

Oracle Cloud InfrastructureのHyper-Vのデプロイ

ORACLE WHITE PAPER | 2018年11月



免責事項

下記事項は、弊社の一般的な製品の方向性に関する概要を説明するものです。また、情報提供を唯一の目的とするものであり、いかなる契約にも組み込むことはできません。マテリアルやコード、機能の提供をコミットメント(確約)するものではなく、購買を決定する際の判断材料になさらないで下さい。オラクルの製品に関して記載されている機能の開発、リリース、および時期については、弊社の裁量により決定されます。

改定履歴

このホワイト・ペーパーが初めて公開されて以降、次の改訂が加えられています。

日付	改訂内容
2018年11月9日	<ul style="list-style-type: none">• VNICを直接使用できるゲストの構成に関する情報を追加しました。• VNICを直接使用(直接アクセス)するゲストと、ヘルパー・ゲストを使用(間接アクセス)するゲストを区別しました。• Hyper-Vホストに2つ目の物理NICを構成するための要件を削除しました。• SRIOVブリッジを使用して、ゲストが直接アクセス方式で相互に通信できるようにする情報を追加しました。インストールされている場合、これにはhvnatとhvrouterゲストが含まれます。• VCNにhvnat/hvrouter接続するための2つ目のVCNサブネットの要件を削除しました。• hvnat/hvrouterゲスト用のBroadcomドライバの要件を削除しました。• 図を更新して新しい情報を反映しました。• このホワイト・ペーパーの名前を変更しました。
2018年8月3日	<ul style="list-style-type: none">• 概要を更新して、Hyper-Vに関する背景情報を含めました。• Oracle Cloud InfrastructureへのHyper-Vレプリカの実装を説明する付録を追加しました。
2018年4月20日	<ul style="list-style-type: none">• 図を更新してよりわかりやすくしました。• Microsoft Loopback Adapterをベースとする内部ネットワーク・アダプタを追加しました。• 2つ目のサブネットはVCNへのHyper-Vアクセスに使用する必要があることを示す説明を追加しました(SCVMM、Hyper-VレプリカおよびHyper-Vクラスタリングのデプロイメント・ガイドのサポート)。• Microsoft Loopback Adapterのインストール手順を追加しました。• ゲストOSのライセンスと手順に関する説明と情報を追加しました。

Oracle Cloud Infrastructureの最新版のホワイト・ペーパーは、
<https://cloud.oracle.com/iaas/technical-resources>にあります。

目次

概要	5
このホワイト・ペーパーの目的	6
ゲストのデプロイ方法	6
直接アクセス	6
間接アクセス	8
前提条件	12
Oracle Cloud Infrastructure VCNの設定およびHyper-V用 ベア・メタル・インスタンスのデプロイ	12
Windows Server、Hyper-Vおよびサポートするネットワーク・サービスの構成	15
Hyper-Vのインストール	15
Hyper-Vの構成	16
間接アクセスの構成	16
Windows DHCP、DNSおよびMicrosoft Loopback Adapterのインストールおよび構成	16
Hyper-Vゲスト用の内部ネットワークの作成	21
Hyper-Vゲスト用のDNSおよびDHCPの構成	22
ヘルパーHyper-Vゲストの作成	25
hvnatおよびhvrouter Hyper-Vゲスト用のWindowsのインストールおよび構成	29
hvnatゲストの構成	30
hvrouterゲストの構成	33
ゲストのインストール	33
Windows仮想マシンの自動ライセンス認証	33
直接アクセスのゲスト	34
間接アクセスのゲスト	36



異なるHyper-Vサーバー上のゲスト間における接続の有効化	37
結論	38
付録A: Hyper-Vレプリカのデプロイ	39
前提条件	39
Hyper-Vターゲット・インスタンスの構成	40
Hyper-Vゲストの構成	43
オンプレミスからOracle Cloud Infrastructureへの ゲスト・レプリケーションの制限事項	43
Hyper-Vゲストの構成	44
ソースとターゲットのHyper-Vインスタンス間でのフェイルオーバー	48

概要

Oracle Cloud Infrastructureを使用すると、柔軟性が高く、シェイプ構成が多様で、CPUとRAMの関係が明確に定義されている、ほとんどのお客様のニーズに対応するゲスト・インスタンスを、堅牢で高度に構成可能な方法で個別にデプロイできます。オペレーティング・システム・プラットフォームのデプロイを検討している場合、特定のアプリケーション・スタックでオペレーショナル・エクセレンスを実現する最善の方法は、Oracle Cloud Infrastructureでベア・メタル・インスタンスまたは仮想インスタンスを使用することです。

ただし、Oracle Cloud Infrastructureで様々なインスタンス・タイプの機能を使用できない、特定の状況があります。次に、そのような状況の一部を示します。

- インスタンスまたはアプリケーションが、CPUの数とRAMの容量の間に特定の関係を必要とし、それが標準の仮想インスタンスで指定されている割合と異なる場合
- Oracle Cloud Infrastructureで提供されていないレガシーまたはその他のオペレーティング・システムの要件があり、仮想インスタンスで実行できない場合
- オペレーティング・システムが、既存のハイパーバイザに含まれていない場合、またはOracle Cloud Infrastructureのイメージのインポート・プロセスと互換性がない形式で提供されている場合
- 運用上の要件で、既存の運用基準、ツール、実行基準を維持する場合

このような状況やその他の状況により、お客様がインストールしたハイパーバイザを使用して必要な環境を整え、クラウドでのアプリケーションの実行と、それに伴うメリットの実現が必要になる場合があります。そのような状況を支援するために、Oracle Cloud Infrastructureでは、次のハイパーバイザのインストールがサポートされています: Oracle VM、KVMおよびMicrosoft Hyper-V。

Microsoft Hyper-Vは、多くの環境で選択されているハイパーバイザです。多数の組織がWindows管理者の経験を活かせるだけでなく、異種のオペレーティング・システムを共通のハードウェア・プラットフォームで実行することも可能です。オンプレミス環境でHyper-Vを使用するためのツールセットや運用上の慣例が数多く開発されており、このホワイト・ペーパーで説明するプロセスも、そうした慣例をOracle Cloud Infrastructure環境に拡張したものです。

このホワイト・ペーパーの目的

このホワイト・ペーパーでは、Oracle Cloud InfrastructureにHyper-Vをデプロイする方法を説明します。デプロイ方法はオンプレミスで使用される方法とは異なりますが、Microsoft SCVMMなど、標準的なオンプレミスの管理ツールと互換性のある構成になります。

また、ゲストのデプロイでは、直接と間接の異なる2つの方法も説明します。ゲストの要件によって異なりますが、ゲストはどちらの方法でも、単一のHyper-Vホストにデプロイできます。方法の選び方は、それぞれの方法の説明に記載されています。Hyper-V自体をデプロイする前にゲストのデプロイ方法を選択する必要はありませんが、基本的なHyper-Vのデプロイが完了したら、ゲストごとにデプロイ方法を特定する必要があります。

最後に、このホワイト・ペーパーでは、制限付きの構成におけるHyper-Vレプリカ(異なるHyper-Vホスト間で実際のゲストをレプリケートする方法)の基本的なデプロイについても説明します。説明で詳しく述べるとおり、Hyper-Vレプリカのデプロイには特殊な制限のセットがあり、間接方式でデプロイされたゲストにのみ適用できます。

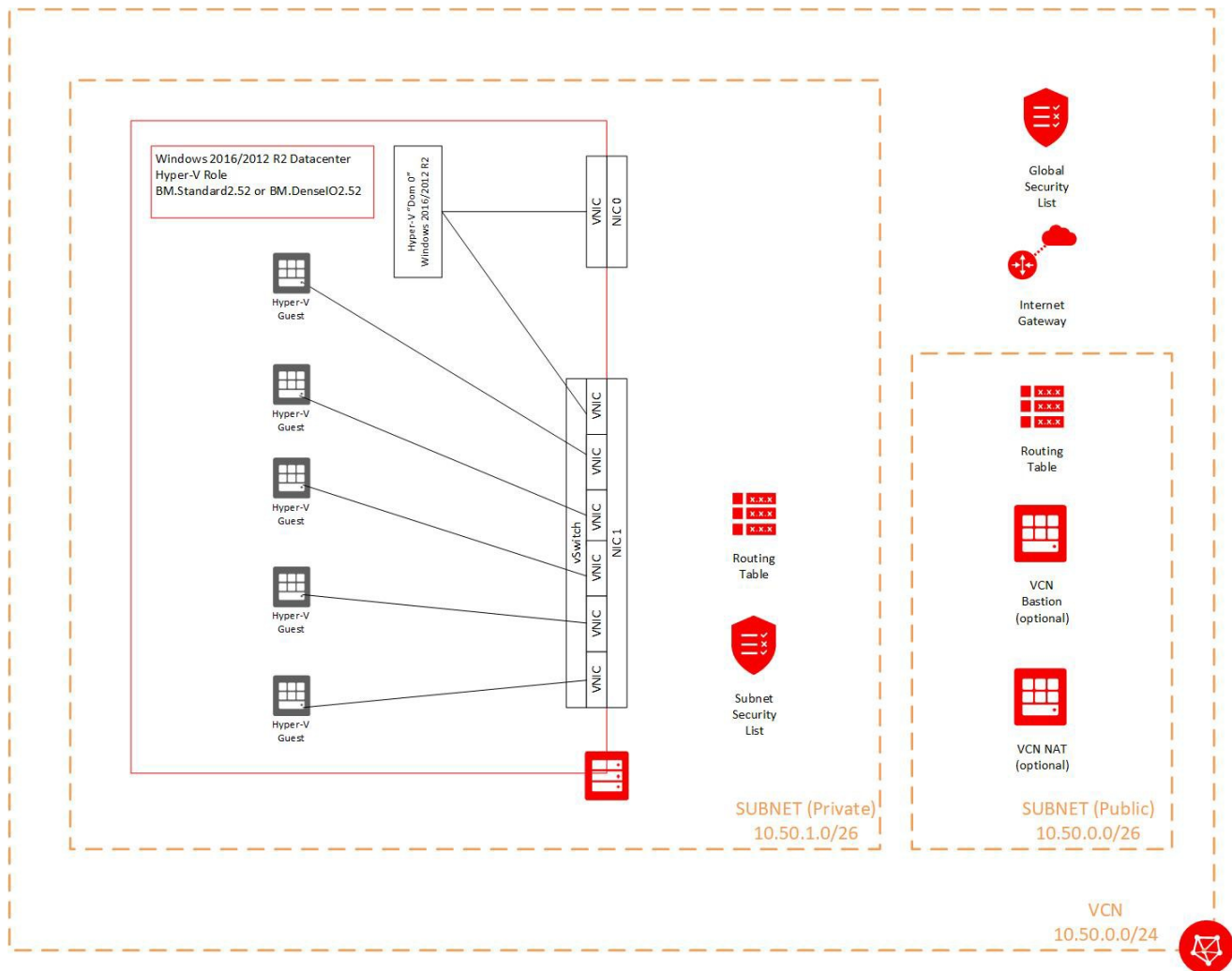
ゲストのデプロイ方法

Hyper-Vをデプロイする際、現在では、2つの方法でゲストをデプロイできます。どちらの方法を使用しても、Oracle Cloud Infrastructure、Windows ServerおよびHyper-Vのサービスが統合されており、Hyper-Vで実行しているゲストに、Oracle Cloud Infrastructureのインスタンスやサービスとやり取りする機能や、Oracle Cloud Infrastructureで実行しているゲストに、Hyper-Vのインスタンスやサービスとやり取りする機能をシームレスに提供する環境が作成されます。

直接アクセス

直接アクセス方式では、Hyper-Vのそれぞれのゲストに個別のVNICが割り当てられます。ゲストには、VNICがアタッチされているサブネット上のIPアドレスが付与されます。また、ゲストはVNICのMACアドレスをゲスト自身のものとして使用する必要があります。ゲストの構成は、デプロイメント・プロセスとは別に、IPアドレスの情報を使用して手動で行う必要があります。

次の図で、直接アクセス方式に関連付けたサンプル・アーキテクチャを示します。



アーキテクチャには次の要素があります。

- CIDRが10.50.0.0/24のVCN
- CIDRが10.50.1.0/26のプライベート・サブネット
- CIDRが10.50.0.0/26のパブリック・サブネット(オプション)
- Hyper-V役割がインストールされたWindows 2016 Datacenterを実行するベア・メタルのOracle Cloud Infrastructure Computeインスタンス
- インターネット・ゲートウェイ、ローカルとグローバルのセキュリティ・リスト、およびVCNをサポートするルート表

- パブリック・サブネットに配置されたプライベート・サブネット用のNATゲートウェイおよび要塞ホスト(オプション)

Hyper-Vを実行するベア・メタル・インスタンスには、次の要素があります。

- 2つ目の物理NIC (NIC1)へのプロビジョニングおよび割当てが行われたVNIC
- シングル・ルートI/O仮想化(SR-IOV)が有効化され、NIC1を使用する外部vSwitch

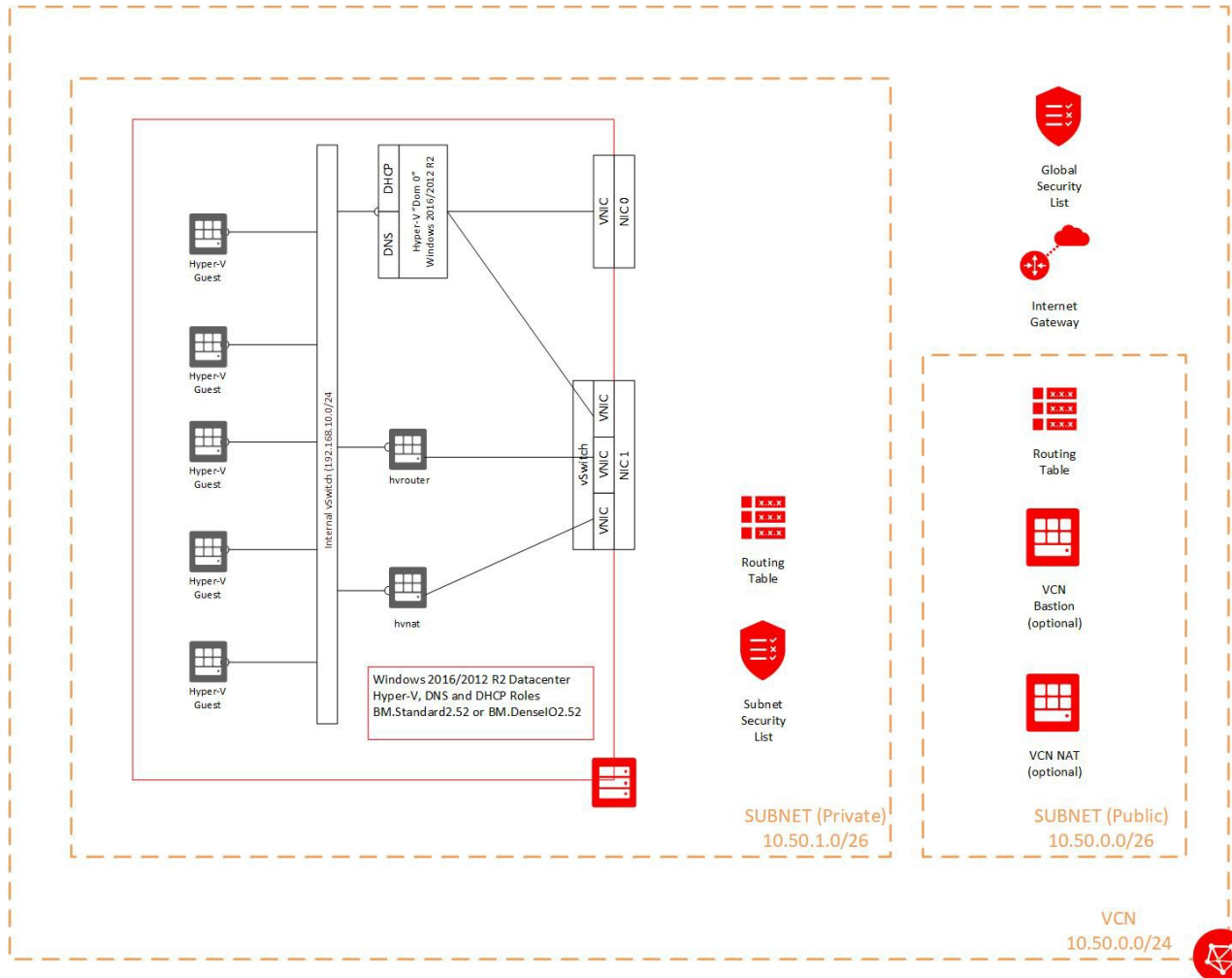
直接アクセスのメリットは、パフォーマンスが制限される可能性があるヘルパー・ゲストを介さずに、Oracle Cloud Infrastructureのリソースにゲストが直接アクセスできることです。SR-IOVを使用することで、各ゲストにVCNサブネットへの個別の接続が用意され、共有ハードウェア接続の利用により、最大限のパフォーマンスが実現されます。また、ゲストには、プライベート接続(VCNへのFastConnectおよびVPNアクセス)経由、またはパブリックIPアドレスを使用したインターネット経由で、オンプレミスから直接アクセスすることも可能です。

ただし、考慮が必要な制限がいくつかあります。単一のHyper-Vホストにデプロイできる直接アクセスのゲスト数は、現在のところ24に制限されています。24を超えるゲストのデプロイが必要な場合、この方法は使用できません。また、このホワイト・ペーパーで後から説明するHyper-Vレプリカ方式でゲストを移行することができません。現在実装されているVNICテクノロジーでは、VNICとそれに関連付けられているIPアドレスをHyper-Vホスト間で移植できないため、レプリカ・プロセスの一部としてターゲット・ゲストを作成する機能が制限されます。

間接アクセス

間接アクセス方式は、このホワイト・ペーパーの以前のバージョンで詳しく説明しました。この方式では、VCNルートからIPへの機能と2つのヘルパーHyper-Vゲストを組み合わせ使用し、Hyper-Vホスト自体に配置されているプライベート・サブネットと相互にトラフィックをルーティングできるようにしています。ゲストには、プライベートDHCPサーバー経由でIPアドレス(VCNアドレス空間に含まれないアドレス)が割り当てられ、ゲストの構成にはローカルで生成されたMACアドレスが使用されます。

次の図で、間接アクセス方式のサンプル・アーキテクチャを示します。



アーキテクチャには次の要素があります。

- CIDRが10.50.0.0/24のVCN
- CIDRが10.50.1.0/26のVCN内のプライベート・サブネット
- CIDRが10.50.0.0/26のVCN内のパブリック・サブネット(オプション)
- Hyper-V役割がインストールされたWindows 2016 Datacenterを実行するベア・メタルの Oracle Cloud Infrastructure Computeインスタンス
- インターネット・ゲートウェイ、ローカルとグローバルのセキュリティ・リスト、および VCNをサポートするルート表

- パブリック・サブネットに配置されたプライベート・サブネット用のNATゲートウェイおよび要塞ホスト(オプション)
- Hyper-V内のゲストがアクセス可能なサブネット上の代表的なリソース

Hyper-Vを実行するベア・メタル・インスタンスには、次の要素があります。

- シングル・ルートI/O仮想化(SR-IOV)が有効化されている外部タイプのvSwitch
- SR-IOVを有効化する必要がない、ゲスト用の外部タイプのvSwitch(内部とラベル付けされます)
- 内部ゲスト(hvnat/hvrouter)用のNATゲートウェイおよびルーターとして機能する、特別な目的の2つのHyper-Vヘルパー・ゲスト
- Windows 2016 Hyper-V “Dom0” で実行され、内部vSwitchにバインドされたDHCPサーバー(Hyper-Vゲストにアドレス/ネットワークの情報を提供します)
- Windows 2016 Hyper-V “Dom0” で実行され、内部vSwitchにバインドされたDNSサーバー(Hyper-Vゲストに名前の解決サービスを提供します)

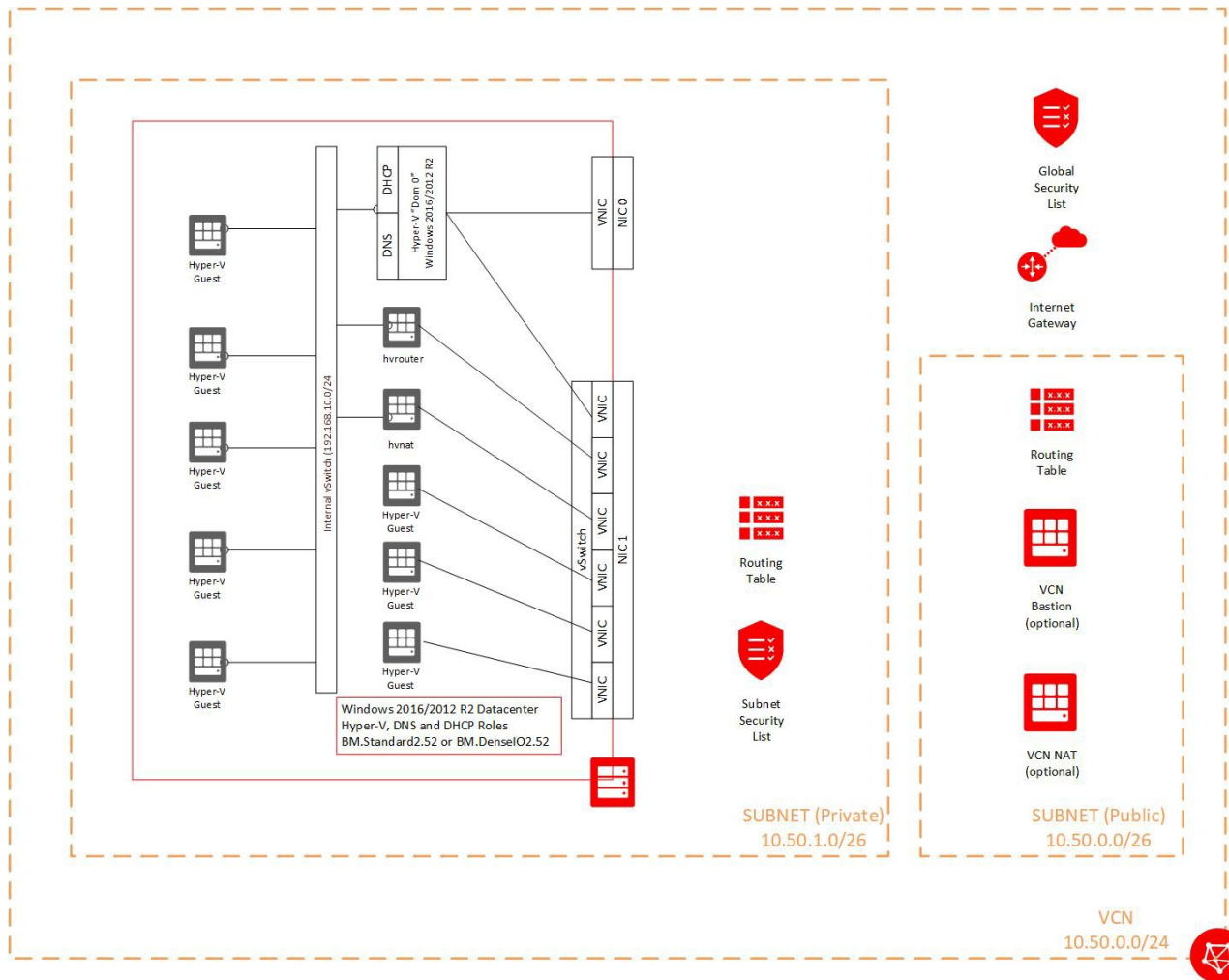
この方式には、いくつかのメリットがあります。

- この環境へのゲストのデプロイは比較的簡単です。この方式の一部として内部のDHCPおよびDNSサーバーが提供されるため、最小限のやり取りでゲストを環境にインストールできます。DHCP用に構成されているゲストには、ゲストのデプロイメント・プロセスの一部として、IPアドレス、ルートおよびDNSの情報が提供されます。
- 許可されるゲストの数が、直接アクセス方式よりはるかに多くなります。VNICの数に基づく制限がないため、ゲストの構成によっては、単一のHyper-Vホストに数百のゲストをデプロイできます。
- Hyper-Vレプリカ方式を使用して、Hyper-Vホスト間でゲストを移行できます。

ただし、直接アクセス方式のメリットが、間接アクセス方式のデメリットになります。

- 2つのヘルパー・ゲストには、プライベートのHyper-VサブネットとVCNサブネット間でトラフィックを効率よくルーティングする機能がありますが、それによって、ゲストのネットワーク・パフォーマンスが制限されます。
- この方式を使用するHyper-Vホスト内のゲストは外部のリソースやターゲットにアクセスできますが、現在のところ、ローカルVCNの外にあるソースからHyper-V内のゲストにアクセスする方法がありません。オンプレミス・ネットワークからアクセスする必要があるゲストのホスティングに間接方式を使用する場合は、VCN内にターミナル・サーバー、プロキシまたはその他のタイプのジャンプ・ホストをデプロイしてゲストにアクセスする必要があります。

方式は混在させることが可能です。たとえば、VCN以外をベースとする場所からのアクセスが必要な一連のインスタンスがある場合、それらのインスタンスを直接アクセスで作成できます。その後、同じHyper-Vホスト上に、アプリケーション用に必要なインスタンスをより高い密度で作成し、ヘルパー・ゲスト経由で相互にアクセスすることが可能です。次の図に、この設定を示します。



前提条件

デプロイを開始する前に、次のアイテムの準備をしてください。

- パブリック・サブネットを少なくとも1つ使用可能にするか、NATゲートウェイのあるプライベート・サブネットに接続します。ゲストがインターネットに接続する場合は、ルーティングに使用するセカンダリVNICもパブリック・サブネットに配置するか、NATゲートウェイのあるプライベート・サブネットに接続する必要があります。
 - Oracle Cloud InfrastructureにNATゲートウェイを構成する手順は、ドキュメントの[NATゲートウェイのトピック](#)に記載されています。
 - 将来、クラスタリングを使用する場合、セカンダリVNICに使用するサブネットは、プライマリ・インタフェースとは別のサブネットに配置する必要があります。インストールがスタンドアロン・インストールの場合は、プライマリとセカンダリのサブネットを同じサブネットにコロケートできます。
- (間接アクセスのみ)内部Hyper-Vネットワークに使用するIP範囲を、VCN IPの範囲以外で選択します。Hyper-Vが使用するIP範囲の最初の3つのアドレスを特定します。
 - デフォルト・ゲートウェイ(hvnat)
 - VCNゲートウェイ(hvrouter)
 - DNS/DHCP

Oracle Cloud Infrastructure VCNの設定およびHyper-V用ベア・メタル・インスタンスのデプロイ

最初の2つのステップは、直接アクセスと間接アクセスのどちらの方式にも当てはまります。

- V2 (BM 2.xタイプ)ベア・メタル・インスタンスを作成し、ブロック・ストレージ・ボリュームを少なくとも1つアタッチします。手順は、Oracle Cloud Infrastructure ドキュメントの次のトピックを参照してください。
 - [インスタンスの作成](#)
 - [ブロック・ボリュームの概要](#)
- インスタンスをプロビジョニングしたら、可能な場合は、ベア・メタル・インスタンスに使用しているものとは異なるサブネットに、ベア・メタル・インスタンスの2つ目のNIC (NIC 1)用のVNICをプロビジョニングします。セカンダリVNICのデプロイ方法の手順は、Oracle Cloud Infrastructure Networkingサービスのドキュメントの[仮想ネットワーク・インタフェース・カード\(VNIC\)のトピック](#)を参照してください。

PHYSICAL NIC

NIC 1 (3 VNICs allocated)

☐ Skip Source/Destination Check

The source/destination check causes this VNIC to drop any network traffic whose source or destination is not this VNIC. Only check the checkbox if you want this VNIC

「ソース/宛先チェックのスキップ」オプションは選択しないでください。このVNICは、パブリックとプライベートのどちらのサブネットに配置してもかまいません。プライベート・サブネットに配置する場合は、「前提条件」の項に記載されているように、NATゲートウェイの構成をお勧めします。また、一貫性を保つため、プライベートIPアドレスを手動で割り当てることをお勧めします。NICのプライベートIPアドレスをメモします。

間接アクセスを使用する場合は、次のステップを実行します。直接アクセス方式を使用する場合は、次の項にスキップしてください。

3. 2つ目のNIC (NIC 1)用に、2つのセカンダリVNICを作成します。

NAME (Optional)

hvnat

VIRTUAL CLOUD NETWORK

c4-vcn1

SUBNET

c4-vcn1-ad3-sn3

PHYSICAL NIC

NIC 1 (3 VNICs allocated)

☒ Skip Source/Destination Check

The source/destination check causes this VNIC to drop any network traffic whose

このステップで作成するどちらのVNICでも、「ソース/宛先チェックのスキップ」オプションを必ず選択してください。VNICはパブリックとプライベートのどちらのサブネットに配置してもかまいませんが、2つ目の物理NICに割り当てられているのと同じサブネット、またはプライマリの物理NICに使用しているものとは別のサブネットに配置してください。プライベート・サブネットに配置する場合は、「前提条件」の項に記載されているように、NATゲートウェイの構成をお勧めします。また、一貫性を保つために、プライベートIPアドレスを手動で割り当てることをお勧めしますが、必須ではありません。MACアドレスとプライベートIPアドレス、およびこれらのセカンダリVNICのVLAN IDをメモします。

4. ルート・ターゲット(hvrouter)としていずれかのセカンダリVNICを選択し、選択したターゲットのIPアドレスをメモします。
5. Hyper-Vサーバーを構成しているVCNのルート表を開き、ルート・ルールを追加します。Hyper-Vデプロイメント用に選択したIPアドレス範囲のルート・ターゲットとして選択したプライベートIPアドレスを入力します。

たとえば、Hyper-Vのアドレス空間として、192.168.11.0/24を選択したとします。そのHyper-VサーバーのセカンダリVNICは、IPアドレス10.50.0.69で選択されています。結果のルート表エントリは、次のようになります。

DESTINATION CIDR BLOCK	TARGET TYPE	TARGET SELECTION
192.168.11.0/24	Private IP	10.50.0.69
		OCID: ...2qgn4a

ルート表管理の詳細は、Networkingサービスのドキュメントの[ルート表のトピック](#)を参照してください。

6. サブネットのセキュリティ・リストを開きます。VCNにグローバル・セキュリティ・リストを構成してある場合は、かわりにそのセキュリティ・リストを使用してください。
7. エントリを追加して、Hyper-Vの内部ネットワークからのトラフィックが、VCN内のインスタンスに受け入れられるようにします。たとえば、VCNに、VCN全体を対象とするグローバル・セキュリティ・リストがある場合、そのグローバル・セキュリティ・リストに追加されるエントリは次のようになります。

	SOURCE CIDR	IP PROTOCOL
<input checked="" type="checkbox"/> STATELESS (more information) <i>Allows all traffic for all ports</i>	192.168.11.0/24	All Protocols (more information)

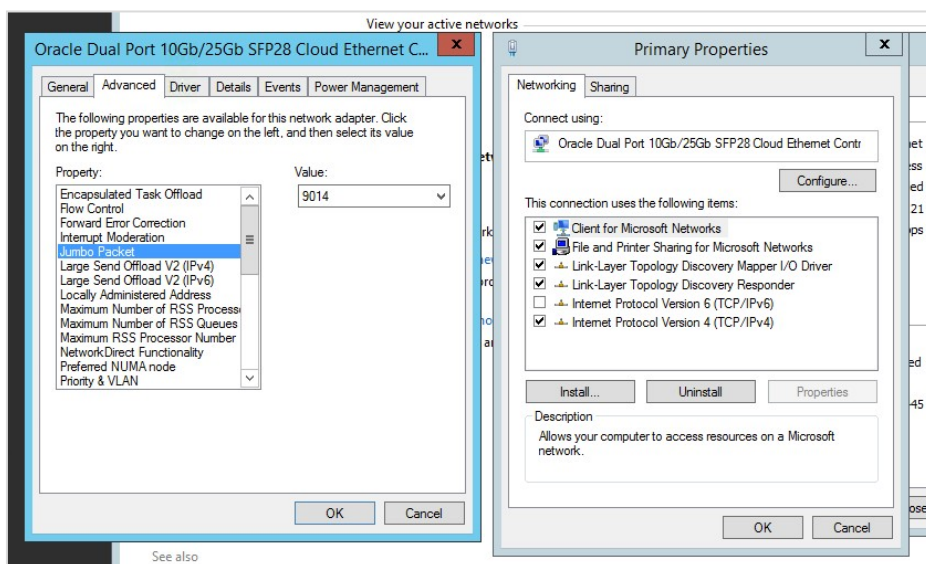
セキュリティ・リストの管理および更新方法の詳細は、Networkingサービスのドキュメントの[セキュリティ・リストのトピック](#)を参照してください。

Windows Server、Hyper-Vおよびサポートするネットワーク・サービスの構成

この項では、Hyper-Vのインストールと構成、Hyper-Vゲスト用のDNSとDHCPの構成、最初のHyper-Vゲストの作成、Hyper-Vゲスト用のWindowsの構成に関する手順を説明します。

Hyper-Vのインストール

1. プロビジョニングされたWindowsベア・メタル・インスタンスにログインします。
2. Windowsのファイアウォールで、ベア・メタル・インスタンスのICMPを有効化します。
ICMPのファイアウォール・ルールは、「ファイルとプリンターの共有 (エコー要求 - ICMPv4受信)」とラベル付けされています。
3. ベア・メタル・インスタンスのブロック・ボリュームにマウントしてフォーマットします。
4. 各NICのMTUが9014に設定されていることを確認します。
 - A. 各ネットワーク・アダプタのプロパティにアクセスします。
 - B. 「構成」をクリックします。
 - C. 「詳細設定」タブで、「ジャンボパケット」の値が9014であることを確認します。

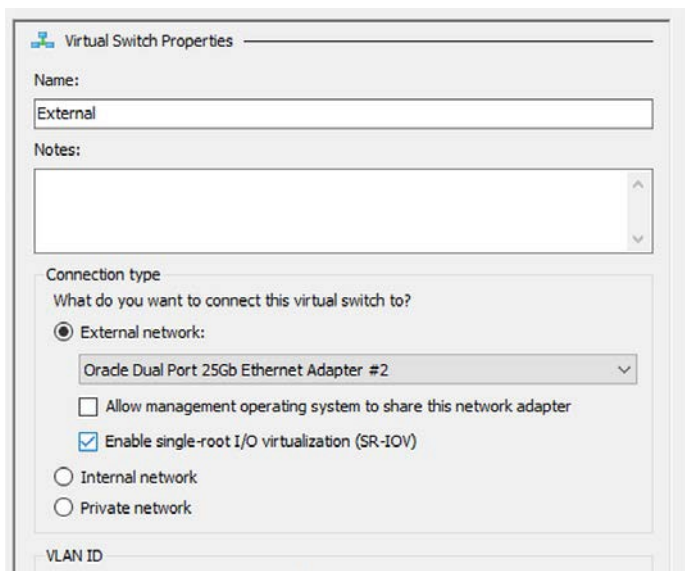


注意: まだシステムを再起動しないでください。

5. サーバーにHyper-V役割をインストールします。
6. (直接アクセスのみ)ベア・メタル・インスタンスを再起動します。

Hyper-Vの構成

1. Hyper-Vマネージャーを開きます。
2. 仮想スイッチ マネージャーを開いて、**External**という名前の新しい外部vSwitchを作成します。「シングルルートI/O仮想化(SR-IOV)を有効にする」オプションのみを選択します。



間接アクセスの構成

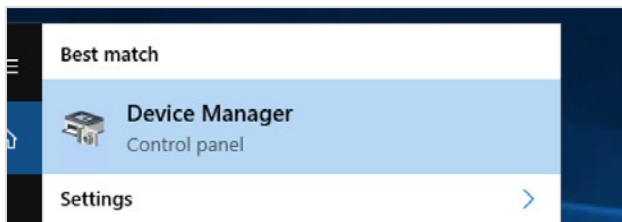
後続のステップは、間接アクセス方式を使用してHyper-Vにゲストをデプロイする場合にのみ必要です。この方式を使用しない場合は、次の項にスキップしてください。

Windows DHCP、DNSおよびMicrosoft Loopback Adapterのインストールおよび構成

1. 次のWindows機能をインストールします。
 - DHCP
 - DNS

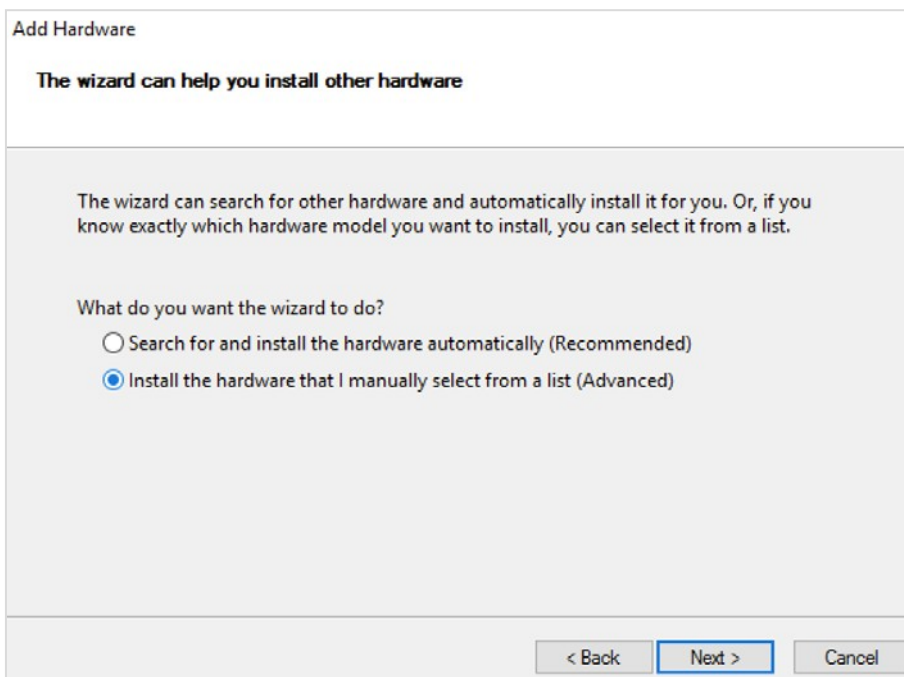
2. Microsoft KM-TEST Loopback Adapter (ローカライズされたループバック・ネットワーク・アダプタで、ゲストの接続に使用)をインストールします。

A. デバイス マネージャーを開きます。

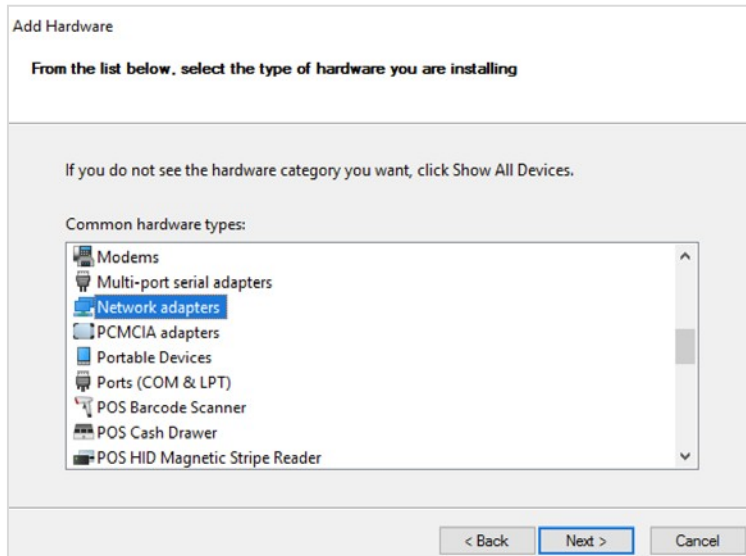


B. サーバー(デバイス・ツリーの最上位)を右クリックして、「レガシ ハードウェアの追加」を選択します。

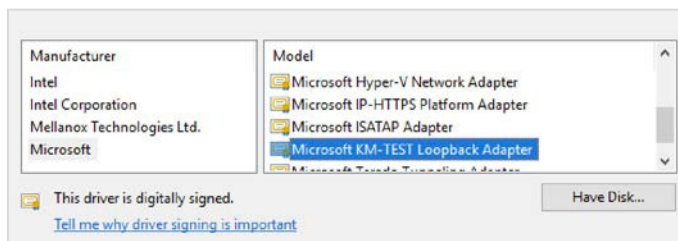
C. ウィザードで、「詳細」オプションを選択します。



- D. オプションのリストで、「ネットワーク アダプター」を選択します。



- E. 左側のボックスで「Microsoft」を選択し、右側のボックスで「Microsoft KM-TEST Loopback Adapter」を選択します。



- F. インストール・ウィザードを終了します。
3. Hyper-VのDNS/DHCPインタフェースに割り当てるIPアドレスでループバック・アダプタを構成します。ここでは、デフォルトのゲートウェイやDNSアドレスは割り当てないでください。

この構成を実行するプロセスで、次の警告が表示されます。無視して問題ありません。



このインストールは、PowerShellで実行できます。この操作を実行するスクリプトは、次のようになります。

```
$internalIpBase="<IP address range with CIDR>"
$hvIp="<IP Address of Internal Hyper-V adapter>"

$instance=$(ConvertFrom-Json $(Invoke-WebRequest
( "http://169.254.169.254/opc/v1/instance/" ) ).Content)
$vnics=$(ConvertFrom-Json $(Invoke-WebRequest
("http://169.254.169.254/opc/v1/vnics/" ) ).Content)

$secondVnic=""
$primaryVnic=""
$secondAdapter=""
$primaryAdapter=""
$loopAdapter=""

foreach ($vnic in $vnics) {
    $vnic.macAddr = $vnic.macAddr.replace(":", "-").toupper()
    if ($vnic.nicIndex -eq 1 -and $vnic.vlanTag -eq 0) {
        $secondVnic = $vnic
    } elseif ($vnic.nicIndex -eq 0 -and $vnic.vlanTag -eq 0) {
        $primaryVnic = $vnic
    }
}

foreach ($phys in Get-NetAdapter) {

    if ($secondVnic.macAddr -eq $phys.MacAddress) {
        $secondAdapter=$phys
        Rename-NetAdapter -Name $phys.Name -NewName "External-HV"
        continue
    }

    if ($primaryVnic.macAddr -eq $phys.MacAddress) {
        $primaryAdapter=$phys
        Rename-NetAdapter -Name $phys.Name -NewName "Primary"
```

```

        continue
    }

    $loopAdapter=$phys
    Rename-NetAdapter -Name $phys.Name -NewName "Internal-HV"
}

Update-Help -Force:$true
$intPrefix=$internalIpBase.split("/") [1]
$netPrefix=$secondVnic.subnetCidrBlock.split("/") [1]
New-NetIPAddress -InterfaceIndex $secondAdapter.ifIndex -IPAddress
$secondVnic.privateIp -PrefixLength $netPrefix -DefaultGateway
$secondVnic.virtualRouterIp
New-NetIPAddress -InterfaceIndex $loopAdapter.ifIndex -IPAddress $hvIp -
PrefixLength $intPrefix -Confirm:$false
Start-Sleep 10
Set-DnsClientServerAddress -InterfaceIndex $secondAdapter.ifIndex
- ServerAddresses "169.254.169.254"
Set-NetAdapterAdvancedProperty -Name * -RegistryKeyword "*JumboPacket" -
RegistryValue 9014 -NoRestart
Enable-NetFirewallRule -DisplayName "File and Printer Sharing (Echo
Request - ICMPv4-In)"

$nrTargetPortal=$(New-IsctsiTargetPortal -TargetPortalAddress 169.254.2.2)
Get-IsctsiTarget -IsctsiTargetPortal $nrTargetPortal | Connect-IsctsiTarget -
IsPersistent $true
$nrDisk=Get-Disk | Where-Object {$_.IsSystem -eq
$false} Initialize-Disk -Number $nrDisk.Number
New-Partition -DiskNumber $nrDisk.Number -UseMaximumSize
- AssignDriveLetter
$nrPart=$(Get-Partition -DiskNumber $nrDisk.Number | where-object {$_.Type
-match "Basic"})
Format-Volume -Partition $nrPart -NewFileSystemLabel "hvsystem"
- Confirm:$false

Install-WindowsFeature -Name "DHCP" -IncludeManagementTools
Install-WindowsFeature -Name "DNS" -IncludeManagementTools
Install-WindowsFeature -Name "Hyper-V" -IncludeManagementTools
- IncludeAllSubFeature -Restart

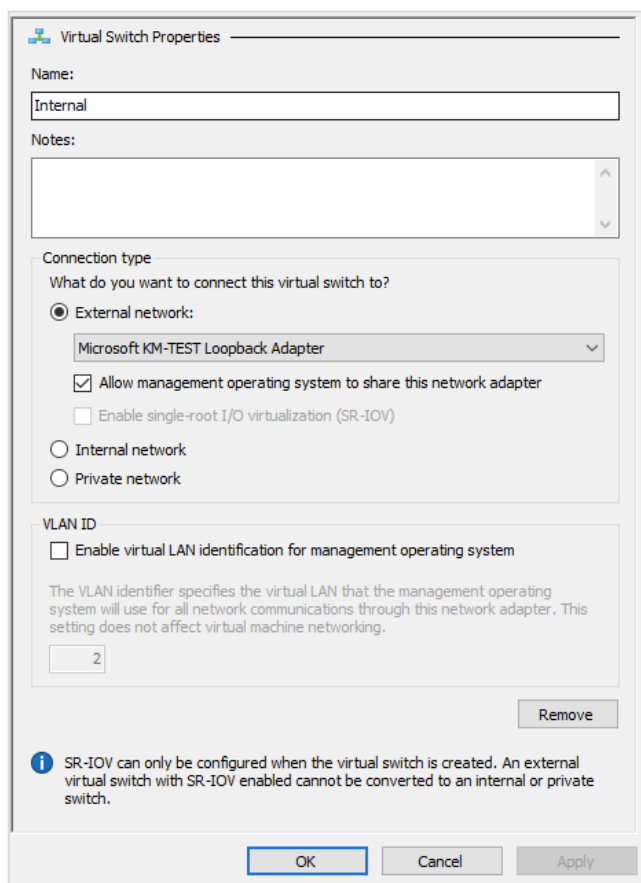
```

注意: このスクリプトでは、ループバック・アダプタはインストールされません。このスクリプトを実行する前に、通常のGUIを使用して、ループバック・アダプタを別途インストールする必要があります。ループバック・アダプタをインストールする前に、このようなスクリプトの実行を試行しないでください。

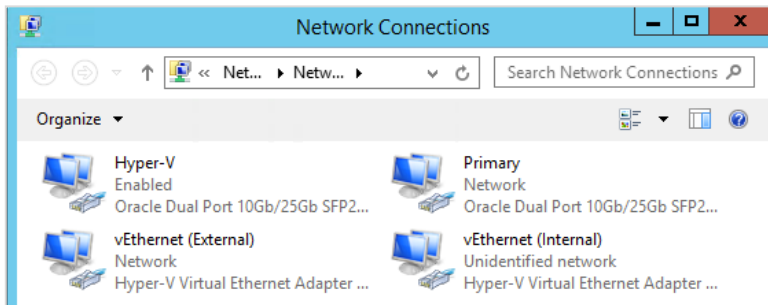
4. インスタンスを再起動して、再度ログインします。

Hyper-Vゲスト用の内部ネットワークの作成

1. Hyper-Vマネージャーを開きます。
2. 仮想スイッチ マネージャーを開いて、**Internal**という名前の新しい内部vSwitchを作成します。「**外部ネットワーク**」オプションを選択して、先ほどDNS/DHCPアダプタとして構成したMicrosoft Loopback Adapterを選択します。「**管理オペレーティング システムにこのネットワーク アダプターの共有を許可する**」オプションを選択します。



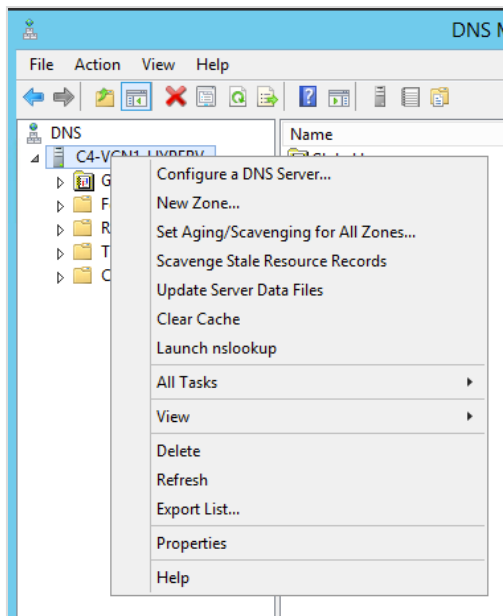
3. インスタンスのネットワーク構成を開きます。
- 3つのネットワーク・インタフェースがあり、そのうちの1つがvEthernetインタフェースです。「**内部**」というラベルが付いたvEthernetインタフェースの構成を開きます。



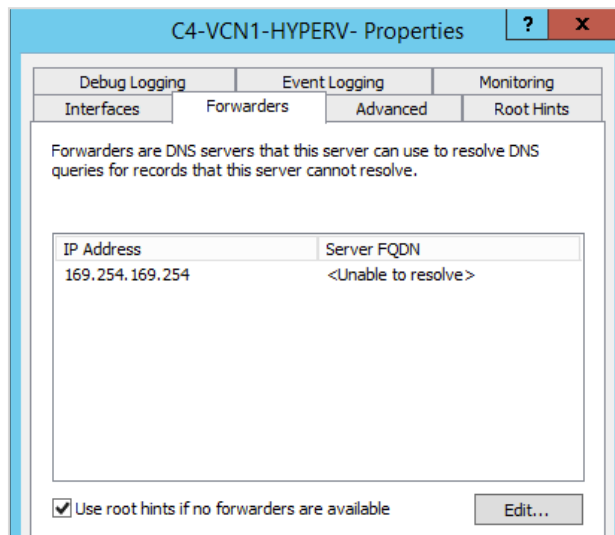
4. NICで実行したのと同じ手順で、両方のvEthernetアダプタのMTUを9014に変更します。
ここでは再起動しないでください。

Hyper-Vゲスト用のDNSおよびDHCPの構成

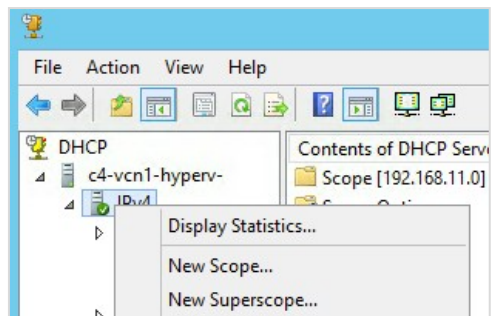
1. DNSの管理アプリケーションを開き、サーバーを右クリックして「プロパティ」を選択します。



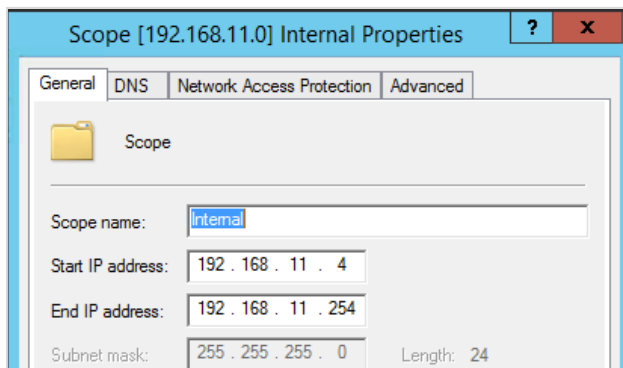
2. 「フォワーダー」タブで「編集」をクリックして、169.254.169.254のエントリを作成します。FQDNが解決されませんが、それが通常の状態です。



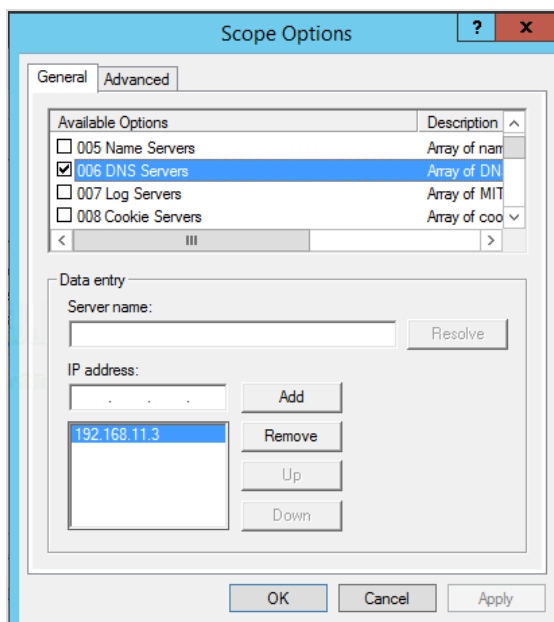
3. 構成を保存してDNSを再起動します。
4. DHCP管理アプリケーションを開きます。
5. サーバーを展開して「IPv4」を右クリックし、「新しいスコープ」を選択します。



6. Hyper-Vに選択したIPアドレスの範囲を使用してスコープを作成します。このプロセスに使用している3つの直後に続くアドレスで開始します。

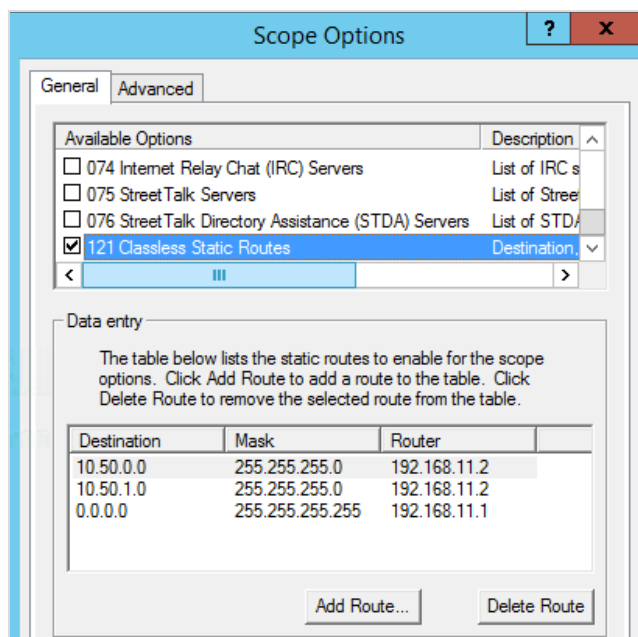


7. スコープを作成したら、左のナビゲーション・ペインでそのスコープを展開し、「スコープ オプション」フォルダを右クリックして「オプションの構成」を選択します。
8. 「スコープ オプション」ダイアログ・ボックスで、DNSオプションを選択し、DHCP/DNSに選択したIPアドレスを入力します。



9. 「利用可能なオプション」の下で、「121クラスレス静的ルート」を選択して、(最低限)次のルートを追加します。動的ルーティング・ゲートウェイ(DRG)を経由するその他のVCNやネットワークがある場合は、VCNゲートウェイやルーター・アドレスを使用して、それらもここで入力します。

宛先	マスク	ルーター
0.0.0.0	0.0.0.0	デフォルトのゲートウェイ/NATに先ほど選択したIPアドレス
VCNネットワーク領域	VCNのネットマスク	VCNゲートウェイ/ルーターに先ほど選択したIPアドレス

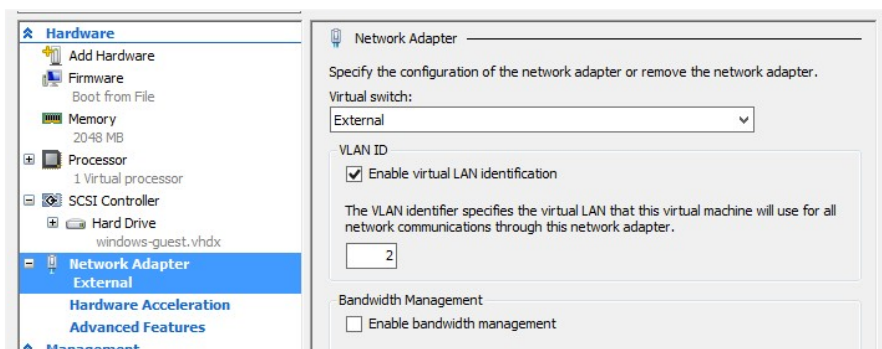


10. 構成を保存してDHCPを再起動します。

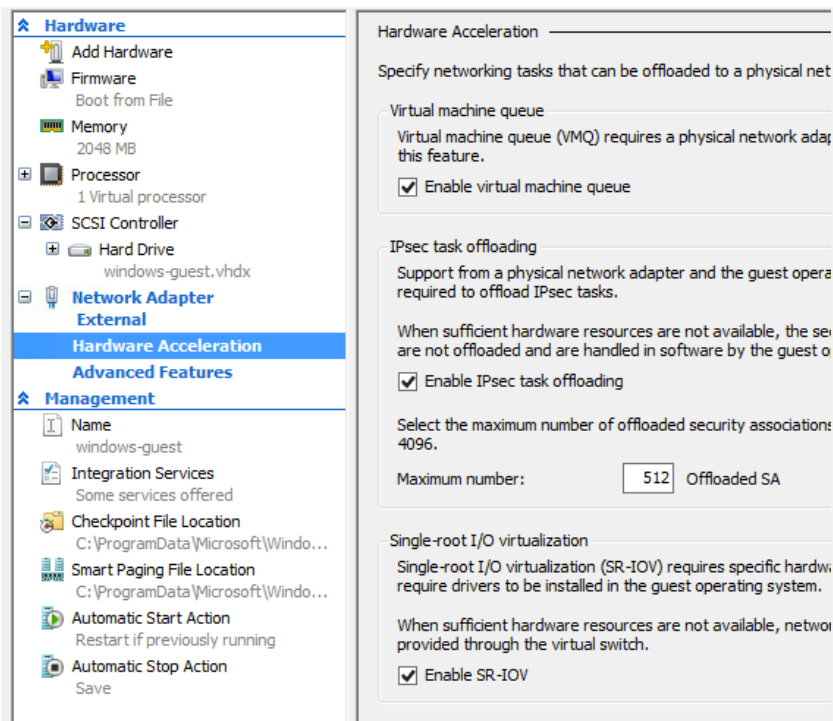
ヘルパーHyper-Vゲストの作成

- Hyper-Vマネージャーを開き、1つはhvnatという名前で、もう1つはhvrouterという名前で、新しいVMを2つ作成します。VMに次の特性を定義します。
 - 第2世代のVM
 - 最低限4196MBのメモリ(動的メモリ)
 - 外部vSwitchへのネットワーク接続
 - ブロック・ストレージ・デバイスにあるVHDX用に100Gの領域(通常はD:ドライブ)

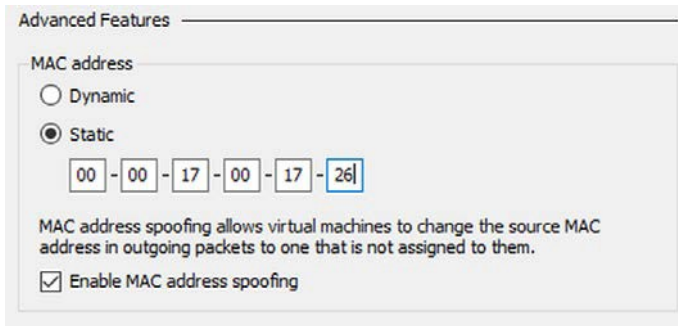
2. 作成したら、hvnat VMを選択して「設定」を選択します。
3. ルート・ターゲットとして選択されていないセカンダリVNICの情報を取得して、「設定」ダイアログ・ボックスで次のステップを実行します。
 - A. 左のナビゲーション・ペインで、「ネットワーク アダプター外部」を選択します。
 - B. 「仮想LAN IDを有効にする」チェック・ボックスを選択します。
 - C. セカンダリVNICのVLAN IDを入力します。



4. 左のナビゲーション・ペインで、「ハードウェア アクセラレータ」(「ネットワーク アダプター外部」の下)を選択して、「SR-IOVを有効にする」チェック・ボックスを選択します。



5. 左のナビゲーション・ペインで、「高度な機能」(「ネットワーク アダプター外部」の下)をクリックします。右側の「MACアドレス」セクションで、「静的」オプションを選択して、使用しているセカンダリVNICに関連付けられているMACアドレスを入力します。「MACアドレスのスプーフィングを有効にする」チェック・ボックスを選択します。



Advanced Features

MAC address

☐ Dynamic

☒ Static

00 - 00 - 17 - 00 - 17 - 26

MAC address spoofing allows virtual machines to change the source MAC address in outgoing packets to one that is not assigned to them.

☒ Enable MAC address spoofing

6. 左のナビゲーション・ペインで、「ハードウェアの追加」、「ネットワーク アダプター」の順に選択します。
7. 内部ネットワーク・アダプタを追加し、デフォルトの設定はすべてそのままにします。
8. 構成を保存します。
9. hvrouter VMに対して、ここまでのステップを繰り返します。

前の3つのセクションの構成アイテムは、PowerShellでも実行できます。次のサンプル・スクリプト(hvrouting.ps1)で、これらのステップを実行するテンプレートを示します。

```
Function ConvertTo-NetMask($cidr) {
    $mask=[Convert]::ToString(([Math]::Pow(2,$cidr) - 1) -shl (32 - $cidr), 2)
    $netmask = @()
    for($x = 0; $x -lt 4; $x++) {
        $netmask += [Convert]::ToUInt32($mask.Substring((8 *
$х),8),2).ToString()
    }
    return [String]::Join(".", $netmask)
}

$instance=$(ConvertFrom-Json $(Invoke-WebRequest
( "http://169.254.169.254/opc/v1/instance/" ) ).Content)
$vnics=$(ConvertFrom-Json $(Invoke-WebRequest
("http://169.254.169.254/opc/v1/vnics/" ) ).Content)
$secondVnic=""
$adapter=""
$хVnics=@()

$internalIpBase="192.168.11.0/24"
$хIp="192.168.11.3"
$хIpRange="192.168.11.4"
```

```

$endIpRange = "192.168.11.254"

foreach ($vnic in $vnics) {
    if ($vnic.nicIndex -eq 1 -and $vnic.vlanTag -eq 0) {
        $secondVnic = $vnic
        foreach ($phys in Get-NetAdapter) {
            $vnicMac = $secondVnic.macAddr.replace(":", "-")
            $.toupper() if ($vnicMac -eq $phys.MacAddress) {
                $adapter=$phys
                break
            }
        }
    } elseif ($vnic.nicIndex -eq 1 -and $vnic.vlanTag -gt 0) {
        $hvVnics+=$vnic
    }
}

New-VMSwitch -Name "External" -AllowManagementOS $true -NetAdapterName
$adapter.InterfaceAlias -EnableIov $true
New-VMSwitch -SwitchType Internal -Name "Internal"
$intAdapter=$(Get-NetAdapter | Where-Object {$_.Name -match "internal"})
$extAdapter=$(Get-NetAdapter | Where-Object {$_.Name -match "external"})

New-NetIPAddress -InterfaceIndex $intAdapter.ifIndex -IPAddress $hvIp -
PrefixLength $internalIpBase.split("/")[1]
Set-DnsServerForwarder -IPAddress 169.254.169.254
sleep 30
Add-DhcpServerv4Scope -Name "Internal" -EndRange $endIpRange -StartRange
$beginIpRange -SubnetMask $(ConvertTo-NetMask
([Convert]::ToInt16($internalIpBase.split("/")[1])))
Set-DhcpServerv4OptionValue -ScopeId $internalIpBase.split("/")[0] -DnsServer
$hvip
Set-DhcpServerv4Binding -InterfaceAlias $intAdapter.InterfaceAlias -BindingState
$true
Set-DhcpServerv4Binding -InterfaceAlias $extAdapter.InterfaceAlias -BindingState
$false

New-Item -ItemType Directory -Path "D:\Virtual Machines"
$hvnets=@("hvnat","hvrouter")
$count=0
foreach ($guest in $hvnets) {
    New-Item -ItemType Directory -Path ("D:\Virtual Machines\" + $guest)
    New-VM -Name $guest -MemoryStartupBytes (4* [Math]::Pow(1024,3)) -NewVHDPATH
("D:\Virtual Machines\" + $guest + "\" + $guest + ".vhd") -NewVHDSizeBytes (100
* [Math]::Pow(1024, 3)) -Generation 2 -SwitchName
"External" Add-VMdvdDrive -VMName $guest
Set-VMFirmware -VMName $guest -BootOrder @($(Get-VMdvdDrive -VMName $guest),
$(Get-VMHardDiskDrive -VMName $guest))
Set-VM -Name $guest -DynamicMemory -MemoryMinimumBytes (4*
[Math]::Pow(1024,3))

```

```
Set-VMNetworkAdapter -VMName $guest -StaticMacAddress  
$hvVnics[$count].macAddr -IovWeight 100  
Set-VMNetworkAdapterVlan -VMName $guest -Access -VlanId  
$hvVnics[$count].vlanTag  
Add-VMNetworkAdapter -VMName $guest -SwitchName "Internal"  
$count++  
}  
  
Set-NetAdapterAdvancedProperty -Name * -RegistryKeyword "*JumboPacket" -  
RegistryValue 9014
```

hvnatおよびhvrrouter Hyper-Vゲスト用のWindowsのインストールおよび構成

1. hvnat VMとhvrrouter VMの両方に、Windows 2012 R2をインストールします。
2. 各ゲストに対して、次のステップを実行します。
 - A. セカンダリVNICに関連付けられているインタフェースを特定します。これを実行するには、インスタンスの仮想NICのMACアドレスを参照します。
 - B. 特定のインスタンスについて識別された情報を使用して、セカンダリVNICのIPアドレス、サブネット・マスクおよびデフォルトのゲートウェイを構成します。
 - C. 機能に選択されたIPアドレスを使用して、2つ目のインタフェースを構成します。
 - hvnatゲストをVCNのルート・ターゲットにすることはできず、デフォルトのゲートウェイ/NATに関連付けられているHyper-Vのアドレスを取得する必要があります。
 - hvrrouterゲストでは、セカンダリVNICをルート・ターゲット・アドレスに関連付け、VCNゲートウェイ/ルーターに関連付けられているHyper-Vのアドレスを取得する必要があります。

Hyper-Vアドレスのインタフェースではデフォルトのゲートウェイを構成することはできませんが、DNSアドレスを割り当てる必要があります。DNSアドレスは、Hyper-VのDNS/DHCP機能に関連付けられた内部アドレスにする必要があります。

- D. 各インスタンスが、VCNのサブネットのデフォルト・ゲートウェイと内部DNS/DHCPのアドレスをpingできること、インターネットに接続できることを確認します。
- E. オペレーティング・システムに、現在のWindowsパッチをすべて適用します。

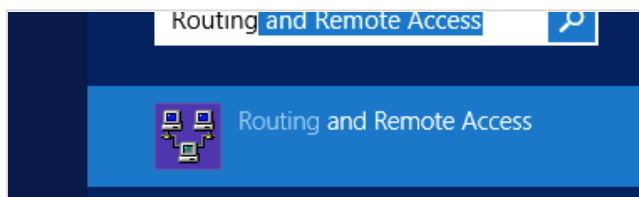
hvnatゲストの構成

次のステップを実行する前に、hvnatゲストのすべてのネットワークが構成済で機能していることを確認してください。ネットワークのテストには、hvnatゲストのVCN側のインスタンスと、内部Hyper-V側のネットワーク・ターゲットの両方と通信できることが含まれます。簡単なpingテストで十分です。

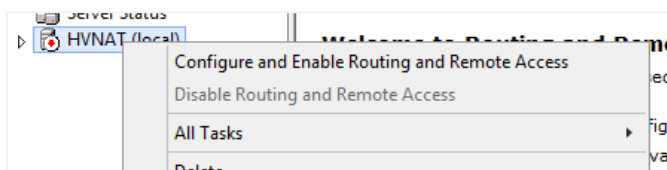
1. hvnatインスタンスに、Routing and Remote Accessサービス(RRAS)のルーティングのみをインストールします。このステップは、次のPowerShellコマンドを使用して、管理者として実行します。

```
Install-WindowsFeature -Name "Routing" -IncludeSubFeature  
- IncludeManagementTools -Confirm:$false
```

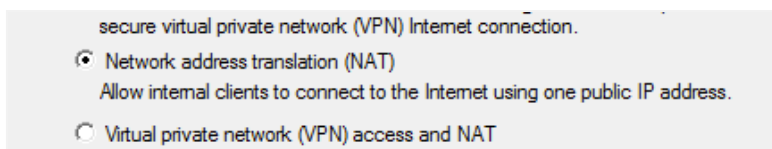
2. ルーティングとリモート アクセス・ ツールを開きます。



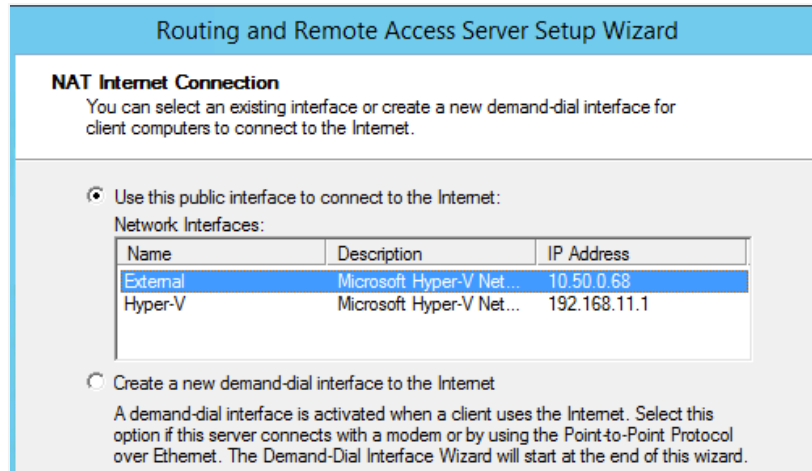
3. サーバーを右クリックして、「ルーティングとリモート アクセスの構成と有効化」を選択します。



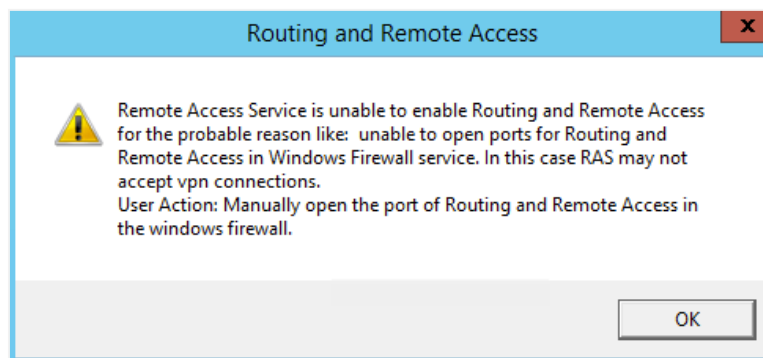
4. ウィザードの開始ページで、「次へ」をクリックします。
5. 「構成」 ページで、「ネットワーク アドレス変換(NAT)」を選択して、「次へ」をクリックします。



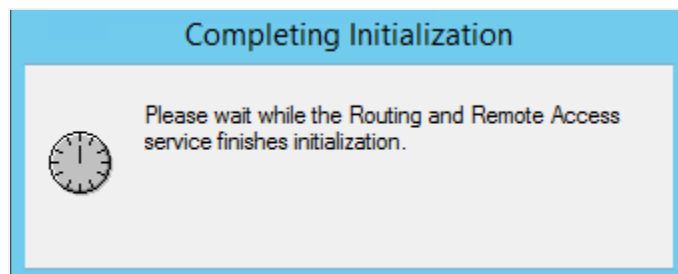
6. 「NATインターネット接続」ページで、インターネットに直接接続しているインターフェースのVCN IPアドレスがあるインターフェースを選択して、「次へ」をクリックします。



7. 「完了」をクリックします。
8. 次の警告が表示されたら、無視して「OK」をクリックします。



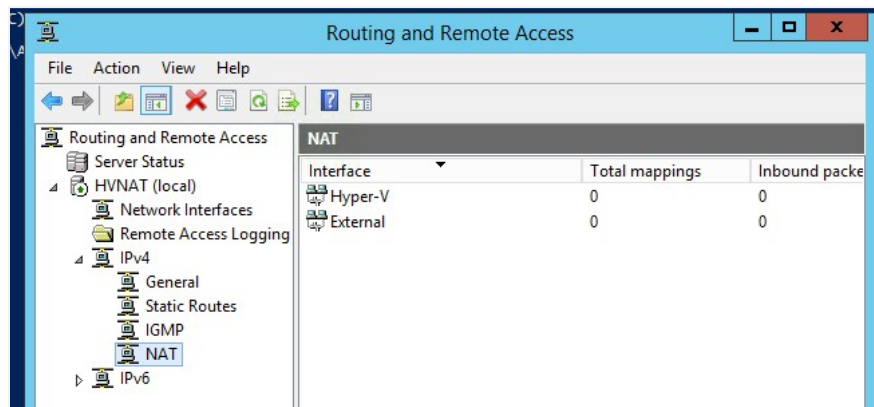
構成を実行中であることを示すダイアログ・ボックスが表示されます。



このプロセスは応答しなくなる場合があります。10分程度経過してもダイアログ・ボックスが消えない場合は、インスタンスを再起動します。

9. ルーティングとリモート アクセス・ツールで、サーバーを展開して「NAT」をクリックします。

ウィンドウの右側に、次のようなエントリが表示されます。



10. Hyper-Vアドレス経由で、VCNサブネットのデフォルト・ゲートウェイにpingできることを確認します。次の例では、VCNゲートウェイが10.50.0.65で、hvnatのHyper-Vアドレスは192.168.11.1です。PowerShellウィンドウを開いて、コマンドを発行します。

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> ping 10.50.0.65

Pinging 10.50.0.65 with 32 bytes of data:
Reply from 10.50.0.65: bytes=32 time<1ms TTL=128
Reply from 10.50.0.65: bytes=32 time<1ms TTL=128

Ping statistics for 10.50.0.65:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
PS C:\Users\Administrator> ping -S 192.168.11.1 10.50.0.65

Pinging 10.50.0.65 from 192.168.11.1 with 32 bytes of data:
Reply from 10.50.0.65: bytes=32 time<1ms TTL=125
Reply from 10.50.0.65: bytes=32 time<1ms TTL=125
Reply from 10.50.0.65: bytes=32 time<1ms TTL=125

Ping statistics for 10.50.0.65:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
PS C:\Users\Administrator>
```

ping -Sコマンドは、指定されたインターフェースからpingを送信します。

hvrouterゲストの構成

次のステップを実行する前に、hvrouterゲストのすべてのネットワークが構成済で機能していることを確認してください。ネットワークのテストには、hvrouterゲストのVCN側のインスタンスと、内部Hyper-V側のネットワーク・ターゲットの両方と通信できることが含まれます。簡単なpingテストで十分です。

1. hvrouterインスタンスにログインします。
2. PowerShellウィンドウを管理者として開きます。
3. 次のコマンドを実行して、インタフェース索引番号を特定します。

```
Get-NetAdapter
```

各Hyper-VインタフェースのifIndex番号をメモします。

4. 特定された各インタフェース番号について次のコマンドを実行して、それぞれのインタフェースに転送を構成します。

```
Set-NetIPInterface -InterfaceIndex <ifIndex_number> -Forwarding Enabled
```

5. VCNサブネット上のインスタンスからHyper-Vインタフェースをpingできることを確認するテストを行います。

これで構成は完了です。

ゲストのインストール

ゲスト・インスタンスは、Hyper-Vゲストの作成に関連する通常のプロセスでインストールできますが、次の変更点があります。

Windows仮想マシンの自動ライセンス認証

次の表にリストされているWindowsゲストは、仮想マシンの自動ライセンス認証(AVMA)プロセスの対象となるため、Windows 2016 Datacenter Hyper-V役割にゲストをインストールすることが可能で、ライセンスも継続されます。Linuxやその他のオペレーティング・システムの実行にWindowsのライセンスは必要ありません。Windowsデスクトップのライセンスはこの構成ではカバーされませんのでご注意ください。

オペレーティング・システムのバージョン	AVMAキー
Windows Server 2012 R2 Essentials	K2XGM-NMBT3-2R6Q8-WF2FK-P36R2
Windows Server 2012 R2 Standard	DBGBW-NPF86-BJVTX-K3WKJ-MTB6V
Windows Server 2012 R2 Datacenter	Y4TGP-NPTV9-HTC2H-7MGQ3-DV4TW

オペレーティング・システムのバージョン	AVMAキー
Windows Server 2016 Essentials	B4YNW-62DX9-W8V6M-82649-MHBKQ
Windows Server 2016 Standard	C3RCX-M6NRP-6CXC9-TW2F2-4RHYD

これらのキーは公表されているもので、Hyper-Vの管理下にあるこれらのオペレーティング・システムすべてのインストールに有効です。各ゲストで次の手順を実行すると、ゲストをアクティブ化できます。

1. コマンド・プロンプトを管理者として起動します。
2. 次のコマンドを入力します。

```
slmgr /ipk <AVMA_key>
```

3. コマンド・プロンプトを閉じます。

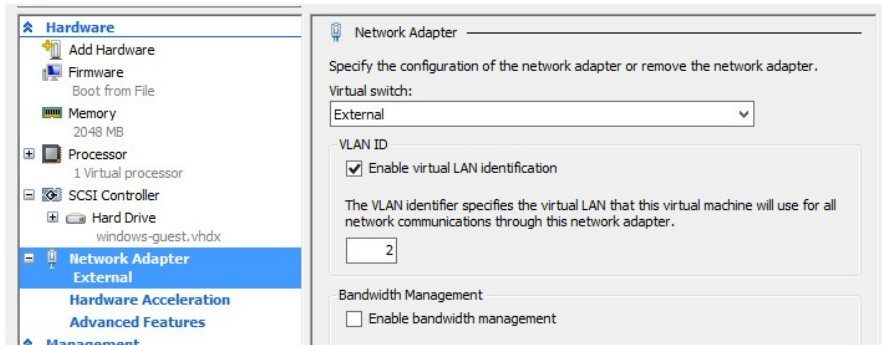
AVMAの詳細は、altaro.comのブログ投稿「[Hyper-V Automatic Virtual Machine Activation in Windows Server 2016](#)」を参照してください。

直接アクセスのゲスト

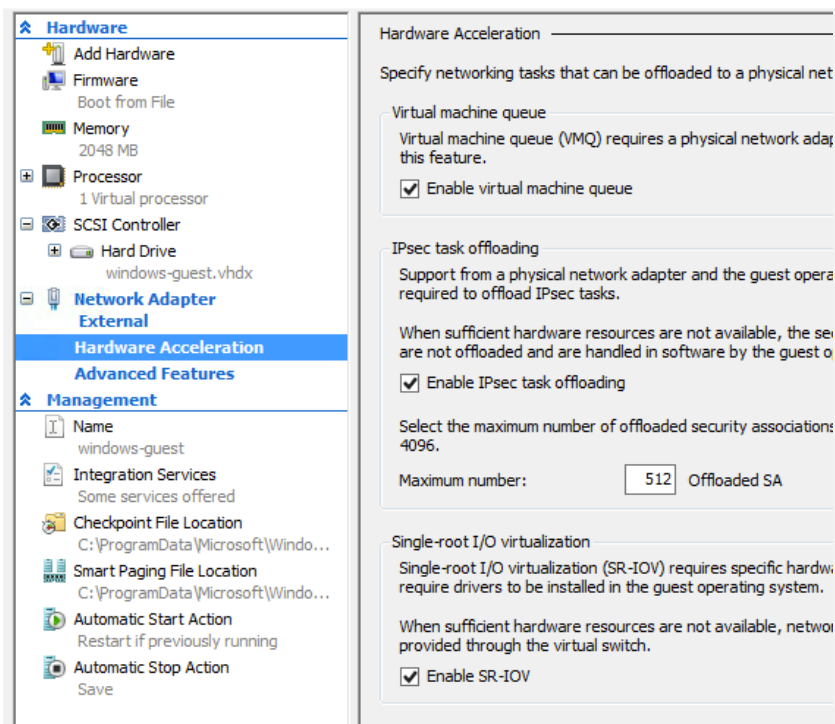
直接アクセスのゲストには、通常のHyper-Vゲストの構成に加え、ネットワーク構成の要件がいくつかあります。

1. 直接アクセスのゲストはVNICを使用するため、インストール前に、各ゲストにVNICを割り当てる必要があります。VNICは、必ず、Hyper-Vホスト上のNIC1に割り当ててください。
2. VNICをアタッチしたら、そのVNICに関する次の情報を収集します。
 - IPアドレス、サブネットのデフォルト・ゲートウェイ、およびサブネット・マスク
 - MACアドレス
 - VLANタグ
3. ゲスト・オペレーティング・システムをインストールするか、通常のゲストとしてインポートします。ゲストを外部vSwitchに接続します。
4. ゲストを起動する前に、ゲストを選択して「**設定**」をクリックします。
5. ステップ1で収集した情報を使用し、「**設定**」ダイアログ・ボックスで次のステップを実行します。
 - A. 左のナビゲーション・ペインで、「**ネットワーク アダプター外部**」をクリックします。
 - B. 「**仮想LAN IDを有効にする**」チェック・ボックスを選択します。

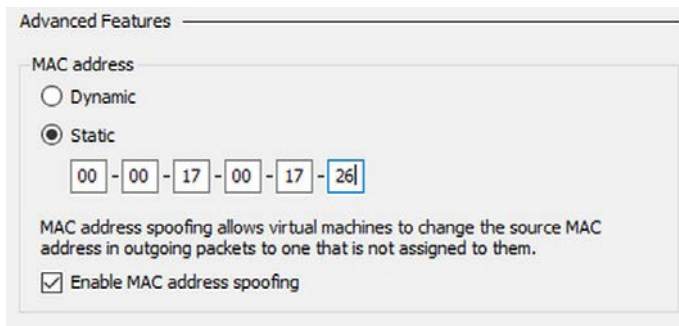
C. VLAN IDを入力します。



6. 左のナビゲーション・ペインで、「ハードウェア アクセラレータ」(「ネットワーク アダプター外部」の下)をクリックして、「SR-IOVを有効にする」チェック・ボックスを選択します。



7. 左のナビゲーション・ペインで、「高度な機能」(「ネットワーク アダプター外部」の下)をクリックします。右側の「MACアドレス」セクションで、「静的」オプションを選択し、使用しているセカンダリVNICに関連付けられているMACアドレスを入力します。「MACアドレスのスプーフィングを有効にする」チェック・ボックスを選択します。



8. 内部ネットワーク・アダプタを追加し、デフォルトの設定はすべてそのままにします。
9. 構成を保存します。
10. ゲストを起動します。これが新しいインストールの場合は、使用しているオペレーティング・システムの指示に従って、静的IP構成を使用するようゲストを構成します。インポートの場合は、静的IPアドレス構成になるよう、ネットワーク・インタフェースを再構成します。
11. Linuxオペレーティング・システムをインストールする場合は、Hyper-V固有のドライバのロードが必要な場合があります。特定のLinuxディストリビューションの詳細は、MicrosoftのWebサイトで、[「Supported Linux and FreeBSD virtual machines for Hyper-V on Windows」](#)を参照してください。

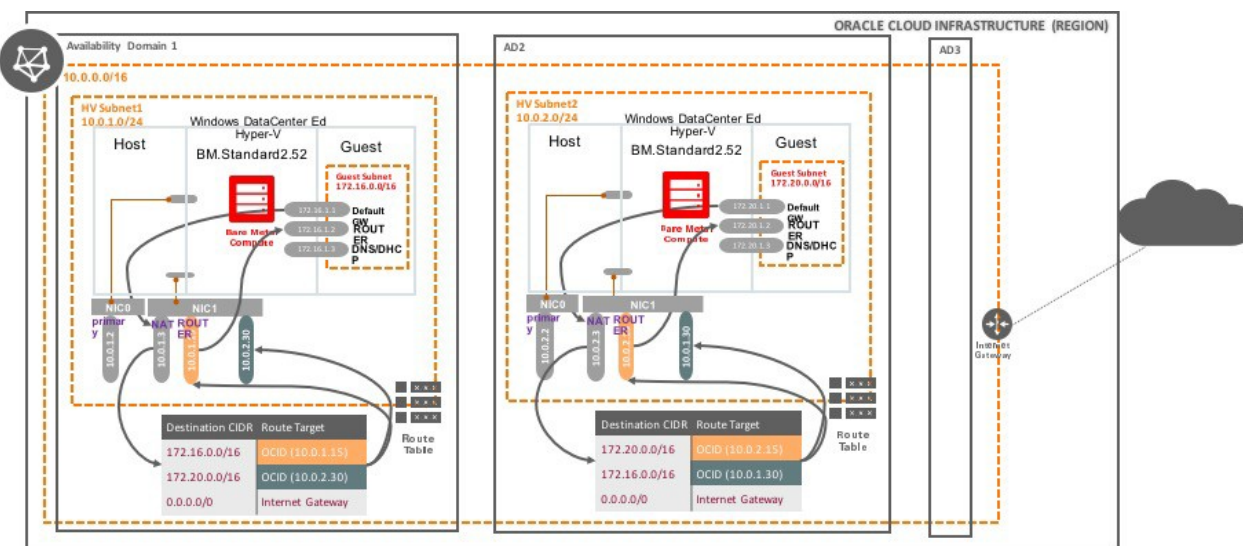
間接アクセスのゲスト

間接アクセスのゲストのネットワーク構成要件はシンプルです。間接アクセスのゲストを構成する際は、次のガイドラインに従います。

- ゲストは、外部vSwitchではなく、内部のHyper-VネットワークvSwitchのみへのアクセスで構成する必要があります。
- ゲストは常にDHCPを使用する必要があります。静的アドレスが必要な場合は、ゲストのMACアドレスをHyper-VベースのDHCPサーバー内にDHCP予約として登録するか、次の情報を使用してゲストを構成し、DHCPに除外を追加します。
 - **IPアドレス:** 割り当てられたIPアドレス
 - **ネットマスク:** IPサブネットのネットマスク
 - **デフォルト・ゲートウェイ:** hvnatインスタンスのHyper-Vアドレス
 - **DNS:** ハイパーバイザのHyper-Vアドレス(先ほど構成したDNS/DHCP)
 - **VCNゲートウェイ(hvrouter)のアドレス経路で、VCNサブネットやその他の内部ネットワークへのルートを手動で追加**

異なるHyper-Vサーバー上のゲスト間における接続の有効化

このプロセスでは、間接アクセス方式でHyper-Vサーバーにインストールされたゲストが、別のサーバー上のゲストと十分にやり取りできるようにします。Oracle Cloud Infrastructure環境全体がこの構成を暗黙的に示しているため、直接アクセス方式のゲストにこのプロセスは必要ありません。次の図に、この構成のアーキテクチャを示します。



このプロセスは、同じVCNで稼働しているすべてのHyper-Vサーバーに適用できます。説明では、Hyper-VサーバーはSvr1とSvr2の2つで、それぞれのゲストのIPアドレスは2つの異なる範囲であると仮定します。この手順を実行する前に、このホワイト・ペーパーで説明したプロセスを使用して、両方のHyper-Vサーバーを構成する必要があります。このプロセスを開始する前に、各Hyper-VサーバーのゲストIPサブネット、関連付けられているネットマスク、hvrouterのIPアドレスを特定しておく必要があります。

1. Svr1のDHCPサーバーを開きます。
2. 「Hyper-Vゲスト用のDNSおよびDHCPの構成」で作成したスコープを選択します。
3. 「スコープ オプション」ダイアログ・ボックスを開き、「121クラスレス静的ルート」を選択します。
4. 次のルート情報を入力します。
 - **宛先:** Svr2に配置されているゲストのIPサブネット
 - **マスク:** Svr2上のゲストのIPサブネット・マスク
 - **ルーター:** Svr1に作成されたhvrouterのIPアドレス
5. 構成を保存してDHCPを再起動します。

6. Svr1で実行しているすべてのゲストのDHCPリースを更新します。
7. Svr2のDHCPサーバーを開きます。
8. 「Hyper-Vゲスト用のDNSおよびDHCPの構成」で作成したスコープを選択します。
9. 「スコープ オプション」ダイアログ・ボックスを開き、「121クラスレス静的ルート」を選択します。
10. 次のルート情報を入力します。
 - 宛先: Svr1上のゲストのIPサブネット
 - マスク: Svr1上のゲストのIPサブネット・マスク
 - ルーター: Svr2に作成されたhvrouterのIPアドレス
11. 構成を保存してDHCPを再起動します。
12. Svr2で実行しているすべてのゲストのDHCPリースを更新します。

各Hyper-VサーバーのVCNのルート表にセキュリティ・リストとエントリを作成してある場合は、これで、各Hyper-Vサーバーのゲスト間で通信できるようになります。関係に加える必要があるその他のHyper-Vサーバーそれぞれにルーティング情報を追加することで、追加のサーバーにこのモデルを拡張できます。

結論

ベア・メタルと仮想インスタンス・タイプは、オペレーティング・システムやアプリケーションをデプロイする際に推奨される方法ではありますが、これらの方法を使用できない状況は多くあります。Windows Serverが一般的である環境では、Hyper-V内でゲストの管理を強力にサポートする運用上の慣例が発達しました。このホワイト・ペーパーで説明したHyper-Vのデプロイ方法では、最小限の中断でその運用をクラウドに拡張できるだけでなく、レガシー・オペレーティング・システムをデプロイする方法が用意されており、CPUとRAMの割合を調整することも可能です。そして、このいずれもクラウド運用に移行しながら行うことができます。

付録A: Hyper-Vレプリカのデプロイ

注意: 先に述べたように、Hyper-Vレプリカを適用できるのは、間接アクセス方式でインストールされたゲストのみです。

その他のハイパーバイザと同じように、Microsoft Hyper-Vを使用してOracle Cloud Infrastructure環境にゲストを作成することは可能ですが、ゲストは単一障害点となります。Oracle Cloud Infrastructureなどのクラウド環境は自己回復性のある運用環境ですが、多くのユーザーが、ワークロードの可用性とビジネス継続性を確保するには、強力な高可用性(HA)の維持が必要だと感じています。強力なHAの維持をサポートするため、Oracle Cloud Infrastructureでは、Hyper-Vレプリカを使用して、2つのHyper-Vインスタンス間でレプリケーション接続を確立できるようになっています。

Hyper-VレプリカはHyper-Vの組込み機能で、これを利用することにより、ストレージ・リソースを共有せずに、オンラインでゲスト・オペレーティング・システムをターゲット・システムにレプリケートできます。Hyper-Vレプリカは、ソース・ゲストの仮想ハード・ディスク(VHD)内の変更追跡を行い、それらの変更をTCPネットワーク接続経由で、レプリカ・ターゲットとして機能している任意のHyper-Vサーバーにレプリケートします。

この付録では、Oracle Cloud Infrastructure内に作成された2つのHyper-Vインスタンス間に、Hyper-Vレプリカ接続を確立するプロセスを説明します。ここで説明するプロセスは、オンプレミス・インスタンスからOracle Cloud Infrastructureインスタンスにデプロイされたレプリカにも適用できます。

前提条件

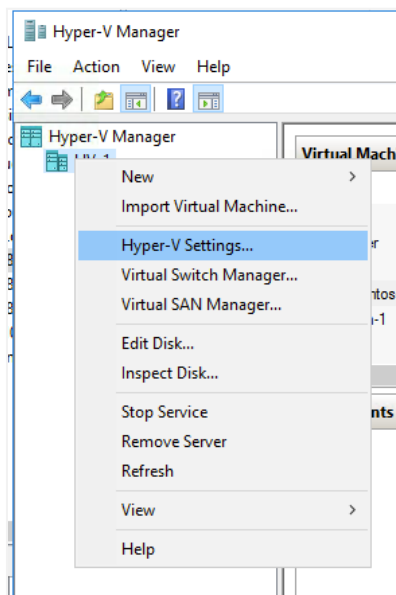
このプロセスを設計どおりに機能させるには、次の前提条件を満たす必要があります。

- リージョン内のレプリカの場合は、このホワイト・ペーパーのメインの部分で説明したとおり、2台のHyper-Vサーバーをデプロイします。Oracle Cloud InfrastructureがオンプレミスからのHyper-Vレプリカ・ターゲットとして機能している場合、必要なHyper-Vサーバーは1台のみです。
- ソースとターゲットのHyper-Vインスタンスが、双方向で接続されていることを確認してください。接続テストは、簡単なpingで十分です。
- ソースとターゲットのHyper-Vインスタンス間で、ホスト名を解決できることを確認してください。
- サブネット内で、TCPポート80と443を使用できるようにします。Oracle Cloud Infrastructureの[セキュリティ・リスト](#)を適切に構成してください。
- レプリカのHyper-Vゲスト用のリポジトリとして機能させるには、追加の[Oracle Cloud Infrastructure Block Volumeストレージ・ボリューム](#)をアタッチするか、Hyper-Vインスタンスにアタッチされた既存のブロック・ストレージ・ボリューム内のディレクトリを特定します。

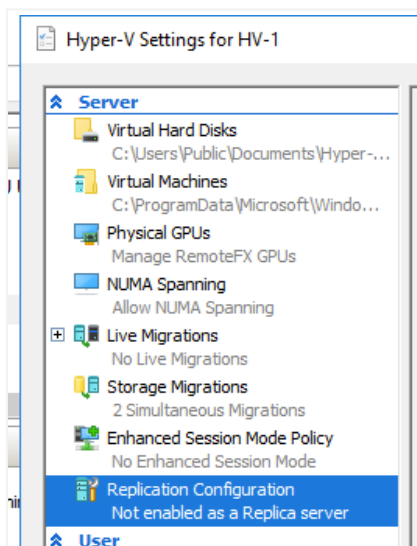
Hyper-Vターゲット・インスタンスの構成

Hyper-Vインスタンスをデプロイしてテストしたら、次の手順を使用して、レプリケーションのターゲットであるインスタンスにHyper-Vレプリカを構成します。

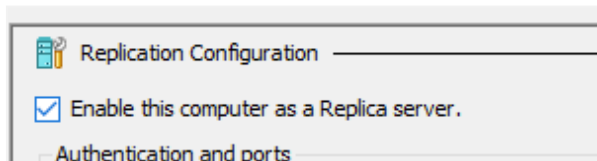
1. Hyper-Vマネージャーを開きます。
2. 左側のペインでHyper-Vホストを右クリックして、「**Hyper-Vの設定**」を選択します。



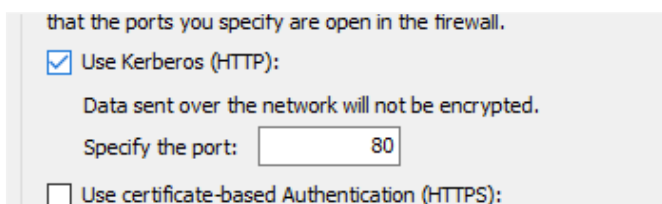
3. 「**Hyper-Vの設定**」ダイアログ・ボックスの左側のペインで、「**レプリケーションの構成**」をクリックします。



4. 右上のペインで、「レプリカ サーバーとしてこのコンピューターを有効にする」を選択します。

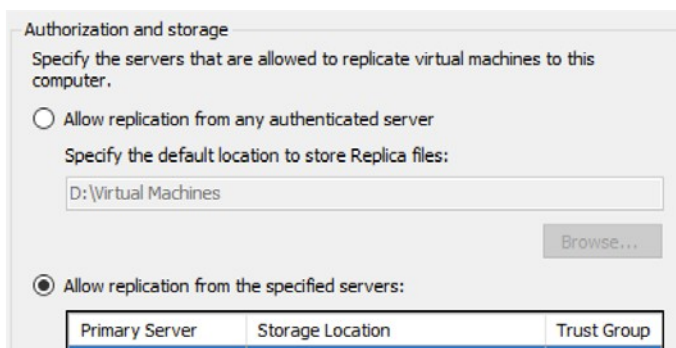


5. 「認証とポート」セクションで、「Kerberosを使用する(HTTP)」を選択します。
TCPポートの値は80のままにします。



注意: この構成では、証明書ベースの認証(HTTPS)が可能ですが、その方法の設定についてはこのホワイト・ペーパーの範疇を超えています。Windows Server 2016における証明書プロバイダの構成に関する、Microsoftの適切なドキュメントを参照してください。

6. 「承認と記憶域」セクションで、「指定したサーバーからのレプリケーションを許可する」オプションを選択します。

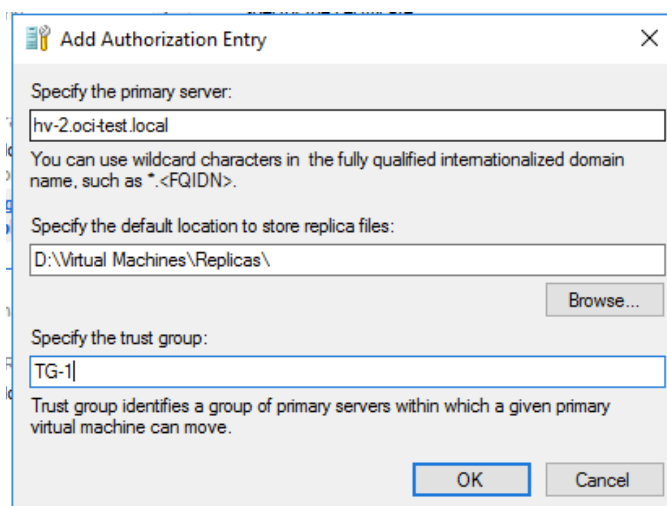


注意: 「認証されたすべてのサーバーからのレプリケーションを許可する」も機能しますが、セキュリティ上の理由から推奨されません。

7. 「追加」をクリックします。

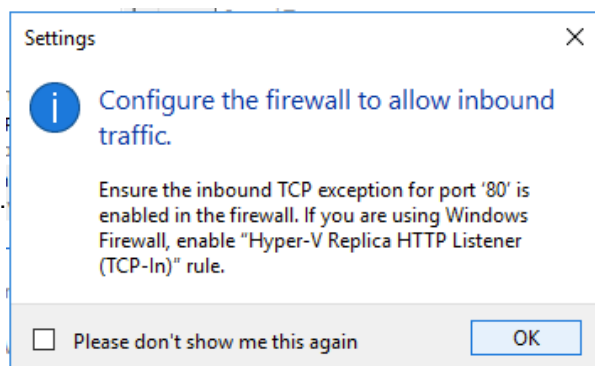
8. 「承認エントリの追加」ダイアログ・ボックスに、次の情報を追加します。

- **プライマリ・サーバー:** これは、レプリカ情報のソース・サーバーです。前提条件の一部としてホスト名の解決で確認したホスト名です。
- **レプリカ・ファイルの場所:** レプリカのターゲットのHyper-Vインスタンスにアタッチされている追加のブロック・ストレージ・ボリューム、またはこのインスタンスのプライマリHyper-Vゲストにアタッチされているブロック・ストレージ・ボリュームへのフルパスです。ブート・ボリュームをレプリカの場所として使用しないでください。
- **信頼グループ:** レプリケーション関係内の参加者のHyper-Vインスタンスを識別する任意のグループ名です。双方向のレプリケーションを可能にする場合は、ソースとターゲットのインスタンス間で、この名前を一致させる必要があります。



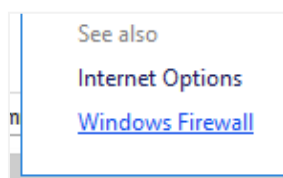
9. 「OK」をクリックして、「レプリケーションの構成」セクションの「OK」をクリックします。

10. 表示される設定メッセージの「OK」をクリックします。

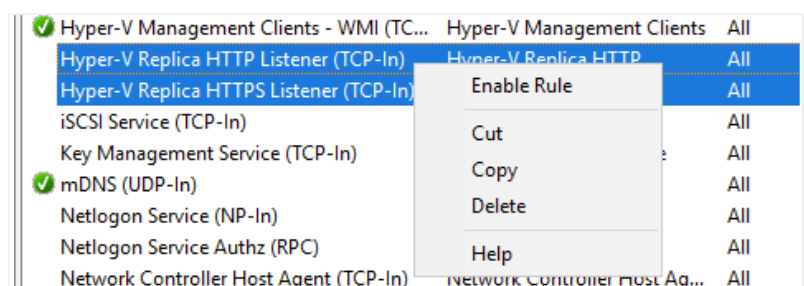


11. Windowsのコントロール パネルで、「ネットワークと共有センター」を開きます。

12. ウィンドウの左下にある「**Windowsファイアウォール**」をクリックします。



13. 「**Windowsファイアウォール**」ウィンドウで、「**詳細設定**」をクリックします。
14. 「**セキュリティが強化されたWindowsファイアウォール**」ウィンドウで、「**受信の規則**」をクリックします。
15. 次のスクリーンショットに表示されているように、スクロール・ダウンして、2つのHyper-Vレプリカ規則を見つけます。規則を両方選択して右クリックし、「**規則の有効化**」を選択します。



16. 「Windowsファイアウォール」ウィンドウを両方とも閉じます。

これで、指定したHyper-Vインスタンスのレプリカを受信するよう、インスタンスが設定されます。双方向のレプリケーションを有効にする場合は、ソースのHyper-Vインスタンスでこのプロセスを繰り返します。

Hyper-Vゲストの構成

ターゲットのHyper-Vインスタンスを構成したら、ターゲットのHyper-Vインスタンスにレプリケートするよう、ソースのHyper-Vインスタンス内のゲストを個別に構成します。

オンプレミスからOracle Cloud Infrastructureへのゲスト・レプリケーションの制限事項

オンプレミスからOracle Cloud Infrastructureにレプリケートされたゲストは、ネットワーク構成やドメイン・ステータス、DNS登録によっては、いくつかの構成の変更が必要な場合があります。デフォルトの構成では、Oracle Cloud Infrastructure環境内に作成されたゲストは、ネットワークの1つのvSwitchにしかアクセスできません。同じ制限が、オンプレミスのインスタンスからOracle Cloud InfrastructureのHyper-Vインスタンスにレプリケートされたゲストにも適用されます。Oracle Cloud Infrastructureにレプリケートされた場合、vSwitchが複数アタッチされているオンプレミスのゲストには、ネットワーク・インタフェースが1つしかないため、構成が必要になります。

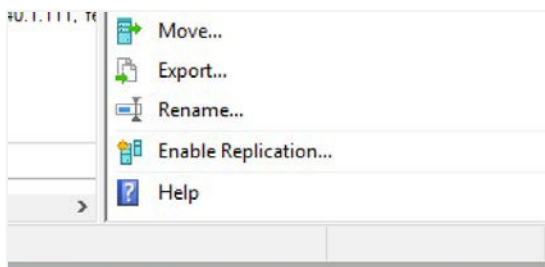
ドメインに参加したゲストは、Oracle Cloud Infrastructureにレプリケートした後、ドメイン・コントローラに到達できない場合、認証の問題が発生する可能性があります。ドメインに参加したゲストをOracle Cloud InfrastructureのHyper-Vインスタンスにレプリケートする場合は、レイテンシが大きいこと、またはドメインが切断されていることが原因の認証の問題を回避するために、Oracle Cloud Infrastructure内にプライマリ・ドメイン・コントローラ、バックアップのドメイン・コントローラ、または読み取り専用のドメイン・コントローラを作成することをお勧めします。

ドメインに参加していないゲスト、またはWindows以外のゲストがDNSサービスを使用している場合は特に、ゲストのホスト名の解決が失敗する場合があります。Oracle Cloud Infrastructure内に作成されたドメイン・サービスのサポートで、Windows DNSサービスが作成されていない場合にも、解決が失敗します。フェイルオーバー後にゲストとの接続を維持するために、DNSを手動で確認し、レプリカに割り当てられている現在のIPアドレスが、適切なDNSゾーンに正しく挿入されていることの確認をお勧めします。ホスト名を正しく解決するために、DNSの手動での更新が必要になる場合があります。現在、Oracle Cloud InfrastructureのDNSサービスでは、Hyper-Vまたはその他の外部DNSサービスからの更新が正しく認識されないか受け付けられません。

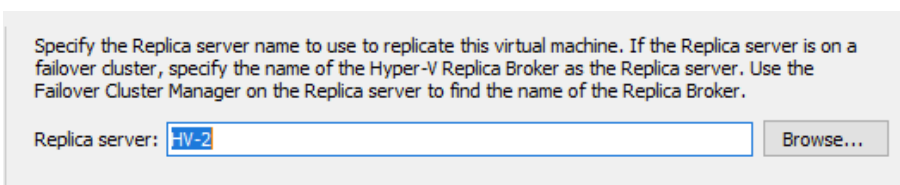
Hyper-Vゲストの構成

次の手順に従って、各ゲストを構成します。

1. Hyper-Vマネージャーを開いて、レプリケートするゲストを選択します。
2. 右下のペインで、「**レプリケーションを有効にする**」をクリックします。

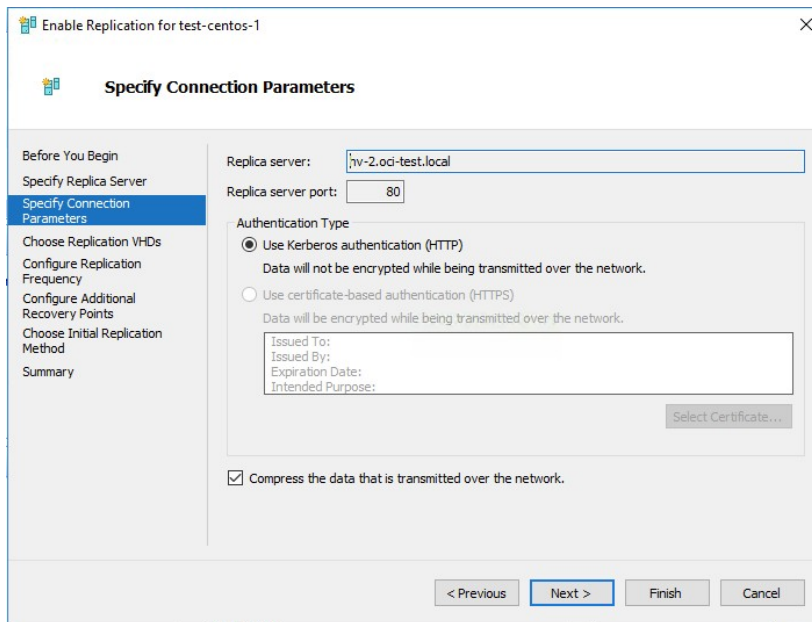


3. ウィザードの最初のページで、「**次へ**」をクリックします。
4. 次のページで、「**レプリカ サーバー**」ボックスにターゲットのHyper-Vインスタンスのホスト名を入力し、「**次へ**」をクリックします。



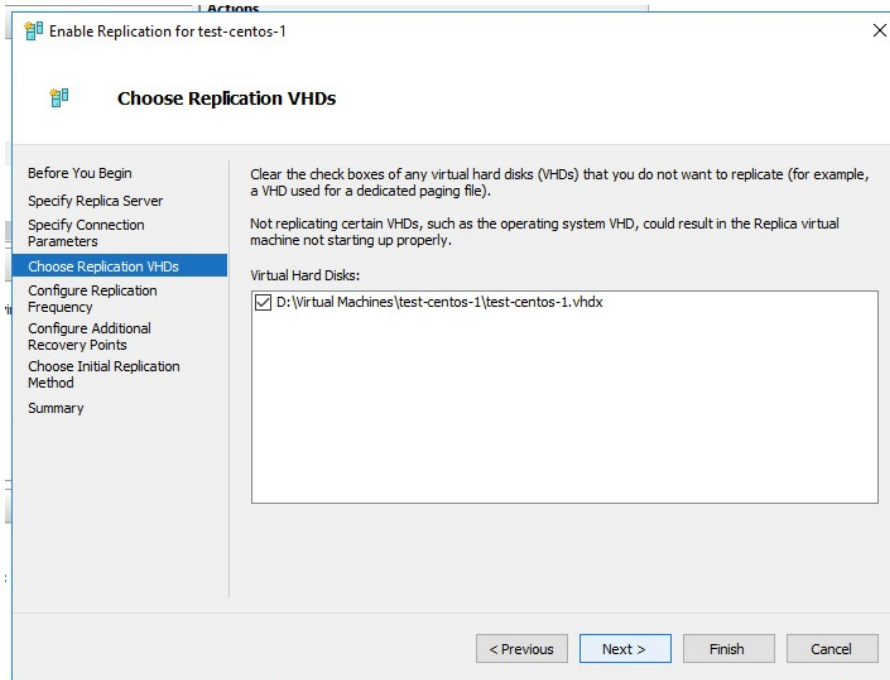
注意: ソースとターゲットのHyper-Vインスタンス間の通信エラーは、ホスト名の解決が主な原因です。エラーが発生した場合は、ボックスに入力したホスト名が、その正確なホスト名で解決できることを確認してください。適切に接続するためにFQDNが必要になる場合があります。また、ソースのHyper-Vインスタンス名が、「Hyper-Vターゲット・インスタンスの構成」の手順で詳しく説明した、承認エントリの追加ステップで設定したものに一致する必要があります。

通信に成功すると、「**接続パラメータの指定**」ページが表示されます。

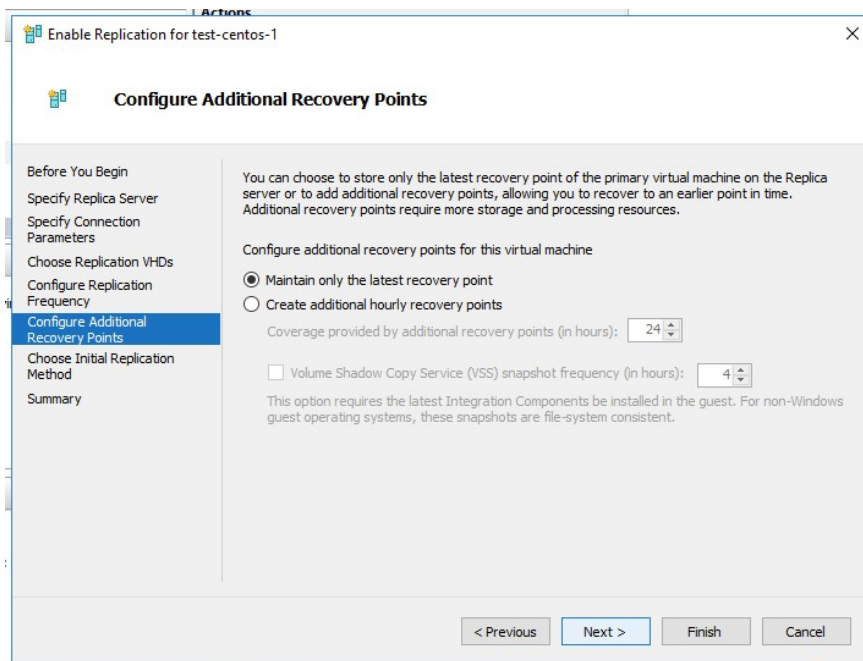


5. 「**Kerberos認証を使用する(HTTP)**」オプションを選択し、「**ネットワーク経由で送信されたデータを圧縮する**」チェック・ボックスを選択して、「**次へ**」をクリックします。

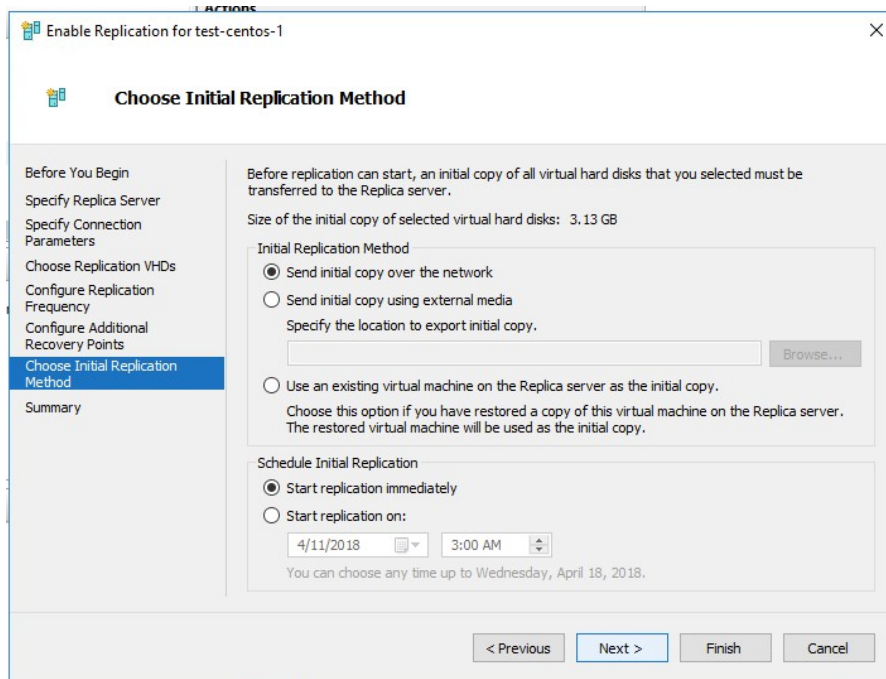
6. このゲストに関連付けられているすべてのVHDを選択して、「次へ」をクリックします。



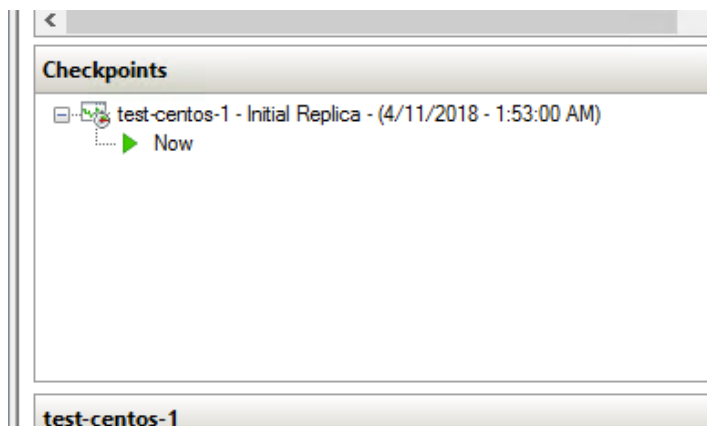
7. レプリケーションの頻度を選択して、「次へ」をクリックします。
8. 保持する回復ポイントの数を選択します。複数の回復ポイントを選択した場合は、VSSオプションを選択しないでください。



9. 初期レプリケーションの方法として、「初期コピーをネットワーク経由で送信する」を選択し、初期レプリケーションのスケジュールを環境に合わせて選択します。「完了」をクリックします。



すぐにレプリケートすることを選択した場合は、レプリケートしているゲストのHyper-V マネージャーに、次のようなエントリが表示されます。



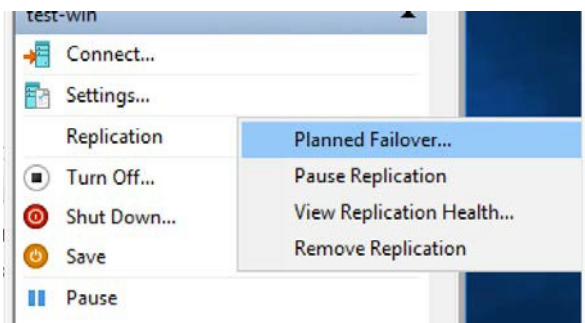
ソースとターゲットのHyper-Vインスタンス間でのフェイルオーバー

使い始める前に、この構成を使用して、インスタンスを手動でレプリカ・ターゲットにフェイルオーバーする必要があります。

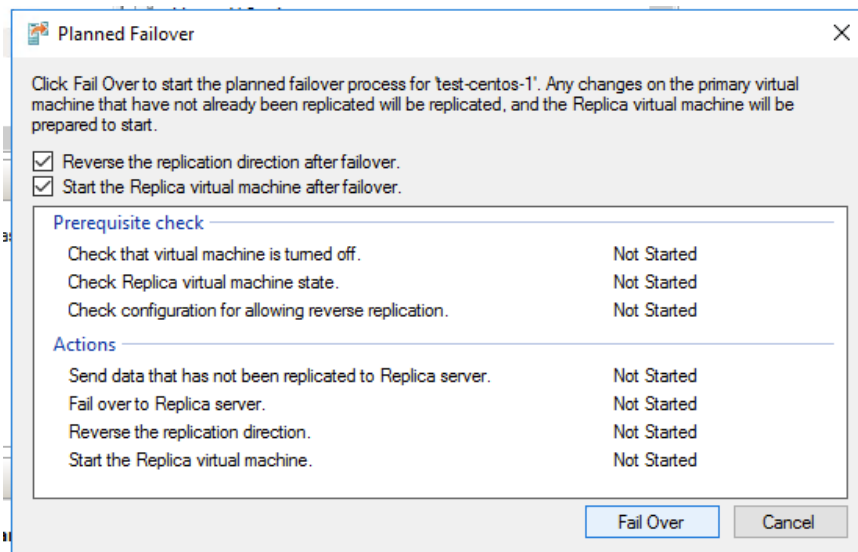
注意: ターゲットのHyper-Vインスタンスにフェイルオーバーしたゲスト(特にオンプレミス環境からのゲスト)は、「オンプレミスからOracle Cloud Infrastructureへのゲスト・レプリケーションの制限事項」にリストされている制限事項の対象です。

次の手順を使用して、Hyper-Vゲストをレプリカ・インスタンスにフェイルオーバーします。

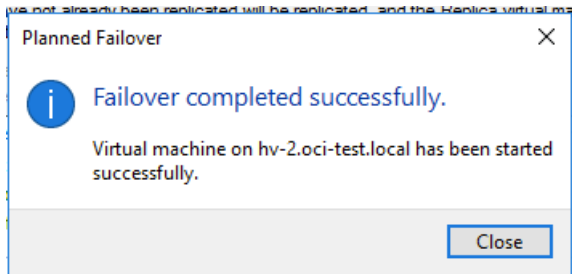
1. ソース・インスタンスのHyper-Vマネージャーを開き、Hyper-Vゲストを停止します。
2. Hyper-Vマネージャーでゲストが選択された状態で、右下のペインで「レプリケーション」を右クリックして、メニューから「計画フェールオーバー」を選択します。



3. 「計画フェールオーバー」ダイアログ・ボックスで、運用の必要性に合わせて、「フェールオーバー後にレプリケーションの方向を反転する」チェック・ボックス、「フェールオーバー後にレプリカ仮想マシンを起動する」チェック・ボックス、またはその両方を選択します。その後、「フェールオーバー」をクリックします。



ボックスにリストされているステップの順にレプリケーションが実行され、各ステップの成功に関するフィードバックが表示されます。レプリケーションが成功すると、次のメッセージが表示されます。



ゲストを元のHyper-Vインスタンスにフェイルオーバーしなおすには、ターゲットのHyper-Vインスタンスにログインし、このプロセスを逆に行います。



Oracle Corporation, World Headquarters

500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries

Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US



blogs.oracle.com/oracle



facebook.com/oracle



twitter.com/oracle



oracle.com

Integrated Cloud Applications & Platform Services

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. 本文書は情報提供のみを目的として提供されており、ここに記載されている内容は予告なく変更されることがあります。本文書は一切間違いがないことを保証するものではなく、さらに、口述による明示または法律による黙示を問わず、特定の目的に対する商品性もしくは適合性についての黙示的な保証を含み、いかなる他の保証や条件も提供するものではありません。オラクル社は本文書に関するいかなる法的責任も明確に否認し、本文書によって直接的または間接的に確立される契約義務はないものとします。本文書はオラクル社の書面による許可を前もって得ることなく、いかなる目的のためにも、電子または印刷を含むいかなる形式や手段によっても再作成または送信することはできません。

OracleおよびJavaはオラクルおよびその関連会社の登録商標です。その他の社名、商品名等は各社の商標または登録商標である場合があります。

Intel、Intel Xeonは、Intel Corporationの商標または登録商標です。すべてのSPARCの商標はライセンスをもとに使用し、SPARC International, Inc.の商標または登録商標です。AMD、Opteron、AMDロゴ、AMD Opteronロゴは、Advanced Micro Devices, Inc.の商標または登録商標です。UNIXは、The Open Groupの登録商標です。1118

Oracle Cloud InfrastructureのHyper-Vのデプロイ

2018年11月

著者: Steven B. Nelson



Oracle is committed to developing practices and products that help protect the environment.