Microsoft

Microsoft Azure

Azure Site Recovery を利用した オンプレミスから Azure のサイト回復

目次

- Azure Site Recovery の概要
- サービスの価格
- オンプレミスから Azure のサイト回復 システム要件
- オンプレミスから Azure のサイト回復 導入手順
- フェールオーバーの管理

Microsoft Azure の全体像と Azure Site Recovery

世界規模のクラウド基盤

サーバー/ ネットワーク/ データセンター

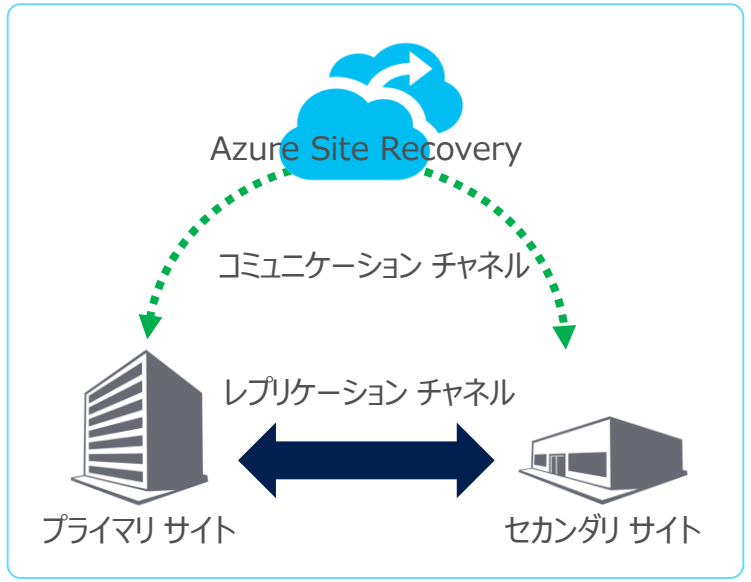
- 高度な自動化
- 柔軟性
- 統合リソース管理
- 従量課金

北米4カ所、ヨーロッパ2カ所、アジア2カ所、日本2カ所
豪州2カ所 + CDN 24 カ所

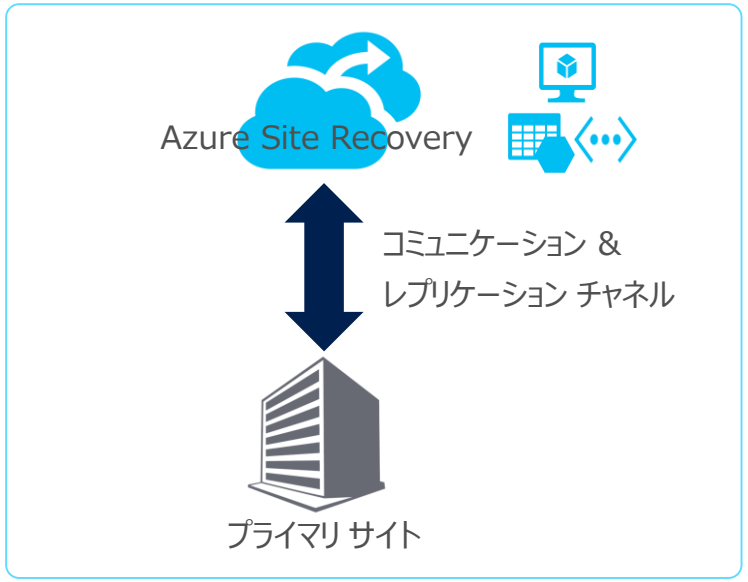
Azure Site Recovery の概要

Azure Site Recovery とは？

- Hyper-V レプリカを利用した Virtual Machine Manager (VMM) クラウドの障害・災害復旧 (ディザスタ リカバリ: DR) 機能をサービスとしてパブリック クラウドから提供
- オンプレミスのサイト間、またはオンプレミスと Azure 間で保護
- 最短 30 秒以下の RPO (目標復旧時点) を提供
- ワン クリック フェールオーバー
- 東日本・西日本リージョンからのサービス提供開始 (2014 年 8 月 22 日より)
- InMage Scount の提供開始 (2014 年 8 月 1 日より)



オンプレミスからオンプレミス

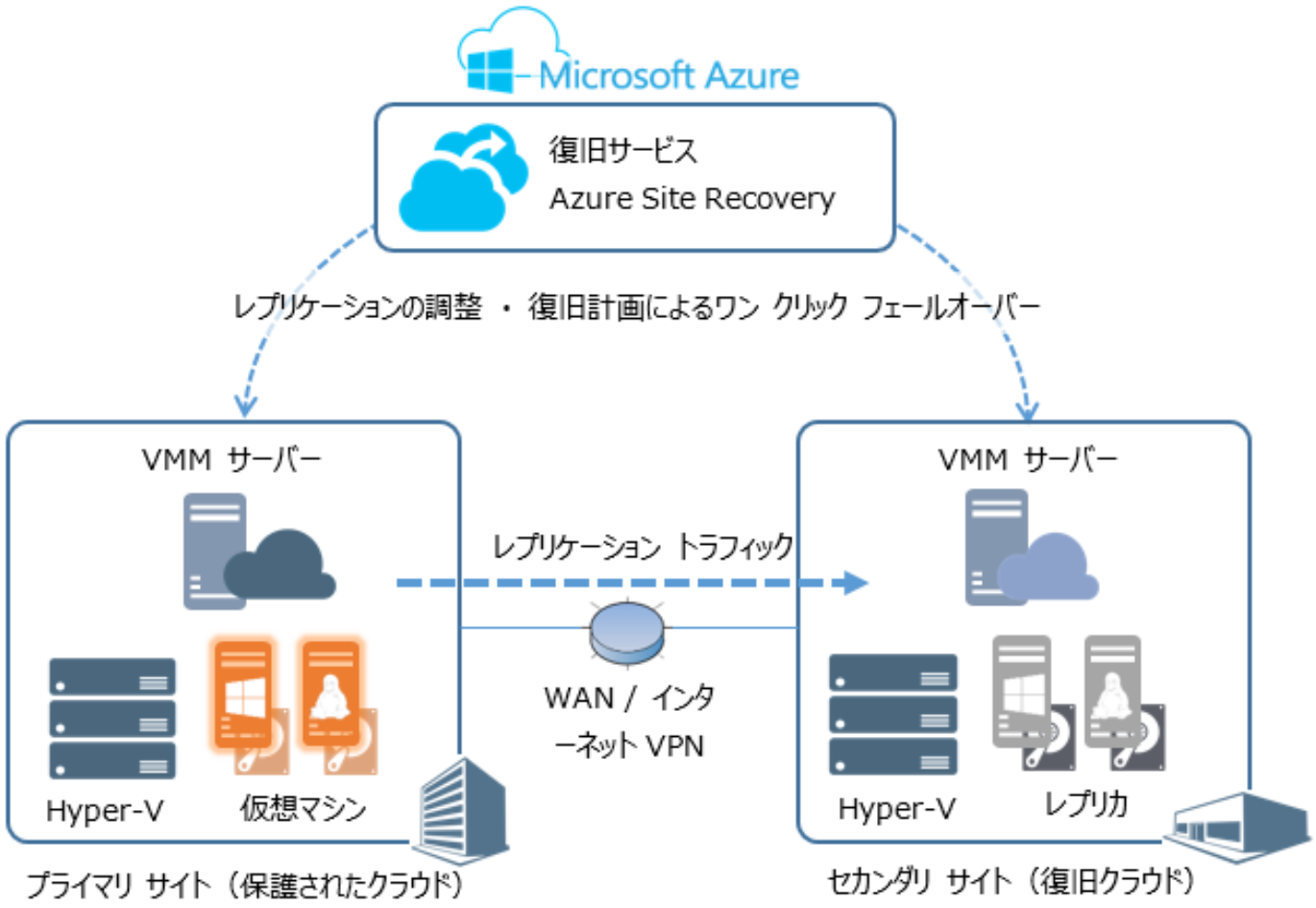


オンプレミスから Azure

Microsoft Azure

オンプレミスからオンプレミスのサイト回復

- Hyper-V Recovery Manager からの機能 (2014 年 1 月に GA)
- Virtual Machine Manager (VMM) の 2 拠点のクラウド間でレプリケーションを構成*
- 復旧計画によるワン クリック フェールオーバー、スクリプトの自動実行をサポート
- System Center 2012 SP1 以降の VMM クラウドおよび Windows Server 2012 以降の Hyper-V をサポート

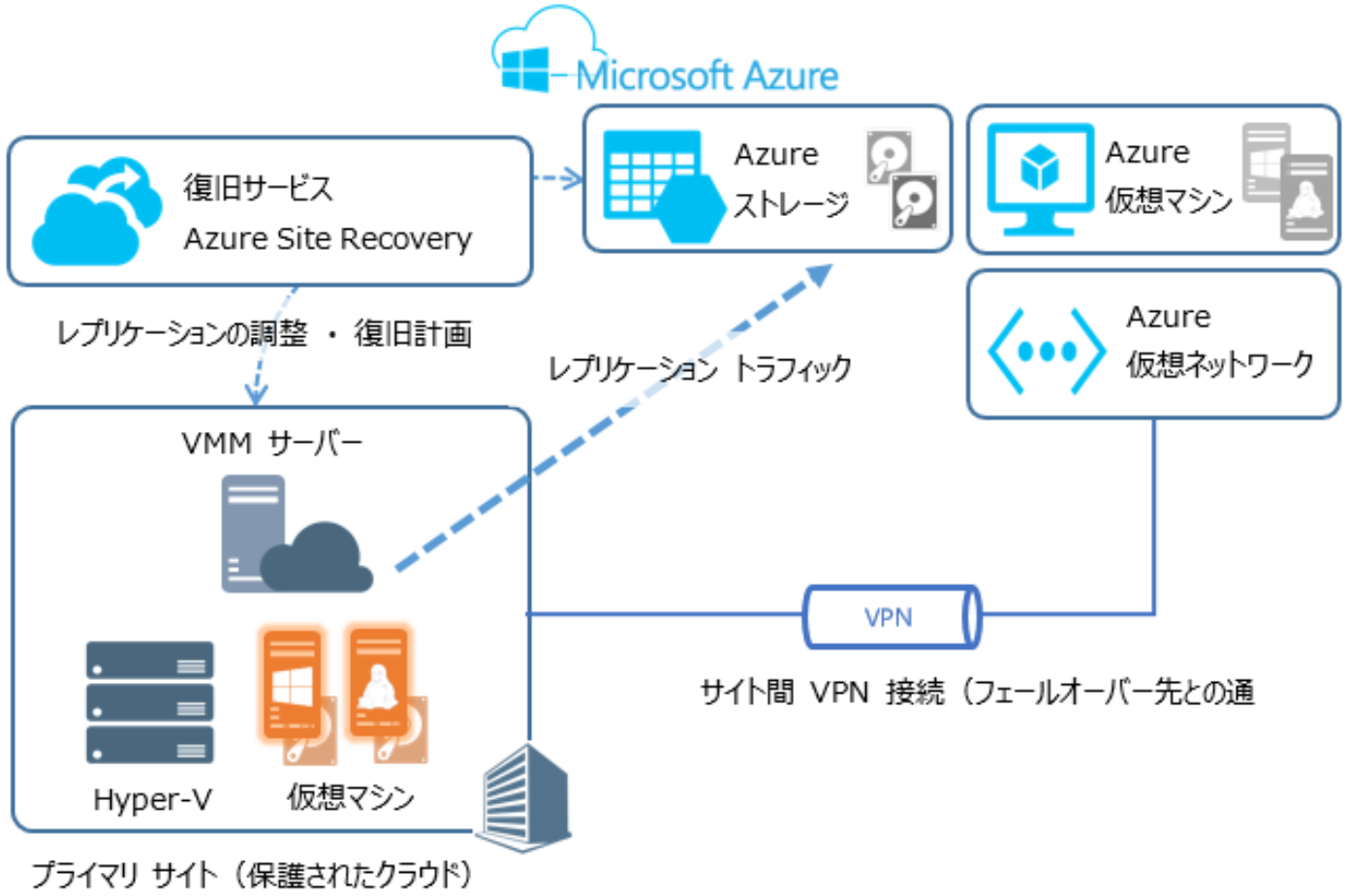


* 1 拠点で構成することも可能だが、その場合、VMM 管理環境を復旧するために余計に復旧時間がかかる場合がある

Microsoft Azure

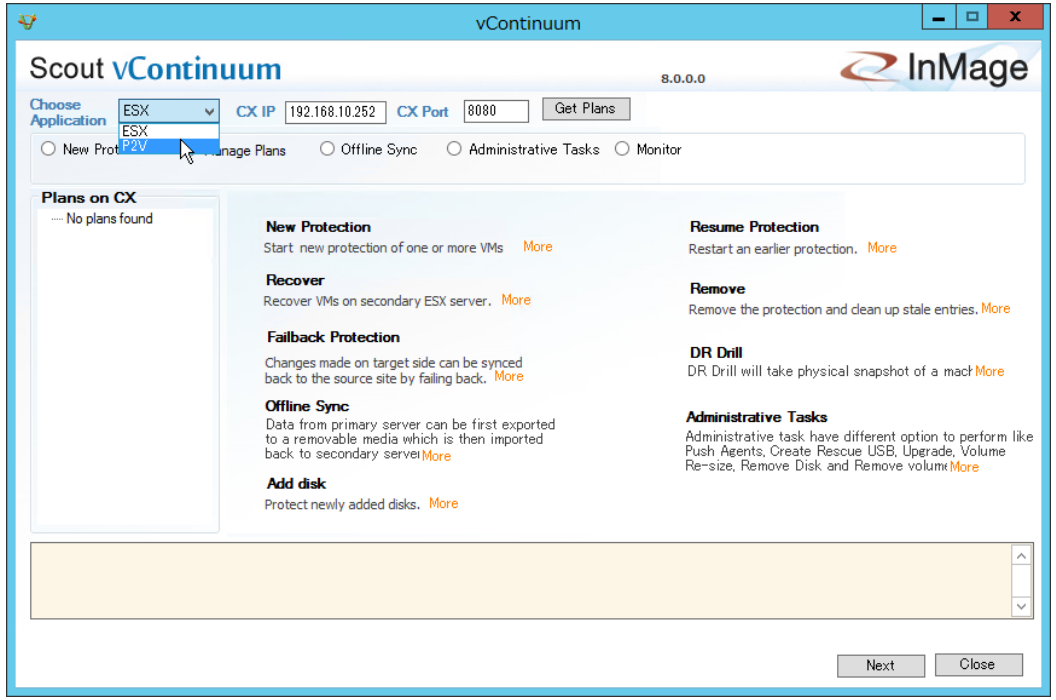
オンプレミスから Azure のサイト回復

- オンプレミスの VMM クラウドから Azure に対してレプリケーションを行う展開方法 (2014 年 6 月にプレビュー開始、近日 GA)
- DR 用のセカンダリ サイトは不要
- レプリケーション先およびフェールオーバー後の仮想マシンの実行環境として Azure の IaaS を利用
- HTTPS の暗号化＋お客様管理の暗号化キーによるレプリケーション データの暗号化
- System Center 2012 R2 の VMM クラウドおよび Windows Server 2012 R2 の Hyper-V をサポート



VMware サイトの保護 (InMage Scout)

- マイクロソフトが買収した InMage Systems 社の InMage Scount ソフトウェアを使用した、オンプレミスのサイト間での DR およびバックアップ ソリューション
- VMware 仮想マシン、物理マシン、Windows、Linux のヘテロジニアス環境をセカンダリ サイトの VMware vSphere ESX クラウド上に V2V または P2V で保護
- 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
- 現状、Azure Site Recovery とのサービス連携はなし
- Microsoft Migration Accelerator による Azure へのマイグレーションに対応 (2014 年 9 月より限定プレビュー開始)



Migration Accelerator Preview

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

Microsoft Azure

サービスの価格

Azure Site Recovery の価格

従量課金制プランでの提供

- 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
- 月額の料金は、保護される仮想マシンの 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

  例: 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。

- オンプレミスとオンプレミスのサイト回復と、オンプレミスと Azure のサイト回復では、保護される仮想マシンあたりの月額単価が異なる

Azure Site Recovery 料金の詳細
http://azure.microsoft.com/ja-jp/pricing/details/site-recovery/

オンプレミスから Azure のサイト回復におけるその他の課金

Azure ストレージに対する課金

- レプリケーション データの格納に使用されるストレージ領域およびストレージ トランザクションに対する従量課金

データ転送に対する課金

- Azure 側からの送信データに対する従量課金。Azure へのレプリケーション方向には課金されない

Azure 仮想マシンに対する課金

- フェールオーバー時に作成される Azure 仮想マシンに対する従量課金。ゲスト OS の種類 (Windows または Linux) やインスタンス サイズに応じて価格が異なる。Azure に対してフェールオーバーしない限り課金は発生しない

Azure 仮想ネットワークに対する課金

- オンプレミスのネットワークとのサイト間 VPN 接続に使用されるアクティブなゲートウェイに対する従量課金

Azure Site Recovery サブスクリプション

- 2014 年 8 月 1 日より Microsoft Enterprise Agreement (EA) を通じて提供
- 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利用枠を提供
- 仮想マシンあたり 100 GB/月を超過した分は通常の課金レートにて従量課金
- InMage Scount ソフトウェアを使用して VMware 仮想マシンおよび物理サーバーを保護する権利を提供

オンプレミスから Azure のサイト回復 システム要件

※注意: オンプレミスのサイト間のサイト回復とは要件が異なります。

Azure 側のサービスの要件

Azure Site Recovery 資格情報コンテナー

- Azure Site Recovery を提供する 8 か所のリージョンから選択
- 日本国内で利用する場合は、東日本または西日本リージョンを選択することでネットワーク遅延の影響を最小化

Azure 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ストレージ アカウントを事前に準備
- ジオ (主要地域) 冗長が必須。東日本と西日本のペアによるジオ冗長が可能

Azure 仮想ネットワーク

- Azure Site Recovery 資格情報コンテナーと同じリージョンに事前に作成し、オンプレミスとサイト間 VPN 接続を構成しておく

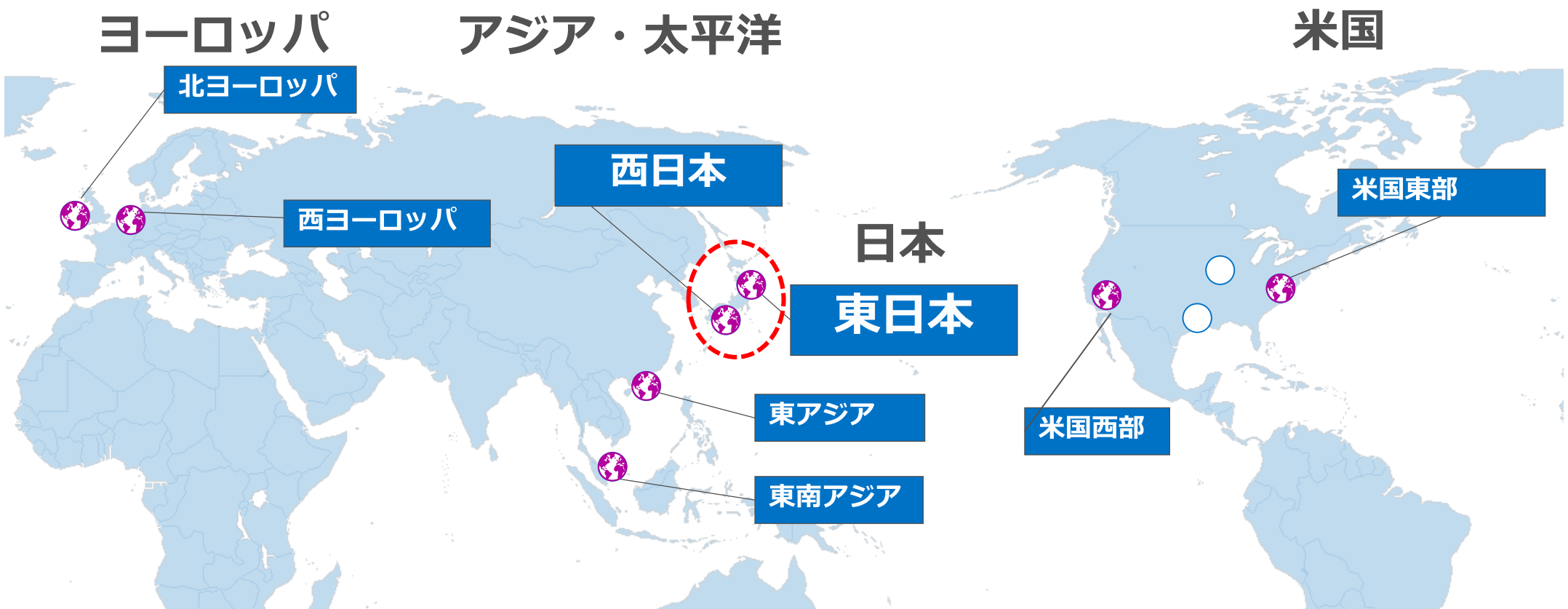
Azure 仮想マシン

- Azure へのフェールオーバー実行時に自動作成。事前準備不要

※ すべて Microsoft Azure 1 か月無料評価版の枠内で評価可能

Microsoft Azure

世界 8 か所のリージョンからサービス提供



- 2014 年 9 月現在、東日本・西日本を含む世界 8 か所のリージョンからサービスを提供中
- オンプレミスから Azure のサイト回復に必要なジオ (主要地域) 冗長ストレージ、Azure 仮想マシン、Azure 仮想ネットワークも、東日本・西日本リージョンだけで構成可能

Microsoft Azure

VMM クラウドの要件

Virtual Machine Manager

- オンプレミス側には System Center 2012 R2 Virtual Machine Manager の管理サーバーで管理される VMM クラウドが必要
- VMM クラウドの機能プロファイルで「Hyper-V」が有効になっていること
- 直接またはプロキシ サーバーを介してインターネットと HTTPS (出力方向)で通信できること

Hyper-V ホスト

- VMM クラウドは、Windows Server 2012 R2 の Hyper-V ホストまたは Hyper-V ホスト クラスターで構成されていること
- Server Core インストールをサポート (エージェント バージョン 2.0.8689.0 以降)
- Hyper-V ホスト は直接またはプロキシ サーバーを介してインターネットと HTTPS (出力方向)で通信できること

保護される仮想マシンのゲスト OS

オンプレミスから Azure のサイト回復では、以下の **64 ビット** ゲスト OS を実行する Hyper-V 仮想マシンの保護をサポート

- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2 SP1
- Windows Server 2008 SP2 x64
- CentOS
- openSUSE
- SUSE Linux Enterprise Server
- Ubuntu

※ 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を推奨

保護される仮想マシンのハードウェア構成

保護される仮想マシンは、以下のハードウェア構成要件を満たしている必要がある

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、最大 127 GB × 1 ディスク
データ ディスク	IDE または SCSI コントローラー接続、最大 1 TB × 最大 16 ディスク
仮想ハード ディスクの形式	VHD または VHDX、容量固定/容量可変/差分ディスクをサポート。物理ディスク (パススルー ディスク) 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、DHCP による IPv4 アドレスの動的割り当ての構成が必要。複数のネットワーク アダプターがある場合、フェールオーバー時に 1 つを自動または手動で選択
仮想マシン名	1 ～ 63 文字。アルファベット、数字、およびハイフンを使用可。先頭および末尾のハイフンは不可

Microsoft Azure

オンプレミスから Azure のサイト回復 導入手順

※注意: オンプレミスのサイト間のサイト回復とは手順が異なります。

評価のための最小構成

本ドキュメントでは、以下の小規模な評価環境を想定して Azure Site Recovery の導入および利用手順を説明する。オンプレミス側のサーバーの OS、Active Directory ドメイン、および VMM 管理環境は既に展開済みであることを前提とする。

オンプレミス側の環境

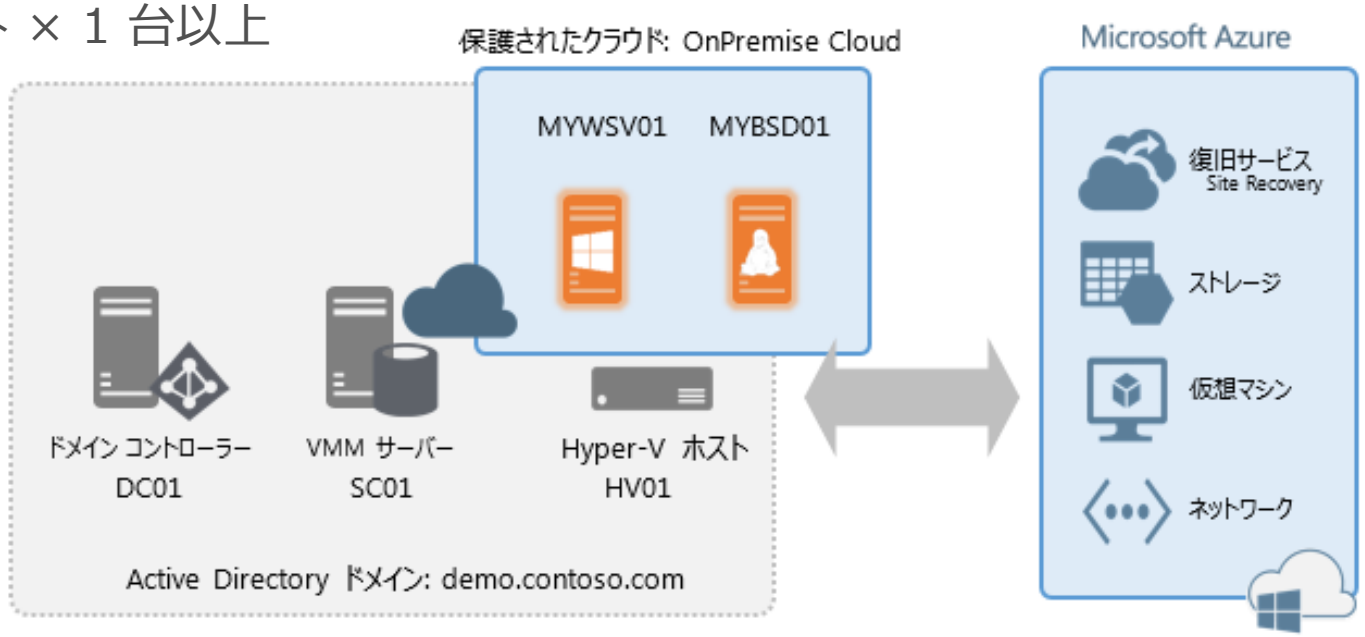
- Windows Server 2012 R2 ドメイン コントローラー × 1 台以上
- System Center 2012 R2 VMM 管理サーバー × 1 台
- Windows Server 2012 R2 Hyper-V ホスト × 1 台以上
- 既存の Windows Server または Linux 仮想マシン × 1 台以上

Azure 側の環境

- 有効な Azure サブスクリプション契約

  または、Azure 1 か月無料評価版

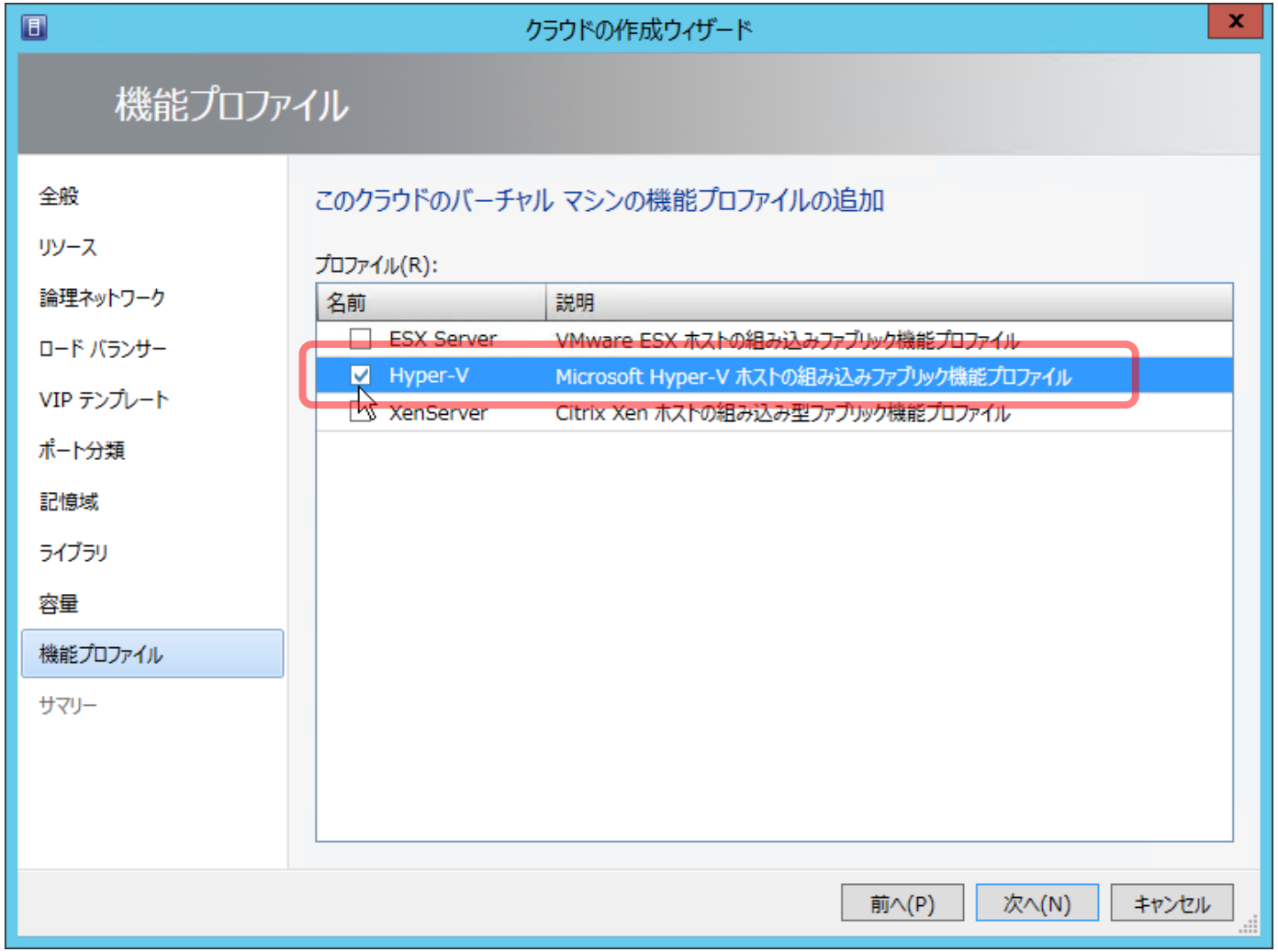
  http://azure.microsoft.com/ja-jp/pricing/free-traial/



Microsoft Azure

VMM クラウドの準備

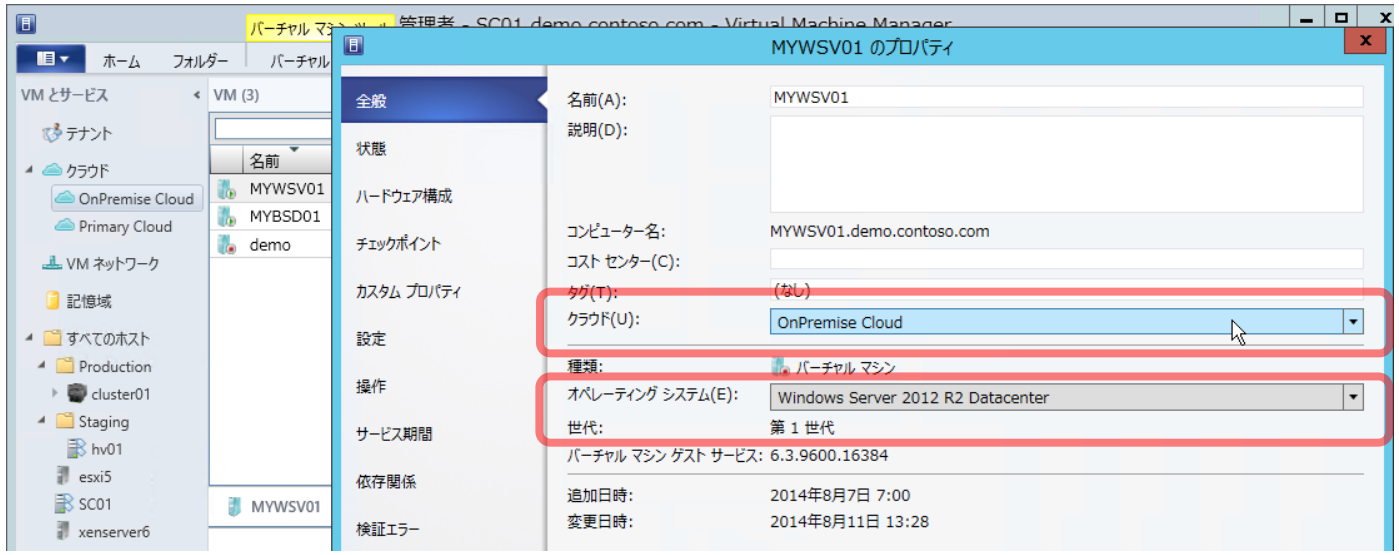
- Windows Server 2012 R2 Hyper-V ホストで構成されるホスト グループを作成する
- VMM クラウドを作成し、上記ホスト グループを関連付ける
- VMM クラウドの機能プロファイルとして［Hyper-V］を指定する

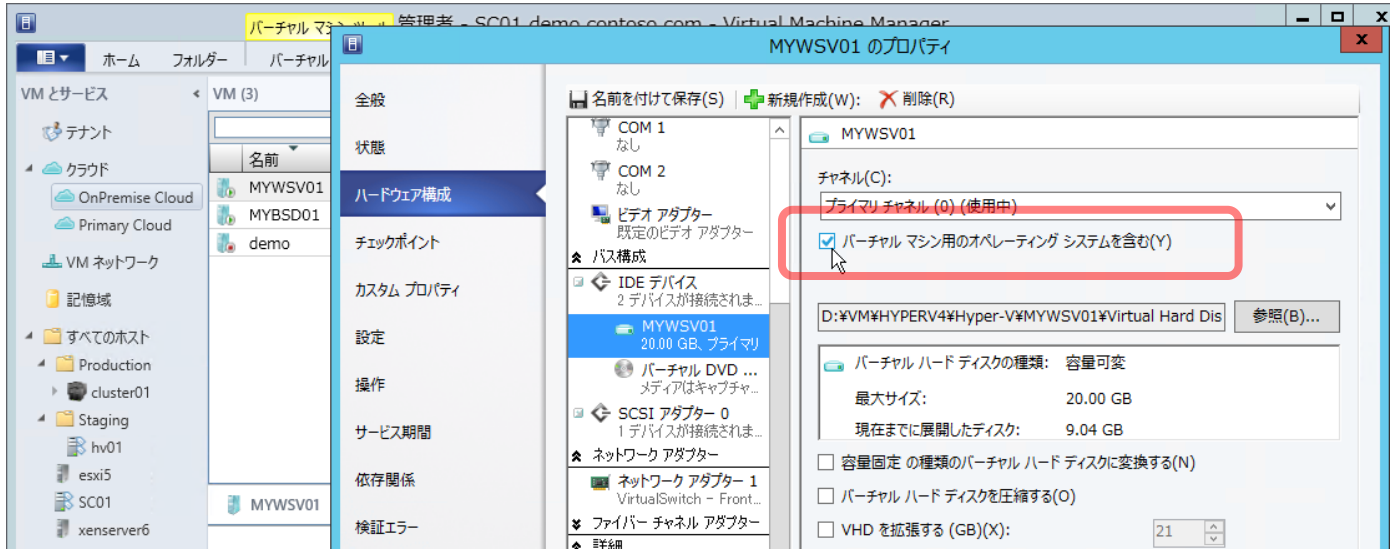


Microsoft Azure

保護される仮想マシンの準備

- 仮想マシンは第 1 世代で作成する
- 仮想マシンにはサポート対象のゲスト OS と最新の統合サービスをインストールしておく
  - ✓ Windows Server 2012 R2 および主要な Linux ゲストには最新の Hyper-V 統合サービスがビルトインされている
  - ✓ リモート管理用に RDP (Windows) または SSH (Linux) の構成を推奨
- 仮想マシンを VMM クラウドに関連付け、OS プロパティを設定する
- OS 用ディスク (1 つのみ) のプロパティで［バーチャル マシン用オペレーティング システムを含む］がチェックされていることを確認する
- ゲスト OS のネットワークの構成は、DHCP による自動割り当てにする



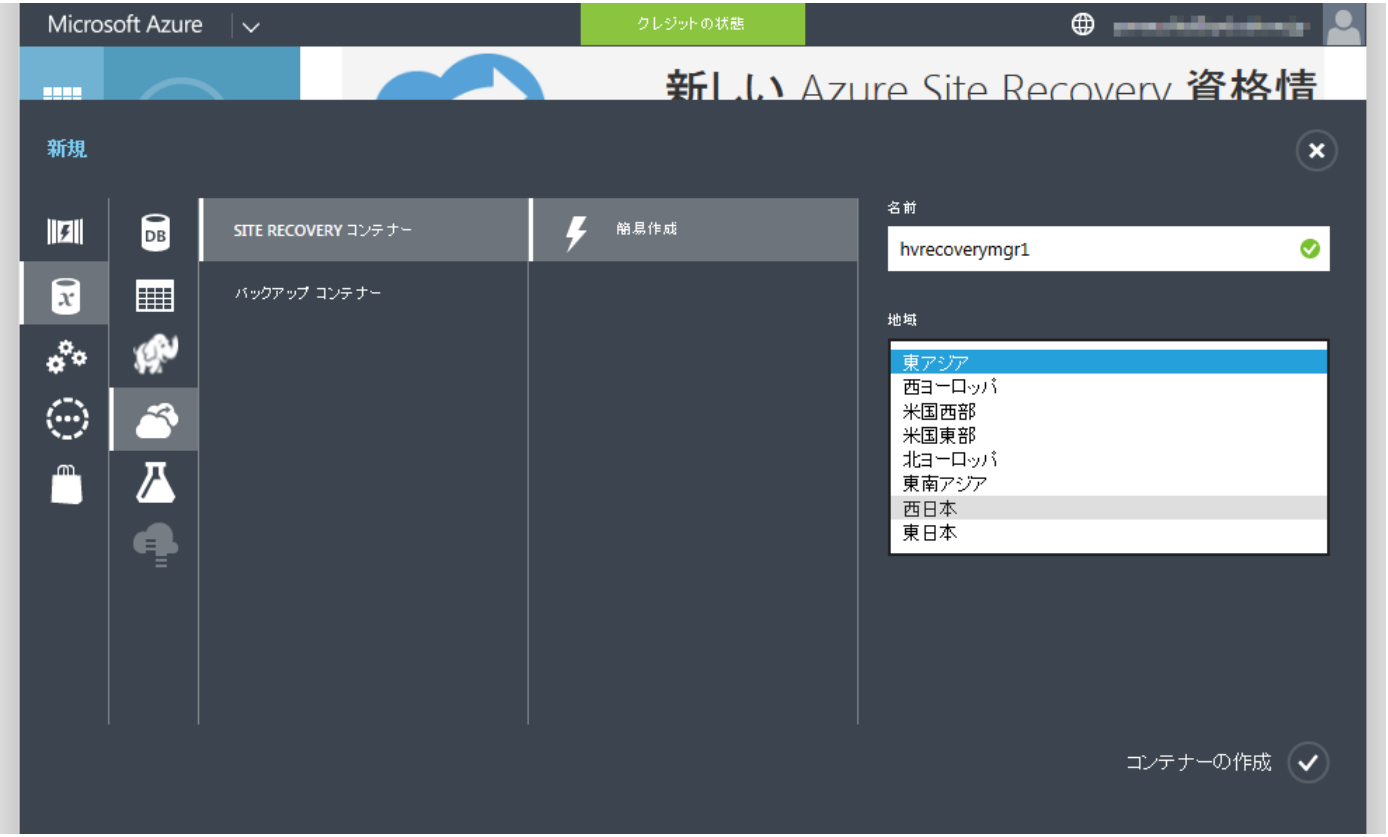


Microsoft Azure

Azure 側のサービスの準備 (1)

Azure 管理ポータルにサインインし、Azure Site Recovery 資格情報コンテナー (サイト回復コンテナー) を作成する。このコンテナーは、サービスの構成に関する情報 (メタデータ) を格納および保護するために使用される

- Azure 簡易ポータルのページ下部の［+新規］メニューから［データ サービス］→［復旧サービス］→［SITE RECOVRY コンテナー］→［簡易作成］と選択して作成
- フェールオーバー後の Azure 仮想マシンを実行したいリージョン (例: 東日本または西日本) と同じリージョンを選択



Azure 側のサービスの準備 (2)

Azure Site Recovery 資格情報コンテナーのページを開き、クイック スタート ページでこの後の手順を確認する

- 回復のセットアップから［内部設置型 Hyper-V サイトと Microsoft Azure の間］を選択する
- オンプレミスと Azure のサイト回復のために必要な 5 つの手順とオンプレミス側に導入する必要があるコンポーネントのリンクが表示される
  - ✓ 以前は 6 つの手順。9 月 12 日から証明書の準備とアップロードが不要に！

Microsoft Azure

Azure 側のサービスの準備 (3)

レプリケーション データ (仮想マシンの仮想ハード ディスクのレプリカ) の保存先となる Azure ストレージ アカウントを作成する

- Azure 簡易ポータルのページ下部の［+新規］メニューから［データ サービス］→［ストレージ］→［簡易作成］と選択して作成
- Azure Site Recovery 資格情報コンテナーと同じリージョンを選択
- ジオ (主要地域) 冗長を選択 (既定)

※ジオ (主要地域) 冗長は同一地域内の 2 つのリージョンで自動構成される。例えば、西日本を選択すると、セカンダリ リージョンとして東日本が自動選択される

Azure 側のサービスの準備 (4)

フェールオーバー後の仮想マシンを接続する Azure 仮想ネットワークを作成する

- Azure 簡易ポータルのページ下部の［+新規］メニューから［ネットワーク サービス］→［仮想ネットワーク］→［簡易作成］または［カスタム作成］を選択して作成
- Azure Site Recovery 資格情報コンテナーと同じリージョンを選択
- Azure 仮想ネットワークにゲートウェイを作成して、オンプレミスのネットワークとの間でサイト間 VPN 接続を完了しておく

Microsoft Azure

Azure Site Recovery プロバイダーの展開 (1)

VMM 管理サーバーに Azure Site Recovery プロバイダーをインストールする

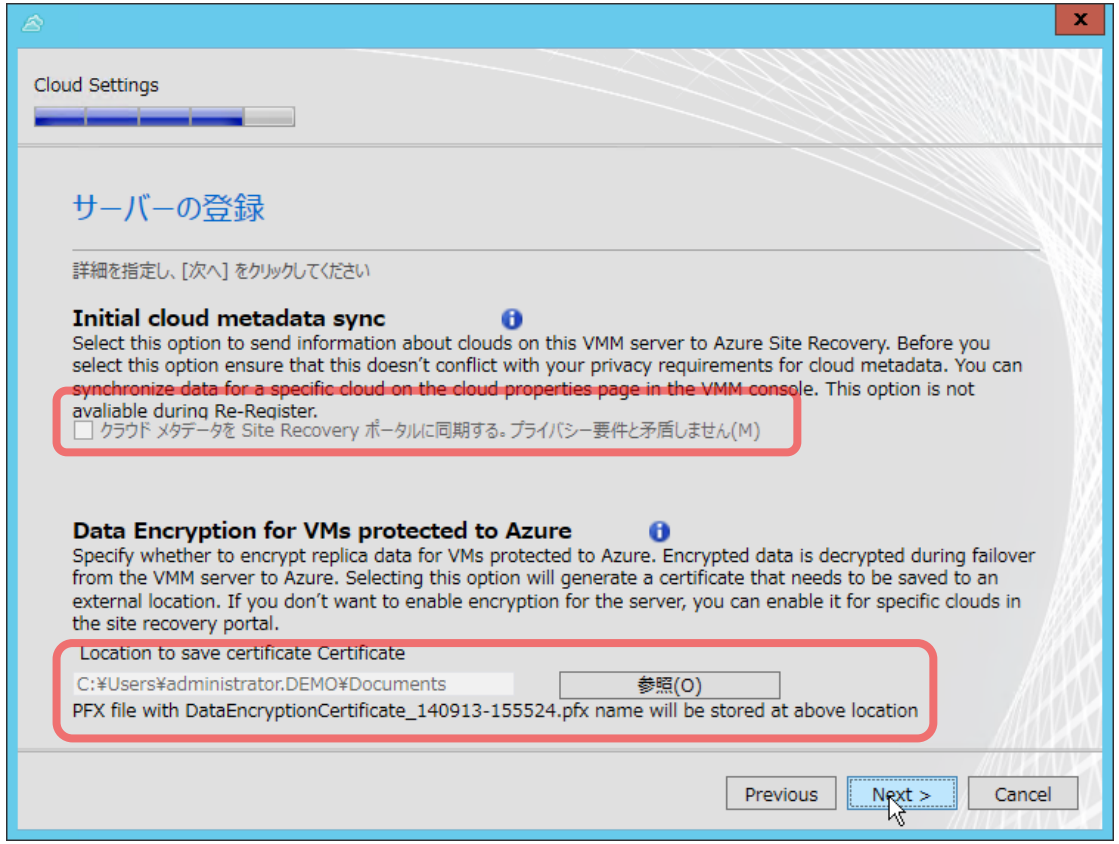
- Azure 管理ポータルのクイック スタート ページから Azure Site Recovery プロバイダーのインストーラー (VMMASRProvider_x64.exe) をダウンロード
- VMM 管理サーバーに Azure Site Recovery プロバイダーをインストール
  - ✓ インストール中、System Center Virtual Machine Manager (SCVMMService) サービスは停止される
- Azure Site Recovery のサービスとの通信 (HTTPS) にプロキシ サーバーが必要な場合はプロキシを構成
- 登録キー ファイルを指定して、Azure Site Recovery 資格情報コンテナーにサーバーを登録
  - ✓ 登録キー ファイルは Azure ポータルで生成し、ダウンロード (コンテナー名_日付.VaultCredentials)

Microsoft Azure

Azure Site Recovery プロバイダーの展開 (2)

- VMM クラウドの構成データ (メタデータ) の初期同期の方法を選択
  - ✓ 既存のすべての VMM クラウドのメタデータを同期して良い場合はメタデータの同期をチェック
  - ✓ ここでメタデータの同期を選択しない場合は、後で VMM 管理コンソールを使用して、VMM クラウドの全般プロパティで同期を有効化

- 暗号証明書 (暗号化キー) の保存先パスの指定
  - ✓ 暗号証明書は、フェールオーバー実行時にレプリケーション データ (仮想ハード ディスク) の暗号化を解除するために使用

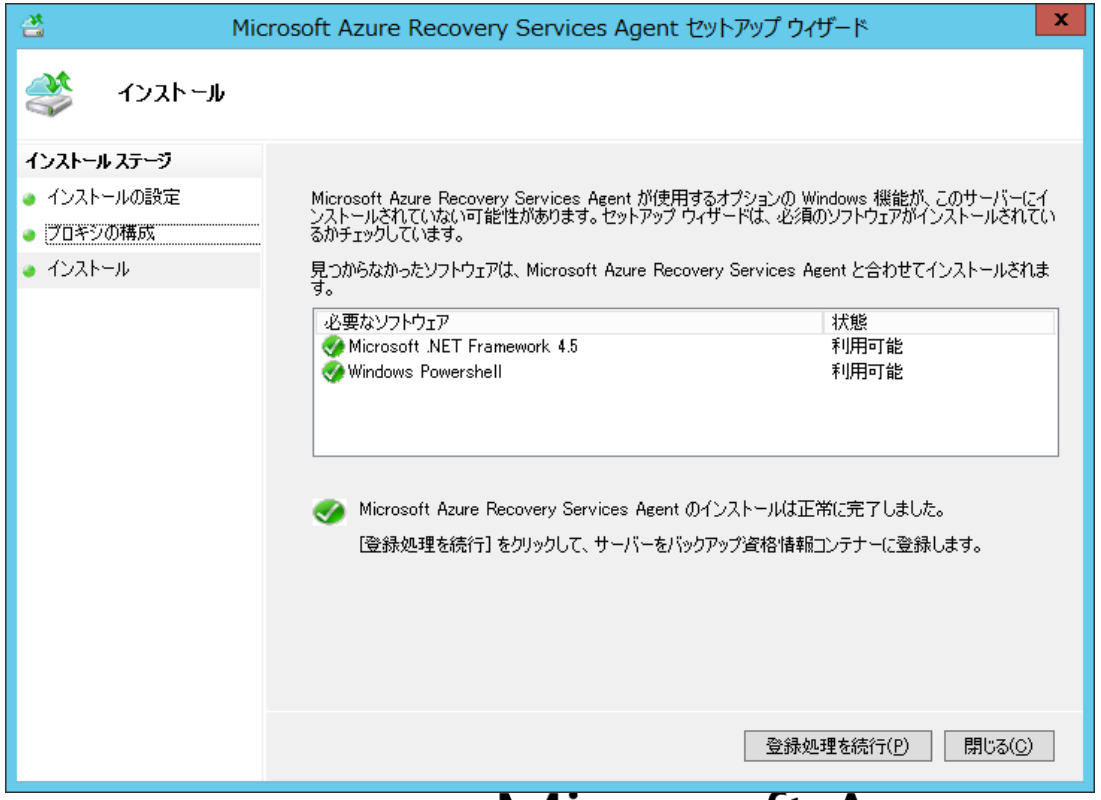


Microsoft Azure

Azure Recovery Services エージェントの展開

Hyper-V ホストに Azure Recovery Services エージェントをインストールする

- Azure 管理ポータルのクイック スタート ページから Azure Recovery Services エージェントのインストーラー (MARSAgentInstaller.exe) をダウンロード
- 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
  - ✓ 前提コンポーネントが不足していれば自動的にインストールされる
  - ✓ ［登録処理を続行］の実行は Azure Backup 用なので不要
  - ✓ エージェントは Azure Backup と共通。プロキシの構成を変更する場合は、［Microsoft Azure Backup］スナップインのプロパティで設定可能

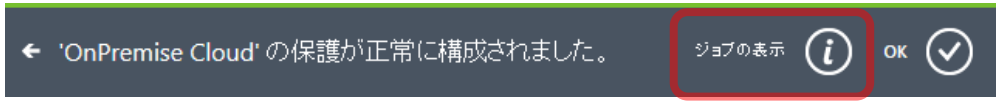


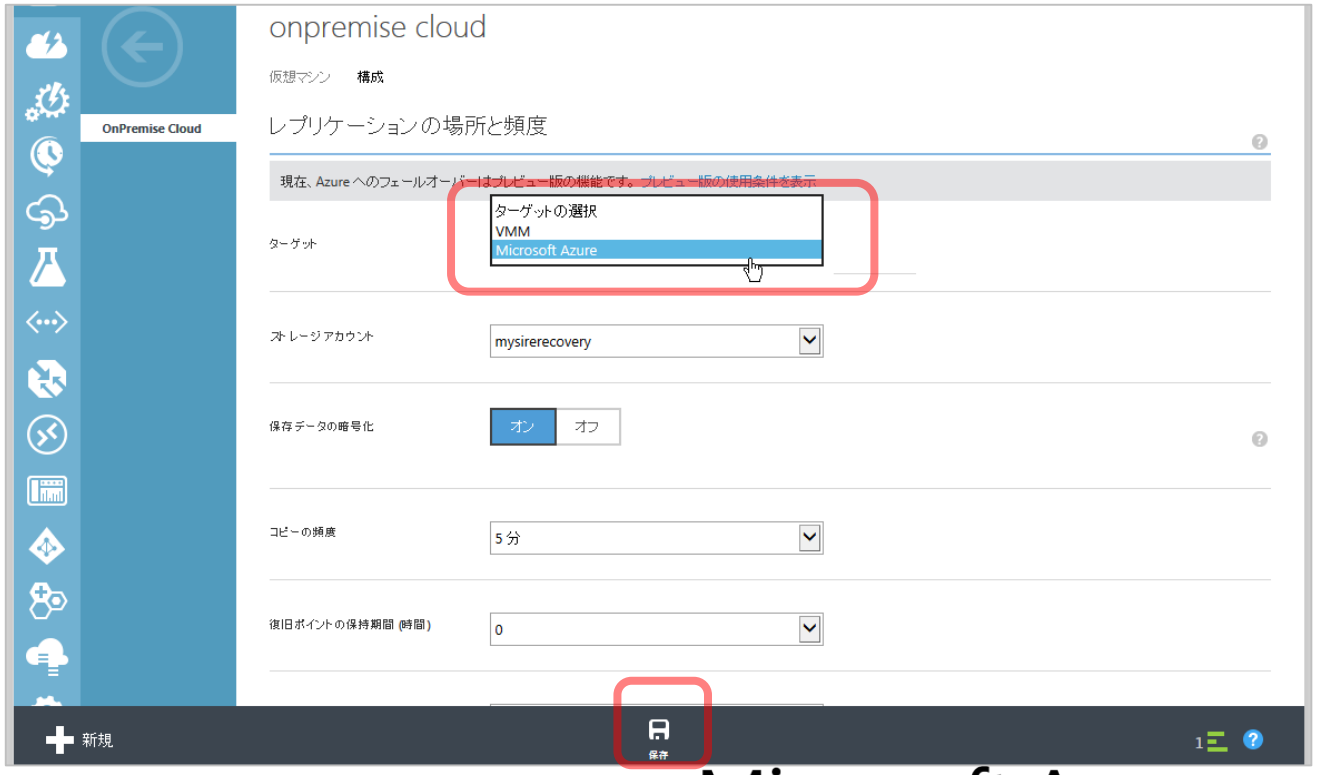
Microsoft Azure

VMM クラウドの保護の構成 (1)

VMM クラウドの保護を構成する

- Azure 管理ポータルで Azure Site Recovery の資格情報コンテナーの［保護された項目］を開く
- VMM 管理サーバーに存在する VMM クラウドがリストされるので、保護対象の VMM クラウドのページを開く
- 構成ページで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を構成する
- 構成を保存すると、VMM 管理サーバーを介して Hyper-V ホストの Hyper-V レプリカが自動構成される
- 構成の成功、失敗は、Azure 管理ポータルでジョブの詳細を参照





Microsoft Azure

VMM クラウドの保護の構成 (2)

レプリケーションの場所と頻度	
ターゲット	Microsoft Azure を選択
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
保存データの暗号化	暗号化する場合はオン。Azure Site Recovery プロバイダーのインストール時に暗号化オプションを有効化した場合にのみオンにできる
コピーの頻度	30 秒、5 分 (既定)、または 15 分
復旧ポイントの保存期間 (時間)	0 (既定) ～ 24 最初の 1 時間は常に［60 / コピーの頻度］の数の復旧ポイントが作成される。1 以上の保持期間が設定された場合、1 時間に 1 回の頻度で復旧ポイントが作成され、指定した数だけ保存
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 1 以上を指定した場合、指定し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を作成

レプリケーション設定	
レプリケーションの開始時間	すぐに、または開始時間を 30 分単位で指定

Microsoft Azure

仮想マシンの保護の有効化 (1)

仮想マシンの保護を有効化する

方法 1 ••• Azure 管理ポータルからの有効化

- Azure 管理ポータルの［保護された項目］ – ［仮想マシン］ページから［保護を有効にする］または［仮想マシンの追加］をクリックして対象を選択

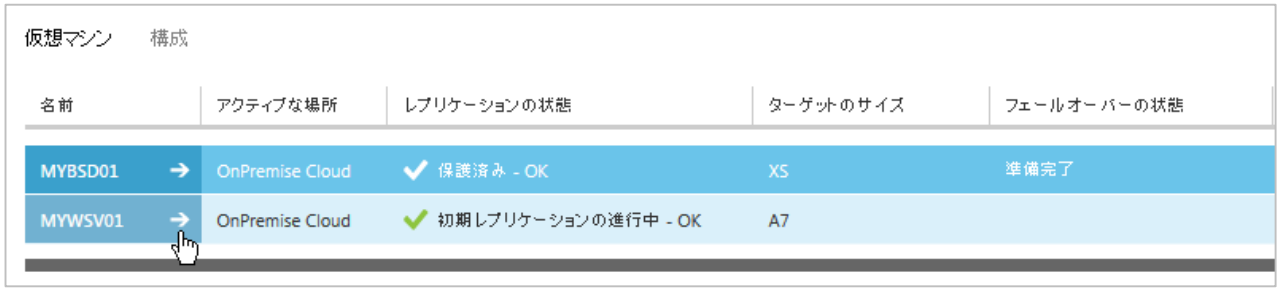
方法 2 ••• VMM 管理コンソールからの有効化

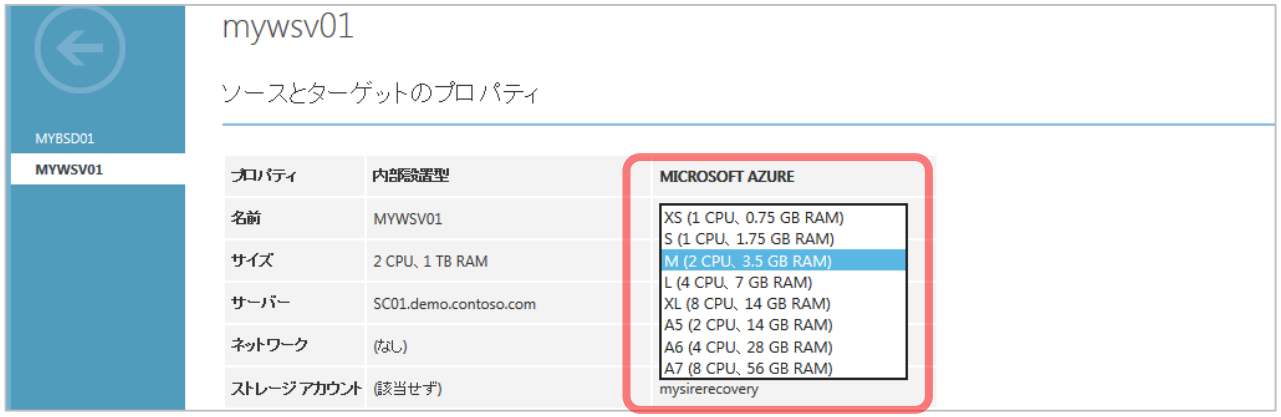
- VMM 管理コンソールで仮想マシンを選択し、［保護の管理］をクリックして、［このバーチャル マシンの Hyper-V Recovery Manager 保護を有効化する］をオン

Microsoft Azure

仮想マシンの保護の有効化 (2)

- 仮想マシンの保護の有効化の成功、失敗はジョブの詳細で確認
  - ✓失敗した場合は原因を取り除いてからジョブを再起動するか、保護の有効化を再実行
  - ✓保護の有効化が成功すると、初期レプリケーションが始まる
- 保護の状態は［保護された項目］－［仮想マシン］ページで確認
  - ✓保護なし → 処理初期レプリケーションの進行中 → 保護済み (フェールオーバーの準備完了)
- 仮想マシンの［ソースとターゲットのプロパティ］を開き、レプリカ仮想マシンの構成を確認
  - ✓Azure 仮想マシンのインスタンス サイズを調整
  - ✓仮想マシンの名前の調整 (名前がエラーになる場合)
  - ✓ネットワークのマッピングの調整 (保護対象の仮想マシンに複数の NIC がある場合)

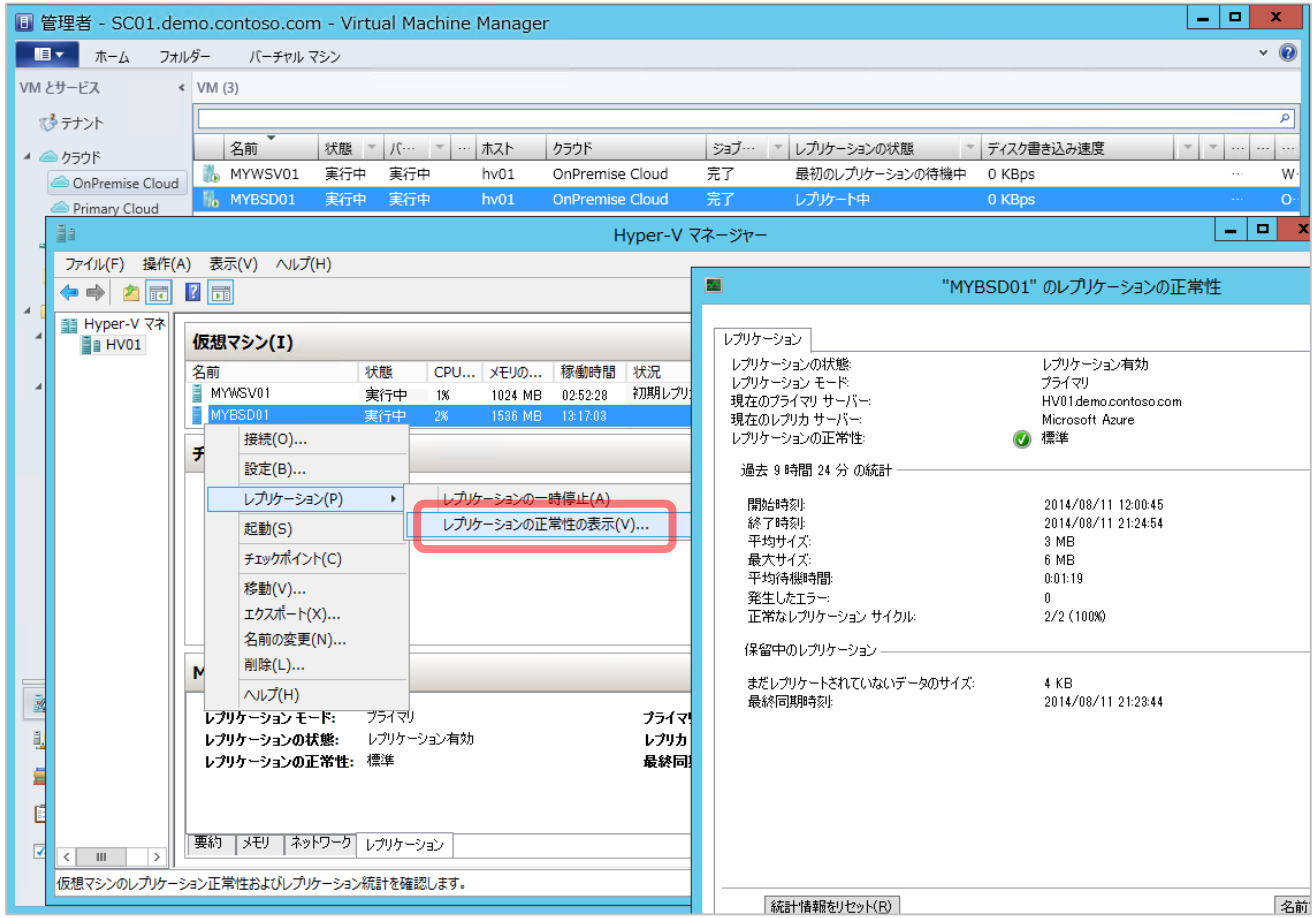




Microsoft Azure

レプリケーションの正常性の監視

- レプリケーションの正常性の詳細は、［Hyper-V マネージャー］の［レプリケーションの正常性の表示］から確認可能
  - ✓プライマリ サーバーは Hyper-V ホスト、レプリカ サーバーは Microsoft Azure
  - ✓利用可能な帯域幅の問題で、コピーの頻度の時間内にレプリケーションが完了しない場合、正常性は“重大”に。その場合、コピーの頻度の調整が必要
- イベント ログの［アプリケーションとサービス¥MicrosoftAzureRecoveryServices ］ログでもレプリケーションの詳細情報を確認できる



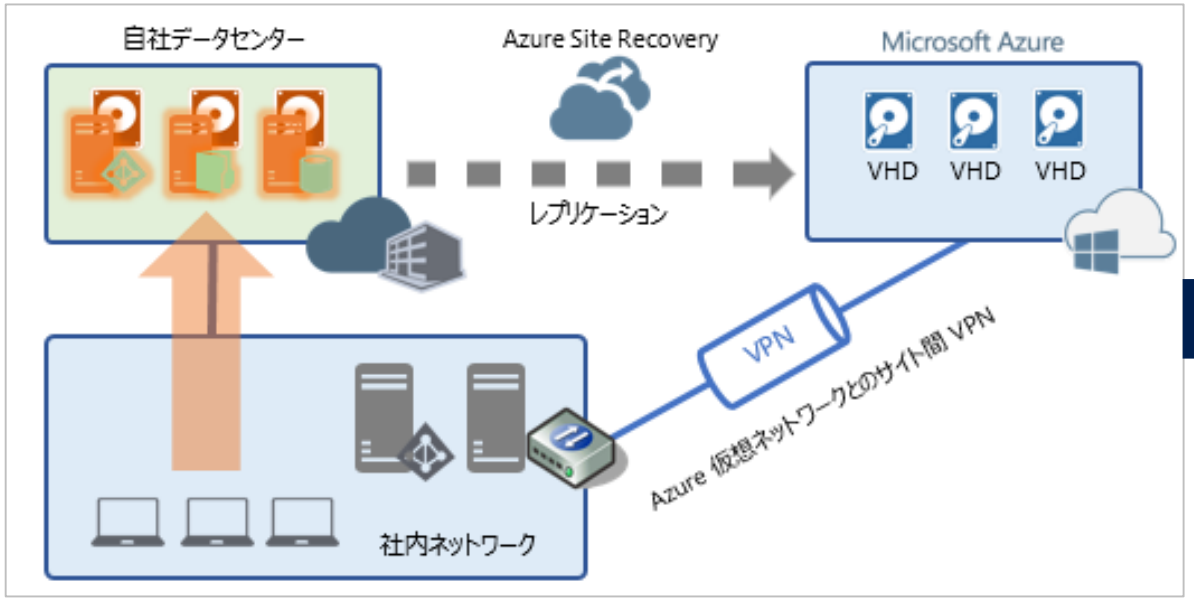
Microsoft Azure

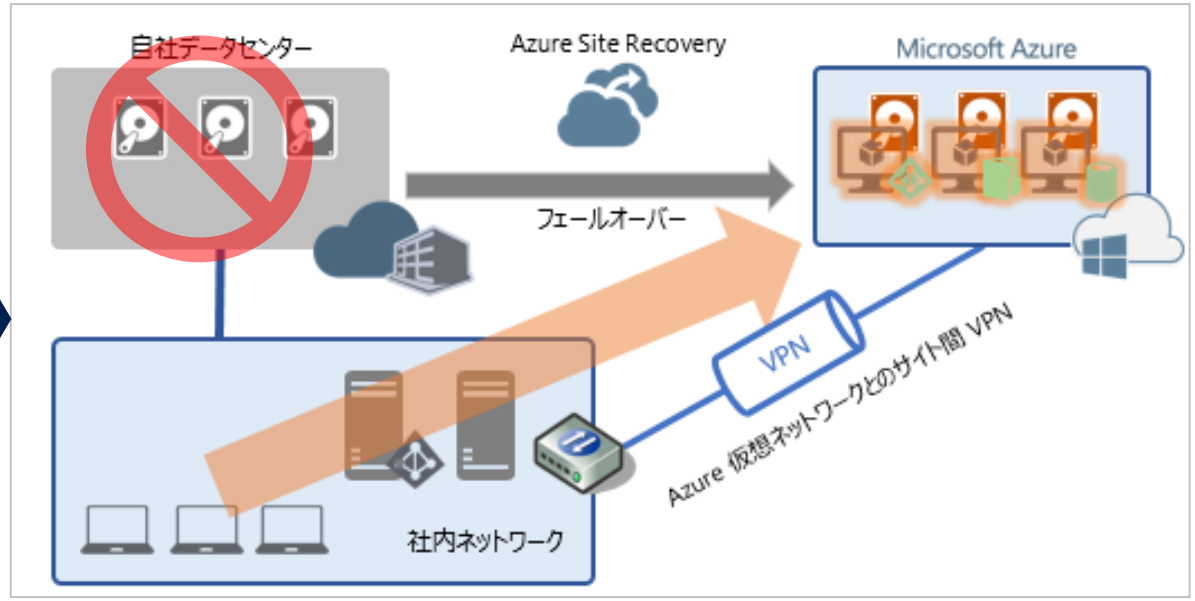
フェールオーバーの管理

※注意: オンプレミスのサイト間のフェールオーバーとは手順が異なります。

フェールオーバーとは

- プライマリ サイトが利用できない場合に二次拠点 (Azure) のレプリカ仮想マシンに切り替え、仮想マシンをすばやく復旧するプロセス
- 仮想マシンごと、または復旧計画を使用してフェールオーバーを実行
  - ✓ テスト フェールオーバー ･･･ レプリカを Azure 仮想マシンで起動できるかどうかを隔離された環境でテスト
  - ✓ 計画されたフェールオーバー ･･･ 未同期のデータを完全に同期してからレプリカに切り替え (データ損失ゼロ)
  - ✓ 計画されていないフェールオーバー ･･･ 最後の同期データを使用してレプリカで復旧(データ損失ニア ゼロ)





復旧計画の作成

- 復旧計画とは、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、自動化するためのプロセスの定義
- Azure 管理ポータルの［復旧計画］ページに作成

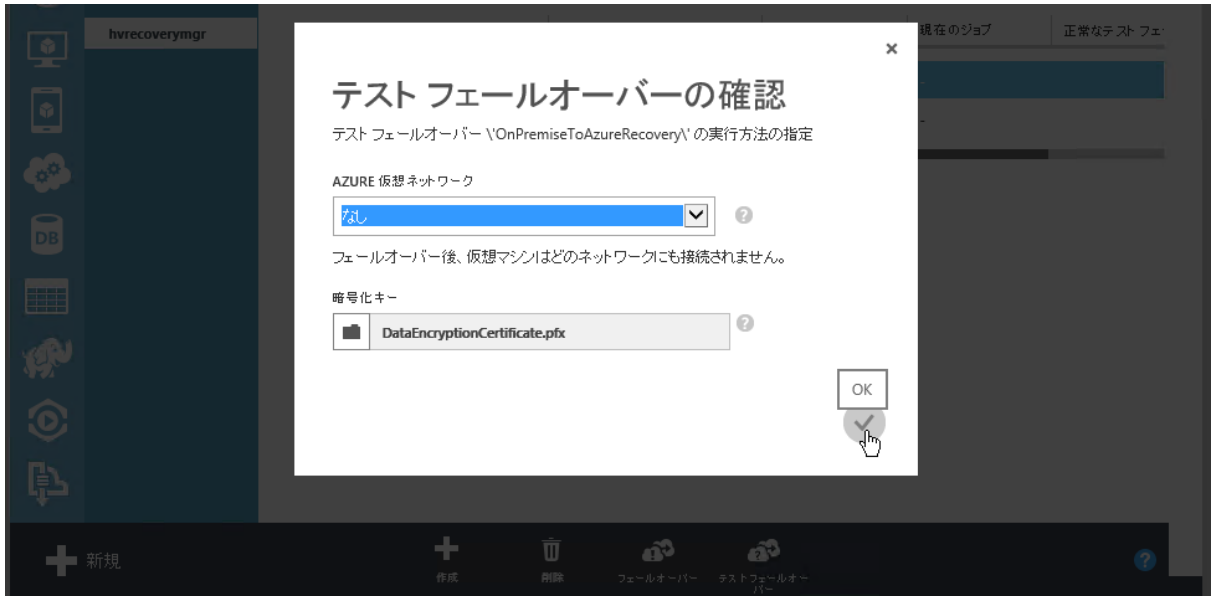
  - ✓ 1 台以上の仮想マシンを 1 つ以上のグループでグループ化し、グループ単位で順番に仮想マシンを開始
  - ✓ 計画されたフェールオーバーおよびフェールバック時のシャットダウン処理は、暗黙的に逆順に処理
  - ✓ 手動アクションを追加すると、処理を中断し、続行の指示待ちに
  - ✓ スクリプト (PowerShell） はオンプレミスからオンプレミスの保護でのみサポート

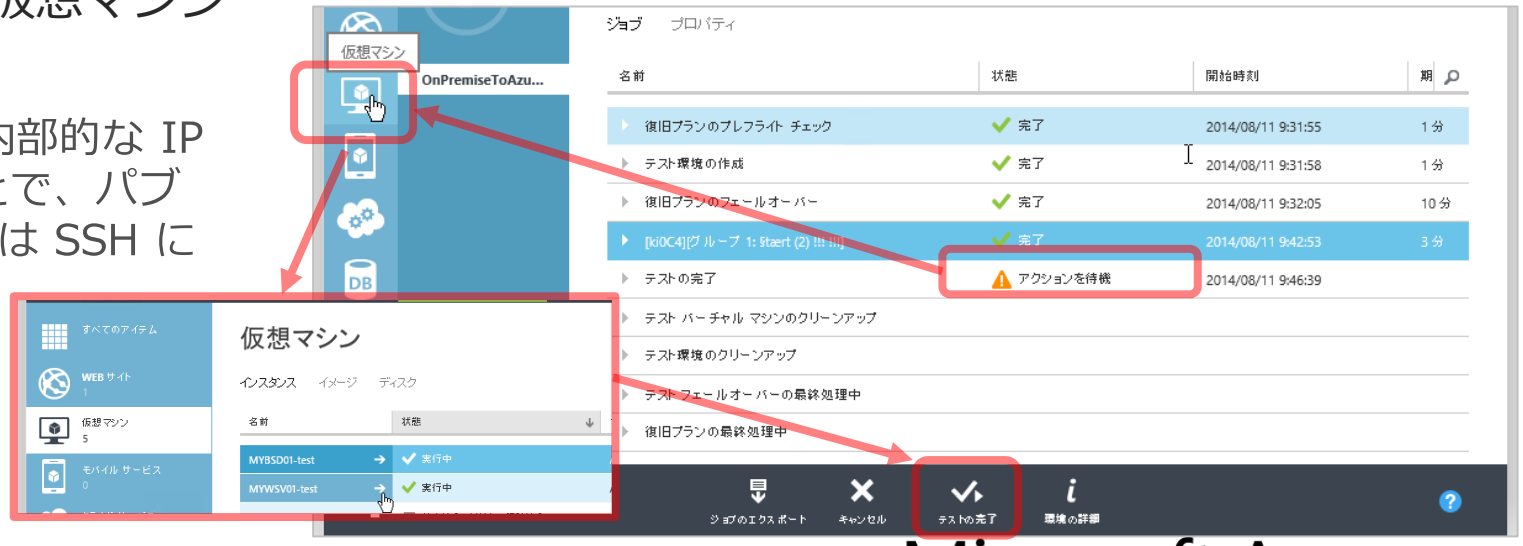
  → オンプレミスから Azure への復旧計画においても、2014 年 9 月 12 日に Azure Automation (プレビュー) との統合によるスクリプト (Runbook) 実行機能を追加

Microsoft Azure

テスト フェールオーバー

1. 仮想マシンまたは復旧計画を選択して、[テスト フェールオーバー]をクリック
2. 接続先の Azure 仮想ネットワークを［なし］にしてフェールオーバーを実行
   - ✓ 暗号化オンにした場合は、暗号化キーとして暗号証明書を指定
3. ジョブで進行状況を確認し、［テストの完了: アクションを待機］の状態になったら、Azure 仮想マシンのページを開き、テスト用の仮想マシンの実行を確認
   - ✓ Azure 仮想マシンへの接続なしでも、内部的な IP に対するエンドポイントを作成することで、パブリック仮想 IP (VIP) による RDP または SSH によるリモート接続が可能
4. 仮想マシンの動作を確認したら、ジョブで［テストの完了］を実行
   - ✓ Azure 仮想マシンは自動的に削除

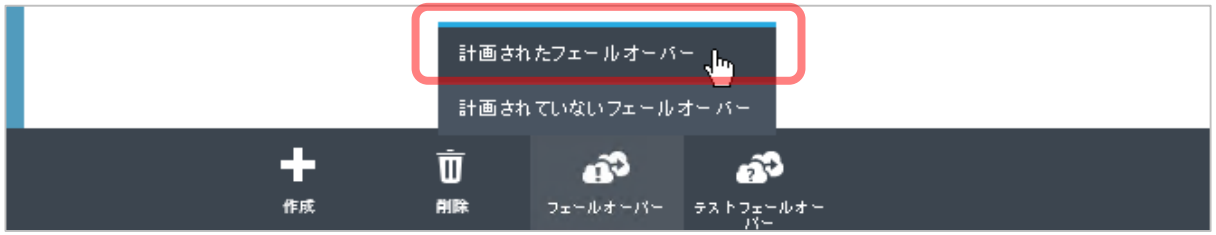




Microsoft Azure

計画されたフェールオーバー

1. 仮想マシンまたは復旧計画を選択して、[フェールオーバー > 計画されたフェールオーバー]をクリック
2. フェールオーバーの方向 (VMM から Azure) を確認してフェールオーバーを実行
   - ✓ 暗号化オンにした場合は、暗号化キーとして暗号証明書を指定
3. ジョブで進行状況を確認する。フェールオーバーが完了すると、仮想マシンまたは復旧計画が［コミット待機中］の状態になるので［コミット］をクリックする
   - ✓ VMM クラウド側の仮想マシンは自動的にシャットダウンされ、未同期のデータが完全に同期される
   - ✓ プライマリと同じ状態になった仮想ハード ディスクを使用して Azure 仮想マシンが作成、開始される
4. フェールオーバーが完了すると、仮想マシンまたは復旧計画が［コミット待機中］の状態になるので［コミット］をクリックする
5. Azure 仮想マシンのページを開き、仮想マシンが 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ることを確認



Microsoft Azure

計画されていないフェールオーバー

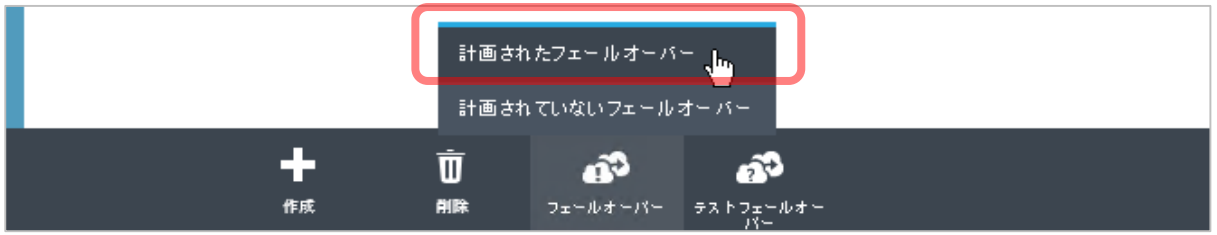
1. 仮想マシンまたは復旧計画を選択して、[フェールオーバー > 計画されていないフェールオーバー]をクリック
   - ✓ VMM 管理サーバーとの通信は断絶していても OK
2. フェールオーバーの方向 (VMM から Azure) を確認してフェールオーバーを実行
   - ✓ 暗号化オンにした場合は、暗号化キーとして暗号証明書を指定
3. ジョブで進行状況を確認する。フェールオーバーが完了すると、仮想マシンまたは復旧計画が［コミット待機中］の状態になるので［コミット］をクリックする
   - ✓ 最後のレプリケーション データを使用して Azure 仮想マシンが作成、開始される
4. フェールオーバーが完了すると、仮想マシンまたは復旧計画が［コミット待機中］の状態になるので［コミット］をクリックする
   - ✓ コミットする前であれば、仮想マシンごとに復旧ポイントの変更が可能
5. Azure 仮想マシンのページを開き、仮想マシンが 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ることを確認

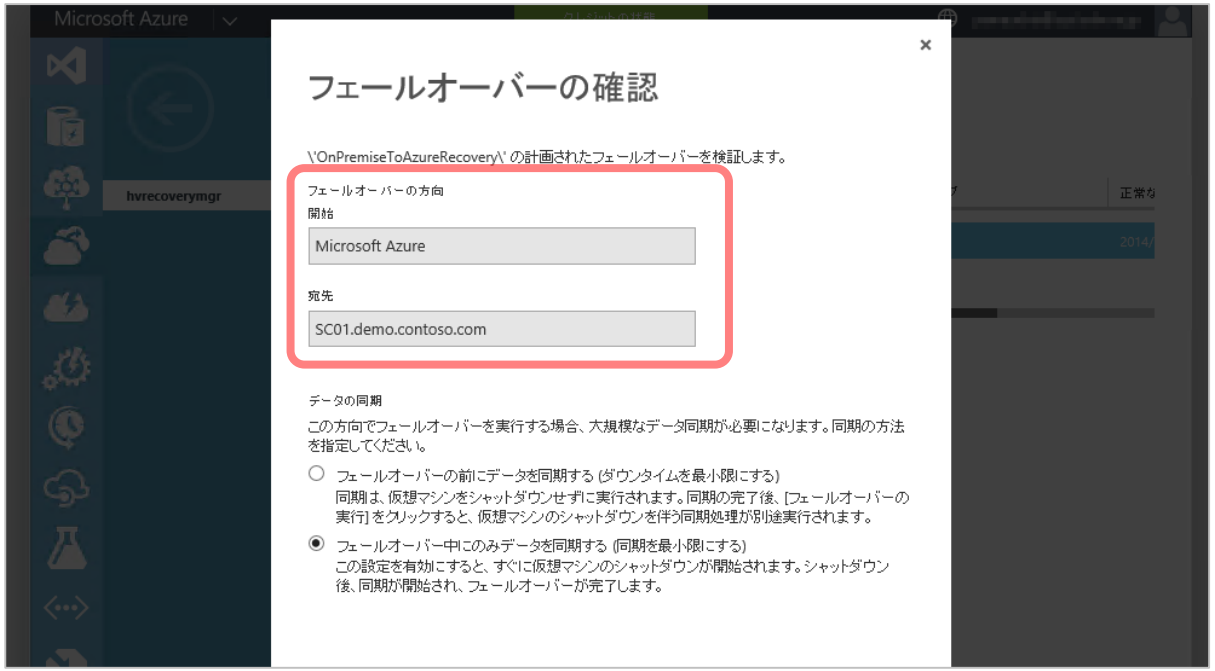
Microsoft Azure

フェールバック

プライマリ サイトの VMM クラウドが利用可能になったら、逆方向の計画されたフェールオーバーを実行して、仮想マシンを VMM クラウドにフェールバックする

1. 仮想マシンまたは復旧計画を選択して、[フェールオーバー > 計画されたフェールオーバー]をクリック
2. フェールオーバーの方向 (Azure から VMM) を確認し、次のいずれかを選択して開始
   - ✓ 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)
   - ✓ フェールオーバー中にのみデータを同期する (同期を最小限にする)
3. ジョブで進行状況を確認する
   - ✓ フェールオーバーの前に同期するように選択した場合は、フェールオーバーの準備ができると［フェールオーバーの実行］の指示待ちの状態になる
4. フェールオーバーが完了すると［コミット待機中］の状態になるので［コミット］をクリックする
   - ✓ VMM クラウドから Azure への初期レプリケーションが開始
   - ✓ Azure 仮想マシンは自動削除





Microsoft Azure

参考: Azure へのマイグレーション

Azure Site Recovery を利用して、オンプレミスの Hyper-V 仮想マシンを Azure 仮想マシンにマイグレーションできる

1. 仮想マシンを Azure にフェールオーバー
2. フェールバックせずに仮想マシンの保護を無効化
   - ✓ Azure Site Recovery から保護の構成と VMM 側の保護設定はクリーンアップ
   - ✓ Azure 仮想マシンはそのまま残る
   - ✓ VMM 側の仮想マシンも削除されない (後で手動削除)
3. Azure へのマイグレーション完了

Appendix

利用料金とサブスクリプション ライセンス

- Azure Site Recovery の料金は、保護される仮想マシン 1 台あたりの月額
  - ✓ 保護対象の仮想マシンの 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
  - ✓ オンプレミスからオンプレミスと、オンプレミスから Azure で単価が異なる
  - ✓ 料金には、ストレージ、データ転送、Azure 仮想マシン、Azure 仮想ネットワークの利用料は含まれない
- 以下の料金は各サービスのレートで従量課金
  - ✓ ストレージ サービス ･･･ ストレージ使用、ストレージ トランザクション、Azure から送信方向のデータ転送
  - ✓ Azure 仮想ネットワーク ･･･ ゲートウェイを使用したオンプレミスとのサイト間 VPN 接続がアクティブな間
  - ✓ Azure 仮想マシン ･･･ フェールオーバーで Azure 仮想マシンが作成されてから、フェールバックで仮想マシンが削除されるまで
- Azure Site Recovery サブスクリプション ライセンス
  - ✓ Microsoft Enterprise Agreement を通じて提供
  - ✓ 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
  - ✓ InMage Scount ソフトウェアを使用して VMware サイトや物理マシンを保護する権利

評価版

- 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/

© 2014 Microsoft Corporation. All rights reserved. Microsoft, Windows, Windows Vista and other product names are or may be registered trademarks and/or trademarks in the U.S. and/or other countries.
The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.