



Microsoft Azure

Microsoft Azure 自習書シリーズ No.14

Azure Site Recovery を利用した Hyper-V サイトの DR 対策
(オンプレミスから Azure のサイト回復)

Published: 2014 年 9 月 30 日

本書に含まれる情報は本書の制作時のものであり、将来予告なしに変更されることがあります。提供されるソフトウェアおよびサービスは市場の変化に対応する目的で隨時更新されるため、本書の内容が最新のものではない場合があります。本書の記述が実際のソフトウェアおよびサービスと異なる場合は、実際のソフトウェアおよびサービスが優先されます。Microsoft および Cloudlive は、本書の内容を更新したり最新の情報を反映することについて一切の義務を負わず、これらを行わないことによる責任を負いません。また、Microsoft および Cloudlive は、本書の使用に起因するいかなる状況についても責任を負いません。この状況には、過失、あらゆる破損または損失（業務上の損失、収益または利益などの結果的な損失、間接的な損失、特別の事情から生じた損失を無制限に含む）などが含まれます。

Microsoft、SQL Server、Visual Studio、Windows、Windows Server、MSDN は米国 Microsoft Corporation および、またはその関連会社の、米国およびその他の国における登録商標または商標です。

その他、記載されている会社名および製品名は、各社の商標または登録商標です。

© Copyright 2014 Microsoft Corporation. All rights reserved.

目次

はじめに	4
STEP 1. Azure Site Recovery のサービス概要	6
1.1 Hyper-V レプリカと Azure Site Recovery	7
1.2 Azure Site Recovery の 2 つのソリューション	9
1.3 Azure Site Recovery の利用料金	12
1.4 オンプレミスから Azure のシステム要件	14
STEP 2. サービスの導入	18
2.1 評価環境のシステム構成	19
2.2 Microsoft Azure サブスクリプションの準備	20
2.3 VMM のインストールと構成	21
2.4 保護される仮想マシンの準備	33
2.5 Microsoft Azure 側の準備	35
2.6 Azure Site Recovery のオンプレミス側コンポーネントの展開	40
2.7 VMM クラウドの保護の構成	47
2.8 仮想マシンの保護の有効化	50
2.9 レプリケーションの正常性の監視	52
STEP 3. フェールオーバーの管理	54
3.1 フェールオーバーとは	55
3.2 復旧計画の作成	58
3.3 テスト フェールオーバー	61
3.4 計画されたフェールオーバー	64
3.5 計画されていないフェールオーバー	67
3.6 フェールバック	69
STEP 4. サービスの利用停止	72
4.1 仮想マシンの保護の無効化	73
4.2 クラウドの保護の解除	74
4.3 サーバーの登録解除	75
4.4 クラウド サービスの削除	76
オンプレミスから Azure のサイト回復の FAQ	77
おわりに	84

はじめに

3.11 の東日本大震災とその後の電力需給の逼迫を経験し、企業は大規模な自然災害や電源障害に備えた障害・災害復旧（ディザスター リカバリ：DR）対策の必要性を、企業規模を問わず認識していることでしょう。その時がきたとき、顧客に対するサービスとデータを保護し、事業継続を確実にするには、広範囲な災害や障害の影響を受けない、地理的に離れた代替拠点による DR 対策が必要です。

◆ DR 対策にクラウドを活用するメリット

ここ数年で、多くの企業が仮想化テクノロジを利用して、データセンターへのリソースの集約を進めてきました。仮想化の普及および技術革新により、地理的に離れた拠点を利用した DR 対策の実装は、以前よりも容易かつ柔軟になりました。しかし一方で、第 2 のデータセンターを設置するのにかかる設備コストは、DR 対策を実際に構築する上で大きな課題になります。

そこで注目されるのが、グローバルに展開され、冗長化されたデータセンターから提供される、パブリック クラウドのサービスおよびリソースです。パブリック クラウドは、DR 対策の地理的な条件に合致します。また、設備投資なしで使用に応じた従量課金で利用できることも、コスト削減に貢献すると期待できます。

2014 年 1 月か正式なサービスを開始した Microsoft Azure Hyper-V Recovery Manager は、2014 年 6 月に Microsoft Azure Site Recovery と名前を変え、新たに Microsoft Azure のパブリック クラウド インフラストラクチャを DR 対策用のセカンダリ サイトとして活用できるサービスをプレビュー機能として追加しました。2014 年 9 月にすべての機能が正式リリースとなり、日本国内のデータセンター（東日本、西日本）からのサービス提供も開始されています。

◆ Azure Site Recovery のヒストリー

Microsoft Azure Site Recovery はもともと、Windows Azure Hyper-V Recovery Manager としてサービス提供を開始しました。Microsoft Azure Site Recovery としての正式サービス開始までの歩みは、以下のとおりです。

年月	サービスの更新内容
2013 年 4 月	Windows Azure 復旧サービスの 1 つとして、Windows Azure Hyper-V Recovery Manager の限定プレビューを開始。オンプレミスからオンプレミスのサイト回復の保護を提供。
2013 年 10 月	Windows Azure Hyper-V Recovery Manager のパブリック プレビューを開始。
2014 年 1 月	Windows Azure Hyper-V Recovery Manager の正式サービスを開始。
2014 年 3 月	Windows Azure から Microsoft Azure に名称変更を発表。
2014 年 6 月	Microsoft Azure Hyper-V Recovery Manager から Microsoft Azure Site

	Recovery に名称変更。オンプレミスから Azure のサイト回復機能を追加し、プレビュー提供を開始。
2014 年 7 月	マイクロソフトが InMage Systems の買収を完了。Microsoft Azure Site Recovery のサービス メニューに InMage Scout ソフトウェアを統合。
2014 年 8 月	1 日より Microsoft Enterprise Agreement を通じて Azure Site Recovery サブスクリプション ライセンスの提供を開始。22 日より、日本データセンター（東日本、西日本）からのサービス提供を開始。
2014 年 9 月	オンプレミスから Azure のサイト回復の復旧計画にスクリプトのサポート（Azure Automation プレビューとの統合）を追加

STEP 1. Azure Site Recovery のサービス概要

この STEP では Microsoft Azure 復旧サービスの Azure Site Recovery が提供するサービスの概要について説明します。

この STEP では、次のことを学習します。

- ✓ Azure Site Recovery の要素技術
- ✓ Azure Site Recovery の 2 つの展開パターン
- ✓ Azure Site Recovery の課金について
- ✓ オンプレミスから Azure のサイト回復のシステム要件

1.1 Hyper-V レプリカと Azure Site Recovery

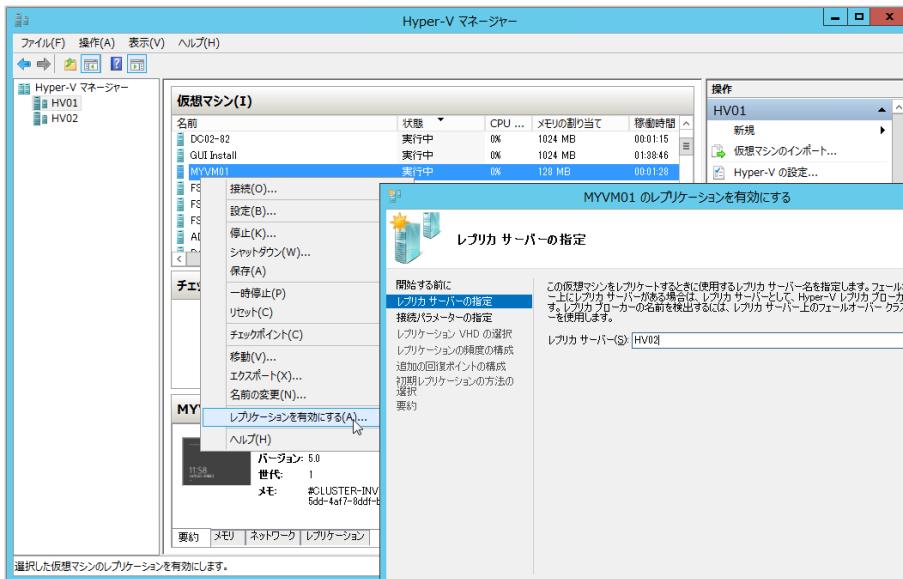
Microsoft Azure Site Recovery は、Microsoft Azure 復旧サービスに含まれるプライベート クラウドの保護サービスです。このサービスは、仮想マシンのサイト間レプリケーションとセカンダリ サイトへの切り替えで、ほとんどゼロに近いデータ損失で、短時間で仮想マシンを復旧する、DR ソリューションです。

Microsoft Azure 復旧サービスには他に Microsoft Azure Backup サービスがありますが、こちらはクラウドのバックアップ領域を利用したデータ バックアップおよび回復サービスであり、Azure Site Recovery とは概念や用途が異ります。

◆ Hyper-V レプリカとは

Windows Server 2012 以降の Hyper-V には、Hyper-V レプリカという仮想マシンの DR 対策機能が標準搭載されています。Hyper-V レプリカは、2 台の Hyper-V ホスト、または 2 つの Hyper-V ホスト クラスター間で簡単に構成でき、運用中のプライマリ サーバーの仮想マシンのレプリカ（複製）を、レプリカ サーバーに作成し、仮想ハード ディスクの変更差分を 5 分間隔（既定）でレプリカ仮想マシンにレプリケーションして、最新の状態に更新します。

電源障害や故障、メンテナンスなどでプライマリ サーバーが利用できなくなった場合は、レプリカサーバーのレプリカ仮想マシンにフェールオーバーし、すばやく仮想マシンを復旧することができます。フェールオーバー後、プライマリとレプリカの関係は自動または手動で反転され、次のフェールオーバー（正常運用体制へのフェールバック）に備えます。



画面: Hyper-V レプリカは、Windows Server 2012 以降の Hyper-V の標準機能。2 台の Hyper-V ホスト間または 2 つのホスト クラスター間で仮想マシンをレプリケーションして障害や災害に備える

Windows Server 2012 の Hyper-V レプリカは 5 分間隔、Windows Server 2012 R2 の Hyper-V レプリカは 30 秒、5 分（既定）、または 15 分間隔でレプリケーションを行い、障害発生時には最後にレプリケーションされたデータを使用して、最小限のデータ損失で仮想マシンを復旧できます。

◆ Virtual Machine Manager をクラウド サービスで拡張

最新の System Center Virtual Machine Manager は最新の Hyper-V の仮想化インフラストラクチャの管理に対応していますが、Hyper-V レプリカを直接管理する機能は提供しません。そのため、Virtual Machine Manager の管理コンソールから Hyper-V レプリカを構成したり、レプリケーションの監視やフェールオーバー操作を実行することはできません。

Azure Site Recovery の前身である Azure Hyper-V Recovery Manager は、Virtual Machine Manager の管理環境に Hyper-V レプリカのレプリケーション保護機能を追加するクラウド サービスとして提供されました。このサービスは、クラウドから Virtual Machine Manager で管理されるクラウド（管理境界の概念、以下、VMM クラウド）のレプリケーションを VMM クラウド間で構成および調整し、グループ単位または仮想マシン単位でのワン クリック フェールオーバー機能を提供します。

地理的に離れた 2 つの VMM クラウド間でレプリケーションを行う関係上、障害や災害発生時にはその拠点の Virtual Machine Manager との通信は途絶えることが想定されます。そのためマイクロソフトは、障害や災害の影響を受けないパブリック クラウドからサービス提供を選択しました。

Azure Hyper-V Recovery Manager はその後、Azure Site Recovery に名称が変更され、同時に VMM クラウドと Microsoft Azure 間でのレプリケーション機能を追加し、DR 対策ソリューションを強化しました。

◆ Azure Site Recovery の RPO と RTO

セカンダリ サイトを用いた DR は、ダントンタイムと潜在的なデータ損失を伴う複雑なタスクです。DR 対策を講じる上で重要になるのが、RPO (Recovery Point Objective: 目標復旧時点) と RTO (Recovery Time Objective: 目標復旧時間) という 2 つの指標です。これらができるだけ小さくすることで、ビジネス継続性に要求される MTD (Maximum Tolerable Downtime: 最大許容停止時間) を達成できます。

RPO (Recovery Point Objective: 目標復旧時点) … 復旧によるデータ損失が許容される最大の時間幅。重要度が高いデータほど、RPO の短縮が求められる

RTO (Recovery Time Objective: 目標復旧時間) … アプリケーションの機能を復旧するために許容する最大の時間。重要度が高いアプリケーションほど、RTO の短縮が求められる

Azure Site Recovery は Hyper-V レプリカの機能を利用しているため、計画されていないセカンダリ サイトへの DR に対して、Windows Server 2012 Hyper-V 環境では 5 分、Windows Server 2012 R2 Hyper-V 環境では 30 秒、5 分、または 15 分の RPO (目標復旧時点) を提供します。Azure Site Recovery では、複数の仮想マシンをグループ化し、依存関係に基づいて順番に仮想マシンを開始したり、追加の復旧処理を実行したりするために復旧計画 (Recovery Plan) を作成できます。復旧計画を使用したフェールオーバーもワン クリックで開始でき、RTO (目標復旧時間) を短縮するとともに、人的なミスを排除した確実な復旧処理を可能にします。

1.2 Azure Site Recovery の 2 つのソリューション

Azure Site Recovery には、オンプレミスのプライベート クラウドまたは仮想化インフラストラクチャを保護する方法として、「オンプレミスからオンプレミス」と「オンプレミスから Azure」の 2 つの展開方法があります。この他にもう 1 つ、InMage Scout ソフトウェアによる保護がありますが、これについては後述するコラムを参照してください。

→ オンプレミスからオンプレミスのサイト回復（お客様所有サイトに対する Azure Site Recovery）

オンプレミスからオンプレミスのサイト回復は、Microsoft Azure Site Recovery が Windows Azure Hyper-V Recovery Manager という名前で登場した当初からの機能です。お客様所有の 2 つのサイト（拠点）にそれぞれ展開された Virtual Machine Manager で管理される 2 つの VMM クラウド間でレプリケーションを構成し、プライマリ サイトの VMM クラウドを、もう一方のセカンダリ サイトの VMM クラウド（復旧クラウド）がバックアップする形で Hyper-V 仮想マシンを保護します。

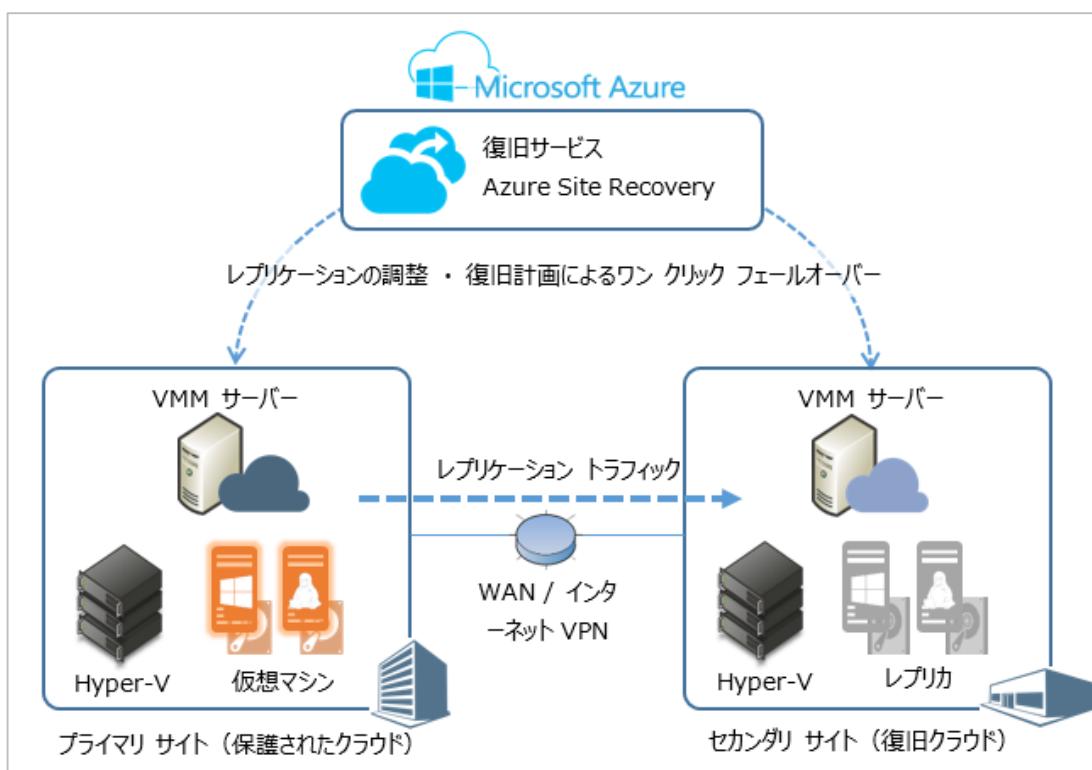


図 1: Azure Site Recovery のオンプレミスからオンプレミスのサイト回復保護（旧 Hyper-V Recovery Manager と同じ機能）

プライマリ サイトが電源障害や大規模災害などで利用できなくなった場合は、Azure Site Recovery ポータルを使用して、あらかじめ定義しておいた復旧計画をワン クリックで開始し、セカンダリ サイトの復旧クラウドに仮想マシンをフェールオーバーして、最後に同期された仮想ハード ディスク (VHD または VHDX) を使って仮想マシンを迅速に復旧できます。障害サイトが復旧した場合は、フェールバックを実行することで、セカンダリ サイトの復旧クラウドで行われた変更をプライマリ サイトのクラウドに完全に同期してから、通常の運用に戻ることができます。

フェールオーバーは、サイト全体のメンテナンス作業のために使用することもできます。それには、計画的フェールオーバーを実行して最新の状態に同期してから、セカンダリ サイトに切り替えます。

名前	ロール	状態	サーバー	仮... ターゲット... リソース ジョブ
Backup Cloud - 2ndDC	復旧クラウド	構成済み	SC02.demo.contoso.com	2
Primary Cloud	保護されたクラウド	構成済み	SC01.demo.contoso.com	2
			SC02.demo.contoso.com	Backup Cloud ...

画面: プライマリ サイトの PrimaryCloud をセカンダリ サイトの Backup Cloud - 2ndDC で保護している状態

▼ オンプレミスから Azure のサイト回復 (Azure に対する Azure Site Recovery)

オンプレミスから Azure のサイト回復は、2014 年 6 月からプレビュー提供が開始され、2014 年 9 月に正式リリースとなった新しい機能です。この機能は、Virtual Machine Manager で管理されたオンプレミスの VMM クラウドから、仮想マシンの仮想ハード ディスクを Microsoft Azure ストレージにレプリケーションすることで、VMM クラウドの Hyper-V 仮想マシンを保護します。ちょうど、オンプレミスからオンプレミスのサイト回復における復旧クラウドを、Microsoft Azure に置き換えた形になります。

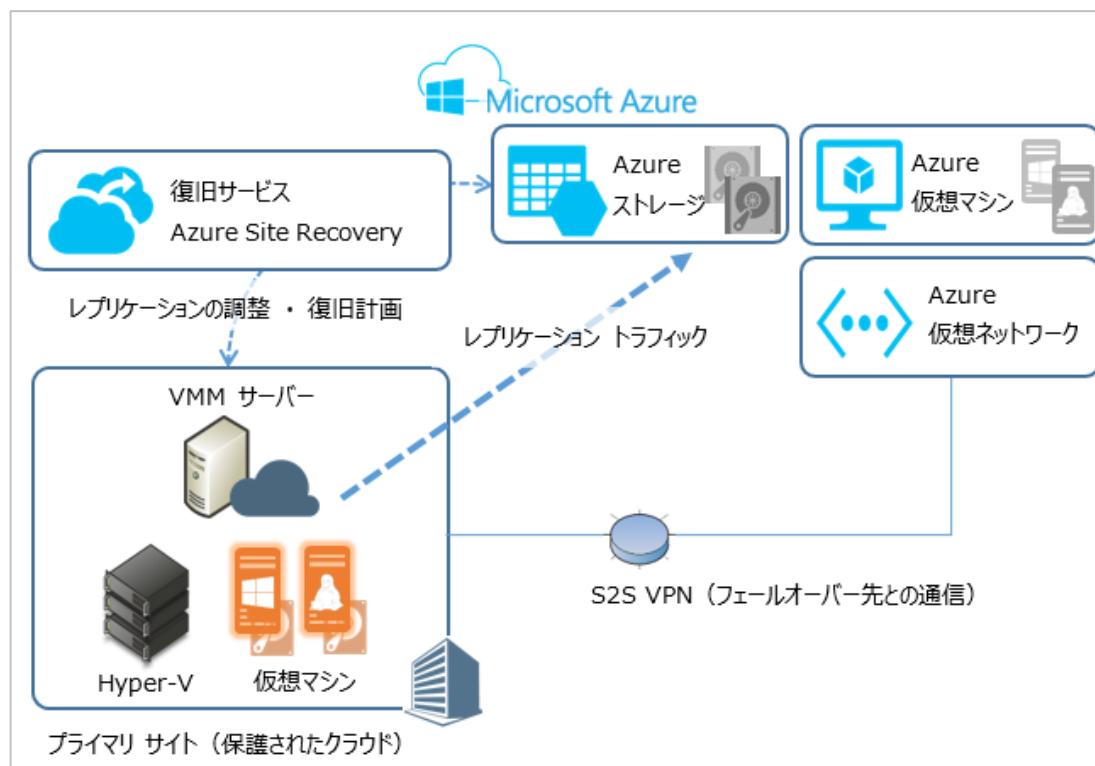


図 2: Azure Site Recovery のオンプレミスから Azure のサイト回復保護。Microsoft Azure の IaaS 環境をフェールオーバー時に利用することで、Microsoft Azure を DR 対策のための第 2 のデータセンターのように活用できる

オンプレミスの VMM クラウドが利用不能になった場合は、Azure Site Recovery ポータルからワン クリックでフェールオーバーを開始し、Microsoft Azure の IaaS (Infrastructure as a

Service) のサービスを利用して、仮想ハード ディスクのレプリカから仮想マシンを作成し、Microsoft Azure 仮想マシンとして復旧します。オンプレミスの企業内ネットワークとは Microsoft Azure 仮想ネットワークのサイト間 VPN 接続で相互接続されるため、エンドユーザーは復旧した仮想マシンのサービスに、社内ネットワークを通じてそのままアクセスできます。



画面：プライマリ サイトであるオンプレミスの OnPremise Cloud を Microsoft Azure をセカンダリ サイトとして保護している状態

自社でセカンダリ サイトを準備する場合、拠点や設備、ハードウェア、ソフトウェア、通信回線など、大きな初期投資および運用コストがかかります。オンプレミスから Azure のサイト回復は、Microsoft Azure のパブリック クラウド インフラストラクチャを DR 対策のためのセカンダリ サイトとして利用できるため、初期投資が不要な上、バックアップ用の資産を抱えることもありません。また、フェールオーバーを開始するまでフェールオーバー先の Microsoft Azure 仮想マシンは作成されないため、通常時にはストレージとデータ転送の使用だけで済み、仮想マシンのためのコンピューティング リソースを消費しないため、リソースを予約しておくような無駄なコストも発生しません。

Note : Azure Site Recovery への InMage Scout ソフトウェアの統合

マイクロソフトは 2014 年 7 月、InMage Systems 社の買収を完了し、VMware 仮想マシンおよび物理サーバー (Windows および Linux) の保護に対応した InMage Scout ソフトウェアを Azure Site Recovery サブスクリプション ライセンスの一部として提供することを発表しました。Azure Site Recovery サブスクリプション ライセンスを購入すると、InMage Scout を使用した VMware サイトおよび物理サーバーの 1 年間の保護を利用できるようになります。InMage Scout のソフトウェアおよび関連ドキュメントは、Microsoft Azure Site Recovery ポータルの [クリック スタート] ページの [回復のセットアップ] から [2 つの内部設置型 VMware サイトの間] を選択することで、ダウンロードできます。

InMage Scout は、保護対象をレプリケーションや P2V テクノロジを用いてセカンダリ サイトの VMware vSphere 仮想化インフラストラクチャ上にバックアップすることで DR 対策を実現します。将来的には、Azure Site Recovery のサービスとの統合も進む予定です。2014 年 9 月上旬には、InMage Scout と連携して VMware 仮想マシンや物理サーバーを Azure 仮想マシンにマイグレーションする、Microsoft Migration Accelerator の限定レビューが開始されています。

Migration Accelerator Preview

<http://azure.microsoft.com/en-us/features/migration-accelerator/>

1.3 Azure Site Recovery の利用料金

◆ 従量課金制プランでの提供

Azure Site Recovery は、保護される仮想マシンごとに、その保護に対して従量課金制で課金されます。月額の料金は、保護する仮想マシンの 1 か月における 1 日あたりの平均数を 1 単位として計算されます。例えば、月の前半はずっと 20 台の仮想マシンを保護し、後半は 1 台も保護しなかった場合、その月の保護する仮想マシンの平均数は 1 日あたり 10 台であり、その月は 10 台ぶんの料金が課金されます。

Azure Site Recovery の展開方法（オンプレミスからオンプレミスのサイト回復、オンプレミスから Azure のサイト回復）によって、保護される仮想マシンあたりの月額単価が異なります。サービスの料金詳細については、以下のサイトにて確認してください。

Azure Site Recovery 料金の詳細

<http://azure.microsoft.com/ja-jp/pricing/details/site-recovery/>

◆ その他の課金の可能性

オンプレミスから Azure のサイト回復を使用する場合、レプリケーションのためのデータ転送とストレージの使用に関して、Microsoft Azure のストレージ サービス（ストレージおよびストレージ トランザクション）と、データ転送（Azure 側からの送信データ）の利用料金がかかります。なお、Microsoft Azure は Azure への受信方向のデータ転送は無料であるため、オンプレミスから Azure 方向へのレプリケーションのためのデータ転送に課金されることはありません。また、Microsoft Azure へのフェールオーバーのために、Microsoft Azure 仮想ネットワークとオンプレミスの VPN 接続にはゲートウェイとデータ転送（Azure 側からの送信データ）の利用料金、および Microsoft Azure 仮想マシンのコンピューティング インスタンスの利用料金がかかります。コンピューティング インスタンスの利用料金は、インスタンスのサイズやゲスト OS の種類（Windows または Linux）によって異なることにも留意してください。各サービスの料金詳細については、以下のサイトにて確認してください。

Storage (ストレージ サービス) の料金詳細

<http://azure.microsoft.com/ja-jp/pricing/details/storage/>

データ転送の料金詳細

<http://azure.microsoft.com/ja-jp/pricing/details/data-transfers/>

Virtual Machines の料金詳細

<http://azure.microsoft.com/ja-jp/pricing/details/virtual-machines/>

Virtual Network (仮想ネットワーク) の料金詳細

<http://azure.microsoft.com/ja-jp/pricing/details/virtual-network/>

◆ Azure Site Recovery サブスクリプション ライセンス

2014 年 8 月 1 日より、Microsoft Enterprise Agreement を通じて、Azure Site Recovery サ

ブスクリプション ライセンスの提供が開始されました。

Azure Site Recovery サブスクリプション ライセンスを購入すると、Azure Site Recovery のオンプレミスから Azure のサイト回復において、保護される仮想マシンごとに 1 か月あたり 100 GB までのレプリケーションとストレージの利用枠が提供されます。なお、1 か月の上限 100 GB を超えた利用分については、ストレージ、ストレージ トランザクション、データ転送の通常の課金レートに基づいて従量課金となります。

また、Azure Site Recovery サブスクリプション ライセンスには、InMage Scout ソフトウェアを使用して VMware および物理サーバーを保護する権利も含まれます。

Enterprise Agreement - マイクロソフト ボリューム ライセンス

<http://www.microsoft.com/ja-jp/licensing/licensing-options/enterprise.aspx>

1.4 オンプレミスから Azure のシステム要件

Azure Site Recovery は展開方法によって、システム要件が異なります。ここでは、オンプレミスから Azure のサイト回復を展開するためのオンプレミス側のシステム要件を示します。

◆ Virtual Machine Manager のバージョン

System Center 2012 R2 Virtual Machine Manager をサポートしています。なお、オンプレミスからオンプレミスのサイト回復については、System Center 2012 Service Pack (SP) 1 以降の Virtual Machine Manager でサポートされます。

◆ Hyper-V のバージョン

Windows Server 2012 R2 Hyper-V をサポートしています。Hyper-V ホストおよび Hyper-V ホスト クラスター（フェールオーバー クラスター構成の Hyper-V ホスト）上の仮想マシンを保護することができます。なお、オンプレミスからオンプレミスのサイト回復については要件が異なり、Windows Server 2012 Hyper-V および Windows Server 2012 R2 Hyper-V がサポートされます。

Note : Hyper-V ホスト クラスターの追加要件

Hyper-V ホスト クラスターが DHCP ではなく、静的な IP アドレスで構成されている場合、Azure Site Recovery による Hyper-V レプリカ ブローカーの自動構成が失敗します。その場合は、以下のサポート技術情報に従って、手動で対処してください。

2961977 - "Hyper-V Replica Cluster Broker is not installed" error when you replicate private clouds to Microsoft Azure

<http://support.microsoft.com/kb/2961977>

◆ 保護される仮想マシンでサポートされるゲスト OS

オンプレミスから Azure のサイト回復では、次のページの表に示す 64 ビット ゲスト OS を実行する Hyper-V 仮想マシンの保護がサポートされます。32 ビット OS はサポートされないことに注意してください。

ゲスト OS には最新の Hyper-V 統合サービスが組み込まれていることが推奨されます。これは、Azure Site Recovery の要件ではなく、Hyper-V 上で動かすための通常の条件です。

通常の Microsoft Azure 仮想マシン向けに提供されている Windows 用および Linux ゲスト用 VM エージェントは、保護対象の仮想マシンに組み込む必要はありません。ゲスト OS および仮想マシンの構成要件を満たしている仮想マシンであれば、Hyper-V 上で運用中の仮想マシンをそのまま保護対象にすることができます。

オペレーティング システム	備考
Windows Server 2012 R2	最新の Hyper-V 統合サービスをビルトイン
Windows Server 2012	Hyper-V 統合サービスのアップグレードが必要
Windows Server 2008 R2 SP1	Hyper-V 統合サービスのアップグレードが必要
Windows Server 2008 SP2 (x64)	Hyper-V 統合サービスのアップグレードが必要
CentOS	CentOS 5.9、6.4 以降、7.0 は Linux Integration Services for Hyper-V をビルトイン。Cent OS 5.8 以前、6.3 以前は、Linux Integration Services v3.5 for Hyper-V (http://www.microsoft.com/en-us/download/details.aspx?id=41554) をインストール
openSUSE	openSUSE 12.04 以降を推奨。Linux Integration Services for Hyper-V をビルトイン
SUSE Linux Enterprise Server (SLES)	SLES 11 SP2 以降を推奨。Linux Integration Services for Hyper-V をビルトイン
Ubuntu Server	Ubuntu 12.04 以降を推奨。Linux Integration Services for Hyper-V をビルトイン

Note : Windows Server 2012 R2 Hyper-V の Linux 対応

サポート対象に含まれない Linux ディストリビューションや FreeBSD については、動作保証外にはなりますが、Azure Site Recovery の仮想マシンの要件を満たす 64 ビットであれば保護することができます。主要な Linux ディストリビューションの最近のリリース、および FreeBSD 10.0 には、Hyper-V 統合サービスをビルトインされているため、Hyper-V 仮想マシンにインストールするだけで Hyper-V 環境に最適化されます。Linux および FreeBSD の Hyper-V 対応については、以下のドキュメントが参考になります。

Linux の仮想化には Hyper-V Server がお勧め! | TechNet

<http://technet.microsoft.com/ja-jp/windowsserver/dn575471.aspx>

FreeBSD and Microsoft Windows Server Hyper-V support

<https://wiki.freebsd.org/HyperV>

◆ 仮想マシンの構成要件

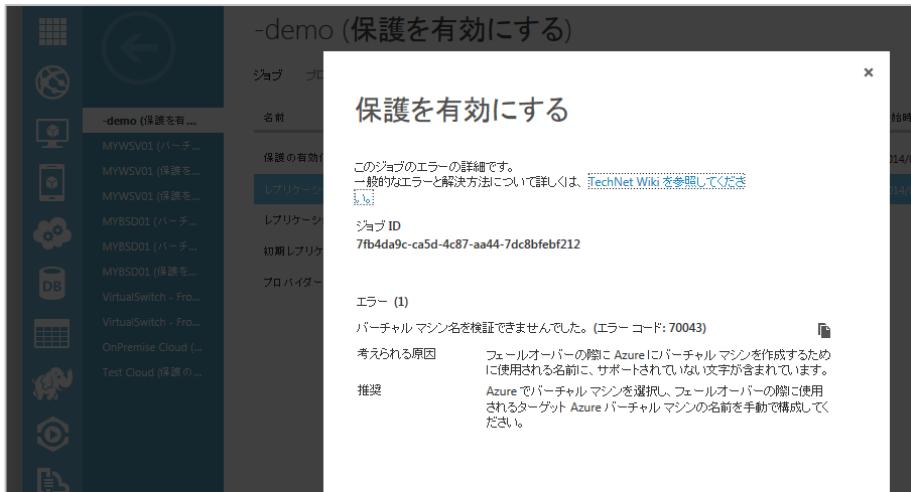
保護対象の仮想マシンは、次の構成要件を満たしている必要があります。

構成項目	構成要件
仮想マシンの世代	第 1 世代仮想マシン
OS ディスク	IDE コントローラー接続の仮想ハードディスク 割り当てサイズ 20 MB ~ 127 GB OS ディスクは最大 1 つまで
データ ディスク	IDE または SCSI コントローラー接続の仮想ハードディスク 割り当てサイズ 20 MB ~ 1,023 GB データ ディスクは最大 16 ディスクまで
仮想ハードディスクのファイル形式	VHD、VHDX
仮想ハードディスクの種類	容量固定、容量可変、差分
サポートされないディスク構成	物理ディスク (バススルーディスク)、iSCSI 接続のディスク、仮想ファイバー チャネル アダプター接続のディスク、仮想ハードディスクの共有はサポートされない
ネットワーク アダプター	1 つのネットワーク アダプターに 1 つの IP アドレスが、DHCP で動的に割り当てられていること。静的 IP アドレスはサポートされない ※複数のネットワーク アダプターがある場合、1 つのネットワーク アダプターが選択される
仮想マシン名	仮想マシン名は 1 ~ 63 文字である必要があります。 名前に使用できるのは、アルファベット、数字、およびハイフンのみです。名前の先頭および末尾にはアルファベットまたは数字を使用する必要があります

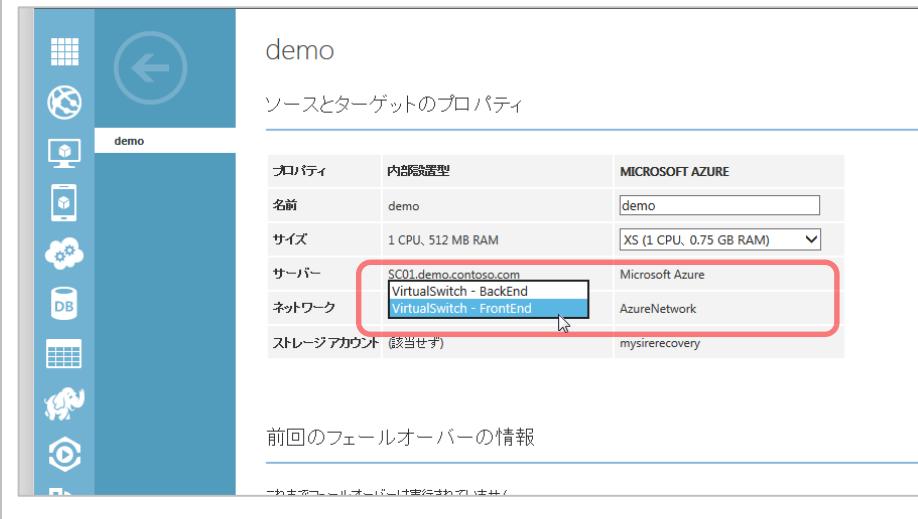
これらの要件は、Azure Site Recovery の将来の機能拡張で変更になる場合があります。

Note : サポートされない仮想マシン名や複数ネットワーク アダプターの使用

仮想マシン名にサポートされない文字のある場合でも、仮想マシンの保護の有効化とレプリケーションは可能です。ただしその場合は、Azure Site Recovery ポータルのフェールオーバー用の仮想マシンの構成（[ソースとターゲットのプロパティ] ページ）で、Microsoft Azure 仮想マシンの名前を手動で構成する必要があります。



仮想マシンに複数のネットワーク アダプターが存在する場合も、仮想マシンの保護の有効化とレプリケーションは可能です。その場合、Azure Site Recovery は 1 つのネットワーク アダプターを選択します。意図しないネットワーク アダプターが選択される場合があるので、Azure Site Recovery ポータルのフェールオーバー用の仮想マシンの構成を開いて自動選択の構成を確認し、必要に応じてネットワーク アダプターの選択を変更してください。



STEP 2. サービスの導入

この STEP では、小規模な Hyper-V サイト (VMM クラウド) の評価環境を想定し、Azure Site Recovery のオンプレミスから Azure のサイト回復の環境を構築する手順について説明します。

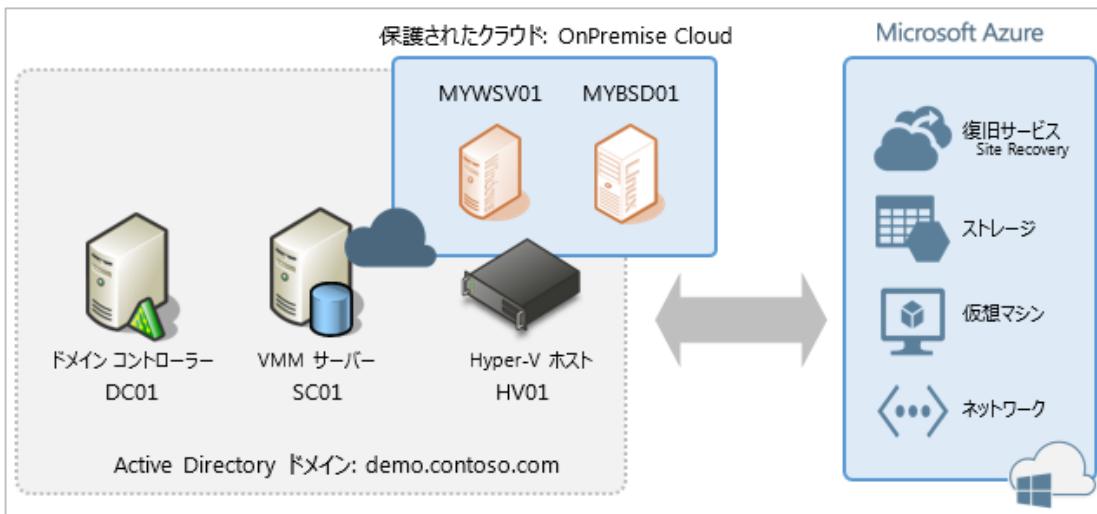
この STEP では、次のことを学習します。

- ✓ VMM のインストールと構成
- ✓ Azure 側のサービスの準備
- ✓ オンプレミス側コンポーネントの展開
- ✓ VMM クラウドの保護の構成
- ✓ 仮想マシンの保護の有効化
- ✓ レプリケーションの正常性の監視

2.1 評価環境のシステム構成

この評価ガイドでは、以下に示す小規模な環境を想定して、評価環境をセットアップします。オンプレミス側の 3 台のサーバー (DC01、SC01、HV01) は、すべて Windows Server 2012 R2 がインストールされ、ドメイン コントローラー DC01 で構成された Active Directory ドメインに、他の 2 台のサーバー SC01 および HV01 のドメイン メンバーとして、ドメイン参加設定は既に完了しているものとして説明します。また、Hyper-V ホストでは、既に Hyper-V の役割が有効になっており、Hyper-V ホストとしての構成 (外部ネットワーク接続用の仮想ネットワーク スイッチなど) が完了しているものとします。

なお、Microsoft Azure のサブスクリプションは既に利用可能になっているものとします。サブスクリプションをお持ちでない場合は、Microsoft Azure 1 か月無料評価版にサインアップして準備してください。



図：この評価ガイドで前提としている評価環境のシステム構成

Note : 無料で利用できるソフトウェアおよびサービスの評価版

Windows Server 2012 R2、System Center 2012 R2 Virtual Machine Manager、SQL Server 2012 の評価版は、この自習書の[最終ページのリンク先](#)から入手できます。

この自習書の以降で説明する Azure Site Recovery のすべての機能は、Microsoft Azure 1 か月無料評価版の使用権の範囲内で評価できます。無料評価版のサインアップすると、1 か月間無料で一定額の使用権を利用でき、その後、有料で使用継続を希望される場合は、サービスの構成を維持したまま従量課金制の Azure サブスクリプションに移行できます。Microsoft Azure 1 か月無料評価版のサインアップ方法については、次の項で説明します。

Microsoft Azure 1 か月無料評価版のサインアップ

<http://azure.microsoft.com/ja-jp/pricing/free-trial/>

2.2 Microsoft Azure サブスクリプションの準備

Azure Site Recovery のサービスを利用または評価するには、Microsoft Azure サブスクリプションをあらかじめ契約しておく必要があります。

既に有効な Microsoft アカウントおよび Microsoft Azure サブスクリプションをお持ちの場合は、この準備作業はスキップしてください。

Note : Microsoft Azure サブスクリプション作成時に必要なもの

Microsoft Azure サブスクリプションの申し込み時に、確認コードを音声または SMS で受け取るための携帯電話、および身元確認のためのクレジットカードが必要になります。

1. Microsoft アカウントの準備

以下の URL をブラウザで開き、新しく Microsoft アカウントを作成します。

Microsoft アカウント登録手続き

<http://www.microsoft.com/ja-jp/msaccount/signup/default.aspx>

2. Microsoft Azure サブスクリプションの申し込み

以下の URL で公開されている手順に従って、Microsoft Azure サブスクリプションを作成します。

Microsoft Azure サブスクリプション申し込み Step by Step

<http://msdn.microsoft.com/ja-jp/windowsazure/ee943806.aspx>

3. サブスクリプション作成後、Microsoft Azure 管理ポータルに接続し、手順 1 で作成した Microsoft アカウントを使用してサインインできれば完了です。

Microsoft Azure 管理ポータル

<https://manage.windowsazure.com/>

2.3 VMM のインストールと構成

Azure Site Recovery のオンプレミスから Azure のサイト回復のためには、System Center 2012 R2 Virtual Machine Manager による仮想化インフラストラクチャの管理環境が必要です。Virtual Machine Manager の管理環境を導入するには、次の手順で Virtual Machine Manager の管理サーバー（以下、VMM 管理サーバー）をインストールして構成します。

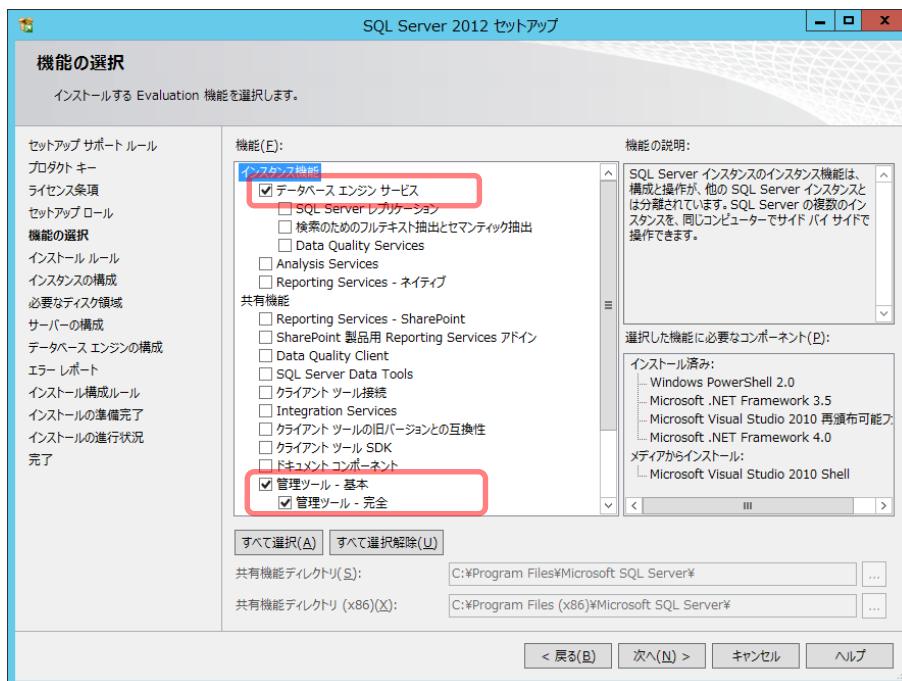
▼ SQL Server の準備

Virtual Machine Manager のデータベースをホストするために、ローカルまたはリモートの SQL Server インスタンスが必要です。Virtual Machine Manager のデータベースとしては、SQL Server 2008 R2 SP1/SP2、SQL Server 2012、SQL Server 2012 SP1 の使用が正式にサポートされています。SQL Server 2012 SP2 および SQL Server 2014 は、この評価ガイドの作成時点ではサポートされていません。最新情報については、以下の URL で確認してください。

SQL Server Requirements for System Center 2012 R2

<http://technet.microsoft.com/library/dn281933.aspx>

SQL Server のコンポーネントとしては、少なくとも [データベース エンジン サービス] および [管理ツール] をインストールしてください。



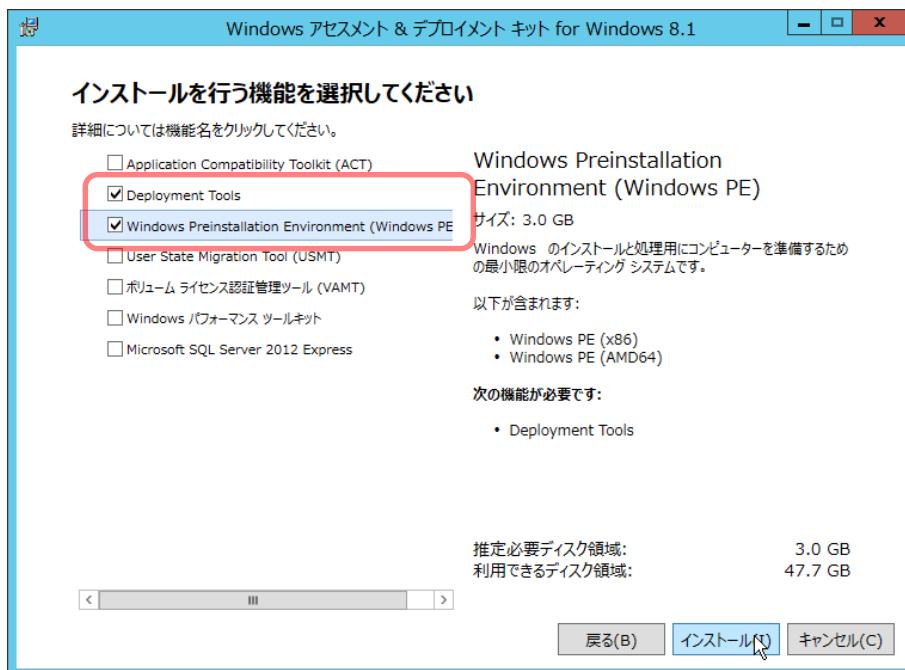
SQL Server のコンポーネントのいくつかは、.NET Framework 3.5 に依存します。Windows Server 2012 R2 は .NET Framework 3.5 をサポートしていますが、既定ではインストールされません。そのため、SQL Server のインストールを開始する前に、Windows Server 2012 R2 の [役割と機能の追加ウィザード] を使用して、機能の一覧から [.NET Framework 3.5 Features] から [.NET Framework 3.5 (.NET 2.0 および 3.0 を含む)] を選択してインストールしてください。

➔ VMM 管理サーバーの前提コンポーネントのインストール

Windows 展開ツールおよび Windows プ雷インストール環境は、VMM 管理サーバーの前提コンポーネントです。以下の Windows 8.1 Update 用の Windows アセスメント&デプロイメントキット (Windows ADK) をダウンロードして、[Deployment Tools] および [Windows Preinstallation Environment (Windows PE)] を選択してインストールしてください。

Windows 8.1 Update 用 Windows アセスメント & デプロイメント キット (Windows ADK)

<http://www.microsoft.com/ja-JP/download/details.aspx?id=39982>



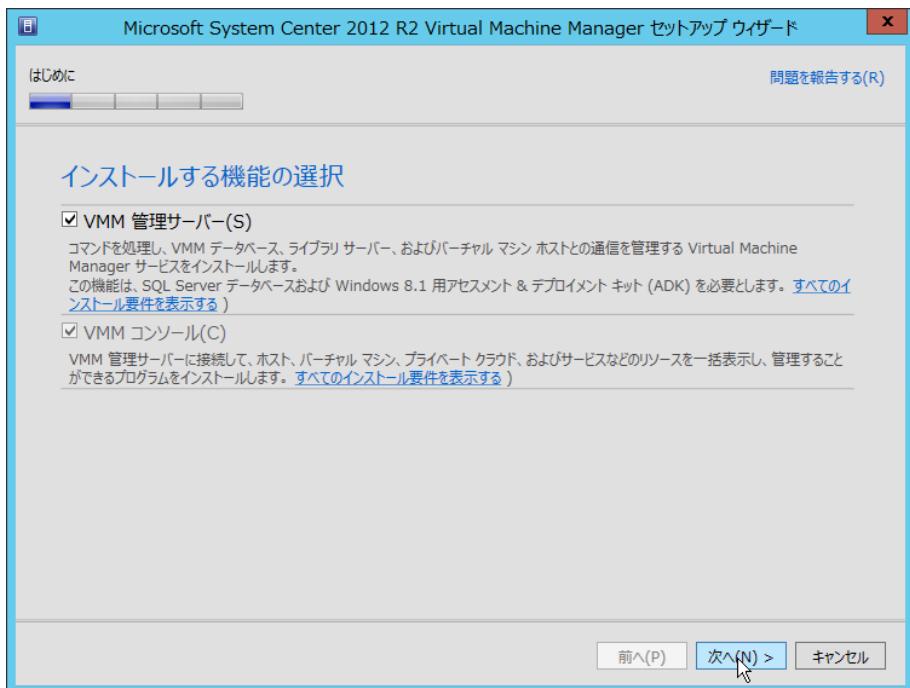
➔ VMM 管理サーバーのインストール

SQL Server と Windows ADK の準備ができたら、VMM 管理サーバーをセットアップします。

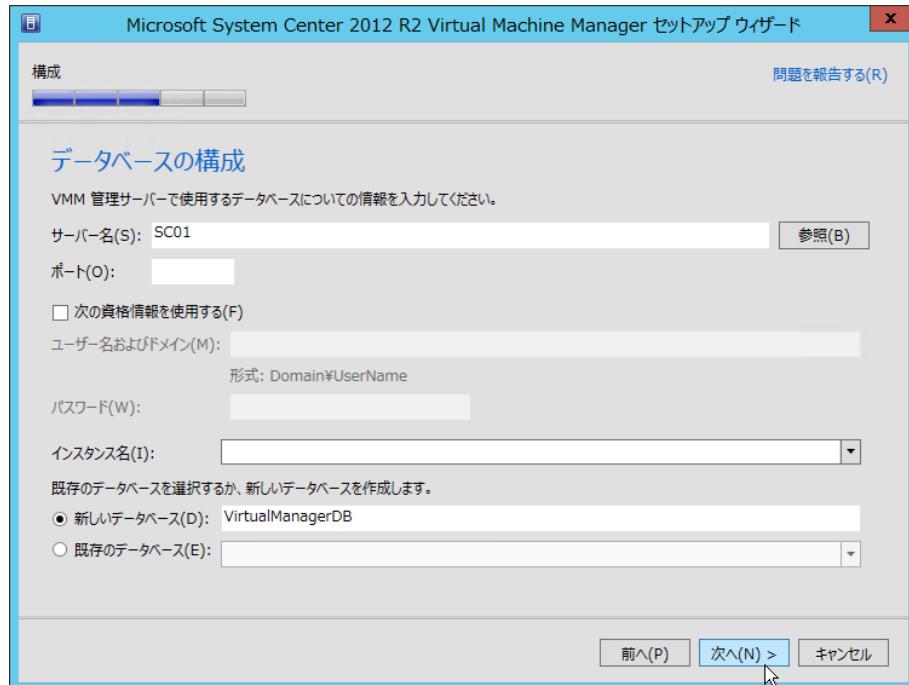
- Virtual Machine Manager のインストール メディアをドライブにセットするか、インストール メディアの ISO イメージをローカルにマウントして、セットアップ ウィザードを開始します。



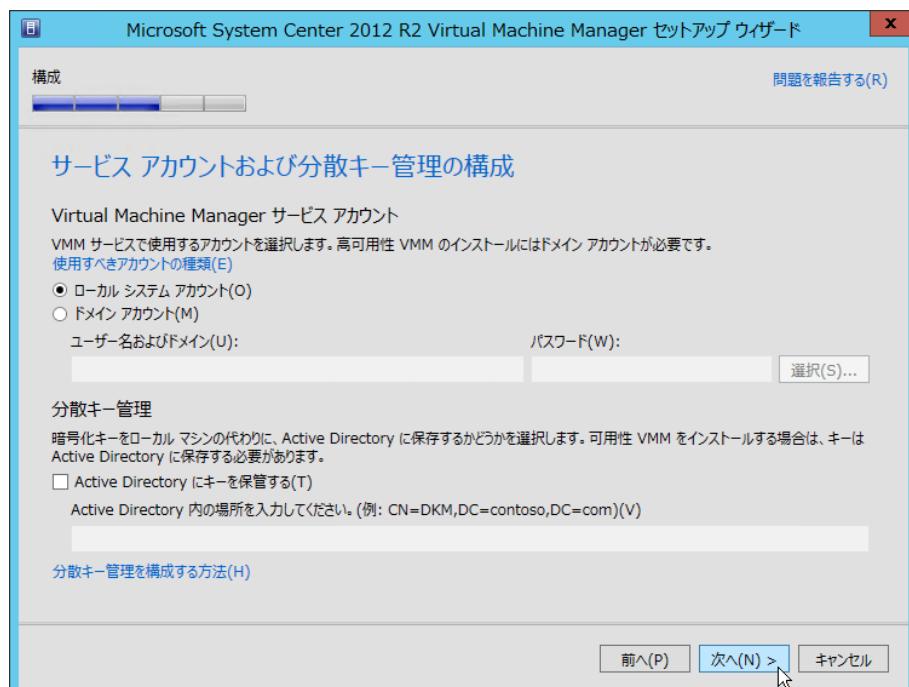
5. [インストールする機能の選択] のページで [VMM 管理サーバー] と [VMM コンソール] (選択解除不可) が選択されていることを確認し、[次へ] ボタンをクリックします。



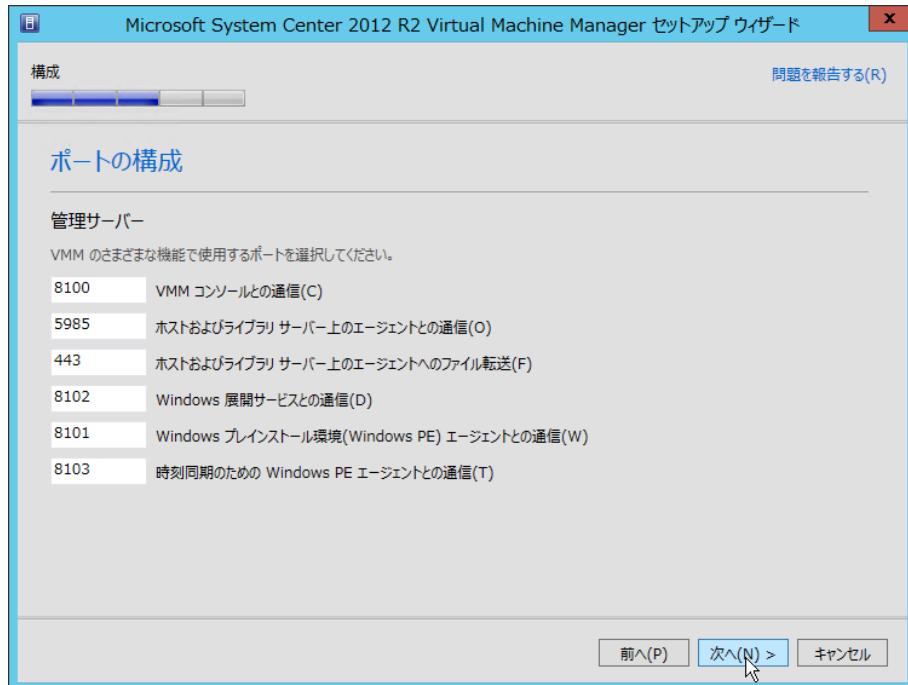
6. [製品の登録情報] のページで、[名前] [組織] [プロダクト キー (評価版の場合は不要)] を入力して、[次へ] ボタンをクリックします。
7. [この使用許諾契約書をお読みください] のページで、契約書の内容を確認し、[使用許諾契約書に同意します] をチェックして、[次へ] ボタンをクリックします。
8. [カスタマー エクスペリエンス向上プログラム (CEIP)] のページで、[はい] または [いいえ] を選択し、[次へ] ボタンをクリックします。カスタマー エクスペリエンス向上プログラムへの参加は任意です。
9. [インストール先] のページで、ソフトウェアのインストール先のパスを確認し、[次へ] ボタンをクリックします。既定のパスは、C:\Program Files\Microsoft System Center 2012 R2\Virtual Machine Manager です。特に理由が無ければ、既定のパスを受け入れてください。
10. [データベースの選択] のページで、VMM 管理サーバーが使用するデータベースの作成先を指定します。ローカルの SQL Server の既定のインスタンス (MSSQLServer) を使用する場合は、ローカルのサーバー名が指定されていることと、[新しいデータベース] が選択され、既定のデータベース名 VirtualManagerDB が指定されていることを確認して、[次へ] ボタンをクリックします。リモートの SQL Server インスタンスを使用する場合は、サーバー名、ポート番号 (通常は 1433)、資格情報、インスタンス名などを指定してください。



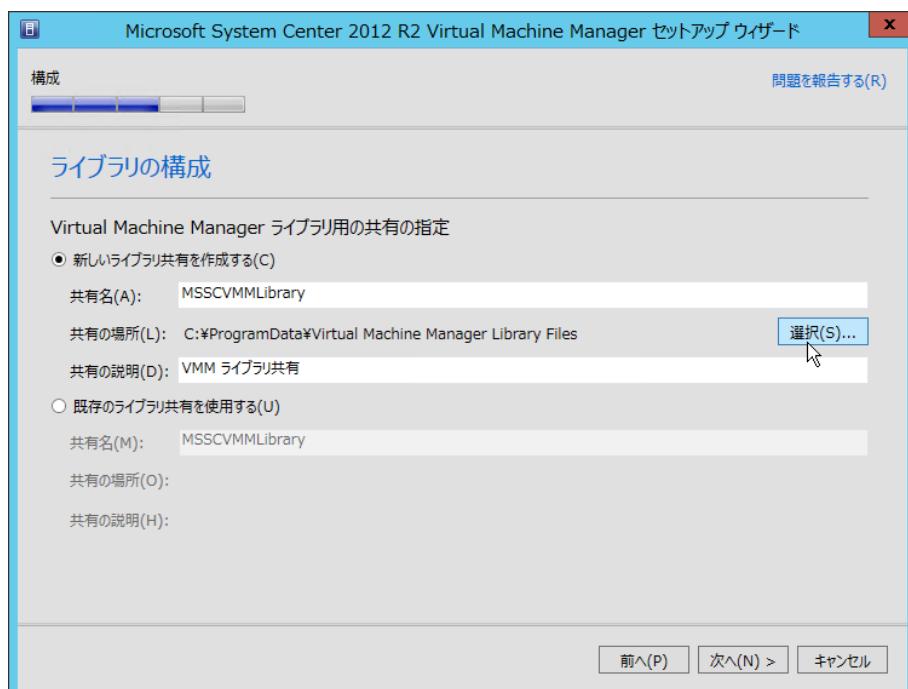
11. [サービス アカウントおよび分散キー管理の構成] のページでは、既定の設定（ローカル システム アカウントをサービス アカウントとして使用）のまま、[次へ] ボタンをクリックします。



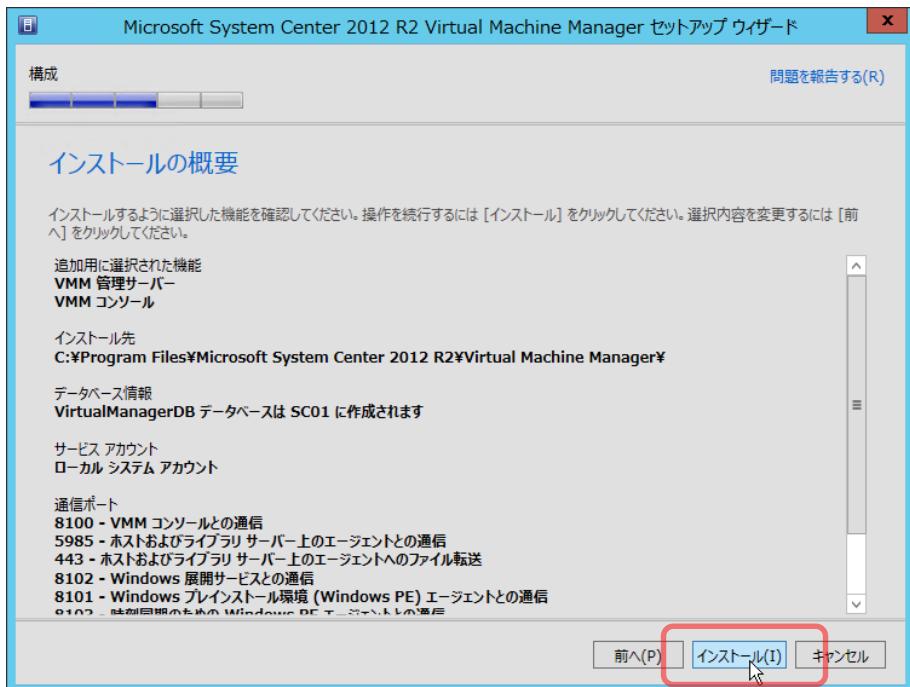
12. [ポートの構成] のページで、既定のポート番号を受け入れ、[次へ] ボタンをクリックします。既存の別のサービスとポート番号が重複する場合は、代替のポート番号をこのページで指定してください。



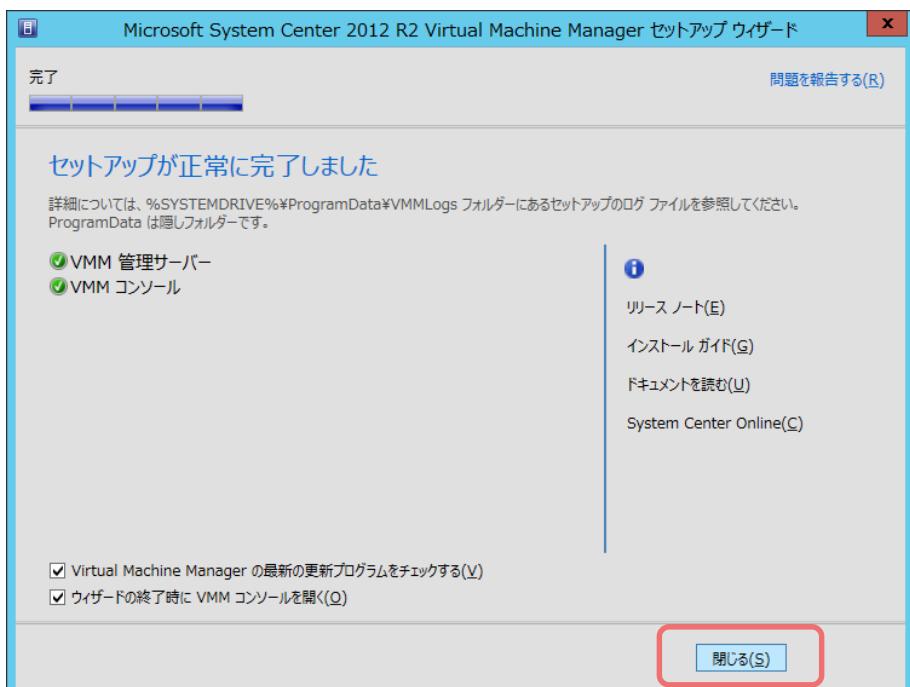
13. [ライブラリの構成] のページでは、VMM 管理サーバーに作成される VMM ライブラリ共有の設定を確認し、[次へ] ボタンをクリックします。既定では、C: ドライブ上の C:\ProgramData\Virtual Machine Manager Library Files が MSSCVMLibrary という名前で共有設定されます。VMM ライブラリは、仮想ハードディスクファイルの格納などで、多くのディスク領域を使用する可能性があるため、C: ドライブとは別のデータ用ボリュームに変更することをお勧めします。



14. [インストールの概要] のページで [インストール] ボタンをクリックして、インストールを開始します。



15. [セットアップが正常に完了しました] と表示されたら、[閉じる] ボタンをクリックしてください。セットアップ ウィザードを終了すると、VMM コンソールが開きます。



16. VMM 管理サーバーとコンソールのインストールが完了したら、できるだけはやく、Windows Update を実行し、Microsoft Update から Virtual Machine Manager や SQL Server の更新プログラムをインストールしてください。この評価ガイドの作成時点では、累積的な更新プログラムとして 2014 年 7 月に公開された System Center 2012 R2 の更新ロールアップ 3 (Update Rollup 3) に更新可能です。なお、SQL Server 2012 を使用している場合は、SQL Server 2012 SP2 が現状で Virtual Machine Manager で正式にサポートされていないことに留意してください。

Note : System Center 2012 R2 用の更新ロールアップ 3 について

System Center 2012 R2 用の更新ロールアップ 3 の詳しい内容、更新後に必要な追加手順については、以下のサポート技術情報で確認してください。

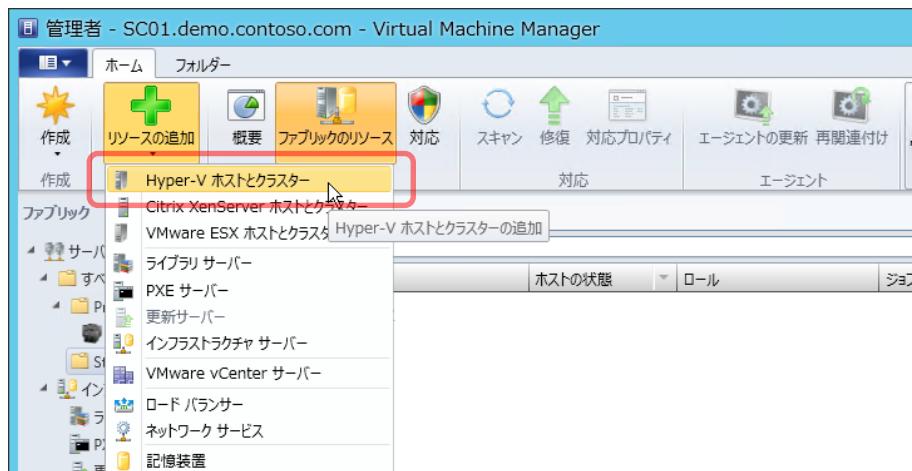
Update Rollup 3 for System Center 2012 R2

<http://support.microsoft.com/kb/2965090>

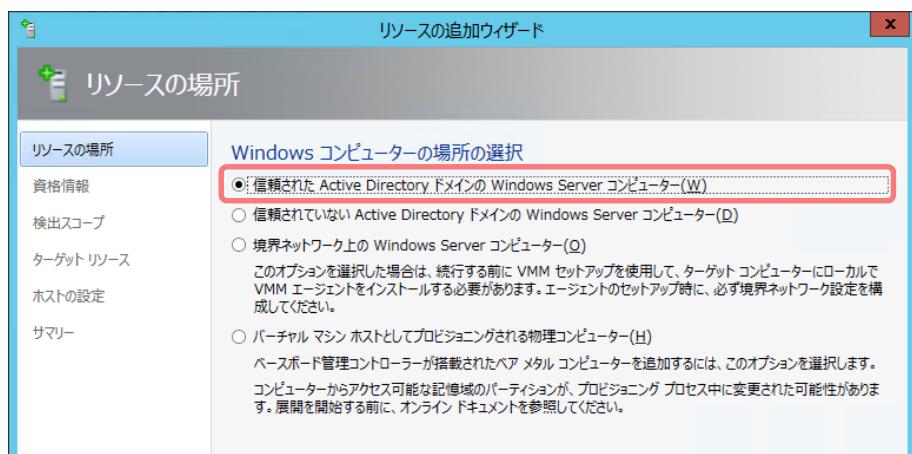
→ Hyper-V ホストの追加

Virtual Machine Manager は、ファブリックという概念で仮想化インフラストラクチャのサーバー、ネットワーク、および記憶域を管理します。既存の Hyper-V の仮想環境を Virtual Machine Manager の管理下にするには、次の手順で Hyper-V ホストをサーバー ファブリックのホストグループに追加します。

1. VMM コンソールで [ファブリック] ページを開き、[ホーム] タブの [リソースの追加] をクリックして、[Hyper-V ホストとクラスター] を選択します。

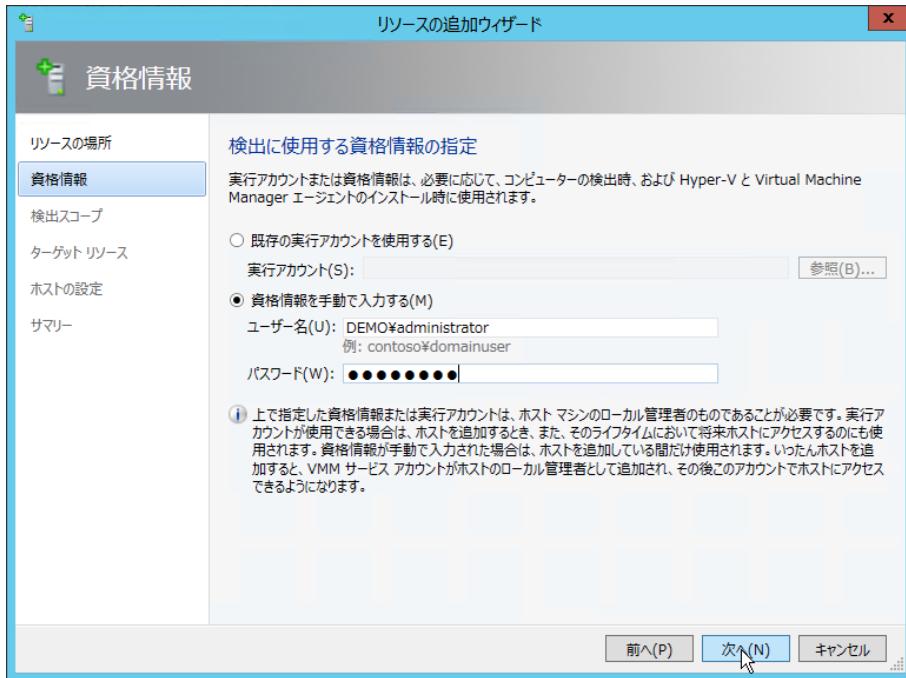


2. [リソースの追加ウィザード] が開始します。最初の [リソースの場所] のページで、[信頼された Active Directory ドメインの Windows コンピューター] を選択し、[次へ] ボタンをクリックします。

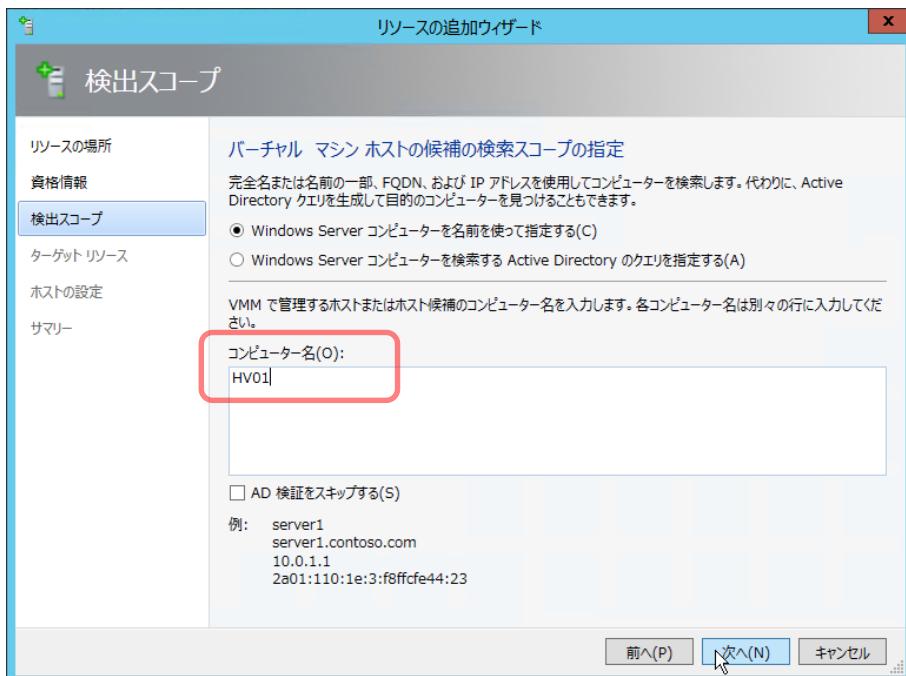


3. [資格情報] のページでは、[資格情報を手動で入力する] を選択し、ドメイン管理者（ドメイ

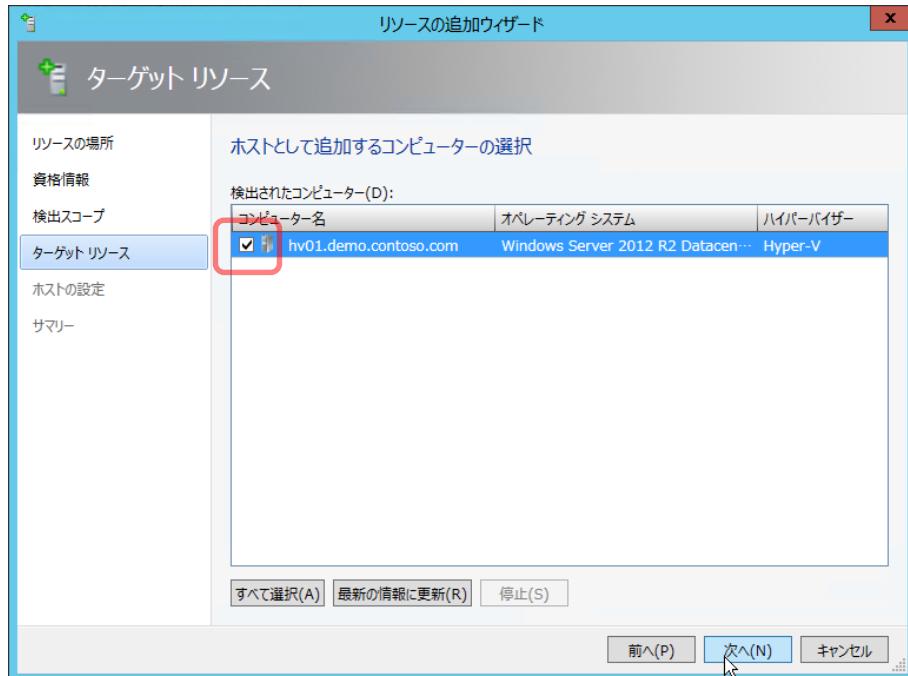
（管理者名￥Administrator）または同等の権限のあるドメイン アカウントの資格情報を入力します。



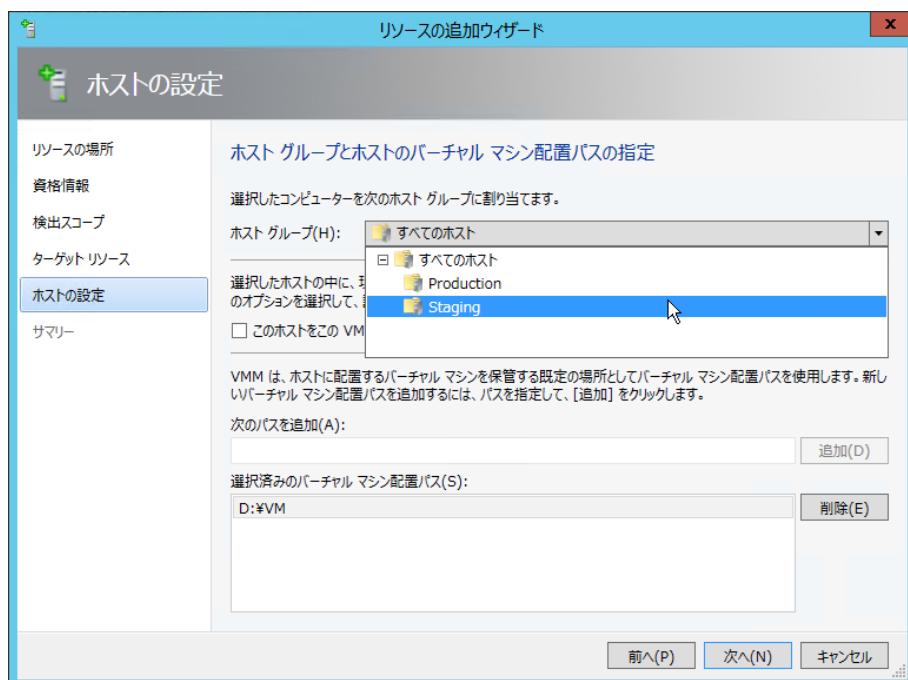
4. [検出スコープ] のページで、[Windows Server コンピューターを名前を使って指定する] を選択し、Hyper-V ホストのコンピューター名を入力します。複数の Hyper-V ホストを同時に追加したい場合は、改行して 2 台目以降のコンピューター名を入力してください。Hyper-V ホスト クラスターを追加する場合は、クラスター名を入力します。



5. [ターゲット リソース] のページに、検出されたコンピューター名が一覧されます。一覧から追加対象の Hyper-V ホストをすべてチェックし、[次へ] ボタンをクリックします。



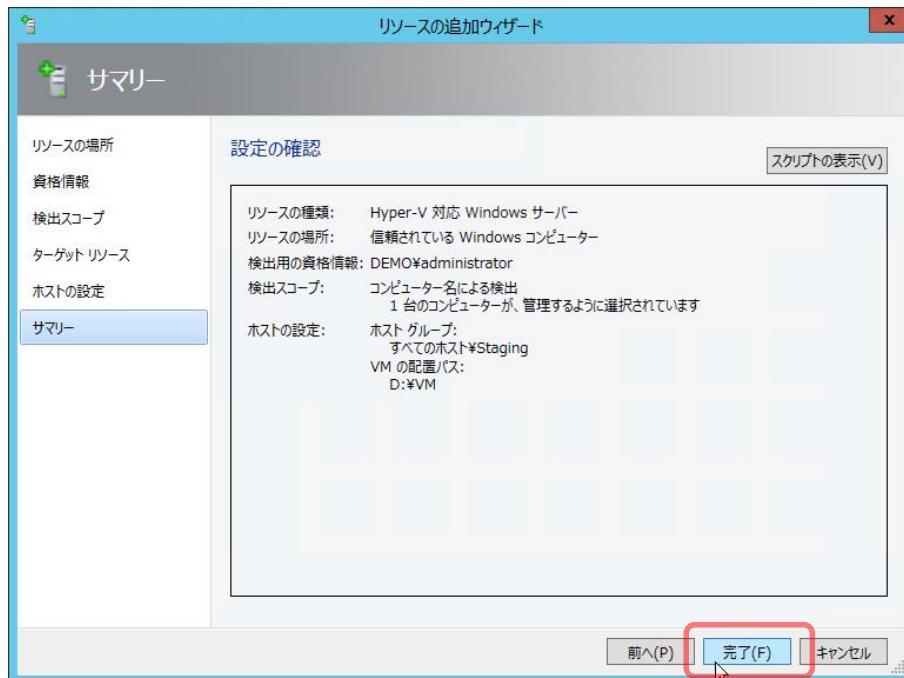
6. [ホストの設定] のページで、Hyper-V ホストを追加するホスト グループと、仮想マシンの既定の保存先にするローカル パスを指定して、[次へ] ボタンをクリックします。



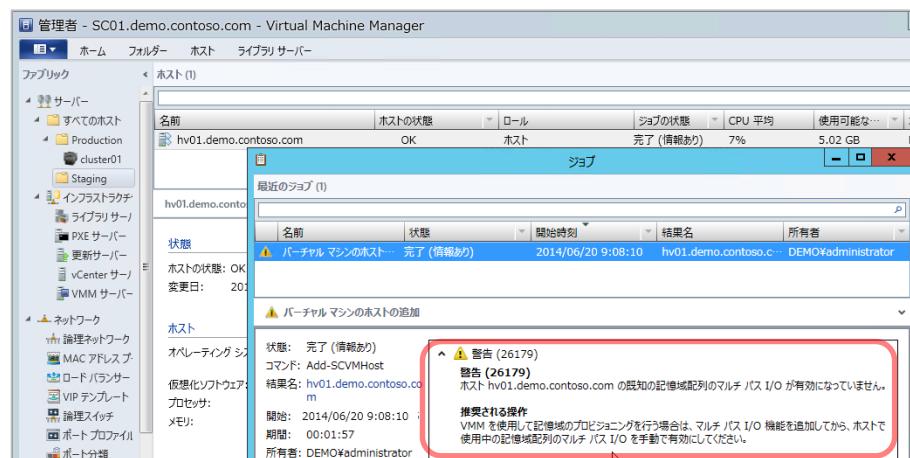
Note : ホスト グループを使用して評価対象 Hyper-V ホストを限定する

VMM 管理サーバーをインストールした直後は、ホスト グループとして「すべてのホスト」が 1 つ作成されます。複数の Hyper-V ホストが存在し、Azure Site Recovery の評価を特定の Hyper-V ホストで行いたい場合は、事前に専用のホスト グループを作成して、Hyper-V ホストをそのホスト グループに割り当ててください。なお、ホスト グループの割り当ては、後で変更できます。

7. [サマリー] のページで [完了] ボタンをクリックし、Hyper-V ホストの追加を開始します。



8. Hyper-V ホストの追加を開始すると、[バーチャル マシンのホストの追加] ジョブが作成され、対象の Hyper-V ホストに VMM エージェントや仮想スイッチ拡張機能のコンポーネントが展開され、[サーバー] ファブリックに追加されます。このとき、対象のサーバーに Hyper-V の役割がインストールされていない場合は、自動的に有効化されます。ジョブの実行が完了したら、ホストの状態やジョブの履歴を確認し、正常に追加されたことを確認してください。ジョブが失敗した場合や、追加の手順が必要な場合は、ジョブの履歴で確認できます。



9. Hyper-V ホストを追加したら、[ネットワーク] ファブリックの [論理ネットワーク] を開き、仮想マシンを接続するための論理ネットワークが作成されていることを確認します。追加した Hyper-V ホストに仮想ネットワーク スイッチが作成済みであれば、同じ名前の論理ネットワークが自動作成されているはずです。



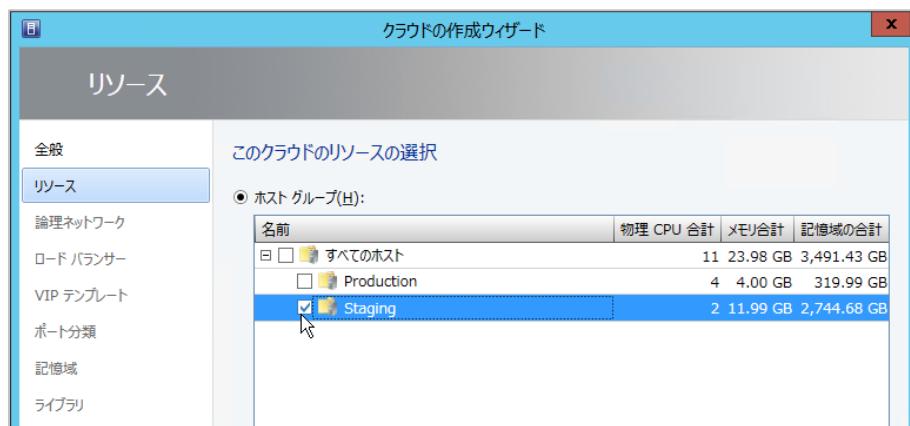
◆ VMM クラウドの作成

Azure Site Recovery は、VMM 管理サーバーで管理されるプライベート クラウド (VMM クラウド) 単位でレプリケーションを構成します。VMM クラウドは次の手順で作成します。

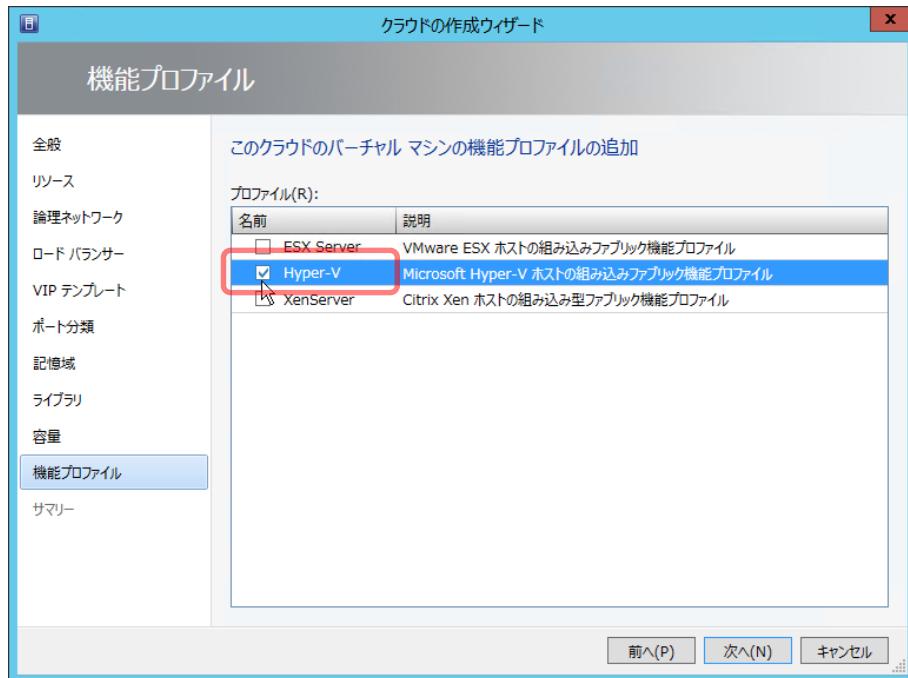
1. VMM 管理コンソールで [VM とサービス] ページを開き、[ホーム] タブの [クラウドの作成] をクリックして、[クラウドの作成ウィザード] を開始します。最初の [全般] ページでは、VMM クラウドの名前を指定します。



2. [リソース] ページで [ホスト グループ] を選択し、VMM クラウドに関連付けるホスト グループを指定します。オンプレミスに複数の Hyper-V ホストがあり、Azure Site Recovery を特定の Hyper-V ホストだけで評価したい場合は、評価に使用する Hyper-V ホストだけを含むホスト グループを作成して VMM クラウドに関連付けるようにしてください。



3. [論理ネットワーク] のページでは、この VMM クラウドで使用する論理ネットワークを選択します。この後の [ロード バランサー] から [容量] までのページは、Azure Site Recovery 用に特別に必要な構成はありません。必要に応じて構成してください。
4. [機能プロファイル] のページでは、[Hyper-V] をチェックします。この設定は、Azure Site Recovery でクラウドの保護を有効化するために、必須の設定になります。



5. [サマリー] ページで [完了] ボタンをクリックし、VMM クラウドを作成します。

Note : 運用中の VMM クラウドを使用する場合

運用中の既存の VMM クラウドを使用する場合は、対象の VMM クラウドのプロパティを開いて、機能プロファイルとして [Hyper-V] がチェックされていることを確認してください。

2.4 保護される仮想マシンの準備

Azure Site Recovery で [サポートされるゲスト OS](#) および [仮想マシンの構成要件](#)を満たしていれば、既に Hyper-V 上で稼働している Windows Server および Linux 仮想マシンを Azure Site Recovery で保護することができます。Azure Site Recovery に対応させるために追加のコンポーネントが必要になることはありません。

保護対象の仮想マシンは、VMM クラウドに関連付けられている必要があります。VMM コンソールから仮想マシンを作成する場合、仮想マシンを Hyper-V ホスト（ホスト グループ）ではなく、VMM クラウドに展開することができます。Hyper-V ホストに対して作成した仮想マシンや、Hyper-V マネージャーで作成した既存の仮想マシンは、VMM コンソールで仮想マシンのプロパティを開いて、特定の VMM クラウドに関連付けることができます。

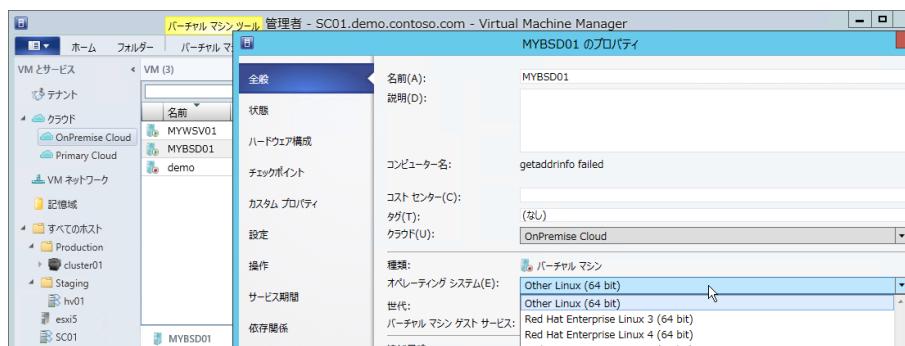
→ 仮想マシンに必須のプロパティ設定

Azure Site Recovery で仮想マシンを保護するためには、仮想マシンの次のプロパティが適切に設定されている必要があります。これらのプロパティに 1 つでも不適切な設定があると、仮想マシンの保護を有効化できません。

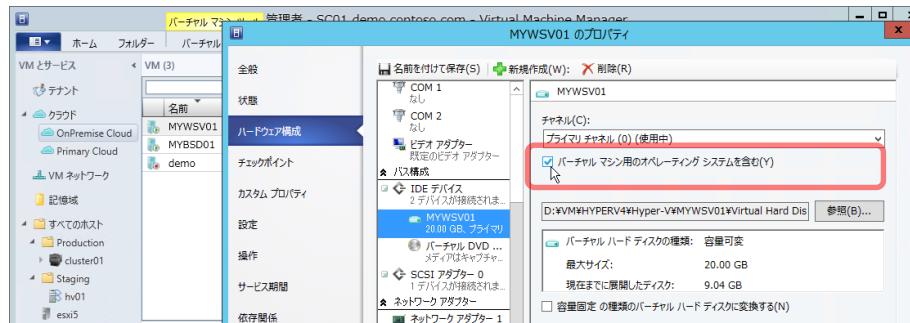
1. VMM コンソールで対象の仮想マシンのプロパティを開き、[全般] ページで仮想マシンが VMM クラウドに関連付けられること、およびオペレーティング システムとしてサポート対象の Windows Server バージョンまたは Linux ディストリビューションが指定されていることを確認してください。



Linux 仮想マシンの場合で、該当するディストリビューションやバージョンが一覧に無い場合は、[Other Linux (64-bit)] を選択します。例えば、FreeBSD 10.0 は Linux ではありませんが、[Other Linux (64-bit)] を指定することで、Azure Site Recovery で保護できます。

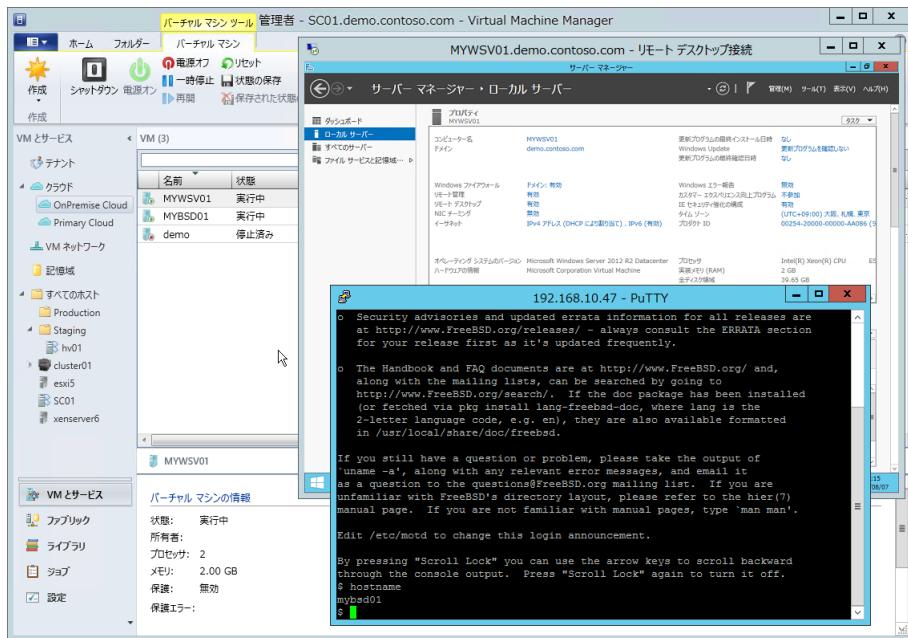


2. [ハードウェア構成] ページで [IDE デバイス] の項目を開き、ゲスト OS 用の仮想ハードディスクの [バーチャル マシン用のオペレーティング システムを含む] オプションがチェックされていることを確認します。同じ仮想マシンの 2 つ以上のディスクでこのオプションがチェックされていないようにしてください。



→ リモート操作のための RDP または SSH の有効化

オンプレミスの Hyper-V 環境とは異なり、Microsoft Azure 仮想マシンはゲスト OS のローカル コンソールへの接続手段を提供しません。フェールオーバー後の仮想マシンをリモート操作できるように、Windows Server 仮想マシンの場合はリモート デスクトップ接続を、Linux 仮想マシンの場合は SSH を有効化し、接続できることを確認しておくことをお勧めします。ローカルのファイアウォールで RDP ポート 3389/TCP や SSH ポート 22/TCP の受信を許可しておくことも忘れないでください。



2.5 Microsoft Azure 側の準備

Azure Site Recovery のサービスの利用を開始するには、Microsoft Azure 管理ポータルにサインインして、Azure Site Recovery 資格情報コンテナーを作成し、Azure Site Recovery で使用する他の関連サービスの準備をします。

Microsoft Azure 管理ポータル

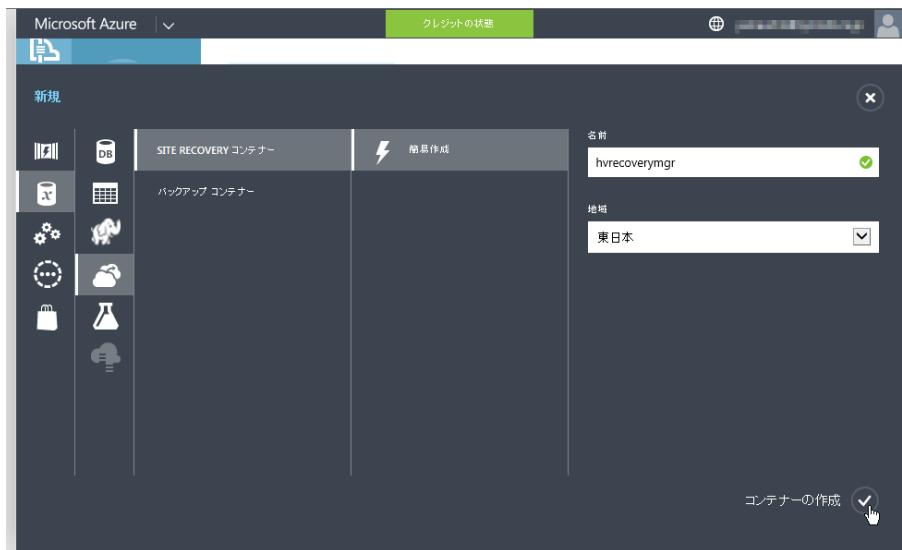
<https://manage.windowsazure.com/>

Microsoft Azure では現在、新しいポータル (<https://portal.azure.com/>) がプレビュー提供されていますが、この評価ガイドではすべてのサービスを構成可能な従来のポータルで説明します。

◆ Azure Site Recovery 資格情報コンテナーの作成

Azure Site Recovery 資格情報コンテナーを作成するには、次の手順で操作します。

1. Microsoft Azure 管理ポータルを Web ブラウザーで開き、Microsoft Azure サブスクリプションに Microsoft アカウントの資格情報を入力してサインインします。
2. ポータルの左下にある [+新規] をクリックし、[データ サービス] [復旧] [SITE RECOVERY コンテナー] [簡易作成] の順番にポイントして、Azure Site Recovery 資格情報コンテナーの名前を入力し、使用するリージョン (データセンターのある地域) をサービス提供中のリージョンの一覧から選択して、[コンテナーの作成] をクリックします。Microsoft Azure の日本国内のデータセンターを使用する場合は、[東日本] または [西日本] リージョンを選択してください。なお、この評価ガイドでは、[東アジア] リージョンでセットアップしています。



3. Azure Site Recovery 資格情報コンテナーの作成が完了すると、[復旧サービス] のページの中に作成されたコンテナーが表示されます。このコンテナーは、VMM 管理サーバーや VMM クラウドのメタデータ (構成データ) を保存し、レプリケーションの構成やフェールオーバータスクを実行するために使用します。

4. Azure Site Recovery 資格情報コンテナーの名前部分 (または アイコン)をクリックすると、Azure Site Recovery を管理するためのワークスペース (以下、Azure Site Recovery ポータル) が開きます。Azure Site Recovery ポータルを初めて開いたときは、[クイック スタート] ページが開きます。[クイック スタート] ページの [回復のセットアップ] で [内部設置型 Hyper-V サイトと Microsoft Azure の間] を選択してください。すると、オンプレミスから Azure のサイト回復の利用に必要な、以降の手順が示されます。

なお、[クイック スタート] ページをスキップするように構成した場合、[ダッシュボード] ページが開くようになりますが、その場合でもページ上部のメニューの左端のアイコン ([ダッシュボード] の左の アイコン) をクリックすることで、[クイック スタート] ページにアクセスできます。

5. 最初の手順は登録キー ファイルの生成とダウンロードです。登録キー ファイルは、後述する Azure Site Recovery プロバイダーをインストールする際に、この Azure Site Recovery 資格情報コンテナーを識別するために必要になります。[クイック スタート] ページの [1 VMM サーバーの準備] にある [登録キー ファイルの生成] リンクをクリックすることで、登録キー

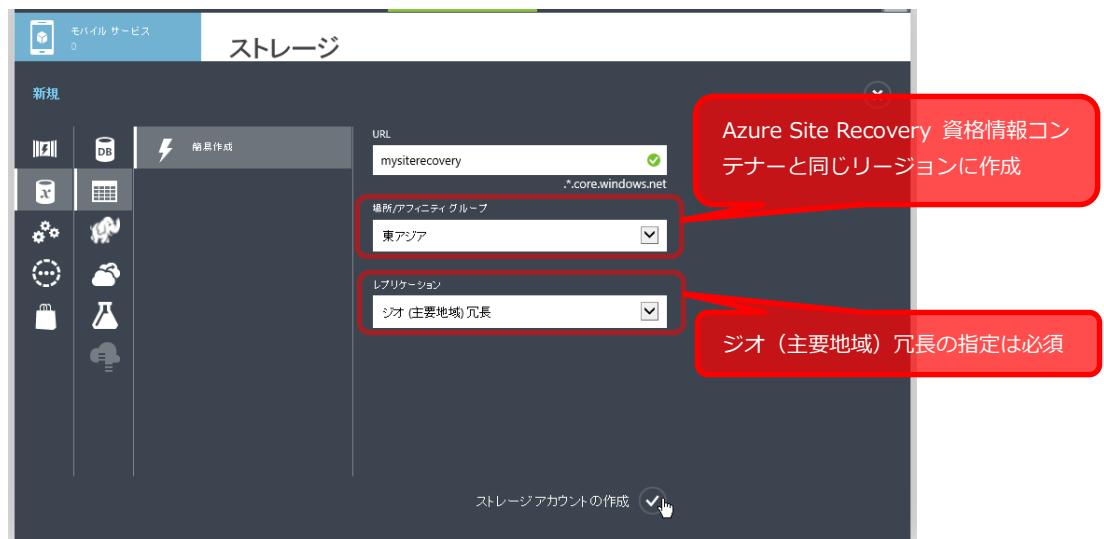
ファイルの生成とダウンロードが可能です。登録キー ファイルは、「コンテナー名_日付.VaultCredentials」というファイル名になります。



◆ Azure ストレージ アカウントの作成

Azure Site Recovery は、レプリケーション データを保存するために Microsoft Azure ストレージを利用します。そのため、次の手順で Azure Site Recovery 用のストレージ アカウントを事前に準備しておきます。Azure Site Recovery のためには、Azure Site Recovery 資格情報コンテナーと同じリージョンに関連付けられた、ジオ冗長（同一地域内の二次拠点とのレプリケーション）が有効なストレージ アカウントを準備しておく必要があります。

1. Microsoft Azure 管理ポータルの左下にある [+ 新規] をクリックし、[データ サービス] [ストレージ] [簡易作成] の順番にポイントします。
2. ストレージ アカウントの URL を決定し、[場所/アフィニティ グループ] で Azure Site Recovery 資格情報コンテナーと同じリージョンを選択して、[レプリケーション] で [ジオ (主要地域) 冗長] を選択したら、[ストレージ アカウントの作成] をクリックします。



3. ジオ (主要地域) 冗長のストレージ アカウントが作成されると、Azure にセカンダリ リージ

ヨン（二次拠点）が自動的に割り当てられます。セカンダリ リージョンは、ストレージ アカウントの【構成】ページで確認することができますが、変更はできません。東日本に作成した場合は西日本、西日本に作成した場合は東日本がセカンダリ リージョンとして割り当てられるはずです。

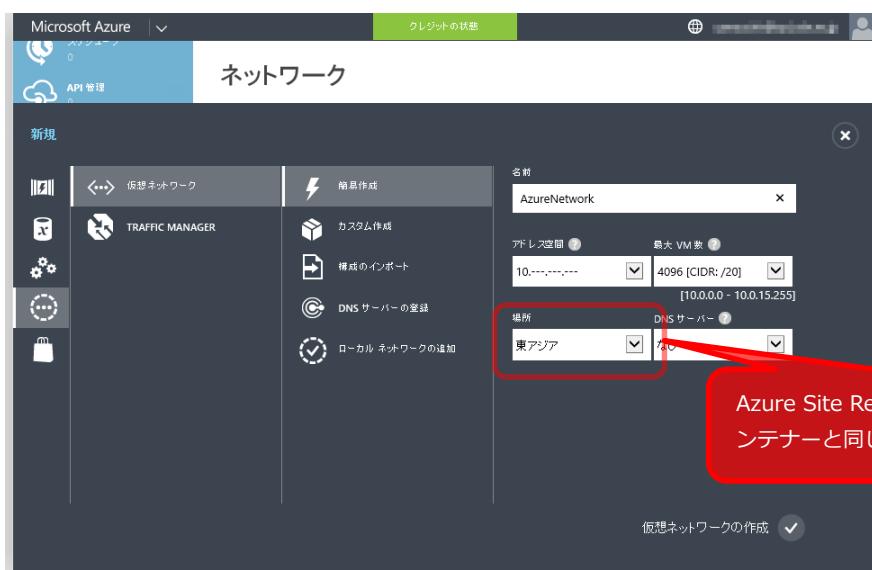
◆ Azure 仮想ネットワークの作成

Azure Site Recovery は、Microsoft Azure 仮想マシンのサービスを利用して仮想マシンをフェールオーバーし、Microsoft Azure 仮想ネットワークに仮想マシンを接続します。Azure Site Recovery のためには、Azure Site Recovery 資格情報コンテナーと同じリージョンに関連付けられた仮想ネットワークを準備しておく必要があります。

この評価ガイドでは、Microsoft Azure 仮想ネットワークのセットアップ手順や、オンプレミスとの VPN 接続の構成や手順については説明しません。サイト間 VPN 接続の環境を準備できない場合は、オンプレミスと接続されていないダミーの閉じた仮想ネットワークを作成することで、ネットワークの接続性を除く、Azure Site Recovery の評価を行うことが可能です。レプリケーションやパブリック仮想 IP (VIP) によるエンドポイントへの接続は、サイト間 VPN 接続を必要としません。

通常は【カスタム作成】を選択して、IP サブネットの構成や DNS サーバーの指定、ゲートウェイの作成と接続などを行い、オンプレミスとのサイト間 VPN 接続をセットアップします。ダミーの仮想ネットワークを利用する場合は、次の手順で簡単に作成できます。

1. Microsoft Azure 管理ポータルの左下にある【+新規】をクリックし、【ネットワーク サービス】【仮想ネットワーク】【簡易作成】の順番にポイントします。
2. 仮想ネットワークの名前を決定し、【場所】として Azure Site Recovery 資格情報コンテナーと同じリージョンを選択します。その他の項目は適当に指定します。



3. 【仮想ネットワークの作成】をクリックして、仮想ネットワークを作成します。

Note : Microsoft Azure 仮想ネットワークに関する技術情報

運用環境において、Azure Site Recovery を使用して Microsoft Azure 側にフェールオーバーしたあと、オンプレミスの社内ネットワークから Azure 側の仮想マシンにシームレスにアクセスできるようにするには、オンプレミスの企業ネットワークを、VPN ゲートウェイ装置や Windows Server の RRAS (ルーティングとリモート アクセスサービス) を使用して、インターネットを介して Microsoft Azure 仮想ネットワークのゲートウェイとサイト間 VPN で相互接続しておく必要があります。Microsoft Azure 仮想ネットワークの機能詳細とセットアップ手順については、以下のドキュメントを参照してください。

Microsoft Azure 仮想ネットワークのドキュメント ページ

<http://azure.microsoft.com/ja-jp/documentation/services/virtual-network/>

Microsoft Azure ネットワーク サービスに関する MSDN ドキュメント

<http://msdn.microsoft.com/ja-jp/library/azure/gg433091.aspx>

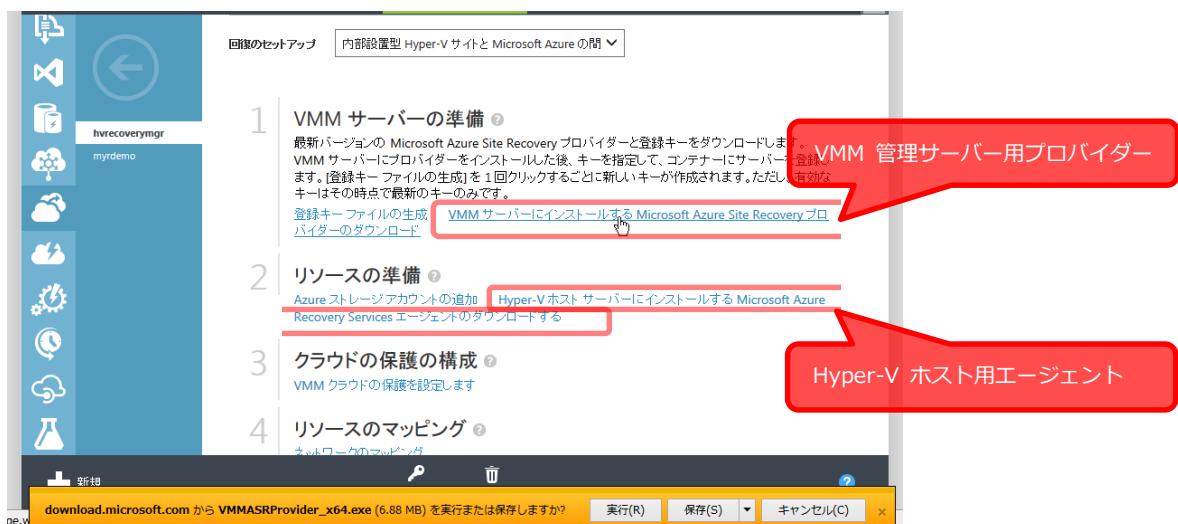
Microsoft Azure のネットワーク セキュリティの内部

http://blogs.msdn.com/cfs-file.ashx/_key/communityserver-blogs-components-weblogfiles/00-00-01-51-80-document/7115.Windows-Azure-Network-Security-Whitepaper_-2D00_-FINAL_5F00_j.docx

2.6 Azure Site Recovery のオンプレミス側コンポーネントの展開

Azure Site Recovery を利用するためには、オンプレミス側に Azure Site Recovery のコンポーネントを展開する必要があります。Azure Site Recovery プロバイダーは、VMM 管理サーバーにインストールするコンポーネントで、Azure Site Recovery の展開方法に関係なく必要です。Azure Recovery Services エージェントは、オンプレミスから Azure のサイト回復でのみ必要なコンポーネントであり、保護される仮想マシンが配置されている Hyper-V ホストにインストールします。

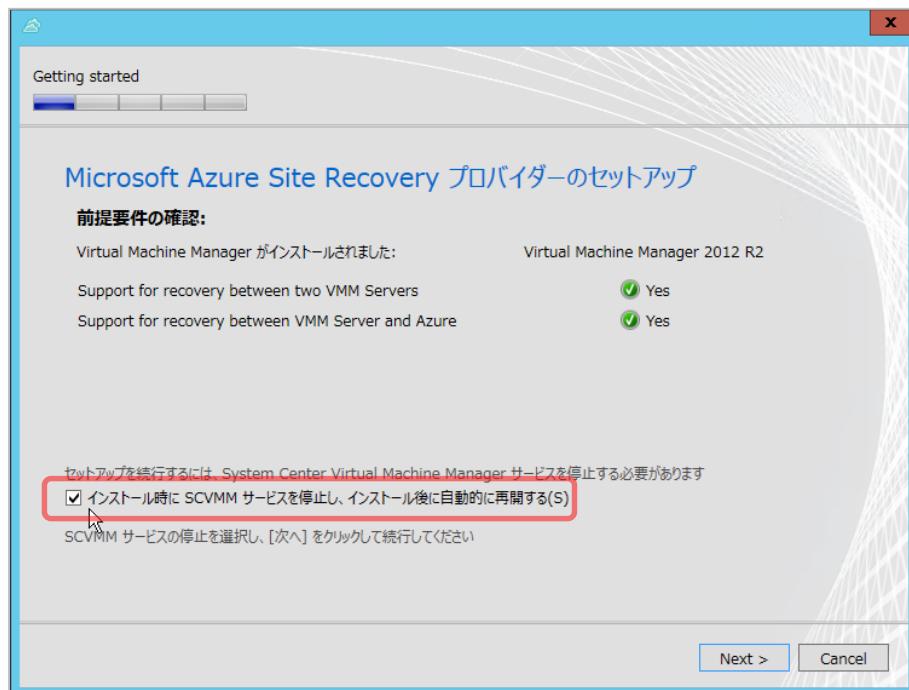
Azure Site Recovery のオンプレミス側コンポーネントのインストーラーは、Azure Site Recovery ポータルの [クイック スタート] または [ダッシュボード] ページからダウンロードできます。



→ VMM 管理サーバーへのプロバイダーのインストール

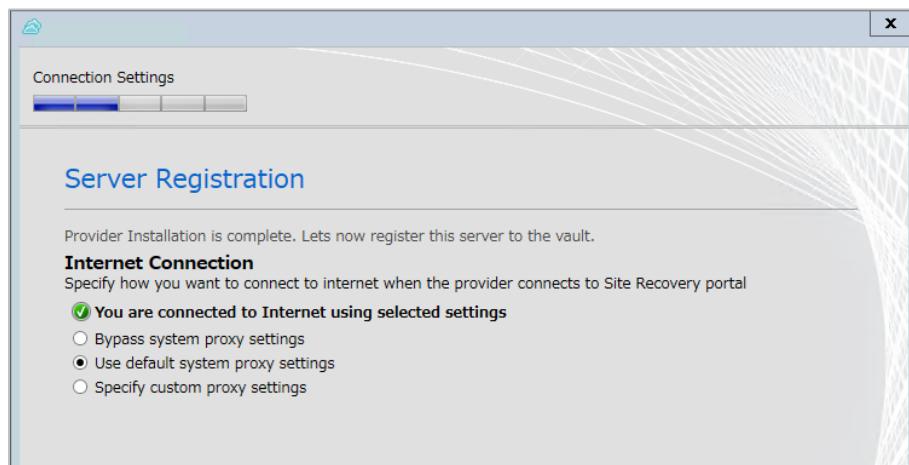
次の手順に従って、VMM 管理サーバーに Azure Site Recovery プロバイダーをインストールします。なお、この手順は、2014 年 9 月時点の Azure Site Recovery プロバイダー バージョン 3.5.468.0 に基づいています。より新しいバージョンでは、UI や手順が変更になる場合があります。

1. Azure Site Recovery ポータルから Azure Site Recovery プロバイダーのインストーラー (VMMASRProvider_x64.exe) を VMM 管理サーバーにダウンロードします。
2. Azure Site Recovery プロバイダーのインストーラー (VMMASRProvider_x64.exe) をダブルクリックし、セットアップ ウィザードを開始します。セットアップ ウィザードが開始したら、最初のページで [インストール時に SCVMM サービスを停止し、インストール後に自動的に再開する] をチェックし、[Next >] ボタンをクリックしてプロバイダーをインストールします。



3. [Server Registration] のページが表示されます。プロバイダーをアップグレードする場合、このページは表示されずにインストールが完了します。その場合は、スタート画面のアプリの一覧から [Azure Site Recovery Configurator] をクリックしてウィザードを開始してください。

最初の [Internet Connection] のページでは、インターネット接続のためにプロキシ サーバーを経由する必要がある場合に、環境にあわせてプロキシ サーバーの設定を行います。プロキシ サーバーの設定が不要な場合は、そのまま [Next >] ボタンをクリックします。プロキシ サーバーを構成する場合は、[Specify custom proxy settings]を選択して構成してください。

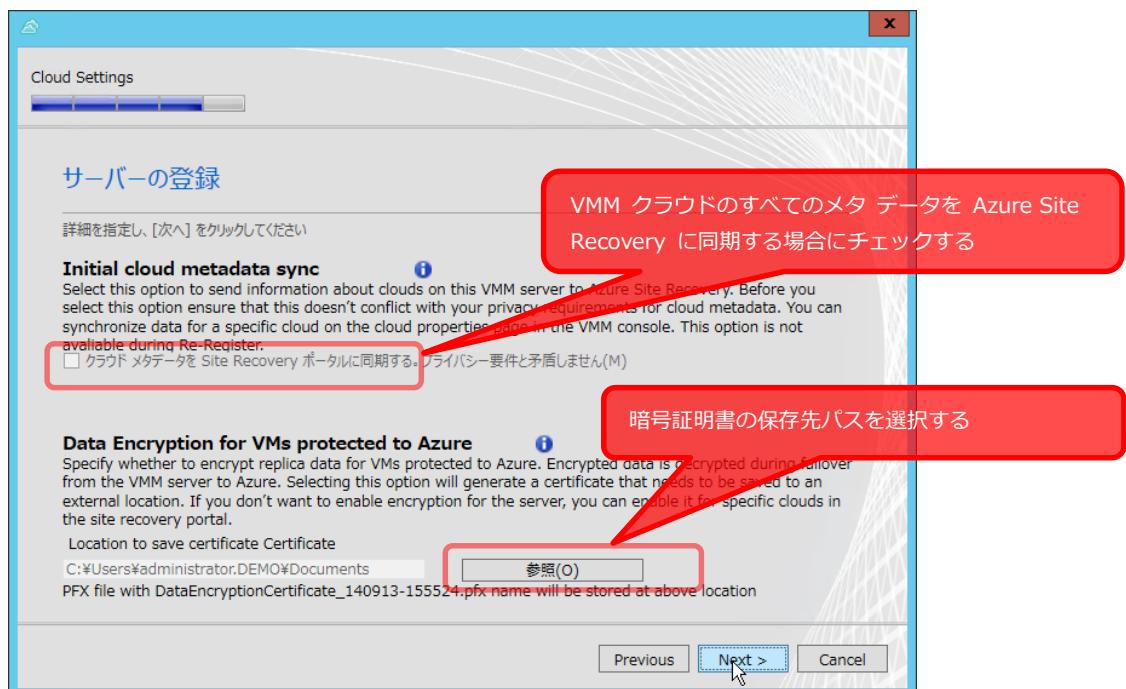


4. [サーバーの登録] のページでは、[参照] ボタンをクリックして事前に取得しておいた登録キー ファイルを指定します。登録キー ファイルを指定すると、Azure Site Recovery 資格情報コンテナーが識別され、[Vault Name] にコンテナ名が表示されます。[Server Name] には、VMM 管理サーバーを Azure Site Recovery ポータル上で識別するためのフレンドリ名を設定します。既定で、VMM 管理サーバーの FQDN が設定されます。



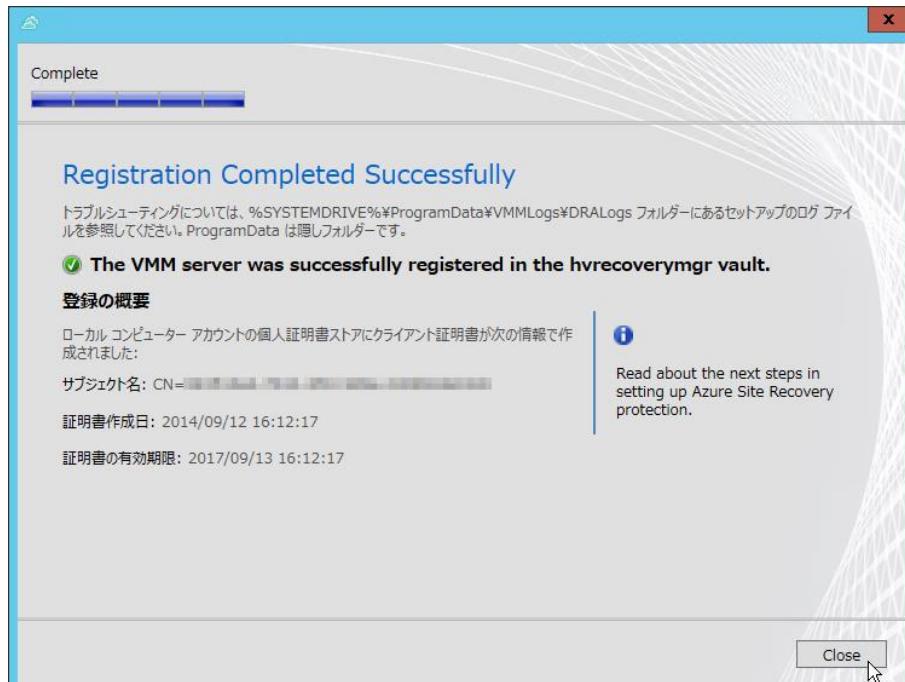
5. [サーバーの登録] の次のページでは、VMM クラウド側のメタデータを Azure Site Recovery に同期する方法を選択します。すべてのメタデータを同期する場合は、[クラウド メタデータを Site Recovery ポータルに同期する] をチェックします。特定の VMM クラウドのみを同期したい場合は、このオプションはチェックせずに、後で VMM 管理コンソールで VMM クラウドごとにメタデータの同期を有効にします。

また、このページで [参照] ボタンをクリックして、レプリケーション データの暗号化に使用する暗号証明書の保存先パスを指定します。暗号証明書 (DataEncryptionCertificate.pfx) は、フェールオーバーを実行する際の暗号化解除のために必要になるものなので、安全な場所に大切に保管してください。



6. [サーバーの登録] のページで [Next >] ボタンをクリックすると、Azure Site Recovery 資格情報コンテナーへのサーバーの登録処理が始まります。

[Registration Completed Successfully (登録は正常に完了しました)] と表示されたら、[Close] ボタンをクリックしてセットアップ ウィザードを終了します。ウィザードを終了すると、プロバイダーのインストールのために停止された System Center Virtual Machine Manager (SCVMMService) サービスが再開されます。



Note : VMM クラウドごとのメタデータの同期

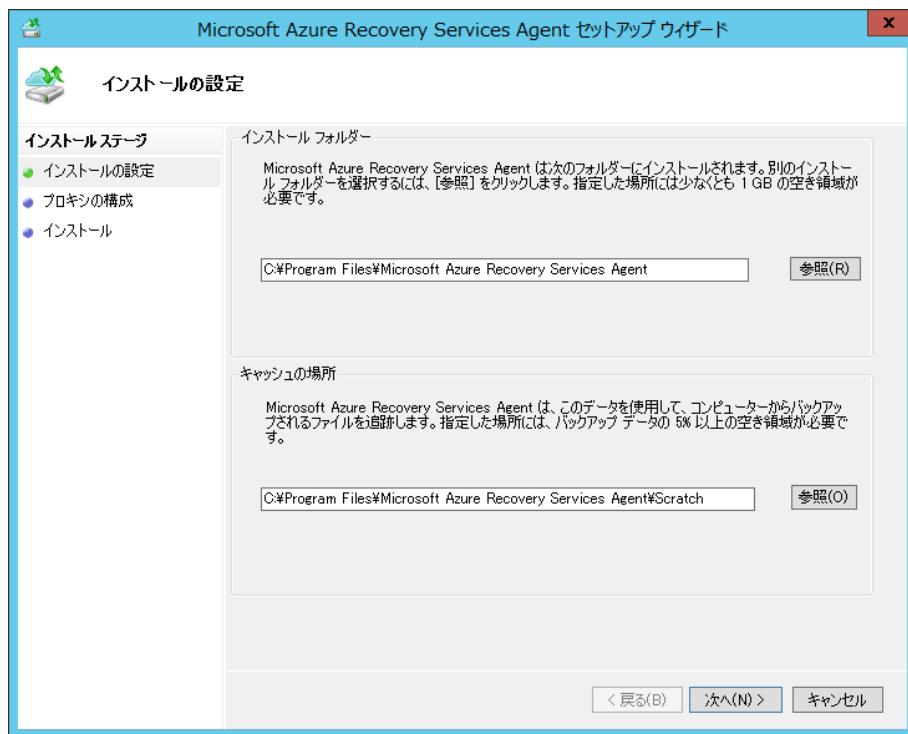
Azure Site Recovery プロバイダーのインストール時にメタデータの同期オプションを有効にしなかった場合は、VMM 管理コンソールを使用して、Azure Site Recovery の保護を利用する VMM クラウドのプロパティを開き、[このクラウドに関する構成データを Windows Azure Hyper-V Recovery Manager に送信する] オプションをチェックします。



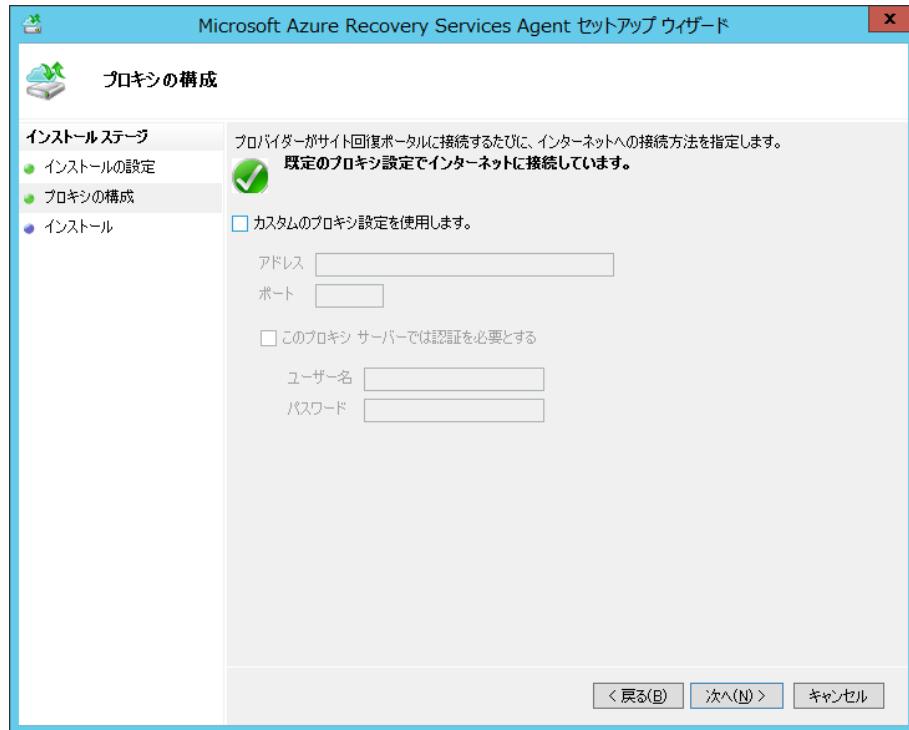
◆ Hyper-V ホストへのエージェントのインストール

次の手順に従って、保護しようとしている VMM クラウドに存在するすべての Hyper-V ホストに Azure Recovery Services エージェントをインストールします。なお、この手順は、2014 年 9 月時点の Azure Site Recovery プロバイダー バージョン 2.0.8689.0 に基づいています。より新しいバージョンでは、UI や手順が変更になる場合があります。

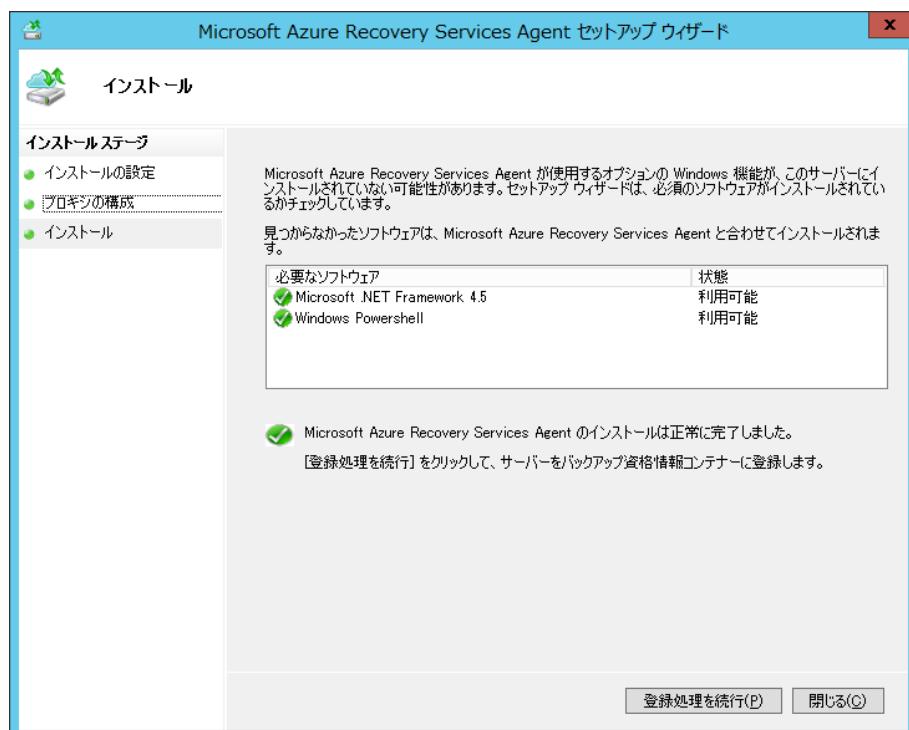
1. Azure Site Recovery ポータルから Azure Recovery Services エージェントのインストーラー (MARSAgentInstaller.exe) を Hyper-V ホストにダウンロードし、インストーラーをダブル クリックして開始します。
2. [インストールの設定] のページで、インストール先とキャッシュの場所のパスを確認し、[次へ] ボタンをクリックします。インストール先には 1 GB の空き領域が、キャッシュの場所には同期データの 10% に相当する空き領域が必要です。ディスク使用が大きくなる可能性があるキャッシュの場所については、必要に応じて別のドライブ上のパスを指定してください。



3. [プロキシの構成] のページでは、Hyper-V ホストが Azure Site Recovery のサービスと通信するためにプロキシ サーバーを経由する必要がある場合にプロキシ サーバーの構成を行います。必要があればプロキシ サーバーを構成し、[次へ] ボタンをクリックします。



4. [インストール] のページに、Azure Recovery Services エージェントの前提コンポーネントの現在のインストール状態が表示されます。不足しているコンポーネントがある場合は、Azure Recovery Services エージェントのインストールと合わせて自動的にインストールされます。
5. [インストール] ボタンをクリックし、Azure Recovery Services エージェントのインストールを開始します。「Microsoft Azure Recovery Services Agent のインストールは正常に完了しました」と表示されたら、[閉じる] ボタンをクリックしてウィザードを終了します。[登録処理を続行] ボタンは Azure Backup サービス用のものなのでクリックしないでください。



Note : Azure Backup サービスとエージェントの共通化

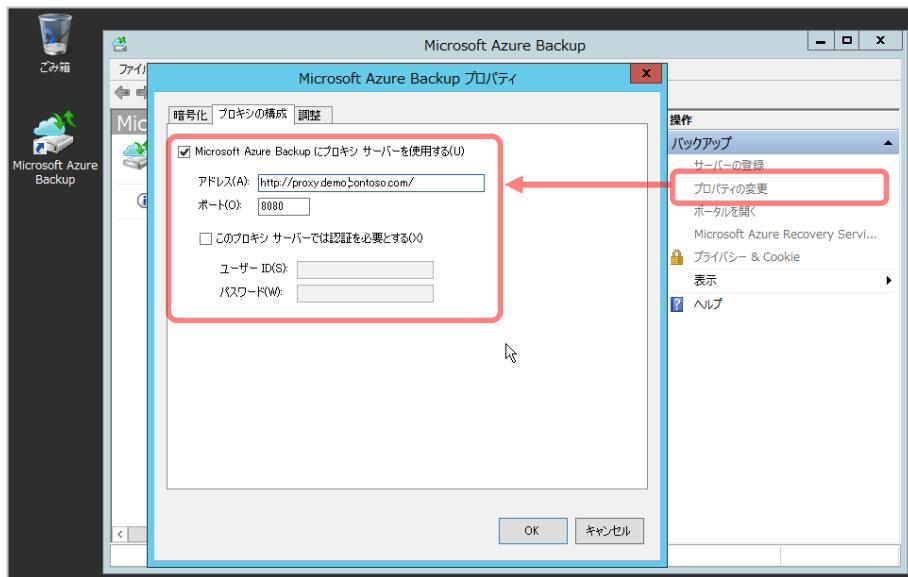
Azure Recovery Services エージェントは、Microsoft Azure の Backup サービスと共通のものを使用します。

Hyper-V ホストに以前のバージョン Azure Backup エージェントがインストールされている場合は、Azure Recovery Services エージェントはアップグレード インストールになり、Azure Recovery Services エージェントに置き換えられます。

◆ Azure Recovery Services エージェントのためのプロキシ サーバーの変更

VMM 管理サーバーは、Azure Site Recovery の展開方法に関わらず、直接またはプロキシ サーバーを介して、Microsoft Azure の Azure Site Recovery サービスに対して HTTPS (443/TCP) で通信できる必要があります。Azure Site Recovery のオンプレミスから Azure のサイト回復ではさらに、Hyper-V ホストと Azure ストレージ間のレプリケーションのために、インターネットに対して出力方向の HTTPS (443/TCP) トラフィックが発生します。どちらも、オンプレミス側からの発信のみのトラフィックであり、オンプレミス側への HTTPS の着信はありません。

Hyper-V ホストがインターネットと通信するためにプロキシ サーバーを経由するように構成を変更する必要がある場合は、Azure Recovery Services エージェントで使用するプロキシ サーバーを構成する必要があります。Azure Recovery Services エージェントは Azure Backup サービスと共にになっており、エージェントをインストールすると Hyper-V ホストのデスクトップに [Microsoft Azure Backup] コンソールのショートカットが追加されます。この [Microsoft Azure Backup] コンソールを開いて、[操作] ペインにある [プロパティの変更] をクリックすると、[プロキシの構成] タブでプロキシ サーバーを構成できます。



2.7 VMM クラウドの保護の構成

VMM 管理サーバーの登録と Hyper-V ホストのエージェントの準備ができたら、Microsoft Azure 管理ポータルの Azure Site Recovery ポータルを使用して、VMM クラウドのレプリケーション設定を構成します。

1. Azure Site Recovery ポータルを開き、Azure Site Recovery 資格情報コンテナーのページに移動します。
2. ページ上部の [保護された項目] をクリックします。このページに、登録した VMM 管理サーバーに存在する VMM クラウドが表示されるので、名前の横にある  をクリックします。



3. [レプリケーションの場所と頻度] および [レプリケーション設定] の設定ページが表示されるので、ターゲットを [Microsoft Azure] に設定し、VMM クラウドと Microsoft Azure 間のレプリケーション パラメーターを構成します。



各パラメーターの設定については、以下の表を参考にしてください。

レプリケーションの場所と頻度	
ターゲット	Microsoft Azure を選択します。
ストレージ アカウント	Azure Site Recovery 資格情報コンテナーと同じリージョンにある、ジオ（主要地域）冗長が有効なストレージ アカウントを指定する必要があります。

保存データの暗号化	VMM 管理サーバーへの Azure Site Recovery プロバイダーのインストール時に有効化した場合は、暗号化をオンにできます。なお、ここで暗号化をオンにしない場合でも、レプリケーション トライフィックは Azure ストレージへの HTTPS 暗号化で保護されます。
コピーの頻度	30 秒、5 分 (既定)、15 分から選択します。
復旧ポイントの保持期間 (時間)	0 (既定) ~ 24 から選択します。 最初の 1 時間は [60/コピーの頻度] の数の復旧ポイントが作成され、1 以上の保持期間が設定された場合、その後の 1 時間に 1 回の頻度で復旧ポイントが作成されます
アプリケーション整合性スナップショットの頻度	なし (既定)、または 1 ~ 12 時間から選択します。 1 以上の頻度を指定した場合、標準のスナップショットとは別に、指定された時間ごとにアプリケーション整合性スナップショットが作成されます。アプリケーション整合性スナップショットは、ゲスト OS のボリューム シャドウ コピー サービス (VSS) を使用して作成されるアプリケーションの一貫性のあるスナップショットです。Linux 仮想マシンの場合は、ファイル システムと整合性のあるスナップショットが作成されます。
レプリケーション設定	
レプリケーションの開始時刻	すぐに、または開始時刻 (30 分単位) を指定します。 最初の初期レプリケーションは、大きなデータ転送を伴うため、ネットワークのピーク時間帯を避けるために開始時刻を調整できます。

- レプリケーションのパラメーターを構成したら、ページ下部中央にある [保存] をクリックします。すると、Azure Site Recovery のサービスは [クラウド名 (保護の構成)] ジョブを作成して開始し、VMM 管理サーバーのプロバイダーと通信し、VMM 管理サーバーの機能を介して VMM クラウドに含まれる Hyper-V ホストの Hyper-V レプリカを自動構成します。
- ジョブが正常に完了したことをポータル下部の通知で確認してください。ジョブの進行状況および実行結果の詳細は、[ジョブの表示] をクリックして確認できます。

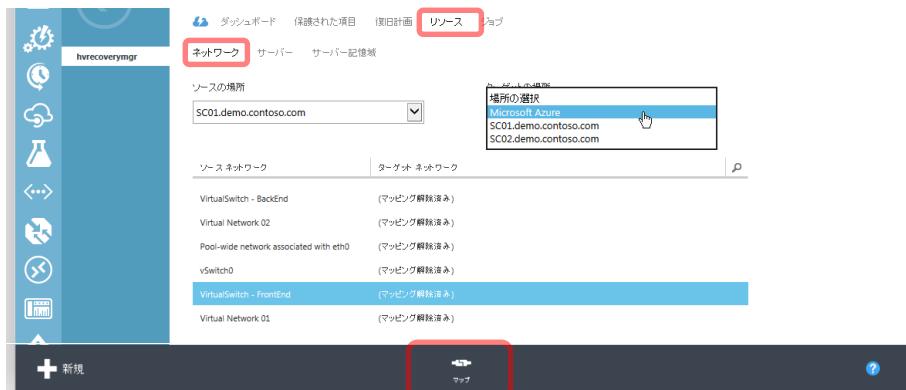


保護の構成に失敗した場合は、ジョブの詳細を参照して原因を調査し、問題を取り除いてから

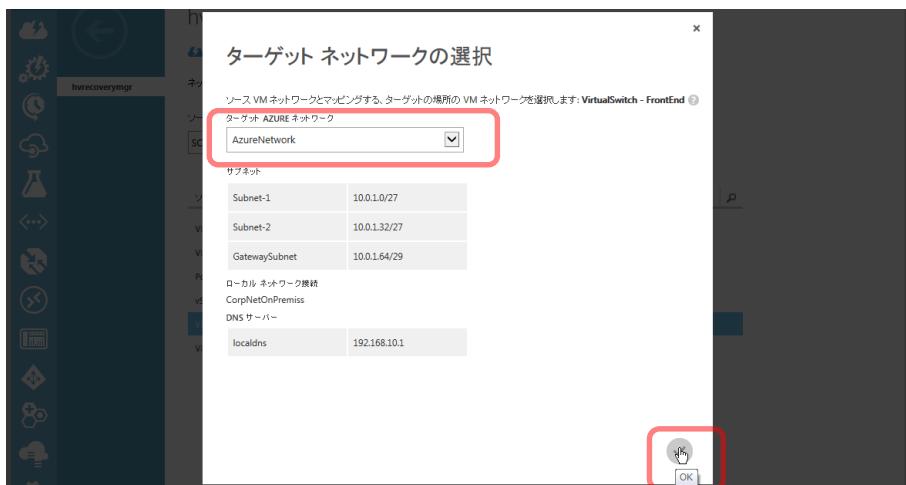
再度、保護を構成してください。



6. 続いて、Azure Site Recovery ポータルの上部にある [リソース] をクリックし、[リソース] ページを開きます。ここで、VMM クラウド側の論理ネットワーク (Hyper-V 仮想スイッチ) と Microsoft Azure 側の仮想ネットワークをマッピングします。[リソース] ページの [ネットワーク] をクリックし、[ソースの場所] を VMM クラウドに、[ターゲットの場所] を Microsoft Azure に設定したら、マッピングしたい VMM クラウド側の論理ネットワークを選択し、ページ下部の [マップ] をクリックします。



7. [ターゲット ネットワークの選択] ダイアログ ボックスが表示されるので、事前に作成しておいた Microsoft Azure 仮想ネットワークを指定し、OK ボタン (✔) をクリックします。



2.8 仮想マシンの保護の有効化

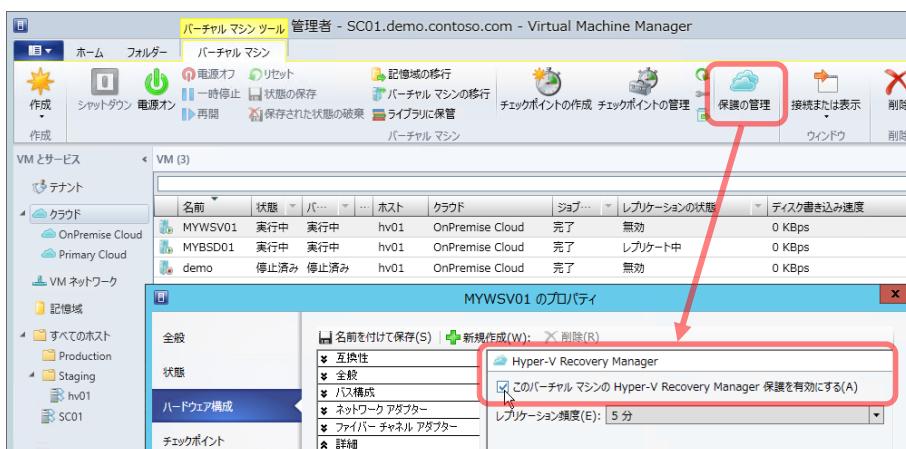
VMM クラウドの保護を構成したら、続いて、保護したい仮想マシンで Azure Site Recovery の保護を有効化します。保護を有効化するために、オンプレミス側の稼働中の仮想マシンを停止する必要はありません。

- 仮想マシンの保護の有効化には 2 つの方法があります。1 つは、Azure Site Recovery ポータルから有効化する方法、もう 1 つは、VMM コンソールから有効化する方法です。

Azure Site Recovery ポータルから有効化するには、[保護された項目] ページを開き、先ほど保護を構成した VMM クラウドのページに移動します。ページ上部の [仮想マシン] をクリックし、ページ下部にある [仮想マシンの追加] をクリックします。すると、[仮想マシンの保護の有効化] ダイアログ ボックスに、VMM クラウド内のまだ保護されていない仮想マシンがリストされるので、保護したい仮想マシンを選択し、OK ボタン (✔) をクリックします。



VMM コンソールから操作する場合は、[VM とサービス] の [クラウド] を開き、保護したい仮想マシンを選択して、[バーチャル マシン] タブにある [保護の管理] をクリックします。すると、仮想マシンのプロパティの該当ページが開くので、[このバーチャル マシンの Hyper-V Recovery Manager 保護を有効化する] をチェックし、[OK] ボタンをクリックして仮想マシンのプロパティを閉じます。



2. どちらの方法で保護を有効化した場合でも、Azure Site Recovery のサービスは「仮想マシン名（保護の構成）」ジョブを作成して開始し、VMM 管理サーバーを介して仮想マシンのレプリケーション設定を自動構成します。ジョブの進行状況および実行結果の詳細は、Azure Site Recovery の [ジョブ] ページで確認できます。ジョブが失敗する場合は、ジョブの詳細を参照して原因を調査し、問題を取り除いてから再度、仮想マシンの保護を有効化してください。

名前	状態	開始時間	期間
保護の有効化に関する操作	完了	2014/08/08 7:40:33	1 分
レプリケーションターゲットの検定中	完了	2014/08/08 7:40:33	1 分
レプリケーションを有効にする	完了	2014/08/08 7:41:21	1 分
初期レプリケーションの開始中	完了	2014/08/08 7:41:29	1 分
プロバイダー状態の更新中	完了	2014/08/08 7:41:38	1 分

3. 仮想マシンの保護の有効化が完了すると、Azure Site Recovery ポータルの [保護された項目] の VMM クラウドの [仮想マシン] ページに保護された仮想マシンがリストされます。

名前	アクティブな場所	レプリケーションの状態	ターゲットのサイズ	フェールオーバーの状態
MYBSD01	OnPremise Cloud	保護済み - OK	XS	準備完了
MYWSV01	OnPremise Cloud	初期レプリケーションの進行中 - OK	A7	

4. VMM クラウド側の仮想マシンの構成 (CPU 数、割り当てメモリ、ディスクの数) にあわせて、フェールオーバー後に Microsoft Azure 側に作成される仮想マシンのインスタンス サイズが自動設定されます。仮想マシンのインスタンス サイズは、フェールオーバーした際の Microsoft Azure 仮想マシンの課金レートに直接的に関係するので、不適切なサイズが設定されていないかどうかを確認してください。例えば、VMM クラウド側の仮想マシンで動的メモリが有効になっている場合、最大 RAM の値にあわせて大きなインスタンス サイズが割り当てられる場合があります。仮想マシンのインスタンス サイズは、Azure Site Recovery ポータルの各仮想マシンのページから変更できます。

Microsoft Azure

XS (1 CPU, 0.75 GB RAM)
S (1 CPU, 1.75 GB RAM)
M (2 CPU, 3.5 GB RAM)
L (4 CPU, 7 GB RAM)
XL (8 CPU, 14 GB RAM)
A5 (2 CPU, 14 GB RAM)
A6 (4 CPU, 28 GB RAM)
A7 (8 CPU, 56 GB RAM)

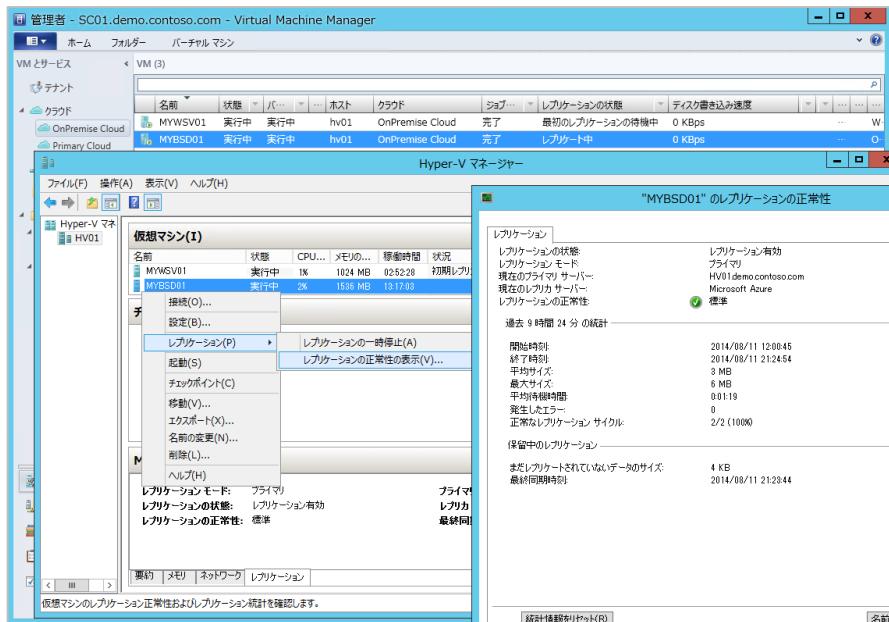
2.9 レプリケーションの正常性の監視

仮想マシンの保護が有効化されると、初期レプリケーションが開始され、初期レプリケーション完了後、フェールオーバーの実行が可能な状態になります。また、初期レプリケーションが完了すると、以降は VMM クラウドの保護の構成で指定した頻度で、VMM クラウド側の変更がレプリケートされるようになります。

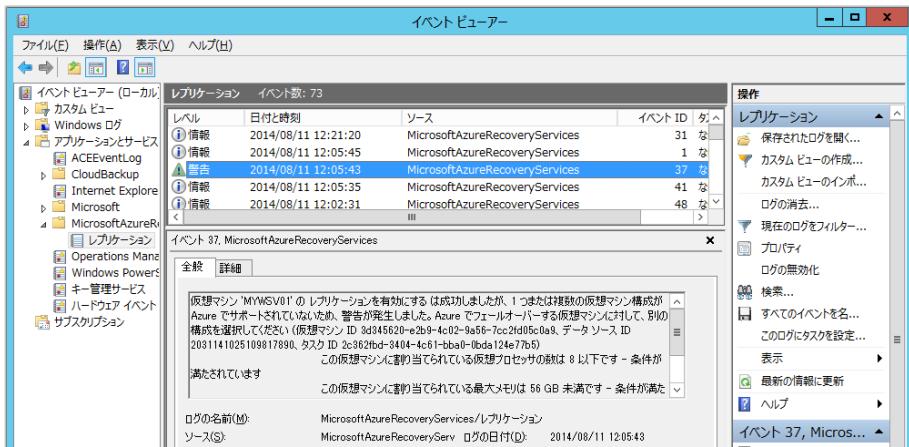
仮想ハード ディスクのサイズや数、利用可能なネットワーク帯域にも依存しますが、大量のデータ送信が伴うため、初期レプリケーションが完了するまでには数時間からそれ以上の時間を要します。

初期レプリケーションの待機中、および初期レプリケーションが完了し、定期的なレプリケート中の状態になったことは、VMM コンソールや Azure Site Recovery ポータルの【保護された項目】の【仮想マシン】ページで確認できます。しかし、レプリケーションの進捗といった詳細情報は得られません。

レプリケーションの詳細な状態は、Hyper-V マネージャーで Hyper-V レプリカのレプリケーションの正常性を監視するのと同じ方法で確認することができます。通常の Hyper-V レプリカは、プライマリ サーバーからレプリカ サーバーに作成されたレプリカ仮想マシンに対して、レプリケーションが行われます。一方、Azure Site Recovery のオンプレミスから Azure のサイト回復の保護の場合、レプリカ サーバーが Microsoft Azure という構成になります。

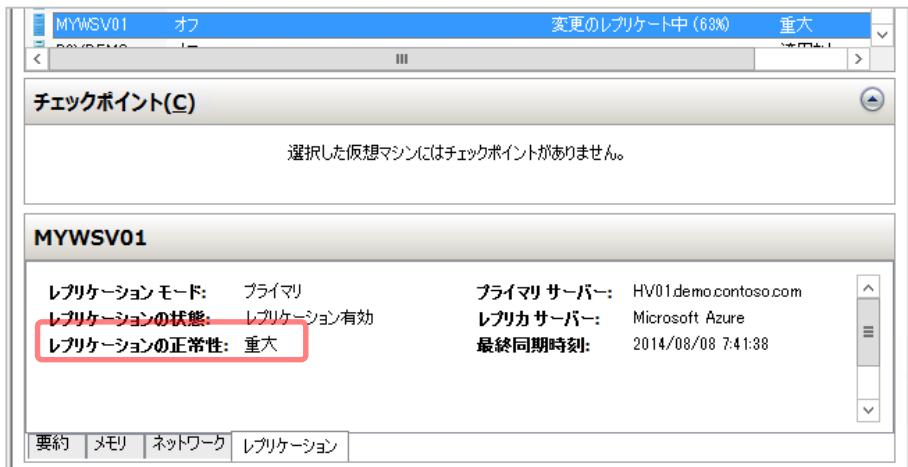


Azure Site Recovery のレプリケーションの状態に関しては、Hyper-V ホストのイベント ログの MicrosoftAzureRecoveryServices ログにも詳細情報が記録されます。



Note : レプリケーション頻度の調整

変更のレプリケーションが、レプリケーションの頻度に指定した期間内に実行しない場合、以下の画面のように、変更のレプリケートが問題なく進行中のようにあっても、レプリケーションの正常性が重大と報告されます。



VMM クラウドの保護の構成でレプリケーションの頻度を既定の 5 分または 30 秒で構成してある場合は、より長い 15 分または 5 分に変更することでこの状態を解消できる場合があります。最長の 15 分間隔で解消しない場合、使用中のインターネット接続回線では帯域幅が不足しています。インターネット接続回線の帯域幅の増強を検討してください。なお、レプリケーションの頻度は RPO (目標復旧時点) に影響することに留意してください。



STEP 3. フェールオーバーの管理

この STEP では オンプレミスから Azure への仮想マシンのフェールオーバー、
および Azure からオンプレミスへの仮想マシンのフェールバックについて説明
します。

この STEP では、次のことを学習します。

- ✓ フェールオーバーに利用される Microsoft Azure の IaaS 機能
- ✓ 復旧計画の作成
- ✓ テスト フェールオーバーの実行
- ✓ 計画されたフェールオーバーの実行
- ✓ 計画されていないフェールオーバーの実行
- ✓ フェールバックの実行

3.1 フェールオーバーとは

Azure Site Recovery のオンプレミスから Azure のサイト回復は、オンプレミス側の VMM クラウドで稼働中の仮想マシンの仮想ハードディスク (VHD または VHDX) のコピーを、Microsoft Azure ストレージに作成し、オンプレミス側の仮想ハードディスクに加えられた変更をレプリケーションの頻度に指定した間隔 (30 秒、5 分、または 15 分) で Microsoft Azure ストレージ側にレプリケーションして同期します。

平常運用時、企業ネットワーク上のクライアントは、オンプレミスのデータセンターの VMM クラウドで稼働する仮想マシンにアクセスします。

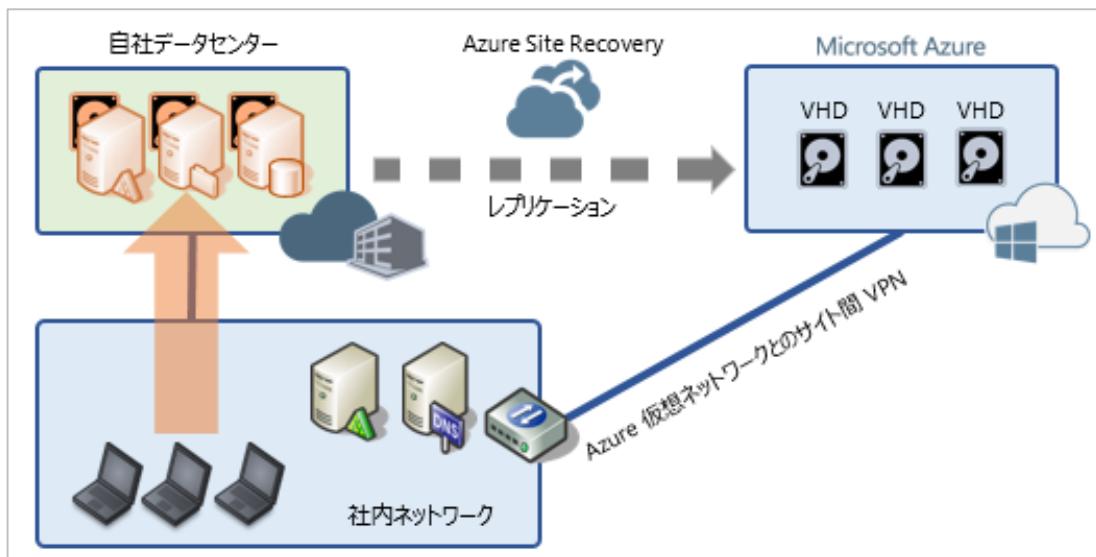


図 4: 通常運用時のクライアント アクセスは、データセンター内のサーバーへ

オンプレミスから Azure のサイト回復におけるフェールオーバーとは、障害や災害、計画的なメンテナンス作業のために、オンプレミス側の VMM クラウドのインフラストラクチャが利用できなくなった場合に、Microsoft Azure ストレージに保存されている仮想ハードディスクの最新のコピー、または過去の回復ポイントを使用して、Microsoft Azure 側で仮想マシンを復旧することを指します。

Microsoft Azure 側での仮想マシンの復旧には、Microsoft Azure ストレージに加えて、Microsoft Azure 仮想マシンおよび Microsoft Azure 仮想ネットワークという、Microsoft Azure の IaaS 機能が利用されます。Microsoft Azure 仮想ネットワークはお客様専用の分離されたネットワークであり、お客様のオンプレミスの企業ネットワークとサイト間 VPN 接続でシームレスに相互接続されます。企業ネットワーク上のクライアントは、動的 DNS による名前解決により、特別な切り替え操作なしで Microsoft Azure 側で復旧した仮想マシンに引き続きアクセスすることが可能です。

Microsoft Azure 側の仮想マシンはフェールオーバーの際にのみ作成されますが、Microsoft Azure 仮想ネットワークとのサイト間 VPN 接続は常時です。そのため、通常の Microsoft Azure 仮想マシンの Windows 仮想マシンや Linux 仮想マシンを Azure Site Recovery で使用するのと同じ仮想ネットワークに接続し、企業のネットワーク インフラストラクチャの延長として利用

することができます。例えば、Azure Site Recovery による保護とは別に、Active Directory の 2 台目以降のドメイン コントローラーや DNS サーバーを Microsoft Azure 側で常時稼働させ、ディレクトリのレプリケーションを双方向で行うことで、企業のネットワーク インフラストラクチャの冗長性を高めることができます。

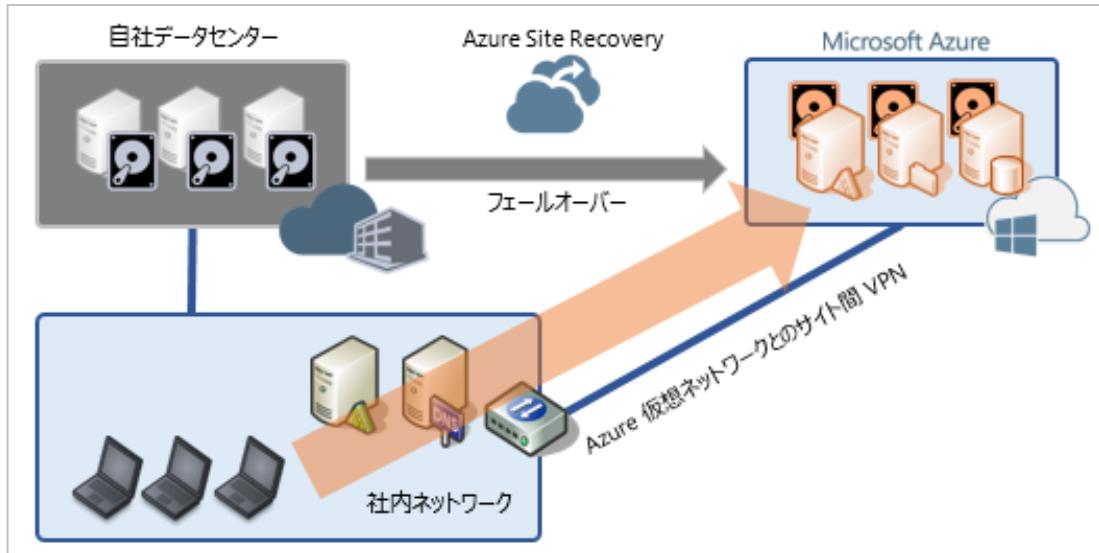


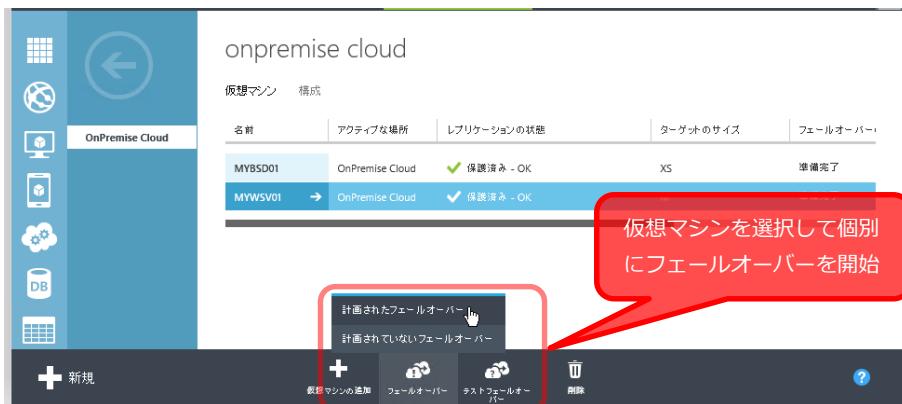
図 5: フェールオーバー後のクライアント アクセスは、Azure 側で復旧させたサーバーへ。Azure 側での変更は、フェールバック時にレプリケーションを反転して同期される

フェールオーバーには、次の表に示す 3 つの種類があります。

フェールオーバー VMM との 説明		
の種類	接続性	
テスト フェールオーバー	不要	レプリケーションされた仮想ハード ディスクで仮想マシンを実行できるかどうかを Azure 側でテストします。レプリケーション データは変更されません。
計画されたフェールオーバー	必須	仮想マシンをシャットダウンして、未同期のデータのレプリケーションを完了させたあと、フェールオーバーを実行し、レプリカ仮想マシンを作成、開始します。もう一度、反対方向の計画されたフェールオーバーを実行することで、通常運用の状態にフェールバックします。RPO (目標復旧時点) はゼロ。
計画されていない フェールオーバー	不要	オンプレミスの VMM クラウドが利用できなくなった場合に、Azure 側にフェールオーバーし、レプリカ仮想マシンを作成、開始して仮想マシンを復旧します。オンプレミスの VMM クラウドが復旧したら、反対方向の計画されたフェールオーバーを実行してフェールバックします。RPO (目標復旧時点) は 30 秒、5 分、または 15 分。

フェールオーバーは、仮想マシンごと、あるいは次に説明する復旧計画（Recovery Plan）を使用してワン クリックで開始できます。

仮想マシンごとにフェールオーバーを実行するには、Azure Site Recovery ポータルの【保護された項目】の【仮想マシン】ページで対象の仮想マシンを選択し、ページ下部のメニューを使用してフェールオーバーを開始します。



復旧計画を使用してフェールオーバーを実行するには、Azure Site Recovery ポータルの【復旧計画】ページで対象の復旧計画を選択し、ページ下部のメニューを使用してフェールオーバーを開始します。

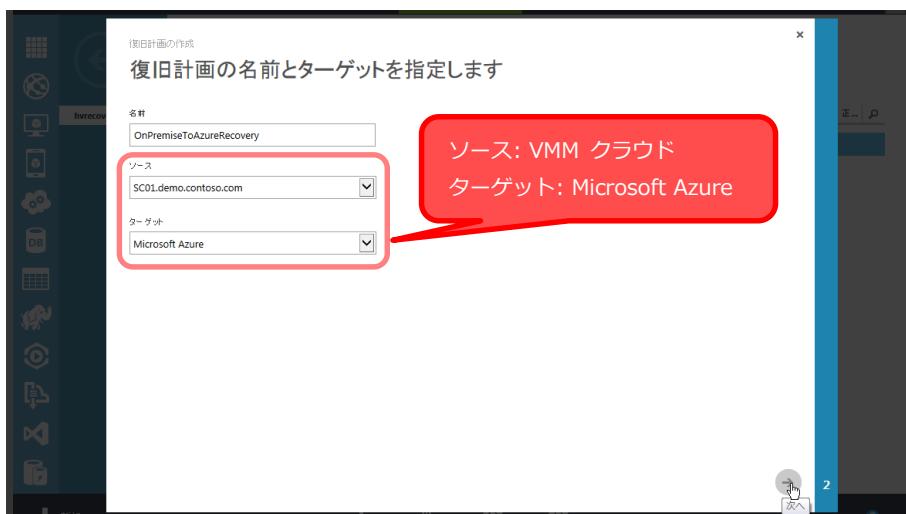


3.2 復旧計画の作成

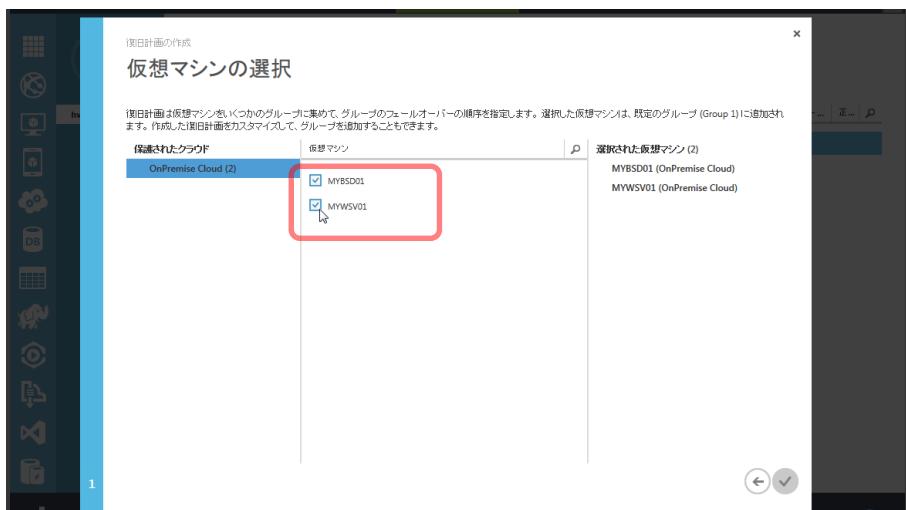
復旧計画 (Recovery Plan) とは、複数の仮想マシンを対象としたフェールオーバーの処理をワンクリックで開始し、自動化するための手続きを事前に定義したものです。復旧計画では、仮想マシンをグループ化し、仮想マシンを開始する順番をグループごとに制御できます。また、指示があるまで処理を中断する手動アクションを処理の前後または途中に追加できます。復旧計画は、RTO (Recovery Time Objective: 目標復旧時間) の短縮に役立ちます。

復旧計画を作成するには、次の手順で操作します。

1. Azure Site Recovery ポータルを開き、ページ上部の【復旧計画】をクリックしてページを開き、ページ下部の【作成】をクリックします。
2. 【復旧計画の作成】ウィザードが開始します。1 ページ目では、復旧計画の名前を決定し、【ソース】に VMM クラウドの VMM 管理サーバーを、【ターゲット】に Microsoft Azure を指定します。



3. 2 ページ目では、この復旧計画でフェールオーバーする対象の 1 台以上の仮想マシンを選択して、ウィザードを完了します。



4. これで、選択した仮想マシンを同時にフェールオーバーおよびフェールバックするための復旧計画が作成されました。仮想マシンのグループ化や開始順序の調整、手動アクションの追加など、さらにカスタマイズするには、作成した復旧計画をクリックしてカスタマイズ ページを開き、カスタマイズが完了したら [保存] をクリックします。



例えば、Web フロントエンド、ミドルウェア、バックエンド データベースからなる 3 階層システムを複数台の仮想マシンで実行している場合、3 つのグループを作成し、各グループに各階層の仮想マシンを登録することで、フェールオーバー時にバックエンド、ミドルウェア、Web フロントエンドの順番で仮想マシンを開始させることができます。計画されたシャットダウンにおけるオンプレミス側のシャットダウン処理は暗黙的にその逆順に行われます。



Note : 手動アクションについて

例えば、復旧計画の最後の処理として、次のような手動アクションを追加したとしましょう。



この場合、計画されたフェールオーバーや計画されていないフェールオーバーを実行すると、次のようにアクション待機中のジョブが通知されます。



[ジョブ] ページで [手動アクションの完了] をクリックすると、手動アクションのアクション手順のテキストが表示され、ジョブを続行させることができます。手動アクションの確認画面では、任意でメモを残すことができます。



Note : Azure Automation (プレビュー)との統合によるスクリプトのサポート

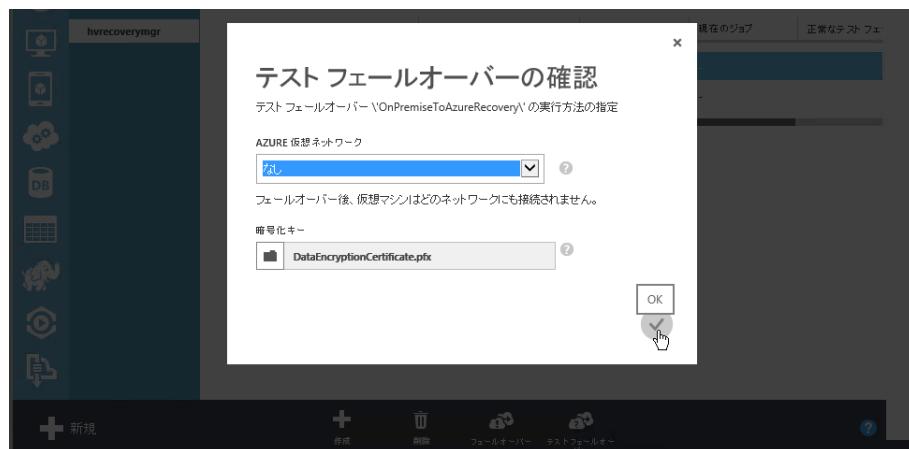
9月11日(日本時間)より、Azure Automation (プレビュー)との統合によるスクリプト実行機能が追加されました。この機能を利用するには、スクリプトとして実行する Runbook を含む Azure Automation (プレビュー) アカウントが必要です。

3.3 テスト フェールオーバー

テスト フェールオーバーは、Microsoft Azure 側にレプリケーションされた仮想ハード ディスクで仮想マシンを正常に起動できるかどうかを Microsoft Azure 側でテストするために使用します。テスト フェールオーバーは、閉じた環境で実行され、レプリケーション データが変更されることはありません。そのため、オンプレミスの VMM クラウド側の状態に関係なく実行できます。

テスト フェールオーバーを実行するには、次の手順で操作します。

1. Azure Site Recovery ポータルで仮想マシンまたは復旧計画を選択し、ページ下部の [テスト フェールオーバー] をクリックします。
2. [テスト フェールオーバーの確認] ダイアログ ボックスが開きます。テスト フェールオーバーは通常、Microsoft Azure 仮想ネットワークに接続されない、企業ネットワークとは隔離された環境で行います。そのため、[AZURE 仮想ネットワーク] は [なし] に設定します。レプリケーション データの暗号化を行っている場合は、[暗号化キー] に [Azure Site Recovery プロバイダーのインストール時に保存しておいた暗号化証明書ファイル](#)を指定して、OK ボタン (✔) をクリックします。



3. [仮想マシン名または復旧計画名 (テスト フェールオーバー)] ジョブが開始され、レプリケートされた仮想ハード ディスクを使用して、Microsoft Azure 仮想マシンが作成、開始されます。このジョブは、[テストの完了] ステップのところで [アクションを待機] の状態でストップします。



4. ジョブが【アクションを待機】状態になつたら、Microsoft Azure 管理ポータルの【仮想マシン】のポータルを開きます。テスト フェールオーバーで作成された仮想マシンが実行中の状態になっているはずです。仮想マシンが表示されない場合は、F5 キーを押して表示をリフレッシュしてください。

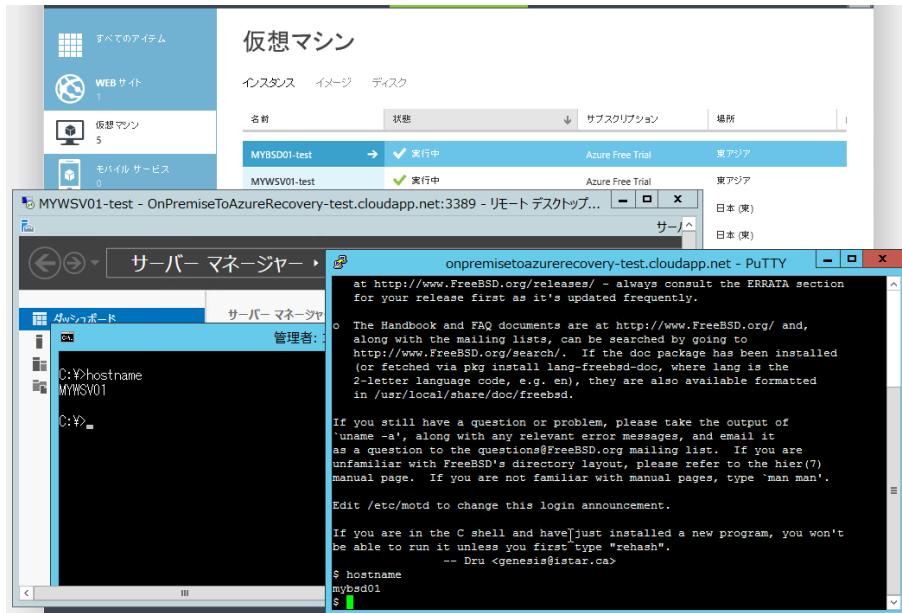
The screenshot shows the Azure portal's 'Virtual Machines' blade. On the left sidebar, 'Virtual Machines' is selected. The main area displays a table of VMs with columns for Name, Status, Subscription, and Region. Two VMs are highlighted with a red border: 'MYBS01-test' and 'MYWS01-test', both showing 'Running' status. Other VMs listed are 'myrhe165', 'myvs2013win81', and 'mywin2012r2u1', all in a 'Stopped (S1)' state.

※ この画面の停止済みの 3 台の仮想マシンは、Azure Site Recovery とは関係なく、Microsoft Azure 仮想マシンのギャラリーから作成した通常の仮想マシンです

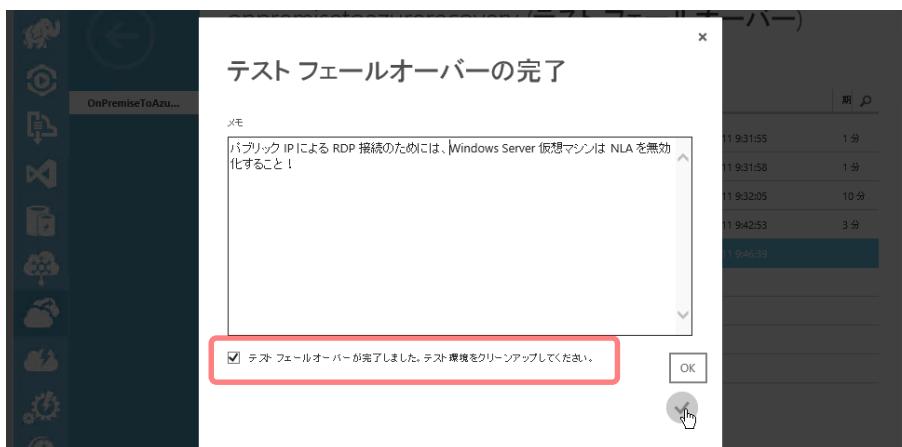
5. テスト フェールオーバーで作成された仮想マシンは、Microsoft Azure 仮想ネットワークには接続されませんが、Microsoft Azure の内部ネットワークには接続され、エンドポイントを追加することでパブリック仮想 IP (VIP) アドレスまたは VIP に対応したクラウド サービスの DNS 名 (仮想マシン名-test.cloudapp.net、または、復旧計画名-test.cloudapp.net) でインターネットを介してアクセスすることが可能です。

The screenshot shows the 'Add endpoint' dialog for the VM 'myws01-test'. The dialog title is 'Endpoint details specified'. It contains fields for 'Name' (set to 'Remote Desktop'), 'Protocol' (set to 'TCP'), 'Public port' (set to '3389'), and 'Private port' (set to '3389'). There is also a checkbox for 'Load balancing set creation' which is unchecked. A note at the bottom states: 'リモート デスクトップ、Windows PowerShell リモート処理、または SSH エンドポイントの Direct Server Return が有効にすることもできます' (You can enable Remote Desktop, Windows PowerShell remote processing, or SSH endpoint's Direct Server Return). At the bottom right are '完了' (Done) and '次へ' (Next) buttons.

Windows 仮想マシンの場合は Remote Desktop の 3389 ポート、Linux 仮想マシンの場合は SSH の 22 ポートに対するエンドポイントを作成することで、リモート デスクトップ接続や SSH クライアントから接続することができます。いずれかの方法で仮想マシンのコンソールにリモート接続して、仮想マシンのゲスト OS が正常に動作していること、OS ディスク以外のデータ ディスクがマウントされていることなどを確認してください。



6. 仮想マシンの動作確認のテストが完了したら、実行中の仮想マシンはそのままで Azure Site Recovery ポータルの [ジョブ] ページに戻ります。テスト フェールオーバーを終了するために、[仮想マシン名または復旧計画名 (テスト フェールオーバー)] ジョブで待機中となっていた [テストの完了] ステップを選択して、ページ下部の [テストの完了] をクリックします。[テスト フェールオーバーの完了] ダイアログ ボックスが表示されるので、必要があればメモを残し、[テスト フェールオーバーが完了しました。テスト環境をクリーンアップしてください] をチェックして、OK ボタン (✔) をクリックします。



7. ジョブの実行が完了すると、テスト フェールオーバーのために Microsoft Azure 側に作成された仮想マシンは削除されます。仮想マシンが残っている場合は、F5 キーで表示をリフレッシュしてください。



3.4 計画されたフェールオーバー

計画されたフェールオーバーは、オンプレミス側の計画されたメンテナンス作業（ソフトウェアやハードウェアの更新作業や電源工事など）で VMM クラウドが一時的に利用できない場合などに、オンプレミス側の仮想マシンを Microsoft Azure 側に一時的に退避してサービスを継続するためご利用できます。

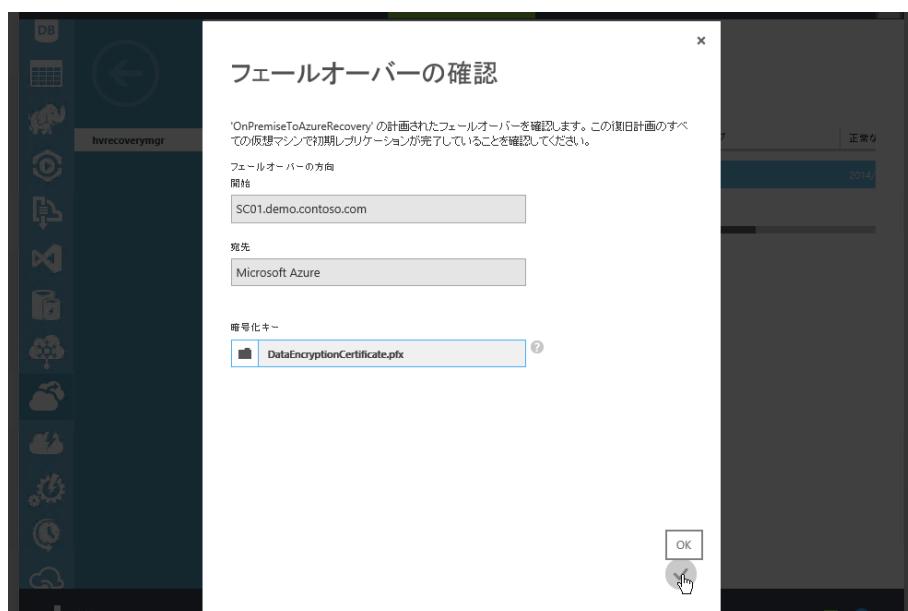
計画されたフェールオーバーは、VMM クラウドが正常に稼働している状態で開始できます。フェールオーバー完了後は、メンテナンス作業のため VMM クラウドがダウン状態でも問題ありません。VMM クラウドが正常な稼働状態に復帰後に、逆方向の計画されたフェールオーバー（フェールバック）を実行することで、通常の運用体制に戻すことができます。

計画されたフェールオーバーを実行するには、次の手順で操作します。

1. Azure Site Recovery ポータルで仮想マシンまたは復旧計画を選択し、ページ下部の [フェールオーバー] をポイントして、[計画されたフェールオーバー] をクリックします。このとき、オンプレミス側の仮想マシンは実行中でもかまいません。フェールオーバーの一連の処理の中で、自動的にシャットダウンされたあと、まだレプリケートされていないデータが完全に同期されます。



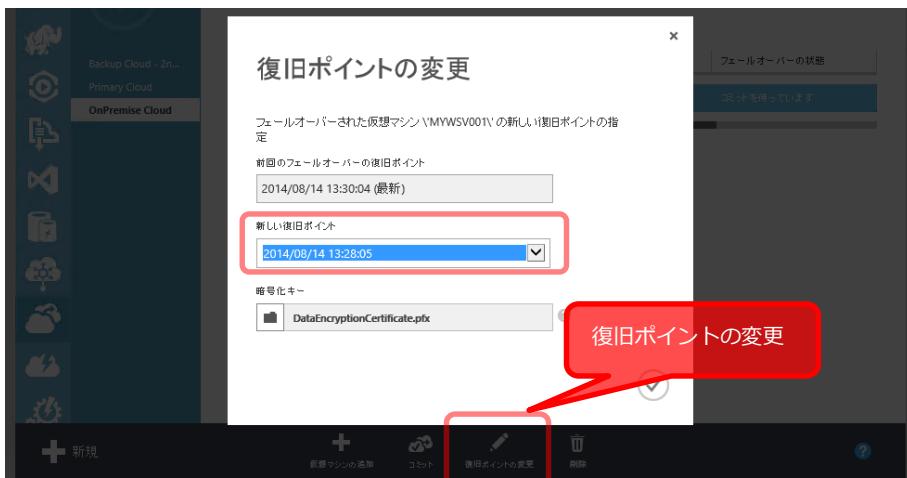
2. [フェールオーバーの確認] ダイアログ ボックスが開きます。フェールオーバーの方向がオンプレミスから Microsoft Azure になっていることを確認し、[暗号化キー] に [Azure Site Recovery プロバイダーのインストール時に保存](#) しておいた暗号化証明書ファイルを指定して、OK ボタン (✔) をクリックします。



3. [仮想マシン名または復旧計画名 (計画されたフェールオーバー)] ジョブが開始され、オンプレミス側の仮想マシンのシャットダウンやレプリケーションの完全な同期、Microsoft Azure 側の仮想マシンの作成、仮想マシンの開始といった一連のステップが実行されます。ジョブが完了すると、仮想マシンまたは復旧計画は [コミット待機中] 状態になります。この状態で、Microsoft Azure 仮想マシンが作成され、Microsoft Azure 仮想ネットワークに接続された状態で実行中になっていますが、[コミット] をクリックすることでフェールオーバーが確定します。



なお、コミットする前であれば、別の復旧ポイントに変更して仮想マシンを開始することができます。コミットを実行すると、すべての回復ポイント（スナップショット）が Azure 側の仮想ハードディスクにマージされます。



4. Azure Site Recovery ポータルの [保護された項目] の [仮想マシン] ページを開くと、保護された仮想マシンの [アクティブな場所] が [Microsoft Azure] に切り替わっていることを確認できます。

名前	アクティブな場所	レプリケーションの状態	ターゲットのサイズ	フェールオーバーの状態
MYBS01	Microsoft Azure	保護済み - OK	XS	準備完了
MYWSV01	Microsoft Azure	保護済み - OK	M	準備完了

さらに、仮想マシンのプロパティ ページを開くと、Microsoft Azure 側にある仮想マシンの状態（仮想ネットワークやストレージ アカウントの使用）を確認することができます。

オブジェクト	内蔵属性型	MICROSOFT AZURE
名前	MYWSV01	MYWSV01
サイズ	2 CPU, 1 TB RAM	M (2 CPU, 3.5 GB RAM)
サーバー	SC01.demo.contoso.com	Microsoft Azure
ネットワーク	VirtualSwitch - FrontEnd	AzureNetwork
ストレージ アカウント (該当せず)		mysirerecovery

5. 計画されたフェールオーバーで作成され、実行中になった仮想マシンは、Microsoft Azure 仮想ネットワークのサイト間 VPN 接続を通じて、オンプレミス側の企業ネットワークと接続されます。そのため、仮想マシンの仮想パブリック IP (VIP) アドレスやクラウド サービスの DNS 名（仮想マシン名.cludapp.net、または、復旧計画名.cludapp.net）に対応したエンドポイントを作成しなくても、仮想ネットワークで自動割り当てされた内部 IP アドレスに対応する社内 DNS の名前解決で企業ネットワーク側からアクセスすることができます。

状態
実行中

DNS 名
onpremisetoadazurerecovery.cloudapp.net

ホスト名
MYWSV01

パブリック仮想 IP (VIP) アドレス
23.97.65.209

内部 IP アドレス
10.0.1.4

サイズ
Standard_A2 (2 コア, 3.5 GB メモリ)

RDP 証明書のサムプリント
-

場所
AzureBureau01 (東日本)

Note : 計画されたフェールオーバーでは、オンプレミス側の仮想マシンの起動はブロックされる

計画されたフェールオーバーで、仮想マシンが Microsoft Azure 側でアクティブになると、オンプレミス側の仮想マシンの起動はブロックされます。

名前	状態	停止済み	停止済み	ホスト	場所	操作
MYBS01	完了	停止済み	停止済み	hv01	OnPremise Cloud	---
MYWSV01	失敗	停止済み	停止済み	hv01	OnPremise Cloud	---

3.5 計画されていないフェールオーバー

計画されていないフェールオーバーは、障害や災害などで、オンプレミス側の VMM クラウドが利用できなくなったときに、Microsoft Azure 側の最後のレプリケーション データを使用して、Microsoft Azure 側で仮想マシンを復旧する操作になります。

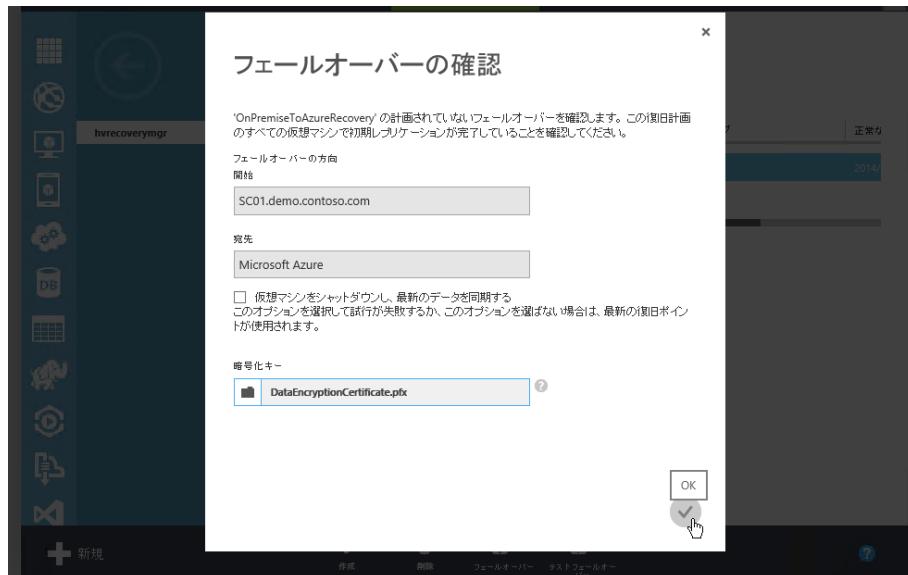


計画されていないフェールオーバーを実行するには、次の手順で操作します。

1. Azure Site Recovery ポータルで仮想マシンまたは復旧計画を選択し、ページ下部の [フェールオーバー] をポイントし、[計画されていないフェールオーバー] をクリックします。



2. [フェールオーバーの確認] ダイアログ ボックスが開きます。フェールオーバーの方向がオンプレミスから Microsoft Azure になっていることを確認し、[暗号化キー] に [Azure Site Recovery プロバイダーのインストール時に保存](#) しておいた暗号化証明書ファイルを指定して、OK ボタン (✔) をクリックします。[仮想マシンをシャットダウンし、最新のデータを同期する] オプションは、オンプレミス側との通信を試みて、可能な場合は最新データを同期するオプションです。同期ができなかった場合でも、計画されていないフェールオーバーは処理を継続します。



3. [仮想マシン名または復旧計画名 (計画されていないフェールオーバー)] ジョブが開始され、Microsoft Azure 側の仮想マシンの作成、仮想マシンの開始といった一連のステップが実行されます。ジョブが完了すると、仮想マシンまたは復旧計画は【コミット待機中】状態になります。この状態で、Microsoft Azure 仮想マシンが作成され、Microsoft Azure 仮想ネットワークに接続された状態で実行中になっていますが、【コミット】をクリックすることでフェールオーバーが確定します。コミットする前であれば、別の復旧ポイントに変更して仮想マシンを開始することができます。



Note : 計画されていないフェールオーバーでは、オンプレミス側の仮想マシンの起動はブロックされない

計画されていないフェールオーバーを実行した場合、計画されたフェールオーバーとは異なり、オンプレミス側の仮想マシンの起動がブロックされない場合があります。仮想マシンを開始した場合、企業ネットワーク上で Microsoft Azure 側の仮想マシンとネットワーク名が重複するなど問題が生じるおそれがあるため、仮想マシンを開始しないように注意してください。仮想マシンを開始して、オンプレミス側に変更があった場合でも、次にフェールバックした際に変更内容は失われます。

3.6 フェールバック

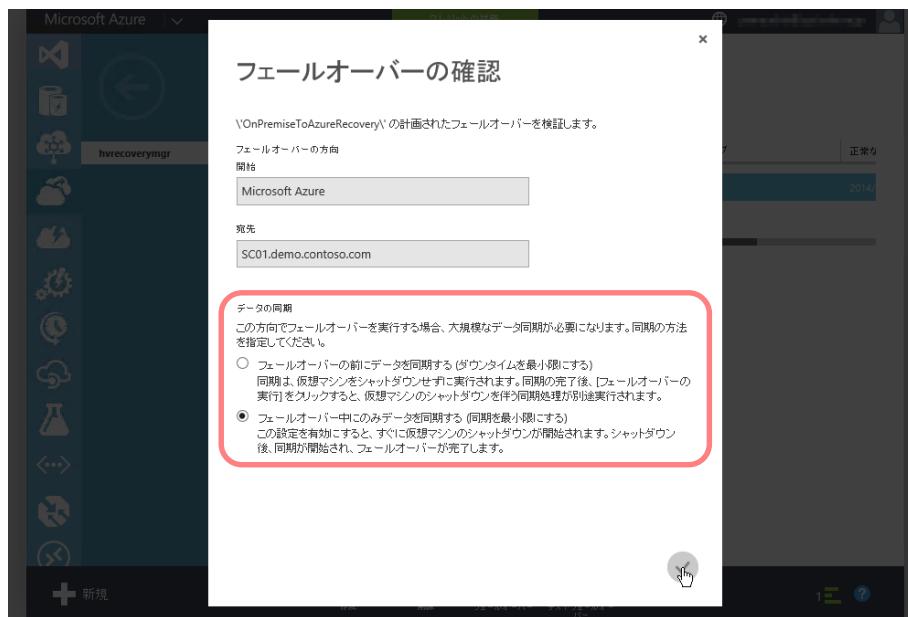
計画されたフェールオーバー、または計画されていないフェールオーバーを実行し、Microsoft Azure 側の仮想マシンに切り替えた場合は、逆方向の計画されたフェールオーバー（フェールバック）を実行することで、通常の運用形態に戻すことができます。

フェールバックを実行するには、次の手順で操作します。

1. Azure Site Recovery ポータルで仮想マシンまたは復旧計画を選択し、ページ下部の [フェールオーバー] をポイントし、[計画されたフェールオーバー] をクリックします。このとき、[計画されていないフェールオーバー] は選択できないようにグレー アウト表示になっています。



2. [フェールオーバーの確認] ダイアログ ボックスが表示されます。フェールオーバーの方向が Microsoft Azure からオンプレミスになっていることを確認し、データの同期方法を選択して OK ボタン (✓) をクリックします。データの同期方法としては、[フェールオーバーの前にデータを同期する (ダウンタイムを最小限にする)] と [フェールオーバー中にのみデータを同期する (同期を最小限にする)] のいずれかを選択します。



フェールオーバーの前にデータを同期する (ダウンタイムを最小限にする) … フェールオーバーを実行する前に、レプリケーションを反転させ、Microsoft Azure 側で仮想マシンを実行中のままレプリケーションを行い、レプリケーションされていないデータを最小限にしたうえで、ユーザーの対話指示によりフェールオーバーを開始します。

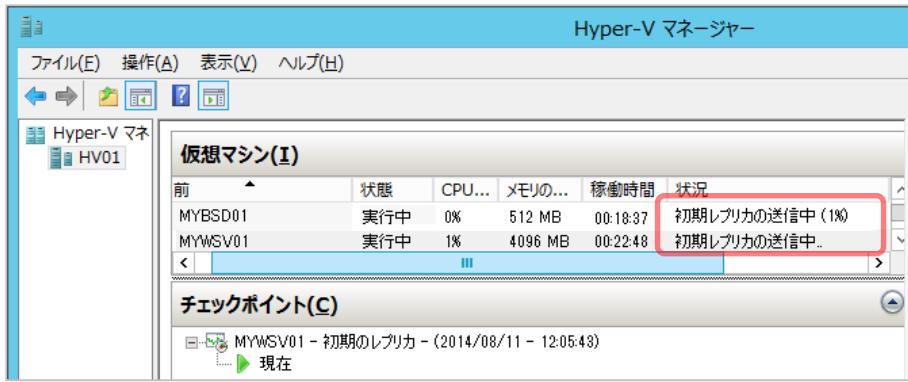
フェールオーバー中にのみデータを同期する（同期を最小限にする）… すぐに仮想マシンのシャットダウンを開始し、レプリケーションを反転させ、同期したあと、フェールオーバーの処理を開始します。

3. 計画されたフェールオーバーのジョブが完了すると、[コミット待機中] の状態になるので、[コミット] をクリックしてフェールオーバーを完了します。この時点で Microsoft Azure 側の仮想マシンは完全に削除され、課金対象外になります。

4. フェールバック操作の場合は、コミットが完了すると、次に [レプリケーションの反転 待機中] の状態になります。[レプリケーションの反転] をクリックして、待機中の状態を解消します。なお、[レプリケーションの反転 待機中] の状態でも、実際にはレプリケーションはオンプレミスから Microsoft Azure の方向に既に切り替わっています。[レプリケーションの反転] を完了することで、次のフェールオーバーの準備完了の状態に切り替わります。

Note : フェールバック後は初期レプリケーションから

フェールバックが完了し、レプリケーションがオンプレミスから Microsoft Azure への方向に戻ると、初期レプリカの送信が始まります。初期レプリケーションには大量のデータ送信が必要になるため、再びフェールオーバーの準備が整うには、仮想マシンの保護を有効化したときと同等の時間を要します。



STEP 4. サービスの利用停止

この STEP では、Azure Site Recovery によるオンプレミスから Azure のサイト間保護を無効化し、評価環境をクリーンアップする手順について説明します。

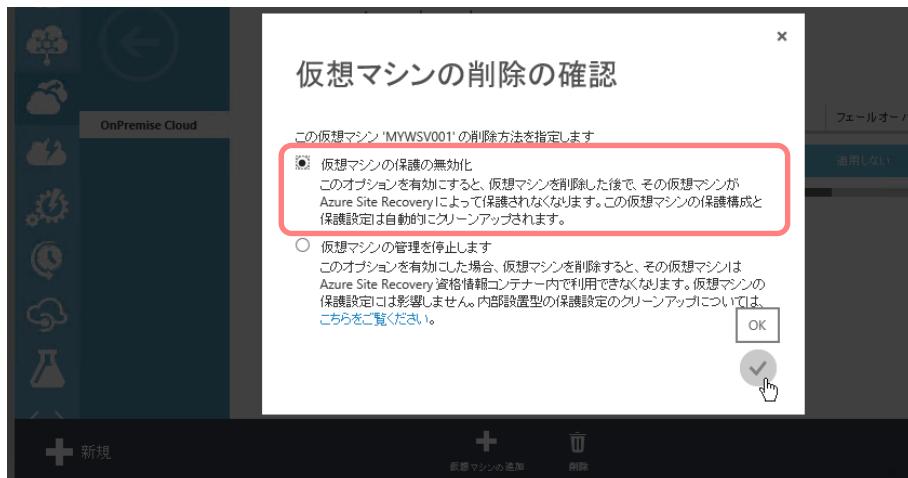
この STEP では、次のことを学習します。

- ✓ 仮想マシンの保護の無効化
- ✓ クラウドの保護の解除
- ✓ サーバーの登録解除
- ✓ Azure Site Recovery サービスの利用停止

4.1 仮想マシンの保護の無効化

Azure Site Recovery のサービスの利用を完全に終了するには、仮想マシンの保護の無効化、クラウドの保護の解除、サーバーの登録解除の順番で操作します。

仮想マシンの保護を無効化するには、Azure Site Recovery ポータルの【保護された項目】の【仮想マシン】ページを開き、仮想マシンを選択してページ下部の【削除】をクリックします。【仮想マシンの削除の確認】ダイアログ ボックスが表示されるので、【仮想マシンの保護の無効化】を選択し、OK ボタン (✓) をクリックします。



保護を構成した VMM クラウドのすべての仮想マシンについて、保護を削除し、「クラウド内に、保護が有効になっている仮想マシンがありません」と表示される状態にします。

Note : VMM 管理サーバー側での仮想マシンの保護のクリーンアップ

【仮想マシンの削除の確認】の【仮想マシンの管理を停止します】は、通常、オンプレミスの VMM クラウドが利用できないとき、つまり VMM 管理サーバーが Azure Site Recovery のサービスに接続されていない状態のときに選択します。

【仮想マシンの管理を停止します】を選択した場合は、VMM クラウドが利用可能になり次第、次の手順で VMM 管理サーバー側の保護設定をクリーン アップしてください。

1. VMM 管理サーバーで次の Windows PowerShell スクリプトを実行し、仮想マシンの保護設定を無効化します。

```
$vm = get-scvirtualmachine -Name "仮想マシン名"
Set-SCVirtualMachine -VM $vm -ClearDRProtection
```

2. VMM 管理サーバーまたは仮想マシンが存在する Hyper-V ホストで次の Windows PowerShell スクリプトを実行し、Hyper-V レプリカの設定を無効化します。

```
$vmName = "仮想マシン名"
$hostName = "Hyper-V ホストの FQDN";
$vm = Get-WmiObject -Namespace $namespace -Query "Select * From
MsVm_ComputerSystem Where ElementName = '$vmName'" -computername $hostName
$replicationService = Get-WmiObject -Namespace "root\virtualization\v2"
-Query "Select * From MsVm_ReplicationService" -computername $hostName
$replicationService.RemoveReplicationRelationship($vm.__PATH);
```

4.2 クラウドの保護の解除

保護された仮想マシンが存在しない状態になったら、VMM クラウドの保護を無効化します。Azure Site Recovery ポータルの [保護された項目] ページを開き、VMM クラウドを選択した状態でページ下部の [保護の解除] をクリックします。確認メッセージに [はい] と答えて、VMM クラウドの保護を無効化します。



4.3 サーバーの登録解除

クラウドの保護を解除したら、Azure Site Recovery ポータルの [リソース] にある [サーバー] ページを開き、VMM 管理サーバーを選択して、ページ下部の [削除] をクリックします。[削除の確認] ダイアログ ボックスが開くので、サーバーを登録解除する理由を一覧から選択し、OK ボタン (✓) をクリックします。



Azure Site Recovery 資格情報コンテナーから VMM 管理サーバーの登録を削除できたら、VMM 管理サーバーから Azure Site Recovery プロバイダーをアンインストールできます。また、Azure Recovery Services エージェントを展開した Hyper-V ホストから、エージェントをアンインストールできます。

Note : VMM 管理サーバーが接続されていない状態でサーバーの登録を解除した場合

VMM 管理サーバーが Azure Site Recovery のサービスに接続されていない状態で Azure Site Recovery ポータルからサーバーを削除した場合は、以下のスクリプトを使用することで Virtual Machine Manager の管理サーバー側の設定をクリーン アップできます。

Cleanup Script for Windows Azure Hyper-V Recovery Manager customers

<http://go.microsoft.com/fwlink/?LinkId=389878>

4.4 クラウド サービスの削除

この時点で、Azure Site Recovery で利用していた Azure Site Recovery 資格情報コンテナー、ストレージ アカウント、および仮想ネットワークの各サービスを Microsoft Azure 側からは削除できます。

Microsoft Azure 管理ポータルで各サービスのワークスペースを開き、不要になったサービスを削除してください。なお、作成済みのストレージ アカウントおよび仮想ネットワークは、Azure Site Recovery 以外の目的にも利用可能であるため、再利用のために残しておくことも可能です。

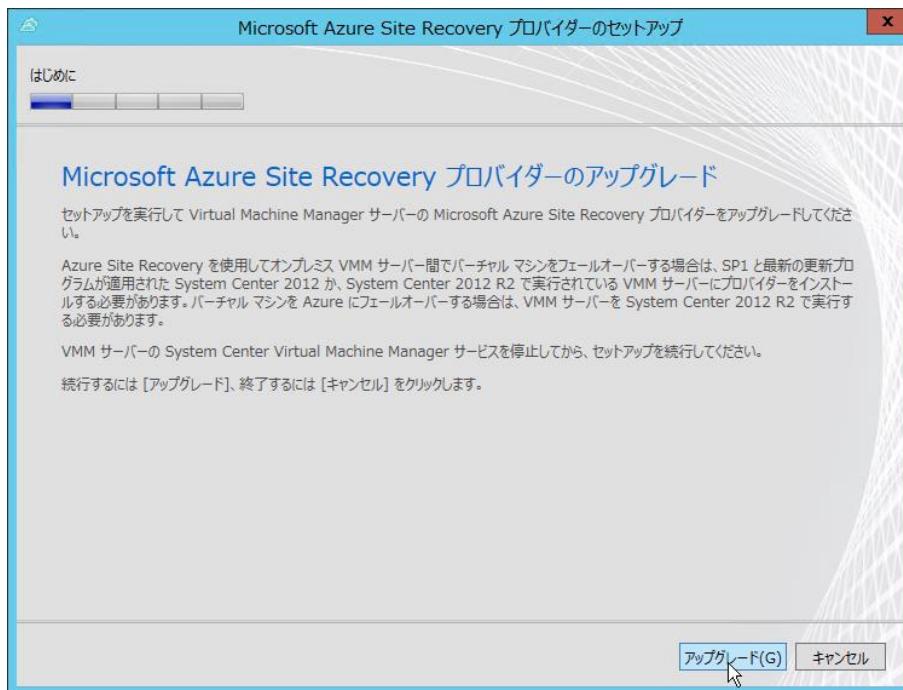


オンプレミスから Azure のサイト回復の FAQ

➔ サービスの導入に関する FAQ

Q. Hyper-V Recovery Manager で構築した保護設定を Azure Site Recovery に移行できますか？

はい。 2014 年 6 月の Azure Site Recovery 提供開始以前に構成されたお客様の保護設定は、自動的に Azure Site Recovery に移行されます。ただし、Virtual Machine Manager の管理サーバーの Microsoft Azure Site Recovery プロバイダーをアップグレードする必要があります。ご利用の環境でアップグレードが必要な場合は、Azure Site Recovery ポータルに通知されます。



Q. オンプレミスからオンプレミスのサイト回復を、オンプレミスから Azure のサイト回復に切り替えることはできますか？

はい。 Azure Site Recovery ポータルを使用して、現在のすべての仮想マシンの保護を削除し、クラウドの保護を解除したあと、クラウドの保護を再設定してください。なお、オンプレミスから Azure のサイト回復のためには、Hyper-V ホストに Azure Recovery Services エージェントを導入する必要があります。また、オンプレミスからオンプレミスのサイト回復でサポートされる、System Center 2012 SP1 Virtual Machine Manager および Windows Server 2012 Hyper-V は、オンプレミスから Azure のサイト回復ではサポートされないことに注意してください。オンプレミスから Azure のサイト回復のためには、System Center 2012 R2 Virtual Machine Manager および Windows Server 2012 R2 Hyper-V ベースの仮想化インフラストラクチャが必要です。

Q. クラウドの保護の構成がエラーで失敗します

Azure Site Recovery ポータルの [ジョブ] ページで、「クラウド名（保護の構成）」ジョブを開き、

エラーの詳細を確認してください。

Virtual Machine Manager の管理コンソールで保護対象のクラウドのプロパティを開き、機能プロファイルとして [Hyper-V] が選択されていることを確認してください。この設定が無いと、保護の構成に失敗します。また、保護対象のクラウドに関連付いたホスト グループに、停止中または存在しない Hyper-V ホストが存在する場合も失敗する場合があるので、ホスト グループから除外（別のホスト グループに移動するか、ホストを削除）してください。

Q. クラウドの保護の構成で保存データの暗号化をオンにできません

VMM 管理サーバーで Azure Site Recovery プロバイダー (VMMASRProvider_x64.exe) を再実行し、[データの暗号化] ページで [レプリケートされたデータを暗号化する] オプションをチェックして、暗号証明書を生成、保存してください。その後、クラウドの保護設定をいったん解除し、再設定してください。



Q. 仮想マシンの保護が有効化されません

Azure Site Recovery ポータルの [ジョブ] ページで、「仮想マシン名 (保護を有効にする)」ジョブを開き、エラーの詳細を確認してください。

仮想マシンのハードウェア構成が [サポートされる構成](#)であること、Virtual Machine Manager 管理コンソールで仮想マシンのプロパティを開き、[全般] ページの [オペレーティング システム] にサポート対象のゲスト OS の種類が設定されていること、[ハードウェア構成] ページで IDE デバイスに接続された OS 用のディスクで [バーチャル マシン用のオペレーティング システムを含む] がチェックされていることを確認してください。

Q. Hyper-V ホストはインターネットと通信できる必要がありますか？

はい。 Azure Site Recovery のオンプレミスから Azure のサイト回復では、Hyper-V ホストと Azure ストレージ間のレプリケーションのために、インターネットに対して出力方向の HTTPS トランザクションが発生します。Hyper-V ホストがインターネットと通信するためにプロキシ サーバーを経由する必要がある場合は、Azure Recovery Services エージェントでプロキシ サーバーを構成してください。Azure Recovery Services エージェントは、Azure Backup サービスと共に構成されており、エージェントのインストールで Hyper-V ホストのデスクトップに追加される [Microsoft Azure Backup] コンソールを使用して、プロキシ サーバーを構成することができます。

Q. Azure Site Recovery の導入やトラブルシューティングについて無料で質問できるところ

ろはありますか？

はい。以下の TechNet フォーラムまたは MSDN フォーラムを無料でご利用いただけます。

TechNet forums - Microsoft Azure Site Recovery

<http://social.technet.microsoft.com/Forums/en-US/home?forum=hypervrecovmgr>

Msdn forums - Microsoft Azure Site Recovery

<http://social.msdn.microsoft.com/Forums/windowsazure/en-US/home?forum=hypervrecovmgr>

▼ サービスの課金に関する FAQ

Q. Microsoft Azure にフェールオーバーした仮想マシンの実行は、Azure Site Recovery の料金に含まれますか？

いいえ。 Azure Site Recovery の料金は、保護対象の仮想マシンの数に対して課金されます。レプリケーションのためのデータ転送 (Azure 側から見た受信方向へのデータ転送は無料) やストレージ使用、フェールオーバー時に使用した Microsoft Azure 仮想マシンおよび Microsoft Azure 仮想ネットワークは、その使用量に応じて通常の従量課金制プランのレートに基づいて課金されます。

Q. 1 か月の途中で仮想マシンの保護を停止した場合、1 か月ぶん課金されますか？

いいえ。 Azure Site Recovery は、保護する仮想マシンの 1 か月における 1 日あたりの平均数を 1 単位として課金されます。例えば、月の前半はずっと 20 台の仮想マシンを保護し、後半は 1 台も保護しなかった場合、その月の保護する仮想マシンの平均数は 1 日あたり 10 台であり、その月は 10 台ぶんの使用量を課金されます。

Q. Azure Site Recovery サブスクリプション ライセンスの購入は必須ですか？

いいえ。 Azure Site Recovery のサービスを利用するため、Azure Site Recovery サブスクリプションを購入は必須ではありません。ただしその場合、オンプレミスから Azure のサイト回復において、Azure Site Recovery の仮想マシンごとの通常料金に加えて、ストレージ、ストレージ トランザクション、データ転送 (Azure 側からの送信方向) に通常の従量課金制プランのレートに基づいて課金されます。

保護対象の仮想マシンのインスタンスごとに Azure Site Recovery サブスクリプションを購入してある場合は、その仮想マシン 1 か月あたり、100 GB までのストレージ、ストレージ トランザクション、およびデータ転送 (Azure 側からの送信方向) を追加コストなしで利用できます。また、InMage Scout ソフトウェアの使用権も提供されます。なお、100 GB を超える利用については、通常の従量課金レートで課金されます。

Q. Microsoft Azure の 1 か月無料試用版で評価しようと考えています。無料枠を使い切った場合、課金されますか？

いいえ。 Microsoft Azure 1 か月無料評価版では 20,500 円相当（2014 年 9 月時点、金額は変更される場合があります）のクレジットが無料で提供され、さらにクレジットを超えないように使用制限が設けられています。そのため、無料評価期間中に課金され、登録されたクレジットカードに請求されることはありません。使用制限を使いきってしまった場合、サブスクリプションは中断され、無料評価の残りの期間のサービスは無効化されます。サブスクリプションを従量課金制プランにアップグレードすることで、サブスクリプションを再有効化することができます。



◆ サービスの詳細に関する FAQ

Q. 保護できる仮想マシンの数に上限はありますか？

Azure Site Recovery には制限はありませんが、以下のドキュメントで説明されている Microsoft Azure のサブスクリプションの上限、および Azure Site Recovery に関するサービス（ストレージ、データ転送、仮想マシン、仮想ネットワーク）の上限に従います。

Azure Subscription and Service Limits, Quotas, and Constraints

<http://azure.microsoft.com/en-us/documentation/articles/azure-subscription-service-limits/>

Q. フェールオーバーした仮想マシンを日本リージョンで実行することはできますか？

はい。 Azure Site Recovery 資格情報コンテナー、ストレージ アカウント、および仮想ネットワークを、すべて [東日本] または [西日本] リージョンを指定して作成してください。

Q. フェールバック後に Microsoft Azure 仮想マシンは自動で削除されますか？

はい。 フェールオーバー時に作成された Microsoft Azure 仮想マシンは、フェールバック時に自動的に削除されます。このため、平常運用時に Microsoft Azure 仮想マシンのために課金されることはありません。

Q. 第 2 世代仮想マシンの保護はサポートされますか？

いいえ。 オンプレミスから Azure のサイト回復は、Windows Server 2012 R2 Hyper-V の第 2 世代仮想マシンの保護をサポートしていません。オンプレミスからオンプレミスのサイト回復では、第 2 世代仮想マシンの保護もサポートされます。

Q. 容量可変、差分ディスク、VHDX はサポートされますか？

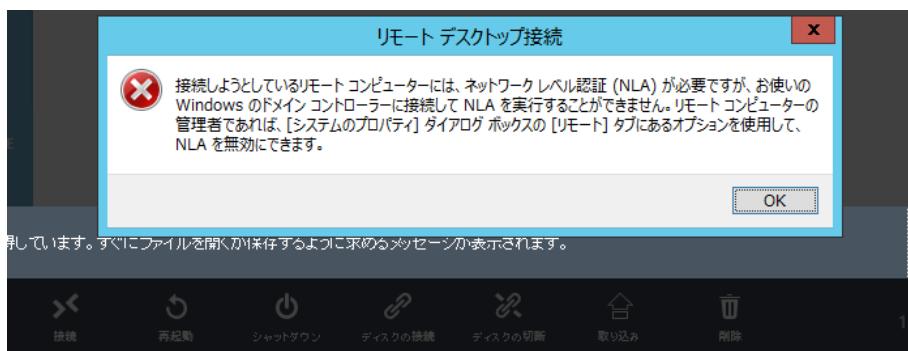
はい。通常の Microsoft Azure 仮想マシンでは、VHD 形式の容量固定タイプの仮想ハード ディスクを使用する必要がありますが、Azure Site Recovery で保護される仮想マシンでは、VHD と VHDX の両方のファイル形式、および容量固定、容量可変、差分のすべてのタイプの使用がサポートされ、フェールオーバー先の Microsoft Azure 仮想マシンでも使用できます。

Q. 保護される仮想マシンのゲスト OS に Microsoft Azure 仮想マシン用の VM エージェントや Azure Linux エージェントを組み込む必要はありますか？

いいえ。Microsoft Azure 仮想マシンの Windows 仮想マシン用の VM エージェントや、Linux 仮想マシン用の Azure Linux エージェント (waagent) は必要ありません。仮想マシンのゲスト OS には、Hyper-V 環境で動作させるための Hyper-V 統合サービスが組み込まれていれば十分です。Hyper-V 統合サービスは、Microsoft Azure 側での仮想マシンのデバイスの認識やシャットダウン操作に使用されます。つまり、[Azure Site Recovery のサポート対象のゲスト OS](#) を実行し、[Azure Site Recovery でサポートされる構成の仮想マシン](#)であれば、オンプレミスの Hyper-V で運用中の Windows 仮想マシンまたは Linux 仮想マシンをそのまま Azure Site Recovery で保護することができます。

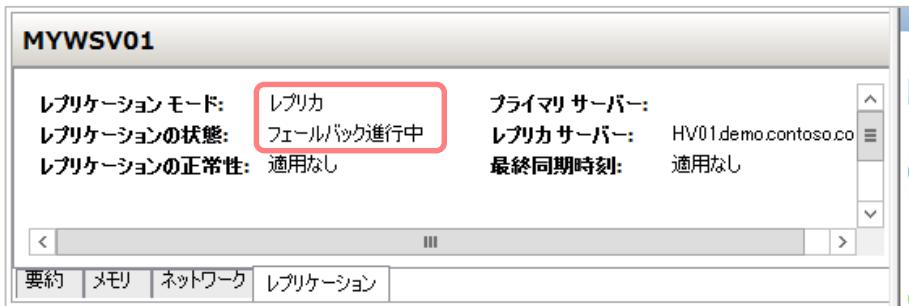
Q. フェールオーバーした仮想マシンに接続しようとすると、ネットワーク レベル認証 (NLA) が必要と言われ、接続できません

テスト フェールオーバーで作成された仮想マシンは企業ネットワークに接続されないため、ドメイン アカウントの資格情報での接続はネットワーク レベル認証 (NLA) の影響で拒否されます。ローカル管理者アカウント（コンピューター名¥Administrator）の資格情報を指定してログオンしてください。あるいは、リモート デスクトップの設定でネットワーク レベル認証 (NLA) を要求しないように構成してください。



Q. 計画されたフェールオーバーを実行しても Hyper-V 側の仮想マシンはプライマリのままなのですか？

フェールオーバー後にレプリケーションの反転は行われません。次に Azure からオンプレミス方向の計画されたフェールオーバー（フェールバック）を実行する際の処理の一部としてレプリケーションが反転され、変更の同期が行われます。



Q. 計画されたまたは計画されてないフェールオーバーを実行後、コミットせずキャンセルすることはできますか？

いいえ。仮想マシンや復旧計画の計画されたまたは計画されていないフェールオーバーを開始し、“コミット待機中”の状態にある場合、コミットせずにフェールオーバーをキャンセルするということはできません。実行済みのフェールオーバーを取り消したい場合は、仮想マシンの保護をいつたん削除し、仮想マシンの保護を再度有効化して、初期レプリケーションからやり直してください。

なお、Azure 側で仮想マシンがアクティブな状態で保護を削除すると、Azure 側の仮想マシンが実行中のまま残ってしまいます。無駄に課金されてしまうことを避けるため、不要になった Azure 側の仮想マシンは接続されたディスクとともに手動で削除してください。

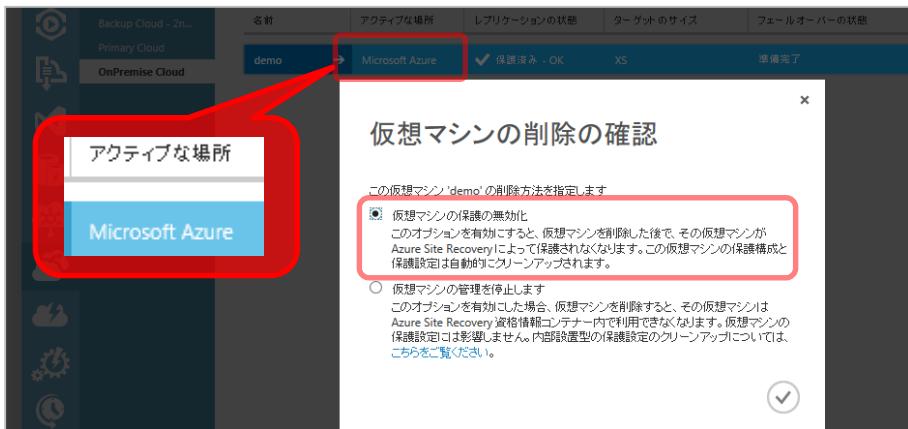


Q. 復旧計画でスクリプトを自動実行させることはできますか？

はい。2014 年 9 月 12 日 (日本時間) より、オンプレミスから Azure への復旧計画において、Azure Automation (プレビュー) との統合によるスクリプト実行機能が追加されました。この機能を利用するには、スクリプトとして実行する Runbook を含む Azure Automation (プレビュー) アカウントが必要です。

Q. Hyper-V 仮想マシンを Azure に移行するために Azure Site Recovery を利用できますか？

はい。オンプレミスの仮想マシンの Azure へのマイグレーションは、Azure Site Recovery の利用シナリオの 1 つです。Azure に仮想マシンをフェールオーバーした後に Azure Site Recovery から仮想マシンを削除（仮想マシンの保護の無効化）すると、フェールオーバー時に作成された Azure 仮想マシンを引き続き Azure 側で利用できます。



Q. 仮想マシンのゲスト OS およびソフトウェアのライセンスについて考慮点はありますか？

はい。 保護される仮想マシンにインストールされているすべてのライセンス ソフトウェアについて、バックアップ コピーの作成やパブリック クラウドへのインスタンスの移動が許可されているかどうか、許可されていない場合は追加のライセンスを購入する必要があるかどうかを確認してください。

Windows Server を Microsoft Azure 仮想マシン環境で実行するためのライセンス料（サーバーライセンスおよび Windows Server CAL）は、Windows 仮想マシンの分単位の料金に含まれるため考慮する必要はありません。その他の Microsoft サーバー ソフトウェアについては、Microsoft サーバー ソフトウェアおよび関連するクライアント アクセス ライセンス (CAL) のソフトウェア アシュアランス (SA) を保有されるお客様は、SA 特典として障害復旧用のコード バックアップ サーバー ライセンスを無料で利用できため、復旧用イメージのために追加の サーバー ライセンスの購入は不要です。

仮想マシンのライセンス FAQ

<http://azure.microsoft.com/ja-jp/pricing/licensing-faq/>

ライセンス簡易ガイド 障害復旧用ライセンス - Microsoft ソフトウェア アシュアランスの特典

http://download.microsoft.com/download/5/8/f/58fce148-01d7-457d-9a8b-52df61fb27ba/Brief_DisasterRecovery.pdf

おわりに

Azure Site Recovery は、自社でセカンダリ サイトを用意するのに比べて、少ないコストで導入できる DR 対策ソリューションです。パブリック クラウドは、DR 対策に必要な地理的な条件を満たす上、設備やハードウェアへの初期投資が不要であり、使用量に対して支払う従量課金制であるため無駄なコストが発生しないというメリットがあります。DR 対策が喫緊の課題であると認識しながら、DR 対策用のセカンダリ サイトを準備するまで手が回らないという企業であっても、Azure Site Recovery ならコストをかけずにすぐに DR 対策を開始できます。

➔ 評価版の入手

評価版のダウンロード: Windows Server 2012 R2

<http://technet.microsoft.com/ja-jp/evalcenter/dn205286.aspx>

評価版のダウンロード: System Center 2012 R2

<http://technet.microsoft.com/ja-JP/evalcenter/dn205295>

SQL Server 2012 Evaluation 180 日評価版のダウンロード

<http://www.microsoft.com/ja-jp/download/details.aspx?id=29066>

Microsoft Azure 1 か月無料評価版のサインアップ

<http://azure.microsoft.com/ja-jp/pricing/free-trial/>

➔ 評価ドキュメント

Microsoft Azure Site Recovery のドキュメント ページ

<http://azure.microsoft.com/ja-jp/documentation/services/site-recovery/>

Microsoft Azure Site Recovery に関する MSDN ドキュメント

<http://msdn.microsoft.com/en-us/library/dn440569.aspx>

Virtual Machine Manager に関する MSDN ドキュメント

<http://technet.microsoft.com/en-us/library/gg610610.aspx>

➔ ユーザー フォーラム

TechNet forums - Microsoft Azure Site Recovery

<http://social.technet.microsoft.com/Forums/en-US/home?forum=hypervrecovmgr>

Msdn forums - Microsoft Azure Site Recovery

<http://social.msdn.microsoft.com/Forums/windowsazure/en-US/home?forum=hypervrecovmgr>