS コンテナワークロードについて

Red Hat OpenShift support for Windows Containers は、OpenShift Container Platform で Microsoft Windows Server コンテナを実行するための組み込みサポートを提供します。Linux と Windows ワークロードの組み合わせを使用して異種環境を管理する場合、OpenShift Container Platform では、Windows Server コンテナで実行されている Windows ワークロードをデプロイできますが、Red Hat Enterprise Linux CoreOS (RHCOS) または Red Hat Enterprise Linux (RHEL) でホストされる従来の Linux ワークロードも提供できます。

注記

Windows ノードを持つクラスターのマルチテナンシーはサポートされません。マルチテナントの悪意のある使用により、すべての Kubernetes 環境でのセキュリティ上のリスクが導入されます。[Pod セキュリティポリシー](#)、またはノードのより詳細なロールベースアクセス制御 (RBAC) などの追加のセキュリティ機能により、悪用がより困難になります。ただし、悪意のあるマルチテナントワークロードの実行を選択する場合、ハイパーバイザーは使用する必要のある唯一のセキュリティオプションになります。Kubernetes のセキュリティドメインは、個別のノードではなく、クラスター全体に対応します。これらのタイプの悪意のあるマルチテナントワークロードには、物理的に分離されたクラスターを使用する必要があります。

Windows Server コンテナは共有カーネルを使用してリソース分離を行います。悪意のあるマルチテナンシーのシナリオで使用することは意図されていません。悪意のあるマルチテナンシーを使用するシナリオの場合、テナントを確実に分離するために Hyper-V 分離コンテナを使用する必要があります。

3.1. WINDOWS MACHINE CONFIG OPERATOR の前提条件

以下では、Windows Machine Config Operator のサポート対象のプラットフォームバージョン、Windows Server バージョン、およびネットワーク設定について詳しく説明します。対象のプラットフォームのみに関連する情報については、vSphere のドキュメントを参照してください。

3.1.1. OpenShift Container Platform および WMCO バージョンをベースとするサポートされるプラットフォーム

プラットフォーム	サポート対象の Red Hat OpenShift Container Platform バージョン	サポート対象の WMCO バージョン	インストーラーでプロビジョニングされるインフラストラクチャーのインストールサポート	ユーザーによってプロビジョニングされるインフラストラクチャーのインストールサポート
Amazon Web Services (AWS)	4.6+	WMCO 1.0+	GA	
Microsoft Azure	4.6+	WMCO 1.0+	GA	
VMware vSphere	4.7+	WMCO 2.0+	GA	

3.1.2. OpenShift Container Platform および WMCO バージョンをベースとした BYOH (Bring-Your-Own-Host) インスタンスでサポートされるプラットフォーム

プラットフォーム	サポート対象の Red Hat OpenShift Container Platform バージョン	サポート対象の WMCO バージョン	インストーラーでプロビジョニングされるインフラストラクチャーのインストールサポート用の BYOH	ユーザーによってプロビジョニングされるインフラストラクチャーのインストールサポート用 BYOH
Amazon Web Services (AWS)	4.8 以降	WMCO 3.1+	GA	
Microsoft Azure	4.8 以降	WMCO 3.1+	GA	
VMware vSphere	4.8 以降	WMCO 3.1+	GA	
プロバイダーに依存しない (プラットフォーム: なし)	4.8 以降	WMCO 3.1+		GA

3.1.3. サポート対象の Windows Server バージョン

以下の表は、適用可能なプラットフォームを基にした、サポート対象の [Windows Server バージョン](#) の一覧です。リストに含まれない Windows Server バージョンはサポートされず、エラーを引き起こします。これらのエラーを回避するには、使用中のプラットフォームに合わせて適切なバージョンのみを使用します。

プラットフォーム	サポート対象の Windows Server バージョン
Amazon Web Services (AWS)	Windows Server 長期サービスチャネル (Long-Term Servicing Channel, LTSC): Windows Server 2019
Microsoft Azure	Windows Server 長期サービスチャネル (Long-Term Servicing Channel, LTSC): Windows Server 2019
VMware vSphere	Windows Server 長期サービスチャネル (LTSC): Windows Server 2022 (OS ビルド 20348.681 以降)
ベアメタル	Windows Server 長期サービスチャネル (Long-Term Servicing Channel, LTSC): Windows Server 2019

3.1.4. サポート対象のネットワーク

サポート対象のネットワーク設定は、OVN-Kubernetes を使用したハイブリッドネットワークのみです。この機能の詳細は、以下の追加リソースを参照してください。以下の表は、プラットフォームで使用するネットワーク設定の種類と Windows Server バージョンの概要を示しています。クラスタのインストール時にネットワーク設定を指定する必要があります。OpenShift SDN ネットワークは OpenShift Container Platform クラスタのデフォルトのネットワークであることに注意してください。ただし、OpenShift SDN は WMCO ではサポートされません。

表3.1 プラットフォームネットワーキングサポート

プラットフォーム	サポート対象のネットワーク
Amazon Web Services (AWS)	OVN-Kubernetes を使用したハイブリッドネットワーク
Microsoft Azure	OVN-Kubernetes を使用したハイブリッドネットワーク
VMware vSphere	カスタム VXLAN ポートを備えた OVN-Kubernetes でのハイブリッドネットワーク
ベアメタル	OVN-Kubernetes を使用したハイブリッドネットワーク

表3.2 ハイブリッド OVN-Kubernetes Windows Server のサポート

OVN-Kubernetes を使用したハイブリッドネットワーク	サポート対象の Windows Server バージョン
デフォルトの VXLAN ポート	Windows Server 長期サービスチャネル (Long-Term Servicing Channel, LTSC): Windows Server 2019
カスタム VXLAN ポート	Windows Server 長期サービスチャネル (LTSC): Windows Server 2022 (OS ビルド 20348.681 以降)

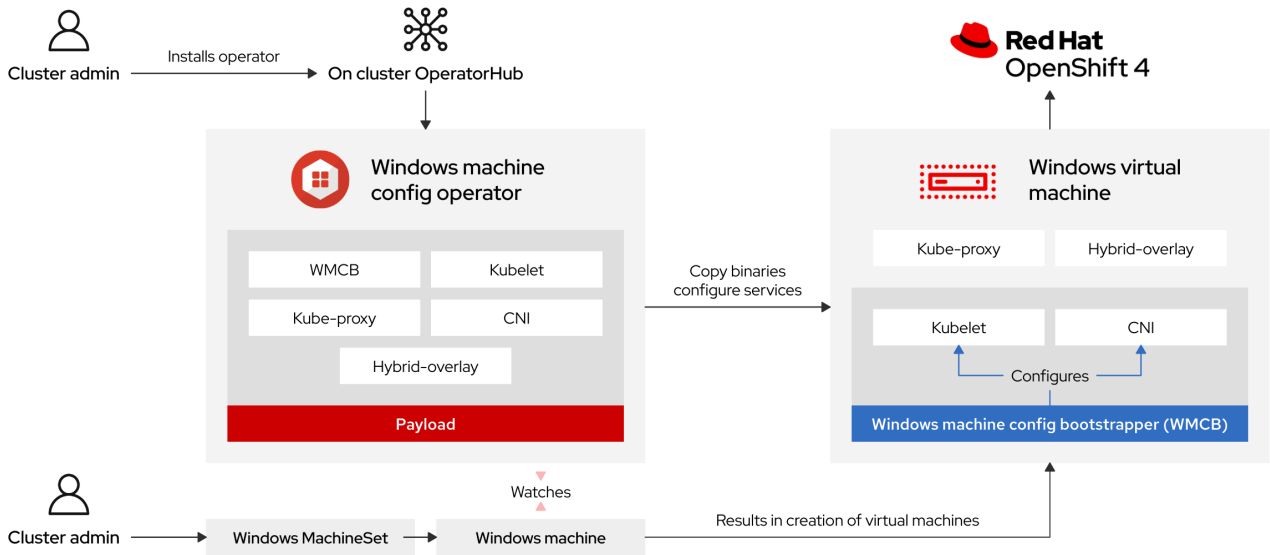
関連情報

- [OVN-Kubernetes を使用したハイブリッドネットワークの設定](#) を参照してください。

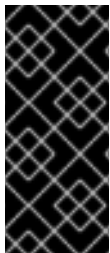
3.2. WINDOWS ワークロード管理

クラスターで Windows ワークロードを実行するには、まず Windows Machine Config Operator (WMCO) をインストールする必要があります。WMCO は Linux ベースのコントロールプレーンおよびコンピュートノードで実行される Linux ベースの Operator です。WMCO は、クラスター上で Windows ワークロードをデプロイし、管理するプロセスをオーケストレーションします。

図3.1 WMCO の設計



Windows ワークロードをデプロイする前に、Windows コンピュートノードを作成し、これをクラスターに参加させる必要があります。Windows ノードは、クラスター内の Windows ワークロードをホストし、他の Linux ベースのコンピューターノードと共に実行できます。Windows Server コンピューターマシンをホストする Windows マシンセットを作成して、Windows コンピューターノードを作成することができます。Docker 形式のコンテナランタイムアドオンが有効にされた Windows OS イメージを指定する Windows 固有のラベルをマシンセットに適用する必要があります。

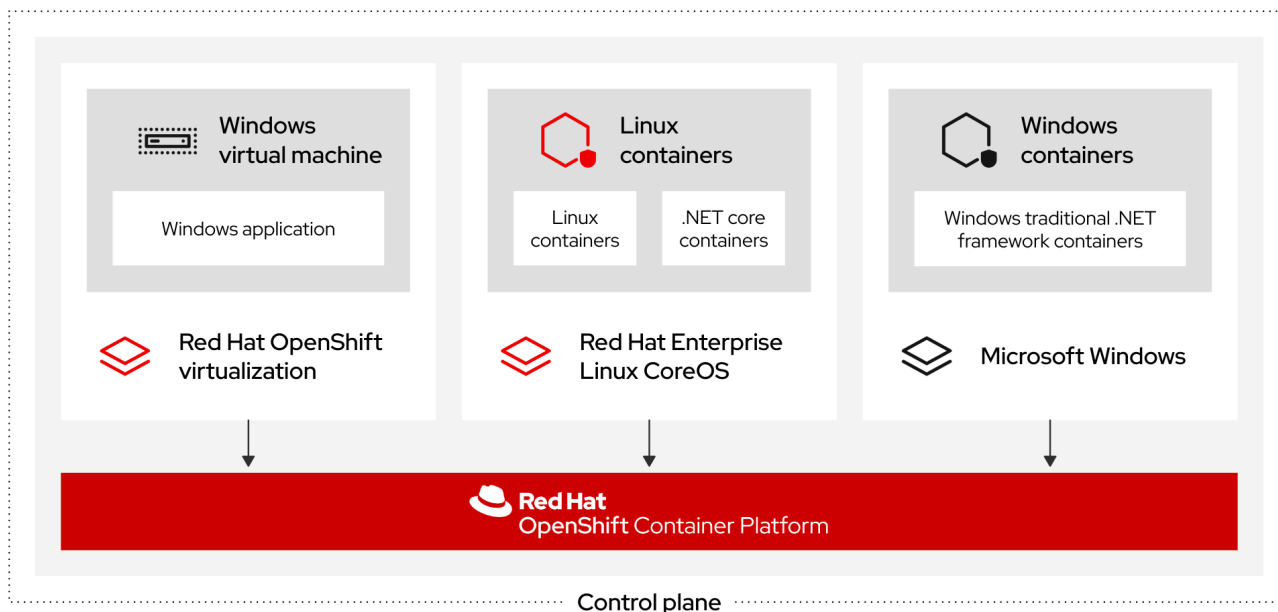


重要

現時点で、Docker 形式のコンテナランタイムは Windows ノードで使用されます。Kubernetes では、コンテナランタイムとしての Docker を非推奨としています。詳細は、Kubernetes ドキュメントの [Docker の非推奨](#) について参照してください。Containerd は、今後の Kubernetes リリースで Windows ノードについてサポートされる新しいコンテナランタイムになります。

WMCO は Windows ラベルの付いたマシンを監視します。Windows マシンセットを検出し、そのそれぞれのマシンがプロビジョニングされると、WMCO は基礎となる Windows 仮想マシン (VM) を設定し、それがコンピューターノードとしてクラスターに参加できるようにします。

図3.2 Windows および Linux ワークロードの組み合わせ



WMCO は、Windows インスタンスとの対話に使用されるプライベートキーが含まれる namespace に事前に決定されたシークレットがあることを想定します。WMCO は起動時にこのシークレットの有無を確認し、作成した Windows **MachineSet** オブジェクトで参照する必要があるユーザーデータのシークレットを作成します。次に WMCO は、プライベートキーに対応するパブリックキーでユーザーデータのシークレットを設定します。このデータが適用されると、クラスターは SSH 接続を使用して Windows 仮想マシンに接続できます。

クラスターが Windows 仮想マシンとの接続を確立した後に、Linux ベースのノードの場合と同様の手法を使用して Windows ノードを管理できます。



注記

OpenShift Container Platform Web コンソールは、Linux ノードで利用可能な機能と同じモニターリング機能のほとんどを Windows ノードについて提供します。ただし、現時点で Windows ノードで実行されている Pod のワークロードグラフを監視する機能は利用できません。

Windows ワークロードの Windows ノードへのスケジュールは、テイント、容認、ノードセクターなどの一般的な Pod スケジュールの手法を使用して実行できますが、**RuntimeClass** オブジェクトを使用して Windows ワークロードを Linux ワークロードおよび他の Windows 版のワークロードから区別できます。

3.3. WINDOWS ノードサービス

以下の Windows 固有のサービスは、各 Windows ノードにインストールされます。

サービス	説明
kubelet	Windows ノードを登録し、そのステータスを管理します。
Container Network Interface (CNI) プラグイン	Windows ノードの ネットワーク を公開します。

サービス	説明
Windows Machine Config Bootstrapper (WMCB)	kubelet および CNI プラグインを設定します。
Windows Exporter	Windows ノードから Prometheus メトリクスをエクスポートします。
hybrid-overlay	OpenShift Container Platform Host Network Service (HNS) を作成します。
kube-proxy	外部との通信を許可するノードでネットワークルールを維持します。

3.4. 既知の制限

WMCO によって管理される Windows ノード (Windows ノード) を使用する場合は、次の制限に注意してください。

- 以下の OpenShift Container Platform 機能は、Windows ノードではサポートされていません。
 - Red Hat OpenShift Developer CLI (odo)
 - イメージビルド
 - OpenShift Pipeline
 - OpenShift Service Mesh
 - ユーザー定義プロジェクトの OpenShift モニタリング
 - OpenShift Serverless
 - Horizontal Pod Autoscaling
 - Vertical Pod Autoscaling
- 次の Red Hat 機能は、Windows ノードではサポートされていません。
 - [Red Hat のコスト管理](#)
 - [Red Hat OpenShift Local](#)
- Windows ノードは、プライベートレジストリーからのコンテナイメージのプルをサポートしていません。パブリックレジストリーのイメージを使用するか、イメージを事前にプルすることができます。
- Windows ノードは、デプロイ設定を使用して作成されたワークロードをサポートしていません。デプロイまたはその他の方法を使用して、ワークロードをデプロイできます。
- Windows ノードは、クラスター全体のプロキシを使用するクラスターではサポートされていません。これは、WMCO がワークロードのプロキシ接続を介してトラフィックをルーティングできないためです。
- Windows ノードは、切断された環境にあるクラスターではサポートされていません。

- Red Hat OpenShift による Windows コンテナのサポートでは、トランクポートを介したクラスターへの Windows ノードの追加はサポートされていません。Windows ノードを追加するためにサポートされている唯一のネットワーク設定は、VLAN のトラフィックを伝送するアクセスポート経由です。
- Windows コンテナの Red Hat OpenShift サポートは、すべてのクラウドプロバイダーのツリー内ストレージドライバーのみをサポートします。
- Kubernetes は、次の [ノード機能の制限](#) を特定しました。
 - Windows コンテナでは Huge Page はサポートされていません。
 - 特権コンテナは、Windows コンテナではサポートされていません。
 - Pod 終了の猶予期間では、containerd コンテナランタイムを Windows ノードにインストールする必要があります。
- Kubernetes は、[いくつかの API 互換性の問題](#) を特定しました。

第4章 WINDOWS コンテナワークロードの有効化

Windows ワークロードをクラスターに追加する前に、OpenShift Container Platform OperatorHub で利用可能な Windows Machine Config Operator (WMCO) をインストールする必要があります。WMCO は、クラスター上で Windows ワークロードをデプロイし、管理するプロセスをオーケストレーションします。



注記

デュアル NIC は、WMCO が管理する Windows インスタンスではサポートされていません。

前提条件

- **cluster-admin** パーミッションを持つアカウントを使用して OpenShift Container Platform クラスターにアクセスできる。
- OpenShift CLI (**oc**) がインストールされている。
- `installer-provisioned infrastructure` を使用してクラスターをインストールしたか、または **install-config.yaml** ファイルに **platform: none** フィールドを設定した `user-provisioned infrastructure` を使用してインストールした場合。
- クラスターに OVN-Kubernetes を使用してハイブリッドネットワークを設定している。これは、クラスターのインストール時に完了する必要があります。詳細は、[Configuring hybrid networking](#) を参照してください。
- OpenShift Container Platform クラスター (バージョン 4.6.8 以降) を実行している。



注記

WMCO はワークロードのプロキシ接続を介してトラフィックをルーティングできないため、[クラスター全体のプロキシ](#) を使用するクラスターではサポートされません。

関連情報

- Windows Machine Config Operator の全前提条件については、[Windows コンテナワークロードについて](#) を参照してください。

4.1. WINDOWS MACHINE CONFIG OPERATOR のインストール

Web コンソールまたは OpenShift CLI (**oc**) のいずれかを使用して Windows Machine Config Operator をインストールできます。

4.1.1. Web コンソールを使用した Windows Machine Config Operator のインストール

OpenShift Container Platform Web コンソールを使って Windows Machine Config Operator (WMCO) をインストールすることができます。



注記

デュアル NIC は、WMCO が管理する Windows インスタンスではサポートされていません。

手順

1. OpenShift Container Platform Web コンソールの **Administrator** パースペクティブから、**Operators → OperatorHub** ページに移動します。
2. **Filter by keyword** ボックスを使用して、カタログで **Windows Machine Config Operator** を検索します。 **Windows Machine Config Operator** タイルをクリックします。
3. Operator についての情報を確認してから、**Install** をクリックします。
4. **Install Operator** ページで以下を行います。
 - a. **Update Channel** として **stable** チャンネルを選択します。 **stable** チャンネルを使用すると、WMCO の最新の安定したリリースをインストールできます。
 - b. WMCO は単一の namespace でのみ利用できるようにする必要があるため、**インストールモード** は事前に設定されます。
 - c. WMCO の **Installed Namespace** を選択します。デフォルトの Operator の推奨される namespace は **openshift-windows-machine-config-operator** です。
 - d. **Enable Operator recommended cluster monitoring on the Namespace** チェックボックスをクリックし、WMCO についてクラスターのモニタリングを有効にします。
 - e. **Approval Strategy** を選択します。
 - **Automatic** ストラテジーにより、Operator Lifecycle Manager (OLM) は新規バージョンが利用可能になると Operator を自動的に更新できます。
 - **Manual** ストラテジーには、Operator の更新を承認するための適切な認証情報を持つユーザーが必要です。
1. **Install** をクリックします。WMCO が **Installed Operators** ページに一覧表示されます。



注記

WMCO は、**openshift-windows-machine-config-operator** などのように、定義した namespace に自動的にインストールされます。

2. **Status** に **Succeeded** が表示されていることを検証し、WMCO のインストールが正常に行われたことを確認します。

4.1.2. CLI を使用した Windows Machine Config Operator のインストール

OpenShift CLI (**oc**) を使用して、Windows Machine Config Operator (WMCO) をインストールできます。



注記

デュアル NIC は、WMCO が管理する Windows インスタンスではサポートされていません。

手順

1. WMCO の namespace を作成します。

- a. WMCO の **Namespace** オブジェクト YAML ファイルを作成します。例: **wmco-namespace.yaml**

```
apiVersion: v1
kind: Namespace
metadata:
  name: openshift-windows-machine-config-operator ❶
labels:
  openshift.io/cluster-monitoring: "true" ❷
```

- ❶ WMCO を **openshift-windows-machine-config-operator** namespace にデプロイすることが推奨されます。
- ❷ このラベルは、WMCO についてクラスターモニタリングを有効にするために必要です。

- b. namespace を作成します。

```
$ oc create -f <file-name>.yaml
```

以下に例を示します。

```
$ oc create -f wmco-namespace.yaml
```

2. WMCO の Operator グループを作成します。

- a. **OperatorGroup** オブジェクト YAML ファイルを作成します。例: **wmco-og.yaml**

```
apiVersion: operators.coreos.com/v1
kind: OperatorGroup
metadata:
  name: windows-machine-config-operator
  namespace: openshift-windows-machine-config-operator
spec:
  targetNamespaces:
    - openshift-windows-machine-config-operator
```

- b. Operator グループを作成します。

```
$ oc create -f <file-name>.yaml
```

以下に例を示します。

```
$ oc create -f wmco-og.yaml
```

3. namespace を WMCO にサブスクライブします。

- a. **Subscription** オブジェクト YAML ファイルを作成します。例: **wmco-sub.yaml**

```
apiVersion: operators.coreos.com/v1alpha1
kind: Subscription
metadata:
  name: windows-machine-config-operator
```



```
namespace: openshift-windows-machine-config-operator
spec:
  channel: "stable" ❶
  installPlanApproval: "Automatic" ❷
  name: "windows-machine-config-operator"
  source: "redhat-operators" ❸
  sourceNamespace: "openshift-marketplace" ❹
```

- ❶ **stable** をチャンネルとして指定します。
- ❷ 承認ストラテジーを設定します。 **Automatic** または **Manual** を設定できます。
- ❸ **windows-machine-config-operator** パッケージマニフェストが含まれる、 **redhat-operators** カタログソースを指定します。 OpenShift Container Platform が、非接続クラスターとも呼ばれる制限されたネットワークにインストールされている場合、Operator LifeCycle Manager (OLM) の設定時に作成した **CatalogSource** オブジェクトの名前を指定します。
- ❹ カタログソースの namespace。デフォルトの OperatorHub カタログソースには **openshift-marketplace** を使用します。

b. サブスクリプションを作成します。

```
$ oc create -f <file-name>.yaml
```

以下に例を示します。

```
$ oc create -f wmco-sub.yaml
```

WMCO が **openshift-windows-machine-config-operator** にインストールされるようになりました。

4. WMCO インストールを確認します。

```
$ oc get csv -n openshift-windows-machine-config-operator
```

出力例

```
NAME                                DISPLAY                                VERSION REPLACES PHASE
windows-machine-config-operator.2.0.0  Windows Machine Config Operator  2.0.0
Succeeded
```

4.2. WINDOWS MACHINE CONFIG OPERATOR のシークレットの設定

Windows Machine Config Operator (WMCO) を実行するには、プライベートキーを含む WMCO namespace でシークレットを作成する必要があります。これは、WMCO が Windows 仮想マシン (VM) と通信できるようにするために必要です。

前提条件

- Operator Lifecycle Manager (OLM) を使用して Windows Machine Config Operator (WMCO) をインストールしている。

- RSA キーが含まれる PEM でエンコードされたファイルを作成します。

手順

- Windows 仮想マシンへのアクセスに必要なシークレットを定義します。

```
$ oc create secret generic cloud-private-key --from-file=private-  
key.pem=${HOME}/.ssh/<key> \  
-n openshift-windows-machine-config-operator ①
```

- ① **openshift-windows-machine-config-operator** などの、WMCO namespace のプライベートキーを作成する必要があります。

クラスターのインストール時に使用されるものとは異なるプライベートキーを使用することが推奨されます。

4.3. 関連情報

- [クラスターノードの SSH アクセス用のキーペアの生成](#)
- [Operator のクラスターへの追加](#)

第5章 WINDOWS MACHINESET オブジェクトの作成

5.1. AWS での WINDOWS MACHINESET オブジェクトの作成

Amazon Web Services (AWS) で OpenShift Container Platform クラスターの特定の機能を果たすように **MachineSet** オブジェクトを作成することができます。たとえば、インフラストラクチャー Windows マシンセットおよび関連マシンを作成して、サポートする Windows ワークロードを新規の Windows マシンに移動できます。

前提条件

- Operator Lifecycle Manager (OLM) を使用して Windows Machine Config Operator (WMCO) をインストールしている。
- Docker フォーマットのコンテナランタイムアドオンが有効な状態で、サポートされている Windows Server をオペレーティングシステムのイメージとして使用している。次の **aws** コマンドを使用して、有効な AMI イメージを照会します。

```
$ aws ec2 describe-images --region <aws region name> --filters
"Name=name,Values=Windows_Server-2019*English*Full*Containers*" "Name=is-
public,Values=true" --query "reverse(sort_by(Images, &CreationDate))[*].{name: Name, id:
ImageId}" --output table
```



重要

現時点で、Docker 形式のコンテナランタイムは Windows ノードで使用されま
す。Kubernetes では、コンテナランタイムとしての Docker を非推奨として
います。詳細は、Kubernetes ドキュメントの [Docker の非推奨](#) について参照し
てください。Containerd は、今後の Kubernetes リリースで Windows ノードに
ついてサポートされる新しいコンテナランタイムになります。

5.1.1. マシン API の概要

マシン API は、アップストリームのクラスター API プロジェクトおよびカスタム OpenShift Container Platform リソースに基づく重要なリソースの組み合わせです。

OpenShift Container Platform 4.9 クラスターの場合、マシン API はクラスターインストールの終了後にすべてのノードホストのプロビジョニングの管理アクションを実行します。このシステムにより、OpenShift Container Platform 4.9 はパブリックまたはプライベートのクラウドインフラストラクチャーに加えて弾力性があり、動的なプロビジョニング方法を提供します。

以下の 2 つのリソースは重要なリソースになります。

Machines

ノードのホストを記述する基本的なユニットです。マシンには、複数の異なるクラウドプラットフォーム用に提供されるコンピュートノードのタイプを記述する **providerSpec** 仕様があります。たとえば、Amazon Web Services (AWS) 上のワーカーノードのマシンタイプは特定のマシンタイプおよび必要なメタデータを定義する場合があります。

マシンセット

MachineSet リソースはマシンのグループです。マシンセットとマシンの関係は、レプリカセットと Pod の関係と同様です。マシンを追加する必要がある場合や、マシンの数を縮小したりする必要がある場合、コンピューティングのニーズに応じてマシンセットの **replicas** フィールドを変更します。

**警告**

コントロールプレーンマシンは、マシンセットで管理することはできません。

以下のカスタムリソースは、クラスターに機能を追加します。

Machine Autoscaler

MachineAutoscaler リソースは、クラウド内のコンピューティングマシンを自動的にスケーリングします。指定したコンピューティングマシンセット内のノードの最小および最大スケーリング境界を設定でき Machine Autoscaler はそのノード範囲を維持します。

MachineAutoscaler オブジェクトは **ClusterAutoscaler** オブジェクトの設定後に有効になります。 **ClusterAutoscaler** および **MachineAutoscaler** リソースは、どちらも **ClusterAutoscalerOperator** オブジェクトによって利用可能にされます。

Cluster Autoscaler

このリソースはアップストリームの Cluster Autoscaler プロジェクトに基づいています。OpenShift Container Platform の実装では、これはマシンセット API を拡張することによってクラスター API に統合されます。コア、ノード、メモリー、および GPU などのリソースのクラスター全体でのスケーリング制限を設定できます。優先順位を設定することにより、重要度の低い Pod のために新規ノードがオンラインにならないようにクラスターで Pod の優先順位付けを実行できます。また、スケーリングポリシーを設定してノードをスケールダウンせずにスケールアップできるようにすることもできます。

マシンのヘルスチェック

MachineHealthCheck リソースはマシンの正常でない状態を検知し、マシンを削除し、サポートされているプラットフォームでは新規マシンを作成します。

OpenShift Container Platform バージョン 3.11 では、クラスターでマシンのプロビジョニングが管理されないためにマルチゾーンアーキテクチャーを容易に展開することができませんでした。しかし、OpenShift Container Platform バージョン 4.1 以降、このプロセスはより簡単になりました。それぞれのマシンセットのスコープが単一ゾーンに設定されるため、インストールプログラムはユーザーに代わって、アベイラビリティゾーン全体にマシンセットを送信します。さらに、コンピューティングは動的に展開されるため、ゾーンに障害が発生した場合、マシンのリバランスが必要な場合に使用するゾーンを常に確保できます。Autoscaler はクラスターの有効期間中にベストエフォートでbalancingを提供します。

5.1.2. AWS の Windows MachineSet オブジェクトのサンプル YAML

このサンプル YAML は、Windows Machine Config Operator (WMCO) が応答する Amazon Web Services (AWS) で実行される Windows **MachineSet** オブジェクトを定義します。

```
apiVersion: machine.openshift.io/v1beta1
kind: MachineSet
metadata:
  labels:
    machine.openshift.io/cluster-api-cluster: <infrastructure_id> 1
  name: <infrastructure_id>-windows-worker-<zone> 2
  namespace: openshift-machine-api
spec:
```

```
replicas: 1
selector:
  matchLabels:
    machine.openshift.io/cluster-api-cluster: <infrastructure_id> 3
    machine.openshift.io/cluster-api-machineset: <infrastructure_id>-windows-worker-<zone> 4
template:
  metadata:
    labels:
      machine.openshift.io/cluster-api-cluster: <infrastructure_id> 5
      machine.openshift.io/cluster-api-machine-role: worker
      machine.openshift.io/cluster-api-machine-type: worker
      machine.openshift.io/cluster-api-machineset: <infrastructure_id>-windows-worker-<zone> 6
      machine.openshift.io/os-id: Windows 7
  spec:
    metadata:
      labels:
        node-role.kubernetes.io/worker: "" 8
    providerSpec:
      value:
        ami:
          id: <windows_container_ami> 9
        apiVersion: awsproviderconfig.openshift.io/v1beta1
        blockDevices:
          - ebs:
              iops: 0
              volumeSize: 120
              volumeType: gp2
        credentialsSecret:
          name: aws-cloud-credentials
        deviceIndex: 0
        iamInstanceProfile:
          id: <infrastructure_id>-worker-profile 10
        instanceType: m5a.large
        kind: AWSMachineProviderConfig
        placement:
          availabilityZone: <zone> 11
          region: <region> 12
        securityGroups:
          - filters:
              - name: tag:Name
                values:
                  - <infrastructure_id>-worker-sg 13
        subnet:
          filters:
            - name: tag:Name
              values:
                - <infrastructure_id>-private-<zone> 14
        tags:
          - name: kubernetes.io/cluster/<infrastructure_id> 15
            value: owned
        userDataSecret:
          name: windows-user-data 16
          namespace: openshift-machine-api
```

- 1 3 5 10 13 14 15 クラスターのプロビジョニング時に設定したクラスター ID を基にするインフラストラクチャー ID を指定します。以下のコマンドを実行してインフラストラク

```
$ oc get -o jsonpath='{.status.infrastructureName}' infrastructure cluster
```

- 2 4 6 インフラストラクチャー ID、ワーカーラベル、およびゾーンを指定します。
- 7 Windows マシンとしてマシンセットを設定します。
- 8 Windows ノードをコンピュータマシンとして設定します。
- 9 コンテナランタイムがインストールされている Windows イメージの AMI ID を指定します。Windows Server 2019 を使用する必要があります。
- 11 **us-east-1a** などの AWS ゾーンを指定します。
- 12 **us-east-1** などの AWS リージョンを指定します。
- 16 最初の Windows マシンの設定時に WMCO によって作成されます。その後、後続のすべてのマシンセットで **windows-user-data** を消費できるようになります。

5.1.3. マシンセットの作成

インストールプログラムによって作成されるコンピュータマシンセットの他に、独自に作成して、選択する特定のワークロードに対するマシンのコンピュータリソースを動的に管理することができます。

前提条件

- OpenShift Container Platform クラスターをデプロイすること。
- OpenShift CLI (**oc**) をインストールしている。
- **cluster-admin** パーミッションを持つユーザーとして、**oc** にログインする。

手順

1. 説明されているようにマシンセット カスタムリソース (CR) サンプルを含む新規 YAML ファイルを作成し、そのファイルに **<file_name>.yaml** という名前を付けます。
<clusterID> および **<role>** パラメーターの値を設定していることを確認します。
2. オプション：特定のフィールドに設定する値が不明な場合は、クラスターから既存のコンピュータマシンセットを確認できます。
 - a. クラスター内のコンピュータマシンセットを一覧表示するには、以下のコマンドを実行します。

```
$ oc get machinesets -n openshift-machine-api
```

出力例

```
NAME                                DESIRED  CURRENT  READY  AVAILABLE  AGE
agl030519-vplxx-worker-us-east-1a  1        1        1      1          55m
agl030519-vplxx-worker-us-east-1b  1        1        1      1          55m
agl030519-vplxx-worker-us-east-1c  1        1        1      1          55m
```

```
agl030519-vplxk-worker-us-east-1d 0 0 55m
agl030519-vplxk-worker-us-east-1e 0 0 55m
agl030519-vplxk-worker-us-east-1f 0 0 55m
```

- b. 特定のコンピュータマシンセットカスタムリソース(CR)の値を表示するには、以下のコマンドを実行します。

```
$ oc get machineset <machineset_name> \
-n openshift-machine-api -o yaml
```

出力例

```
apiVersion: machine.openshift.io/v1beta1
kind: MachineSet
metadata:
  labels:
    machine.openshift.io/cluster-api-cluster: <infrastructure_id> 1
    name: <infrastructure_id>-<role> 2
    namespace: openshift-machine-api
spec:
  replicas: 1
  selector:
    matchLabels:
      machine.openshift.io/cluster-api-cluster: <infrastructure_id>
      machine.openshift.io/cluster-api-machineset: <infrastructure_id>-<role>
  template:
    metadata:
      labels:
        machine.openshift.io/cluster-api-cluster: <infrastructure_id>
        machine.openshift.io/cluster-api-machine-role: <role>
        machine.openshift.io/cluster-api-machine-type: <role>
        machine.openshift.io/cluster-api-machineset: <infrastructure_id>-<role>
    spec:
      providerSpec: 3
      ...
```

1 クラスタインフラストラクチャー ID。

2 デフォルトのノードラベル。



注記

ユーザーによってプロビジョニングされるインフラストラクチャーを持つクラスターの場合、コンピュータマシンセットは **ワーカー** および **インフラ** タイプのマシンのみを作成できます。

3 コンピュータマシンセット CR の **<providerSpec>** セクションの値はプラットフォーム固有です。CR の **<providerSpec>** パラメーターの詳細は、プロバイダーのコンピュータマシンセット CR の設定例を参照してください。

3. 以下のコマンドを実行して **MachineSet** CR を作成します。

```
$ oc create -f <file_name>.yaml
```

検証

- 次のコマンドを実行して、コンピューティングマシンのリストを表示します。

```
$ oc get machineset -n openshift-machine-api
```

出力例

NAME	DESIRED	CURRENT	READY	AVAILABLE	AGE
agl030519-vplxk-windows-worker-us-east-1a	1	1	1	1	11m
agl030519-vplxk-worker-us-east-1a	1	1	1	1	55m
agl030519-vplxk-worker-us-east-1b	1	1	1	1	55m
agl030519-vplxk-worker-us-east-1c	1	1	1	1	55m
agl030519-vplxk-worker-us-east-1d	0	0			55m
agl030519-vplxk-worker-us-east-1e	0	0			55m
agl030519-vplxk-worker-us-east-1f	0	0			55m

新規のマシンセットが利用可能な場合、**DESIRED** および **CURRENT** の値は一致します。マシンセットが利用可能でない場合、数分待機してからコマンドを再度実行します。

5.1.4. 関連情報

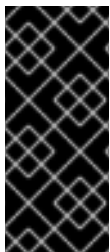
- マシンセットの管理に関する詳細は、[マシン管理セクション](#)を参照してください。

5.2. AZURE での WINDOWS MACHINESET オブジェクトの作成

Microsoft Azure 上の OpenShift Container Platform クラスタで特定の機能を果たすように Windows **MachineSet** オブジェクトを作成できます。たとえば、インフラストラクチャー Windows マシンセットおよび関連マシンを作成して、サポートする Windows ワークロードを新規の Windows マシンに移動できます。

前提条件

- Operator Lifecycle Manager (OLM) を使用して Windows Machine Config Operator (WMCO) をインストールしている。
- Docker フォーマットのコンテナランタイムアドオンが有効な状態で、サポートされている Windows Server をオペレーティングシステムのイメージとして使用している。



重要

現時点で、Docker 形式のコンテナランタイムは Windows ノードで使用されます。Kubernetes では、コンテナランタイムとしての Docker を非推奨としています。詳細は、Kubernetes ドキュメントの [Docker の非推奨](#) について参照してください。Containerd は、今後の Kubernetes リリースで Windows ノードについてサポートされる新しいコンテナランタイムになります。

5.2.1. マシン API の概要

マシン API は、アップストリームのクラスタ API プロジェクトおよびカスタム OpenShift Container Platform リソースに基づく重要なリソースの組み合わせです。

OpenShift Container Platform 4.9 クラスターの場合、マシン API はクラスターインストールの終了後にすべてのノードホストのプロビジョニングの管理アクションを実行します。このシステムにより、OpenShift Container Platform 4.9 はパブリックまたはプライベートのクラウドインフラストラクチャーに加えて弾力性があり、動的なプロビジョニング方法を提供します。

以下の2つのリソースは重要なリソースになります。

Machines

ノードのホストを記述する基本的なユニットです。マシンには、複数の異なるクラウドプラットフォーム用に提供されるコンピュートノードのタイプを記述する **providerSpec** 仕様があります。たとえば、Amazon Web Services (AWS) 上のワーカーノードのマシンタイプは特定のマシンタイプおよび必要なメタデータを定義する場合があります。

マシンセット

MachineSet リソースはマシンのグループです。マシンセットとマシンの関係は、レプリカセットと Pod の関係と同様です。マシンを追加する必要がある場合や、マシンの数を縮小したりする必要がある場合、コンピューティングのニーズに応じてマシンセットの **replicas** フィールドを変更します。



警告

コントロールプレーンマシンは、マシンセットで管理することはできません。

以下のカスタムリソースは、クラスターに機能を追加します。

Machine Autoscaler

MachineAutoscaler リソースは、クラウド内のコンピューティングマシンを自動的にスケーリングします。指定したコンピューティングマシンセット内のノードの最小および最大スケーリング境界を設定でき Machine Autoscaler はそのノード範囲を維持します。

MachineAutoscaler オブジェクトは **ClusterAutoscaler** オブジェクトの設定後に有効になります。**ClusterAutoscaler** および **MachineAutoscaler** リソースは、どちらも **ClusterAutoscalerOperator** オブジェクトによって利用可能にされます。

Cluster Autoscaler

このリソースはアップストリームの Cluster Autoscaler プロジェクトに基づいています。OpenShift Container Platform の実装では、これはマシンセット API を拡張することによってクラスター API に統合されます。コア、ノード、メモリー、および GPU などのリソースのクラスター全体でのスケーリング制限を設定できます。優先順位を設定することにより、重要度の低い Pod のために新規ノードがオンラインにならないようにクラスターで Pod の優先順位付けを実行できます。また、スケーリングポリシーを設定してノードをスケールダウンせずにスケールアップできるようにすることもできます。

マシンのヘルスチェック

MachineHealthCheck リソースはマシンの正常でない状態を検知し、マシンを削除し、サポートされているプラットフォームでは新規マシンを作成します。

OpenShift Container Platform バージョン 3.11 では、クラスターでマシンのプロビジョニングが管理されないためにマルチゾーンアーキテクチャーを容易に展開することができませんでした。しかし、OpenShift Container Platform バージョン 4.1以降、このプロセスはより簡単になりました。それぞれ

のマシンセットの範囲が単一ゾーンに設定されるため、インストールプログラムはユーザーに代わって、アベイラビリティゾーン全体にマシンセットを送信します。さらに、コンピューティングは動的に展開されるため、ゾーンに障害が発生した場合、マシンのリバランスが必要な場合に使用するゾーンを常に確保できます。Autoscaler はクラスターの有効期間中にベストエフォートでバランスを提供します。

5.2.2. Azure の Windows MachineSet オブジェクトのサンプル YAML

このサンプル YAML は、Windows Machine Config Operator (WMCO) が応答する Microsoft Azure で実行される Windows **MachineSet** オブジェクトを定義します。

```

apiVersion: machine.openshift.io/v1beta1
kind: MachineSet
metadata:
  labels:
    machine.openshift.io/cluster-api-cluster: <infrastructure_id> ❶
  name: <windows_machine_set_name> ❷
  namespace: openshift-machine-api
spec:
  replicas: 1
  selector:
    matchLabels:
      machine.openshift.io/cluster-api-cluster: <infrastructure_id> ❸
      machine.openshift.io/cluster-api-machineset: <windows_machine_set_name> ❹
  template:
    metadata:
      labels:
        machine.openshift.io/cluster-api-cluster: <infrastructure_id> ❺
        machine.openshift.io/cluster-api-machine-role: worker
        machine.openshift.io/cluster-api-machine-type: worker
        machine.openshift.io/cluster-api-machineset: <windows_machine_set_name> ❻
        machine.openshift.io/os-id: Windows ❼
    spec:
      metadata:
        labels:
          node-role.kubernetes.io/worker: "" ❽
      providerSpec:
        value:
          apiVersion: azureproviderconfig.openshift.io/v1beta1
          credentialsSecret:
            name: azure-cloud-credentials
            namespace: openshift-machine-api
          image: ❾
          offer: WindowsServer
          publisher: MicrosoftWindowsServer
          resourceID: ""
          sku: 2019-Datacenter-with-Containers
          version: latest
          kind: AzureMachineProviderSpec
          location: <location> ❿
          managedIdentity: <infrastructure_id>-identity ⓫
          networkResourceGroup: <infrastructure_id>-rg ⓬
          osDisk:
            diskSizeGB: 128

```

```

managedDisk:
  storageAccountType: Premium_LRS
osType: Windows
publicIP: false
resourceGroup: <infrastructure_id>-rg 13
subnet: <infrastructure_id>-worker-subnet
userDataSecret:
  name: windows-user-data 14
  namespace: openshift-machine-api
vmSize: Standard_D2s_v3
vnet: <infrastructure_id>-vnet 15
zone: "<zone>" 16

```

- 1 3 5 11 12 13 15 クラスターのプロビジョニング時に設定したクラスター ID を基にするインフラストラクチャー ID を指定します。以下のコマンドを実行してインフラストラクチャー ID を取得できます。

```
$ oc get -o jsonpath='{.status.infrastructureName}' infrastructure cluster
```

- 2 4 6 Windows マシンセット名を指定します。Azure の Windows マシン名は 15 文字を超えることができません。そのため、マシン名の生成方法により、マシンセット名は 9 文字を超えることができません。
- 7 Windows マシンとしてマシンセットを設定します。
- 8 Windows ノードをコンピュータマシンとして設定します。
- 9 **2019-Datacenter-with-Containers** SKU を定義する **WindowsServer** イメージオフリングを指定します。
- 10 **centralus** などの Azure リージョンを指定します。
- 14 最初の Windows マシンの設定時に WMCO によって作成されます。その後、後続のすべてのマシンセットで **windows-user-data** を消費できるようになります。
- 16 マシンを配置するリージョン内のゾーンを指定します。リージョンがゾーンをサポートすることを確認してください。

5.2.3. マシンセットの作成

インストールプログラムによって作成されるコンピュータマシンセットの他に、独自に作成して、選択する特定のワークロードに対するマシンのコンピュータリソースを動的に管理することができます。

前提条件

- OpenShift Container Platform クラスターをデプロイすること。
- OpenShift CLI (**oc**) をインストールしている。
- **cluster-admin** パーミッションを持つユーザーとして、**oc** にログインする。

手順

1. 説明されているようにマシンセット カスタムリソース (CR) サンプルを含む新規 YAML ファイルを作成し、そのファイルに `<file_name>.yaml` という名前を付けます。
`<clusterID>` および `<role>` パラメーターの値を設定していることを確認します。
2. オプション：特定のフィールドに設定する値が不明な場合は、クラスターから既存のコンピュートマシンセットを確認できます。
 - a. クラスター内のコンピュートマシンセットを一覧表示するには、以下のコマンドを実行します。

```
$ oc get machinesets -n openshift-machine-api
```

出力例

```
NAME                                DESIRED  CURRENT  READY  AVAILABLE  AGE
agl030519-vplxk-worker-us-east-1a  1        1        1      1          55m
agl030519-vplxk-worker-us-east-1b  1        1        1      1          55m
agl030519-vplxk-worker-us-east-1c  1        1        1      1          55m
agl030519-vplxk-worker-us-east-1d  0        0                55m
agl030519-vplxk-worker-us-east-1e  0        0                55m
agl030519-vplxk-worker-us-east-1f  0        0                55m
```

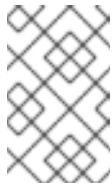
- b. 特定のコンピュートマシンセットカスタムリソース(CR)の値を表示するには、以下のコマンドを実行します。

```
$ oc get machineset <machineset_name> \
-n openshift-machine-api -o yaml
```

出力例

```
apiVersion: machine.openshift.io/v1beta1
kind: MachineSet
metadata:
  labels:
    machine.openshift.io/cluster-api-cluster: <infrastructure_id> ❶
  name: <infrastructure_id>-<role> ❷
  namespace: openshift-machine-api
spec:
  replicas: 1
  selector:
    matchLabels:
      machine.openshift.io/cluster-api-cluster: <infrastructure_id>
      machine.openshift.io/cluster-api-machineset: <infrastructure_id>-<role>
  template:
    metadata:
      labels:
        machine.openshift.io/cluster-api-cluster: <infrastructure_id>
        machine.openshift.io/cluster-api-machine-role: <role>
        machine.openshift.io/cluster-api-machine-type: <role>
        machine.openshift.io/cluster-api-machineset: <infrastructure_id>-<role>
    spec:
      providerSpec: ❸
      ...
```

- 1 クラスターインフラストラクチャー ID。
- 2 デフォルトのノードラベル。



注記

ユーザーによってプロビジョニングされるインフラストラクチャーを持つクラスターの場合、コンピュータマシンセットは **ワーカー** および **インフラ** タイプのマシンのみを作成できます。

- 3 コンピュータマシンセット CR の **<providerSpec>** セクションの値はプラットフォーム固有です。CR の **<providerSpec>** パラメーターの詳細は、プロバイダーのコンピュータマシンセット CR の設定例を参照してください。

3. 以下のコマンドを実行して **MachineSet** CR を作成します。

```
$ oc create -f <file_name>.yaml
```

検証

- 次のコマンドを実行して、コンピュータマシンセットのリストを表示します。

```
$ oc get machineset -n openshift-machine-api
```

出力例

NAME	DESIRED	CURRENT	READY	AVAILABLE	AGE
agl030519-vplxk-windows-worker-us-east-1a	1	1	1	1	11m
agl030519-vplxk-worker-us-east-1a	1	1	1	1	55m
agl030519-vplxk-worker-us-east-1b	1	1	1	1	55m
agl030519-vplxk-worker-us-east-1c	1	1	1	1	55m
agl030519-vplxk-worker-us-east-1d	0	0			55m
agl030519-vplxk-worker-us-east-1e	0	0			55m
agl030519-vplxk-worker-us-east-1f	0	0			55m

新規のマシンセットが利用可能な場合、**DESIRED** および **CURRENT** の値は一致します。マシンセットが利用可能でない場合、数分待機してからコマンドを再度実行します。

5.2.4. 関連情報

- マシンセットの管理に関する詳細は、**マシン管理**セクションを参照してください。

5.3. VSPHERE での WINDOWS MACHINESET オブジェクトの作成

VMware vSphere 上の OpenShift Container Platform クラスターで特定の機能を果たすように Windows **MachineSet** オブジェクトを作成できます。たとえば、インフラストラクチャー Windows マシンセットおよび関連マシンを作成して、サポートする Windows ワークロードを新規の Windows マシンに移動できます。

前提条件

- Operator Lifecycle Manager (OLM) を使用して Windows Machine Config Operator (WMCO) をインストールしている。
- Docker フォーマットのコンテナランタイムアドオンが有効な状態で、サポートされている Windows Server をオペレーティングシステムのイメージとして使用している。



重要

現時点で、Docker 形式のコンテナランタイムは Windows ノードで使用されます。Kubernetes では、コンテナランタイムとしての Docker を非推奨としています。詳細は、Kubernetes ドキュメントの [Docker の非推奨](#) について参照してください。Containerd は、今後の Kubernetes リリースで Windows ノードについてサポートされる新しいコンテナランタイムになります。

5.3.1. マシン API の概要

マシン API は、アップストリームのクラスター API プロジェクトおよびカスタム OpenShift Container Platform リソースに基づく重要なリソースの組み合わせです。

OpenShift Container Platform 4.9 クラスターの場合、マシン API はクラスターインストールの終了後にすべてのノードホストのプロビジョニングの管理アクションを実行します。このシステムにより、OpenShift Container Platform 4.9 はパブリックまたはプライベートのクラウドインフラストラクチャーに加えて弾力性があり、動的なプロビジョニング方法を提供します。

以下の 2 つのリソースは重要なリソースになります。

Machines

ノードのホストを記述する基本的なユニットです。マシンには、複数の異なるクラウドプラットフォーム用に提供されるコンピュートノードのタイプを記述する **providerSpec** 仕様があります。たとえば、Amazon Web Services (AWS) 上のワーカーノードのマシンタイプは特定のマシンタイプおよび必要なメタデータを定義する場合があります。

マシンセット

MachineSet リソースはマシンのグループです。マシンセットとマシンの関係は、レプリカセットと Pod の関係と同様です。マシンを追加する必要がある場合や、マシンの数を縮小したりする必要がある場合、コンピューティングのニーズに応じてマシンセットの **replicas** フィールドを変更します。



警告

コントロールプレーンマシンは、マシンセットで管理することはできません。

以下のカスタムリソースは、クラスターに機能を追加します。

Machine Autoscaler

MachineAutoscaler リソースは、クラウド内のコンピューティングマシンを自動的にスケールリングします。指定したコンピューティングマシンセット内のノードの最小および最大スケールリング境界を設定でき Machine Autoscaler はそのノード範囲を維持します。

MachineAutoscaler オブジェクトは **ClusterAutoscaler** オブジェクトの設定後に有効になります。**ClusterAutoscaler** および **MachineAutoscaler** リソースは、どちらも **ClusterAutoscalerOperator** オブジェクトによって利用可能にされます。

Cluster Autoscaler

このリソースはアップストリームの Cluster Autoscaler プロジェクトに基づいています。OpenShift Container Platform の実装では、これはマシンセット API を拡張することによってクラスター API に統合されます。コア、ノード、メモリー、および GPU などのリソースのクラスター全体でのスケール制限を設定できます。優先順位を設定することにより、重要度の低い Pod のために新規ノードがオンラインにならないようにクラスターで Pod の優先順位付けを実行できます。また、スケールポリシーを設定してノードをスケールダウンせずにスケールアップできるようにすることもできます。

マシンのヘルスチェック

MachineHealthCheck リソースはマシンの正常でない状態を検知し、マシンを削除し、サポートされているプラットフォームでは新規マシンを作成します。

OpenShift Container Platform バージョン 3.11 では、クラスターでマシンのプロビジョニングが管理されないためにマルチゾーンアーキテクチャーを容易に展開することができませんでした。しかし、OpenShift Container Platform バージョン 4.1 以降、このプロセスはより簡単になりました。それぞれのマシンセットのスコープが単一ゾーンに設定されるため、インストールプログラムはユーザーに代わって、アベイラビリティゾーン全体にマシンセットを送信します。さらに、コンピューティングは動的に展開されるため、ゾーンに障害が発生した場合、マシンのリバランスが必要な場合に使用するゾーンを常に確保できます。Autoscaler はクラスターの有効期間中にベストエフォートでバルランシングを提供します。

5.3.2. Windows コンテナワークロード用の vSphere 環境の準備

vSphere Windows 仮想マシンのゴールドイメージを作成し、WMCO の内部 API サーバーとの通信を有効にして、Windows コンテナのワークロード用に vSphere 環境を準備する必要があります。

5.3.2.1. vSphere Windows 仮想マシンのゴールドイメージの作成

vSphere Windows 仮想マシン (VM) のゴールドイメージを作成します。

前提条件

- OpenSSH サーバーで鍵ベースの認証を設定するのに使用する、秘密鍵/公開鍵ペアを作成している。プライベートキーは Windows Machine Config Operator(WMCO) namespace でも設定される必要があります。これは、WMCO が Windows 仮想マシンと通信できるようにするために必要です。詳細は、Windows Machine Config Operator のシークレットの設定のセクションを参照してください。

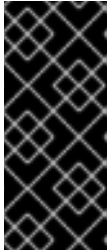


注記

Windows 仮想マシンを作成する際には、複数のケースで [Microsoft PowerShell](#) コマンドを使用する必要があります。本書の PowerShell コマンドは、**PS C:\>** 接頭辞によって区別されます。

手順

1. Windows Server Semi-Annual Channel (SAC) ([Microsoft パッチ KB4565351](#) を含む Windows Server 20H2 ISO イメージ) を使用して、vSphere クライアントに新しい仮想マシンを作成します。このパッチは、vSphere にインストールされたクラスターに必要な VXLAN UDP ポートの設定に必要です。詳細は、[VMware ドキュメント](#) を参照してください。



重要

VM の仮想ハードウェアバージョンは、OpenShift Container Platform のインフラストラクチャー要件を満たしている必要があります。詳細については、OpenShift Container Platform ドキュメントの VMware vSphere インフラストラクチャーの要件セクションを参照してください。また、[仮想マシンのハードウェアバージョン](#) に関する VMware のドキュメントを参照することもできます。

2. Windows 仮想マシンに VMware Tools バージョン 11.0.6 以降をインストールし、設定します。詳細は、[VMware Tools のドキュメント](#) を参照してください。
3. Windows 仮想マシンに VMware Tools をインストールした後、以下を確認します。
 - a. **C:\ProgramData\VMware\VMware Tools\tools.conf** ファイルが、以下のエントリーとともに存在します。

```
exclude-nics=
```

tools.conf ファイルが存在しない場合は、**exclude-nics** オプションでコメント解除した状態でこれを作成し、空の値に設定します。

このエントリーにより、ハイブリッドオーバーレイで Windows 仮想マシンで生成され、クローン作成された vNIC は無視されないようにします。

- b. Windows 仮想マシンには、vCenter で有効な IP アドレスがあります。

```
C:\> ipconfig
```

- c. VMTools Windows サービスが実行中である。

```
PS C:\> Get-Service -Name VMTools | Select Status, StartType
```

4. Windows 仮想マシンに OpenSSH Server をインストールし、設定します。詳細は、Microsoft ドキュメントの [Installing OpenSSH](#) を参照してください。
5. 管理ユーザーの SSH アクセスを設定します。そのためには、Microsoft のドキュメント [Administrative user](#) を参照してください。



重要

命令に使用されるパブリックキーは、シークレットを保持する WMCO namespace で後に作成するプライベートキーに対応している必要があります。詳細は、Windows Machine Config Operator のシークレットの設定のセクションを参照してください。

6. [Microsoft ドキュメント](#) に従って、Windows 仮想マシンに **docker** コンテナランタイムをインストールします。
7. コンテナログの受信接続を可能にする新しいファイアウォールルールを Windows 仮想マシンに作成する必要があります。以下の PowerShell コマンドを実行して、TCP ポート 10250 にファイアウォールルールを作成します。

```
PS C:\> New-NetFirewallRule -DisplayName "ContainerLogsPort" -LocalPort 10250 -Enabled True -Direction Inbound -Protocol TCP -Action Allow -EdgeTraversalPolicy Allow
```


8. Windows 仮想マシンのクローンを作成し、再利用可能なイメージにします。詳細は、VMware ドキュメントで [既存の仮想マシンのクローンを作成](#) する方法を参照してください。
9. クローン作成した Windows 仮想マシンで、[Windows Sysprep ツール](#) を実行します。

```
C:\> C:\Windows\System32\Sysprep\sysprep.exe /generalize /oobe /shutdown /unattend:
<path_to_unattend.xml> ❶
```

- ❶ **unattend.xml** ファイルへのパスを指定します。



注記

Windows イメージで **sysprep** コマンドを実行することができる回数に制限があります。詳細は、Microsoft の [ドキュメント](#) を参照してください。

サンプルの **unattend.xml** が提供され、これは WMCO で必要なすべての変更を維持します。この例では変更する必要があります。直接使用することはできません。

例5.1 サンプル unattend.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<unattend xmlns="urn:schemas-microsoft-com:unattend">
  <settings pass="specialize">
    <component xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" name="Microsoft-Windows-
      International-Core" processorArchitecture="amd64"
      publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS">
      <InputLocale>0409:00000409</InputLocale>
      <SystemLocale>en-US</SystemLocale>
      <UILanguage>en-US</UILanguage>
      <UILanguageFallback>en-US</UILanguageFallback>
      <UserLocale>en-US</UserLocale>
    </component>
    <component xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" name="Microsoft-Windows-
      Security-SPP-UX" processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35"
      language="neutral" versionScope="nonSxS">
      <SkipAutoActivation>true</SkipAutoActivation>
    </component>
    <component xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" name="Microsoft-Windows-
      SQMApi" processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35"
      language="neutral" versionScope="nonSxS">
      <CEIPEnabled>0</CEIPEnabled>
    </component>
    <component xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" name="Microsoft-Windows-
      Shell-Setup" processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35"
      language="neutral" versionScope="nonSxS">
      <ComputerName>winhost</ComputerName> ❶
    </component>
  </settings>
</settings pass="oobeSystem">
```

```

<component xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" name="Microsoft-Windows-
Shell-Setup" processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35"
language="neutral" versionScope="nonSxS">
  <AutoLogon>
    <Enabled>>false</Enabled> 2
  </AutoLogon>
  <OOBE>
    <HideEULAPage>>true</HideEULAPage>
    <HideLocalAccountScreen>>true</HideLocalAccountScreen>
    <HideOEMRegistrationScreen>>true</HideOEMRegistrationScreen>
    <HideOnlineAccountScreens>>true</HideOnlineAccountScreens>
    <HideWirelessSetupInOOBE>>true</HideWirelessSetupInOOBE>
    <NetworkLocation>Work</NetworkLocation>
    <ProtectYourPC>1</ProtectYourPC>
    <SkipMachineOOBE>>true</SkipMachineOOBE>
    <SkipUserOOBE>>true</SkipUserOOBE>
  </OOBE>
  <RegisteredOrganization>Organization</RegisteredOrganization>
  <RegisteredOwner>Owner</RegisteredOwner>
  <DisableAutoDaylightTimeSet>>false</DisableAutoDaylightTimeSet>
  <TimeZone>Eastern Standard Time</TimeZone>
  <UserAccounts>
    <AdministratorPassword>
      <Value>MyPassword</Value> 3
      <PlainText>>true</PlainText>
    </AdministratorPassword>
  </UserAccounts>
</component>
</settings>
</unattend>

```

- 1 **Kubernetes の名前**の仕様 に従いなければならない **ComputerName** を指定します。これらの仕様は、新規仮想マシンの作成時に作成されるテンプレートで実行されるゲスト OS のカスタマイズにも適用されます。
- 2 自動ログオンを無効にして、起動時に管理者権限で開いているターミナルをそのまま残すセキュリティの問題を回避します。これはデフォルト値であるため、変更しないでください。
- 3 **MyPassword** プレースホルダーを Administrator アカウントのパスワードに置き換えます。これにより、組み込みの Administrator アカウントはデフォルトで空のパスワードを持つことを防ぎます。Microsoft の [パスワードを選択するベストプラクティス](#) に従ってください。

Sysprep ツールが完了すると、Windows 仮想マシンの電源がオフになります。この仮想マシンで使用または電源は使用しないでください。

10. Windows 仮想マシンを [vCenter のテンプレート](#) に変換します。

5.3.2.1.1. 関連情報

- [Windows Machine Config Operator のシークレットの設定](#)

- VMware vSphere インフラストラクチャーの要件

5.3.2.2. vSphere での WMCO についての内部 API サーバーとの通信の有効化

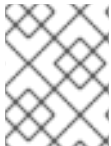
Windows Machine Config Operator (WMCO) は Ignition 設定ファイルを内部 API サーバーエンドポイントからダウンロードします。Windows 仮想マシン (VM) が Ignition 設定ファイルをダウンロードできるように、また設定された仮想マシンが kubelet が内部 API サーバーとのみ通信できるように内部 API サーバーとの通信を有効にする必要があります。

前提条件

- クラスタを vSphere にインストールしている。

手順

- 外部 API サーバー URL `api.<cluster_name>.<base_domain>` を参照する `api-int.<cluster_name>.<base_domain>` の新規 DNS エントリを追加します。これには、CNAME または追加の A レコードを指定できます。



注記

外部 API エンドポイントは、vSphere への初期クラスタインストールの一部としてすでに作成されています。

5.3.3. vSphere での Windows の MachineSet オブジェクトのサンプル YAML

このサンプル YAML は、Windows Machine Config Operator (WMCO) が応答する VMware vSphere で実行される Windows **MachineSet** オブジェクトを定義します。

```
apiVersion: machine.openshift.io/v1beta1
kind: MachineSet
metadata:
  labels:
    machine.openshift.io/cluster-api-cluster: <infrastructure_id> ❶
  name: <windows_machine_set_name> ❷
  namespace: openshift-machine-api
spec:
  replicas: 1
  selector:
    matchLabels:
      machine.openshift.io/cluster-api-cluster: <infrastructure_id> ❸
      machine.openshift.io/cluster-api-machineset: <windows_machine_set_name> ❹
  template:
    metadata:
      labels:
        machine.openshift.io/cluster-api-cluster: <infrastructure_id> ❺
        machine.openshift.io/cluster-api-machine-role: worker
        machine.openshift.io/cluster-api-machine-type: worker
        machine.openshift.io/cluster-api-machineset: <windows_machine_set_name> ❻
        machine.openshift.io/os-id: Windows ❼
    spec:
      metadata:
        labels:
```

```

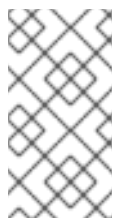
node-role.kubernetes.io/worker: "" 8
providerSpec:
  value:
    apiVersion: vsphereprovider.openshift.io/v1beta1
    credentialsSecret:
      name: vsphere-cloud-credentials
    diskGiB: 128 9
    kind: VSphereMachineProviderSpec
    memoryMiB: 16384
    network:
      devices:
        - networkName: "<vm_network_name>" 10
    numCPUs: 4
    numCoresPerSocket: 1
    snapshot: ""
    template: <windows_vm_template_name> 11
    userDataSecret:
      name: windows-user-data 12
    workspace:
      datacenter: <vcenter_datacenter_name> 13
      datastore: <vcenter_datastore_name> 14
      folder: <vcenter_vm_folder_path> 15
      resourcePool: <vsphere_resource_pool> 16
      server: <vcenter_server_ip> 17

```

- 1 3 5 クラスターのプロビジョニング時に設定したクラスター ID を基にするインフラストラクチャー ID を指定します。以下のコマンドを実行してインフラストラクチャー ID を取得できません。

```
$ oc get -o jsonpath='{.status.infrastructureName}' infrastructure cluster
```

- 2 4 6 Windows マシンセット名を指定します。マシンセットの名前は、マシン名が vSphere で生成される方法により、9 文字を超えることができません。
- 7 Windows マシンとしてマシンセットを設定します。
- 8 Windows ノードをコンピュータマシンとして設定します。
- 9 vSphere 仮想マシンディスク (VMDK) のサイズを指定します。



注記

このパラメーターは、Windows パーティションのサイズを設定しません。**unattend.xml** ファイルを使用するか、必要なディスクサイズで vSphere Windows 仮想マシン (VM) ゴールデンイメージを作成することにより、Windows パーティションのサイズを変更できます。

- 10 マシンセットをデプロイする vSphere 仮想マシンネットワークを指定します。この仮想マシンネットワークは、他の Linux コンピューティングマシンがクラスター内に存在する場所である必要があります。
- 11 **golden-images/windows-server-template** などの、使用する Windows vSphere 仮想マシンテンプレートの完全パスを指定します。名前は一意である必要があります。



重要

元の仮想マシンテンプレートは指定しないでください。仮想マシンテンプレートは停止した状態でなければなりません。また、新規の Windows マシン用にクローン作成する必要があります。仮想マシンテンプレートを起動すると、仮想マシンテンプレートがプラットフォームの仮想マシンとして設定されるので、これをマシンセットで設定を適用できるテンプレートとして使用できなくなります。

- 12 **windows-user-data** は、最初の Windows マシンの設定時に WMCO によって作成されます。その後、後続のすべてのマシンセットで **windows-user-data** を消費できるようになります。
- 13 マシンセットをデプロイする vCenter Datacenter を指定します。
- 14 マシンセットをデプロイする vCenter Datastore を指定します。
- 15 `/dc1/vm/user-inst-5ddjd` などの vCenter の vSphere 仮想マシンフォルダーへのパスを指定します。
- 16 オプション: Windows 仮想マシンの vSphere リソースプールを指定します。
- 17 vCenter サーバーの IP または完全修飾ドメイン名を指定します。

5.3.4. マシンセットの作成

インストールプログラムによって作成されるコンピュータマシンセットの他に、独自に作成して、選択する特定のワークロードに対するマシンのコンピュータリソースを動的に管理することができます。

前提条件

- OpenShift Container Platform クラスタをデプロイすること。
- OpenShift CLI (**oc**) をインストールしている。
- **cluster-admin** パーミッションを持つユーザーとして、**oc** にログインする。

手順

1. 説明されているようにマシンセット カスタムリソース (CR) サンプルを含む新規 YAML ファイルを作成し、そのファイルに `<file_name>.yaml` という名前を付けます。
`<clusterID>` および `<role>` パラメーターの値を設定していることを確認します。
2. オプション: 特定のフィールドに設定する値が不明な場合は、クラスタから既存のコンピュータマシンセットを確認できます。
 - a. クラスタ内のコンピュータマシンセットを一覧表示するには、以下のコマンドを実行します。

```
$ oc get machinesets -n openshift-machine-api
```

出力例

```
NAME                                DESIRED  CURRENT  READY  AVAILABLE  AGE
agl030519-vplxk-worker-us-east-1a  1        1        1      1          55m
agl030519-vplxk-worker-us-east-1b  1        1        1      1          55m
```

```

agl030519-vplxx-worker-us-east-1c 1 1 1 1 55m
agl030519-vplxx-worker-us-east-1d 0 0 0 0 55m
agl030519-vplxx-worker-us-east-1e 0 0 0 0 55m
agl030519-vplxx-worker-us-east-1f 0 0 0 0 55m

```

- b. 特定のコンピュータマシンセットカスタムリソース(CR)の値を表示するには、以下のコマンドを実行します。

```

$ oc get machineset <machineset_name> \
-n openshift-machine-api -o yaml

```

出力例

```

apiVersion: machine.openshift.io/v1beta1
kind: MachineSet
metadata:
  labels:
    machine.openshift.io/cluster-api-cluster: <infrastructure_id> ❶
    name: <infrastructure_id>-<role> ❷
    namespace: openshift-machine-api
spec:
  replicas: 1
  selector:
    matchLabels:
      machine.openshift.io/cluster-api-cluster: <infrastructure_id>
      machine.openshift.io/cluster-api-machineset: <infrastructure_id>-<role>
  template:
    metadata:
      labels:
        machine.openshift.io/cluster-api-cluster: <infrastructure_id>
        machine.openshift.io/cluster-api-machine-role: <role>
        machine.openshift.io/cluster-api-machine-type: <role>
        machine.openshift.io/cluster-api-machineset: <infrastructure_id>-<role>
    spec:
      providerSpec: ❸
      ...

```

❶ クラスタインフラストラクチャー ID。

❷ デフォルトのノードラベル。



注記

ユーザーによってプロビジョニングされるインフラストラクチャーを持つクラスタの場合、コンピュータマシンセットは **ワーカー** および **インフラ** タイプのマシンのみを作成できます。

❸ コンピュータマシンセット CR の **<providerSpec>** セクションの値はプラットフォーム固有です。CR の **<providerSpec>** パラメーターの詳細は、プロバイダーのコンピュータマシンセット CR の設定例を参照してください。

3. 以下のコマンドを実行して **MachineSet** CR を作成します。

```
$ oc create -f <file_name>.yaml
```

検証

- 次のコマンドを実行して、コンピュータマシンセットのリストを表示します。

```
$ oc get machineset -n openshift-machine-api
```

出力例

NAME	DESIRED	CURRENT	READY	AVAILABLE	AGE
agl030519-vplxk-windows-worker-us-east-1a	1	1	1	1	11m
agl030519-vplxk-worker-us-east-1a	1	1	1	1	55m
agl030519-vplxk-worker-us-east-1b	1	1	1	1	55m
agl030519-vplxk-worker-us-east-1c	1	1	1	1	55m
agl030519-vplxk-worker-us-east-1d	0	0		55m	
agl030519-vplxk-worker-us-east-1e	0	0		55m	
agl030519-vplxk-worker-us-east-1f	0	0		55m	

新規のマシンセットが利用可能な場合、**DESIRED** および **CURRENT** の値は一致します。マシンセットが利用可能でない場合、数分待機してからコマンドを再度実行します。

5.3.5. 関連情報

- マシンセットの管理に関する詳細は、[マシン管理セクション](#)を参照してください。

第6章 WINDOWS コンテナワークロードのスケジューリング

Windows ワークロードを Windows コンピュートノードにスケジューリングすることができます。



注記

WMCO はワークロードのプロキシ接続を介してトラフィックをルーティングできないため、[クラスター全体のプロキシ](#)を使用するクラスターではサポートされません。

前提条件

- Operator Lifecycle Manager (OLM) を使用して Windows Machine Config Operator (WMCO) をインストールしている。
- Docker 形式のコンテナランタイムが有効な状態で Windows コンテナを OS イメージとして使用している。
- Windows マシンセットを作成している。



重要

現時点で、Docker 形式のコンテナランタイムは Windows ノードで使用されます。Kubernetes では、コンテナランタイムとしての Docker を非推奨としています。詳細は、Kubernetes ドキュメントの [Docker の非推奨](#) について参照してください。Containerd は、今後の Kubernetes リリースで Windows ノードについてサポートされる新しいコンテナランタイムになります。

6.1. WINDOWS POD の配置

Windows ワークロードをクラスターにデプロイする前に、Pod が適切に割り当てられるように Windows ノードのスケジューリングを設定する必要があります。Windows ノードをホストするマシンがあるので、これは Linux ベースのノードと同じように管理できます。同様に、テイント、容認およびノードセクターなどのメカニズムを使用して、Windows Pod の適切な Windows ノードへのスケジューリングも同様に実行されます。

複数のオペレーティングシステム、および同じクラスターで複数の Windows OS バリエーションを実行する機能で、**RuntimeClass** オブジェクトを使用して Windows Pod をベース Windows OS バリエーションにマップする必要があります。たとえば、複数の Windows ノードが複数の Windows Server コンテナのバージョンで実行されている場合、クラスターは Windows Pod を互換性のない Windows OS バリエーションにスケジューリングする可能性があります。クラスター上の Windows OS バリエーションごとに **RuntimeClass** オブジェクトを設定する必要があります。クラスターで1つの Windows OS バリエーションのみが利用可能である場合、**RuntimeClass** オブジェクトを使用することも推奨されます。

詳細は、[ホストとコンテナのバージョンの互換性](#) を参照してください。



重要

コンテナの基本イメージは、コンテナがスケジューリングされるノードで実行されているものと同じ Windows OS バージョンおよびビルド番号である必要があります。

また、Windows ノードをあるバージョンから別のバージョンにアップグレードする場合 (たとえば、20H2 から 2022 に移行する場合)、新しいバージョンに一致するようにコンテナの基本イメージをアップグレードする必要があります。詳細については、[Windows コンテナのバージョンの互換性](#) を参照してください。

関連情報

- [スケジューラーによる Pod 配置の制御](#)
- [ノードテイントを使用した Pod 配置の制御](#)
- [ノードセレクターの使用による特定ノードへの Pod の配置](#)

6.2. スケジューリングメカニズムをカプセル化するための RUNTIMECLASS オブジェクトの作成

RuntimeClass オブジェクトを使用することにより、テイントおよび容認などのスケジューリングの仕組みの使用を単純化できます。テイントおよび容認をカプセル化するランタイムクラスをデプロイしてから、これを Pod に適用して Pod を適切なノードにスケジューリングできるようにします。ランタイムクラスの作成は、複数のオペレーティングシステムのバリエーションをサポートするクラスターでも必要になります。

手順

1. **RuntimeClass** オブジェクト YAML ファイルを作成します。例: **runtime-class.yaml**

```
apiVersion: node.k8s.io/v1beta1
kind: RuntimeClass
metadata:
  name: <runtime_class_name> ❶
handler: 'docker'
scheduling:
  nodeSelector: ❷
    kubernetes.io/os: 'windows'
    kubernetes.io/arch: 'amd64'
    node.kubernetes.io/windows-build: '10.0.17763'
  tolerations: ❸
  - effect: NoSchedule
    key: os
    operator: Equal
    value: "Windows"
```

- ❶ このランタイムクラスで管理する必要のある Pod で定義される **RuntimeClass** オブジェクト名を指定します。
- ❷ このランタイムクラスをサポートするノードに存在する必要があるラベルを指定します。このランタイムクラスを使用する Pod は、このセレクターに一致するノードにのみスケジューリングできます。ランタイムクラスのノードセレクターは Pod の既存のノードセレクターとマージされます。競合が発生した場合は、Pod をノードにスケジューリングできなくなります。
- ❸ Pod に追加する容認を指定します。ただし、受付時にこのランタイムクラスで実行される重複を除きます。これによって、Pod によって許容されるノードのセットとランタイムクラスが組み合わされます。

2. **RuntimeClass** オブジェクトを作成します。

```
$ oc create -f <file-name>.yaml
```

以下に例を示します。

```
$ oc create -f runtime-class.yaml
```

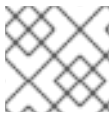
3. **RuntimeClass** オブジェクトを Pod に適用し、これが適切なオペレーティングシステムバリエーションにスケジュールされていることを確認します。

```
apiVersion: v1
kind: Pod
metadata:
  name: my-windows-pod
spec:
  runtimeClassName: <runtime_class_name> ❶
  ...
```

- ❶ Pod のスケジュールを管理するためにランタイムクラスを指定します。

6.3. WINDOWS コンテナワークロードのデプロイメント例

Windows コンピュートノードが利用可能になる時点で、Windows コンテナワークロードをクラスターにデプロイできます。



注記

このサンプルデプロイメントは参照用にのみ提供されます。

Service オブジェクトの例

```
apiVersion: v1
kind: Service
metadata:
  name: win-webserver
labels:
  app: win-webserver
spec:
  ports:
    # the port that this service should serve on
    - port: 80
      targetPort: 80
  selector:
    app: win-webserver
  type: LoadBalancer
```

Deployment オブジェクトの例

```
apiVersion: apps/v1
kind: Deployment
metadata:
  labels:
    app: win-webserver
  name: win-webserver
spec:
```

```

selector:
  matchLabels:
    app: win-webserver
replicas: 1
template:
  metadata:
    labels:
      app: win-webserver
      name: win-webserver
  spec:
    tolerations:
      - key: "os"
        value: "Windows"
        Effect: "NoSchedule"
    containers:
      - name: windowswebserver
        image: mcr.microsoft.com/windows/servercore:ltsc2019
        imagePullPolicy: IfNotPresent
        command:
          - powershell.exe
          - -command
            - $listener = New-Object System.Net.HttpListener; $listener.Prefixes.Add("http://*:80/");
              $listener.Start();Write-Host('Listening at http://*:80/'); while ($listener.IsListening) { $context =
                $listener.GetContext(); $response = $context.Response; $content='<html><body><H1>Red Hat
                OpenShift + Windows Container Workloads</H1></body></html>'; $buffer =
                [System.Text.Encoding]::UTF8.GetBytes($content); $response.ContentLength64 = $buffer.Length;
                $response.OutputStream.Write($buffer, 0, $buffer.Length); $response.Close(); };
        securityContext:
          runAsNonRoot: false
        windowsOptions:
          runAsUserName: "ContainerAdministrator"
  nodeSelector:
    kubernetes.io/os: windows

```



注記

mcr.microsoft.com/powershell: コンテナイメージを使用する場合、コマンドを **pwsh.exe** として定義する必要があります。**mcr.microsoft.com/windows/servercore:** **<tag>** コンテナイメージを使用している場合、コマンドを **powershell.exe** として定義する必要があります。詳細は、Microsoft のドキュメントを参照してください。

6.4. マシンセットの手動によるスケーリング

マシンセットのマシンのインスタンスを追加したり、削除したりする必要がある場合、マシンセットを手動でスケーリングできます。

本書のガイダンスは、完全に自動化されたインストーラーでプロビジョニングされるインフラストラクチャーのインストールに関連します。ユーザーによってプロビジョニングされるインフラストラクチャーのカスタマイズされたインストールにはマシンセットがありません。

前提条件

- OpenShift Container Platform クラスターおよび **oc** コマンドラインをインストールすること。
- **cluster-admin** パーミッションを持つユーザーとして、**oc** にログインする。

手順

1. クラスタにあるマシンセットを表示します。

```
$ oc get machinesets -n openshift-machine-api
```

マシンセットは **<clusterid>-worker-<aws-region-az>** の形式で一覧表示されます。

2. クラスタ内にあるマシンを表示します。

```
$ oc get machine -n openshift-machine-api
```

3. 削除するマシンに注釈を設定します。

```
$ oc annotate machine/<machine_name> -n openshift-machine-api  
machine.openshift.io/cluster-api-delete-machine="true"
```

4. 削除するノードを分離して解放します。

```
$ oc adm cordon <node_name>  
$ oc adm drain <node_name>
```

5. マシンセットをスケーリングします。

```
$ oc scale --replicas=2 machineset <machineset> -n openshift-machine-api
```

または、以下を実行します。

```
$ oc edit machineset <machineset> -n openshift-machine-api
```

ヒント

または、以下の YAML を適用してマシンセットをスケーリングすることもできます。

```
apiVersion: machine.openshift.io/v1beta1  
kind: MachineSet  
metadata:  
  name: <machineset>  
  namespace: openshift-machine-api  
spec:  
  replicas: 2
```

マシンセットをスケールアップまたはスケールダウンできます。新規マシンが利用可能になるまで数分の時間がかかります。

検証

- 目的のマシンの削除を確認します。

```
$ oc get machines
```

第7章 WINDOWS ノードのアップグレード

Windows Machine Config Operator (WMCO) をアップグレードすることで、Windows ノードに最新の更新が含まれることを確認できます。

7.1. WINDOWS MACHINE CONFIG OPERATOR のアップグレード

現在のクラスターバージョンと互換性のある Windows Machine Config Operator (WMCO) の新規バージョンがリリースされると、Operator はアップグレードチャンネル、および Operator Lifecycle Manager (OLM) を使用する際にインストールに使用されたサブスクリプションの承認ストラテジーに基づいてアップグレードされます。WMCO のアップグレードにより、Windows マシンの Kubernetes コンポーネントがアップグレードされます。



注記

WMCO の新規バージョンにアップグレードする場合でクラスターモニターリングを使用する必要がある場合は、WMCO namespace に `openshift.io/cluster-monitoring=true` ラベルが必要です。ラベルを既存の WMCO namespace に追加し、すでに Windows ノードが設定されている場合は、WMCO Pod を再起動してモニターリンググラフを表示できるようにします。

中断なしのアップグレードの場合、WMCO は以前のバージョンの WMCO で設定された Windows マシンを中止し、現行バージョンを使用してそれらを再作成します。これは、**Machine** オブジェクトを削除して実行されます。これにより、Windows ノードのドレイン (解放) および削除が実行されます。アップグレードを容易にするために、WMCO は設定されたすべてのノードにバージョンのアノテーションを追加します。アップグレード時に、バージョンのアノテーションで不一致があると、Windows マシンが削除され、再作成されます。アップグレード時のサービスの中断を最小限にするために、WMCO は一度に1つの Windows マシンのみを更新します。



重要

WMCO は Kubernetes コンポーネントの更新のみを行い、Windows オペレーティングシステムの更新は行いません。仮想マシンの作成時に Windows イメージを指定できるため、更新されたイメージを指定できます。**MachineSet** 仕様でイメージ設定を変更して、更新された Windows イメージを指定できます。

Operator Lifecycle Manager (OLM) を使用した Operator のアップグレードの詳細は、[インストールされた Operator のアップグレード](#) を参照してください。

第8章 BYOH (BRING-YOUR-OWN-HOST) WINDOWS インスタンスをノードとして使用

BYOH (Bring-Your-Own-Host) を使用すると、ユーザーは Windows Server 仮想マシンを再利用して、OpenShift Container Platform に移動できます。BYOH Windows インスタンスは、Windows サーバーがオフラインになった場合に、主要な中断を軽減するのに役立ちます。

8.1. BYOH WINDOWS インスタンスの設定

BYOH Windows インスタンスを作成するには、Windows Machine Config Operator (WMCO) namespace に Config Map を作成する必要があります。

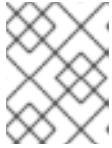
前提条件

ノードとしてクラスターに割り当てられる Windows インスタンスはすべて、以下の要件を満たす必要があります。

- Docker コンテナランタイムがインスタンスにインストールされている必要があります。
- インスタンスは、クラスターの Linux ワーカーノードと同じネットワーク上にある必要があります。
- ポート 22 が開いていて、SSH サーバーを実行している必要があります。
- SSH サーバーのデフォルトシェルは、[Windows コマンドシェル](#) または **cmd.exe** である必要があります。
- ログコレクションに対してポート 10250 を開く必要があります。
- 管理者ユーザーは、認可された SSH キーとしてシークレットセットで使用される秘密鍵とともに存在します。
- インストーラーによってプロビジョニングされたインフラストラクチャー (IPI) AWS クラスター用に BYOH Windows インスタンスを作成する場合は、ワーカーノード用に設定されたマシンの **spec.template.spec.value.tag** 値と一致する AWS インスタンスにタグを追加する必要があります。たとえば、**kubernetes.io/cluster/<cluster_id>: owned** または **kubernetes.io/cluster/<cluster_id>: shared** です。
- vSphere で BYOH Windows インスタンスを作成する場合は、内部 API サーバーとの通信を有効にする必要があります。
- インスタンスのホスト名は、以下の標準を含む [RFC 1123](#) DNS ラベルの要件に従う必要があります。
 - 小文字の英数字またはハイフン (-) のみが含まれます。
 - 英数字から始まります。
 - 英数字の文字で終わります。

手順

1. 追加する Windows インスタンスを記述する WMCO namespace に **windows-instances** という名前の ConfigMap を作成します。



注記

値を **username=<username>** としてフォーマットし、アドレスをキーとして使用し、設定マップの data セクションの各エントリーをフォーマットします。

設定マップの例

```
kind: ConfigMap
apiVersion: v1
metadata:
  name: windows-instances
  namespace: openshift-windows-machine-config-operator
data:
  10.1.42.1: |- ①
    username=Administrator ②
  instance.example.com: |-
    username=core
```

- ① WMCO が SSH 経由でインスタンスに到達するために使用するアドレス (DNS 名または IPv4 アドレス)。このアドレスの DNS PTR レコードが存在する必要があります。組織が DHCP を使用して IP アドレスを割り当てる場合は、BYOH インスタンスで DNS 名を使用することをお勧めします。そうでない場合は、インスタンスに新しい IP アドレスが割り当てられるたびに、**windows-instances** ConfigMap を更新する必要があります。
- ② 前提条件で作成した管理者ユーザーの名前。

8.2. BYOH WINDOWS インスタンスの削除

設定マップでインスタンスのエントリーを削除して、クラスターに割り当てられた BYOH インスタンスを削除できます。インスタンスを削除すると、クラスターに追加する前にそのインスタンスがその状態に戻ります。ログおよびコンテナランタイムアーティファクトは、これらのインスタンスには追加されません。

インスタンスを正常に削除するには、WMCO に提供される現在のプライベートキーを使用してアクセスする必要があります。たとえば、直前の例から **10.1.42.1** インスタンスを削除するには、設定マップを以下に変更します。

```
kind: ConfigMap
apiVersion: v1
metadata:
  name: windows-instances
  namespace: openshift-windows-machine-config-operator
data:
  instance.example.com: |-
    username=core
```

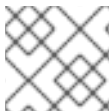
windows-instances を削除すると、ノードとして追加されるすべての Windows インスタンスを分解する要求として表示されます。

第9章 WINDOWS ノードの削除

ホスト Windows マシンを削除して、Windows ノードを削除できます。

9.1. 特定マシンの削除

特定のマシンを削除できます。



注記

コントロールプレーンマシンは削除できません。

前提条件

- OpenShift Container Platform クラスタをインストールします。
- OpenShift CLI (**oc**) をインストールしている。
- **cluster-admin** パーミッションを持つユーザーとして、**oc** にログインする。

手順

1. クラスタにあるマシンを表示し、削除するマシンを特定します。

```
$ oc get machine -n openshift-machine-api
```

コマンド出力には、**<clusterid>-worker-<cloud_region>** 形式のマシンの一覧が含まれます。

2. マシンを削除します。

```
$ oc delete machine <machine> -n openshift-machine-api
```



重要

デフォルトでは、マシンコントローラーは、成功するまでマシンによってサポートされるノードをドレイン (解放) しようとします。Pod の Disruption Budget (停止状態の予算) が正しく設定されていない場合などには、ドレイン (解放) の操作を実行してもマシンの削除を防ぐことができない場合があります。特定のマシンの "machine.openshift.io/exclude-node-draining" にアノテーションを付けると、ノードのドレイン (解放) を省略できます。削除中のマシンがマシンセットに属する場合、指定されたレプリカ数に対応するために新規マシンが即時に作成されます。

第10章 WINDOWS コンテナワークロードの無効化

Windows コンテナワークロードを実行する機能を無効にするには、Windows Machine Config Operator (WMCO) をアンインストールし、WMCO のインストール時にデフォルトで追加された namespace を削除します。

10.1. WINDOWS MACHINE CONFIG OPERATOR のアンインストール

クラスターから Windows Machine Config Operator (WMCO) をアンインストールできます。

前提条件

- Windows ワークロードをホストする Windows **Machine** オブジェクトを削除します。

手順

1. Operators → OperatorHub ページから、Filter by keyword ボックスを使用して、**Red Hat Windows Machine Config Operator** を検索します。
2. **Red Hat Windows Machine Config Operator** タイルをクリックします。Operator タイルはこれがインストールされていることを示します。
3. **Windows Machine Config Operator** 記述子ページで、**Uninstall** をクリックします。

10.2. WINDOWS MACHINE CONFIG OPERATOR NAMESPACE の削除

デフォルトで Windows Machine Config Operator (WMCO) 用に生成された namespace を削除できます。

前提条件

- WMCO がクラスターから削除される。

手順

1. **openshift-windows-machine-config-operator** namespace で作成されたすべての Windows ワークロードを削除します。

```
$ oc delete --all pods --namespace=openshift-windows-machine-config-operator
```

2. **openshift-windows-machine-config-operator** namespace のすべての Pod が削除されているか、または終了状態を報告していることを確認します。

```
$ oc get pods --namespace openshift-windows-machine-config-operator
```

3. **openshift-windows-machine-config-operator** namespace を削除します。

```
$ oc delete namespace openshift-windows-machine-config-operator
```

関連情報

- [クラスターからの Operator の削除](#)

- [Windows ノードの削除](#)