

企業システムを、ビジネスを、ワークスタイルを
新たなステージへと導く最新プラットフォームOS

Windows Server 2012 World

企業のイノベーションを加速し、新たな価値を創造するために

[Interview]

Windows Server 2012は
本格的なクラウド世代を見据えた
新たな世代の“the Cloud OS”

サーバープラットフォームビジネス本部 業務執行役員 本部長 梅田 成二氏

[Concept]

Windows Server 2012で変わるIT基盤

[Scenario]

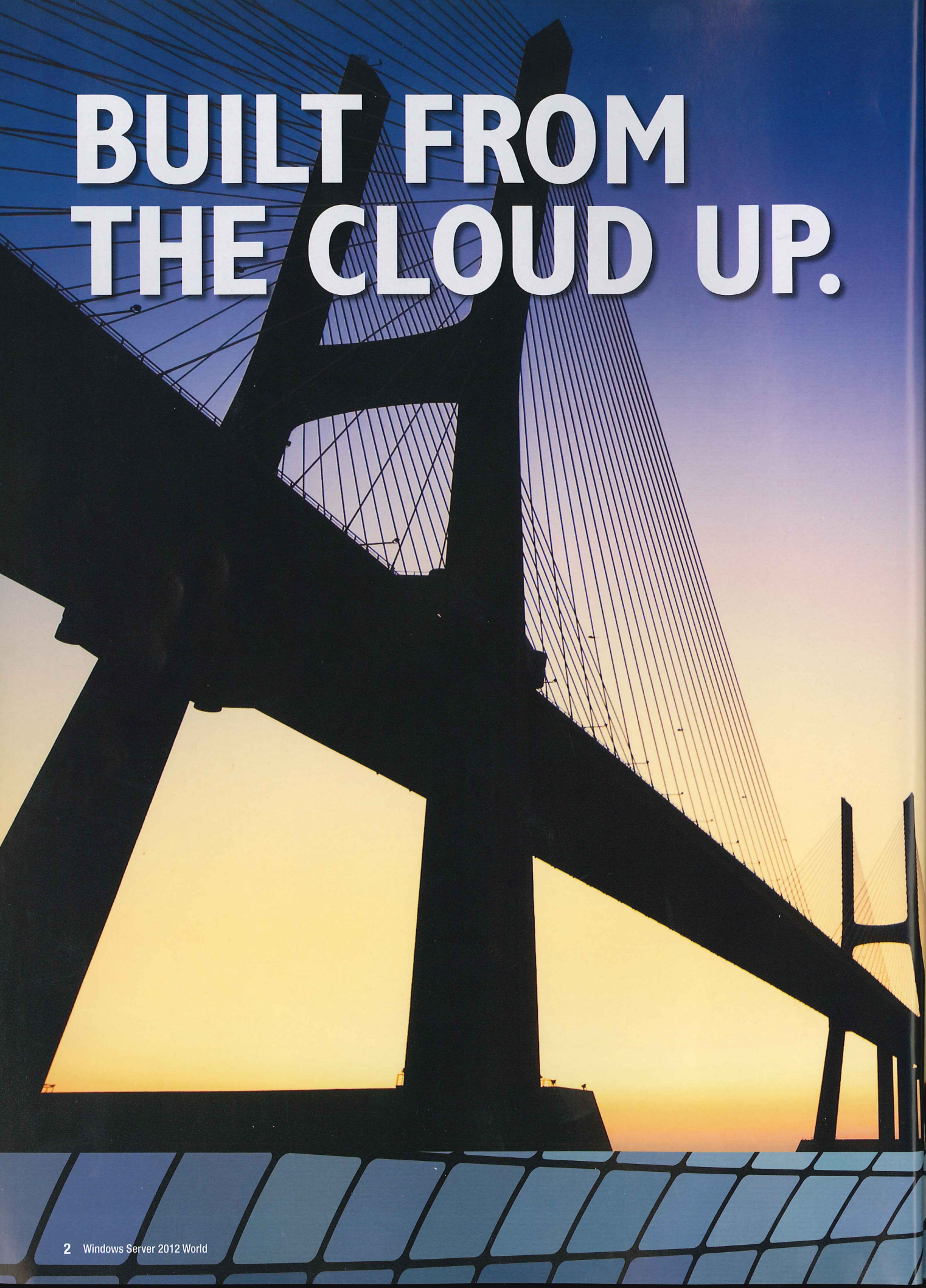
Windows Server 2012 導入と活用のシナリオ

[Function]

Windows Server 2012 機能詳細

[Edition]

早わかり!
Windows Server 2012
製品体系



BUILT FROM THE CLOUD UP.

企業システムを、ビジネスを、ワークスタイルを
新たなステージへと導く最新プラットフォームOS

Windows Server 2012 World VOL.01

企業のイノベーションを加速し、新たな価値を創造するために

Interview

Windows Server 2012は
本格的なクラウド世代を見据えた
新たな世代の“the Cloud OS” 02

サーバープラットフォームビジネス本部 業務執行役員 本部長 梅田 成二 氏

Concept

Windows Server 2012で変わるIT基盤 05
～今、企業システムは新たな段階へと進化する～

Scenario

Windows Server 2012 導入と活用のシナリオ 09
～5つのシナリオで理解する導入と活用のメリット～

Function

Windows Server 2012 機能詳細 24
～イノベーションを加速するダイナミックなIT基盤を支えるテクノロジー～

Edition

早わかり! Windows Server 2012 製品体系 48
～シンプル&高い投資効率でIT基盤の進化を強力に支援～

制作/日経BPコンサルティング デザイン/中島 隆夫(Art of NOISE) 印刷/大日本印刷

©本冊子に掲載の記事、写真、図版、図表の無断転載は堅くお断りいたします。



Windows Server 2012は 本格的なクラウド世代を見据えた 新たな世代の“the Cloud OS”

2012年9月1日にボリュームライセンス提供を開始し、9月26日にはパッケージ版もリリース——。品質と完成度の高さを背景に、Windows Server 2012は順調な立ち上がりを見せている。その位置付けをひと言で表せば、“the Cloud OS”。クラウド時代のサーバー OSとして、Windows Azureでの成果がふんだんに取り込まれていることがポイントだ。その意義と特長について、日本マイクロソフトの梅田成二氏に話を聞いた。

クラウドとオンプレミスをつなぎ 大きな1つのコンピューターとして扱う

「転換点となったのは、2010年3月にCEO(最高経営責任者)のスティーブ・バルマーが発した“*We're all in.*”の大号令でした」

Windows Server 2012が“the Cloud OS”に位置付けられることになった背景を、梅田成二氏(サーバープラットフォームビジネス本部 業務執行役員 本部長)はこのように語る。

“クラウドコンピューティング”という言葉が世に現れたのは、2006年のこと。もっとも、ITサービスをネットワーク経由で提供する形態はその前からかなり普及していた。電子メールやグループウェア、ソーシャルメッセージ／ソーシャルネットワークサービス、サービス型アプリケーションなど、現在では「SaaS (Software as a Service)」と呼ばれているサービスである。

一方、企業内にあるオンプレミスのサーバーとクラウドをシームレスにつなぎ、真のクラウドコンピューティングが実際に始まったのは、この1～2年のことだ。そのタイミングをとらえて、マイクロソフトはオンプレミス主体のビジネスからクラウド中心のビジネスへと大きく舵を切ったのである。

そうした新しい世代のコンピューティングモデルとしてマイクロソフトが示しているのが、「the Cloud OS」という考え方だ。そのポイントは、マイクロソフトのクラウド(Windows Azure)／サービスプロバイ

ダーのクラウド／オンプレミスのサーバーにまたがるコンピューター資源をさも1台のコンピューターであるかのように取り扱える統合的なプラットフォームを提供すること。そこでは「オープンな開発環境」「一元的なシステム管理」「共通のIDとセキュリティ基盤」「プラットフォームとしての仮想化」が提供され、サービス利用者にとっては、Windows Server(オンプレミス)とWindows Azure(クラウド)が一体化されたプラットフォームとして利用可能になる。

「企業内のサーバーに置かれていたアプリケーションをそのままの形でクラウドに持っていったり、クラウドから戻したりすることができなければなりません。また、ハイパフォーマンス・コンピューティングのように計算量がバースト的に増減するタイプの処理には、不足するコンピューティング・リソースをクラウド側で一時的にまかなえるようにする必要があります。これまでは物理サーバーという箱の中に限定されていた境界を、クラウドにまで押し広げ、クラウドを大きな1つのコンピューターであるかのように扱う——。このようなことを可能にするクラウド生まれのサーバーOSとして、われわれはWindows Server 2012を位置付けました」

クラウドやソーシャルへの対応を 5つの領域の機能強化で実現

それでは、Windows Server 2012を開発するにあたって、マイクロソフトはどのような点に力を注いだのだろうか——。



クラウド時代に必要なテクノロジーをすべて盛り込んだのが、Windows Server 2012です。

日本マイクロソフト株式会社
サーバープラットフォームビジネス本部
業務執行役員 本部長

梅田 成二 氏

Seiji Umeda



Windows Server 2012でストレージを仮想化すれば
ストレージにかかるコストをさらに圧縮できます。

ビジネスの観点からは、サーバーを取り巻く環境の変化、すなわち「クラウドの普及」「ソーシャルの広がり」と新しいアプリケーション」「データの爆発的増大」「デバイスの多様化」への対応を重視したと梅田氏は説明する。

「クラウドについては、クラウドとオンプレミス間の連携を高めるとともに、Windows Azureで使われたテクノロジーをサーバーOSへ搭載することも狙いました。ただし、Windows Serverという1つの製品だけでビジネスのすべての課題に対応できるとは考えていません。例えば、クラウドとオンプレミスを一元的に管理するという、システム管理面はSystem Center製品群が担当しますし、各種センサーやソーシャルメディアから収集した大量データから未来の売れ筋を発見する“ビッグデータ”のような使い方はSQL Server 2012との連携プレーで行うこととなりますが、Windows Server 2012がクラウドOSの中心にあることは間違いありません」

一方、テクノロジー面では、主に5つの領域で機能強化が図られた(図1)。

「新しい時代の“the Cloud OS”とするために力を注いだのが、『仮想化の進化』と『クラウド連携』の2項目。オンプレミス用の汎用サーバーOSとしては『さらなるコスト削減』『事業継続オプション』『モバイルワーク』に注力しました」

梅田氏によれば、前バージョンのWindows Server

2008 R2までのHyper-Vで実現できるスケーラビリティには限界があったため、Windows Azureではハイパーバイザ層に独自の拡張を加えて100万台規模のデータセンターのプラットフォームとして使用していたとのこと。Windows Server 2012のHyper-Vには、このクラウド用ハイパーバイザと同じものが搭載されたことで、仮想化環境のオーバーヘッドは従来のHyper-Vよりも小さく、1台の物理サーバー当たりの仮想マシン台数(集約率)も増加しているという。

また、稼働中の仮想マシンの移動を可能にする「ライブマイグレーション(Live Migration)」もより導入の敷居が低くなった。シェアードナッシング方式を選べば、クラスターシステムも共有ストレージも用意する必要はなく、LANだけで仮想マシンを移動できる。

クラウド連携のポイントとしては、ネットワーク仮想化とクラウド対応のID連携がある。ネットワーク仮想化はWindows Server 2012に新設された「Hyper-V拡張スイッチ」によって実現される機能で、物理ネットワークなどを共有するユーザーどうしを低コストで隔離(マルチテナント化)するのに役立つ。もちろん、OpenFlowなどのSoftware Defined Network (SDN)対応のネットワーク装置によるネットワーク仮想化も可能だ。

汎用OSとして多くの顧客にコストメリットを提供できる機能として、Windows Server 2012にはストレージ仮想化機能が標準で組み込まれている。いわゆるシンプロビジョニングと同様、物理容量の合計より大きな記憶域プールも定義できるので、実際の需要に合わせてストレージやディスクを買い足していく堅実なデータセンター運営にも最適だ。従来は一部のストレージにしか装備されていなかった「重複データ除去」機能も実装されている。

事業継続については、シェアードナッシング方式のライブマイグレーションと同じテクノロジーを使った「Hyper-Vレプリカ」が新たに搭載された。WAN回線さえ用意しておけば仮想マシンの複製(レプリカ)を離れた場所に確保できるので、中堅・中小規模の企業での事業継続対策を容易に実施できるようになる。

図1 Windows Server 2012の強化点

仮想化の進化	Hyper-Vのスペック向上、高速化 シェアードナッシング環境での仮想マシン移動が可能に
クラウド連携	ネットワークの仮想化 ID連携により、クラウドでもシングルサインオンを実現
さらなるコスト削減	ストレージの仮想化 ストレージ上のデータから重複を除去して容量を削減
事業継続オプション	Hyper-Vレプリカ Microsoftオンラインバックアップサービス
モバイルワーク	VDI(RemoteFXによるRDP 8.0の高速化) Direct Accessにより、ユーザー操作の要らないリモートアクセス環境

「モバイルワークに関しては、仮想デスクトップ基盤(VDI)にアクセスするためのRemote Desktop Protocol(RDP)を高速化したほか、Windows 8のスレートデバイスの入力機能へも対応しています。VDI利用時でもマルチタッチやジェスチャーによる入力が可能になりますから、ユーザーはそのアプリケーションがどの環境で動作しているかどうかを意識する必要はありません」

ファイルサーバーやデータベースも 仮想化によりさらに効率化される

Windows Server 2012のこのような機能拡張を生かせる活用シナリオとして、梅田氏はファイルサーバー用ストレージの最適化をまず挙げる。

「企業システムではHyper-Vによって、ファイルサーバーの仮想化と集約はかなり進みました。しかし、そのデータを格納するためのストレージやディスクは手付かずになっていることが多いようです。そこで、ファイルサーバーの仮想化が一段落したところで、

Windows Server 2012でストレージも仮想化して効率を高めてはどうでしょうか。それと併せて重複データ除去機能を利用することで、ストレージにかかるコストをさらに圧縮できます」

また、従来はサーバー仮想化の対象外とされることが多かったデータベース(DB)サーバーについても、SQL Server 2012とWindows Server 2012を組み合わせることで高い信頼性を保ったまま仮想化できると梅田氏は説明する。

「基幹系システムでは、SQL Server 2012の新しい高可用性のための機能『Always On』に引っ張られるかたちで、それを動作させるためのサーバーOSとしてWindows Server 2012が採用されていくと見えています。従来、DBサーバーは物理サーバーで動作させることが多かったのですが、先進的なお客様ではそうしたワークロードも含めて仮想化されるケースが増えてきました。Windows Server 2012のHyper-Vはオーバーヘッドも小さく、より多くのCPUやメモリを仮想マシンに割り当てられるように



なり、NUMAサーバーに“遠い”ところにあるメモリをアサインしないようにする仕組みも採用しました。ですから、DBサーバーを仮想化しても、十分に高いパフォーマンスを得ることができます」

数多くの仮想マシンを効率的にハンドリングできるWindows Server 2012のHyper-Vは、VDIのためのプラットフォームとしても最適だ。

「VDIを使われているお客様は、集約率を気にされていると思います。あるお客様の事例ではWindows XPなら1台の物理サーバーで仮想マシンを50個程度動かしていたのですが、Windows 7やWindows 8はソフトウェア機能が進化しているため、集約率がど

うしても半分程度になってしまっていました。そこで、Windows Server 2012のHyper-VとWindows 8を組み合わせてみたところオーバーヘッドを減らすためのさまざまな仕組みが利用できて、Windows XPと同程度の仮想マシンを動かせるようになりました。VDI用の仮想マシンを物理サーバー間で移動するライブマイグレーションも短時間で完了しますから、メンテナンスも楽になるでしょう。また、障害発生時にダンプを取得し、原因がどこにあるのか——ネットワークなのか、クライアント側なのか、サーバー側なのか——、どんなイベントが発生していたかを調べるためのツールも標準で用意されています」

ベータ版の段階から完成度が高く 対応製品も短期間でそろそろ見込み

Windows Server 2012は、2012年2月にベータ版、2012年6月に製品候補(RC)版がリリースされた後、9月1日にボリュームライセンスでの提供が始まった(図2)。RC版公開から製品版正式リリースまでの期間はおおかたの予想よりも短く、最初から完成度が高かったことをうかがわせる。

「ベータテスターの方々や早期導入にご協力いただいた企業からは、品質の高さを評価する反応を数多くいただきました。過去のWindows Serverでは新機能を試すにはRC版を待たなければならないことが多かったのですが、今回の注目機能であったHyper-Vレプリカなどはベータ版の時点でもほぼ完成品に近い状態でテストしていただくことができました」

「実際のところ、機能を新たに追加してほしいといった要望はほとんどありませんでした。むしろ多かったのは、新しい機能を使いこなすにはシステムをどのように構成したらよいか、マイクロソフトではどのように使っているのか、といったフィードバックでした。そうしたお客様には米国にあるEnterprise Engineering Center(EEC)や、東京・品川本社にあるマイクロソフトテクノロジーセンター(MTC)をご紹介し、EECやMTCで構築・評価された結果をお



図2 Windows Server 2012のエディション



持ち帰りいただけるようにしました。2011年に起きた東日本大震災の直後ということもあり、ほとんどの企業がHyper-Vレプリカを試されていたようです」

また、Windows Server 2012対応製品を開発・販売するパートナー企業も対応を急ピッチで進めている。「Windows Server Catalog」([URL http://www.windowsservercatalog.com/](http://www.windowsservercatalog.com/))に掲載されている「Certified for Windows Server 2012」取得済み製品は、ハードウェアが671件(2012年9月8日現在)、ソフトウェアが94件(同)。APIの仕様はWindows Server 2008 R2とほぼ同じなので、既存のハードウェア/ソフトウェア製品をWindows Server 2012に対応させるのにそれほど時間はかからないと梅田氏は見ている。

クラウドと新規データセンターに 踏み込んでいくことが当面の重要目標

マイクロソフトの2013会計年度(2012年7月1日～2013年6月30日)の注力分野は、「デバイス」「クラウド」「ソリューション」の3つ。このすべての分野に関係するWindows Server 2012には、過去最大級の投資(2012会計年度の2倍)をすると同社は発表している。

「ぜひ踏み込んでいきたい市場としては、クラウドと新規データセンターがあります。Windows Server 2012ではそうした市場向けの機能を特に強化してありますから、お客様にも必ず大きなメリットをもたらすことでしょう」

アプリケーション開発者が集まるコミュニティに

対しても、これまでと同様、積極的な働きかけをしていきたいと梅田氏は言う。

「ソーシャルメディアやソーシャルゲームのソフトウェアを開発している業界、企業では、質の高いプログラマーを恒常的に求めています。そこで、われわれは、Windowsプログラマーの方々とソーシャル業界をマッチングさせるお手伝いをしたいと考えています。ソーシャルの世界でもWindows Serverは広く使われているということが知られていけば、望ましい成果が出るのではないのでしょうか。エモーショナルな側面も含めてアプリケーション開発者の方々を動かしていくことにより、必ずや望ましい結果が表れてくるものと期待しています」

「Windows Server 2012は、本格的なクラウド時代を迎えてリリースされる最初のサーバーOSとなる製品です。MSNのようなポータルサービス、Bingのような検索サービス、Windows Update Servicesのようなソフトウェア配布サービス、全世界で数百万台のサーバーを稼働させているWindows Azureなど、マイクロソフトはこれまでも多様なクラウドサービスを手がけてきました。これらのサービスを開発・運用する過程でわかった『これが要る』『あれが必要』といったテクノロジーをすべて盛り込んだのが、Windows Server 2012です。中堅・中小規模の企業のオフィスに置かれた1台のサーバーから、エンタープライズの大型データセンターまで、このサーバーOSで“未来を搭載”していただければと思います」

(取材／文 山口学)

評価していただいた方々からは、品質の高さを評価する反応を数多くいただきました。

Concept

Windows Server 2012で 変わるIT基盤

～今、企業システムは新たな段階へと進化する～

ついに正式提供が開始されたマイクロソフトの次世代サーバー・オペレーティングシステム(OS)「Windows Server 2012」。2008年に発売されたWindows Server 2008から4年が経過するあいだに、Windows ServerとITを取り巻く世界はどのように変化したのだろうか。まずは、Windows Server 2012のコンセプトから探ってみよう。

創報 山近 慶一 / Microsoft MVP Windows Server System - Microsoft Update Service

クラウドサービスのための 新たなサーバーOSへ

Windows Server 2012は、かつてないほど明確なコンセプトに基づいて設計開発が進められてきた。現在より一步先のサーバーOSに求められる機能を提供するために、一部は最新のクライアントOSとなる「Windows 8」や統合システム運用管理スイート製品である「System Center 2012」と組み合わせることで実現されるが、まちがいにWindows Server 2012はこれからの企業ITを支えるコアとなるOSである。

しかし、ITの世界も世の中の流れと無縁ではられない。長引く不況、円高、株安、少子高齢化といった現在の社会・経済環境下においては、ITにも強烈なコストダウンの要求が突きつけられている。そこでWindows Server 2012では、「クラウド」と「仮想化」という、非常に重要なテクノロジーを2大コンセプトとして全面に打ち出すことで、このシビアな状況を乗り越えようとしているのだ。

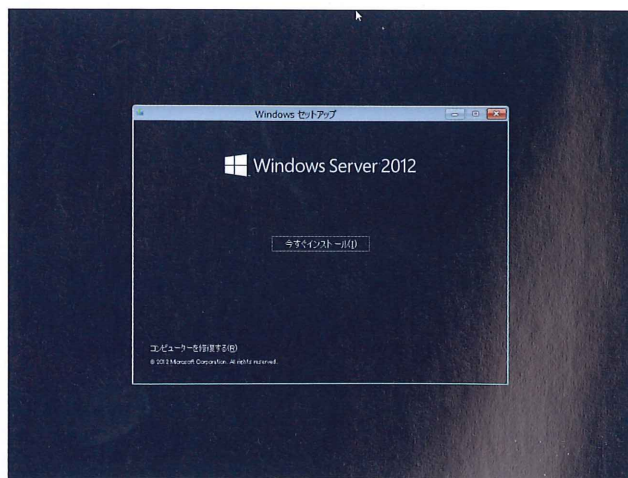
また、2010年から2011年にかけて急激に普及率を伸ばしたスマートフォン、いわゆる「スマホ」は、外見上は「ハンディPC＋電話」である。同様の製品はすでに何年も前からPHSなどで実現されていたので、実はそれほど真新しいものではない。重要なのは「高速モバイルネットワークへの常時接続」というバックボーンに支えられた、いつでも、どこでも“サービスをタイムリー

に利用する”という消費行動の変化、つまり「クラウドサービス」の浸透である。

Windows Server 2012には、クラウドサービスをエンタープライズで展開するために必要な機能が積極的に搭載されている(画面1)。その中心となるのが、仮想化技術「Hyper-V」とWindows Azureになる(画面2)。

ハイブリッドクラウドへの 本格対応を実現するテクノロジー

Windows Server 2012では、OSと仮想化基盤(Hyper-V)



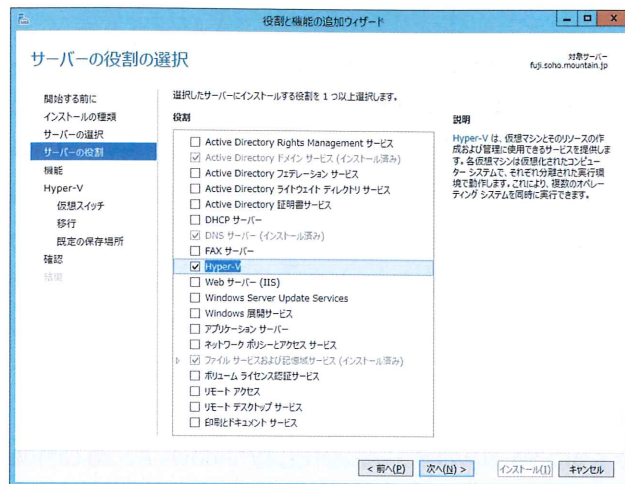
画面1: Windows Server 2012のインストール画面。Windows Server 2012は企業内でクラウドサービスを展開するための機能が多数搭載されている

が1つのパッケージになっており、仮想デスクトップインフラストラクチャ(VDI)を容易に構築できるようになっている(画面3)。例えば、DaaS(Desktop as a Service)としてパーソナライズされた仮想デスクトップをユーザーに割り当てたり、共通の仮想デスクトップ環境を公開したりすることも可能だ(※便宜上DaaSはOSをサービスとして公開する形式と定義した)。

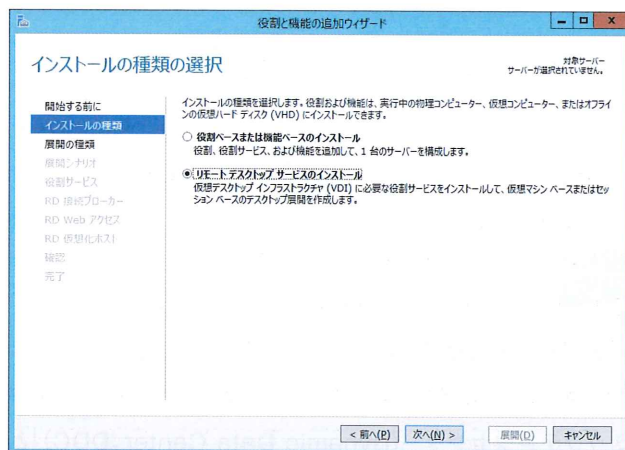
また、仮想化環境上で実行するアプリケーションを「RemoteApp」として公開し、ユーザーにアプリケーションを提供するSaaS(Software as a Service)を構築することもできる。このように、プライベートクラウド構築の基盤として、大規模なシステム構築に耐えるスケーラビリティと、IaaS(Infrastructure as a Service)からSaaSまで構築可能な汎用性、柔軟性を兼ね備えているのがWindows Server 2012なのである。

外部プロバイダーが提供する「パブリッククラウド」と、エンタープライズ内のプライベートクラウドを組み合わせることで、システム/サービス展開スピードの向上、利用シーンの拡大、セキュリティ維持、コストダウン、柔軟性アップなどを目指すのが「ハイブリッドクラウド」だ。効果的なハイブリッドクラウド環境を構築するためには、「データベースのデータ同期」「アプリケーション連携」「相互認証」「システム間の仮想ネットワーク接続」などのポイントがあるが、パブリッククラウドサービスにWindows AzureおよびパートナーがWindows Server 2012をベースに提供するクラウドサービスを、プライベートクラウドにWindows Server 2012を採用することにより、両社同じプラットフォーム、同じデータベース、同じアプリケーションで構築することが可能となり、両者間のシームレスな連携も非常に容易になる。

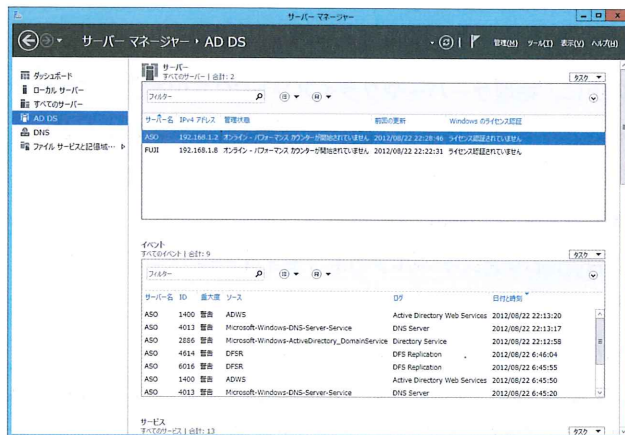
例えば、クラウドシステムにおいては、ユーザー、コンピューター、Webサイト、モバイル端末、ネットワーク機器などを認証する機能は必須になるが、認証情報をすべてパブリッククラウドに置くと、セキュリティリスクと管理コストが高くなってしまふ。そこで、オンプレミスの「Active Directoryドメインサービス(AD DS)」をパブリッククラウドでも利用できるようにするために、Windows Server 2012には「Active Directoryフェデレーションサービス」が搭載されている(画面4)。



画面2: Windows Server 2012には仮想化基盤「Hyper-V」が標準搭載される



画面3: Windows Server 2012では、標準機能だけで容易に「仮想デスクトップインフラストラクチャ (VDI)」環境を構築できる



画面4: Windows Server 2012の「Active Directoryドメインサービス (AD DS)」

また、クライアントPC資産管理とセキュリティ管理サービスの「Windows Intune」、Officeアプリケーション&コラボレーションサービスの「Office 365」、顧客管理システムの「Microsoft Dynamics CRM Online」は、Windows Azureの認証サービスである「Windows Azure Active Directory」を利用して構築されている。すでにActive Directoryの認証サービスまでがクラウドサービス化されており、シングルサインオン(SSO)環境とアプリケーションの利用制限をハイブリッドクラウド環境で容易に構築することができる。

さらに、Windows Server 2012に「Windows Azure Online Backup Agent」をインストールすることで、Windows Azure Online Backupサービスを利用したクラウドへのバックアップも可能になる。

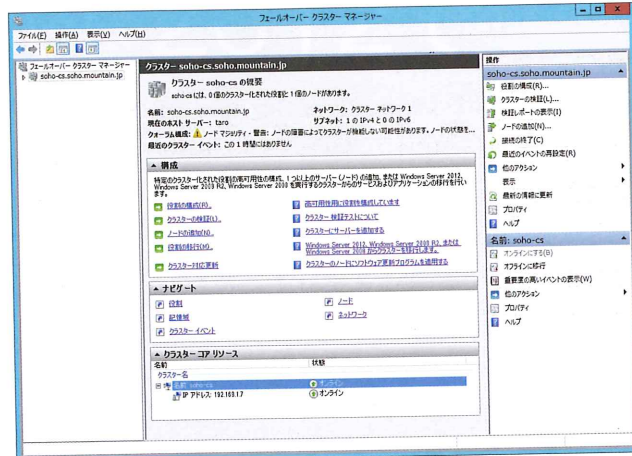
このように、Windows Server 2012はOS単体で完結するのではなく、Windows Azureなどのパブリッククラウドとの連携を強く打ち出した、最初のWindows Serverとなる。

ダイナミックデータセンターの実現に向けた進化

ユーザーが必要とするリソースをタイムリーに提供し、ニーズの変化にも迅速に対応可能なデータセンターを、「ダイナミックデータセンター(Dynamic Data Center:DDC)」と呼ぶ。DDCを構築するためのポイントが、「統合化」「仮想化」「自動化」の3つになる。

Windows Server 2012では、仮想化基盤であるHyper-Vの上に、物理サーバーやクライアントPCを仮想化して集約することが可能だ。また、迅速な障害復旧で可用性を高める「フェールオーバークラスタリング」と、ファイル共有サーバー機能を組み合わせた「スケールアウトファイルサーバー」、さらにHyper-Vとスケールアウトファイルサーバーを組み合わせた「Hyper-V over SMB」なども、統合化と仮想化をローコストで実現するための重要な新機能である(画面5)。

Windows Server 2012では、DDCを実現するために表1のような仮想化機能の基本性能の底上げが行われている。高性能なCPU、大容量メモリ、大容量ディスクを搭載したサーバー



画面5:「フェールオーバークラスタリング」により、障害が発生しても迅速に復旧することが可能になる

表1: Windows Server 2012で強化された仮想化機能の基本性能

物理環境	Windows Server 2012	Windows Server 2008 R2 SP1
物理プロセッサ数(ソケット数)	64CPU	64CPU
論理プロセッサ数	640CPU	256CPU
メインメモリ容量	4TB	1TB
仮想化環境	Windows Server 2012	Windows Server 2008 R2 SP1
仮想プロセッサ数	2,048CPU	512CPU
仮想マシン1台あたりの仮想プロセッサ数	64CPU	4CPU
仮想マシン1台あたりのメインメモリ容量	1TB	64GB
仮想ディスクのサイズ	64TB (VHDX)	2TB (VHD)
クラスター環境	Windows Server 2012	Windows Server 2008 R2 SP1
クラスターノード数(物理サーバー)	64ノード	16ノード
クラスターノード数(仮想マシン)	8,000ノード	1,000ノード

ハードウェアがリーズナブルな価格で入手可能になったことから、従来はコスト的にも運用的にも大規模なデータセンターでしかできなかったようなシステムの集約化と仮想化が、企業の一部門レベルでも可能になってきている。特に、マルチCPU、マルチコア環境を実現する「NUMA(Non-Uniform Memory Access)」システムへの最適化を積極的に推し進めたことで、論理CPUとメモリの利用効率が向上したことも、大規模な仮想化環境を容易に構築できるようになった要因の1つである。

3つ目のポイントとなる自動化については、Windows

Server 2012にはHyper-V仮想マシンのサイト間複製を自動的に実行する「Hyper-Vレプリカ」や、リモートデスクトップサービスで仮想マシンを自動的に複製して必要量の仮想デスクトップ環境を構築する「仮想マシンの自動作成」などがあり、運用管理の一部を自動化することができる。より本格的な自動化が必要であれば、Windows Server 2012をベースとしてSystem Center 2012による運用管理サービス環境を構築することで対応可能だ。

ライセンスモデルからみた Windows Server 2012のコンセプト

Windows Server 2012では、「Datacenter」「Standard」「Essentials」「Foundation」の4つのエディションが用意される(表2)。一般的なビジネス向けのエディションが、DatacenterとStandardになる。EssentialsとFoundationはクライアント数や機能に制限があり、スモールビジネスや単機能サーバー向けのエディションといえる。エディションとライセンス体系についてはPart4で詳説する。

DatacenterとStandardでは、物理プロセッサ数(物理

CPU数)と仮想マシンのインスタンス数によってライセンスを区分する「プロセッサライセンス」が導入された。どちらも1プロセッサライセンスで2個の物理CPUをカバーするが、Datacenterでは仮想マシンを無制限に実行できるのに対して、Standardでは最大2インスタンスの実行に制限される。例えば、2CPUシステムで4台の仮想マシンを実行するには、Datacenterでは1プロセッサライセンスでよいが、Standardでは2プロセッサライセンスが必要となる。

以上のように、仮想化を強力に推進し、分散したサーバーを集約する方針がライセンス体系にも表れている。高速で信頼性の高いネットワーク環境が安価で構築できるようになった現在、Windows Server 2012を利用して全国各地に分散したサーバー群をデータセンターに集約し、リモートから利用することでコストダウンと人、金、モノの集約をはかるシステム設計、すなわちプライベートクラウドの構築と、不足するサービスは外部から安価でスピーディに調達し、プライベートクラウドと組み合わせてシステム全体の価値を高めるハイブリッドクラウドが、現在の情報システムに求められている“現実解”となるだろう。

表2: Windows Server 2012のエディション構成とライセンス体系(筆者調べ)

エディション	Datacenter	Standard	Essentials	Foundation
最適な用途	データセンター 高集約度の仮想化サーバー プライベートクラウド	通常集約度の 仮想化サーバー プライベートクラウド	スモールビジネス	単機能サーバー
ライセンスモデル	プロセッサライセンス + CAL	プロセッサライセンス + CAL	サーバーライセンス (最大25ユーザー アカウント)	サーバーライセンス (最大15ユーザー アカウント)
1プロセッサライセンスで実行可能なOSインスタンス数 (物理環境)	1	1	1 (仮想化環境と排他利用)	1
1プロセッサライセンスで実行可能なOSインスタンス数 (仮想化環境)	無制限	最大2インスタンス	1 (仮想化環境と排他利用)	—
1プロセッサライセンスでサポートする 物理プロセッサ数	2	2	2	1
販売チャネル	ボリュームライセンス OEM Services Provider License Agreement (SPLA)	ボリュームライセンス OEM 店頭 SPLA	ボリュームライセンス OEM 店頭 SPLA	OEMのみ

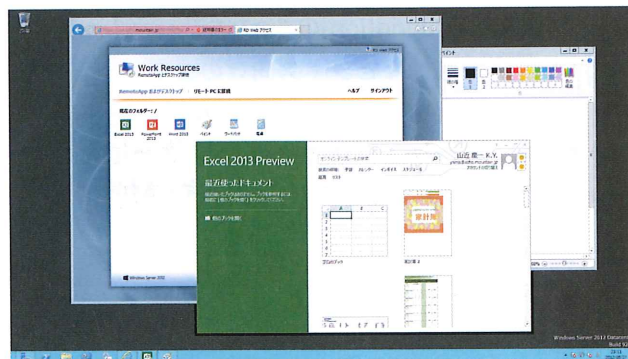
“Better Together”を実現するのは Windows 8

最後に、新しいクライアントOSとなる「Windows 8」との関係についても触れておこう。Windows 8は、タブレット（スレート）PCやマルチタッチ向けの新しいユーザーインターフェース、マイクロソフトのクラウドサービス（メールサービスのOutlook.comや、ストレージサービスのSkyDriveなど）との連携が注目されている（画面6）。しかし、Windows Server 2012との連携で実現されるさまざまなエンタープライズ向けの高機能がある。



画面6：最新のクライアントOSとなるWindows 8は、Windows Server 2012との高い親和性が最大のウリだ

Windows 8はWindows Server 2012と同じコードベースで開発が進められてきたこともあり、当然、Windows Server 2012との親和性も高い。例えば、Windows Server 2012でさらに強化されたActive Directoryドメインサービスが提供する「グループポリシー」は、Windows 8に完全対応済み。クライアントPC環境やセキュリティの集中管理もこれまでよりもはるかにきめ細かく、そして容易になるだろう。また、セキュアなリモートアクセス環境を実現する「DirectAccess」や「RemoteApp」も、より簡単に展開が可能になる（画面7）。このほか、最新のリモートデスクトッププロトコル[RDP 8.0]により、VDIゲストとしてのエクスペリエンスも向上する。



画面7：Windows Server 2012とWindows 8の連携で実現する「RemoteApp」

【参考Webサイト】

- ▶ **Windows Server 2012 のコンセプトを知る**
[URL](http://www.ustream.tv/recorded/23181844) <http://www.ustream.tv/recorded/23181844>
- ▶ **ハイブリッドクラウド：全体像とシナリオを理解する | TechNet**
[URL](http://technet.microsoft.com/ja-jp/cloud/gg545335.aspx) <http://technet.microsoft.com/ja-jp/cloud/gg545335.aspx>
- ▶ **Windows Azure Active Directory**
[URL](http://technet.microsoft.com/ja-jp/library/hh967619) <http://technet.microsoft.com/ja-jp/library/hh967619>
- ▶ **Announcing the Developer Preview of Windows Azure Active Directory**
[URL](http://blogs.msdn.com/b/windowsazure/archive/2012/07/12/announcing-the-developer-preview-of-windows-azure-active-directory.aspx) <http://blogs.msdn.com/b/windowsazure/archive/2012/07/12/announcing-the-developer-preview-of-windows-azure-active-directory.aspx>
- ▶ **Single Sign On with Windows Azure Active Directory : a Deep Dive**
[URL](http://blogs.msdn.com/b/vbertocci/archive/2012/07/12/single-sign-on-with-windows-azure-active-directory-a-deep-dive.aspx) <http://blogs.msdn.com/b/vbertocci/archive/2012/07/12/single-sign-on-with-windows-azure-active-directory-a-deep-dive.aspx>
- ▶ **Windows Azure Active Directory ID**
[URL](http://www.windowsazure.com/ja-jp/home/features/identity/) <http://www.windowsazure.com/ja-jp/home/features/identity/>
- ▶ **Dynamic Data Center**
[URL](http://www.microsoft.com/ja-jp/hosting/dynamicdatacenter/default.aspx) <http://www.microsoft.com/ja-jp/hosting/dynamicdatacenter/default.aspx>
- ▶ **Microsoft Online Backup Service Overview**
[URL](http://technet.microsoft.com/en-us/library/hh831419.aspx) <http://technet.microsoft.com/en-us/library/hh831419.aspx>

Windows Server 2012 導入と活用のシナリオ

～ 5つのシナリオで理解する導入と活用のメリット～

Windows Server 2012には“クラウド”と“仮想化”をコンセプトとした新機能、機能強化が多数盛り込まれている。本稿では「Active Directoryドメインサービス」「スケールアウトファイルサーバー」「リモートデスクトップ」「仮想デスクトップインフラストラクチャ (VDI)」をテーマにして、導入のメリットと具体的な構築手順をチェックする。

創報 山近 慶一 / Microsoft MVP Windows Server System - Microsoft Update Service

[シナリオその1]

Active Directory ドメインサービス① ドメインコントローラーを追加する

Windowsベースの企業ネットワークにおいて、Active Directoryはユーザー認証とアクセス制御をつかさどる最重要基盤となる。Windows Server 2012のユーザー認証機能は、「Active Directoryドメインサービス(AD DS)」をコアとして構築される。システム内部的にはWindows Server 2008以降、「Active Directory Domain Services」という1つのバックグラウンドサービスとして実装されているので、AD DSをメンテナンスするためにドメインコントローラー(DC)を停止しなくて済むようになっている。また、DCをHyper-Vの仮想マシン上で実行可能になった点も見逃せない。

さて、これからWindows Server 2012 DCを全国展開しようとする場合、基本的には既存のActive DirectoryドメインにWindows Server 2012 DCを追加し、新旧のWindows Serverを並行運用しながら、順次DCをリプレースすることになるだろう。また、Windows Server 2012 DCを信頼できる拠点でセットアップしてから、全国の各拠点に移送、設置する必要もある。既存のDCが64ビット版のWindows Serverで構築されていれば、そのDCを直接Windows Server 2012にアップグレードする「インプレースアップグレー

ド」も可能だ。しかし、32ビット版のWindows Serverの場合、インプレースアップグレードを実行することはできないので、別のサーバー機にWindows Server 2012 DCを用意して切り替えることになる。

これまで、既存のActive Directoryドメインに新しいDCを追加するには、物理サーバーにWindows ServerのユニークなインスタンスをインストールしてからDCに昇格し、その後、全国の拠点に送り届けてから運用することが多かった。その理由は、仮想化環境上でのDCの実行が推奨されていなかったためである(詳しくは次稿で解説する)。また、この方法では、Windows Serverのインストールと昇格操作に必要な情報をあらかじめ「応答ファイル」に記述しておけば無人インストールを実現できるとはいえ、基本的にクリーンインストールが必要となるので時間がかかるし、運搬と設置までを考えると相当な労力とコストが必要になる。

Windows Server 2012では、Hyper-V仮想マシン上でDCを安全に実行およびメンテナンスできるようになった。これにより、DCの展開は仮想マシンをネットワーク経由で拠点に送信し、拠点にあるHyper-Vサーバー上で起動するだけになった。しかも、Windows Server 2012では特定の仮想マシン上のDCを複製することで、新しいDCを作り出す「クローニング」による展開も可能になっている。クローニングによる展開はSysprepでの展開とは異なり、複製したソース

を再びオンラインにするだけでDCの機能を継続できるので、展開コストは最初の1台をセットアップするぶんだけというメリットもある。

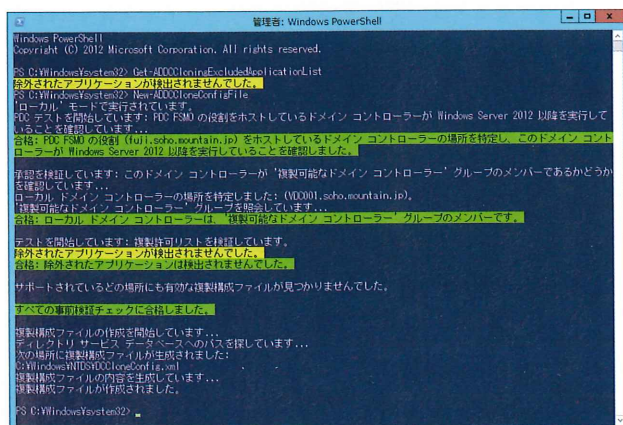
【このシナリオで利用する役割と機能】

Active Directory ドメインサービス、DNS サーバー、Hyper-V

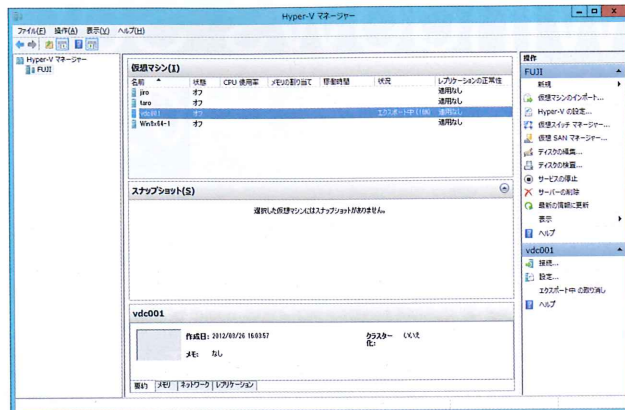
【構築手順】

- ①複製ソースとなるDCのコンピューターアカウントを「Cloneable Domain Controllers」グループのメンバーに追加する。
- ②複製ソースDC上で、Windows PowerShellを「管理者モード」で開き、PowerShellコマンドレット「Get-ADDCCloningExcludedApplicationList」「New-ADDCCloneConfigFile」を実行する(画面8)。
- ③複製ソースDCをシャットダウンし、Hyper-V マネージャーで仮想マシンをエクスポートする(画面9)。
- ④展開先のHyper-V マネージャーで、「仮想マシンをコピーする(新しい一意なIDを作成する)」オプションを選択してインポートする(画面10)。
- ⑤クローンDCの仮想マシン設定、IPアドレス、DNS参照設定、サイトやサブネットを適切に調整する。

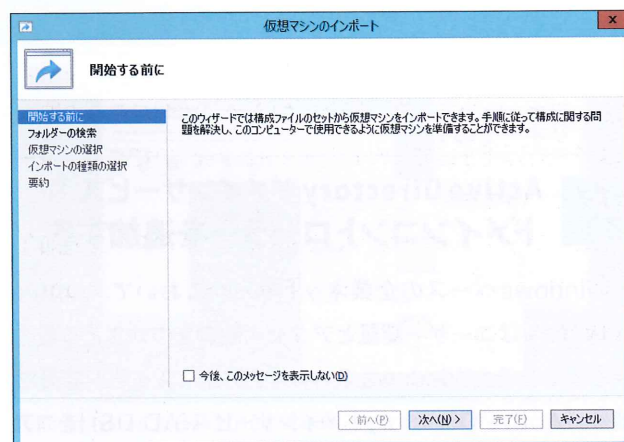
※ New-ADDCCloneConfigFile コマンドレットを引数なしで実行すると、ホスト名は「<ソースDC名>-CLnnnn」(nnnnは4けたの連番)、IPアドレスとDNS参照設定はDHCPによる自動設定となる。



画面8：PowerShellコマンドレットを管理者モードで実行する



画面9：複製ソースとなるDCをHyper-V マネージャーでエクスポートする



画面10：展開先のHyper-V マネージャーで、仮想マシンをインポートする

【参考Webサイト】

▶ Introduction to Active Directory Domain Services (AD DS) Virtualization

URL <http://technet.microsoft.com/en-us/library/hh831734.aspx>

【シナリオその2】

Active Directory ドメインサービス② インプレースアップグレードを実行する

64ビット版のWindows Server 2008またはWindows Server 2008 R2でDCを構築している環境は、Windows Server 2012に「インプレースアップグレード」できる可能性がある。インプレースアップグレードは既存の設定をすべて引

き継いだままでWindows Server 2012に移行できる、もっとも低コストのアップグレード方法となる。

インプレースアップグレードを行うには、次の3つの条件をクリアしている必要がある。

条件1：既存のDCが64ビット版のWindows Server 2008

またはWindows Server 2008 R2を実行している

条件2：ハードウェア(デバイスドライバ)とアプリケーションがWindows Server 2012に対応している

条件3：フォレストの機能レベルが「Windows Server 2003」以上である

Windows Server 2003(R2)は直接アップグレードすることはできないので、先に紹介した「シナリオ1」のDCの追加による並行運用を経て、Windows Server 2012にリプレースするとよいだろう。

なお、フォレスト内のすべてのドメインで次の2つの追加条件を満たす場合のみ、フォレストの機能レベルを「Windows Server 2003」以上に設定できる。

条件3-1：DCがすべてWindows Server 2003以降である

条件3-2：ドメインの機能レベルが「Windows Server 2003」以上である

したがって、まず機能レベルの要件を満たすようにフォレストを再構成することが、Active Directoryドメインのアップグレード工程における最初のステップとなる。そのためには、機能レベルを引き上げる前に、ドメインやフォレストの機能レベルを上げることで有効になる新機能と、その影響をチェックする必要がある。

ドメイン内のすべてのDCがWindows Server 2012を実行している場合は、新しいドメイン機能レベル「Windows Server 2012」を選択することができる。この機能レベルでは、Kerberos認証に関する次のグループポリシー設定を利用できる(画面11)。

ポリシーのパス：[コンピューターの構成]-[ポリシー]-[管理用テンプレート]-[システム]-[KDC]

ポリシーの名前：KDCで信頼性情報、複合認証、およびKerberos防御をサポートする

ポリシーの設定：[常に信頼性情報を提供する]または[防御されていない要求を失敗とする]

そして、全ドメインの機能レベルが「Windows Server 2012」であれば、フォレストの機能レベルも「Windows Server 2012」に設定できる。ただし、Windows Server 2012のリリース時点において、このフォレスト機能レベルによる新機能は特にない。

【このシナリオで利用する役割と機能】

Active Directoryドメインサービス、DNSサーバー

【構築手順】

①全ドメインのDCをWindows Server 2003以降にして、ドメインの機能レベルを「Windows Server 2003」以降に引き上げる。

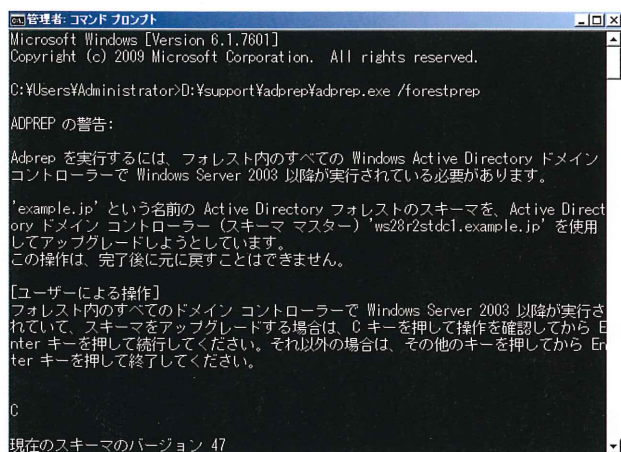
②フォレストの機能レベルを「Windows Server 2003」以降



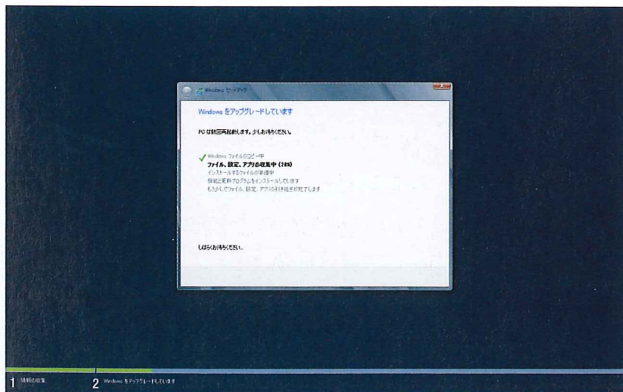
画面11：Windows Server 2012で利用可能なKerberos認証に関するグループポリシー設定

に引き上げる。

- ③ 64ビット版のWindows Server 2008(R2)を実行するDCに、Windows Server 2012のインストールメディアをセットする。
- ④ 「<ソースドライブ>%support¥adprep¥adprep.exe」コマンドを、「/forestprep」「/domainprep」「/domainprep /gpprep」「/rodcprep」の各スイッチを指定して順番に実行し、ディレクトリデータベースのスキーマを拡張する(画面12)。
- ⑤ Windows Server 2012のセットアップを開始して、アップグレードインストールを実行する(画面13)。



画面12: 「adprep.exe」コマンドを実行して、ディレクトリデータベースのスキーマを拡張する



画面13: Windows Server 2012のアップグレードインストールを実行する

【参考Webサイト】

▶ Windows Server 2012 へのドメインコントローラーのアップグレード

URL <http://technet.microsoft.com/ja-jp/library/hh994618.aspx>

【シナリオその3】

スケールアウトファイルサーバー 低コストで信頼性、可用性、保守性を向上

システムのコストを押し上げる要因として無視できないものに、ストレージの容量と価格が挙げられる。簡単に言えば、大容量、高速、高信頼性のストレージサブシステムは高価で手がかかるのである。もし、SQL ServerのデータベースファイルやHyper-Vの仮想ディスクファイルを安価なファイルサーバーの共有フォルダーに保存することができれば、ストレージの価格も安くなるし、アプリケーションサーバーの増減のたびにSAN(Storage Area Network)のファブリックを再構成するコストも不要になる。

もちろん、単なる共有フォルダーにはSANを置換できるほどの高い信頼性、可用性、保守性はない。もし、1台の物理サーバーと1台の物理ディスクでファイルサーバーを構築すれば、そのサーバー本体やハードディスクが単一障害点(Single Point of Failure: SPOF)となり、性能や稼働率などのサービスレベルを満たすことはできないだろう。

そこで、信頼性、可用性、保守性を向上させると同時にコストを抑えるWindows Server 2012の標準機能が「スケールアウトファイルサーバー(SOFS)」になる。SOFSは最大4ノードで構成されたフェールオーバークラスターを基盤とし、ノード間の共有ディスク上に構成した共有フォルダーをクライアントに公開することができる。

SOFSは全ノードが同時にアクティブになる「アクティブアクティブ」構成となるので、どのノードもクライアントのファイル読み書き要求を受けられるだけでなく、同じ共有ディスク上の記憶領域を同時に読み書きできるので、ノードを増設(スケールアウト)するほど、また共有ディスクを増設するほど、サー

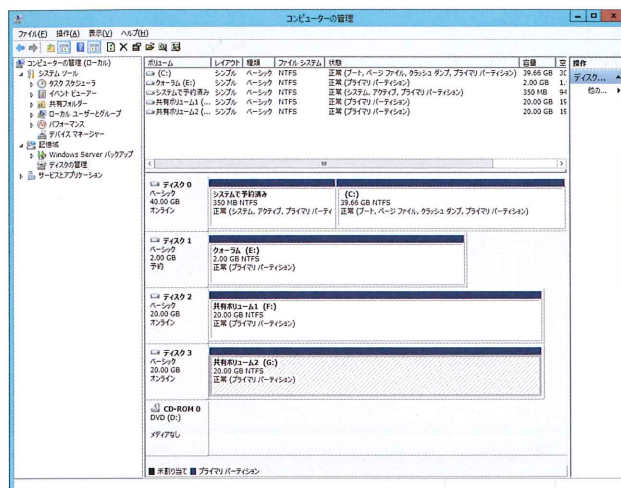
バー、ディスク、ネットワークの使用率が高まり、より多くのクライアントが接続できるスケーラブルなファイルサーバーを構築できる。フェールオーバークラスタリングは、Hyper-Vを使って仮想マシンで簡単に構築できる。

【このシナリオで利用する役割と機能】

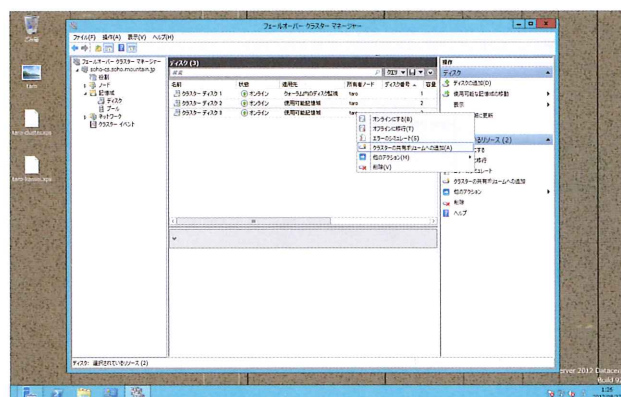
フェールオーバークラスタリング、クラスターの共有ボリューム、ファイルサーバー(SMB 3.0、SMB透過フェールオーバー、SMBマルチチャネル、SMBダイレクト)、Hyper-V

【構築手順】

- ① ドメインのメンバーコンピューターを2台以上用意し、フェールオーバークラスタリングを構築する。
- ② 1台のノードを残して全ノードをシャットダウンし、[コンピューターの管理] - [記憶域] - [ディスクの管理]で、SOFSに使用する共有ディスク領域を準備する(画面14)。
- ③ 「フェールオーバークラスタマネージャー」で、[ディスクの追加]を実行する。
- ④ シャットダウンしたノードを起動する。
- ⑤ フェールオーバークラスタマネージャーで、SOFSに利用するディスクを選択して[クラスターの共有ボリュームへの追加]を実行する(画面15)。
- ⑥ サーバーマネージャーの[役割と機能の追加]で、全ノードに[ファイルサービスおよび記憶域サービス] - [ファイルサービスおよびiSCSIサービス] - [ファイルサーバー]の役割サービスをインストールする。
- ⑦ フェールオーバークラスタマネージャーで、[クラスター名] - [役割]を右クリックして[役割の構成]を実行する。
- ⑧ [高可用性ウィザード]で[ファイルサーバー]の役割を選択し、[アプリケーションデータ用のスケールアウトファイルサーバー]を指定する(次ページの画面16)。
- ⑨ クライアントがアクセスするSOFSの名前を指定して、高可用性ウィザードを完了する。
- ⑩ 作成した役割を右クリックして[ファイル共有の追加]を実行し、[SMB共有 - アプリケーション]を選択する。
- ⑪ ボリューム、共有名、アクセス権を設定して公開する(次ページの画面17)。



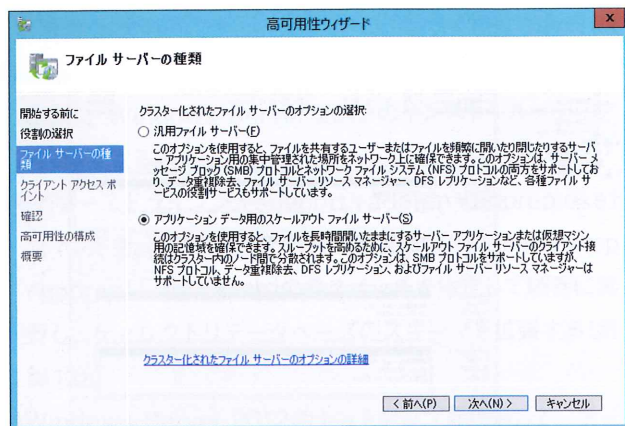
画面14: SOFSに使用する共有ディスク領域を準備する



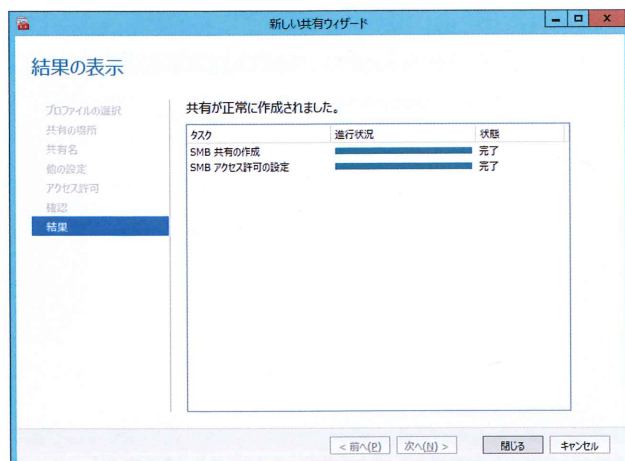
画面15: SOFSに利用するディスクを選択して [クラスターの共有ボリュームへの追加]を実行する

- ⑫ Hyper-Vで仮想マシンを作成して、手順①で設定した共有フォルダーに仮想ディスクファイルを保存する。

なお、[Active Directoryユーザーとコンピューター]で、クラスターノードのコンピューターアカウントを既定の[Computers]コンテナから任意のOUに移動した場合は、そのOUに対してクラスター名のコンピューターアカウントがコンピューターオブジェクトの追加や削除を実行できるように、あらかじめ委任を行っておく必要がある。委任設定ができていないと、高可用性ウィザードでファイルサーバーの役割を作成したとき、正常終了にもかかわらず実行時にエラーになってしまうので注意してほしい。



画面16: [高可用性ウィザード]で、[アプリケーションデータ用のスケールアウトファイルサーバー]を指定する



画面17: ボリューム、共有名、アクセス権を設定し、確認後に公開する

【参考ドキュメント】

▶ Understand and Troubleshoot Scale-out File Servers in Windows Server

URL http://download.microsoft.com/download/9/A/9/A9FE5A9-53CC-4D48-BF17-6CC533FDAD80/Understand_and_Troubleshoot_Scale-Out_File_Servers_in_Windows_Server_8_Beta.docx

【シナリオその4】



リモートデスクトップサービス デスクトップエクスペリエンスを向上させる

ユーザーごとに1台ずつPCを用意し、ローカルPCにインストールしたアプリケーションを利用してもらう一般的なシステム構成は、ユーザーの自由度が最も高くなる反面、PCやアプリケーションの構成を管理したり、適切なセキュリティレベルを維持したり、リプレース計画を立てたりするための運用管理コストや負荷が増えてしまう可能性がある。

Windows Server 2012の「リモートデスクトップサービス(Remote Desktop Services: RDS)」が提供する「セッション仮想化」のシナリオを展開すれば、旧式のPCや性能の低いPCでもWindows Server 2012やWindows 8の最新のデスクトップエクスペリエンスを利用できるようになる。クライアントPCはマウスやキーボード、画面の入出力インターフェースとなり、アプリケーションの実行やデスクトップ描画の処理はサーバー側で行われるためだ。

また、RDSサーバー上のアプリケーションを公開して利用してもらう「RemoteApp」を展開すれば、「SaaS」的なシステムをシンプルに構築することも可能になる。RemoteAppでは、アプリケーションはRDSサーバーにのみインストールするので、アプリケーションのバージョンアップ、リプレース、ライセンス管理などが非常に容易になる。

Windows Server 2012にはスピーディにRemoteApp環境を構築できる「クイックスタート展開」機能が搭載されており、RDSのインストールから構成までが自動で行われるようになっている。

RemoteAppをユーザーに違和感なく利用してもらうためには、クライアントPCのデスクトップやスタートメニューに、起動用のショートカットアイコンを登録するなどの配慮が必要になる。ただし、これらの方法ではショートカットアイコンの配布方法とメンテナンスコストが問題になる場合があるだろう。

そこで、Webブラウザ経由でRemoteAppを利用してもらう方法を検討してはどうだろうか。例えば、企業内で利用しているポータルサイトのトップページに「リモートデスクトップ

Webアクセス(RD Webアクセス)やRemoteAppへのリンクを掲載すれば、ユーザーはすぐにRemoteAppにたどり着くことができるので、ショートカットアイコンの配布コストについては考慮する必要がなくなる(画面18)。

【このシナリオで利用する役割と機能】

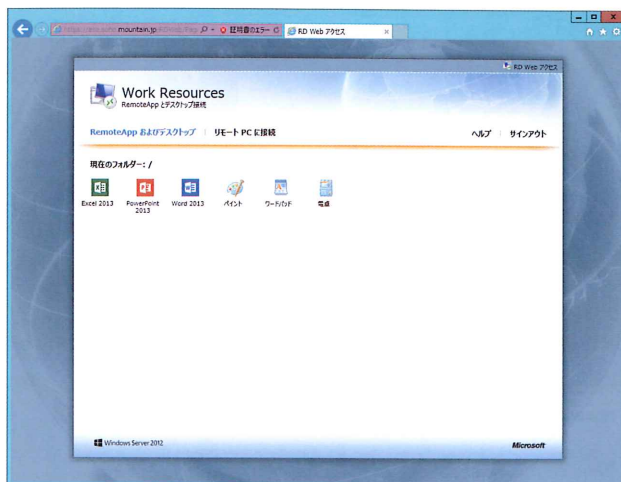
RDS、リモートデスクトップ接続クライアント(RDC)、Webサーバー(IIS 8)

※このシナリオではライセンスを考慮していない。継続的に利用するには、適切なサーバーに「リモートデスクトップライセンスマネージャー (RDLM)」をインストールしてアクティブ化し、別途購入したリモートデスクトップCALを登録する必要があります。

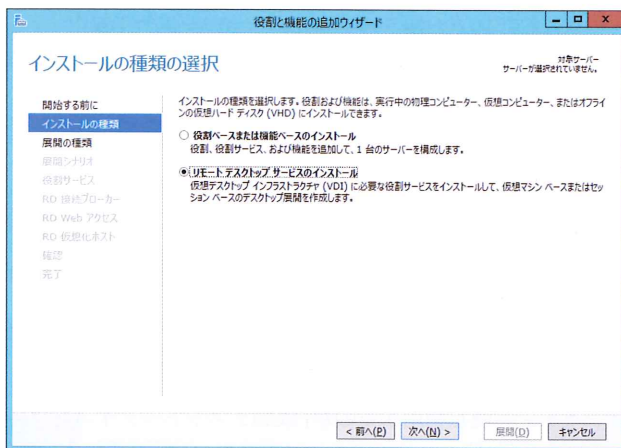
【構築手順】

- 1 RDSサーバーに「Microsoft Office」など、Remote Appとして公開したいアプリケーションをインストールする。
- 2 サーバーマネージャーの「役割と機能の追加」から「リモートデスクトップサービスのインストール」を開始する(画面19)。
- 3 「展開の種類を選択」画面で「クイックスタート」を選択して、次の3つの役割サービスをまとめてインストールする。ただし、DCにRD 接続ブローカーはインストールできない。
 - ・リモートデスクトップセッションホスト(RD セッションホスト)
 - ・リモートデスクトップ接続ブローカー(RD 接続ブローカー)
 - ・リモートデスクトップWebアクセス(RD Webアクセス)
- 4 「展開シナリオの選択」画面で「セッションベースのデスクトップ展開」を選択して、RDSをインストールするサーバーを指定する。
- 5 サーバーマネージャーで「リモートデスクトップサービス」→「コレクション」→「QuickSessionCollection」を展開して、自動的にRemoteAppとして公開されているアプリケーションを確認する(画面20)。既定では「ペイント」「ワードパッド」「電卓」が公開される。
- 6 「RemoteAppプログラム」の「タスク」→「RemoteAppプログラムの公開」を実行して、任意のアプリケーションを公開する。
- 7 クライアントPCのWebブラウザで次のURLに接続してサインイン(ログオン)し、RemoteAppを起動する(次ページの画面21)。

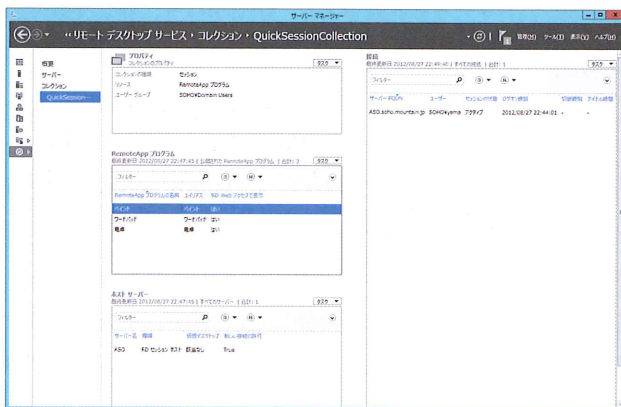
<https://<RDSサーバーのFQDN>/rdweb/>



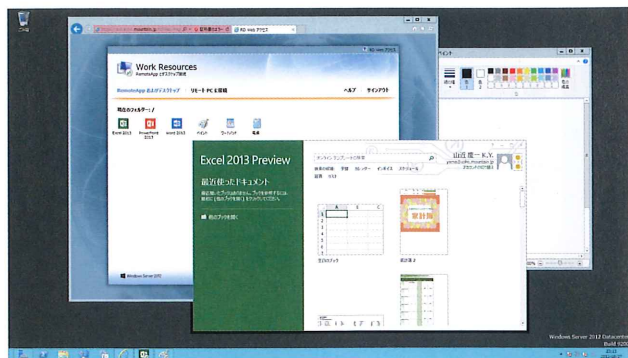
画面18: Webブラウザやポータルサイト経由ならば、ユーザーも違和感なくRemoteAppを利用できる



画面19: 「役割と機能の追加」から「リモートデスクトップサービスのインストール」を開始する



画面20: 「QuickSessionCollection」を展開して、自動的にRemoteAppとして公開されているアプリケーションを確認する



画面 21 : Webブラウザでサインイン (ログオン) し、RemoteApp (Excel 2013 Preview) を起動した様子

【参考ドキュメント】

▶ Understand and Troubleshoot Remote Desktop Services in Windows Server

URL <http://www.microsoft.com/en-us/download/details.aspx?id=29006>

【シナリオその5】

仮想デスクトップインフラストラクチャ (VDI) 柔軟なコンピューティング環境を構築する

RDSを応用して、ユーザーごとに独立した仮想マシンを割り当て、クライアントPCやシンクライアントシステムからデスクトップ環境を利用するのが「仮想デスクトップインフラストラクチャ (Virtual Desktop Infrastructure: VDI)」である。

RDSでは全ユーザーがRDセッションホストのデスクトップエクスペリエンスを共有するが、VDIではユーザーごとに異なるOSインスタンスを割り当てるため、「ローカルPCの利用とほぼ同じシステム環境」を手に入れることができる。すなわち「DaaS」的なシステムを構築できる。

ユーザーに割り当てた仮想マシンでWindows XPなど旧バージョンのWindowsを実行して、既存システムとの互換性を保つこともできるし、最新のWindows 8を提供することもできる。ローカルPCに接続したUSBデバイスを仮想マシンからも利用できるのも、ほとんど違和感がないのがVDIの特徴だ。

どちらのシナリオでも、PCのライフサイクル管理コストが

低減し、オンデマンドで柔軟なコンピューティング環境の提供が可能になる。また、セキュリティが高まりコンプライアンスの向上にもつながる。

【このシナリオで利用する役割と機能】

RDS、RDC、Webサーバー (IIS 8)、Hyper-V

※このシナリオは、RemoteApp用に [クイックスタート] で構成したRDSを使用する。また、継続的に使用するには「リモートデスクトップライセンスマネージャー (RDLM)」をアクティブ化して、別途購入したリモートデスクトップCALを登録する必要がある。

【構築手順】

- ① サーバーマネージャーの [役割と機能の追加] から [リモートデスクトップサービスのインストール] を開始する。
- ② [展開の種類を選択] 画面で、[標準の展開] を選択する。
- ③ [展開シナリオの選択] 画面で、[仮想マシンベースのデスクトップ展開] を選択する (画面 22)。
- ④ RD 接続ブロッカー、RD Webアクセスを選択する。
- ⑤ 「リモートデスクトップ仮想化ホスト (RD 仮想化ホスト)」を選択して、[選択したサーバーに新しい仮想スイッチを作成する] をチェックする。
- ⑥ 「Hyper-V マネージャー」を起動して、仮想デスクトップを自動的に展開するための [テンプレート仮想マシン] を準備する。アプリケーションのインストール、更新プログラムの適用、ユーザープロファイルの編集などを行い、次のコマンドを実行して汎用化 (generalize) しておく。

```
%Windir%\System32\Sysprep\Sysprep.exe /generalize /oobe /shutdown /mode:vm
```
- ⑦ サーバーマネージャーで [リモートデスクトップサービス] - [コレクション] を展開して、[コレクション] グループの [タスク] - [仮想デスクトップコレクションの作成] を実行する。[コレクションの作成ウィザード] で、仮想マシンをグループ化して管理する「コレクション」を作成する。コレクションには「プールされた仮想デスクトップ」と「個人用仮想デスクトップ」があるが、ここでは「個人用仮想デスクトップ」のコレクションを使用する (画面 23)。選択によって表3の操作を実行する。
- ⑧ 手順⑥ で用意したテンプレート仮想マシンを指定して、ユー

表3：仮想デスクトップのコレクションの種類と機能

コレクションの種類	コレクションの機能
プールされた仮想デスクトップ	仮想デスクトップ テンプレートに基づいて仮想デスクトップを新規作成
	仮想デスクトップ テンプレートに基づいて仮想デスクトップを再作成
	ユーザー プロファイル ディスクにユーザー設定を格納
個人用仮想デスクトップ	仮想デスクトップ テンプレートに基づいて仮想デスクトップを新規作成
	仮想デスクトップへの恒久的なユーザー割り当て
	仮想デスクトップに対する管理用のアクセス権

ザーの割り当て方法を選択する。既定では、新しいユーザーが接続したときに、コレクション内の未割り当ての仮想マシンを自動的に割り当てる。

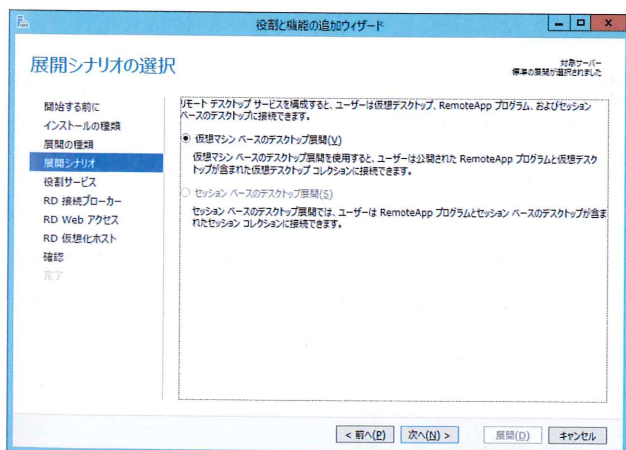
- ⑨ 参加させるドメイン名やコンピューター名の生成規則、自動生成する仮想マシンの数、仮想マシンの保存先などを入力して[作成]をクリックすると、テンプレートから指定数ぶんの仮想マシンが作成される。
- ⑩ クライアントPCのWebブラウザで次のURLに接続してサインイン(ログオン)し、手順⑦で作成したコレクション名をクリックして仮想マシンに接続する(画面24)。

<https://<RDSサーバーのFQDN>/rdweb/>

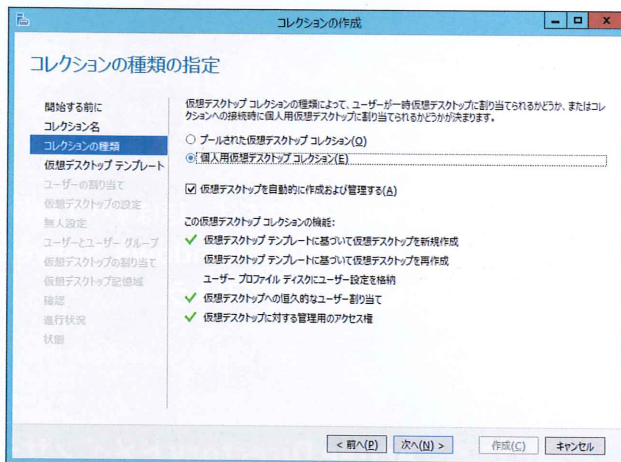
【参考ドキュメント】

▶ Understand and Troubleshoot Desktop Virtualization in Windows Server

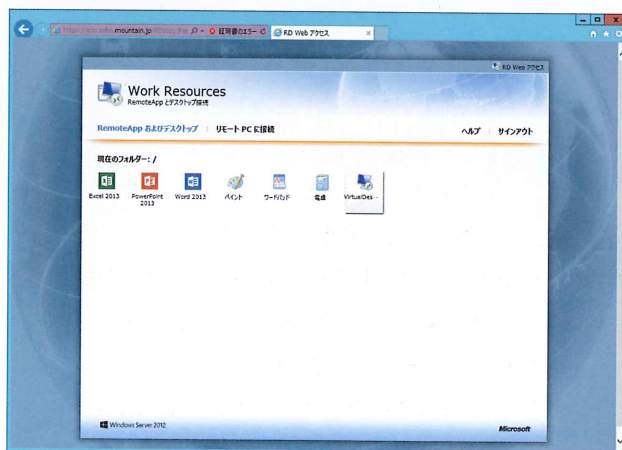
URL <http://www.microsoft.com/en-us/download/details.aspx?id=29022>



画面22：[展開シナリオの選択]で、[仮想マシンベースのデスクトップ展開]を選択する



画面23：「個人用仮想デスクトップコレクション」を選択する(既定値はプール)



画面24：Webブラウザから仮想マシンに接続する

Function

Windows Server 2012 機能詳細

イノベーションを加速する ダイナミックなIT基盤を支えるテクノロジー

Windows Server 2012では、ほぼすべての役割と役割サービス、機能について改良が行われている。本稿では、Windows Server 2012の代表的な役割について新機能と機能強化点をチェックしてみよう。

創報 山近 慶一 / Microsoft MVP Windows Server System - Microsoft Update Service

- [Function 01] Active Directoryドメインサービス
- [Function 02] DHCPサーバー
- [Function 03] DNSサーバー
- [Function 04] Hyper-V
- [Function 05] Webサーバー (IIS)
- [Function 06] ファイルサービスおよび記憶域サービス
- [Function 07] リモートアクセス
- [Function 08] 印刷とドキュメントサービス
- [Function 09] リモートデスクトップサービス
- [Function 10] フェールオーバークラスタリング

[Function 01]

Active Directoryドメインサービス

仮想化対応強化、 展開の柔軟性が向上

「Active Directoryドメインサービス(AD DS)」は、ディレクトリサービスによってユーザー認証基盤を提供する、Windows Serverの中核機能である。Windows 2000から数えて6世代目となるWindows Server 2012のAD DSの主な改良点

は、仮想化環境への対応、迅速なドメインコントローラーの展開、管理ツールである「Active Directory管理センター」のパワーアップなどがある(次ページの画面25)。

Windows Server 2012におけるActive Directoryの新機能と強化点は表4のとおり。

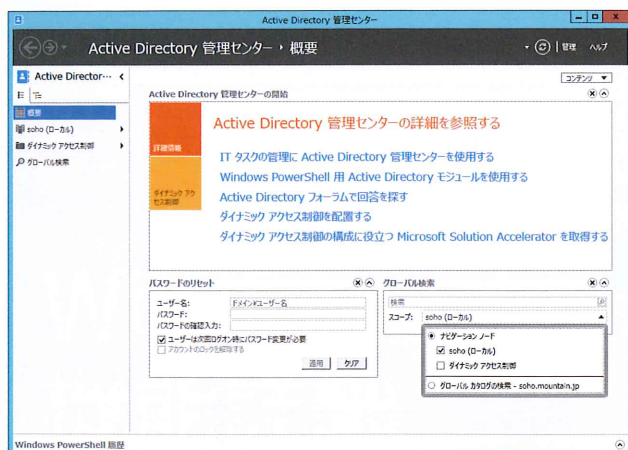


安全なDC仮想化

これまで、ドメインコントローラー(Domain Controller : DC)を仮想化環境上で実行すると、以下のような問題が発生する可能性があることから、仮想化環境上でのDCの実行は積極的に推奨されていなかった。どうしてもDCを仮想環境上で実行したければ、基本的に仮想化環境のメリットであるスナップショット、エクスポートとインポート、仮想マシンや

表4: Active Directoryの新機能と強化点

新機能	安全なDC仮想化	仮想マシンにセットされたGeneration IDを調べてディレクトリデータベースなどのロールバックを検出し、ディレクトリデータベースの不整合やGUIDの重複発行を防止するとともに、自動的に修正する。
	仮想化したDCのクローニング	Hyper-Vの仮想マシン上に構築したDCを複製して、簡単に多数のDCを展開できる。
	Windows PowerShell用AD DSモジュール	AD DSの構成と展開、オブジェクト管理、サイト管理などのための新しいPowerShell用コマンドレットを利用できる。
	ダイナミックアクセス制御	ユーザーやデバイスの証明書に基づいた、信頼性情報(クレーム)によるリソースアクセス許可の直接制御と監査を可能にする。
	ADによるライセンス認証	「ボリュームライセンス認証サービス」と連携して、Windows 8およびWindows Server 2012クライアントについて、AD DSでボリュームライセンス認証オブジェクトを保持する。
機能強化	展開の簡略化	Dcpromoコマンドを廃止し、サーバー マネージャーから昇格と降格の操作を実行できる。インストール プロセスはPowerShellのスク립トとしてエクスポートできるので、他のDCの展開に利用できる。Adprepコマンドによるフォレストやドメインの事前準備作業がインストール プロセスに統合されたため、既存ドメインにWindows Server 2012 DCを追加する際の準備作業が不要になった。ただし、DCのインプレースアップグレード時はAdprepコマンドを手動で実行する必要がある。
	新しい機能レベル	フォレストとドメインの機能レベルに「Windows Server 2012」が追加された。この機能レベルでは、ダイナミックアクセス制御などWindows Server 2012の新機能をすべて利用できる。
	スキーマ更新	Windows Server 2012用にスキーマが拡張されており、バージョン番号が「56」になった。以下は過去のバージョンのActive Directoryのスキーマ バージョン番号一覧である。 Windows 2000:13 Windows Server 2003:30 Windows Server 2003 R2:31 Windows Server 2008:44 Windows Server 2008 R2:47 Windows Server 2012:56
	Active Directory管理センター	ダイナミックアクセス制御の管理と、「Active Directoryのごみ箱」機能の有効化を実行できる。「PowerShell履歴」から、過去の操作をコマンドで参照および再現できる。「細かい設定が可能なパスワード ポリシー」をGUIで設定できる。
	RID管理	オブジェクトに使用する相対ID(RID)の総数が、2の30乗個から2の31乗個(約21億個)に増えたため、IDが不足しにくくなった。相対IDを1億個使用したときや残り10%を切ったときに、イベント ログにイベントを記録する。相対IDの不用意な消費を防ぐため、1度に要求が可能なID数を15,000個までに制限した。
	オフラインドメイン参加	ドメインがDirect Accessを許可していれば、クライアントをインターネット経由でドメインに参加させることができる。
	グループの管理されたサービス アカウント	アプリケーションやサービスの実行ユーザーを、「グループの管理されたサービス アカウント」で実行すると、パスワードをDCただ1カ所で更新するだけで全アプリケーションおよびサービスに反映されるので、メンテナンス コストが低減する。



画面 25 : Windows Server 2012 で強化された「Active Directory 管理センター」

仮想ディスクの複製、差分ディスクの利用、仮想化ホストとの時刻同期といった便利な機能を一切利用せず、Active Directoryに対応したバックアップと復元の仕組みのみを利用することが条件だった。

【問題1】 スナップショットの復元時にディレクトリデータベースの「更新シーケンス番号(USN)」がロールバック(若返り)し、オブジェクトの不整合や複製エラーが発生する。この問題を解決するには、USNがロールバックしたDCを強制的に降格して、メタデータをクリーンアップする必要がある。

【問題2】 GUID(Globally Unique Identifier : グローバル一意識別子)が退行したり、重複したGUIDでオブジェクトが作成されたりする。この問題を解決するには、重複したオブジェクトを探して手動で削除する。

【問題3】 仮想マシンの時刻がPDC(プライマリドメインコントローラー)エミュレータと5分以上ずれることで、Kerberos認証ができなくなる。この問題を解決するには、仮想化環境のホストとは異なるタイムソース、例えば物理サーバー上で実行するDCをタイムソースに指定する。

Windows Server 2012のHyper-V環境では、仮想マシンごとに割り当てられた128ビットの「Generation ID」を使って上記の「問題1」と「問題2」を解決している。具体的には、バックアップやスナップショットからの復元時、仮想マシンのコピーやインポート、クローニング時などにGeneration IDが変化

するので、以前と値が異なっていればロールバックが発生したものと見なし、次の操作を自動的に実行してディレクトリデータベースを自己修復する。

- ◎「invocationID」(ディレクトリデータベースのID)をリセットして不整合を解消する
- ◎相対ID(RID)プールを破棄し、同じIDを持ったオブジェクトが作成されないようにする
- ◎他のDCのディレクトリデータベースを複製して、ディレクトリデータベースをロールフォワードする

この仕組みによって、Hyper-Vのスナップショットやエクスポート／インポート機能などが安全に利用できるようになり、DCの運用管理が非常に楽になる。また、バックアップや復元のためのダウンタイムも最小化することができるので、サービスレベルも向上する。

ところで、2012年8月末日現在、Windows Server 2012のHyper-V以外の仮想化環境はGeneration IDをサポートしていないので、仮想マシンでDCを運用する際には次の点に注意しよう。

- ◎仮想ディスクファイルの盗難、誤消去、不用意なコピーに十分注意する
- ◎仮想マシンをエクスポート／インポートしない
- ◎仮想マシンを長期間オフライン状態にしない
- ◎差分ディスク機能とスナップショット機能を使用しない
- ◎Windowsがサポートしている復元方法以外で復元しない
- ◎仮想化環境が単一障害点(SPOF)になることを避ける
- ◎タイムソースとして、物理サーバーのDCを1台以上用意する

ここで、仮想マシンのオフライン状態について、少し説明しておこう。ディレクトリデータベースには、オブジェクトの有効期間を決定する「tombstoneLifetime」という設定値があり、基本的に「180日」に設定されている。tombstoneLifetimeの値を超えてオフライン状態に置かれたDCでは、ディレクトリデータベースの内容が古すぎて使えなくなってしまう。DCの古すぎるバックアップからの単純な復元が許されないのも同じ理由だ。

また、Active Directoryの「ごみ箱」機能を利用している



画面 26 : tombstoneLifetime の設定値は、Dsquery コマンドで確認できる

場合は、削除されたオブジェクトの有効期間を決定する「msDS-deletedObjectLifetime」という設定値もある。こちらはごみ箱に入ったオブジェクトを復活できるタイムリミットである。

ディレクトリデータベースの“消費期限”、つまり tombstoneLifetime の設定値は次のコマンドで知ることができる(画面 26)。

Dsquery * "CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,DC=<ドメイン名>" -scope base -attr tombstoneLifetime

tombstoneLifetime オブジェクトが見つからない場合は、システムの既定値が採用される。

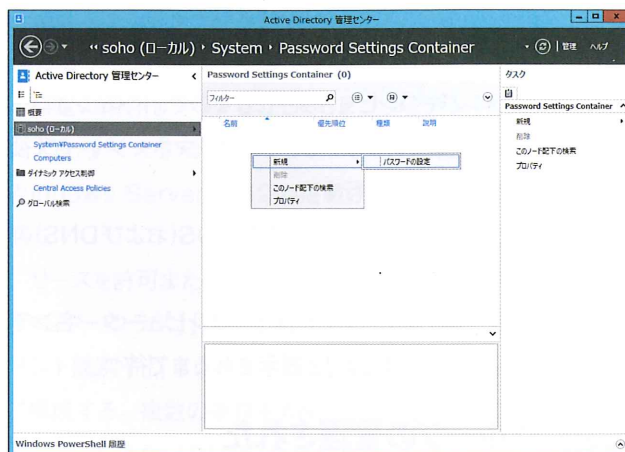
システムの既定値は、Windows Server 2003 までは「60 日」と「180 日」の 2 つが混在しているが、Windows Server 2008 以降では「180 日」に統一されている。とはいえ、旧バージョンの Windows Server からアップグレードした場合は「60 日」の設定を継承している可能性があるので、設定値をしっかりと確認しておこう。



Active Directory 管理センター

DC やオブジェクトの管理を行う「Active Directory 管理センター (Active Directory Administrative Center: ADAC)」では、「ダイナミックアクセス制御」の管理、「Active Directory のごみ箱」機能の有効化、「PowerShell 履歴」によるコマンド参照、「細かい設定が可能なパスワードポリシー」の設定を実行できるように機能が強化された(画面 27)。日常的な運用管理は、すべて Active Directory 管理センターで実行することができる。

例えば、ユーザーやグループ単位でパスワードのポリシーを設定するには、Active Directory 管理センターを次のように操作する。以前のバージョンの Windows Server では、ディレクトリデータベースの中身を直接編集する必要があったが、Windows Server 2012 では GUI で簡単かつ安全に設定できる。



画面 27 : 「細かい設定が可能なパスワードポリシー」も設定可能になった

- ① Active Directory 管理センターの左ペインで、ドメイン名をクリックする。
- ② 中ペインで「System」コンテナをダブルクリックする。
- ③ さらに「Password Settings Container」をダブルクリックする。
- ④ 中ペインで右クリックして、[新規]→[パスワードの設定]をクリックする。
- ⑤ [パスワードの設定の作成] ダイアログで、設定の名前と優先順位、詳細なパスワードオプション、適用先のユーザーやグループを指定する。



DC の昇格と降格

Windows Server 2012 では、DC の昇格と降格を実行する「Dcpromo」コマンドが廃止された。サーバーマネージャーの「役割と機能の追加」で AD DS の役割をインストールした後で、[このサーバーをドメインコントローラーに昇格する]のリンクをクリックして昇格操作を開始するように変更された。

一方、DC の降格は「役割と機能の削除」から次の手順で実行する。

- ① サーバーマネージャーで「役割と機能の削除」を実行して、AD DS の役割の削除を選択する。
- ② 「役割と機能の削除ウィザード」が AD DS を実行中であることを自動検出して、エラーで停止する。
- ③ [このドメインコントローラーを降格する]リンクをクリックして、「Active Directory ドメインサービスの構成ウィザード」を起動する。

- ④ ローカルの「Administrator」のパスワードなどを入力してDCを降格し、再起動する。
- ⑤ ドメインのメンバーコンピューターになるので、ドメインかローカルの管理者としてログオンし、サーバーマネージャーで「役割と機能の削除」を再実行する。
- ⑥ 「役割と機能の削除ウィザード」でAD DS(およびDNS)の役割を削除し、再起動する。
- ⑦ 「役割と機能の削除ウィザード」が「<コンピューター名>で削除が正常に完了しました」と表示されるまで待つ。

グループの管理されたサービスアカウント

「グループの管理されたサービスアカウント」は、実行時に特定のユーザーアカウントを必要とするアプリケーションやサービスのための特別なユーザーアカウントである。

従来の「管理されたサービスアカウント」で用意したアカウントはドメイン内でシェアできるが、パスワードについてはそのアカウントを実際に使用したコンピューターで自動的に変更される。そのため、複数のコンピューターで同じアカウントを使うと、異なるパスワードがコンピューターの数だけ設定されることになり、不整合が発生するという欠点があった。

Windows Server 2012の「グループの管理されたサービスアカウント」は、この欠点を解消するためにパスワード変更をDCでのみ行うようになっている。

[Function 02]

DHCPサーバー

可用性向上で
さらなる安定稼働を実現

Dynamic Host Configuration Protocol(DHCP)は、IPアドレスやデフォルトゲートウェイ、DNS参照設定などを通信機器に自動的に割り当てるプロトコルだ。Windows Server 2012では、2台のDHCPサーバーにまったく同じアドレス範囲(スコープ)を定義して、Hyper-Vを使わずに

表5: DHCPサーバーの新機能と強化点

新機能	
DHCPフェールオーバー	同一スコープをホストする複数のDHCPサーバー間で、サービス停止時にフェールオーバーすることで、ダウンタイムを短縮する。
ポリシーベースの割り当て	ポリシーに従ってDHCPクライアントをグループ化し、適切なIPアドレスをリースする。
機能強化	
Windows PowerShell用DHCPモジュール	DHCPサーバーの構成と展開を管理するための、新しいPowerShell用コマンドレットを利用できる。

DHCPサーバー間でフェールオーバーや負荷分散を構成することが可能になった。

Windows Server 2012におけるDHCPサーバーの新機能と強化点は表5のとおり。

DHCPフェールオーバー

Windows Server 2012のDHCPサーバーには、同じアドレス範囲(スコープ)をホストする2台のDHCPサーバー間で、フェールオーバーまたは負荷分散のリレーションシップを構築する機能が搭載された(画面28)。

DHCPサーバーの可用性を高める方法としては、フェールオーバークラスター上でDHCPサーバーをホストする方法と、DHCPサーバーごとに異なるスコープ(例えば「192.168.1.1~127」と、

フェールオーバーの構成

jiro.soho.mountain.jp と taro.soho.mountain.jp の間のフェールオーバーが次のパラメーターで作成されます

スコープ:
10.0.0.0

関係名: jiro.soho.mountain.jp-taro.soho.mountain.jp
クライアントの最大リードタイム: 1 時間 0 分
モード: ホットスタンバイ
状態の切り替えの閾値: 無効

ホットスタンバイの構成
パートナーサーバーの役割: アクティブ
スタンバイ用に予約されているアドレス: 5%

< 戻る(B) 完了 キャンセル

画面28: 2台のDHCPサーバー間で、フェールオーバーまたは負荷分散のリレーションシップを構築できる

「192.168.1.128～254」まで)を定義する方法があるが、前者はコストパフォーマンスの問題があり、後者は1台のDHCPでリース可能なIPアドレスが減るという問題がある。

これに対して、新しいDHCPサーバーではフェールオーバークラスタリングを使わずに、DHCPサーバー間で独自のフェールオーバーまたは負荷分散環境を構築できるようになった。同じスコープをホストする2台のDHCPサーバー間で相互にリース情報を交換することで、重複IPアドレスのリースを防ぎながら、DHCPシステム全体の稼働率を単体のDHCPサーバーより高めることができる。

DHCP フェールオーバー機能を利用するには、2台のDHCPサーバーをインストールして、1台目のDHCPサーバーでスコープやオプションを定義し、「フェールオーバーの構成」ウィザードを実行する。もう1台のDHCPサーバーをパートナーとして選択し、[負荷分散]または[ホットスタンバイ]を選択してパートナーシップを締結する(画面29)。スコープとオプションは自動的にパートナーに転送されるので、2台目のDHCPサーバーに定義する必要はない。また、負荷分散とホットスタンバイはスコープごとに選択できるので、両者の混在環境も可能である。締結したパートナーシップは、スコープのプロパティ「フェールオーバー」タブで確認できる。

画面29: [負荷分散]または[ホットスタンバイ]を選択してパートナーシップを締結する

ポリシーベースの割り当て

特定の条件をクリアしたDHCPクライアントだけにIPアドレスをリースする、「ポリシーベースの割り当て」機能もWindows Server 2012で搭載された新機能の1つだ(画面30)。

リースを許可または拒否する条件の集合を「ポリシー」といい、「ベンダークラス」「ユーザークラス」「MACアドレス」「クライアント識別子」「リレーエージェントの情報」を1つ以上指定して構成する。複数の条件をANDまたはORで結合することで、さまざまな条件でDHCPクライアントをグループ化し、IPアドレスのリースをコントロールすることができる。

複数のポリシーを定義した場合は、評価の優先順位を設定することができる。

また、あるスコープの中から、ポリシーごとにIPアドレス範囲を切り出してリースすることも可能だ。さらに、スコープ全体をカバーするポリシーを作成して、ポリシーに適合しないDHCPクライアントにはIPアドレスをリースしないように設定することもできる。

画面30: 新たに追加された「ポリシーベースの割り当て」機能

[Function 03]

DNSサーバー

よりセキュアに 正常進化

AD DSにおいて、名前解決やフォレストのツリー構造を決定する「ドメインネームシステム(DNS)」サービスにも、セキュリティ強化の波が訪れた。従来のDNSには、ゾーンやレコード情報の信憑性を検査する仕組みがなかったため、意図的に偽レコード情報を流して、本物とは異なるWebサイトなどに誘導する攻撃手法が編み出された。これに対抗するために、Windows Server 2012のDNSサーバーには「DNSSEC (DNS Security Extensions)」が搭載された。

Windows Server 2012におけるDNSサーバーの新機能と強化点は表6のとおり。

DNSSEC対応

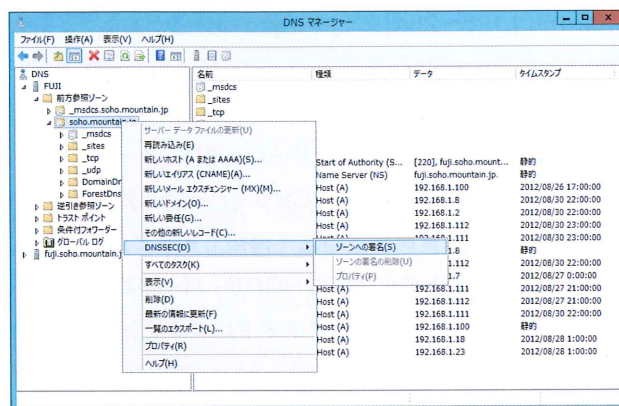
Windows Server 2012のDNSサーバーは、公開鍵暗号方式とデジタル署名を利用してレコードの正当性を検証可能にした「DNSSEC」に対応している(画面31)。DNSSECでは、次の4種類のリソースレコードを追加で使用する(画面32、表7)。

DNSSECに対応したDNSサーバー間では、次の手順で応答の信憑性とデータの完全性を検証する。

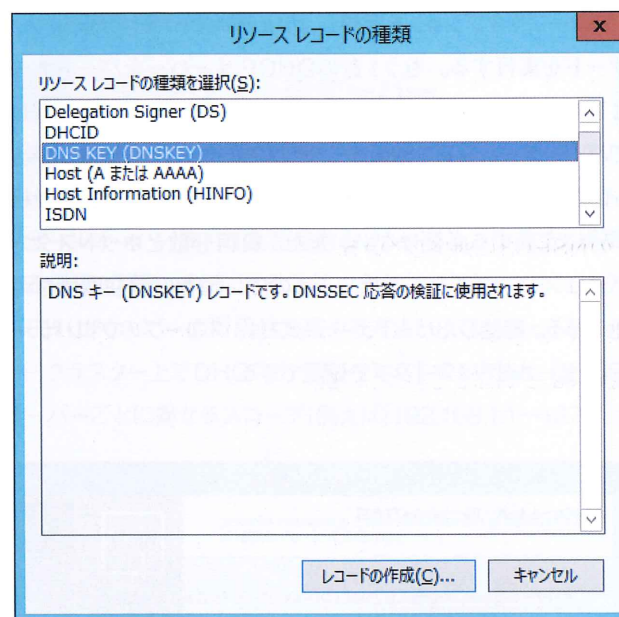
- ① DNS1では、ゾーン1に対して秘密鍵を使って暗号化を行い、DNSKEYレコードで対応する公開鍵を提供している。また、リソースレコードについてもハッシュ値を秘密鍵で暗号化

表6：DNSサーバーの新機能と強化点

新機能	
DNSSEC対応	DNSSEC (NSEC3)に対応し、AD統合ゾーンと動的更新レコードにもデジタル署名を設定できる。
機能強化	
Windows PowerShell用DNSモジュール	DNSサーバーの構成と展開を管理するための、新しいPowerShell用コマンドレットを利用できる。



画面31：公開鍵暗号方式とデジタル署名を利用してレコードの正当性を検証できる「DNSSEC」に対応した



画面32：DNSSECに対応したリソースレコードの種類

表7：DNSSECで使用するリソースレコード

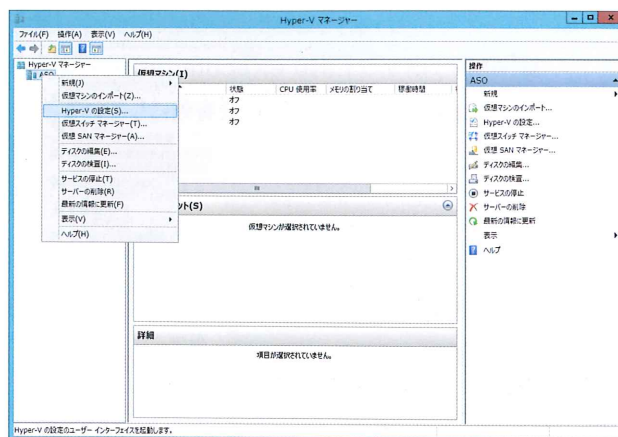
レコードの種類	
DNSKEY (DNS Public Key)	ゾーンの暗号化に使用する秘密鍵に対応する公開鍵を記述する。秘密鍵は決して公開しない。
RRSIG (Resource Record Signature)	リソースレコードのデータを、ある計算式に通してハッシュ値を得る。このハッシュ値を秘密鍵で暗号化して、得られたデジタル署名を記述する。
DS (Delegation Signer)	DNSKEYのハッシュ値を設定する。この値を親ゾーン側で暗号化して公開すると新たなデジタル署名となり、「信頼の連鎖」ができる。
NSEC (Next Secure)	ゾーン不在応答に付加する、辞書的に整列した次のゾーン名情報を示す。

して、RRSIGレコードでデジタル署名として公開している。

- ② DNS2からDNS1に問い合わせを行い、ゾーンの公開鍵、リソースレコードのデータ、レコードに対応するデジタル署名を得る。
- ③ ゾーンの公開鍵でデジタル署名を復号化してハッシュ値1を得る。また、リソースレコードのデータを同じ計算式を通してハッシュ値2を得て、ハッシュ値1と比較する。
- ④ ハッシュ値1とハッシュ値2が等しければ、ゾーンやレコード情報は間違いなくDNS1から得られたもので、改ざんが行われていないことが証明できる。

しかし、NSECレコードを使うと次々と実在するゾーン名を取り出す「ゾーン列挙(Zone enumeration)」が可能になり、新たな攻撃の足がかりに利用されてしまうことが判明した。そこで、ゾーン名の代わりにゾーンのハッシュ値を返すことで、ドメイン名が流出しないように改良を加えたのが「NSEC3」レコードになる。Windows Server 2012のDNSサーバーは、このNSEC3に対応している。

なお、DNSSECで使用する秘密鍵と公開鍵の生成、保管、期限切れ、交換については、AD DSと「自動ロールオーバー」機能によって簡略化されている。



画面 33 : Windows Server 2012の「Hyper-V マネージャー」

ション(Live Migration)、仮想マシンに割り当て可能なリソースの拡充、新しい仮想ディスクフォーマット(VHDX)の採用といった機能強化が図られている。

さらに、VMwareの仮想マシンをHyper-V仮想マシンに変換するユーティリティ、「Microsoft Virtual Machine Converter」の開発も進行中で、RC(Release Candidate : リリース候補)版が公開中だ(2012年8月末日現在)。

▶ Microsoft Virtual Machine Converter

URL <http://technet.microsoft.com/en-us/library/hh967435.aspx>

Windows Server 2012におけるHyper-Vの新機能と強化点は次ページの表8のとおり。



Hyper-Vの必要システム

Hyper-Vを実行するには、Windows Server 2012のシステム要件に加えて、次の2つの条件を満たす必要がある。レビュー版などで必要とされたSLAT(Second Level Address Translation)への対応は不要となったので、旧型のCPUでも広くHyper-Vを利用できるようになっている。

【条件1】ハードウェアによる仮想化サポート

「インテルバーチャライゼーションテクノロジー(インテルVT)」または「AMD Virtualization(AMD-V)テクノロジー」を搭載したCPUを使用し、これらの機能を有効にしていること

【条件2】ハードウェアによるデータ実行防止(DEP)

[Function 04]

Hyper-V

さらなるスケールアップで最強の仮想化基盤に

Windows Server 2012(およびWindows 8)に搭載されている最新の「Hyper-V」は、データセンターの大規模な仮想化システムから、クライアントPC上で実行する「クライアントHyper-V」まで幅広くカバーした仮想化基盤テクノロジーだ(画面33)。

新しいHyper-Vでは、「Hyper-Vレプリカ」「仮想スイッチ」「仮想マシンの記憶域の移動」「オフロードデータ転送」などの新機能と、クラスターシステムを必要としないライブマイグレー

「インテルXDビット(eXecute Disable bit)」または「AMD NXビット(No eXecute bit)」を搭載したCPUを使用し、これらの機能を有効にしていること

Hyper-VがサポートするゲストOS

Windows Server 2012のHyper-Vは、表9のサーバーOSをゲストとしてサポートしている。サポートされたゲストOSで利用可能な「Hyper-V 統合サービス」によって、クリッ

表8: Windows Server 2012に搭載されたHyper-Vの新機能と強化点

新機能	Hyper-Vレプリカ	Hyper-Vホスト間で、仮想マシンを相互に複製する。ダウンタイムを最小化しビジネス継続性を高める。
	記憶域の移動	仮想マシンを別のコンピューターに移動したり、実行中の仮想マシンの仮想ディスクを無停止で別の場所に移動したりする。
	Windows PowerShell用Hyper-Vモジュール	Hyper-Vホストおよび仮想マシンを管理するための、新しいPowerShell用コマンドレットを利用できる。
	仮想ファイバー チャンネル	仮想マシン内のゲストOSから、ファイバー チャンネルで接続された記憶域にアクセスできる。
	クライアントHyper-V	Windows 8上でデスクトップOSを実行するためのHyper-V環境を提供する。
	リソース メータリング	PowerShellのコマンドレットおよびWMIを使って仮想マシンのCPUやメモリ使用量などを測定する。
	Hyper-V Administratorsグループ	Hyper-Vホストの管理を許可された、専用のローカル セキュリティグループを新設した。
	Single Root I/O Virtualization	ネットワークアクセスの調停を、Hyper-Vのスーパーバイザーではなくネットワーク アダプターのハードウェア側で行うことで、CPU負荷を低減し使用効率を高める。
	Hyper-V over SMB	SMB 3.0プロトコルを使って、仮想マシンのファイル群をファイル共有に保存できる。
機能強化	仮想NUMA	Non-Uniform Memory Access (NUMA)を仮想マシンから利用可能になり、CPUとメモリの割り当てを効率化できる。
	ライブ マイグレーション	クラスター化されていない環境でもライブ マイグレーションを実行できる。また、複数のライブ マイグレーションを並列実行できる。
	規模の拡大	仮想マシンに提供可能なリソースが次のように強化された。 仮想プロセッサ数(合計):2,048CPU 仮想マシンごとの最大仮想プロセッサ数:64CPU 仮想マシンごとの最大メモリ容量:1TB 仮想マシンごとの最大仮想ディスクサイズ:64TB
	仮想ディスク フォーマット	可変ブロックサイズや4KBセクタ、メタデータのログ機能を搭載した、拡張された仮想ディスクフォーマット(拡張子は.vhdx)で、最大64TBをサポートする。
	仮想スイッチ	ネットワークを仮想化し、プライベートVLANを搭載することで、同一IPアドレスを持つゲストを分離して並列実行できる。
	動的メモリ	最小メモリを保証するスマート ページングによって、メモリ不足によるゲストOSの起動エラーなどを回避する。
	仮想マシンのインポート	インポート中に仮想マシンの構成をチェックして修正し、インポートの信頼性を高める。

表9: Hyper-VがサポートするゲストOS (サーバー OS) (筆者調べ)

ゲストOS (サーバー)	サポートされるエディション	ビット数	Hyper-V統合サービス
Windows Server 2012	すべて	32 / 64ビット	組み込み済み
Windows Server 2008 R2	Datacenter Enterprise Standard Web	64ビット	インストールが必要
Windows Server 2008 SP2	Datacenter Enterprise Standard Web	32 / 64ビット	インストールが必要
Windows Home Server 2011	すべて	64ビット	インストールが必要
Windows Small Business Server 2011	Enterprise Standard	64ビット	インストールが必要
Windows Server 2003 R2 SP2	Datacenter Enterprise Standard Web	32 / 64ビット	インストールが必要
Windows Server 2003 SP2	Datacenter Enterprise Standard Web	32 / 64ビット	インストールが必要
CentOS 6.0 ~ 6.2	すべて	32 / 64ビット	「Linux統合サービスv3.2」をダウンロードしてインストール
Red Hat Enterprise Linux 6.0 ~ 6.2	すべて	32 / 64ビット	「Linux統合サービスv3.2」をダウンロードしてインストール
SUSE Linux Enterprise Server 11 SP2	すべて	32 / 64ビット	組み込み済み

ブロードを介したホストとゲスト間のコピー&ペーストや、ホストとの時刻同期などが実行できるようになる。なお、ゲストOSとしてのWindows Server 2012にはHyper-V統合サービスがすでに組み込まれているので、新たにインストールする必要はない。

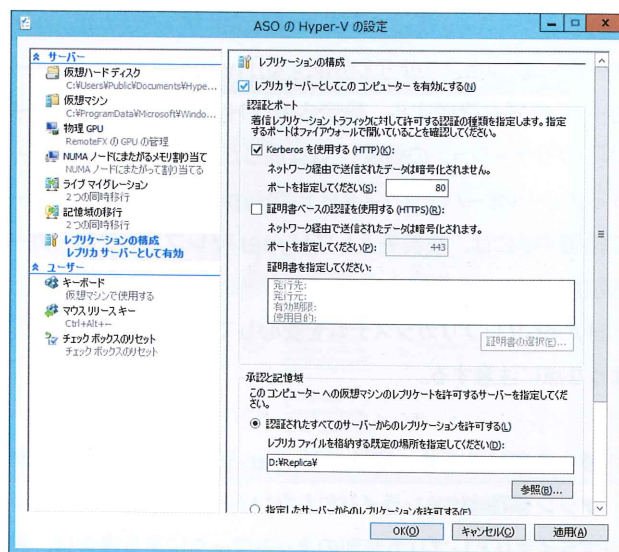
また、クライアントOSでサポートされるのは、Windows XP Service Pack(SP)3以降(Windows XP x64 Edition SP2を含む)のWindowsファミリで、ビジネス向けエディション(Windows XP Professional、Windows Vista Business、Windows 7 Ultimateなど)である。Windows 8についてはHyper-V統合サービスが組み込み済みだ(表10)。

Hyper-Vレプリカ

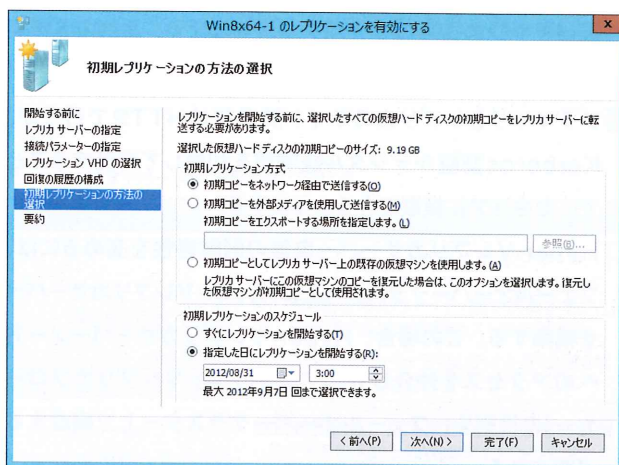
「Hyper-Vレプリカ」は、複数のHyper-Vサーバー間で仮想マシンを自動的に複製して、耐障害性や可用性を高める機能だ(画面34)。複製元のHyper-Vサーバーを「プライマリサーバー」、複製先のHyper-Vサーバーを「レプリカサーバー」と呼ぶ(画面35)。

例えば、プライマリサーバーのダウン時にレプリカサーバー上の仮想マシンをオンラインにすることで、VDI(Virtual Desktop Infrastructure)環境のダウンタイムを最小限にとどめることができる。これがHyper-Vレプリカの「フェールオーバー」のシナリオだ。

逆に、レプリカサーバーからプライマリサーバーへの「逆コピー」も可能なので、プライマリサーバーの復帰時に仮想マシンを「フェールバック」することができる。オンプレミスのプライマリサーバーと、データセンターに置いたレプリカサーバー



画面34: 複数のHyper-Vサーバー間で仮想マシンを自動的に複製して、耐障害性や可用性を高める「Hyper-Vレプリカ」



画面35: 「Hyper-Vレプリカ」設定後は初期レプリケーションの方法を指定する

表10: Hyper-VがサポートするゲストOS(クライアントOS) (筆者調べ)

ゲストOS (クライアント)	サポートされる エディション	ビット数	Hyper-V 統合サービス
Windows 8	すべて	32/64ビット	組み込み済み
Windows 7	Ultimate Enterprise	32/64ビット	インストールが 必要
Windows Vista SP2	Business Enterprise Ultimate	32/64ビット	インストールが 必要
Windows XP SP3	Professional	32ビット	インストールが 必要
Windows XP x64 Edition SP2	Professional	64ビット	インストールが 必要

で、耐障害性を高めるといった使い方も可能になる。

その他のシナリオとしては、本社のプライマリサーバーで一括管理しているHyper-V仮想マシンを支社のレプリカサーバーに複製したり、逆に支社のプライマリサーバーの仮想マシンを、データセンターのレプリカサーバーに集約したりするといった使い方が考えられる。双方向の複製を構成することで、プライマリサーバーとレプリカサーバーの関係を安全で簡単に入れ替えることができるので、バックアップ、集約、配布のどのシナリオにも応用できる。

Hyper-Vレプリカサーバーをフェールオーバークラスター上に構築すれば、ダウンタイムを最小化して可用性をさらに高めることができる。フェールオーバークラスター上にHyper-V

レプリカサーバーを構築するには、Hyper-Vレプリカサーバーノードへのアクセスを仲介し分配する「Hyper-Vレプリカブローカー」の役割を構成する。設定内容はHyper-Vマネージャーの「レプリケーションの構成」とほぼ同じだ。プライマリサーバーからフェールオーバークラスター上のHyper-Vレプリカサーバーに複製するには、複製先としてHyper-Vレプリカブローカーの接続ポイントを指定する。

Hyper-Vレプリカシステムを安心して利用するには、次のような点に注意する。

- ◎競合を避けるため、複数のHyper-Vサーバーで同じ仮想マシンを同時にオンラインにしない。
- ◎プライマリとレプリカが別のネットワークにある場合は、複製する仮想マシンのネットワークアダプター設定で「フェールオーバーのTCP/IP」を構成する。
- ◎仮想マシンの複製はリアルタイムではなく、最短で5分間隔で実行されるようにする。
- ◎プライマリとレプリカのサイト間通信はHTTPで行うが、Kerberos認証かデジタル証明書を利用して認証することで、セキュアに複製できるようにする。
- ◎Hyper-Vレプリカサーバー自体の耐障害性を高めるには、フェールオーバークラスター上にHyper-Vレプリカサーバーを構築する。この場合、Hyper-Vレプリカサーバーノードへのアクセスを仲介し分配する「Hyper-Vレプリカブローカー」の役割を、フェールオーバークラスター上で構成する必要がある。



ライブマイグレーション

新しいHyper-Vでは、物理環境から仮想化環境にダイレクトに移行する「ライブマイグレーション」のために、クラスター環境を要求しなくなった。マイグレーション対象のコンピューターとHyper-Vホストをネットワークで接続するだけで、すぐに「P2V(Physical to Virtual:物理→仮想)」を実行できる。



仮想スイッチとプライベートVLAN

Windows Server 2012の「クラウド」と「仮想化」というコンセプトから「集約」に至ったとき、重要な役割を果たすのが「仮想スイッチ」である。ネットワークアダプターを仮想化するだけでなく、「プライベートVLAN(PVLAN)」を設定することで、

同一IPアドレスを割り当てられた複数の仮想コンピューターを、1台のHyper-Vサーバーで同時実行できるようになる(画面36)。つまり、物理サーバーのIPアドレスをまったく変更することなく仮想化して、集約することが可能になる。

PVLANは、「プライマリVLAN ID」と「セカンダリVLAN ID」を使用して、2段フィルターでVLANを構成することで実現している。プライマリVLAN IDは通常のVLAN設定(最初のフィルター)で、大まかに仮想マシンをグループ分けする。同じプライマリVLAN IDを持つ仮想マシンを、さらに細かくグループ分けするのがセカンダリVLAN ID(2番目のフィルター)だ。セカンダリVLAN IDを設定してPVLANを有効にする際に、表11のようにPVLANモードを1つ選択して設定できる。

ただし、セカンダリVLAN IDを設定するGUIは用意されていないので、PVLAN機能を利用するにはPowerShellの「Set-VMNetworkAdapterVlan」コマンドレットを使用する。

▶ Set-VMNetworkAdapterVlan

URL <http://technet.microsoft.com/en-us/library/hh848475.aspx>

```
Windows PowerShell
PS C:\> Get-Help Set-VMNetworkAdapterVlan

名前
Set-VMNetworkAdapterVlan

構文
Set-VMNetworkAdapterVlan [-VMName] <string> [-Untagged] [-Access] [-VlanId <int>] [-Trunk] [-NativeVlanId <int>] [-AllowedVlanIdList <string>] [-Isolated] [-Community] [-Promiscuous] [-PrimaryVlanId <int>] [-SecondaryVlanId <int>] [-Passthru] [-VMNetworkAdapterName <string>] [-ComputerName <string>] [-WhatIf] [-Confirm] [-ComorParameters]

Set-VMNetworkAdapterVlan [-ManagementOS] [-Untagged] [-Access] [-VlanId <int>] [-Trunk] [-NativeVlanId <int>] [-AllowedVlanIdList <string>] [-Isolated] [-Community] [-Promiscuous] [-PrimaryVlanId <int>] [-SecondaryVlanId <int>] [-Passthru] [-VMNetworkAdapterName <string>] [-ComputerName <string>] [-WhatIf] [-Confirm] [-ComorParameters]

Set-VMNetworkAdapterVlan [-VM] <VirtualMachine> [-Untagged] [-Access] [-VlanId <int>] [-Trunk] [-NativeVlanId <int>] [-AllowedVlanIdList <string>] [-Isolated] [-Community] [-Promiscuous] [-PrimaryVlanId <int>] [-SecondaryVlanId <int>] [-Passthru] [-VMNetworkAdapterName <string>] [-ComputerName <string>] [-WhatIf] [-Confirm] [-ComorParameters]

Set-VMNetworkAdapterVlan [-VMNetworkAdapter] <VMNetworkAdapter> [-Untagged] [-Access] [-VlanId <int>] [-Trunk] [-NativeVlanId <int>] [-AllowedVlanIdList <string>] [-Isolated] [-Community] [-Promiscuous] [-PrimaryVlanId <int>] [-SecondaryVlanId <int>] [-Passthru] [-VMNetworkAdapterName <string>] [-ComputerName <string>] [-WhatIf] [-Confirm] [-ComorParameters]

エイリアス
なし

注釈
Get-Help を実行しましたが、このコンピューターにこのコマンドレットのヘルプ ファイルは見つかりませんでした。ヘルプの一部だけが表示されています。
このコマンドレットを含むモジュールのヘルプ ファイルをダウンロードしてインストールするには、Update-Help を使用してください。
このコマンドレットのヘルプ トピックをオンラインで確認するには、(Get-Help Set-VMNetworkAdapterVlan -Online) と入力するか、
http://go.microsoft.com/fwlink/?LinkID=216807 を参照してください。

PS C:\>
```

画面 36: 仮想スイッチでPVLANを有効化するPowerShellコマンドレット

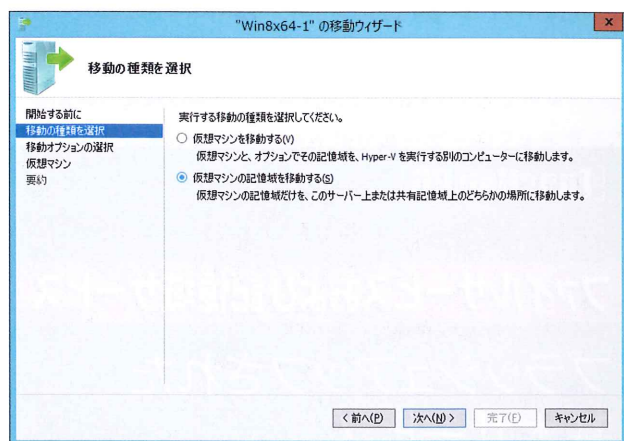
表 11: 設定可能なPVLANモード

PVLANモード	受信ポート	送信ポート
Isolated (分離)	プライマリVLANのみ	セカンダリVLANのみ
Community (コミュニティ)	プライマリVLANとセカンダリVLAN	セカンダリVLANのみ
Promiscuous (無作為検出)	プライマリVLANとセカンダリVLAN	プライマリVLANのみ

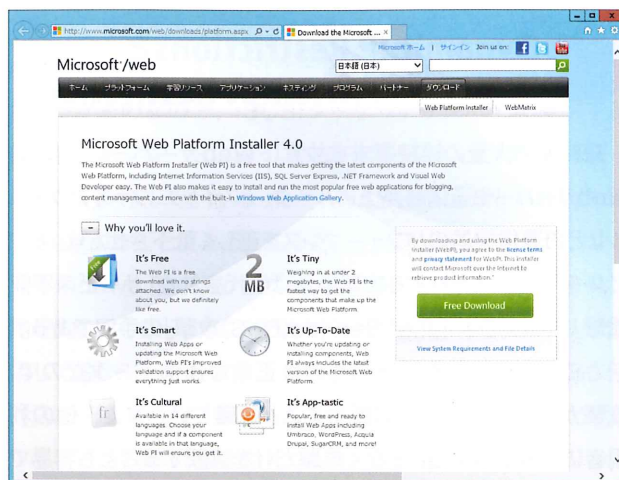


仮想マシンの記憶域の移動

新しいHyper-Vでは、仮想マシンの実行中でも仮想ハードディスクを別の記憶域に移動することができるので、ディスクの使用量やディスクサブシステムの負荷に応じて、ダウンタイムなしで最適な記憶域に移動できる(画面37)。また、ディスクサブシステムのメンテナンスを行う際に、メンテナンス対象のディスクから仮想マシンを無停止で移動できるので、ユーザーにまったく影響を与えることなく、安全にメンテナンス作業を実行できる。



画面37：新しいHyper-Vでは、仮想マシンの実行中でも仮想ハードディスクを別の記憶域に移動できる



画面38：IIS 8.0ではセキュリティ強化とパフォーマンスが改善された

Platform Installer 4.0]Webサイトに案内してくれる(画面38)。

Windows Server 2012におけるWebサーバー(IIS)の新機能と強化点は表12のとおり。

表12：Webサーバー(IIS)の新機能と強化点

新機能	
集中証明書	複数のWebサーバーで構成される「ファーム」に単一のSSL中央証明書ストアを配置して、SSL証明書をWebサーバー間で共有することで、証明書の配布と管理コストを低減する。 1台のWebサーバーでSSLサイトを10,000サイト以上ホストできる。
Dynamic IP Restrictions	指定時間内に、指定回数以上の要求を送信したIPアドレスからのWebサイトへのアクセスをブロックして、サービス不能攻撃(DoS)に対抗する。
FTP Logon Attempt Restrictions	指定時間内に、指定回数以上ログオンに失敗したアカウントをロックアウトして、サービス不能攻撃(DoS)に対抗する。
Server Name Indication (SNI)	HTTPSを使用するバーチャルドメインをホストするため、RFC 3546で定義されたSSL/TLSの拡張機能であるSNIを実装した。
Application Initialization	Webアプリケーションの初回実行時のみパフォーマンスが低下する現象を回避するため、IISの起動時にワーカープロセスが特定のページを呼び出して準備する。
NUMA-Aware Scalability	32~128コアのNUMAシステムに対応し、CPUとメモリの割り当てを効率化できる。
機能強化	
IIS CPU Throttling	複数のWebサイトで単一のアプリケーションプールを共有する場合、CPUやメモリの使用量を制御して、特定のWebサイトにリソースが集中しないように調整できる。

[Function 05]

Webサーバー (IIS)

クラウド時代の 新たなアプリケーション基盤

Windows Server 2012の「Webサーバー(IIS)」は、「インターネットインフォメーションサービス(IIS)8.0」にバージョンアップしており、主にセキュリティ面の強化とパフォーマンスの改良が盛り込まれている。また、「インターネットインフォメーションサービス(IIS)マネージャー」の[新しいWeb Platformコンポーネントの取得]リンクをクリックすると、Webアプリケーションの開発やコンポーネント更新に便利な「Microsoft Web

Dynamic IP Restrictionsと FTP Logon Attempt Restrictions

短時間で大量の接続要求を故意にWebサーバーに送信し、Webサーバーや通信経路上のルーター、スイッチ、ファイアウォールなどの通信機器のパフォーマンスを著しく低下させたり、サービスを停止させたりする攻撃手法は、代表的な「サービス不能攻撃」または「Denial of Service(DoS)攻撃」の手口である。

ところが、接続要求そのものは正常な通信データなので、攻撃が通常の要求かを判断することは難しい。また、他の利用者に影響を与えることなく攻撃だけを遮断することも容易ではない。

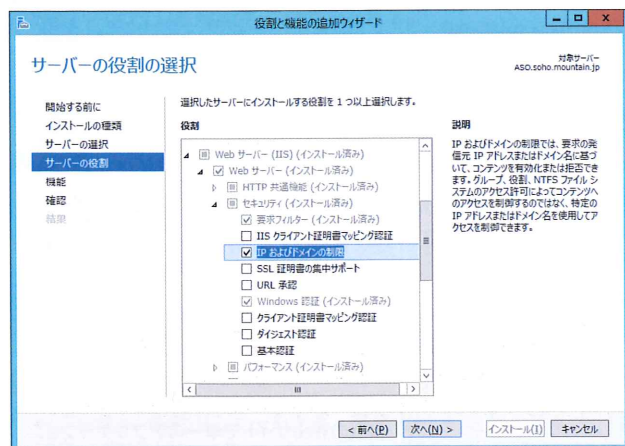
独立行政法人 情報処理推進機構(IPA)が公開しているDoS攻撃への対策調査報告書によると、Webサイトへのアクセスが急増した場合は、まず自社側に新商品発表などの原因がないか調査し、問題がなければ通信パケットの発信元を確認するという手順を紹介している。

▶ 情報処理推進機構：

「サービス妨害攻撃の対策等調査」報告書について

URL <http://www.ipa.go.jp/security/fy22/reports/isec-dos/index.html>

IIS 8.0で「IPおよびドメイン名の制限」の役割サービスをインストールすると有効になる「Dynamic IP Restrictions」機能を利用すると、同一の送信元からしきい値を超える連続アクセスがあった場合、その送信元の通信パケットを自動的に



画面 39：Dynamic IP Restrictionsを使用するには「IPおよびドメイン名の制限」をインストールする

遮断することができるようになる(画面 39)。一般的にはファイアウォールや侵入検知システム(Intrusion Detection System: IDS)、侵入防止システム(Intrusion Prevention System: IPS)などを使って防御するところだが、基本的に手動で対応する必要があった。Windows Server 2012のDynamic IP Restrictionsでは、IISが攻撃を自動判定してブロックしてくれるので、軽微な攻撃であれば人手をかけずにIISだけでも耐えられるようになる。

FTPサーバーについても、同一ユーザーIDによる短時間で多数のログイン試行を検知して、そのユーザーIDをロックアウトする「FTP Logon Attempt Restrictions」機能を搭載している。

[Function 06]

ファイルサービスおよび記憶域サービス

ブラッシュアップされた基本サービス

「ファイルサービスおよび記憶域サービス」の役割には、Windowsの基本機能であるファイルサーバー機能を強化する、重要な新機能が搭載されている。

Windows Server 2012におけるファイルサービスおよび記憶域サービスの新機能は表 13のとおり。

表 13：ファイルサービスおよび記憶域サービスの新機能

新機能	
データ重複除去	ボリューム内の重複データを1つの物理記憶領域にまとめて、データ量を削減する。
iSCSI ターゲット サーバー	別モジュールとしてダウンロード提供されていたiSCSIターゲットサーバー機能を標準搭載した。
記憶域スペースと記憶域プール	複数の物理ディスクをまとめて「プール」を作成し、仮想ディスクを切り出して提供する。
サーバー マネージャー 統合	サーバー マネージャーのダッシュボードからファイルサービスおよび記憶域サービスを管理できる。
Windows PowerShell用ファイルサービスおよび記憶域サービスモジュール	ファイルサービスおよび記憶域サービスの構成と展開を管理するための、新しいPowerShell用コマンドレットを利用できる。



データ重複除去

「データ重複除去(Data Deduplication)」は、ボリューム内の共通データを自動的に検出して、ボリューム上の物理的な記憶領域を1カ所だけに整理することで、ストレージの利用効率を高める技術だ(画面40)。簡単に言えば「ハードディスク上のデータ集約」機能で、既存のファイルやフォルダーの圧縮機能とは根本的に異なる。

システム状態データや暗号化されたファイル、32KB未満の小容量ファイルを除くほとんどのファイルに対して集約が適用されるため、平均的に従来の半分程度のボリューム使用率(仮想化データでは20分の1)まで節約できる。

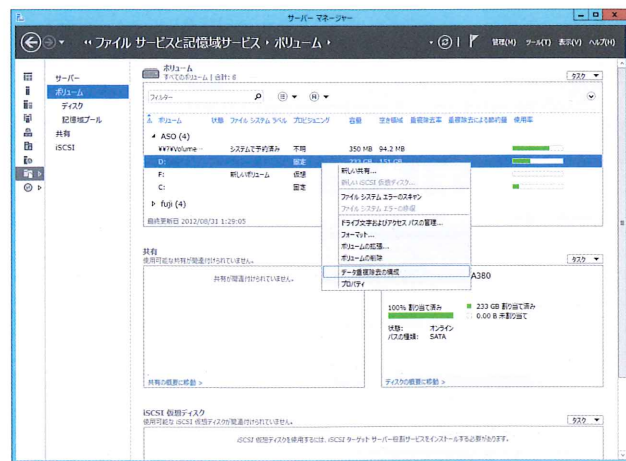
例えば、多数のユーザーが共同で利用するファイルサーバーには、完全に同一内容のファイルがユーザーのフォルダーごとに複製されて保存されていたりする。このようなムダをなくして記憶領域をまとめることを推進すれば、ファイルサーバーのディスクスペースを大きく節約できる。



iSCSIターゲットサーバー

Windows Server 2012に標準搭載されている「iSCSIターゲットサーバー」の役割サービスは、これまでマイクロソフトダウンロードセンターで配布されていた、「Microsoft iSCSI Software Target 3.3」と同等の機能になる。

iSCSIは、SCSIのコマンドセットをTCP/IP上で利用可能にしたプロトコルで、SCSIデバイスをネットワークに公開するサーバーを「iSCSIターゲット」、SCSIデバイスをネットワー

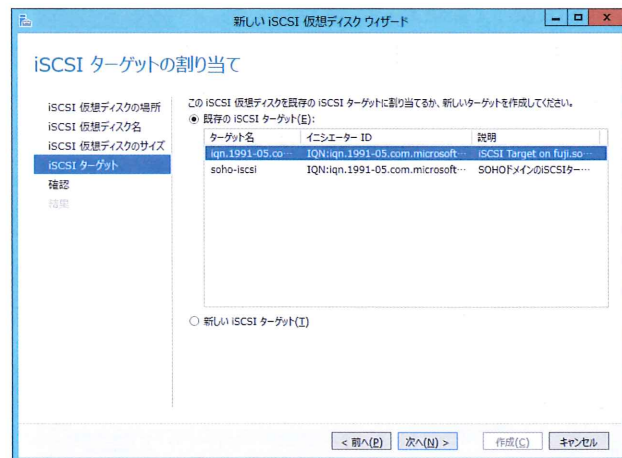


画面40: ストレージの利用効率を高める「データ重複除去(Data Deduplication)」機能が搭載された

ク経由で利用するクライアントを「iSCSIイニシエーター」と呼ぶ。イメージ的にはSCSIケーブルがEthernetに置き換わったようなものなので、iSCSIターゲットサーバーが提供する仮想ディスクは、iSCSIイニシエーターにとってローカルディスクのように見える点が、NAS(Network Attached Storage)などと異なるところだ。

Windows Server 2012のiSCSIターゲットサーバーは、物理的なSCSIデバイスではなく、仮想ディスクファイルを使用してSCSIハードディスクをエミュレートするので、iSCSI対応のディスクサブシステムを必要としない(画面41)。また、クライアント側の「iSCSIイニシエーター」はWindows Vista以降では標準搭載されているので、追加コストなしで容易にiSCSI環境を構築できる。

例えば、iSCSIターゲットサーバーが提供する仮想ディスクは、iSCSIイニシエーター側ではローカルの物理ディスクと同様に扱えるというメリットを生かして、仮想ディスクを共有ディスクにしたフェールオーバークラスターを構築できる。Hyper-V上の仮想マシンをクラスターノードにした、オール仮想化のフェールオーバークラスター環境は、クラスター対応アプリケーションの開発やテスト環境として、非常に高いコストパフォーマンスを発揮する。



画面41: iSCSIターゲットの割り当て

【参考情報】

以前のバージョンのWindows ServerでiSCSIターゲットとiSCSIイニシエーターを利用するには、マイクロソフトダウンロードセンターから次のファイル入手するか、サードパーティ製品を利用する。

▶ Microsoft iSCSI Software Target 3.3

URL <http://www.microsoft.com/ja-jp/download/details.aspx?id=19867>



記憶域スペースと記憶域プール

「記憶域プール」は、複数の未割り当て物理ディスクをグループ化した「プール」を作成し、プールから仮想ディスクを切り出して提供する機能だ(画面42)。仮想ディスクは物理ディスクの境界を越えて作成されるので、単体の物理ディスクよりもサイズの大きな仮想ディスクを作成できる。

また、仮想ディスクの作成時に初期サイズを「最小限」とすることで、プールの総容量を超えて、Windows Server 2012で搭載されたReFSファイルシステム(後述)の上限である、16EB(エクサバイト)の仮想ディスクを作成することも可能だ。もちろん、実際に書き込めるデータ量はプールの総容量までに制限されるが、アプリケーションの限界テストなどに利用することができる。

記憶域プールの作成は、「記憶域プールの新規作成ウィザード」で行う。「Primordial」という記憶域プールのルートの下に、任意の名前プールを作成して、未使用の物理ディスクをメンバーとして登録するだけだ。物理ディスクの割り当ては「ホットスワップ」を選択できるので、耐障害性についても考慮されていることがうかがえる。

記憶域プールが作成できたら、「仮想ディスクの新規作成ウィザード」を使って仮想ディスクを作成する。プール内の物理ディスク数によって、仮想ディスクのデータ配置を「シンプル」(RAID0相当)、「ミラー」(RAID1相当、物理ディスク2台以上)、「パリティ」(RAID5相当、物理ディスク3台以上)から選択できる。

「プロビジョニングの種類」で「最小限」を選択することで、プールの総記憶容量を越えた仮想ディスクを作成することができる。Windows Server 2012では、理論上は16EB(2の64乗バ

イト)の記憶域を扱うことができるが、仮想ディスクのサイズとしては4EB(4,194,304TB)が上限である。最後に「新しいボリューム ウィザード」を実行して、仮想ディスク内にボリューム(ファイルシステム)を作成する。ボリュームのサイズ上限は、ReFSを使用して2PB(ペタバイト、2,048TB)だ(画面43)。

なお、仮想ディスクのサイズとして4,194,305TB以上(4EB超)を指定すると、作成中に「仮想ディスクを作成できませんでした - Invalid Parameter」というエラーが発生する。



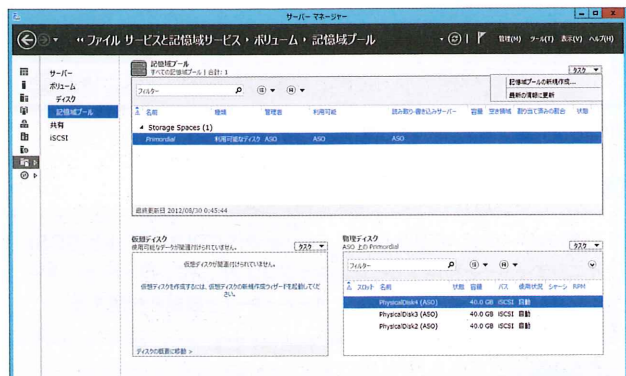
スポット検証サービスとスポット修正

「ファイルサービスおよび記憶域サービス」の役割とはやや異なるが、ファイルシステムについてもクラウドと仮想化を推進するための大きな変更が行われているので紹介しよう。

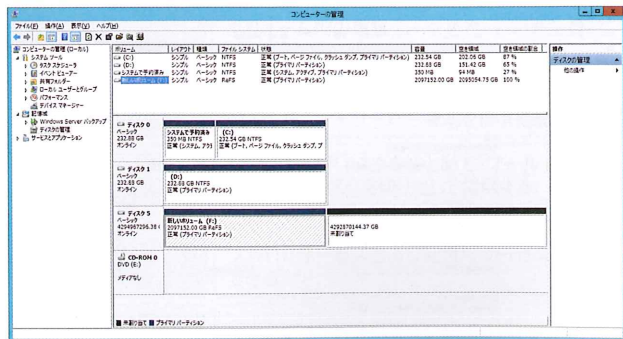
これまで、NTFSファイルシステムではファイルやフォルダー破損が発生した場合、検査と修正を実行する間、ずっとボリューム全体をオフラインにしなければならなかった。オフライン時間はボリュームサイズにほぼ比例するので、TBを越える大容量のボリュームを備えた重要なシステムほど、ダウンタイムも長くなってしまいうという問題があった。

せっかくポテンシャルの高いシステムを使っている、ボリュームの検査と修復にかかる時間を短くするために、あえてボリュームを細分化して小容量で使っているケースもある。現代のシステムでは、サービスレベルを維持して可用性を高めるために、ボリュームの修復で長時間システムダウンすることは許されないのだ。

この問題を解決するため、Windows Server 2012では、NTFSファイルシステムの自己修復機能をより向上させるとともに、ボリュームがオンラインのまま「Chkdsk」コマンドを実行できるシナリオを増やしている。加えて、ボリュームの



画面42: 記憶域プールの新規作成



画面43: 4EBのドライブは、2PBのボリュームを取っても、空き領域の割合が100%になるほど広い

検査とエラー個所の識別と、エラーの修正のタイミングを分離することで、ボリューム全体が長時間オフラインにならないようにしている。

具体的には、バックグラウンドで実行される「スポット検証サービス」(サービス名は「Spot Verifier」)が、オンライン状態のままでボリュームの検査とエラーの識別を行い、修復個所をロギングする(画面44)。エラー修正は、管理者が都合のよいときを見計らって実行するが、このときログを参照してピンポイントでエラー個所を修正する「スポット修正」が行われる。ボリュームがオフラインになるのは、スポット修正を実行中の間だけだ。

Resilient File System

「Resilient File System(ReFS)」は、NTFS(NT File System)と互換性を保ちながら飛躍的に信頼性を向上した新しいファイルシステムだ(画面45)。NTFSの最大ボリュームサイズ(実装値)は256TBだが、ReFSでは表14のように256ZB(ゼタバイト)という超巨大ボリュームと、16EBもの巨大ファイルをサポートできるように設計されている(実装時に制限されることがある)。

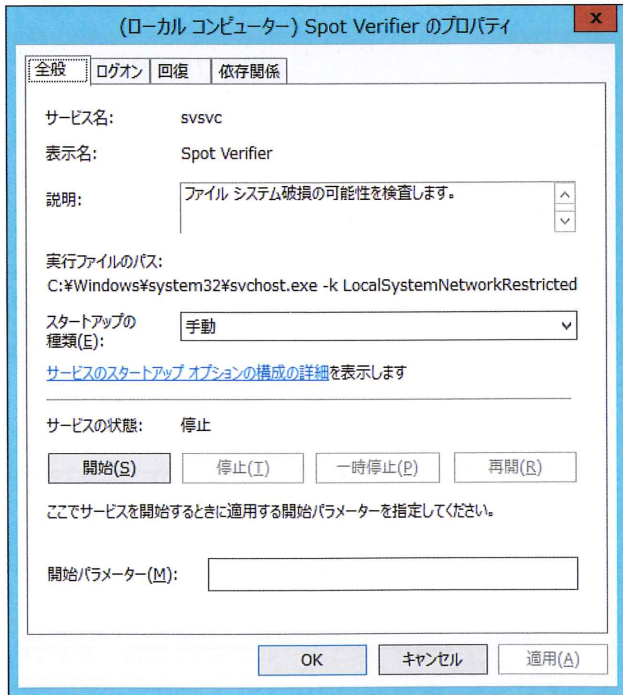
ReFSでは、データを書き換える際に、古いデータの保存

領域を上書きするのではなく、新しい保存領域にデータを書き込んでから、古い保存領域を非利用領域(空きエリア)としてマークすることで、中途半端な上書きが起これないようにしている。

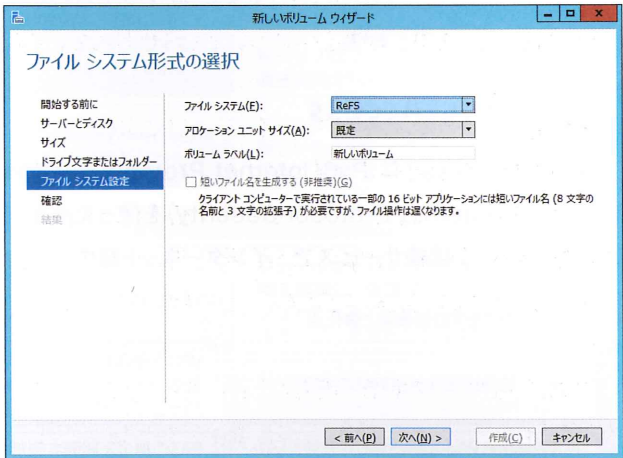
また、NTFSではエラーの修復時にボリューム全体をオフラインにする必要があるが、ReFSではエラー個所だけスポットでオフラインにして、ボリューム全体ではオンラインの状態を保つことができる。

このほか、チェックサムと整合性ストリームによってメタデータとユーザーデータの整合性を確保し、データベースのトランザクションの考え方を応用した原子性の確保手法を採用している。

アクセス権、所有者、監査、シンボリックリンク、ジャンクションポイント、再解析ポイント、マウントポイントなど、NTFS由来の機能が利用可能で、「BitLockerドライブ暗号化」にも対応している。互換性がないのは、ReFSがもはや「8.3」形式の短いファイル名を生成しないことだ。



画面44: ボリュームの検査とエラーの識別を行い、修復個所をロギングする「スポット検証サービス」



画面45: 「Resilient File System (ReFS)」は、信頼性がさらに向上した新しいファイルシステムだ

表14: 新たなファイルシステム「Resilient File System (ReFS)」のスケラビリティ

設定	最大値
最大ボリューム サイズ	16KBクラスター のとき、2の78乗B (256ZB)
最大ファイル サイズ	2の64乗-1バイト (約16EB)
フォルダー内の最大ファイル数	2の64個
ボリューム内の最大フォルダー数	2の64個
ファイル名の最大長	255文字 (Unicode)
パスの最大長	32KB
記憶域プールの最大容量	4PB

[Function 07]

リモートアクセス

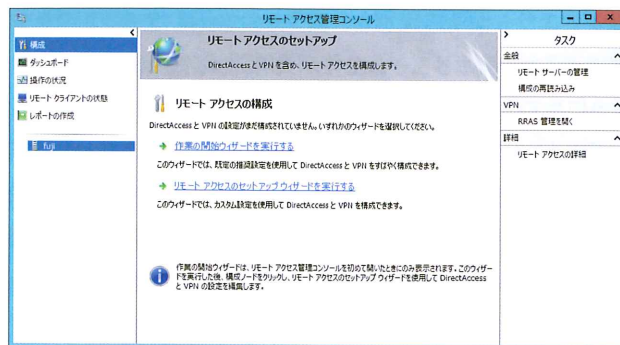
安全なリモートアクセス環境を容易に実現

リモートアクセスは、「DirectAccess」「ルーティング」「リモートアクセス」の3要素からなるネットワーク接続サービスだ(画面46)。Windows Server 2008 R2から搭載されたDirectAccessは、リモートアクセスサーバー(RAS)を設置可能なネットワークの構成、公開鍵基盤(PKI)の構築といった前提条件をクリアするのが難しい面があったが、Windows Server 2012では前提条件が大きく緩和されており、中小規模のネットワークでも利用しやすくなっている。

Windows Server 2012におけるリモートアクセスの新機能と強化点は表15のとおり。

DirectAccess

「DirectAccess」はIPv6(Internet Protocol version 6)とIPSec(Internet Protocol Security)を使ったセキュアなネットワーク接続サービスで、インターネット経由で社内



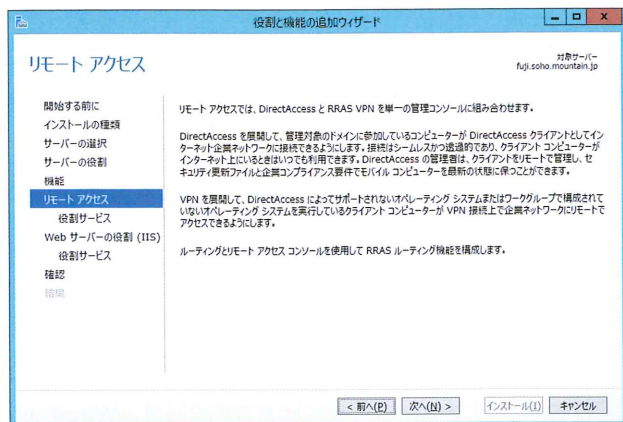
画面46：リモートアクセスは、「DirectAccess」「ルーティング」「リモートアクセス」の3要素からなる

のネットワークに安全にアクセスできる手段を提供する(画面47)。この機能が最初に搭載されたのはWindows Server 2008 R2だ。DirectAccessを構成したPCをインターネットなどに接続すると、自動的に企業ネットワークへのIPSecトンネルが確立されるので、ユーザーはネットワーク接続やVPN(Virtual Private Network)の確立を意識することなく、安全に企業ネットワークを利用できる。

このように便利で安全なDirectAccessだが、Windows Server 2008 R2ではDirectAccessと「ルーティングとリモートアクセス(RRAS)」の機能は排他的で、両方を1台のサーバー上で同時に実行することはできなかった。Windows Server 2012では、両者の接続許可ポリシーを見直すことで共存が可能になった。この他にも次のような改良が加えられており、非常に導入しやすくなっている。

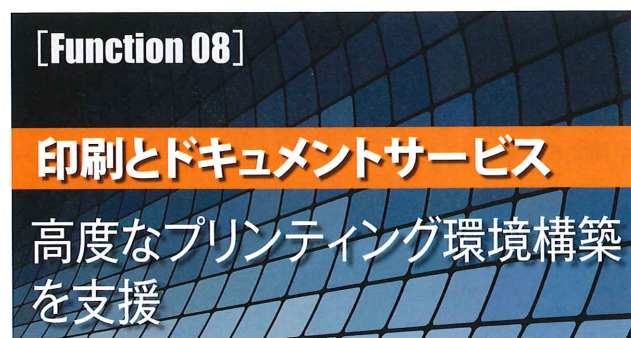
表15：リモートアクセスの新機能と強化点

新機能	DirectAccessとRRASの共存	VPNを使用しないで、インターネットから企業の内部ネットワークに直接接続できるDirectAccess機能と、以前のバージョンのWindows Serverの「ルーティングとリモートアクセス(RRAS)」に相当する機能が、1台のサーバー上で同時に実行できる。
	Windows PowerShell用RASモジュール	RASの構成と展開を管理するための、新しいPowerShell用コマンドレットを利用できる。
	NAT64とDNS64	IPv6を使うDirectAccessクライアントが、内部のIPv4専用リソースにアクセス可能にするための、プロトコルと名前解決の変換機能を提供する。
	ネットワーク負荷分散サポート	ネットワーク負荷分散(NLB)に対応しており、最大8ノードのサーバー展開で可用性とスケーラビリティを向上できる。
	Server Coreサポート	Server Coreインストールでもリモートアクセスの全機能を利用できる。
新機能	簡素化されたDirectAccess展開	新しい作業の開始ウィザードを使って、簡単にDirectAccessをセットアップできる。HTTPSベースのKerberosプロキシが、クライアントからの認証要求をDCに橋渡しするため、公開鍵基盤(PKI)はなくてもよい。
	NAT内部のDirectAccessサーバー	IP over HTTPSを利用することで、NATによって隔離された内部ネットワークにDirectAccessサーバーを設置できる。
	簡素化されたIPsec	従来2つ必要だったIPsecトンネルが、1つでよくなった。
	複数ドメイン サポート	リモートクライアントは、DirectAccessサーバーが所属するドメインとは別のドメインに接続できる。
	NAPの直接サポート	セットアップ中に「ネットワークアクセス保護(NAP)」の正常性チェックを構成できる。



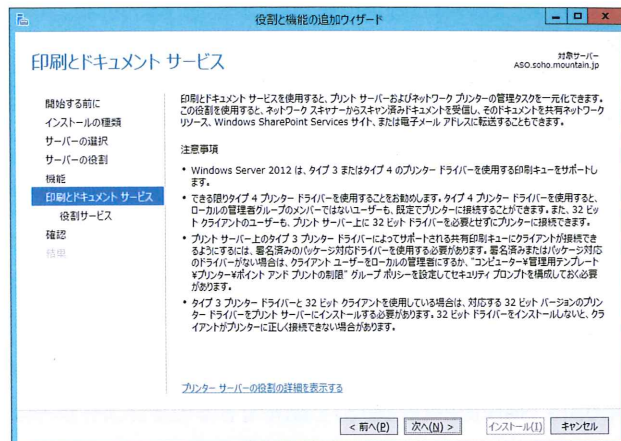
画面 47: DirectAccess はインターネット経由で社内のネットワークに安全にアクセスできる手段を提供する

- ◎RASの構成と展開に必要な、パブリックIPv4アドレスや公開鍵基盤(PKI)などの前提条件が大幅に緩和された
- ◎RASをインターネットと内部ネットワークの境界だけでなく、NATを使った内部ネットワークに設置できる。このとき、RASサーバーのネットワークアダプターは1つだけでよい
- ◎Windows 8に搭載された、Trusted Platform Module (TPM)ベースの仮想スマートカード認証と組み合わせることで、スマートカード発行システムの構築を省略できる



「印刷とドキュメントサービス」の役割は、「プリントサーバー」「LPDサービス」「インターネット印刷」「分散スキャンサーバー」の4つの役割サービスからなる、主にドキュメント印刷のためのサーバー機能を提供する(画面48)。分散スキャンサーバーとは、ネットワークに接続されたスキャナーで読み取ったドキュメントを、適切な宛先にルーティングするサーバーである。

Windows Server 2012における印刷とドキュメントサービスの新機能と強化点は表16のとおり。



画面 48: 「印刷とドキュメントサービス」の役割は、「プリントサーバー」「LPDサービス」「インターネット印刷」「分散スキャンサーバー」の4つ

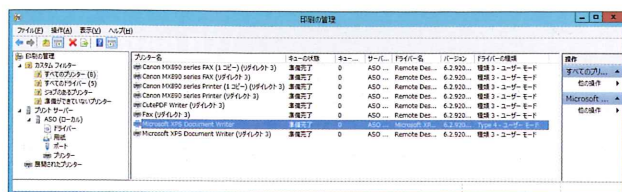
表 16: 印刷とドキュメントサービスの新機能と強化点

新機能	
タイプ4印刷ドライバー	Windows 8およびWindows Server 2012用の、新しい「タイプ4」印刷ドライバーモデルを採用した。タイプ4のプリンタードライバーでは、クライアントのバージョンやアーキテクチャに応じたプリンタードライバーを、サーバー上で共有する必要がない。
ブランチ オフィスダイレクト印刷	プリンター情報を中央で管理していても、印刷ジョブはブランチ オフィスのプリンターに直接送信される。
Windows PowerShell用印刷管理モジュール	プリンターの構成と展開を管理するための、新しいPowerShell用コマンドレットを利用できる。
機能強化	
高可用性印刷	フェールオーバー クラスター上にHyper-V環境を構築し、仮想マシンの監視機能を使ってプリンターサーバーの異常を検出し、フェールオーバーを実行して可用性を高める。
OpenXPSフォーマット	Microsoft XPS Document Writerによる印刷イメージフォーマットとして、OpenXPSフォーマット(拡張子.xps)が追加されて既定のフォーマットになった。

V4 印刷ドライバーモデル

Windows Server 2012およびWindows 8では、従来のプリンタードライバーモデル(タイプ3)に加えて、新しく「タイプ4印刷ドライバー」をサポートしている(次ページの画面49)。タイプ4印刷ドライバーでは、プリンタードライバーを印刷プロトコルに共通の処理をまとめた「印刷クラスドライバー」と、印刷デバイスに特化した「モデル別ドライバー」の2つに分離することができる。

Windowsには印刷クラスドライバーが含まれているので、メー



画面 49：従来のタイプ3ドライバーに加えて、新しいタイプ4ドライバーを利用できる

カーはモデル別ドライバーだけ開発して配布すればよい。モデル別ドライバーは、Windows UpdateやWindows Server Update Services(WSUS)で配布できるので、ユーザーは必要ときに最新のドライバーをすぐに入手できる。

プリンタードライバーの分割によって、ファイル数やファイルサイズが小さく、ドライバー数そのものも少ない印刷ドライバー環境が実現できる。システム管理者にとっては印刷環境の整備と維持が容易になり、メーカーにとっては共通部分を作成する必要がなく、開発コストを抑えながら安定度の高いドライバーを開発できるというメリットがある。印刷環境が安定すれば、さらにシステム管理者の運用コストは低下する。

また、タイプ4印刷ドライバーモデルでは、プリンターサーバー上でプラットフォーム別、アーキテクチャ別のプリンタードライバーをインストールする必要がなくなった。加えてドライバーファイル群はそれぞれ他のドライバーと隔離されているので、同じ名前のドライバーファイルが上書きされる事故を防止できる。

高可用性印刷

Windows Server 2012の高可用性印刷は、フェールオーバークラスターリング上にHyper-V環境を構築し、プリントサーバー仮想マシンを実行して可用性を高める技術だ。具体的には、Hyper-Vの「仮想マシンの監視」機能を使って、各ノードの「Print Spooler」サービスの異常を検出し、別のノードにプリンターサーバーの機能をフェールオーバーする。

Windows Server 2012では、ノードごとにプリンタードライバーをインストールする必要はなく、フェールオーバー環境を実現するために、WMI(Windows Management Instrumentation)やバッチファイルなどでコーディングする必要もないので、構築の敷居が低くなっている。

[Function 09]

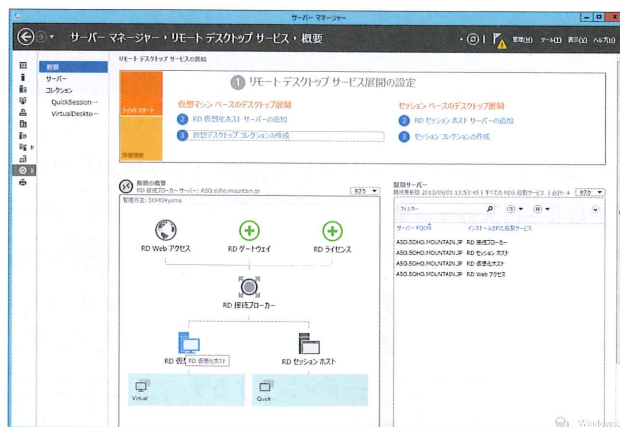
リモートデスクトップサービス

時代が求める柔軟なワークスタイルを実現

「リモートデスクトップサービス(RDS)」は、Windows Server 2012のデスクトップ環境をクライアントに提供したり、Windows Server 2012上で実行する仮想マシンをクライアントに割り当てたりするサービスだ(画面 50)。RDSには6つの役割サービスと1つのクライアントアプリケーションがあるが、ここでは「リモートデスクトップ」を「RD」と省略して、役割サービスの名前を短縮表記する。

最初にVDI(Virtual Desktop Infrastructure：仮想デスクトップ環境)と通常のRDSの違いを簡単に説明しておこう。VDIはユーザーに特定のコンピューターを割り当てる方式で、そのコンピューターを停止しても他のユーザーには影響を与えない。通常のPCから利用する場合は、ユーザーに2台のPCを与えたようなものだ。管理者権限があれば、リモートのコンピューターにアプリケーションや周辺機器をインストールすることもできるし、システム構成を変えることもできる。

一方、RDSは1台のRDセッションホストを全ユーザーで共用するので、RDセッションホストを停止してしまうと、ユーザー全員がリモートデスクトップを利用できなくなる。それでも、



画面 50：「リモートデスクトップサービス」は、柔軟なクライアント環境の構築を可能にする

システム管理者が代表してアプリケーションや周辺機器をインストールすることで、すぐに全ユーザーが利用できるようになるので、集中管理がしやすいというメリットが大きい。

VDIでもRDSでも、利用するデバイスとデスクトップ環境のあるコンピューターが分離されているので、例えば社内の自席にいるときは自分のデスクトップPCから利用するが、社内の別室や外出先、出張先ではノートPCから、リモートコンピューターに接続して、いつでも使い慣れたアプリケーションとデータを利用できるのが特長だ。

Windows Server 2012におけるRDSおよびVDIの概要

と新機能、強化点は表17のとおり。



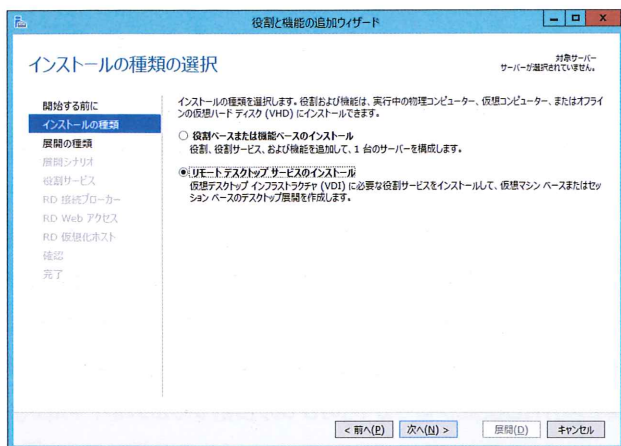
シナリオベースのインストール

RDSをインストールするには、サーバーマネージャーの[役割と機能の追加]で[リモートデスクトップサービスのインストール]オプションを選択する(次ページの画面51)。他の役割や機能とは異なり、独立したインストール手順になる。

RDSの展開の種類には、「標準の展開」と「クイックスタート」の2つがある。どちらも「RDセッションホスト」「RD Webアクセス」「RD接続ブロッカー」の3つの役割サービスをインストー

表17：RDSおよびVDIの概要と新機能、強化点

役割とアプリケーション	RDセッションホスト	RDクライアントからの接続要求を受信して、デスクトップセッションやRemoteAppへの接続を提供する。
	RD Web アクセス	RDCがWebインターフェースを経由してRDセッション ホストやRemoteAppに接続できるようにする。
	RD接続ブロッカー	複数のRDセッション ホストを用意してスケーラビリティを高める構成の場合、RDクライアントがどのRDセッションホストに接続するか調停する。 また、セッションの再接続機能を提供する。
	RDゲートウェイ	外部ネットワークからRDSを利用するための、ゲートウェイ機能を提供する。
	RDライセンス	RDSのためのクライアント アクセス ライセンス (CAL) を管理する。
	RD仮想化ホスト	Hyper-Vを実行して仮想マシンをホストし、仮想デスクトップ インフラストラクチャ (VDI) を構築する。
	RDクライアント (RDC)	RDSを利用するためのクライアント コンポーネント。 Windows Server 2012またはWindows 8と組み合わせることで、最新のユーザー エクスペリエンスを提供する。
新機能	RD管理サービス	従来は役割サービスごとに用意されていた管理ツールを、RD管理サービスに集約した。
	ユーザー プロファイル ディスク	移動ユーザー プロファイルやフォルダー リダイレクトではカバーできないデータ書き込みを、仮想ディスクに一括して保存する。
	RD接続ブロッカーの複数実行	フェールオーバークラスタリングを使用しないで、複数のRD接続ブロッカーを並列に実行することができるので、可用性とスケーラビリティが向上する。
	プールされた仮想マシンの自動作成	VDIにおいて、テンプレート仮想マシンをSysprepで作成し、これを複製して簡単に仮想マシンを増設できる。
	シナリオ ベースのインストール	他の役割や機能のインストールと、RDSのインストールが最初から分離されている。
機能強化	クイックスタート展開	RDセッション ホスト、RD Webアクセス、RD接続ブロッカーの3つの役割サービスと、RD管理サービスを1台のサーバーにまとめてインストールする。 「コレクション」を自動的に構成し、RD Webアクセスをすぐに利用可能な状態にする。
	セッション仮想化	RDセッション ホストを「コレクション」に含めることで、セッション管理をRDセッション ホスト サーバー単位からコレクション単位に仮想化した。
	RemoteAppの機能強化	Windows 7のタスク バーの機能(アプリケーションのグループ化、ジャンプリストなど)をサポートした。
	フェアシェア	CPU、ディスク、ネットワークの使用量を、複数のセッション間で公正に分配する。
	RD Webフォルダー	RemoteAppをグループ化して、RD Webやスタートメニューに表示する。
	シングル サイン オン (SSO)	役割サービスごとに認証を要求されることがなく、ドメインやRD Webへのログオンに使用したユーザー アカウントを一貫して使用する。
	RDゲートウェイ サービスのUDPサポート	HTTPに加えてUDPでの接続が可能になり、通信効率が向上する。
	USBリダイレクト	RDCに接続したUSBデバイスをRDSH側で利用可能にする、包括的なメカニズムを提供する。
	RDクライアント	リモート デスクトップ プロトコル (RDP) 8.0に対応した。 Windows Server 2012およびWindows 8の新しいUIやマルチタッチを利用できる。 ネットワーク接続品質を自動的に検出し、最適なエンコードを自動選択する。
	RemoteFXのネイティブ対応	RemoteFXテクノロジーが標準で組み込まれており、通信状況に応じたエンコード自動選択、マルチタッチとジェスチャー、USBリダイレクトに対応している。



画面 51: 「リモートデスクトップサービスのインストール」オプションを選択する

ルするが、「標準の展開」は役割サービスやオプションを任意に選択できる。一方、「クイックスタート」では、RDSのサーバーや仮想マシン、アプリケーション管理単位である「コレクション」を自動作成して、RemoteAppをWebに公開するところまで一気に自動実行される。

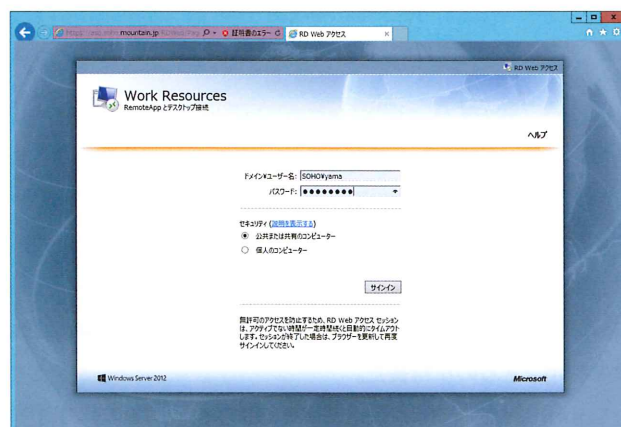
どちらの展開方法を選択しても、さらに続けて「仮想マシンベースのデスクトップ展開」と「セッションベースのデスクトップ展開」を選択する。

「仮想マシンベースのデスクトップ展開」はVDIを構築するオプションで、ユーザーごとに特定の仮想マシンを割り当てたり、汎用の仮想マシンプールを提供したりする。したがって、自動的にHyper-Vの役割もインストールされる。一方、「セッションベースのデスクトップ展開」は通常のRDSを構築するオプションで、RDセッションホストのデスクトップをセッションごとに提供する。

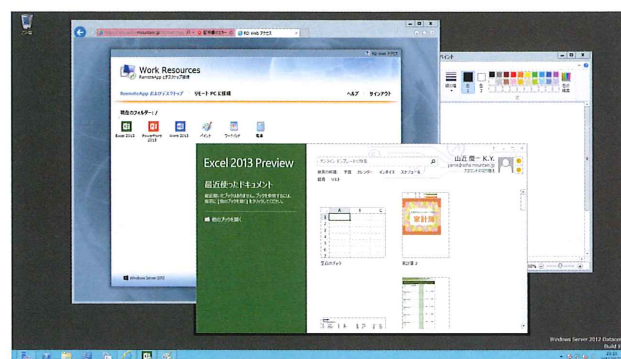
「クイックスタート」で「セッションベースのデスクトップ展開」を選択すると、既定では「QuickSessionCollection」コレクションに、RemoteAppプログラム「ペイント」「ワードパッド」「電卓」を作成して、次のURLで公開するところまで、ほぼ全自動で実行される。短時間でRDSを構築できる便利な展開方法だ(画面52、画面53)。もちろん、シナリオベースのインストールを再実行すれば、他の役割サービスを選択したり、VDI環境を構築したりすることができる。

<https://<RDSサーバーのFQDN>/RDWeb/>

なお、どちらの展開方法を選んでも、RDライセンスサーバー



画面 52: Webブラウザで「https://<RDSサーバーのFQDN>/RDWeb/」にアクセスして、ログインする



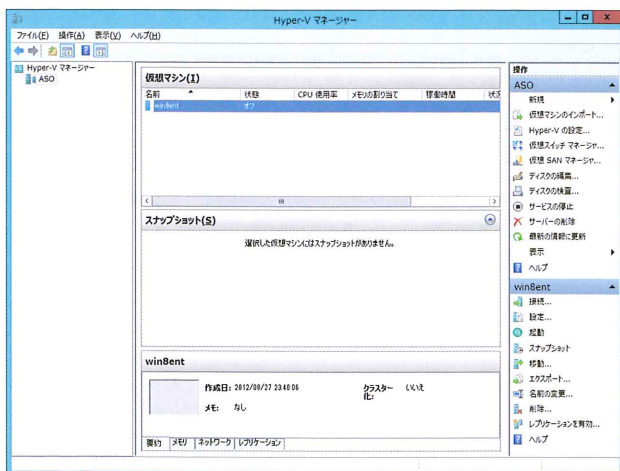
画面 53: RemoteAppはローカルのウィンドウとシームレスに結合する

は別途手動でインストールする必要がある。DCなど適切なコンピュータをRDライセンスサーバーにして、インターネット(Web)か電話でアクティブ化し、別途購入したRDS CALをインストールする。

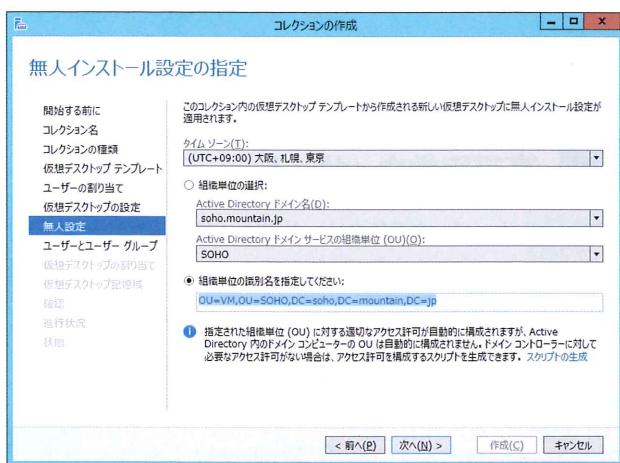
仮想デスクトップテンプレート

VDIでユーザーごとに1台の仮想マシンを割り当てる場合、仮想マシンをユーザー数分構築する作業が発生する。仮想化環境とはいえ、単純に仮想ディスクファイルをコピーして作成することはできないので、それなりの作業は必要になる。

Windows Server 2012のRDSでは、Hyper-V上に用意した1台の仮想マシンを「テンプレート」にして、必要な数だけ安全に複製して自動生成する「仮想デスクトップテンプレート」機能が用意されている。テンプレート仮想マシンは、ユーザーに使わせたいアプリケーションをインストールして、デスクトップ環境などユーザープロファイルをカスタマイズし、最後に次のコマンドを実行して一般化することで作成する(画面54)。



画面 54: テンプレート仮想マシンを準備する



画面 55: 「无人インストール設定の指定」画面で、右下にある「スクリプトの生成」というリンクをクリックする

%Windir%\%System32%\Sysprep\Sysprep.exe /
generalize /oobe /shutdown /mode:vm

テンプレートから生成した仮想マシンをドメインに参加させる際に、特定のOUにコンピューターアカウントを作成する場合は、RD仮想化ホストのコンピューターアカウントがそのOUを操作できるように、あらかじめ委任の設定をする必要がある。

そのためには、「コレクションの作成」ウィザードの「无人インストール設定の指定」画面で、右下にある「スクリプトの生成」というリンクをクリックする(画面 55)。ここで表示されるPowerShellのスクリプトを、適切なテキストファイルにコピー＆ペーストしてDC上で実行すれば、必要なアクセス権がRD仮想化ホストに与えられる。



ユーザープロファイルディスク

VDIでは、「個人用仮想デスクトップコレクション」と「プールされた仮想デスクトップコレクション」を選択してコレクションを作成する。

「プールされた仮想デスクトップコレクション」を選択した場合は、あらかじめストックしておいた仮想マシン群から、ユーザーセッションごとに動的に仮想マシンを割り当てることができる。そして、サインアウト(ログオフ)によってセッションが終了すると、それまで仮想マシンに加えられた変更をリセットして、他のユーザーが使うときに何も残らないようにする。

「プールされた仮想デスクトップコレクション」を利用しながら、ユーザーのデスクトップ設定や作成したファイルなどを保存したい場合は、「ユーザープロファイルディスク」を別途用意して保管するように構成できる。プール内の仮想マシンには変更を加えず、ユーザー環境も保存できる新しい技術だ。



RemoteFXのネイティブ対応

Windows Server 2012のRDSには、GPUを仮想化して仮想デスクトップ環境でDirectX 11を利用可能にする「RemoteFX」が標準で組み込まれており、RDSサーバーがシステム要件を満たせばすぐに利用できる。

◎RemoteFXのシステム要件(RDSサーバー側)

SLAT(Second Level Address Translation)をサポートしたCPU

RemoteFX対応GPU(DirectX 11サポート)

ただし、RemoteFX USBリダイレクトのみを利用する場合は、RemoteFX対応GPUは必要ない。

新しいRemoteFXでは、ネットワークの状態を自動的に検出して、最適なエンコーディング方法を選択する「RemoteFXアダプティブグラフィックス」、クライアント側に接続したUSBデバイスを仮想デスクトップにリダイレクトして利用可能にする「RemoteFX USBリダイレクト」、マルチメディアコンテンツをクライアント側で再生する「RemoteFXメディアリモート処理」、マルチタッチとジェスチャに対応した「RemoteFXマルチタッチ」の各機能を装備しており、Windows 8との高い親和性を提供する。

[Function 10]

フェールオーバークラスタリング

サーバーに高い可用性と
スケーラビリティを提供

Windows Server 2012のフェールオーバークラスタリング機能は、物理サーバー間でも、Hyper-V上の仮想マシン間でもクラスターシステムを構築できる(画面56)。前項で紹介した「スケールアウトファイルサーバー(SOFS)」のように、Hyper-Vの上にフェールオーバークラスタリングを組み合わせた、逆に「高可用性印刷」のようにフェールオーバークラスタリングの上にHyper-Vを配置したりすることで、仮想化環境と高可用性システムの両方のメリットを生かしたシステムを構築できる。フェールオーバークラスタリング環境からHyper-V仮想マシンの状態をモニタリングできるので、さまざまな応用が考えられる。



画面 56: Windows Server 2012のフェールオーバークラスタリングは、「フェールオーバークラスタマネージャー」とPowerShellコマンドレットで管理できる

Windows Server 2012におけるフェールオーバークラスタリングの新機能と強化点は表18のとおり。

高可用性ウィザード

フェールオーバークラスタリングでは、「高可用性ウィザード」を使って次の役割を構成できる(画面57)。クラスターを構成する全ノードには、役割を実行するために必要な役割サービ

表 18: フェールオーバークラスタリングの新機能と強化点

新機能	スケールアウトファイルサーバー	SMB 3.0と「クラスター共有ボリューム(CSV)」を使って、全ノードから同時に読み書き可能な共通の記憶域を構築して、ノードの追加で簡単にスケールアウト(増設による性能拡張)を可能にしたファイルサーバー機能を提供する。
	クラスター対応更新	ノードを順番に停止して更新プログラムを適用し、ノードを再開する手順を自動化した。
	仮想マシンのアプリケーション監視	フェールオーバー クラスター上でHyper-Vを実行し、仮想マシン内のアプリケーションやサービスの状態を監視して、仮想マシンのフェールオーバーを実行できる。
	iSCSI Software Target統合	「iSCSIターゲット サーバー」の役割サービスをインストールしたノードを使って、フェールオーバーに対応した高可用性iSCSIターゲットサーバーを構築できる。
機能強化	スケーラビリティ向上	物理ノード数: 64台 (Windows Server 2008 R2では16台) 仮想マシン: 8,000台 (Windows Server 2008 R2では1,000台)
	クラスターの共有ボリューム	クラスター共有ボリューム(CSV)のバックアップと復元機能を強化した。 ダイレクトI/Oによってアクセスが高速化した。 SMB 3.0をサポートした。 BitLockerドライブ暗号化をサポートした。 記憶域スペースと統合した。
	構成の検証ウィザード	クラスターを構成する前に、ハードウェアやソフトウェアがCSVやHyper-V環境要件、仮想マシン間のフェールオーバーに適合していることを確認できる。
	AD DS統合	クラスター ノードと同じOUに、クラスター コンピューター アカウントなどを作成できる。
	マルチサイトサポート	クォーラムの「票」を持つノードと持たないノードを制御できる。 ノードがシャットダウンされたときに、ノード数を変化させてクォーラムを満たすように調整する「動的クォーラムモデル」を採用した。
	クラスターのアップグレード	Windows Server 2008以降で構築したクラスター システムは、構成を維持したままWindows Server 2012にアップグレードできる。 Hyper-V環境で、エクスポートした仮想マシンを再度インポートできる。

スや機能をインストールしておく。例えば、フェールオーバークラスターの「iSCSI ターゲットサーバー」の役割を構成するには、クラスター内の全ノードで、サーバーマネージャーを使って「iSCSI ターゲットサーバー」の役割サービスをインストールする必要がある。

- ・ DFD 名前空間サーバー
- ・ DHCPサーバー
- ・ Hyper-Vレプリカブローカー
- ・ iSCSI ターゲットサーバー
- ・ iSNSサーバー
- ・ WINSサーバー
- ・ その他のサーバー
- ・ ファイルサーバー
- ・ メッセージキュー
- ・ 仮想マシン
- ・ 汎用アプリケーション
- ・ 汎用サービス
- ・ 汎用スクリプト
- ・ 分散トランザクションコーディネーター(DTC)

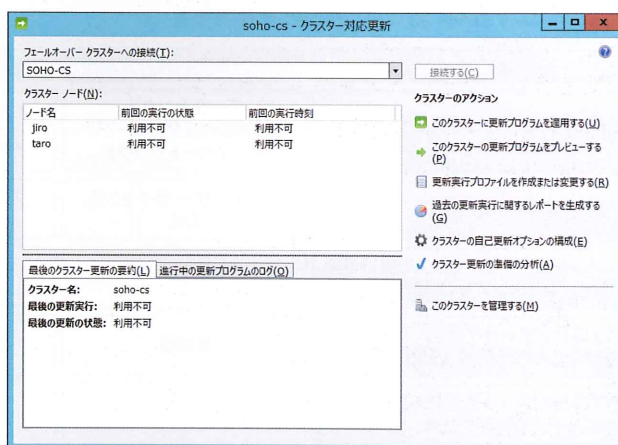
クラスター対応更新

フェールオーバークラスタリング環境でノードに更新プログラムを適用するには、全体としてはサービスを継続しながら、フェールオーバーとフェールバックを計画的に実行してノードを順番にメンテナンスしていく、「ローリングアップデート」と

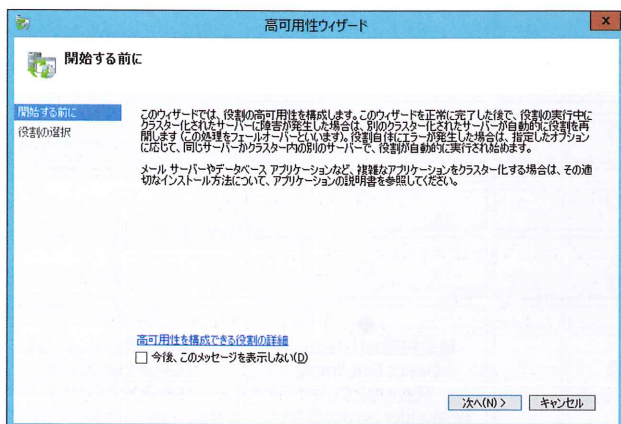
いうテクニックを使うことがある。「クラスター対応更新(CAU)」は、このローリングアップデートを自動的に実行する新機能だ(画面58)。

CAUには、クラスター外のコンピューターが更新プログラムの適用手順を管理する「リモート更新モード」と、クラスター自身が管理する「自己更新モード」がある。リモート更新モードでは「アップデートコーディネーター」と呼ばれるコントローラーPCが必要になる。一方、自己更新モードではクラスターの各ノードにCUAの役割がインストールされて、ノードが順に所有権を握って、所有権のないノードに更新プログラムを適用する(画面59)。

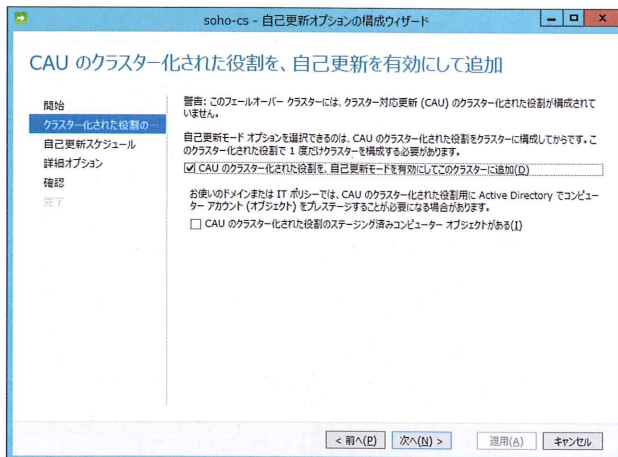
CUAを利用して更新プログラム適用を自動化することで、更新プログラム適用作業からシステム管理者を開放することができるとともに、システム管理者のミスによる可用性の低下を防止できるので、積極的に活用したい機能だ。



画面58: 「クラスター対応更新 (CAU)」は、このローリングアップデートを自動的に実行する新機能だ



画面57: Windows Server 2012の「高可用性ウィザード」



画面59: 「自己更新モード」のオプションの構成ウィザード

Edition

早わかり! Windows Server 2012 製品体系

～シンプル&高い投資効率でIT基盤の進化を強力に支援～

最後に、Windows Server 2012の製品体系とライセンスについて解説しよう。
Windows Server 2012は会社の規模、用途に合わせて容易に導入を検討できるように、
非常にシンプルな製品体系に変更されている。

創報 山近 慶一 / Microsoft MVP Windows Server System - Microsoft Update Service

表 20 : Windows Server 2012のエディション比較(筆者調べ)

エディション	Datacenter	Standard	Essentials	Foundation
最適な用途	データセンター 高集約度の仮想化サーバー プライベートクラウド	通常集約度の 仮想化サーバー プライベートクラウド	スモールビジネス クラウドサービスの利用	単機能サーバー
ライセンス モデル	プロセッサ ライセンス CAL	プロセッサ ライセンス CAL	サーバー ライセンス (最大25ユーザー アカウント)	サーバー ライセンス (最大15ユーザー アカウント)
1プロセッサ ライセンスで実行可能 なOSインスタンス数(物理環境)	1	1	1(仮想化環境と排他利用)	1
1プロセッサ ライセンスで実行可能 なOSインスタンス数(仮想化環境)	無制限	最大2インスタンス	1(仮想化環境と排他利用)	—
1プロセッサ ライセンスで サポートする物理プロセッサ数	2	2	2	1
販売チャネル	ボリュームライセンス OEM Services Provider License Agreement (SPLA)	ボリュームライセンス OEM 店頭 SPLA	ボリュームライセンス OEM 店頭 SPLA	OEMのみ
Active Directory Rights Managementサービス(AD RMS) ※RMS CALが必要	◎	◎	◎	◎
Active Directoryドメイン サービス (AD DS)	◎	◎	●	○ フォレストルートドメインのみ
Active Directoryフェデレーション サービス(AD FS)	◎	◎	◎	◎
Active Directoryライトウェイト ディレクトリ サービス(AD LDS)	◎	◎	◎	◎
Active Directory証明書サービス (AD CS)	◎	◎	● 機能制限あり(Network Device Enrollment ServicesとOnline Responder Serviceがない)	○ 機能制限あり(Network Device Enrollment ServicesとOnline Responder Serviceがない)

シンプルになった製品体系 **4つのエディションで企業を支援**

Windows Server 2012には「Datacenter」「Standard」「Essentials」「Foundation」の4つのエディションが用意されている。すべてx64互換CPU用の64ビット版で、インテルのItaniumプロセッサはサポートされない。DatacenterとStandardに機能的な差異はなく、1サーバーライセンスにおける仮想マシンの同時実行数のみが異なる(表20)。

プロセッサライセンス、サーバーライセンス、クライアントアクセスライセンス CAL)、AD RMS CAL、RDS CALは、OEMや認定ディストリビューター、リセラー、ソリューション

ンプロバイダーなど、多数のチャンネルで入手できる。最適なライセンス形態や必要ライセンス数の確認なども、これらの販売チャンネルに問い合わせるとよいだろう。

■ インストールオプション

Windows Server 2012のインストールオプションには「Server Coreインストール」と「GUI使用サーバー」がある。Windows Server 2012の推奨インストールはServer Coreインストールで、役割や機能のインストールと構成、運用管理はWindows PowerShellで実行する。一方、GUI使用サーバーはWindows 8とほぼ同じスタート画面やデスクトップなどのGUIを使った、リッチな運用管理環境を構築

エディション	Datacenter	Standard	Essentials	Foundation
DHCP サーバー	○	○	○	○
DNS サーバー	○	○	●	○
FAX サーバー	○	○	○	○
Hyper-V	○	○	—	—
Server Core	○	○	—	—
UDDI サービス	○	○	○	○
Webサーバー (IIS)	○	○	○	○
Windows Server Update Services	○	○	—	—
Windows展開サービス (WDS)	○	○	○	○
アプリケーションサーバー	○	○	○	○
ネットワークポリシーとアクセス サービス	○	○	● RRAS:最大50接続 IAS:最大10接続	○ RRAS:最大50接続 IAS:最大10接続
ファイル サービスおよび記憶域サービス	○	○	●	○
フェールオーバー クラスター	○	○	○	○
ボリュームライセンス認証サービス (キー管理サービス)	○	○	○	○
リモートアクセス (VDI、ダイレクトアクセス、ブランチ キャッシュ)	○	○	○	○
ダイレクトアクセス	○	○	○	○
ブランチ キャッシュ	○	○	○	○
リモートデスクトップサービス ※RDS CALが必要	○	○	●	○ 最大20接続
印刷とドキュメント サービス	○	○	○	○
ネットワークアクセス保護 (NAP)	○	○	○	○

○ 完全対応 ● 対応(構成/設定変更不可) ○ 部分応(制限あり) — なし

できる。

Server Coreインストールには次のようなメリットがある。ディスク使用量の削減効果は、特に仮想化環境で効果的だ。また、有効化していない役割や機能のためのファイル群を削除してシステムをシェイプアップする「オンデマンド機能」も搭載しており、ディスク使用量をさらに1GB削減できる。

◎GUIを省略することでCPUやメモリなどのリソースを最大限アプリケーションに割り当てることができる

◎サービスを削減することで、さらにCPUやメモリを節約できる

◎ディスク使用量を4GB削減できる

◎攻撃の対象になる機会を削減する

■アップグレードパス

64ビット版のWindows Server 2008(SP2)と、Windows Server 2008 R2(SP1)からは、Windows Server 2012に直接アップグレードすることができる。いわゆる「インプレースアップグレード」という方法で、Windows Server 2008(R2)を実行中のサーバーに、Windows Server 2012のインストールメディアをセットして、直接アップグレードの手順を実行する方法だ。

Windows Server 2012のエディション構成でも説明したとおり、Windows Server 2012のDatacenterエディションとStandardエディションに機能的な差異はないので、Windows Server 2008(R2)のStandardエディションおよびEnterpriseエディションからは、Windows Server 2012のDatacenterエディションとStandardエディションのどちらにでもアップグレードできる。

なお、次のケースではインプレースアップグレードを実行できないので注意してほしい。

1. 32ビット版Windows ServerからWindows Server 2012へのアップグレード
2. 異なる言語のWindows Server 2012へのアップグレード
3. 異なるビルドタイプ(FRE版とCHK版)のWindows Server

2012へのアップグレード

4. ベータやRCからWindows Server 2012 RTMへのアップグレード
5. Server CoreからGUIサーバーに直接アップグレード (Server CoreからServer Coreにアップグレード後、GUIサーバーに変更するのであればOK)

インプレースアップグレードがサポートされていないバージョンおよびアーキテクチャのWindows Serverを使用している場合は、いったん新しいサーバーにWindows Server 2012をインストールして、Windows Server 2012の「Windows Server移行ツール」機能を使って旧サーバーから役割や機能、システム設定、共有設定、データを取り出す方法がある。

こちらは32ビットおよび64ビットのWindows Server 2003 SP2とWindows Server 2003 R2からの移行もサポートされているので、より多くのシステムをWindows Server 2012に移行できる。移行の詳しい手順は、マイクロソフト「TechNet」の技術文書「Windows Server 2012への役割と機能の移行」および「Windows Server移行ツールのインストール、使用、および削除」を参照してほしい。

【参考Webサイト】

- ▶ Windows Server 2012 のインストール
URL <http://technet.microsoft.com/ja-jp/library/jj134246.aspx>
- ▶ Windows Server 2012 へのドメインコントローラーのアップグレード
URL <http://technet.microsoft.com/ja-jp/library/hh994618.aspx>
- ▶ Evaluation Versions and Upgrade Options for Windows Server 2012
URL <http://technet.microsoft.com/ja-jp/library/jj574204>
- ▶ Windows Server 2012 への役割と機能の移行
URL <http://technet.microsoft.com/ja-jp/library/jj134039.aspx>
- ▶ Windows Server 移行ツールのインストール、使用、および削除
URL <http://technet.microsoft.com/ja-JP/library/jj134202>



Windows Server 2012 で あなたのデータセンターにクラウド級のパワーを。

Windows Server 2012 は、これまでクラウドでしか利用できないと考えられてきた俊敏性、可用性、そして柔軟性をあなたのデータセンターにもたらしめます。

クラウド機能を強化した Windows Server 2012 で、あなたの IT インフラの可能性を最大限に引き出してください。

詳しくは www.microsoft.com/ja-jp/server-cloud/ws2012



Windows Server 2012

BUILT FROM THE CLOUD UP.



マイクロソフトのプライベートクラウドソリューションに関する情報は、以下の URL をご参照ください。

■ マイクロソフトのプライベートクラウドソリューション

<http://www.microsoft.com/ja-jp/server-cloud/private-cloud/default.aspx>

■ Windows Server 2012

<http://www.microsoft.com/ja-jp/server-cloud/windows-server/default.aspx>

■ System Center

<http://www.microsoft.com/ja-jp/server-cloud/system-center/default.aspx>

■ Windows Server TechCenter

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

※ Microsoft、Windows、Windows Server、Hyper-V、System Center は、米国 Microsoft Corporation の米国及びその他の国における登録商標または商標です。

※ Windows の正式名称は、Microsoft Windows Operating System です。

※ その他、記載されている会社名、製品名は、各社の登録商標または商標です

マイクロソフト製品に関するお問い合わせは、次のインフォメーションをご利用ください。

■ インターネットホームページ <http://www.microsoft.com/japan/>

■ マイクロソフト カスタマー インフォメーション センター ☎ 0120-41-6755 (携帯電話 / PHS からご利用いただけます)

(受付時間: 9:30~12:00、13:00~19:00 土日祝日、弊社指定休業日を除きます)

※電話番号のおかけ間違いにご注意ください。

日本マイクロソフト株式会社

〒108-0075 東京都港区港南 2-16-3 品川グランドセントラルタワー