

**Windows Server "8" Beta のリモート デスクトップ サービスの理解およびトラブルシューティング**

Microsoft Corporation

発行日: 2012 年 2 月

**概要**

この『理解およびトラブルシューティング ガイド (UTG)』を読むと、Windows Server "8" Beta のリモート デスクトップ サービスの技術的概念、機能、およびトラブルシューティング方法を学ぶことができます。この UTG では以下を提供します。

* 機能の技術的な概要と機能の説明
* 機能のインストール、構成、管理を実行するために役立つ技術的な概念
* 構成と管理のユーザー インターフェイス オプションおよび設定
* 機能に関連するアーキテクチャと依存関係、および技術的実装
* 機能の主なトラブルシューティング ツールと手段



**著作権情報**

このドキュメントは「現状のまま」提供されています。このドキュメントに表されている情報および見解 (URL および他のインターネット Web サイトの参照を含む) は、予告なしに変更される場合があります。

ここに描写されている一部の例は、図解のみを目的としており、架空のものです。現実との関連または関係を意図したものではなく、それらを意味するものでもありません。

このドキュメントは、いかなる Microsoft 製品のいかなる知的財産に対する法的権利を提供するものではありません。このドキュメントは、内部での参照目的で複製および使用できます。

© 2012 Microsoft. All rights reserved.

Active Directory、Hyper-V、Microsoft、MS-DOS、Visual Basic、Visual Studio、Windows、Windows NT、Windows Server、および Windows Vista は Microsoft グループ企業の商標です。

その他のすべての商標は各社が所有しています。

| **著者について** | |
| --- | --- |
| **著者:** | Don Geddes |
| **略歴:** | Don Geddes は米国テキサス州アービングでマイクロソフト商用テクニカル サポートに従事するシニア サポート エスカレーション エンジニアで、リモート デスクトップ サービスのトラブルシューティングとアドバイザリー サービスを専門としています。Don は TechNet のホワイトペーパーやサポート技術情報の記事を執筆しているほか、Microsoft Press 発行の数冊の書籍にも寄稿しています。また、Don はマイクロソフト認定システム エンジニア、テクノロジ スペシャリスト、およびマイクロソフト認定トレーナーとして、マイクロソフトの従業員に新製品のアーキテクチャを教えています。さらに、マイクロソフト公式の TechNet Ask the Performance Team ブログ、[ASKPERF](http://blogs.technet.com/b/askperf/) にも寄稿しています。 |
| **プロジェクト リード:** |  |
| **略歴:** |  |

目次

[Windows Server "8" Beta のリモート デスクトップ サービスの理解およびトラブルシューティング 1](#_Toc323636309)

[『理解およびトラブルシューティング ガイド』について 1](#_Toc323636310)

[リモート デスクトップ サービスの概要 1](#_Toc323636311)

[技術概要 2](#_Toc323636312)

[リモート デスクトップ サービスのインストールと有効化 23](#_Toc323636313)

[インストール プロセス 25](#_Toc323636314)

[リモート デスクトップ サービスの構成および管理 42](#_Toc323636315)

[管理の考慮事項 42](#_Toc323636316)

[管理と構成 43](#_Toc323636317)

[リモート デスクトップ サービス セッション仮想化のアーキテクチャ 66](#_Toc323636318)

[概要 66](#_Toc323636319)

[リモート デスクトップ サービスのトラブルシューティング 87](#_Toc323636320)

[リモート デスクトップ サービスのトラブルシューティングの概要 87](#_Toc323636321)

[シナリオ ベースのインストールのトラブルシューティング 89](#_Toc323636322)

[コレクション作成のトラブルシューティング 100](#_Toc323636323)

[リモート デスクトップ サービスのトラブルシューティング ツール 101](#_Toc323636324)

[付録 107](#_Toc323636325)

[付録 A — 新規グループ ポリシーの一覧 107](#_Toc323636326)

# Windows Server "8" Beta のリモート デスクトップ サービスの理解およびトラブルシューティング

### 『理解およびトラブルシューティング ガイド』について

『Windows Server "8" Beta の理解およびトラブルシューティング ガイド』は、主要な技術的概念、アーキテクチャ、機能、およびトラブルシューティングのツールとテクニックの理解に役立ちます。これらを理解することで、RTM プレリリース製品の評価段階で無事に早期導入することができます。これは管理者およびアーキテクトを対象としたレベル 300 の資料で、読者が以前のオペレーティング システムの既存の機能に関する広い知識を既に持っていることを前提としています。

## リモート デスクトップ サービスの概要

このガイドでは、リモート デスクトップ サービスは、Windows Server "8" Beta の以下の役割および関連付けられた役割サービスを示します。

* リモート デスクトップ セッション ホスト
* リモート デスクトップ Web アクセス
* リモート デスクトップ接続ブローカー
* リモート デスクトップ ゲートウェイ
* リモート デスクトップ ライセンス
* リモート デスクトップ管理サービス

#### リモート デスクトップ サービスとは

Windows Server "8" Beta のリモート デスクトップ サービスは、集中化されたデスクトップ環境を企業が実装するために必要なプラットフォームを提供し、データ セキュリティを強化してデスクトップとアプリケーションに対する IT の管理能力を高め、柔軟性とコンプライアンスを向上させることができるようになります。

RDS はセッション仮想化および VDI テクノロジを使用する、集中化されたデスクトップおよびアプリケーション プラットフォーム ソリューションで、これによって IT 部門はデスクトップの提供と管理を通して、ユーザーのニーズに柔軟に対応することが可能になります。RDS はターミナル サービスの新しい名称で、ユーザーがどこにいてもデータセンターでデスクトップやアプリケーションを実行できるように、 Windows Server "8" Beta の標準機能で提供可能です。

このガイドでは、リモート デスクトップ セッション ホスト (RDSH)、リモート デスクトップ Web アクセス (RDWeb)、リモート デスクトップ接続ブローカー、リモート デスクトップ ゲートウェイ、リモート デスクトップ ライセンス、およびリモート デスクトップ クライアントといったセッション仮想化に関連するすべての RDS テクノロジについて説明します。Microsoft VDI と RemoteFX については、このガイドと同時に発行される別のガイドで説明します。

#### 目的と利点

RDS は、Windows Server "8" Beta が備えているプラットフォーム機能を活かすマイクロソフト パートナーのテクノロジと共に、あらゆるタイプの組織にとって、コスト効率の良いソリューションとなります。特に、フリーアドレスのオフィス環境や自宅での作業を必要とする契約社員、外部委託先社員、オフィス ワーカーなど、柔軟なデスクトップまたはアプリケーション アクセスを必要とするモバイル ワークフォース、定型業務化されたタスク ワーカー、またはナレッジ ワーカーを擁する組織で、大きな効果を発揮します。RDS を展開することで、どのような規模の組織にも、真のビジネス価値を実現するために必要な柔軟性と機能が提供されます。

### 技術概要

以下のセクションでは、Windows Server "8" Beta リモート デスクトップ サービスの新機能について、技術的な概要を説明します。

#### 前提条件

この『理解およびトラブルシューティング ガイド』は、Windows Server 2008 および Windows Server 2008 R2 に含まれる以前のバージョンのリモート デスクトップ サービスのコンポーネントに精通していることを前提として記述されています。ここでは、これらのコンポーネントの目的や機能に関する基礎は詳述しません。このガイドでは、Windows Server "8" Beta の新機能と向上した機能について説明し、ガイダンスを提供することに重点を置いています。

#### 機能の説明

リモート デスクトップ サービスは、いくつかの役割サービスから構成されています。これらの役割サービスは、個々にインストールして基本的機能を使用することも、他のリモート デスクトップ役割サービスと組み合わせて追加の機能や利点を得ることもできます。この「機能の説明」では、各リモート デスクトップ役割サービスの新機能の概要を説明するだけでなく、役割サービスが連携して追加機能を提供する場合についても示します。Windows Server "8" Beta リモート デスクトップ管理サービス (RDMS) を使用したリモート デスクトップ サービス環境のインストールと構成についても説明します。

##### セキュリティの考慮事項

以前のバージョンの Windows と同様、リモート デスクトップ セッション ホストの役割サービスと Active Directory ドメイン サービスを同じサーバー上に共存させることは推奨されません。この理由は、セキュリティ リスクがあるため、およびパフォーマンスと機能性が低下するおそれがあるためで、ドメイン コントローラーのインストール時にリモート デスクトップ セッション ホストの役割サービスがインストールされていることを DCPROMO が検出すると、ユーザーにこのリスクが通知されます。反対に、既にドメイン コントローラーとなっているサーバーにリモート デスクトップ セッション ホストの役割サービスをインストールしようとした場合も、同じメッセージが表示されます。このメッセージが表示された後もインストールを続行する場合は、このリスクを認識し、受け入れたものと見なされます。

##### リモート デスクトップ管理サービス

リモート デスクトップ サービス (旧称: ターミナル サービス) の管理方法は、Windows NT 4.0 Terminal Services Edition の最初のバージョン以降、それほど変わっていません。後続の各リリースの Windows で新機能が追加されたのに伴い、新機能をサポートする新しいツールとユーザー インターフェイスがいくつか追加されましたが、全体的な管理機能に大きな変更はありません。リリースを重ねるごとに、リモート デスクトップの展開が多様化、複雑化するにつれて、きわめて基本的な展開でさえ、構成と管理に時間がかかるようになり、管理作業はますます断片化していきました。

Windows Server "8" Beta では、リモート デスクトップの管理タスクを簡素化すると共に、リモート デスクトップ サービスのすべての役割サービスとシナリオの一元管理ソリューションを提供することを目的に設計されたリモート デスクトップ管理サービス (RDMS) およびユーザー インターフェイスを導入しました。RDMS では、インストールされている役割サービスごとに別の管理ツールを使用するのではなく、付属の統一ユーザー インターフェイスを使用してリモート デスクトップ サービス環境に含まれているすべてのサーバーの概要を表示できます。また、RDMS は、環境内の各サーバー用の管理インターフェイスも備えています。

###### RDMS の基本

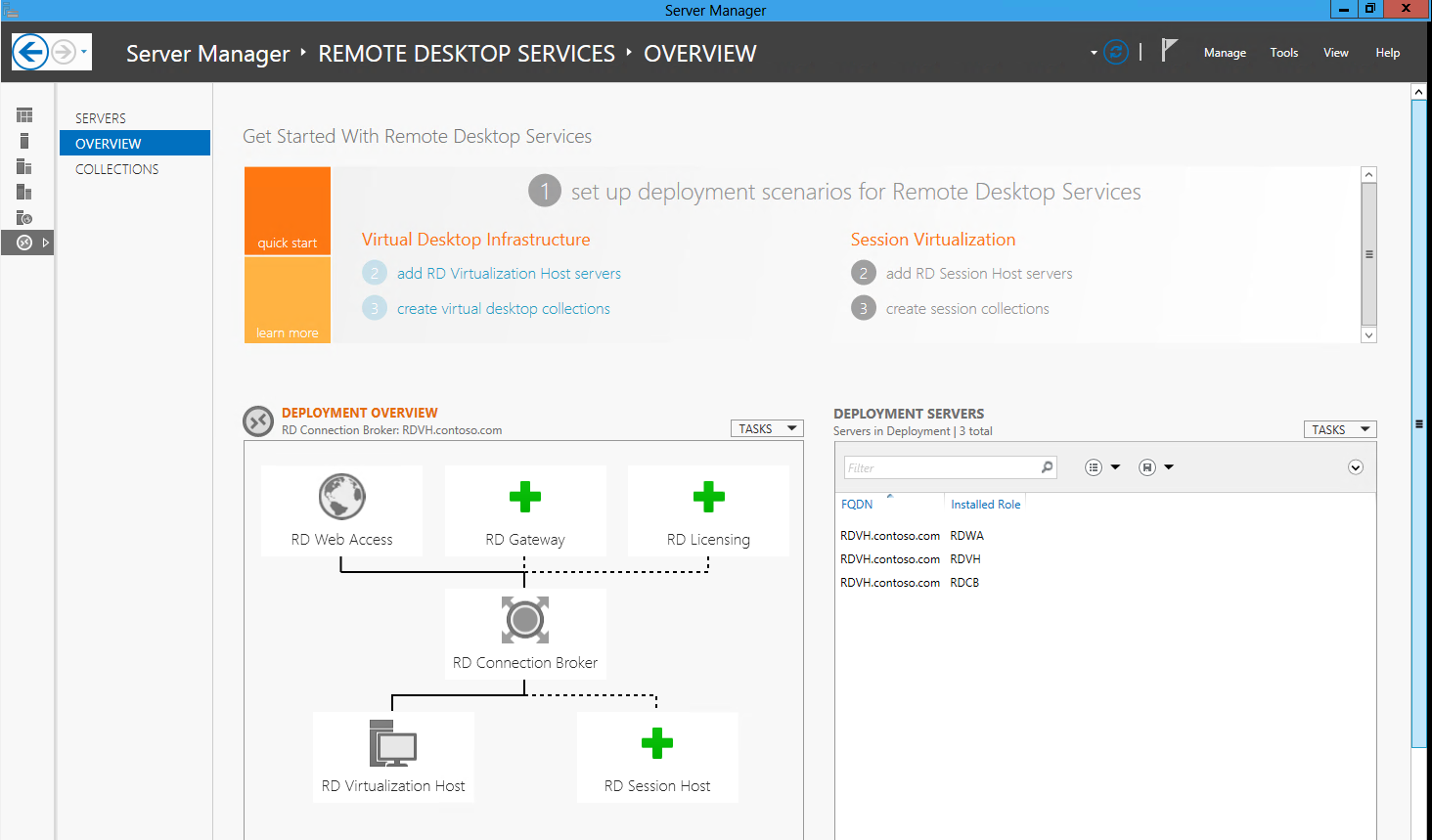
新しい Windows Server "8" Beta サーバー マネージャーのプラグインである RDMS では、検出プロセスによって、サーバー マネージャーのプールに追加された各コンピューター上にインストールされている役割サービスが検出されます。リモート デスクトップ サービスのシナリオ ベースのインストールを実行して、役割サービスが検出されると、RDMS によって、RDS 環境の基本的なトポロジの図と、各サーバーに関する情報 (サービス ステータス、関連イベント、パフォーマンス情報、各役割サービスに関するベスト プラクティス アナライザーの結果など) が表示されます。

|  |  |
| --- | --- |
| 重要: | Windows Server "8" Beta では、リモート デスクトップ サービス マネージャー、リモート デスクトップ セッション ホストの構成、接続ブローカーの構成用接続マネージャー インターフェイスなどの、従来のリモート デスクトップ管理ツールに替わるものとして、RDMS 管理コンソールが導入されました。これまでこれらのツールを使用して実行されていた管理機能はすべて、サーバー マネージャーの RDMS プラグインを使用して実行されるようになりました。 |

###### コレクション

RDMS では、コレクションという概念が導入されています。コレクションは、セッションの仮想化 (リモート デスクトップ セッション ホスト) を提供する仮想マシンまたはサーバーの論理グループとして定義されます。コレクションの初期プロパティを定義してコレクションを作成すると、そのコレクション固有の設定を RDMS によって管理できます。次のスクリーンショットは、リモート デスクトップ管理サービス インターフェイスのホームページを示しています。

図 1: リモート デスクトップ管理サービス



RDMS を使用したリモート デスクトップ環境の管理方法の具体的な詳細は、このドキュメントの「リモート デスクトップ サービスの構成と管理」、「リモート デスクトップ サービスのアーキテクチャ」、および「トラブルシューティング」のセクションで説明します。

##### リモート デスクトップ セッション ホスト

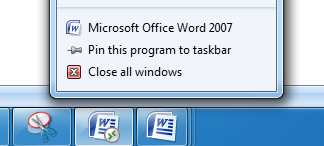
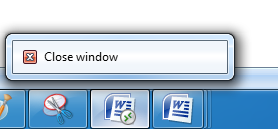
以下のセクションでは、リモート デスクトップ セッション ホストの役割サービスを展開すると有効になる新機能の概要を説明します。

###### RemoteApp の機能強化

Windows 7 では、アプリケーションのグループ化、タスク バーへの表示、ジャンプ リスト、タブ付きウィンドウ、進行状況、およびアイコン オーバーレイといった新しいシェル機能が導入されましたが、RemoteApp はこれらの機能と完全に互換ではありませんでした。Windows Server "8" Beta では、シェルの完全な互換性を目指して、以下のような機能が RemoteApp に追加されています。

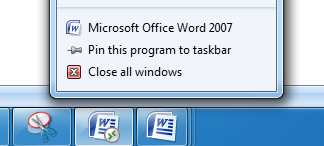
**タスク バーへの表示:** ユーザーは RemoteApp アプリケーションをクライアントのタスク バーに表示できます。

図 2: RemoteApp のタスク バーへの表示



**RemoteApp とワークスペースのアイコン:** ユーザーは一意のアイコンによって RemoteApp とワークスペースを識別できます。このアイコンは、リモート デスクトップのロゴがアプリケーションのアイコンに重なった形になります。

図 3: RemoteApp の識別子



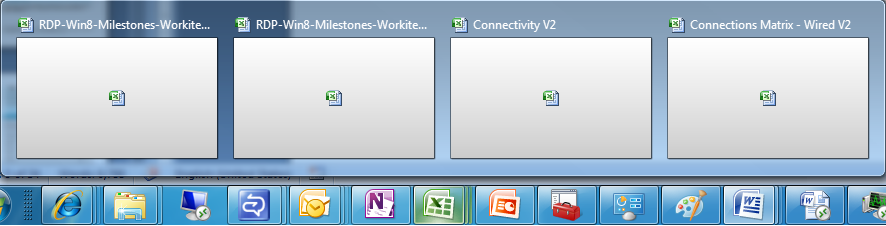
**アイコン オーバーレイ:** ユーザーはアイコン オーバーレイがリモートになることで、アプリケーションの状態の変更を見ることができます。

図 4: アイコン オーバーレイのリモート表示



**タブ付きウィンドウ:** ユーザーは RemoteApp 縮小表示プレビューで複数のタブを確認して、アプリケーションの複数インスタンスを区別できます。

図 5: タブ付きウィンドウ



**正規アイコン:** アプリケーションがローカルにインストールされて実行されているかのように、ユーザーには常にアプリケーションの正規アイコンが表示されます。

図 6: 正規アイコン



###### CPU、ディスク、およびネットワークのフェアシェア

Windows Server "8" Beta のリモート デスクトップ サービスは、Windows Server 2008 R2 に搭載されていたテクノロジに基づいて実装され、ネットワーク帯域幅を制御するための新機能が追加されています。CPU、ディスク、およびネットワークのフェアシェア テクノロジは、既定で有効になっていますが、グループ ポリシーを使用して無効にできます。

**CPU フェアシェア**

リモート デスクトップ セッション ホストのような対話型のマルチユーザー環境では、動的に作成および削除されるセッションに基づき、セッション境界を越えて利用可能な CPU の負荷を分散させる能力が必要です。これは、アクティブなすべてのセッションで一貫したユーザー エクスペリエンスを保証するために必要とされます。この機能は、Windows Server 2008 R2 に含まれていた動的フェアシェア スケジューリング テクノロジ (DFSS) の上に構築されています。

**ディスク フェアシェア**

RDSH のディスクを大量に消費するプロセスは、多くのディスク領域を使用しないユーザー プロセスのためのリソースまで使用して、こうしたプロセスからディスクを使用するチャンスを一切奪ってしまう可能性があります。ディスク フェアシェア機能は、このような事態を緩和するために、異なるセッション間でディスク アクセスを分散させるように試みます。

ディスク フェアシェア機能の総合的な目標は、複数の RDSH セッションがディスクを公正に共有できるようにすることです。ディスク フェアシェアの主な 2 つの機能は、I/O 負荷の均等な分散 (I/O バランサー機能) と過度なディスク使用の調整です。

**ネットワーク フェアシェア**

リモート デスクトップおよび複数セッションは、ネットワーク帯域幅を使用します。1 つのセッションで帯域幅を大量に消費するアプリケーションが実行されると、他のセッションは帯域幅不足になる可能性があります。ネットワーク フェアシェア機能は、ネットワーク帯域幅がセッション間で不公正に消費されるのを防止するために、複数セッション間で利用可能な帯域幅をラウンド ロビン方式で使用するように調整します。

ネットワーク フェアシェア機能の目標は、複数のリモート セッション間で利用可能なネットワーク帯域幅を公正に分割することです。集中コンピューティングのシナリオでは、異なるクライアント セッション間でネットワーク インターフェイス帯域幅の負荷を公正に分散させるためには、これらのクライアント セッション間での動的負荷分散が必要とされます。

###### USB リダイレクト

リモート セッションでは、ユーザーは必要な任意のデバイスを有効に使用できることが必要とされます。Windows Server 2008 R2 リモート デスクトップ サービスは現在、特定の種類のデバイスをリモート セッションで効果的に使用することを可能にする多数のハイレベルなリダイレクト機能を備えていますが、お客様がリモート セッションでの使用を求めているすべての種類のデバイスはカバーされていません。このニーズに対応するために、Windows 7 SP1 および Windows Server 2008 R2 SP1 では RemoteFX VDI のシナリオで使用するための RemoteFX USB リダイレクト機能が搭載されました。特定の種類のデバイスだけをリダイレクトするドライブ リダイレクトといったハイレベルなリダイレクトとは異なり、USB リダイレクトはポート プロトコル (USB 要求ブロックまたは URB) のレベルで実行され、多数の種類の USB デバイスをリダイレクトする包括的なメカニズムとして機能します。以下の表では、これら 2 つのリダイレクト形式を比較しています。

表 1: USB リダイレクトとハイレベルなリダイレクト

| **USB リダイレクト** | **RDP ハイレベル デバイス リダイレクト** |
| --- | --- |
| クライアント上のドライバーは不要です。 | クライアント上にインストールされるデバイスのドライバーが必要です。 |
| サーバー上にデバイス ドライバーをインストールすることが必要です。 | 一般的にサーバー上のドライバーは不要です。 |
| 多数の種類のデバイスに 1 つのリダイレクト方法を使用します。 | リダイレクトされる各種類のデバイスに特定の固有の方法を使用します。 |
| RDP 接続を通してデバイスへ、およびデバイスから、URB を転送します。 | 該当するデバイスの種類に対して最適化されたプロトコルを使用することで、リモート セッションでハイレベルなデバイス機能を公開します。 |
| 一度に 1 つのセッションだけがデバイスを使用できます。RDP セッションがデバイスを使用している間は、ローカル クライアントはデバイスを使用できません。 | ローカル クライアントを含む任意の数のセッションが同時にデバイスにアクセスできます。 |
| LAN 用に最適化されています。 | LAN と WAN の両方で有効です。 |

Windows Server "8" Beta では、USB リダイレクトに以下のようないくつかの機能拡張が行われています。

* USB リダイレクトでは、RemoteFX 3D ビデオ アダプターはもはや不要です。
* USB リダイレクトは以下の SKU で有効になっています。
  + Windows 8 Consumer Preview
  + RDSH の役割がインストールされた Windows Server "8" Beta
* さらに、RDSH 上での USB デバイスへのアクセスは、そのデバイスをリダイレクトしたセッションに対して分離されます。つまり、他のセッションのユーザーは、そのデバイスにアクセスできなくなります。

RDP セッションで使用できるデバイスの一覧を以下に示します。

表 2: デバイスの一覧とリダイレクト方法

|  |  |  |  |
| --- | --- | --- | --- |
| **デバイス** | **状況** | **物理および仮想クライアントのリダイレクト方法** | **RDSH のリダイレクト方法** |
| **プリンター複合機** | 使用可能 | USB リダイレクト | USB リダイレクト |
| **プリンター** | 使用可能 | Easy Print | Easy Print |
| **スキャナー** | 使用可能 | USB リダイレクト | USB リダイレクト |
| **生体認証** | セッション中に 使用可能  ログオン時は使用不可 | USB リダイレクト | USB リダイレクト |
| **PTP カメラ** | 使用可能 | プラグ アンド プレイ  デバイスのリダイレクト | プラグ アンド プレイ  デバイスのリダイレクト |
| **MTP メディア プレーヤー** | 使用可能 | プラグ アンド プレイ  デバイスのリダイレクト | プラグ アンド プレイ  デバイスのリダイレクト |
| **Web カメラ** | 使用可能  (LAN のみ) | USB リダイレクト | USB リダイレクト |
| **VoIP 電話およびヘッドセット** | 使用可能  (LAN のみ) | USB リダイレクト | オーディオ リダイレクト |
| **オーディオ (USB 複合デバイス以外)** | 使用可能 | オーディオ リダイレクト | オーディオ リダイレクト |
| **CD または DVD ドライブ** | 読み取り操作で使用可能 | ドライブ リダイレクト | ドライブ リダイレクト |
| **ハード ドライブまたは USB フラッシュ ドライブ** | 使用可能 | ドライブ リダイレクト | ドライブ リダイレクト |
| **スマート カード リーダー** | 使用可能 | スマート カード  リダイレクト | スマート カード  リダイレクト |
| **USB シリアル** | 使用可能 | USB リダイレクト | USB リダイレクト |
| **USB ネットワーク アダプター (一部の携帯情報端末も含む)** | ブロック対象 | N/A | N/A |
| **USB ディスプレイ** | ブロック対象 | N/A | N/A |
| **USB キーボードまたは マウス** | 使用可能 | 入力のリダイレクト | 入力のリダイレクト |

**ハードウェアおよびソフトウェア要件**

リモート デスクトップ セッション ホストのシナリオにおける USB リダイレクトの要件は次のとおりです。

* クライアント: Windows 8 Consumer Preview (推奨) または Windows 7 SP1 と RDC 8
* サーバー: Windows Server "8" Beta

ゲスト仮想マシンとして Windows Server "8" Beta を使用する仮想化シナリオ (リモートデスクトップ/VDI)

* RDSH の役割がインストールされた Windows Server "8" Beta (推奨)

さらに、どの場合も、前述の表の中でリダイレクト方法として "USB リダイレクト" と示されているデバイスが最低 1 台必要になります。

###### ユーザー プロファイル ディスク

以前のバージョンの Windows では、リモート デスクトップ セッション、または VDI を使用して展開された仮想マシンのユーザー状態の保存には、移動プロファイルとフォルダー リダイレクトが使用されていました。確かに、この方法でユーザー状態を保存することは可能ですが、これらのテクノロジの使用にはいくつか欠点がありました。

* 一部のアプリケーションでは、ユーザー プロファイルの外部の場所にユーザー データやアプリケーション固有データが書き込まれます。
* 移動プロファイルとフォルダー リダイレクトは、特に併用した場合、それらの構成と展開が複雑になることがあります。
* 一部のユーザーは、プールされた VM を使用できません。ローカル プロファイルを使用できるようにするために、プールされた VM の代わりに個人用 VM を使用する必要があります。
* プロファイルがネットワーク経由でロードされるため、ログオンに時間がかかることがあります。
* 移動プロファイルが RDS 環境の外部 (物理コンピューターなど) で使用されている場合、プロファイルが使用不能な状態になったときにデータが損失する可能性があります。

Windows Server "8" Beta では、管理者が、ネットワーク共有上に格納される単一の vhd ファイルにユーザー データとアプリケーション データを格納するように、環境を構成することができます。ユーザー プロファイル ディスクによって、コストが削減され、複雑さが緩和されると共に、ユーザー プロファイルに書き込まれないアプリケーション データの問題を解決できます。また、移動プロファイル、フォルダー リダイレクト、およびユーザー プロファイル ディスクを組み合わせたソリューションを使用して、どのアプリケーションのデータをユーザー プロファイル ディスクに格納し、どのアプリケーションのデータをユーザー プロファイルまたはリダイレクト フォルダーに格納するかを詳細に制御することもできます。

##### リモート デスクトップ クライアント

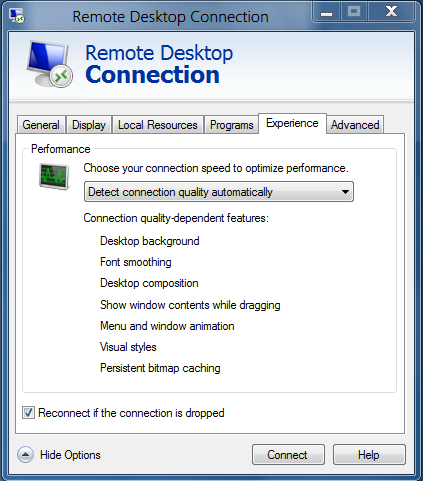
リモート デスクトップ クライアントは Windows のサーバーおよびクライアント の両方に搭載されています。Microsoft VDI を使用して展開されている仮想マシンに接続したり、リモート デスクトップ セッション ホスト サーバーから RemoteApp を実行したり、Windows クライアント コンピューターへのリモート デスクトップ接続を行ったりするには、リモート デスクトップ セッション ホスト サーバーへの RDP 接続を行う必要があります。これまで、リモート デスクトップ クライアントは、RDP プロトコルでサポートされる新機能と各 Windows Server バージョンの新機能をサポートするために、Windows リリース毎にアップグレードされてきました。

Windows Server "8" Beta のいくつかの新しい機能は、Windows 8 Consumer Preview と Windows Server "8" Beta に含まれる RDC クライアントを使用して接続を行う場合のみ機能します。

###### 接続品質の自動検出

RDC 8 は Windows Server "8" Beta サーバーまたは Windows 8 Consumer Preview クライアントへの接続の品質を検出し、この検出の結果に基づいてパフォーマンス設定を調整します。[エクスペリエンス] タブの [パフォーマンス] 設定セクションには、[接続品質の自動検出] という新しいオプションが追加されています。この設定を選択すると、接続品質に依存する特定の機能は、参照用に表示されるだけで、選択できなくなります。

図 7: 接続品質の自動検出



###### 帯域幅の状況の表示

RDC クライアントを全画面表示モードで実行すると、現在の帯域幅を示すポップアップ ウィンドウと視覚的なインジケーターの両方に、接続時に検出された帯域幅が表示されるようになりました。帯域幅は、信号強度メーターによく似たアイコンで表示されます。次の表に、検出された帯域幅によって表示されるアイコンがどのように変化するかを示します。

表 3: 帯域幅の状況の表示

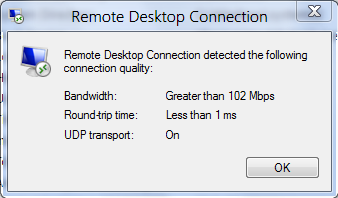
| **帯域幅** | **待機時間** | **アイコン** |
| --- | --- | --- |
| 10 Mbps 以上 | 任意の値 | 4 つのバー 説明: C:\Users\casdvor\Pictures\BBar Icons\Bandwidth\four_bar.png |
| 2,000 ～ 9,999 Kbps | 任意の値 | 3 つのバー 説明: C:\Users\casdvor\Pictures\BBar Icons\Bandwidth\three_bar.png |
| 512 ～ 1,999 Kbps | 任意の値 | 2 つのバー 説明: C:\Users\casdvor\Pictures\BBar Icons\Bandwidth\two_bar.png |
| 512 Kbps 未満 | 任意の値 | 1 つのバー 説明: C:\Users\casdvor\Pictures\BBar Icons\Bandwidth\one_bar.png |
| ダウンレベル サーバーまたは帯域幅の検出なし | 任意の値 | 非表示、アイコンは表示されない |

図 8: RDC 帯域幅の監視機能



アイコンをクリックすると、ポップアップ ウィンドウに現在の帯域幅の詳細が表示されます。

図 9: 帯域幅の詳細

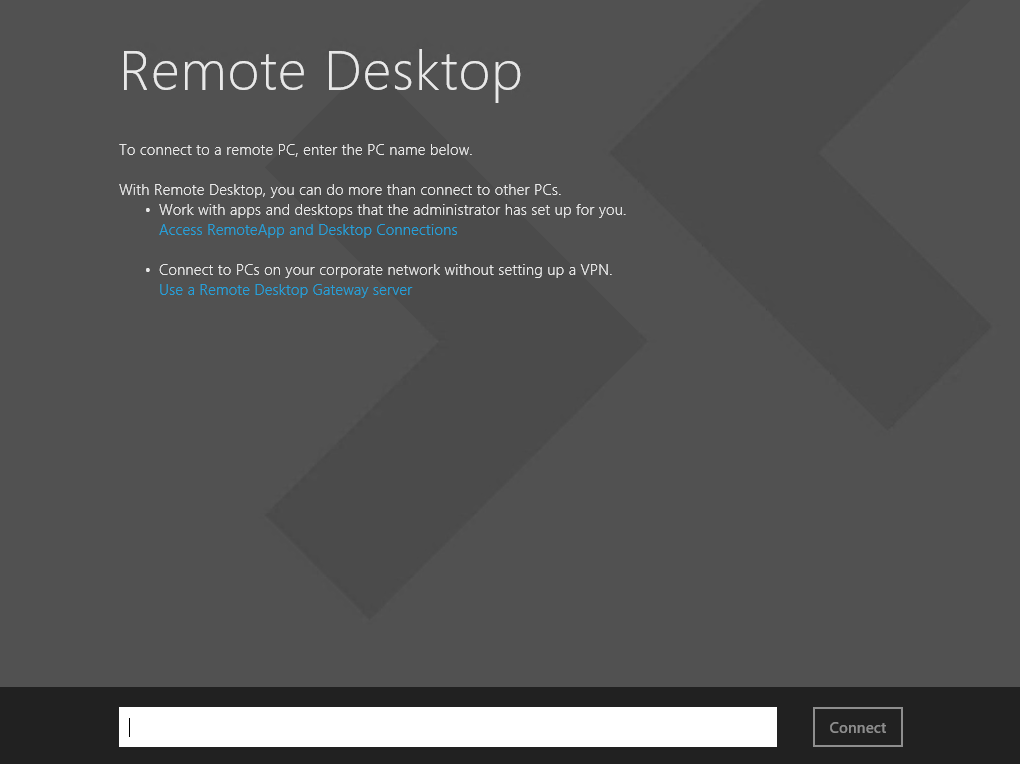


##### 最新のリモート デスクトップ接続 クライアント

Windows 8 Consumer Preview には、最新の Metro スタイルの RDC クライアントとクラシック RDC クライアントの両方が含まれています。どちらの RDC クライアントにも同じ機能が含まれていますが、クラシック RDC クライアントは高度なユーザーを対象としてより詳細な設定を搭載している一方、Metro スタイルの RDC クライアントはエンド ユーザーを対象としています。

Metro スタイルの RDC クライアントは、タッチ式の使いやすいユーザー インターフェイス、タッチとジェスチャのリモート処理、および Windows Server "8" Beta のリモート デスクトップ サービスの全アプリケーション発行機能の完全な統合を提供します。

図 10: 最新のリモート デスクトップ クライアント



##### リモート デスクトップ接続ブローカー

以下のセクションでは、Windows Server "8" Beta におけるリモート デスクトップ接続ブローカーの新機能の概要について説明します。

###### 発行データの一元化

Windows Server 2008 R2 の VDI の環境では、Active Directory を使用してユーザーとコンピューターの割り当てを格納し、アクティブな接続ブローカーが個人用およびプールされたデスクトップのために仮想マシンの調整を行って、リモート接続を処理していました。このモデルの制限事項の 1 つに、一度に 1 つの接続ブローカーだけしかアクティブにできない、ということがありました。

Windows Server "8" Beta では、スケールと構成しやすさを向上させるために、一度に複数のアクティブなブローカーが存在することが可能な、一元化されたデータベースが導入されています。アクティブなブローカーが複数存在できることは、ビジネスおよびエンタープライズ向けの VDI ソリューションの拡張に大いに役立つと同時に、企業や管理者による展開を一段と容易にします。

新しい一元化されたデータベースでは、Windows Server 2003 以来使用されてきた Jet データベースを使用する代わりに、Windows Server の組み込みの Windows Internal Database コンポーネントが使用されています。このデータベースには次のような異なる種類のデータが含まれます。

* 仮想デスクトップ インフラストラクチャ (VDI)
* リモート デスクトップ セッション ホスト (RDSH)
* アプリケーションの発行
* RD ゲートウェイ
* RD ライセンス

###### 可用性の高い接続ブローカー

Windows Server 2003 でのセッション ディレクトリの導入以来、リモート デスクトップ接続ブローカー サービスはフェールオーバー クラスタリングの使用をサポートして、可用性に優れたソリューションを構築してきました。Windows Server 2008 R2 の高可用性接続ブローカーには、次のような欠点がありました。

* 一度に 1 つのアクティブ ブローカーのみ可能 (アクティブ/パッシブ構成)。
* 高可用性接続ブローカーのインストールおよび構成プロセスが複雑で、フェールオーバー クラスタリングに依存するため、手動の手順が多数存在した。
* DNS ラウンド ロビンは接続ブローカー サービスの状態がわからず、停止しているサーバーにユーザーをルーティングする可能性があった。

Windows Server "8" Beta の接続ブローカーでは、Windows Server 2008 R2 モデルと比較して、次の点が強化されています。

* 複数のアクティブな接続ブローカーがサポートされるようになった (アクティブ/アクティブ構成)。
* フェールオーバー クラスタリングは使用されなくなったので、セットアップと展開が大幅に簡素化され、ほとんどの構成が自動化されている。
* アクティブな接続ブローカーが複数あるので、接続ブローカー ノードの 1 つに障害が発生しても、クライアントは必ず、機能している接続ブローカーに確実にルーティングされる。

##### リモート デスクトップ Web アクセス

Windows Server 2008 R2 では大幅に強化された RDWeb インターフェイスが導入されましたが、これは Windows Server "8" Beta でさらに強化されています。強化の内容は、次のとおりです。

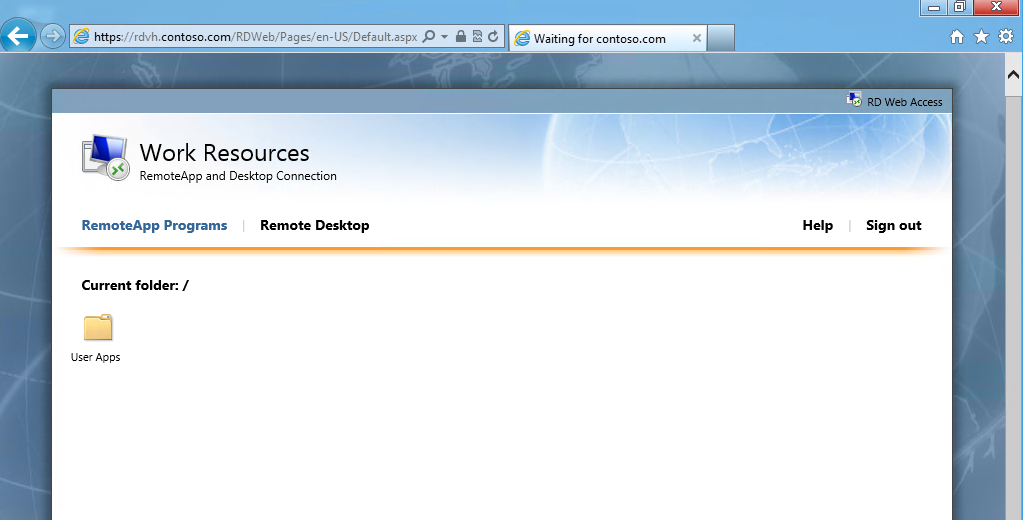
* RDWeb フォルダー
* フィード経由の RDWeb
* ワークスペースの自動検出とサインアップ
* ワークスペースのシングル サインオン
* 期限切れパスワードのサポート

###### RDWeb フォルダー

RDWeb は現在、ユーザーが利用できるアプリケーションを論理的にグループ化することはできません。Windows Server 2008 R2 には、ユーザーとグループに基づいて RemoteApp をフィルターする機能が搭載されていますが、RDWeb ページに複数ページのアイテムを持つユーザーはスクロールしてアプリケーションを見つける必要があり、アプリケーションはアルファベット順にのみグループ化できます。このため、アプリケーションの正確な名前を知らないユーザーは、適切なアプリケーションをなかなか見つけることができず、特定の種類のアプリケーションに絞り込むのさえ困難となっています。

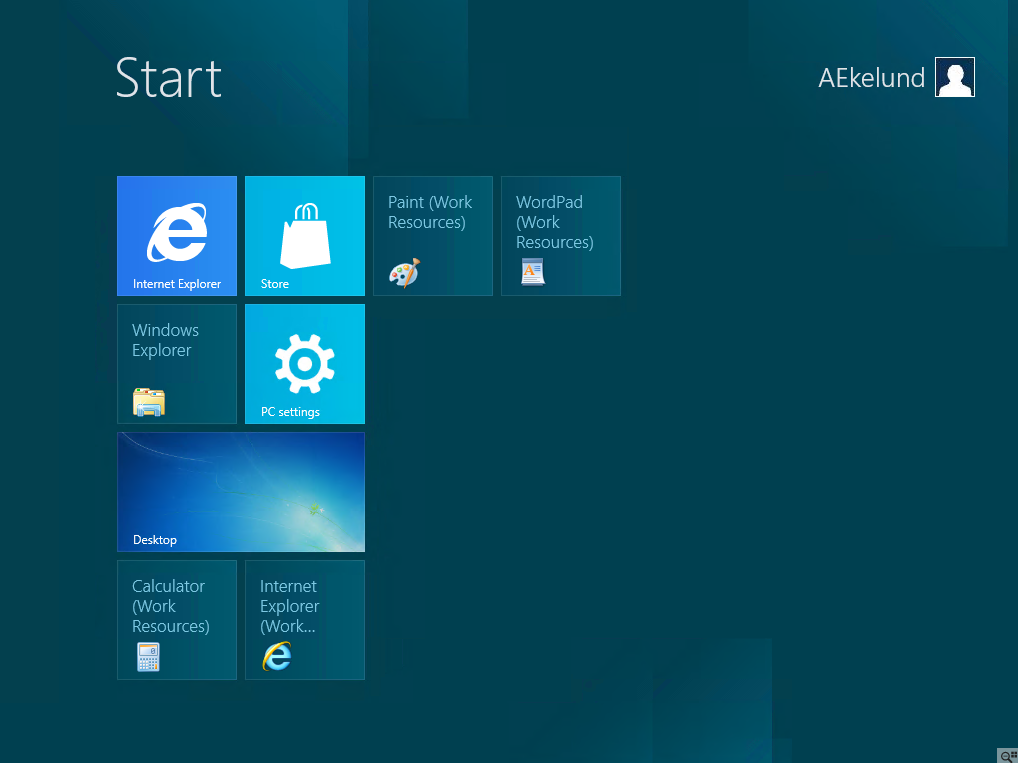
Windows Server "8" Beta の RDWeb は、RemoteApp をフォルダー別にグループ化し、RDWeb ページ上でフォルダー内にそれらを表示するオプションを備えています。

図 11: RDWeb フォルダー



また、ユーザーが RDWeb アプリケーション フィードに接続していると、スタート画面でもアプリケーションをグループ化できます。

図 12: スタート画面の RDWeb フォルダー



###### RDWeb フィード

Windows Server 2008 R2 では、次の 4 つの方法でアプリケーションをエンド ユーザーに発行できました。

* RDWeb (サポートおよび推奨されている方法)
* RemoteApp およびデスクトップ接続を介した [スタート] メニューへの RDWeb フィード (RDWeb のサポートされている代替または補完的方法)
* MSI によって展開された RDP ファイル
* 電子メールまたは SMB 共有を介した RDP ファイル (推奨されない、管理者はこれを手動で実行しなければならない)

これらのうち、MSI 展開方法は Windows Server "8" Beta では使用できなくなりました。Windows Server "8" Beta では、RemoteApp とデスクトップ接続機能が使用するのと同じ XML フィード データを使用するように RDWeb がアプリケーションの Web ページを構築する方法を変更することで、サポートされている 2 つの方法がまとめられています。これによって次の利点がもたらされます。

* RDWeb に新しい機能をより簡単に追加できます。
* 慣れていない管理者でも、シンプルなスタイル シート エディターまたは XSLT タイプのエディターを使用して、既定の Web サイトのページ変更をより簡単に行うことができます。Windows Server 2008 R2 の場合、管理者は、アイコンやイメージ ファイルを表すディスク上のファイルを交換するか、aspx ファイルを開いてテキストを編集する必要があります。しかし、Windows Server "8" Beta で加えられた変更により、管理者は GUI スタイル シートや XSLT エディターの多くを使用してページを変更できるようになっています。
* パートナー様は拡張ソリューションを簡単かつ柔軟に実装できます。

###### ワークスペースの自動検出とサインアップ

Windows 7 クライアントを使用して Windows Server 2008 R2 のクライアント コンピューターにワークスペースを追加するのは、エンド ユーザーにとって容易な作業ではありません。Windows Server 2008 R2 では、ユーザーは次の 2 とおりの方法で Windows 7 クライアントにワークスペースを追加できます。

* ネットワーク管理者がユーザーに特殊なファイル (セットアップ ファイル) を提供する。
* 手動で入力して接続をセットアップできる URL を、ユーザーがネットワーク管理者から入手する。

ワークスペースの自動検出とサインアップは、Windows Server 2008 R2 の方法の問題を回避しながら、プロビジョニングされたワークスペース フィードへのアクセスをユーザーが得るためのより簡単な方法です。この機能を使用すると、ワークスペース リソースを自分のコンピューターに配信するためにユーザーが知っておく必要があるのは、会社の電子メール アドレス (既定の SMTP プロキシ アドレス) だけで済みます。管理対象の企業ドメインに参加しているコンピューターの場合は、管理者はグループ ポリシーを設定してコンピューターの既定のワークスペースを設定できます。

###### ワークスペースのシングル サインオン

シングル サインオン (SSO) は、ユーザーが自分のコンピューターでユーザー名とパスワードを一度入力すると、ユーザーが要求する RDP 接続へのサインオンにそれらの資格情報を使用できる機能です。Windows Server 2008 R2 には、次の 2 つの形式の SSO があります。

* シングル サインオン (資格情報の委任、コンピューターがドメインに参加していることが必要)
* Web シングル サインオン (RDWeb 接続を通して実装、コンピューターがドメインに参加していることは不要)

既存のシングル サインオン ソリューションは、ユーザー エクスペリエンスと管理者エクスペリエンスに分類できます。

**ユーザー エクスペリエンス**

Windows Server 2008 R2 では、ユーザーは接続プロセス時にユーザー名とパスワードの入力を何回も求められる場合があります。RDWeb、RD ゲートウェイ、リダイレクター (VDI または専用ファーム リダイレクトの場合)、あるいは RDSH サーバー (RDSH または RDVH ゲスト) が、ユーザーに資格情報を求める可能性があります。

Windows Server "8" Beta は、ユーザーにユーザー名とパスワードの入力を一度だけ求め、前述のすべての RDP エンドポイントに対する接続プロセスにその情報を使用することで、シングル サインオン ユーザー エクスペリエンスを向上させます。接続プロセス時にユーザー名とパスワードはセキュリティで保護されるので、侵害されることはありません。

ユーザーも、何回もポップアップ表示される警告ダイアログ、プロンプト、または情報ダイアログに応答する必要がなくなり、ローカル アプリケーションと同じように RemoteApp を使用することが可能になります。

**管理者エクスペリエンス**

Windows Server 2008 R2 では、管理者は RDS 環境内で SSO をセットアップするプロセスで、シナリオを有効にするために、多くの場合は複雑なアクションを何回も実行する必要があります。アクションの回数は、環境の構成と複雑さによって決まります。Windows Server "8" Beta では、管理者は簡単な方法でリモート デスクトップ環境を構成して、シングル サインオンを有効にし、不要なポップアップ、プロンプト、またはユーザー名とパスワードの入力ダイアログが表示されることなくユーザーが RemoteApp とリモート デスクトップに接続できるように設定できます。

##### リモート デスクトップ ゲートウェイ

リモート デスクトップ ゲートウェイ (RD ゲートウェイ) は、以前ターミナル サービス ゲートウェイ (TS ゲートウェイ) と呼ばれていたもので、Windows Server "8" Beta に付属しているリモート デスクトップ サービスの役割です。この役割によって、許可されたリモート ユーザーは、リモート デスクトップ接続 (RDC) クライアントの実行が可能な任意のインターネット接続デバイスから社内ネットワークやプライベート ネットワーク上のリソースに接続できます。この場合、ネットワーク リソースは、リモート デスクトップ セッション ホスト (RDSH) サーバー、RemoteApp プログラムを実行する RD セッション ホスト サーバー、またはリモート デスクトップが有効に設定されているコンピューターおよび仮想デスクトップです。RD ゲートウェイは、RDP over HTTPS を使用して、インターネット上のリモート ユーザーと内部ネットワーク リソースとの間で、セキュリティで保護された暗号化接続を確立します。

###### UDP プロトコルのサポート

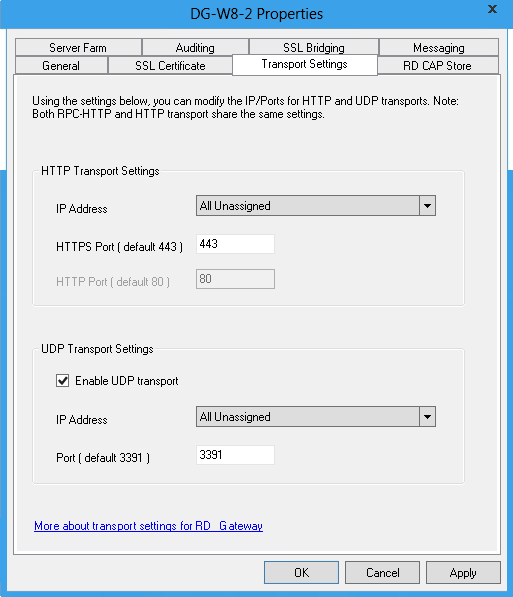
Windows Server "8" Beta のリモート デスクトップ ゲートウェイ (RDG) では、新たな RDP WAN 対応転送機能などの、RDP プロトコルの拡張機能が利用されます。Windows Server "8" Beta の RDG は、UDP を使用した接続のサポートの追加を通じて、待機時間が長いネットワーク上のリアルタイム トラフィックをサポートします。クライアントまたはエンドポイントで UDP がサポートされていない場合、Windows Server "8" Beta の RDG は HTTP プロトコルに戻り、このプロトコルを使用します。

UDP トランスポートを使用することで、ユーザーの物理的な場所やネットワークの特性にかかわらず、リモート デスクトップ ゲートウェイを介した接続のユーザー エクスペリエンスが向上します。管理者がリモート デスクトップ ゲートウェイで UDP プロトコル オプションを有効にしてあり、クライアントと RDP エンドポイントで UDP 接続がサポートされている場合、使用できる最適なトランスポート プロトコルの選択プロセスが、ユーザーに意識されることなく実行されます。

###### リモート デスクトップ ゲートウェイのユーザー インターフェイス

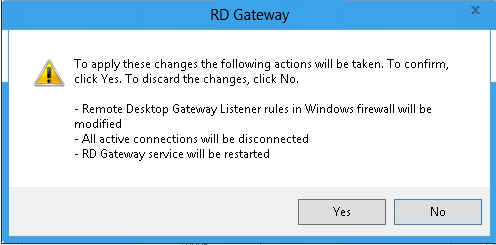
リモート デスクトップ ゲートウェイ マネージャーは、UDP トランスポートの新しい設定とポートの設定オプションを反映するように更新されました。以下に、[トランスポート] タブの新しい設定を示します。

図 13: RDG マネージャーのトランスポート設定



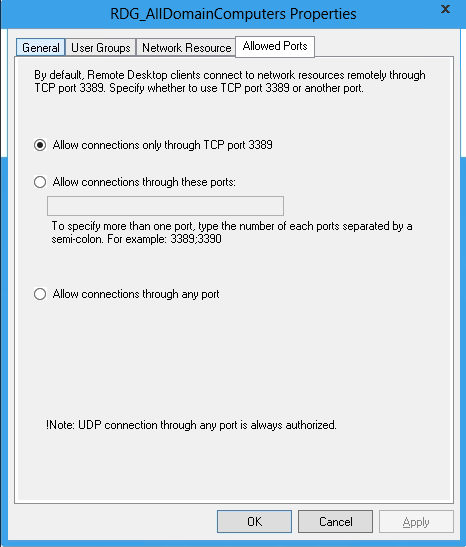
ユーザーがポートの設定を選択して [適用] をクリックすると、ファイアウォールの設定も変更されることがユーザーに通知されます。ユーザーはこれらの設定を確認するように求められます。

図 14: ファイアウォールの設定の確認



リモート アクセス ポリシー (RAP) のプロパティのダイアログでも、UDP トランスポートの有効化時に通知が表示されます。

図 15: RAP のプロパティ



##### リモート デスクトップ ライセンス

リモート デスクトップ ライセンス (RD ライセンス) は、以前ターミナル サービス ライセンス (TS ライセンス) と呼ばれていたもので、この機能によって、各デバイスまたはユーザーがリモート デスクトップ セッション ホスト (RD セッション ホスト) サーバーに接続するときに必要となるリモート デスクトップ サービスのクライアント アクセス ライセンス (RDS CAL) が管理されます。リモート デスクトップ ライセンス サーバーで RDS CAL のインストール、発行、および可用性の追跡を行うには、RD ライセンス機能を使用します。

|  |  |
| --- | --- |
| 注意: | ターミナル サーバーは、Windows Server 2008 R2 から RD セッション ホスト サーバーと呼ばれるようになりました。また、ターミナル サービス クライアントのアクセス ライセンス (TS CAL) は、リモート デスクトップ サービスのクライアント アクセス ライセンス (RDS CAL) と呼ばれるようになりました。このドキュメントでは、以前のバージョンの Windows Server について言及しているときでも、これらの新しい用語を使用します。セキュリティ グループ名については、Windows Server "8" Beta での変更はありません。 |

クライアント (ユーザーまたはデバイス) が RD セッション ホスト サーバーに接続しようとすると、接続先の RD セッション ホスト サーバーによって、RDS CAL が必要かどうかが判断されます。その後、RD セッション ホスト サーバーは、このサーバーに接続しようとしているクライアントに代わって、リモート デスクトップ ライセンス サーバーに RDS CAL を要求します。ライセンス サーバーから適切な RDS CAL を取得できる場合は、その RDS CAL がクライアントに発行され、クライアントは RD セッション ホスト サーバーに接続できるようになります。

ライセンスの猶予期間中はライセンス サーバーは不要ですが、猶予期間が終了すると、クライアントは RD ライセンス サーバーが発行した有効な RDS CAL を事前に取得してからでないと、RD セッション ホスト サーバーにログオンできません。

|  |  |
| --- | --- |
| 重要: | リモート デスクトップでは、コンピューターのリモート管理のための 2 つの同時接続をサポートしています。これらの接続については、ライセンス サーバーは必要ありません。 |

また、リモート デスクトップ サービスを使用するためには、環境内に少なくとも 1 つのライセンス サーバーが展開されていることが必要です。小規模環境では、RD セッション ホストの役割サービスと RD ライセンスの役割サービスの両方を同じコンピューターにインストールできます。大規模環境では、RD セッション ホストの役割サービスのインストール先とは別のコンピューターに RD ライセンスの役割サービスをインストールすることをお勧めします。

RD セッション ホスト サーバーがクライアントからの接続を受け入れるようにするには、RD ライセンスを正しく構成する必要があります。ライセンス サーバーの展開のための時間を十分に確保できるように、リモート デスクトップ サービスでは、ライセンス サーバーを必要としない、RD セッション ホスト サーバーのライセンスの猶予期間を設けています。この猶予期間中、RD セッション ホスト サーバーは、ライセンス サーバーにはアクセスせず、ライセンスのないクライアントからの接続を受け入れます。この猶予期間は、RD セッション ホスト サーバーがクライアントからの接続を初めて受け入れたときを開始点とします。猶予期間は、次のいずれかが初めて発生したときに終了します。

* ライセンス サーバーによる、RD セッション ホスト サーバーに接続するクライアントへの恒久 RDS CAL の発行
* 猶予期間の満了

猶予期間の長さは、RD セッション ホスト サーバー上で実行されているオペレーティング システムに基づきます。以下に猶予期間を示します。

表 4: RDS ライセンスの猶予期間

| **RD セッション ホスト サーバー上で 実行されているオペレーティング システム** | **猶予期間** |
| --- | --- |
| Windows Server "8" Beta | 120 日 |
| Windows Server 2008 R2 | 120 日 |
| Windows Server 2008 | 120 日 |
| Windows Server 2003 | 120 日 |

##### コア RDP プロトコルの機能強化

以下のセクションでは、コア RDP プロトコルの機能強化、および RDP 8 への RemoteFX テクノロジの統合について説明します。

###### RemoteFX 統合

Windows Server "8" Beta では、リモート デスクトップの機能セット全体に RemoteFX テクノロジが統合されており、役割サービスを別にインストールする必要はありません。Windows Server "8" Beta におけるこれらの新機能の概要について以下に説明します。

###### WAN 対応 RemoteFX

Windows Server "8" Beta における WAN 対応 RemoteFX 機能の目標は、ユーザーがブランチ オフィスにいる場合や、ワイヤレス デバイスを使用している場合、WAN 接続を介して自宅で作業を行っている場合など、企業ネットワークの外部でも、すばらしいユーザー エクスペリエンスを実現することです。

WAN 対応 RemoteFX では、RemoteFX アダプティブ グラフィックス機能に新しいインテリジェントな WAN 対応転送が組み合わされています。TCP と UDP の両方が使用できるようになり、これらのプロトコルが自動的に選択されます。また、ネットワーク状態の自動検出によって、コンテンツのエンコーディングがネットワークに合わせて調整されます。

###### RemoteFX アダプティブ グラフィックス

Windows Server "8" Beta の RemoteFX は、ネットワークの状態の変化に動的に対応し、配信するコンテンツに基づいてエンコーディングを最適化します。Windows Server "8" Beta の RemoteFX アダプティブ グラフィックスでは、配信対象のコンテンツの種類に合わせて最適化された複数のコーデックが使用されるようになりました。たとえば、一般的な Web ページの場合、テキスト、イメージ、およびビデオのすべてのコンテンツが、それぞれのコンテンツの種類に合わせて最適化されたコーデックを使用してエンコードされます。

###### RemoteFX メディア リモート処理

メディアの消費は、企業のトレーニング メディア コンテンツの消費から、軽量コンテンツの作成およびオーサリング、デモやマーケティング資料の作成まで、さまざまなエンド ユーザー エクスペリエンスの重要な部分となっています。また、メディアは、オンライン コラボレーション (ライブ ミーティングや電話会議など) やレクリエーション メディア消費の一部としても使用されています。

Windows 7 では、マルチメディア コンテンツの効率的なリダイレクト機能が導入されました。ユーザーがリモート セッションで Windows Media Player を使用してマルチメディア コンテンツを再生しようとすると、再生対象のコンテンツがインターセプトされます。インターセプトされたコンテンツは、その後クライアントにリダイレクトされます。RDP クライアントが、圧縮されたこのコンテンツを受信し、コンテンツをデコードしてローカルで再生します。それによって、コンテンツがクライアント リソースを使用してローカルで表現されるため、エンド ユーザーの使用感はローカルでの操作にきわめて近いものになります。

RemoteFX メディア リモート処理機能の中核を成すのは、ネットワーク検出、グラフィック プロファイル、および RemoteFX シナリオの統合です。この統合により、RDP を介して、メディア利用におけるすばらしい使用感が実現されます。エンド ユーザーには、ローカルでの再生と、リモート セッションを介したメディアの再生との間に差異は意識されにくくなります。

###### RemoteFX マルチタッチ

マルチタッチ統合は、Windows Server "8" Beta におけるきわめて重要なユーザー エクスペリエンス目標の 1 つです。マルチタッチ統合は、ユーザーとオペレーティング システムおよびアプリケーションとの対話の新しい方法を実現し、マルチタッチがユーザーの操作の主要手段として機能するデバイスにまで Windows を拡張します。Windows 8 Consumer Preview では、ローカル オペレーティング システムを操作するときと同じように、リモート デスクトップ セッションを操作できるようにする機能がユーザーから求められています。たとえば、次のような機能です。

* リモート セッションでのマルチタッチ ジェスチャおよび操作のサポート
* タッチだけで、ローカル セッションとリモート セッション間、およびそれぞれのセッション内を移動できる機能
* リモート セッションでの滑らかで応答性のあるマルチタッチ操作

Windows 7 と Windows Server 2008 R2 では、RDP とリモート デスクトップ接続クライアントでのタッチのサポートは、遅い固定レートで取り込まれた、昇格されたマウス イベントに制限されており、タッチ操作への部分的な対応に留まっています。また、Windows Server "8" Beta の RDP では、リモート デスクトップ セッションでのマルチタッチ操作のネイティブ サポートも提供しています。

## リモート デスクトップ サービスのインストールと有効化

Windows Server "8" Beta でリモート デスクトップ サービス コンポーネントのインストールを行う前に、お客様の組織に利益をもたらすリモート デスクトップ シナリオはどのようなものか、またどのような高度な機能が必要なのかを検討してください。Windows Server "8" Beta の新しいサーバー マネージャーが提供するシナリオ ベースのインストール機能は、このようなシナリオに対応しており、インストール時には適切な役割サービスが選択した各サーバーにインストールされるため、展開の一部であるサーバーごとに個別にインストールする必要はありません。

以降のセクションでは、リモート デスクトップ サービスの展開シナリオについて概説すると共に、それぞれのシナリオを構成するコンポーネントのインストールと初期構成を、サーバー マネージャーのシナリオ ベースのインストール機能を使用して実行する方法について説明します。

#### 展開シナリオ

Windows Server "8" Beta のリモート デスクトップ サービスは、複数の異なる役割サービスで構成されています。これらの役割サービスを個別にインストールして基本的な機能をサポートすることができますが、複数の役割サービスを組み合わせてより高度な機能を確保することもできます。リモート デスクトップ サービスのコンポーネントをインストールして高度な機能をサポートする場合は、対象の高度な機能によって実現されるシナリオについて考えることが役立ちます。管理者は Windows Server "8" Beta サーバー マネージャーで、インストール時に展開の種類を選択するように求められるほか、展開される各サーバーにインストールする役割サービスを選択するように求められます。

##### セッション仮想化のシナリオ

リモート デスクトップ セッション ホスト サーバーを展開して、サーバーにインストールされているアプリケーションにアクセスできるようにすることは、セッション仮想化とも呼ばれます。ユーザーは、完全なデスクトップ セッションにアクセスできるか、または RemoteApp として展開されている特定のアプリケーションだけにアクセスできます。管理者は、さらにリモート デスクトップ接続ブローカー サーバーを追加して複数サーバー ファーム シナリオに対応したり、RemoteApp 展開用にリモート デスクトップ Web アクセス サーバーを追加したりすることもできます。Windows Server "8" Beta で役割サービスをインストールする際には、管理者は、サーバー マネージャーのシナリオ ベースのインストール モードで [Shared Desktop Deployment] オプションを選択する必要があります。

このガイドでは、セッション仮想化シナリオに焦点を絞り、デスクトップと RemoteApp の展開のガイダンスを提供します。

##### デスクトップ仮想化のシナリオ

リモート デスクトップ仮想化ホスト サーバーをリモート デスクトップ接続ブローカーおよびリモート デスクトップ Web アクセス サーバーと共に展開して、ユーザーが仮想化されたデスクトップにアクセスできるようにすることは、デスクトップ仮想化とも呼ばれます。Windows Server "8" Beta で役割サービスをインストールする際には、管理者は、サーバー マネージャーのシナリオ ベースのインストール モードで [Virtual Desktop Deployment] オプションを選択する必要があります。

Microsoft VDI とデスクトップ仮想化シナリオの詳細については、『Windows Server "8" Beta VDI and RemoteFX Early Adopters Guide』を参照してください。

##### リモート デスクトップ ゲートウェイ

管理対象および管理対象外のクライアント コンピューターを使用してインターネット経由で RDS 環境にアクセスできるようにするには、リモート デスクトップ ゲートウェイ サーバーをインストールし、構成することを検討してください。RD ゲートウェイはどちらの種類の RDS 環境にも必須ではなく、企業ネットワーク上の RDS サーバーへのインターネット経由のアクセスを可能にするためのオプションの機能です。

RD ゲートウェイの役割サービス用に選択したサーバーには、パブリック ネットワーク上にネットワーク インターフェイスが必要です。多くの場合、このサーバーは DMZ 内のエッジ ネットワーク上に展開されます。RDS 環境に RD Web アクセス サーバーも組み込む場合は、RD ゲートウェイと RD Web アクセスの両方の役割サービスを同じサーバー上にインストールすることも検討してください。

##### リモート デスクトップ ライセンス

「技術概要」のセクションで説明したように、リモート デスクトップ サービスには 120 日の猶予期間があり、その間、ライセンス サーバーを必要とすることなく、このサービスをインストールし、評価することができます。しかし、猶予期間の終了後に、ユーザーがセッション仮想化またはデスクトップ仮想化のどちらかの種類の RDS 環境に接続できるようにするためには、ライセンス サーバーをインストールし、アクティブ化する必要があります。

### インストール プロセス

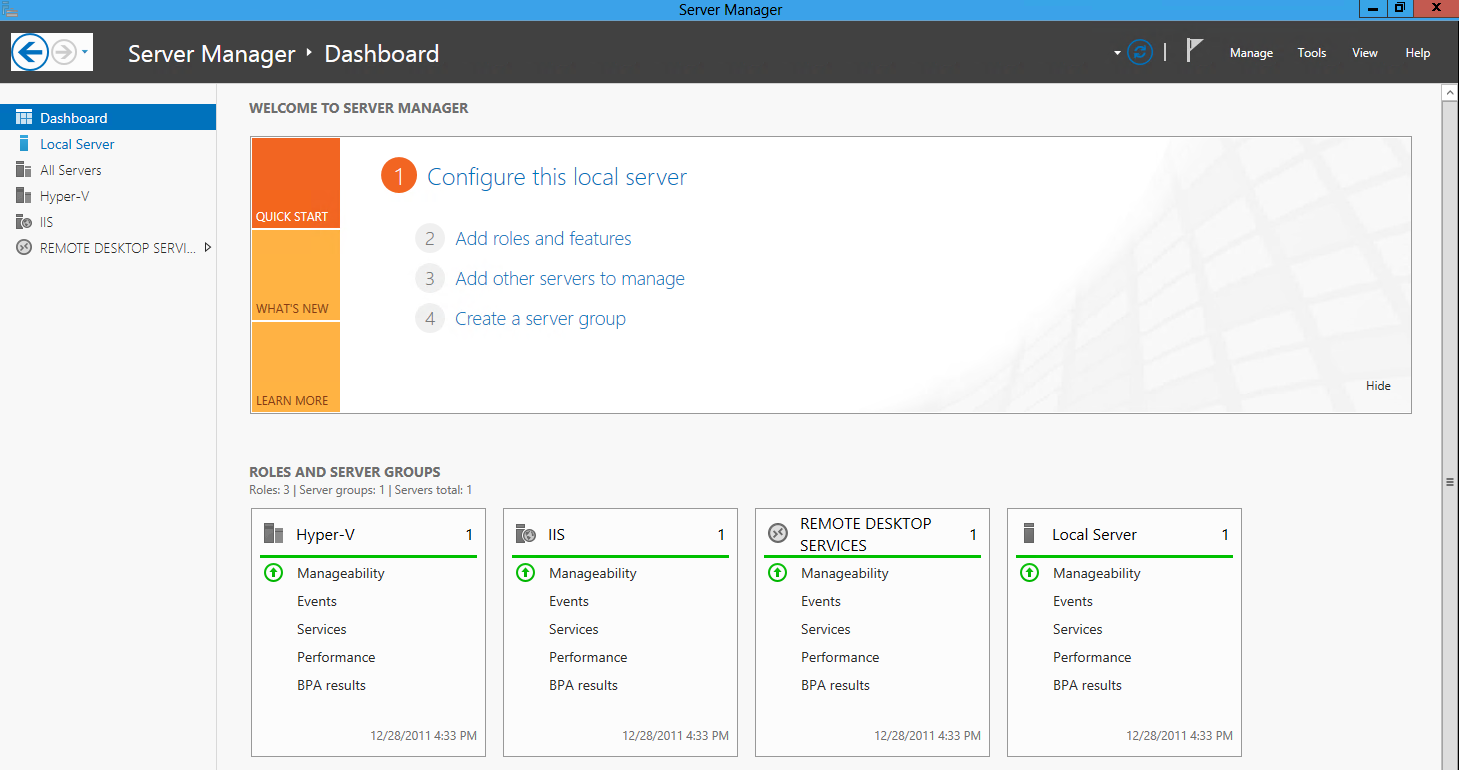
以下のセクションでは、新たなサーバー マネージャー ユーザー インターフェイスについて詳しく紹介し、このインターフェイスを使用して、選択したリモート デスクトップ サービス展開シナリオに必要な役割サービスをインストールする方法を説明します。

#### リモート デスクトップ シナリオ ベースのインストール

リモート デスクトップ サービスのすべての役割とシナリオのインストールには、Windows Server "8" Beta の新しいサーバー マネージャー ユーザー インターフェイスを使用します。この新しいインターフェイスでは、ローカルとリモートの両方のサーバー管理機能が提供され、個々のサーバー機能、役割サービス、展開の種類を管理するための一連のプラグインが使用されます。

以下に、サーバー マネージャーの [ダッシュボード] ページの例を示します。サーバー マネージャーを開くと、このページが最初に表示されます。

図 16: サーバー マネージャーのダッシュボード



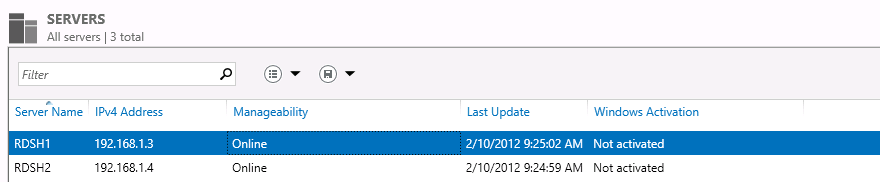
##### サーバー マネージャー プールへのコンピューターの追加

サーバー マネージャーを実行するコンピューターを 1 つ選択し、必要なコンポーネントのインストールを実行します。サーバー マネージャーを使って必要な役割サービスの管理とインストールをリモートから実行できるようにするには、リモート デスクトップ サービス環境の一部とする各サーバーをサーバー マネージャーのサーバー プールに追加する必要があります。

サーバー マネージャーのサーバー プールにサーバーを追加する手順は次のとおりです。

1. **サーバー マネージャー**を開き、ナビゲーション ウィンドウで [すべてのサーバー] をクリックします。
2. サーバー マネージャーのメニュー バーで [管理] をクリックし、[サーバーの追加] をクリックします。
3. "Active Directory" でサーバーを探すか、"DNS" でサーバーを検索するか、またはサーバー名ファイルを "インポート" することによって、各サーバーを一覧に追加します。
4. 各コンピューターが見つかったら、矢印ボタンをクリックして一覧に追加し、すべてのサーバーが [選択済み] 一覧に表示されるようにします。すべてのサーバーを追加したら、[OK] をクリックします。
5. プールに追加した各マシンについて、サーバー マネージャーによってクエリが実行され、IP アドレス、管理の状態、およびアクティブ化の状態が示されます。シナリオ ベースのインストールに進む前に、各サーバーがサーバー マネージャーに "オンライン" として表示されていることを確認してください。

図 17: サーバー マネージャーのサーバー プール



##### シナリオ ベースのインストールの実行

サーバー マネージャーのサーバー プールへのサーバーの追加が完了したら、シナリオ ベースのインストールの実行を開始できます。

共有デスクトップ環境をインストールする手順は次のとおりです。

1. **サーバー マネージャー**を開き、ナビゲーション ウィンドウで [すべてのサーバー] をクリックします。
2. サーバー マネージャーのメニュー バーで [管理] をクリックし、[役割と機能の追加] をクリックします。

|  |  |
| --- | --- |
| 重要: | 以下の前提条件が満たされていることを確認するようユーザーに求める、サーバー マネージャーのメッセージが表示されます。   * 管理者アカウントに強力なパスワードが設定されている * 静的 IP アドレスなどのネットワーク設定が構成されている * Windows Update の最新のセキュリティ更新プログラムがインストールされている   これらの前提条件が満たされていることを確認してから、インストールを続行してください。 |

1. [次へ] をクリックし、[リモート デスクトップ サービス シナリオ ベースのインストール] をクリックして、[次へ] を再びクリックします。
2. [展開の種類の選択] 画面で、展開の種類として [Standard Deployment] をクリックして [次へ] をクリックします。
3. [展開シナリオの選択] 画面で、[セッション仮想化] をクリックして [次へ] をクリックします。
4. [役割サービスの確認] ページには、その展開に必要な役割サービスの一覧と、それぞれのサービスの説明が表示されます。セッション仮想化展開の場合、必要なサーバーの役割は RD 接続ブローカー、RD Web アクセス サーバー、および 1 つ以上の RD セッション ホスト サーバーです。
5. [RD 接続ブローカー] 画面で、リモート デスクトップ接続ブローカーとリモート デスクトップ管理サービス プラグインのインストール先サーバーを選択して [次へ] をクリックします。
6. リモート デスクトップ Web アクセスのインストール先サーバーを選択して [次へ] をクリックします。リモート デスクトップ Web アクセスをリモート デスクトップ接続ブローカーと同じサーバーにインストールする場合は、[Install RD Web Access role service on the RD Connection Broker servers] チェック ボックスをオンにします。
7. リモート デスクトップ セッション ホストの役割のインストール先サーバーを選択して [次へ] をクリックします。

|  |  |
| --- | --- |
| 注意: | 複数サーバーのセッション仮想化コレクションを作成する場合は、前述のプロセスを使用してそれぞれのサーバーをサーバー マネージャーのプールに確実に追加してください。前述の手順 8 でリモート デスクトップ セッション ホストの役割をインストールするすべてのサーバーを選択すると、選択されたすべてのサーバー上に役割サービスがインストールされます。 |

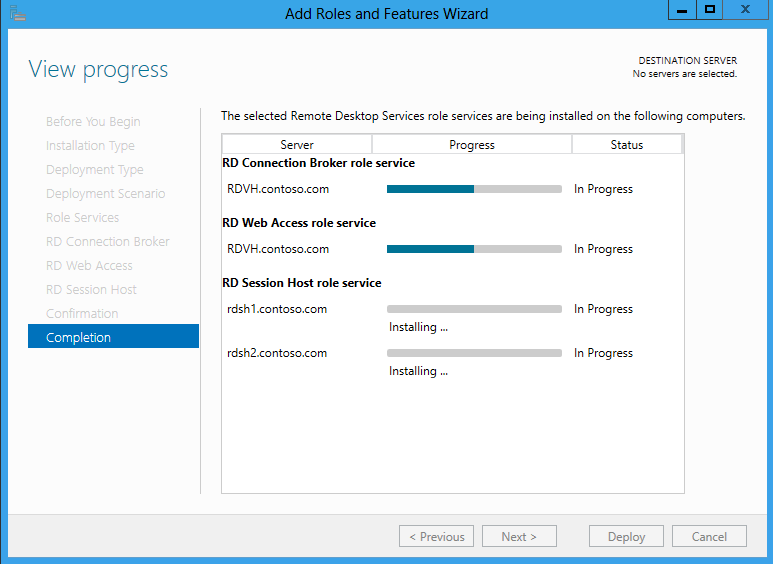
1. サーバー マネージャーにウィザードでの選択内容の概要が表示されます。各サーバーに役割サービスをインストールして展開を作成するには、[Deploy] をクリックします。

|  |  |
| --- | --- |
| 重要: | 展開されるサーバーのいずれかで再起動が必要な場合は、サーバー マネージャーによって再起動が必要なサーバーの一覧が表示されます。この場合、[必要に応じて対象サーバーを自動的に再起動する] チェックボックスをオンにしないと、[Deploy] ボタンは利用できません。 |

サーバー マネージャーに、環境内の各コンピューターでの役割サービスのインストールの状況が表示されます。また、役割のインストールで再起動が必要な場合、自動再起動のオプションを選択していれば、各コンピューターが再起動されます。インストールが完了すると、サーバー マネージャーに [閉じる] ボタンが表示されます。

次のスクリーンショットは、進行中の展開の例を示しています。

図 18: インストールの進行状況



各サーバーへのインストールの進行状況バーに、各サーバーのインストールの現在の状況を示すステータス インジケーターが表示されます。以下は、各ステータス インジケーターの一覧とそれぞれの定義です。

* **インストール中** — 役割サービスが現在インストールされています。
* **進行中** — サーバーのインストールと構成が進行中です。
* **構成保留中** — インストールは完了しましたが、構成で再起動が保留中です。
* **再起動中** — 役割サービスのインストールが完了し、サーバーが現在再起動されています。
* **構成中** — 役割サービスがインストールされ、現在構成されています。
* **成功** — シナリオ ベースの展開でコンピューターへのすべての役割サービスのインストールと構成が完了しました。
* **失敗** — サーバーのインストールまたは構成に失敗しました。ステータス ウィンドウに理由が表示されます。

##### クイック スタート展開の使用

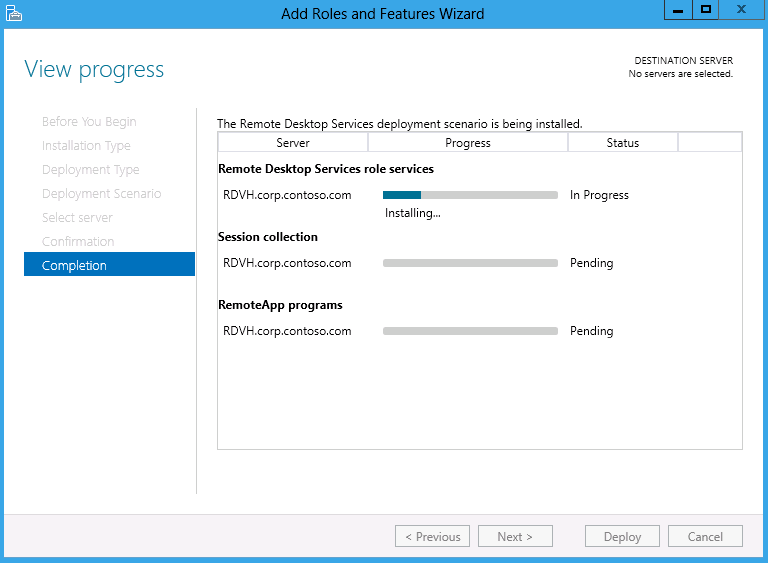
1 台のコンピューターにすべての役割サービスをインストールすることを計画しており、セッション仮想化環境をできるだけ迅速に作成することを望んでいる場合は、クイック スタート展開を使用できます。クイック スタート展開オプションを使用すると、RD セッション ホスト、RD Web アクセス、およびリモート デスクトップ接続ブローカーの各役割が 1 台のコンピューターにインストールされます。クイック スタートでは、必要なすべての役割サービスがインストールされるだけでなく、セッション仮想化のコレクションの作成と RDWeb ページへのコレクションの公開が自動的に実行されます。

クイック スタート展開方法を使用して単一のサーバーにすべての役割サービスをインストールする手順は次のとおりです。

1. サーバー マネージャーを開き、ナビゲーション ウィンドウで [ローカル サーバー] をクリックします。
2. メニュー バーで [管理] をクリックし、[役割と機能の追加] をクリックします。
3. [次へ] をクリックし、[リモート デスクトップ サービス シナリオ ベースのインストール] をクリックして、[次へ] を再びクリックします。
4. [展開の種類の選択] ページで、[クイック スタート] の横のラジオ ボタンをクリックします。
5. [展開シナリオの選択] ページで、[セッション仮想化] をクリックします。
6. [サーバー プール] でローカル サーバーが選択されていることを確認して、[次へ] をクリックします。このサーバーに、リモート デスクトップ接続ブローカー (RDCB)、リモート デスクトップ Web アクセス (RDWA)、およびリモート デスクトップ セッション ホスト (RDSH) の各役割がサーバー マネージャーによってインストールされます。
7. [選択内容の確認] ページで、[必要に応じて対象サーバーを自動的に再起動する] チェック ボックスをオンにします。[Deploy] ボタンをクリックします。

各役割サービスのインストールが表示され、[進行状況] 列に現在のインストールの状況が表示されます。

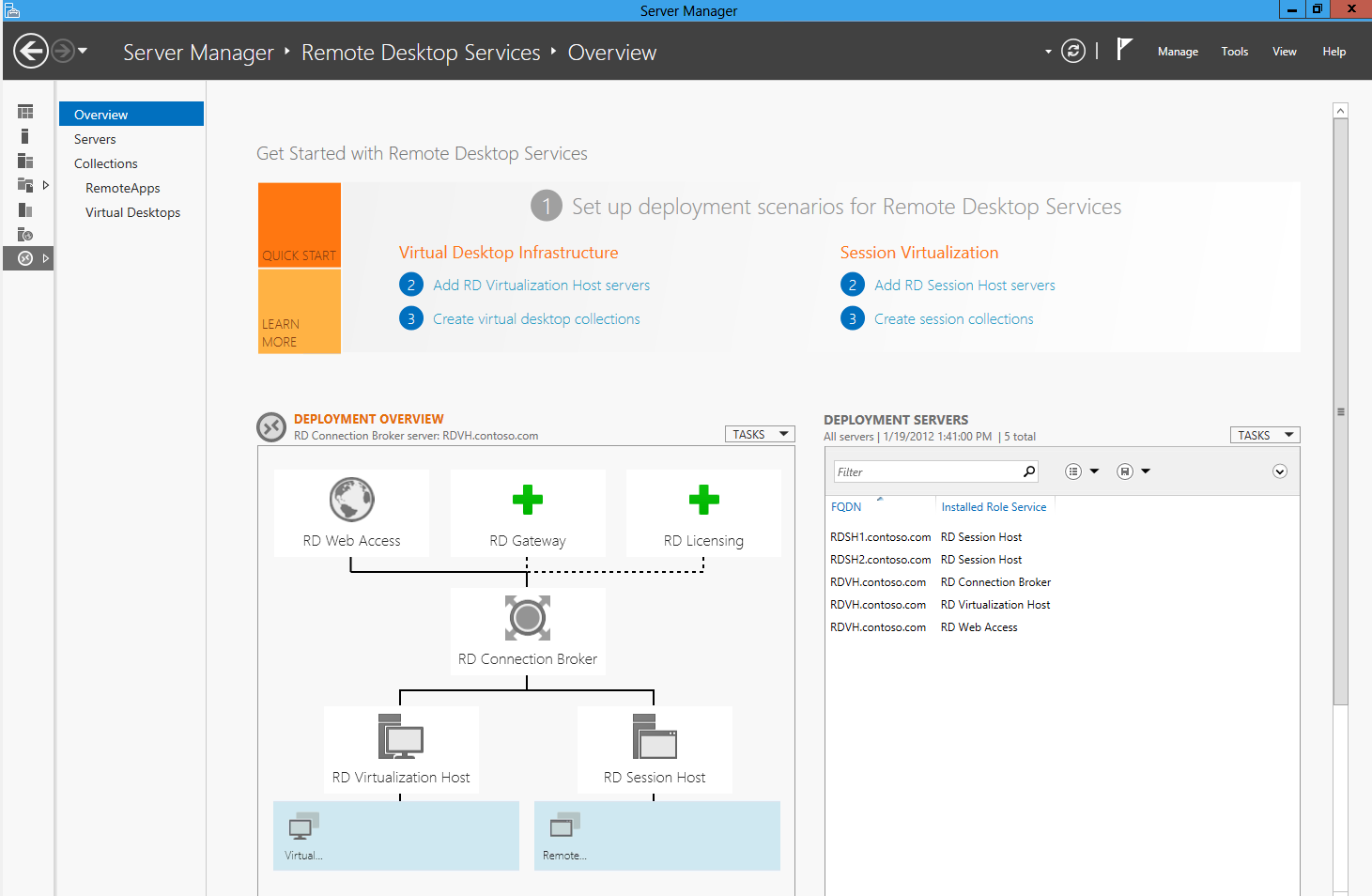
図 19: クイック スタート展開のインストールの進行状況



##### インストールの検証

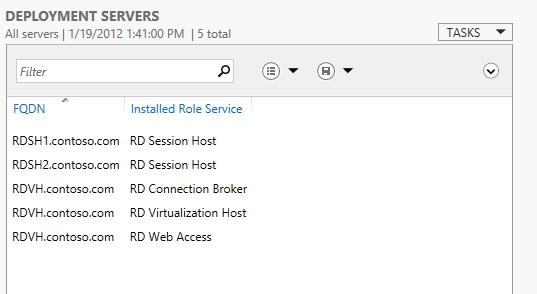
シナリオおよび必要な役割サービスのインストールを検証するには、サーバー マネージャーを一度閉じて、もう一度開くか、または [最新の情報に更新] ボタンを使用して表示を最新の情報に更新します。それにより、サーバー プールに属する各サーバーにインストールされた役割サービスがサーバー マネージャーによって検出されます。この時点で、リモート デスクトップ ノードがサーバー マネージャーでアクティブになっています。このノードをクリックすると、リモート デスクトップ サービス環境の [概要] ページが表示されます。

図 20: リモート デスクトップの [概要] ページ



RDS 環境の一部となっている各サーバーが展開の概要に表示されます。また、[展開サーバー] タイルの [インストールされている役割] に各サーバーにインストールされている役割が表示され、それぞれのサーバーが RDCB に結合されていることが示されます。

図 21: 展開サーバーのタイル



#### リモート デスクトップ セッション ホストのインストール

リモート デスクトップの役割とサービスは、シナリオ ベースのインストール方法を使用しないで、各サーバーに個別にインストールできます。簡易展開を実行する場合は、簡易展開ウィザードを実行する前に、いくつかの役割サービスをインストールする必要がある場合があります。

役割ベースのインストール方法を使用してリモート デスクトップ セッション ホストをインストールする手順は次のとおりです。

1. **サーバー マネージャー**を開き、ナビゲーション ウィンドウで [サーバー] をクリックします。
2. サーバー マネージャーのメニュー バーで [管理] をクリックし、[役割と機能の追加] をクリックします。
3. [次へ] をクリックし、[役割ベースまたは機能ベースのインストール] をクリックして、[次へ] を再びクリックします。
4. [サーバー プール] でローカル サーバーが選択されていることを確認して、[次へ] をクリックします。
5. [サーバーの役割の選択] ページで、[リモート デスクトップ サービス] をクリックして [次へ] をクリックします。
6. [機能] ページで [次へ] をクリックして、[リモート デスクトップ サービス] ページで再び [次へ] をクリックします。
7. [リモート デスクトップ セッション ホスト] チェック ボックスをオンにして [次へ] をクリックします。
8. インストール後、このコンピューターにさらに変更を加える場合は、[必要に応じて対象サーバーを自動的に再起動する] チェック ボックスをオフにします。それ以外の場合は、このチェック ボックスをオンにして [インストール] をクリックします。

|  |  |
| --- | --- |
| 説明: \\medialibrary\TCmedia\ProductionArt\IllustrationLibrary\PowerPoint\LightBulb.png ヒント: | [閉じる] をクリックして、ウィザードの [インストールの進行状況] ウィンドウを閉じることができます。インストールの進行状況を確認するには、サーバー マネージャーの上部ウィンドウにある [タスク] フラグをクリックし、[タスクの詳細] をクリックします。それにより、インストールの進行状況が表示されます。 |

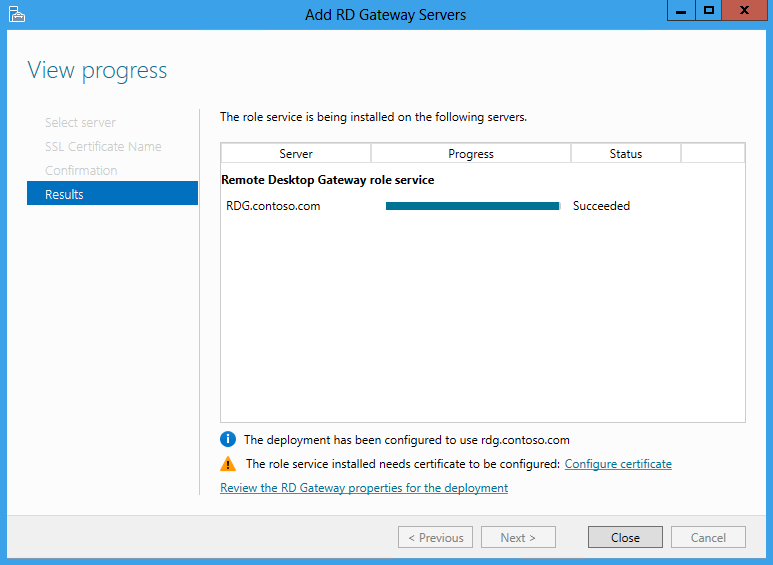
#### リモート デスクトップ ゲートウェイのインストール

ユーザーがインターネット経由でリモート デスクトップ環境にアクセスできるようにするには、少なくとも 1 台のサーバーにリモート デスクトップ ゲートウェイ役割サービスをインストールしてください。RD ゲートウェイの役割サービスをインストールする前に、RD 接続ブローカー サーバーのサーバー マネージャーのサーバー プールに対象サーバーを確実に追加してください。

リモート デスクトップ ゲートウェイをインストールする手順は次のとおりです。

1. RD 接続ブローカー サーバーで**サーバー マネージャー**を開き、[概要] ページをクリックします。
2. トポロジ ビューアーを使用して、トポロジ図の [RD ゲートウェイ] を右クリックし、[Add RD Gateway Servers] をクリックします。
3. RDMS サーバー上のサーバー マネージャーのサーバー プールにあるいずれかのサーバーに RD ゲートウェイの役割サービスを以前インストールしてある場合は、それらのサーバーが [サーバーの選択] ページに表示されます。新しいサーバーに RD ゲートウェイをインストールする場合は、一覧からサーバーを選択して [次へ] をクリックします。
4. インターネット経由で RD ゲートウェイ サーバーにアクセスするときに使用される外部完全修飾ドメイン名を入力します。この名前は外部クライアントによって解決可能であることが必要です。また、この名前は、RD ゲートウェイ サーバー上に自己署名証明書を作成するためにも使用されます。
5. 設定の確認ページで、[Restart remote target machines as needed] チェックボックスをオンにして [追加] をクリックします。
6. インストールが終了すると、リモート デスクトップ証明書の管理インターフェイスへのリンクが表示され、RD ゲートウェイで使用される証明書の構成を実行できます。

図 22: RD ゲートウェイの初期構成



1. [証明書の構成] リンクをクリックして、RD ゲートウェイ サーバーに使用する証明書を選択し、インストールします。証明書設定の構成方法の詳細については、このドキュメントの「[証明書の管理](#_Certificate_Management)」のセクションを参照してください。

#### リモート デスクトップ ライセンスのインストール

リモート デスクトップ サービスの展開では、ライセンス認証され、ユーザーごとまたはデバイスごとにクライアント アクセス ライセンスがインストールされたライセンス サーバーが少なくとも 1 台必要です。RD ライセンスの役割サービスをインストールする前に、RD 接続ブローカー サーバーのサーバー マネージャーのサーバー プールに対象サーバーを確実に追加してください。

RD ライセンス サーバーを追加する手順は次のとおりです。

1. RD 接続ブローカー サーバーで**サーバー マネージャー**を開き、[概要] ページをクリックします。
2. トポロジ ビューアーを使用して、トポロジ図の [RD ゲートウェイ] を右クリックし、[Add RD Licensing Servers] をクリックします。
3. ライセンス役割サービスのインストール先サーバーを選択し、[選択済み] 一覧にそれを追加して、[次へ] をクリックします。
4. 確認ページで [追加] ボタンをクリックすると、選択されたサーバーにリモート デスクトップ ライセンスの役割サービスがインストールされます。

#### 高可用性 RD 接続ブローカーの構成

高可用性 RD 接続ブローカーを展開するためのプロセスは、Windows Server "8" Beta で大きく変更されています。RDMS に追加されたウィザードが、アクティブ/アクティブな RD 接続ブローカーを作成するプロセスを通して管理者をガイドします。

|  |  |
| --- | --- |
| 注意: | 高可用性を提供するように接続ブローカーを構成するのは任意の手順であり、リモート デスクトップ サービス展開の必須事項ではありません。高可用性接続ブローカーの利点の詳細については、このドキュメントの「アーキテクチャ」のセクションを参照してください。 |

##### 前提条件

高可用性 RD 接続ブローカーの展開を開始する前に、次のコンポーネントが既にインストールされていることを確認してください。

* 環境に含まれるすべての RD 接続ブローカー サーバーに対する書き込みアクセス許可が付与された Microsoft SQL Server
* 環境に含まれるすべての RD 接続ブローカー サーバー上に Microsoft SQL Server Native Client がインストールされていること
* 環境に含まれるすべての RD 接続ブローカー サーバーに対して、静的 IP アドレスが割り当てられていること
* 環境に含まれるすべての RD 接続ブローカー サーバーに対して、単一の DNS 名を持つ DNS リソース レコードが作成されていること
* (RD ゲートウェイを使用する場合は) メンバーとして DNS RR 名を使用してローカル グループにアクセスすることを可能にする、新しい RD ゲートウェイ RAP 規則を追加すること

|  |  |
| --- | --- |
| 重要: | SQL サーバー上のファイアウォールは、SQLSERVER.EXE への着信接続を許可するように構成する必要があります。 |

高可用性 RD 接続ブローカー (HA RD 接続ブローカー) を構成するには、以下の手順に従います。

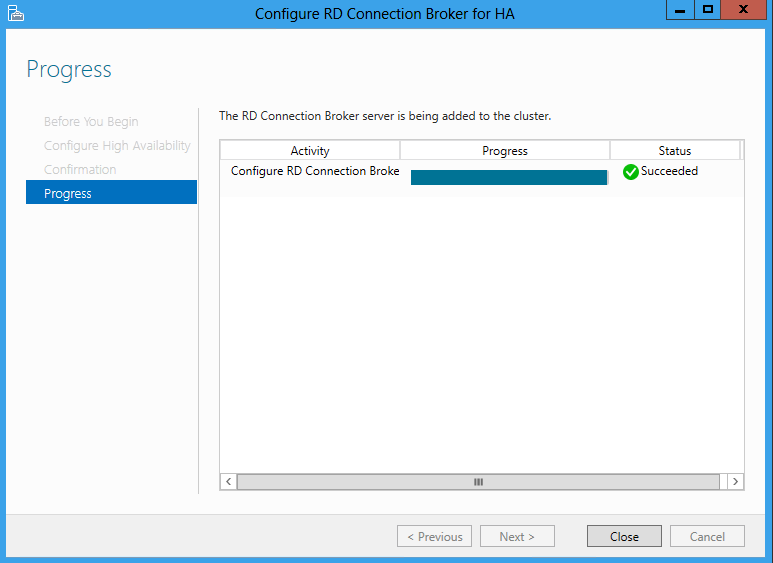
1. サーバー マネージャーを開き、[リモート デスクトップ サービス] ノードをクリックします。
2. [リモート デスクトップ サービス] ページで、[概要] をクリックして、[展開の概要] タイルを表示します。
3. [RD 接続ブローカー] アイコンを右クリックして、[HA の RD 接続ブローカーの構成] をクリックします。
4. [開始する前に] ページの前提条件を確認して、[次へ] をクリックします。
5. [データベース接続文字列] ボックスに、次を入力します。

DRIVER=SQL Server Native Client 10.0;SERVER=<name of SQL server>;Trusted\_Connection=Yes;APP=Remote Desktop Services Connection Broker;Database=<name of database>

<name of SQL server> は両方の接続ブローカー ノードがアクセス許可リストに追加された SQL サーバーの名前、<name of database> は SQL Server上に作成するデータベースの名前です。

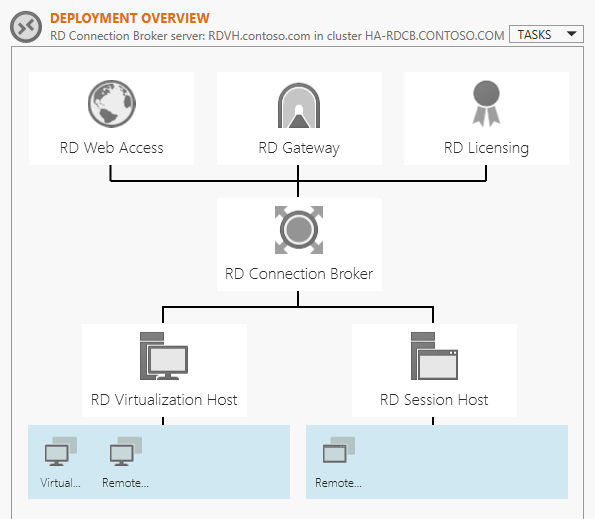
1. [Folder to Store Database Files] ボックスに、データベース ファイルを格納する SQL Server上のローカル フォルダーを入力します。
2. [DNS リソース レコード名] ボックスに、HA RD 接続ブローカーに対して作成された DNS RR レコードの FQDN (完全修飾ドメイン名) を入力して、[次へ] をクリックします。
3. [確認] ページで [構成] をクリックして、HA RD 接続ブローカーを作成します。完了すると、ウィザードに [成功しました] と表示されます。

図 23: HA RD 接続ブローカーのインストール



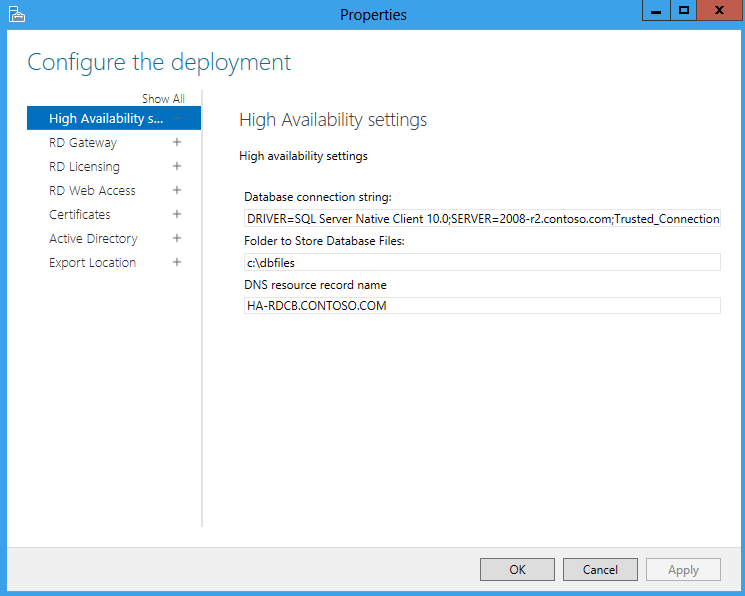
1. [概要] タイルは、RD 接続ブローカー名とクラスター名を表示するように変更されます。

図 24: RD 接続ブローカーのクラスター名



1. 展開プロパティには、高可用性の設定が表示されます。

図 25: 高可用性の設定



高可用性を提供するようにアクティブ/アクティブな RD 接続ブローカーを構成すると、リモート デスクトップ サービス環境は引き続き通常どおり動作し、接続ブローカー ノードの 1 つが機能を停止しても、管理者はコレクションを管理できます。

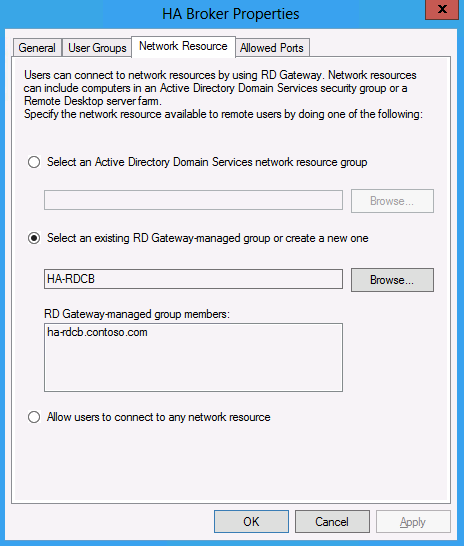
##### RD ゲートウェイの構成

RD ゲートウェイ サーバーを使用する場合は、前述の手順で接続ブローカーをHA構成した後、接続ブローカーへの接続を許可するように、ゲートウェイの RAP 規則を変更する必要があります。既定の RAP 規則では、ドメイン コンピューター グループのコンピューター アカウントに基づいてリソースへの接続が許可されますが、HA 接続ブローカーはドメインにコンピューター アカウントを持っていません。

RD ゲートウェイを通してHA構成の接続ブローカーを持つ RDS 環境への接続を許可するには、以下の手順に従います。

1. 管理者として RD ゲートウェイ サーバーにログオンし、リモート デスクトップ ゲートウェイ マネージャーを開きます。
2. 左側のウィンドウでサーバー名を展開してから [ポリシー] を展開します。
3. [リソース承認ポリシー] をクリックし、[アクション] ウィンドウで [新規ポリシーの作成] をクリックして、次に [ウィザード] をクリックします。
4. [RD RAP のみ作成する] がオンになっていることを確認してから、[次へ] をクリックします。
5. 規則の名前を入力して、[次へ] をクリックします。
6. [グループの追加] ボタンをクリックして、RAP 規則に関連付けられるユーザー グループを追加し、[次へ] をクリックします。
7. [RD ゲートウェイで管理される既存のグループを選択するか、新しいグループを作成する] がオンになっていることを確認してから、[次へ] をクリックします。
8. [RD ゲートウェイで管理される新しいコンピューター グループを作成する] をクリックして、グループの名前を入力し、ネットワーク リソースの名前として HA 接続ブローカーの DNS RR 名を入力します。[追加] をクリックして、HA接続ブローカー名をグループに追加し、[次へ] をクリックします。
9. 環境に許可される TCP ポートを構成して、[次へ] をクリックします。
10. RAP 設定を確認して、[完了] をクリックします。
11. 新しい RAP 規則を開いて、プロパティが次のように表示されることを確認します。

図 26: HA接続ブローカーの RAP 規則



#### 役割サービスのアンインストール

サーバー マネージャーを使用した役割サービスのアンインストールは、一度に 1 台のサーバーについて、手動で行う必要があります。シナリオ ベースの アンインストールによって 1 つのウィザードを使用して複数のリモート コンピューターから役割サービスをアンインストールすることはできませんが、展開されている任意のサーバー上でサーバー マネージャーを実行することで、役割サービスをリモート コンピューターからアンインストールできます。

リモート デスクトップ役割サービスをアンインストールする手順は次のとおりです。

1. サーバー マネージャーを開き、ナビゲーション ウィンドウで [すべてのサーバー] をクリックします。
2. メニュー バーで [管理] をクリックし、[役割と機能の削除] をクリックします。
3. [Select Server Targets] 画面で、役割サービスを削除するサーバーを選択し、[次へ] をクリックします。
4. [Remove Sever Roles] 画面で、削除する役割サービスを選択し、[次へ] をクリックします。
5. [Select Features to Uninstall] 画面で、削除する機能がある場合はそれを選択し、[次へ] をクリックします。
6. [Confirm Deployment Selections] 画面で [削除] をクリックします。
7. 役割サービスを削除する各サーバーについて、手順 1 ～ 6 を繰り返します。

## リモート デスクトップ サービスの構成および管理

### 管理の考慮事項

Windows Server 2008 R2 では、Windows NT 4.0 Terminal Services Edition から使用されている従来のリモート デスクトップ サービス機能の多くを強化しました。現在の Windows Server 2008 R2 の充実した機能セットは、管理面が複雑化しているため、Windows Server "8" Beta では、リモート デスクトップ管理サービス (RDMS) と、サーバー マネージャーのリモート デスクトップ プラグインで新しい管理機能を導入しました。RDMS は、すべてのリモート デスクトップ シナリオのインストール、構成、および管理を簡素化し、容易化するように設計されているだけでなく、リモート デスクトップ管理のパラダイム全体を大幅に変更するものとなっています。

TSADMIN や TSCONFIG のような、旧バージョンの Windows で使用されていた RDS 管理ツールは、Windows Server "8" Beta では廃止されました。これまで管理者がこれらのツールを使用して実行していた管理機能は、新しい RDMS ユーザー インターフェイスを使用して実行されるようになりました。管理者が RDMS を使用してリモート デスクトップ環境を効果的に管理するためには、新しい管理インターフェイスに関連する新たな定義と用語を理解する必要があります。

#### 定義

このドキュメントで使用される用語について、以下に定義します。

**RDMS** — リモート デスクトップ管理サービス。このサービスは、環境内のリモート デスクトップ管理の役割を持つサーバー上で実行されます。このドキュメントでは、新しいリモート デスクトップ管理インターフェイスも RDMS と呼ばれます。

**RDMS UI** — リモート デスクトップ管理サービスのユーザー インターフェイス。これはサーバー マネージャーのプラグインで、ほとんどのリモート デスクトップ管理機能が実行されるユーザー インターフェイスです。

**RDMS プラグイン** — RDMS UI のことです。

**コレクション** — 完全なデスクトップ セッションや RemoteApp を提供するリモート デスクトップ セッション ホスト サーバーの論理グループ、または Microsoft VDI シナリオに展開される仮想マシンの論理グループ。リモート デスクトップ セッション ホスト サーバーのグループは、以前は "リモート デスクトップ セッション ホスト ファーム" と呼ばれていました。

**セッション仮想化** — 以前はターミナル サービスまたはリモート デスクトップ セッションと呼ばれていました。セッション仮想化はリモート デスクトップ セッション ホスト サーバーによって提供され、完全なデスクトップ セッションまたは RemoteApp の形で存在します。

**デスクトップ仮想化** — リモート デスクトップ サービスを使用した完全なデスクトップ ソリューションとして提供される仮想マシン。Microsoft リモート デスクトップ サービスを使用するデスクトップ仮想化は、Microsoft 仮想デスクトップ インフラストラクチャまたは Microsoft VDI とも呼ばれます。

**VDI** — 仮想デスクトップ インフラストラクチャ (VDI) は、ハイパーバイザーまたは仮想化プラットフォームを提供する中央のサーバー上で、仮想マシンとして実行されるようにデスクトップ オペレーティング システムをホストする方法です。

### 管理と構成

このセクションでは、RDMS を使用してリモート デスクトップ環境を管理する方法の詳細と、新しい RDMS 管理インターフェイスを使用しないライセンスなどのリモート デスクトップ コンポーネントの構成方法の詳細を説明します。

#### 管理タスク

リモート デスクトップ セッション仮想化環境の展開と管理は、以下の一連の手順を使用して行います。

1. グローバル設定の構成
2. コレクションの作成
3. コレクションのプロパティと設定の構成
4. コレクションへの RemoteApp の追加 (オプション)
5. ユーザー コレクションの管理
6. サーバーの管理

##### グローバル設定

ライセンス設定など、RDS 環境のすべてのリモート デスクトップ サービス サーバーに適用される設定は、RDMS の展開プロパティ ユーザー インターフェイスを使用して構成します。管理者はこのインターフェイスで、リモート デスクトップ ゲートウェイ、リモート デスクトップ ライセンス、デジタル証明書、および Active Directory の設定を構成できます。

RDS 環境のグローバル設定を構成する手順は次のとおりです。

1. サーバー マネージャーを開き、左側のウィンドウの [リモート デスクトップ] ノードをクリックします。
2. [コレクション] をクリックし、[コレクション] タイルで [タスク] メニューをクリックして、[Edit Deployment Properties] をクリックします。
3. 既定では、RD ゲートウェイ サーバーは構成されません。展開されているサーバーに接続するために RD ゲートウェイ サーバーを使用するには、[自動的に RD ゲートウェイ サーバーの設定を検出する] または [次の RD ゲートウェイ サーバー設定を使用する] をクリックして、RD ゲートウェイ サーバーの FQDN (完全修飾ドメイン名) を指定します。RD ゲートウェイ サーバー名を手動で構成する場合は、[ログオン方法] を設定する必要があります。既定の設定は [パスワード認証] です。
4. 左側のウィンドウで [RD ライセンス] をクリックして、RD ライセンス サーバー名とライセンス モードを入力します。複数の RD ライセンス サーバーを使用する場合は、[上へ移動] または [下へ移動] ボタンを使用してサーバーの使用順序を構成します。
5. 既定のサイトを使用しない場合は、左側のウィンドウで [RD Web アクセス] をクリックして、RD Web アクセス サイトの URL を変更します。
6. [証明書] をクリックして、RDS 環境の証明書を管理します。詳細については、以降の「[**証明書の管理**](#_Certificate_Management)」のセクションを参照してください。
7. 左側のウィンドウで [Active Directory] をクリックして、Active Directory 設定を構成します。これらの設定は、VDI 環境および仮想マシンのコレクションのみに必要とされます。
8. [エクスポート先] をクリックして、仮想マシン コレクション作成のエクスポート パスを構成します。この設定は、VDI 環境および仮想マシンのコレクションのみに必要とされます。

###### 証明書の管理

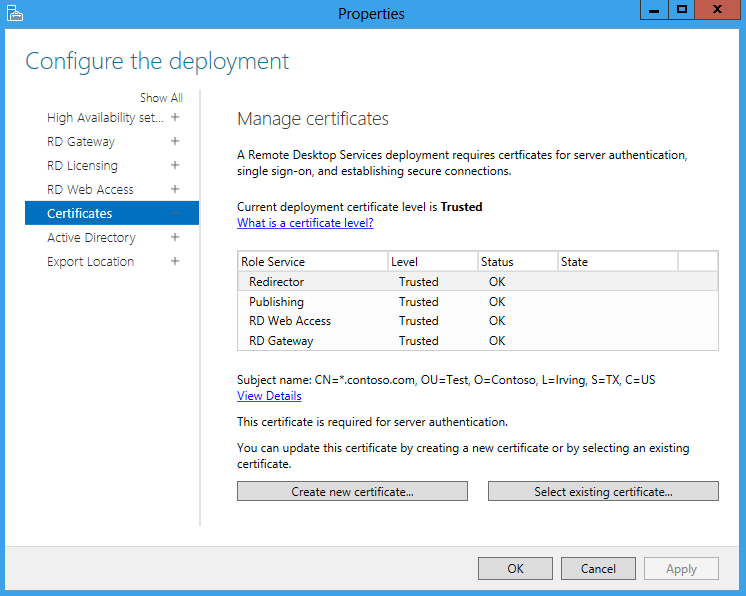
RDMS は、リモート デスクトップ サービス環境に使用される証明書の作成、展開、管理を支援する新しいユーザー インターフェイスを備えています。証明書は、サーバー認証、シングル サインオン、およびセキュリティで保護された接続の確立に使用されます。RDMS の証明書管理機能では、RDS 環境に含まれるすべての役割サービスについて、証明書の表示や編集を行えます。

証明書の展開には、通常、既存の PKI インフラストラクチャとグループ ポリシーを使用しますが、RDMS 証明書管理ユーザー インターフェイスを使用して手動で作成、展開することもできます。

RDS 環境に使用する証明書の作成および管理手順は次のとおりです。

1. サーバー マネージャーを開き、ナビゲーション ウィンドウで [リモート デスクトップ サービス] ノードをクリックします。
2. [コレクション] をクリックし、[コレクション] タイルで [タスク] メニューをクリックして、[Edit Deployment] をクリックします。
3. RDS 証明書を管理するには、[証明書] をクリックします。証明書の使用が可能な各役割サービスと、選択した役割サービスの現在の状態および証明書レベルが表示されます。証明書レベルについての説明を参照するには、[証明書レベルとは] というリンクをクリックします。
4. 役割サービスをクリックし、[新しい証明書の作成] をクリックして自己署名入りの証明書を新規作成するか、[既存の証明書の選択] をクリックして、内部証明機関から取得された証明書またはグループ ポリシーによってインストールされた証明書を使用します。
5. [新しい証明書の作成] をクリックすると、新しい証明書ウィザードが開いて、自己署名入り証明書を作成できます。ユーザーの接続先サーバーの名前を入力するか、ワイルドカードを使用してドメインを指定します (例: \*.contoso.com)。証明書のパスワードを入力します。また、[Store this Certificate] チェック ボックスをオンにして .pfx ファイルのパスを指定し、証明書をクライアントに手動で配信できるようにします。秘密キーおよびパスワードと共に証明書が作成され、指定したパスに格納されます。
6. 役割サービスの変更の状態が [適用の準備完了] に変更されます。[適用] をクリックすると、[信頼済み] または [信頼しない] のレベルでステータスが [OK] に変わります。

図 27: 証明書の管理



1. さらに別の証明書を展開する場合は、役割サービスごとに上記の手順 4 ～ 6 を繰り返すか、または、[既存の証明書の選択] をクリックしてすべての役割サービスに同じ証明書を適用します。
2. 証明書のステータスが [信頼しない] になっている場合は、RDS 環境にアクセスするすべてのクライアント コンピューターに証明書を手動で展開します。証明書のステータスが [信頼済み] になっている場合は、クライアント コンピューターへの展開は不要です。

###### RD ゲートウェイの構成

リモート デスクトップ ゲートウェイの構成には、RDMS プラグインは使用しません。リモート デスクトップ ゲートウェイは、スタート画面またはサーバー マネージャーからアクセスできる別のユーザー インターフェイスを備えています。サーバー マネージャーを使用して、上記の手順に従って RD ゲートウェイをインストールした場合は、既定の接続承認ポリシーとリソース割り当てのポリシーが自動的に作成されます。

リモート デスクトップ ゲートウェイ サーバーを構成する手順は次のとおりです。

1. RD ゲートウェイ サーバーのスタート画面で、[リモート デスクトップ ゲートウェイ マネージャー] をクリックまたはタッチします。
2. サーバーの一覧でゲートウェイ サーバー名を右クリックして [プロパティ] をクリックします。
3. [全般] タブでは、[サポートされている最大同時接続数を許可する] が既定の設定になっています。接続を制限する場合や、RD ゲートウェイ経由の接続を無効にする場合は、対応するラジオ ボタンをクリックします。
4. [SSL 証明書] タブで、使用中の証明書が、展開プロパティで構成された証明書と一致していることを確認します。RDMS 証明書管理を使用して証明書が何も構成されていない場合は、既定の自己署名入り証明書が表示されます。
5. [トランスポート設定] タブでは、[UDP トランスポートを有効にする] チェック ボックスが既定でオンに設定されます。既定の HTTPS ポートは 443、既定の UDP ポートは 3391 ですが、これらのポートはカスタマイズできます。特定のネットワーク インターフェイスと IP アドレスを構成することもできます。既定では、RD ゲートウェイはすべての IP アドレスでリッスンします。
6. [RD CAP ストア] タブでは、接続承認ポリシーを格納するローカル NPS サーバーが選択されます。中央の NPS サーバーを使用する場合は、[NPS を実行するセントラル サーバー] をクリックして、CAP ポリシーを格納するセントラル NPS サーバーの DNS 名を入力します。
7. [サーバー ファーム] タブでは、ファームに含める追加の RD ゲートウェイ サーバー (ローカルの RD ゲートウェイ サーバーを含む) の名前を指定して [追加] をクリックします。
8. [適用] をクリックして、既定の構成に対する変更を確定します。

###### RD ライセンスの構成

Windows Server "8" Beta リモート デスクトップ サービス ライセンス サーバーの構成は Windows Server 2008 R2 から変わっていません。RDLS の役割のインストール後、管理者はローカルの RDLS にログオンできます。または、リモート デスクトップ ライセンス ツールを別のサーバーにインストールしてリモート接続することもできます。

|  |  |
| --- | --- |
| 説明: \\medialibrary\TCmedia\ProductionArt\IllustrationLibrary\PowerPoint\LightBulb.png ヒント: | リモート デスクトップ ライセンス サーバーの構成方法の詳細については、TechNet の次のリンクをご覧ください。  <http://technet.microsoft.com/ja-jp/library/cc754309.aspx> |

##### コレクションの作成

RDMS を使用してリモート デスクトップ セッション仮想化環境を管理する場合は、一連の "コレクション" に環境をグループ化する必要があります。セッション仮想化に関連する設定を構成し、RemoteApp をユーザーのために展開するには、RDMS 内でコレクションを作成する必要があります。

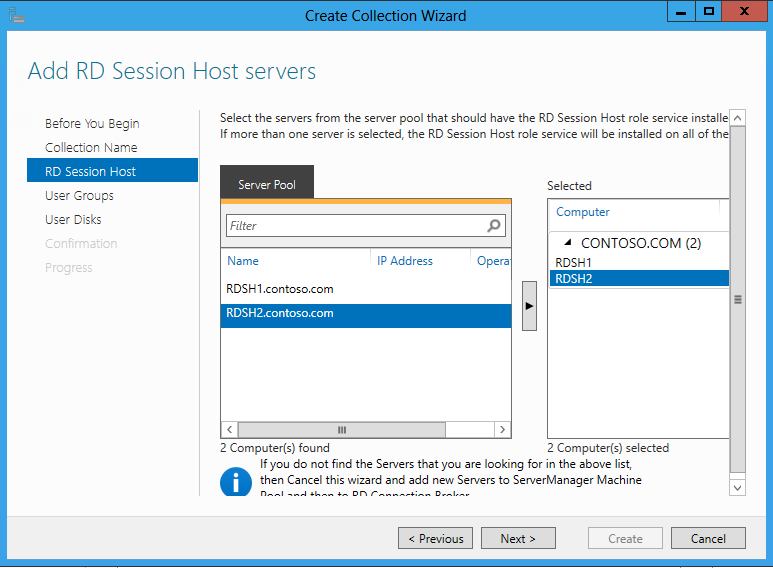
セッション コレクションを作成する手順は次のとおりです。

1. サーバー マネージャーの [リモート デスクトップ サービス] ノードで [コレクション] をクリックします。
2. [コレクション] をクリックし、[コレクション] タイルで [タスク] メニューをクリックして、[Create Session Collection] をクリックします。
3. セッション コレクションの前提条件に関する情報を確認して [次へ] をクリックします。

|  |  |
| --- | --- |
| 注意: | 前提条件のページは、[今後、このメッセージを表示しない] ボックスをクリックすることによって、今後ウィザードを開いたときに表示されないようにすることができます。 |

1. コレクションの名前と、必要に応じて説明を指定し、[次へ] をクリックします。
2. このコレクションに含めるリモート デスクトップ セッション ホスト サーバーのサーバー名をクリックし、矢印をクリックして [選択済み] 一覧にそのサーバーを移動して、[次へ] をクリックします。

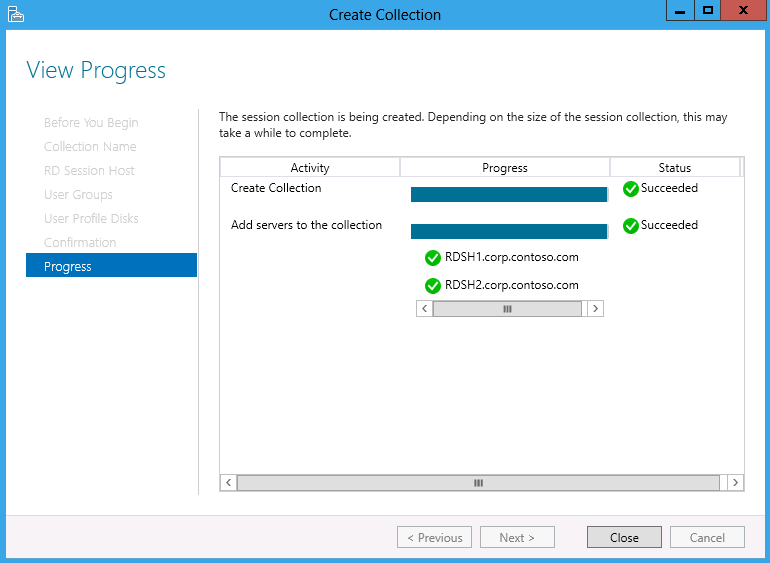
図 28: サーバーの一覧



|  |  |
| --- | --- |
| 説明: \\medialibrary\TCmedia\ProductionArt\IllustrationLibrary\PowerPoint\LightBulb.png ヒント: | 前述の一覧に含めたいサーバーが見つからない場合は、ウィザードを中止して、サーバー マネージャーのコンピューター プールと RD 管理の展開に新しいサーバーを追加します。セッション仮想化を展開するためにシナリオ ベースのインストールを実行した場合は、選択したサーバーがこの一覧に既に表示されています。 |

1. このコレクションへのアクセスを許可するユーザーやグループを追加するために [追加] ボタンをクリックしてから、[次へ] をクリックします。
2. [Enable User Profile Disks] チェックボックスをオンにして、ユーザー プロファイル ディスクに使用される SMB 共有パスを指定し、ユーザー プロファイル ディスクを構成します。
3. コレクションの作成ウィザードに、確認できるように設定が表示されます。コレクションを作成するには、[作成] ボタンをクリックします。コレクションが正常に作成されると、ウィザードには [成功しました] というメッセージが緑色のチェックマークと共に表示されます。

図 29: コレクション作成の成功



1. [閉じる] をクリックすると、RDMS の [コレクション] ウィンドウが更新されて、コレクションが表示されます。各サーバーが [ホスト サーバー] の下にも表示され、[RD セッション ホスト] の種類であるかどうかを確認します。

##### コレクションの管理

接続の時間制限、セキュリティ設定、リダイレクト設定、およびユーザー プロファイル ディスクといったコレクションの設定を構成するには、RDMS インターフェイスを使用してコレクションのプロパティを変更する必要があります。

|  |  |
| --- | --- |
| 重要: | 以下の手順では、一部の構成設定については説明を省略しています。ここでは、既定の設定と新しい設定について示し、それぞれの機能について簡単に説明します。すべての設定の一覧と各設定の説明については、付録を参照してください。 |

###### ユーザー プロファイル ディスク用の共有の作成

ユーザー プロファイル ディスクを使用してユーザー データを格納することを計画している場合は、コレクションの構成前に、ディレクトリを共有して、適切な NTFS アクセス許可を追加する必要があります。ユーザー プロファイル ディスクは、単一の VHD ファイルとして SMB 共有に格納されます。ユーザーのログオン先の RDSH サーバーは、VHD ファイルの作成および更新を実行するために、この共有に対する書き込みアクセス許可を必要とします。ユーザー プロファイル データにユーザー データを格納するコレクションごとに、個別にユーザー プロファイル ディスク共有を作成する必要があります。

ユーザー プロファイル ディスク共有を作成する手順は次のとおりです。

1. ユーザー プロファイル ディスクを格納するファイル サーバーにフォルダーを作成し、このフォルダーを共有します。
2. 共有アクセス許可の設定では、Everyone に対してフル コントロールのアクセス許可を構成します。

|  |  |
| --- | --- |
| 重要: | 上記の共有アクセス許可はユーザー プロファイル ディスク共有の最も単純な管理を許可するものですが、この場合、組織のセキュリティ要件を十分に満たさない場合があります。組織のセキュリティ ポリシーに従うと同時に、少なくとも、SMB 共有に書き込み処理を実行する RDSH サーバーには、フル コントロールのアクセス許可を設定してください。 |

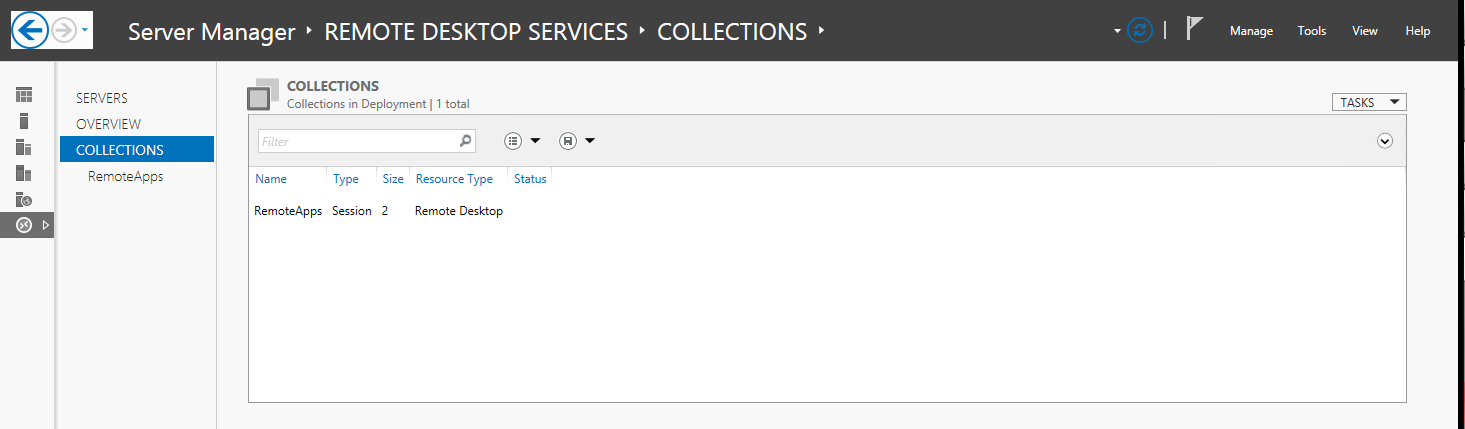
1. NTFS アクセス許可の構成時には、各 RDSH サーバーのコンピューター アカウントをアクセス許可の一覧に追加し、このアカウントに少なくとも書き込みアクセス許可を付与する必要があります。RDSH サーバーのコンピューター アカウントにフル コントロールを与え、既定の NTFS アクセス許可を変更しないことをお勧めします。

###### コレクション プロパティの構成

コレクションのプロパティを構成する手順は次のとおりです。

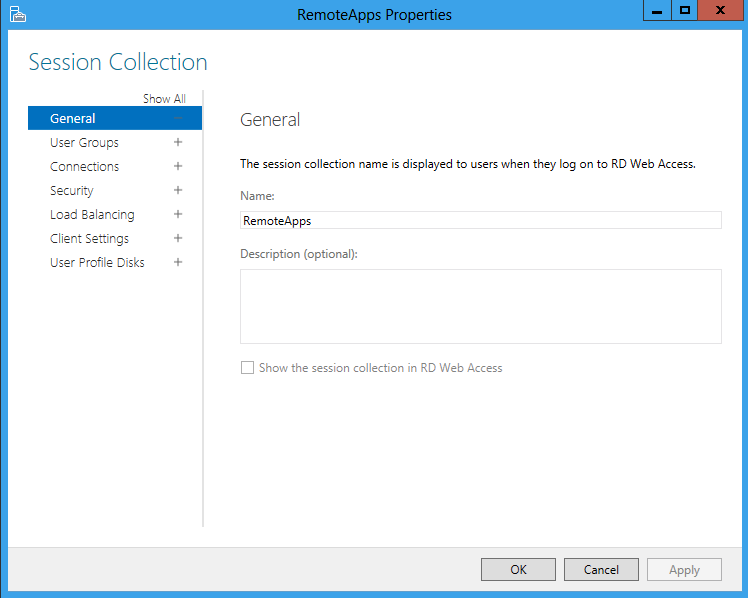
1. サーバー マネージャーの [リモート デスクトップ] ウィンドウで [コレクション] をクリックします。[コレクション] ノードの直下に、作成済みのコレクションが表示されます。

図 30: コレクション ビュー



1. コレクション名をクリックして、コレクションの [プロパティ] ウィンドウにアクセスします。[プロパティ] タイルをクリックして、[タスク] メニューから [プロパティの編集] をクリックします。
2. コレクションのプロパティが読み込まれ、左側のウィンドウに各構成ページの一覧が表示されます。

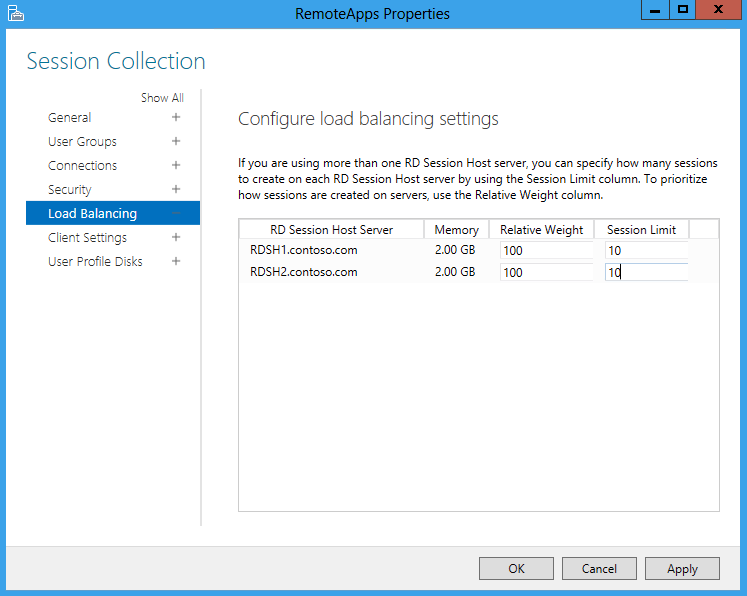
図 31: コレクションのプロパティ ページ



|  |  |
| --- | --- |
| 説明: \\medialibrary\TCmedia\ProductionArt\IllustrationLibrary\PowerPoint\LightBulb.png ヒント: | [プロパティの編集] インターフェイスはウィザードではないため、[次へ] ボタンはありません。構成設定の各グループにアクセスするには、左側のウィンドウで対象の構成設定グループをクリックします。 |

1. [全般] ページで、コレクション名と、オプションの説明を構成します。そのコレクションを [RD Web アクセス] ページに表示しない場合は、[Visibility in Web Access] チェックボックスをオフにします。
2. [ユーザー グループ] ページで、このコレクションへのアクセスを許可するユーザーまたはグループを構成します。
3. [接続] ページで、自動再接続設定、接続の時間制限、および一時フォルダー設定を構成します。
4. [セキュリティ] ページで、コレクションのセキュリティ設定を構成します。[セキュリティ層] の既定の設定は [ネゴシエート] で、[ネットワーク レベル認証でリモート デスクトップを実行しているコンピューターからのみ接続を許可する] も既定でオンになっています。さまざまなクライアント オペレーティング システムを混ぜて使用する場合は、この設定はオフにして、[セキュリティ層] は既定のまま構成することをお勧めします。
5. セッション コレクションに複数の RDSH サーバーが含まれる場合は、[負荷分散] ページで負荷分散の設定を構成します。Windows Server "8" Beta では、管理者は [セッションの最大数] を構成して、サーバーに送信される最大セッション数を制御できるようになっています。[相対的な重み] 設定は、Windows Server 2008 R2 のものと同じように機能します。

図 32: 負荷分散



1. [クライアントの設定] ページで、最大モニター数の設定、プリンター リダイレクト設定、およびデバイスのリダイレクト設定を構成します。これらの設定は、RemoteApp コレクションには使用できません。

|  |  |
| --- | --- |
| 重要: | 前のバージョンの Windows では、各形式のリダイレクトのチェックボックスをオンにすると、機能が有効になるのではなく、"無効" になっていました。これは Windows Server "8" Beta では、チェックボックスをオンにすると機能が "有効" になるように変更されており、以前よりわかりやすくなっています。 |

1. [ユーザー プロファイル ディスク] ページで、[Enable user profile disks] チェック ボックスをオンにして、ユーザー プロファイル ディスクを有効にします。前のセクション「ユーザー プロファイル ディスクの前提条件」を参照して、ユーザー ディスク共有を構成します。最大サイズとフォルダーの除外を構成し、具体的にユーザー プロファイルのどの部分をユーザー ディスクに格納するかを選択します。既定では、すべてのユーザー プロファイル データがユーザー ディスクに格納されます。
2. [OK] または [適用] をクリックして、設定をコレクションに適用します。

##### コレクションへの RemoteApp の公開

コレクションの作成と構成を完了したら、RDMS の [RemoteApp プログラム] タイルを使用して、コレクションに RemoteApp を公開できます。

コレクションに RemoteApp を公開する手順は次のとおりです。

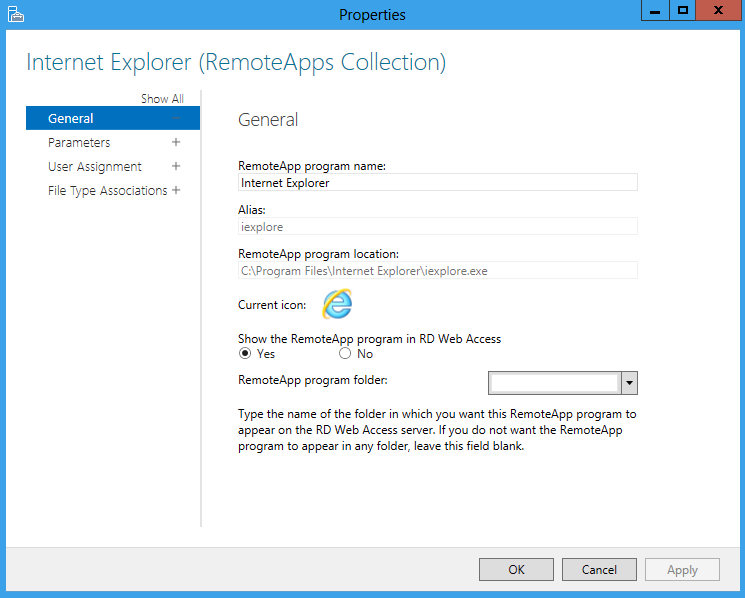
1. コレクション名をクリックして、コレクションの [プロパティ] ウィンドウにアクセスします。
2. [RemoteApp プログラム] の下にある [Publish RemoteApp Programs for the collection] リンクをクリックするか、[タスク] メニューの [RemoteApp プログラムの公開] をクリックします。
3. RDMS によって、コレクション内の RDSH サーバーに対するクエリが実行され、RemoteApp として公開できるインストール済みアプリケーションの一覧が表示されます。必要なアプリケーションが表示されない場合は、[Add another Program] をクリックして、必要な RemoteApp プログラムの場所を参照します。RemoteApp として公開する各インストール済みプログラムの左側のチェックボックスをそれぞれオンにして、[次へ] をクリックします。
4. RDMS に [概要] ページが表示され、設定を確認できます。RemoteApp を公開するには、[公開] をクリックします。
5. RemoteApp が公開されると、[Publishing Status] が [公開済み] に変更され、RemoteApp の隣に緑色のチェック マークが表示されます。

###### RemoteApp の構成

公開済みの RemoteApp を構成する手順は次のとおりです。

1. [RemoteApp プログラム] タイルに表示されている RemoteApp を右クリックして、[プロパティの編集] をクリックします。
2. RDMS に RemoteApp のプロパティが表示されます。各ページをクリックして、設定にアクセスします。

図 33: RemoteApp のプロパティ



1. [全般] ページで、RemoteApp の名前とリモート デスクトップ Web アクセスで RemoteApp が表示されるフォルダーを構成し、ユーザーに表示されるパスとアイコンを確認します。
2. RemoteApp の RDWeb フォルダーを構成するには、[Visibility in Web Access] が [はい] に構成されていることを確認してから、[フォルダー] フィールドの隣に RDWeb フォルダーの名前を入力します。フォルダーが存在しない場合は、自動的に作成されます。また、ドロップダウンからフォルダー名を選択するか、フォルダーの新しい名前を入力することで、既存のフォルダーを選択し、名前を変更できます。
3. [パラメーター] ページで、RemoteApp のコマンド ライン パラメーターがある場合は、それらを構成します。
4. [ユーザーの割り当て] ページで、RemoteApp へのアクセスを許可するユーザーとグループを構成します。既定では、すべてのユーザーが、コレクションで公開されたすべての RemoteApp に対してアクセス可能になります。
5. [ファイルの種類の関連付け] ページで、クライアント コンピューター上でこの RemoteApp と関連付けるファイルの関連付けをクリックします。

|  |  |
| --- | --- |
| 重要: | ファイルの種類の関連付けは、[RemoteApp とデスクトップ接続] フィードを使用して接続しているユーザーにのみ適用されます。RD Web アクセスまたは RDP ファイルによって接続しているユーザーは、ファイルの種類の関連付けを使用できません。 |

##### ユーザー接続の管理

コレクションの作成とコレクションへの RemoteApp の追加が完了すると、ユーザーは、RDWeb ページにログオンするか、または RemoteApp のフィードを購読することによって、そのコレクションに接続し、RemoteApp を実行できるようになります。ユーザーが RemoteApp フィードを購読すると、Windows 8 Consumer Preview コンピューターのスタート画面または Windows 7 コンピューターの [スタート] メニューにアプリケーションが表示されます。

###### RDWeb ページの使用

セッションまたは仮想デスクトップへの接続に使用される RDWeb ポータルには、次の URL を使用してアクセスできます。

https://<fqdn of RDWEB Server>/rdweb

既定の URL は Windows Server 2008 R2 から変わってません。このURLは構成ユーザー インターフェイスを使用してカスタマイズできます。

RDWeb の役割サービスのインストール後、この Web サイトが、自動生成された自己署名入りの証明書を使用するように構成されます。この証明書は RDWeb サイトへの SSL 接続に使用されます。また、RemoteApp の .rdp ファイルとデスクトップ仮想化コレクションの署名に使用することもできます。既定では、自己署名入りの証明書は、クライアント コンピューターで信頼できると見なされませんが、この Web サイトにアクセスするクライアント コンピューターの信頼されたルート証明書ストアにこの証明書をインストールすることによって、クライアントは、証明書の警告を受けることなく、RDWeb サイトにログオンできます。また、環境内のコレクションの署名にこの証明書が使用されている場合、クライアント コンピューターはこの証明書を信頼できる証明書と見なします。

**RDWeb の証明書の設定変更**

運用展開では、ドメインで信頼される証明書またはパブリックで信頼される証明書を使用するように RDWeb サイトを構成します。RD Web アクセスで使用する証明書を構成するには、RDMS 証明書管理ユーザー インターフェイスを使用します。このドキュメント内の先行するセクション「[証明書の管理](#_Certificate_Management)」では、Windows Server "8" Beta の RDS 環境におけるすべての証明書の変更プロセスについて説明しています。

###### RemoteApp とデスクトップ接続のフィードの使用

ユーザーは、RDWeb ページを使用する代わりに、RDWeb フィードを購読することによって、RemoteApp および仮想デスクトップにアクセスすることもできます。RemoteApp とデスクトップ接続のフィードには、RDWeb で利用可能な RemoteApp およびコレクションと同じものが含まれており、クライアント コンピューターの [スタート] メニューからこれらにアクセスできます。ユーザーは RemoteApp とデスクトップ接続のユーザー インターフェイスを使用してフィードに手動で接続できますが、管理者がグループ ポリシーで既定の接続の URL を構成することもできます。

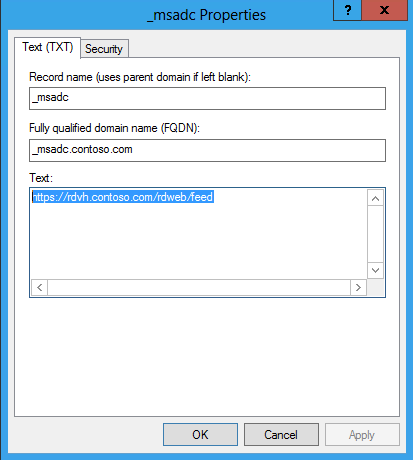
**手動構成**

ユーザーは、管理者から通知された URL を RemoteApp とデスクトップ接続のコントロール パネル インターフェイスに入力することによって、RemoteApp およびコレクションのフィードを手動で購読できます。また、Windows Server "8" Beta では、ユーザーが自分の電子メール アドレスを使用してフィードを購読する機能も追加しています。

ユーザーが自分の電子メール アドレスを使用してフィードを購読できるように DNS サーバーを構成する手順は次のとおりです。

1. DNS サーバーで、TXT 形式の DNS レコードを作成します。Microsoft DNS サーバーの場合は、DNS マネージャーを開き、ドメインの前方参照ゾーンをクリックして、[Other New Records] をクリックします。
2. レコードの種類として [テキスト (TXT)] を選択して、[レコードの作成...] をクリックします。レコード名を「\_msadc」として入力し、[テキスト] フィールドに RDWeb フィードの URL を入力します。Microsoft DNS サーバーでのレコードの作成例を次に示します。

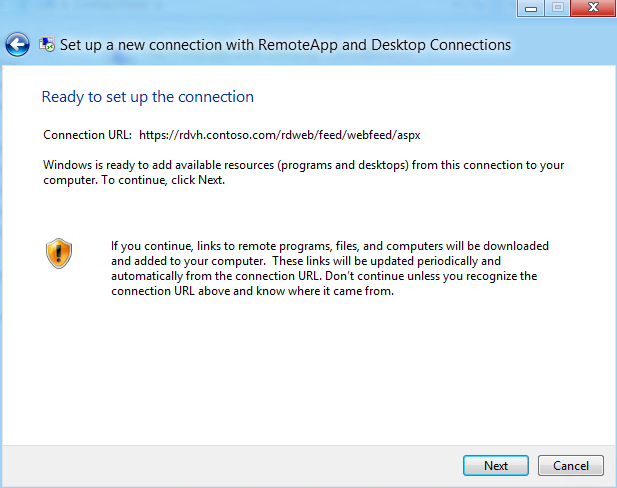
図 34: DNS TXT レコード



Windows 8 Consumer Preview または Windows 7 クライアント コンピューターでフィードへの接続をセットアップする手順は次のとおりです。

1. **コントロール パネル**を開き、RemoteApp を探します。[RemoteApp とデスクトップ接続の新しい接続の設定] リンクをクリックします。
2. 管理者に通知されたフィードの URL を入力するか、必要に応じて自分の電子メール アドレスを入力します。フィードの既定の URL は次の形式のものです。**https://<fqdn of rdweb server>/Rdweb/feed**
3. RDWeb サーバーとの通信に成功すると、[接続を設定する準備ができました] ページが表示されます。

図 35: フィードのセットアップ成功



1. [次へ] をクリックして、このフィードに使用するユーザーの資格情報を入力します。このフィードで利用可能な RemoteApp とデスクトップ接続がダウンロードされ、[スタート] メニューに表示されます。

**グループ ポリシーの使用**

グループ ポリシーを使用して、RemoteApp とデスクトップ接続のフィードの構成をユーザー アカウントに自動的に適用することもできます。"Specify Default Connection URL"は、Windows 8 Consumer Preview クライアントでのみ使用可能な新しいグループ ポリシーです。

グループ ポリシーを構成する手順は次のとおりです。

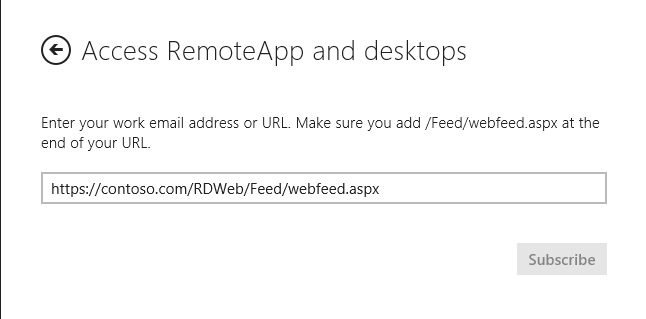
1. グループ ポリシーを開き、[ユーザーの構成]、[ポリシー]、[管理用テンプレート]、[Windows コンポーネント]、[リモート デスクトップ サービス]、[RemoteApp とデスクトップ接続] の順に展開します。
2. [Specify Default Connection URL] ポリシーを有効にし、フィードの URL をこのポリシーに入力することによって、ポリシーの設定を構成します。
3. このフィードにアクセスするユーザー アカウントまたはグループにこのポリシーを適用します。

**最新のリモート デスクトップ クライアントの使用**

最新の Metro スタイルのリモート デスクトップ クライアントを使用してフィード接続をセットアップするには、Windows 8 Consumer Preview クライアント コンピューターで以下の手順に従います。

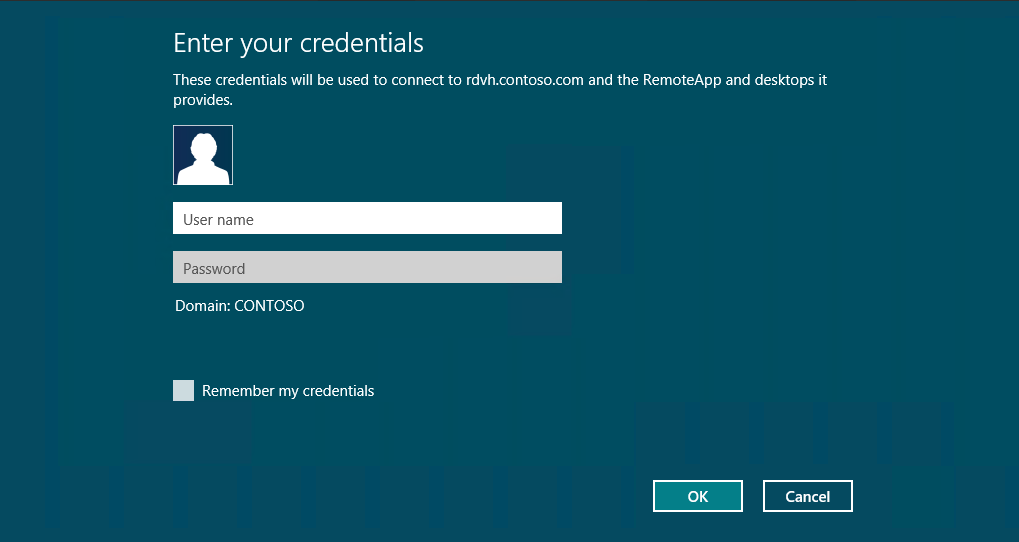
1. スタート画面からMetro スタイルの リモート デスクトップ クライアントを開きます。
2. [Access RemoteApp and Desktop Connections] リンクをクリックまたはタッチします。
3. ユーザーの電子メール アドレスまたはフィードの URL を入力します。

図 36: Metro スタイル クライアントのフィードのセットアップ



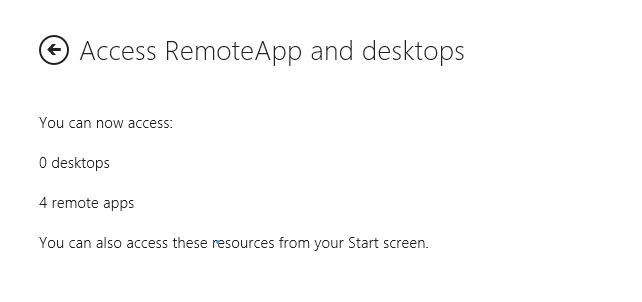
1. ドメインの資格情報を入力して、フィードにアクセスします。

図 37: フィードの資格情報



1. フィードに含まれているデスクトップと RemoteApp の数が表示されます。

図 38: フィードのコンテンツ



1. Metro スタイル RDC クライアントのホーム ページ上で、スタート画面に RemoteApp とデスクトップが表示されます。

図 39: スタート画面の RemoteApp



###### RDMS によるユーザーの管理

RDMS は、セッションまたは仮想デスクトップにログオンするすべてのユーザーと、環境内で作成されたあらゆるコレクションの一元的な管理ポイントを提供します。ユーザーの接続は展開レベルまたはコレクション レベルで管理できます。また、表示フィールドで接続を検索して、特定のデータを表示できます。

接続タイルは、展開ビューでもコレクション ビューでも同じです。各ユーザーについて表示するフィールドはカスタマイズできます。また、ユーザーの一覧では、並べ替えや、任意のフィールドに含まれるテキストの検索によるフィルター処理が可能です。管理者は、後から検索パラメーターにすばやくアクセスできるように、クエリを保存することもできます。

|  |  |
| --- | --- |
| 注意: | 表示フィールドのカスタマイズ、検索、およびクエリの保存手順は、RDMS 内のどのタイルでも同じです。 |

次の表は、既定のフィールドと、管理者によるカスタマイズが可能なフィールドを示しています。

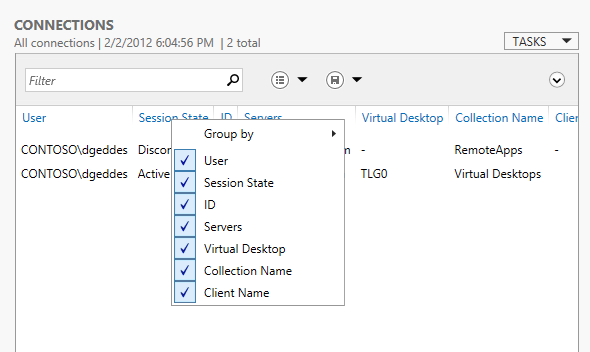
表 5: 接続一覧の表示フィールド

|  |  |  |
| --- | --- | --- |
| **フィールド リスト** | **フィールドの種類と表示データ** | **既定** |
| **ユーザー** | テキスト、ユーザー名 | x |
| **セッション状態** | テキスト、現在のセッションの状態 | x |
| **ID** | 数値、セッション ID | x |
| **サーバー** | テキスト、サーバーの FQDN | x |
| **仮想デスクトップ** | テキスト、ユーザーがログオンしている仮想マシンの名前 |  |
| **コレクション名** | テキスト、コレクションの名前 | x |
| **クライアント名** | テキスト、ユーザーのログオン元のクライアントの名前 |  |

**フィールドのカスタマイズ**

接続タイルに表示されるフィールドをカスタマイズするには、いずれかのフィールドを右クリックし、表示対象とする各フィールドのチェック ボックスをオンにします。次のスクリーンショットに例を示します。

図 40: フィールドのカスタマイズ



**クエリの作成と保存**

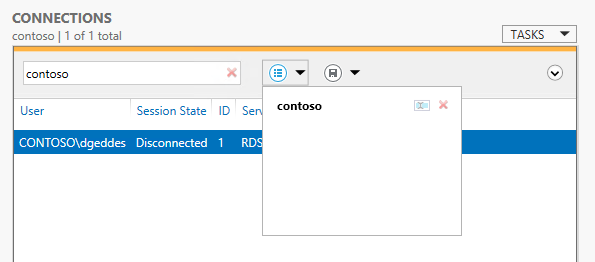
いずれかの表示フィールドを基準にセッションをフィルター処理するには、単に [フィルター] 検索ボックスにテキストを入力します。それにより、入力したテキストに基づいてセッションの一覧がフィルター処理されます。たとえば、ユーザー名にフィルターを適用するには、単に [フィルター] 検索ボックスに完全なユーザー名またはその一部を入力します。クエリを保存するには、[フィルター] 検索ボックスに検索条件を入力して、[保存] ボタンをクリックし、クエリの名前を入力して [OK] をクリックします。次のスクリーンショットに例を示します。

図 41: クエリの保存



クエリを実行して、セッションの一覧をフィルター処理するには、[クエリ] ボタンをクリックして、保存されているクエリを選択します。

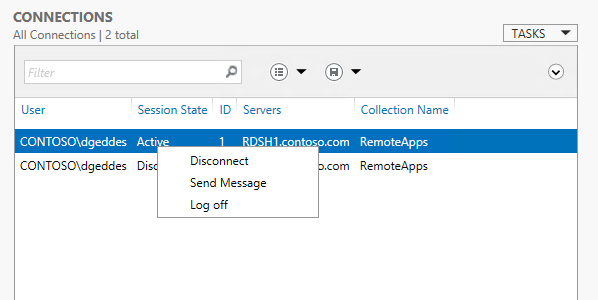
図 42: 保存されているクエリの実行



**セッションの管理**

一覧に表示されるセッションは、いずれも RDMS コンソールから管理できます。切断、メッセージの送信、セッションからのログオフを行うには、管理対象のセッションをクリックし、右クリックして、実行する操作をクリックします。

図 43: セッションの管理



###### 期限切れパスワードのサポート

ユーザーが、RDWeb を介して、または RDC クライアントを使用して直接、リモート デスクトップ環境にログオンしようとした場合、そのユーザーのパスワードが有効期限切れの場合、ログオンを拒否されます。Windows では、Ctrl + Alt + Delete キーなどの組み込みの方法を使用したパスワードの変更方法を提供していますが、インターネットから接続しているユーザーや、Windows オペレーティング システム上で動作する RDC クライアントを使用していないユーザーは、この種の方法を利用できません。

Windows Server "8" Beta の RD Web では、ユーザーが RD Web を介してログオンする場合、期限切れのパスワードを変更できます。ただし、この機能は既定では無効に設定されています。パスワード変更機能を有効にするには、管理者が web.config ファイルを編集して、RD Web のパスワード変更インターフェイスを有効化する必要があります。

RD Web のパスワード変更インターフェイスを有効化する手順は次のとおりです。

1. 管理者として RD Web サーバーにログオンし、管理用の Windows PowerShell またはコマンド プロンプトを開きます。
2. %SYSTEMROOT%\Web\Rdweb\Pages フォルダーに変更します。
3. [Windows Powershell] ウィンドウからメモ帳を実行して、Web.config という名前のファイルを開きます。
4. ファイル内の <configuration> の下にある PasswordChangeEnabled: というセクションを探します。

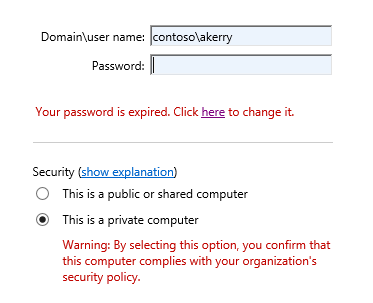
<!-- PasswordChangeEnabled:Provides password change page for users. Value must be "true" or "false" -->

<add key="PasswordChangeEnabled" value="false" />

1. 値を "false" から "true" に変更して、web.config ファイルを保存します。
2. この変更後、ユーザーは Web ページを再読み込みする必要があります。

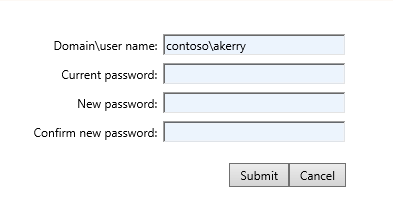
この変更を行った後、パスワードの期限が切れたユーザーが RD Web ページにログオンしようとすると、RD Web のパスワード変更ユーザー インターフェイスがアクティブになります。

図 44: パスワード変更のアクティブ化



ユーザーがリンクをクリックすると、パスワードを変更するためのオプションが表示されます。

図 45: パスワード変更 UI



##### サーバーの管理

RDS 環境に含まれるサーバーの管理は、RDMS 内の [ホスト サーバー] タイルで行います。サーバーはセッション ホスト サーバーまたは仮想化ホスト サーバーとして分類されます。このコンテキストにおいて、サーバーの管理とは、各ホストの仮想マシン数の監視と DRAIN モードの構成を指します。DRAIN モードは、以前はユーザー ログオン モードと呼ばれていたもので、サーバーがユーザーの接続は拒否し、管理者の接続は受け入れることを表します。通常、DRAIN モードは、サーバーでメンテナンス作業を実行するときに使用されます。

次の表は、既定のフィールドと、管理者によるカスタマイズが可能なフィールドを示しています。

表 6: ホスト サーバーのフィールド

|  |  |  |
| --- | --- | --- |
| **フィールド** | **フィールドの種類と表示データ** | **既定** |
| **FQDN** | テキスト、サーバーの完全修飾ドメイン名 |  |
| **サーバー** | テキスト、サーバーの短い名前 (NETBIOS) | x |
| **種類** | テキスト、セッション ホストまたは仮想化ホスト | x |
| **仮想デスクトップ** | 数値、RDVH サーバー上の VM 数 (RDSH サーバーの場合は該当しません) | x |
| **新しい接続の許可** | True/False、DRAIN モードのステータス (RDVH サーバーには該当しません) | x |
| **コレクション** | テキスト、サーバーが関連付けられているコレクション名 |  |

## リモート デスクトップ サービス セッション仮想化のアーキテクチャ

### 概要

以下のセクションには、Windows Server "8" Beta リモート デスクトップ サービスの機能を構成するサービス、モジュール、およびファイルの一覧が含まれます。アーキテクチャ図と、他のコンポーネント、役割、役割サービス、および機能に対する各機能の依存関係の一覧も示されています。各機能の実装の詳細とデータ形式の詳細、および各コンポーネントへのデータの入出方法についても、適宜説明します。

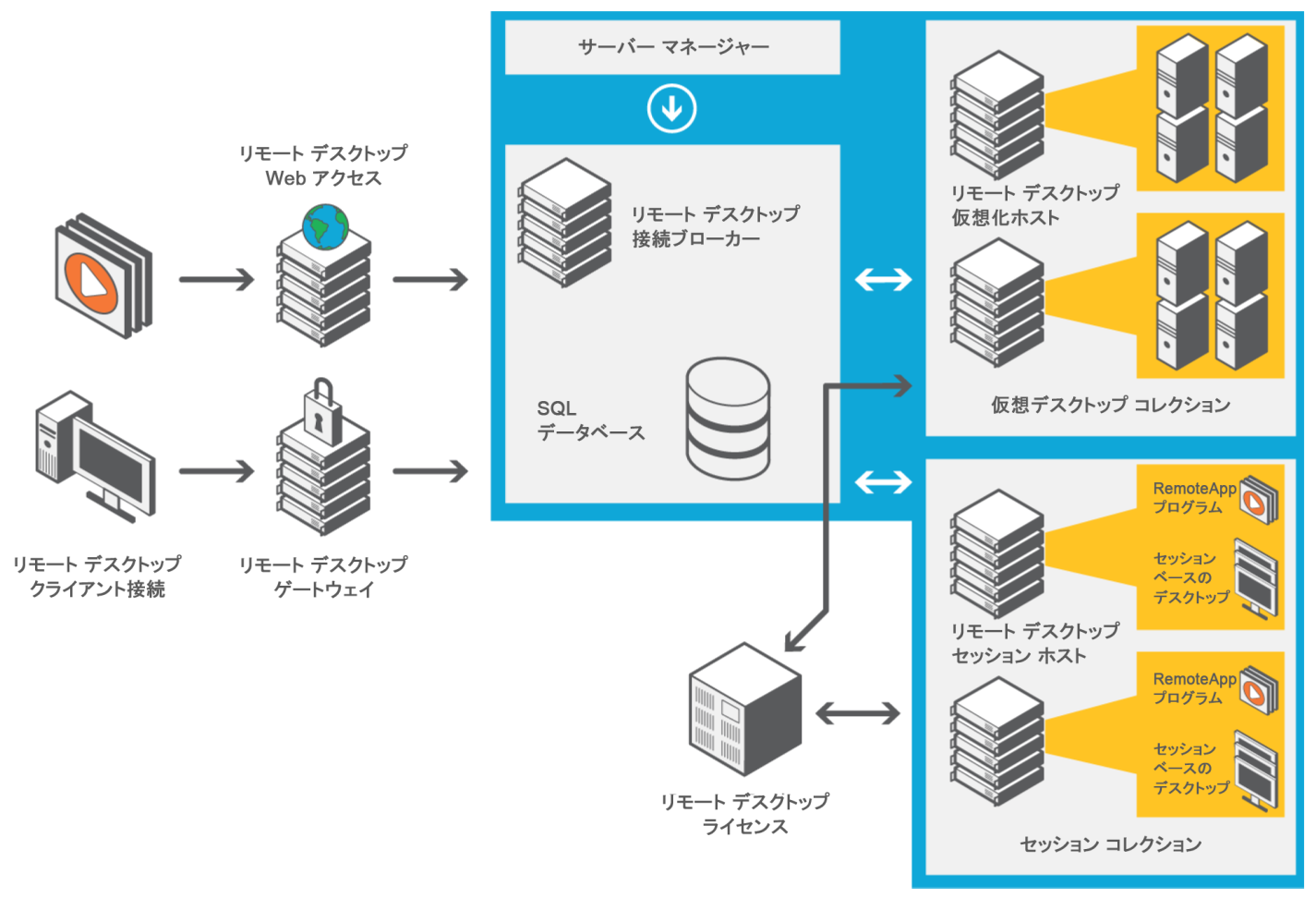
ここでは、以下のリモート デスクトップ サービスの役割サービスと機能のアーキテクチャについて説明します。

* リモート デスクトップ管理サービス (RDMS)
* リモート デスクトップ セッション ホスト (RDSH)
* リモート デスクトップ接続ブローカー (RDCB)
* リモート デスクトップ Web アクセス (RDWA)
* リモート デスクトップ ゲートウェイ (RDG)

#### 展開の概要

次の図は、Windows Server "8" Beta の RDS 環境にそれぞれの RDS 役割サービスがどのように位置付けられるかを示しています。

図 46: 展開の概要



#### リモート デスクトップ管理サービス

Windows Server "8" Beta では、リモート デスクトップの管理タスクを簡素化すると共に、リモート デスクトップ サービスのすべての役割サービスとシナリオの一元管理ソリューションを提供することを目的に設計されたリモート デスクトップ管理サービス (RDMS) およびユーザー インターフェイスを導入しました。RDMS では、インストールされている役割サービスごとに別の管理ツールを使用するのではなく、付属の統一ユーザー インターフェイスを使用してリモート デスクトップ サービス環境に含まれているすべてのサーバーの概要を表示できます。また、RDMS は、RDS 環境内の各サーバー用の管理インターフェイスも備えています。

Windows Server "8" Beta で RDS 展開を作成する際には、管理者は、サーバー マネージャーからリモート デスクトップ サービスのシナリオ ベースの展開ウィザードを実行します。展開プロセスでは、RD 接続ブローカー役割サービスをインストールするサーバーを選択する必要があります。このサーバーはRDMS サーバーになります。1 台の RDMS サーバーで、セッション仮想化またはデスクトップ仮想化のいずれかの、複数の種類のコレクションを管理できます。どのシナリオをインストールしたかに関係なく、シナリオ ベースのインストールが完了すると、以降のシナリオ ベースのインストールには、新しい RDMS サーバーではなく、既存の RDMS サーバーがウィザードによって自動的に選択されます。

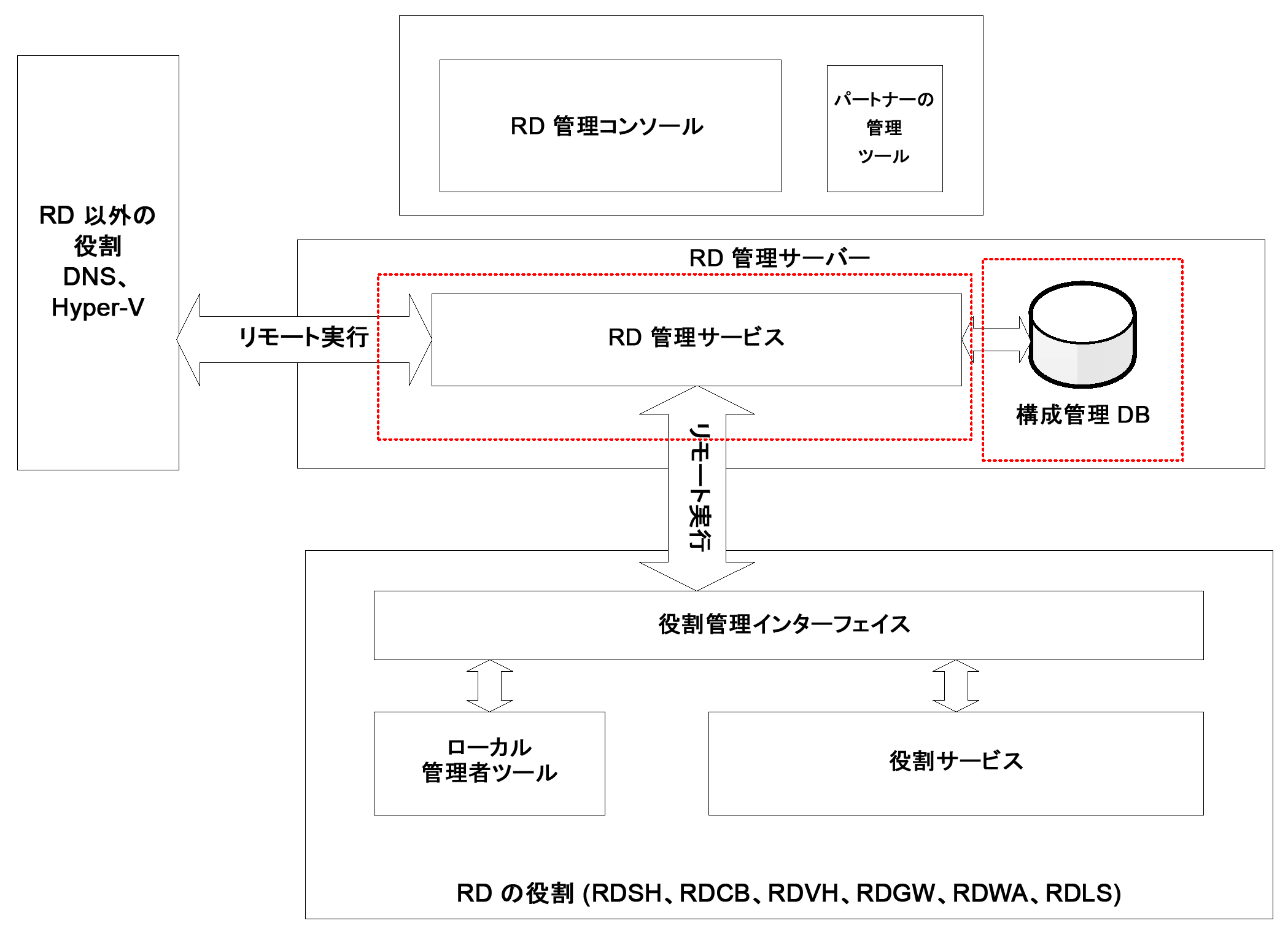
##### RDMS の基本

新しい Windows Server "8" Beta サーバー マネージャーのプラグインである RDMS ユーザー インターフェイスでは、検出プロセスによって、サーバー マネージャーのプールに追加された各コンピューター上にインストールされている役割サービスが検出されます。役割サービスが検出されると、RDMS によって、RDS 環境の基本的なトポロジの図と、環境内の各サーバーに関する情報 (サービス ステータス、関連イベント、パフォーマンス情報、各役割サービスに関するベスト プラクティス アナライザーの結果など) が表示されます。

##### アーキテクチャ

次の図は、RDMS のアーキテクチャの概要を示しています。

図 47: RDMS のアーキテクチャ



##### 主要モジュール/コンポーネント

###### サーバー マネージャーに読み込まれるもの

* RDS プラグイン — Microsoft.Windows.ServerManager.RDSPlugin.dll — メインの RDMS プラグイン DLL

###### RDMS サービスに読み込まれるもの

* rdcentraldbplugin.dll
* rddbobjectfactory.dll
* RDMS.dll — リモート デスクトップ管理サービス
* TSCPUBSvr.dll — RD 公開サービス

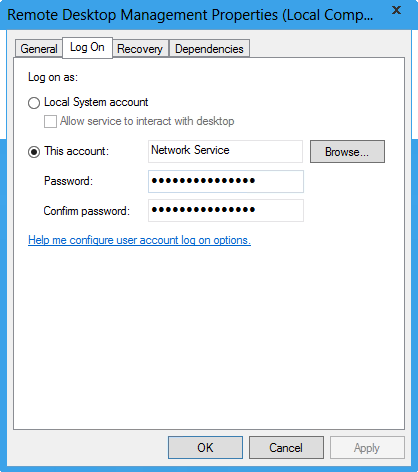
##### 依存関係

RDMS は RPC および Windows Internal Database に依存します。



##### サービスの詳細

RDMS サービスは NetworkServiceRemoteDesktopPublishing グループの共有 svchost で実行されます。この svchost は、RemoteApp およびデスクトップ接続の管理サービスと共有されます。RDMS サービスは [自動 (遅延開始)] オプションを使用し、ネットワーク サービス アカウントを使用してログオンするように構成されます。



#### 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 サーバーは、リモート デスクトップ サービス クライアントのために Windows ベースのプログラムまたは完全な Windows デスクトップをホストするサーバーです。ユーザーは RD セッション ホスト サーバーに接続して、プログラムを実行し、ファイルを保存し、そのサーバー上のネットワーク リソースを使用できます。ユーザーは企業ネットワーク内から、またはインターネットから、リモート デスクトップ接続または RemoteApp を使用して、RD セッション ホスト サーバーにアクセスできます。

ユーザーが RD セッション ホスト サーバー上のプログラムにアクセスすると、サーバー上でプログラムが実行されます。それぞれのユーザーは、各自のセッションのみを認識します。セッションはサーバー オペレーティング システムによって透過的に管理され、他のクライアント セッションとは独立したものになります。

各デバイス上ではなく RD セッション ホスト サーバー上にプログラムを展開すると、次のような多数のメリットがもたらされます。

* 企業全体のコンピューター デバイスに Windows ベースのプログラムを迅速に展開できます。これは、頻繁に更新されるプログラム、あまり使用されないプログラム、または管理の困難なプログラムがある場合に、特に役立ちます。
* ユーザーは RD セッション ホスト サーバー上で実行されているプログラムに、ホーム コンピューター、キオスク、オペレーティング システムやアプリケーションの要件を満たさないハードウェア、および Windows 以外のオペレーティング システムといったデバイスからアクセスできます。
* 一元化されたデータ ストアにアクセスする必要があるブランチ オフィスのワーカーは、RD セッション ホスト サーバー上のプログラムにリモートからアクセスすることで、より優れたプログラム パフォーマンスを得ることができます。データ集約型のプログラムは、低速接続用に最適化されたクライアント/サーバー プロトコルに対応していない場合があります。この種のプログラムは、多くの場合、通常の WAN 接続よりリモート デスクトップ サービス接続を使用したほうがパフォーマンスが向上します。

Windows Server "8" Beta のリモート デスクトップ セッション ホスト役割サービスのアーキテクチャは、Windows Server 2008 R2 の同サービスのアーキテクチャと似ています。フェアシェアのような新機能のサポートは追加されているものの、RDSH サービスの構成は前バージョンの Windows と同じです。

##### 主要モジュール/コンポーネント

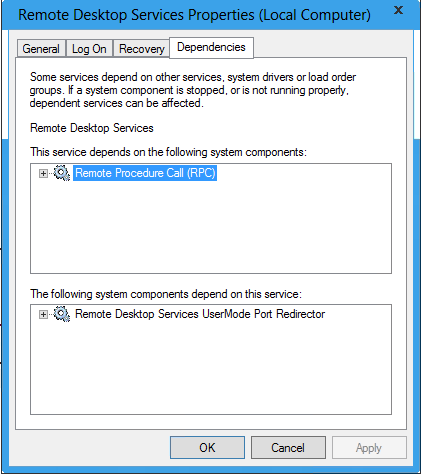
サービスによって読み込まれるもの:

* LSCSHostPolicy.dll — リモート デスクトップ仮想グラフィックス セッション ライセンス ホスト ポリシー
* mstlsapi.dll — リモート デスクトップ ライセンス
* RDSNetFS.dll — リモート デスクトップ サービス ネットワーク フェアシェア クライアント モジュール
* SDClient.dll — セッション ディレクトリ クライアント接続ハンドラー モジュール
* termsrv.dll — リモート デスクトップ セッション ホスト サーバー リモート接続マネージャー (メインのサービス DLL)
* tlscsp.dll — リモート デスクトップ サービスの暗号化ユーティリティ
* TSPKG.dll — Web サービス セキュリティ パッケージ
* tssdjet.dll — リモート デスクトップ セッション ホスト サーバー負荷分散 Jet RPC インターフェイス
* tssrvlic.dll — RD サーバー ライセンス ポリシー モジュール
* winsta.dll — WinStation ライブラリ
* wtsapi32.dll — Windows リモート デスクトップ セッション ホスト サーバー SDK API

##### 依存関係

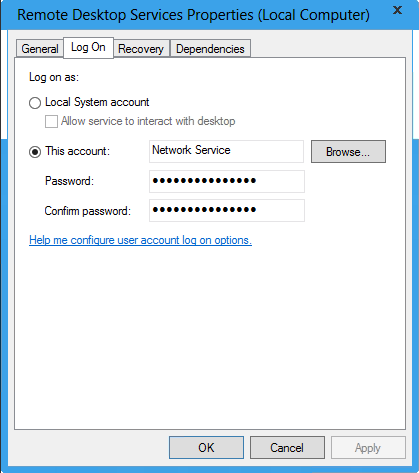
RDSH の役割は、RPC に依存するリモート デスクトップ サービスのサービスに実装されます。リモート デスクトップ サービスの UserMode ポート リダイレクターは、リモート デスクトップ セッション ホストに依存します。

図 48: RDSH 依存関係



##### サービスの詳細

リモート デスクトップ サービスのサービスは termsvcs グループの svchost インスタンスで実行されます。この svchost は単一のインスタンスで、他のサービスとは共有されません。リモート デスクトップ サービスのサービスは [手動] 開始オプションを使用し、ネットワーク サービス アカウントを使用してログオンするように構成されます。



|  |  |
| --- | --- |
| 重要: | リモート デスクトップ サービスは、手動で開始するように設定される唯一の RDS サービスです。これは、リモート デスクトップ サービスのアーキテクチャ上の理由から、このように設計されています。リモート デスクトップ サービスは、システムの起動時に、リモート デスクトップ システム ドライバーによって開始されます。RDS サービスの開始の種類を自動的に開始するように構成すると、リモート デスクトップ サービスおよび他の RDS サービスが正常に機能しなくなる可能性があります。 |

#### リモート デスクトップ接続ブローカー

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) は以前のターミナル サービス セッション ブローカー (TS セッション ブローカー) で、RemoteApp およびデスクトップ接続へのアクセスをユーザーに提供するために使用されます。RemoteApp およびデスクトップ接続は、RemoteApp プログラム、セッション ベースのデスクトップ、および仮想デスクトップに関する、単一の個人用に設定された集約的なビューをユーザーに提供します。RD 接続ブローカーは、RemoteApp やデスクトップ接続を使用してアクセスされる仮想デスクトップ、リモート デスクトップ セッション、および RemoteApp プログラムの負荷分散と既存のセッションへの再接続をサポートします。また、RD 接続ブローカーは、異なる RemoteApp プログラムをホストする可能性がある複数のリモート デスクトップ セッション ホスト (RD セッション ホスト) サーバーから、RemoteApp ソースを集約します。

##### Windows Server "8" Beta の新機能

リモート デスクトップ接続ブローカーは、Windows Server "8" Beta リモート デスクトップ環境の一元化された管理ソリューションとして機能します。セッション仮想化とデスクトップ仮想化環境は、両方とも、Windows Server "8" Beta の新機能である RDMS ユーザー インターフェイスによって管理されます。RDMS アーキテクチャのセクションで詳述されているように、Windows Server "8" Beta のすべてのリモート デスクトップ環境展開には、リモート デスクトップ管理サーバーとして機能するリモート デスクトップ接続ブローカー サーバーが最低 1 台は含まれます。Windows Server "8" Beta 以前は、接続ブローカーはリモート デスクトップ サービス環境の必須コンポーネントではありませんでした。

###### 接続ブローカーの高可用性

Windows Server 2003 でのセッション ディレクトリの導入以来、リモート デスクトップ接続ブローカー サービスはフェールオーバー クラスタリングの使用をサポートして、可用性に優れたソリューションを構築してきました。Windows Server 2008 R2 の高可用性接続ブローカーには、次のような欠点がありました。

* 一度に 1 つのアクティブ ブローカーのみ可能 (アクティブ/パッシブ構成)。
* 高可用性接続ブローカーのインストールおよび構成プロセスが複雑で、フェールオーバー クラスタリングに依存するため、手動の手順が多数存在した。
* DNS ラウンド ロビンは接続ブローカー サービスの状態がわからず、停止しているサーバーにユーザーをルーティングする可能性があった。

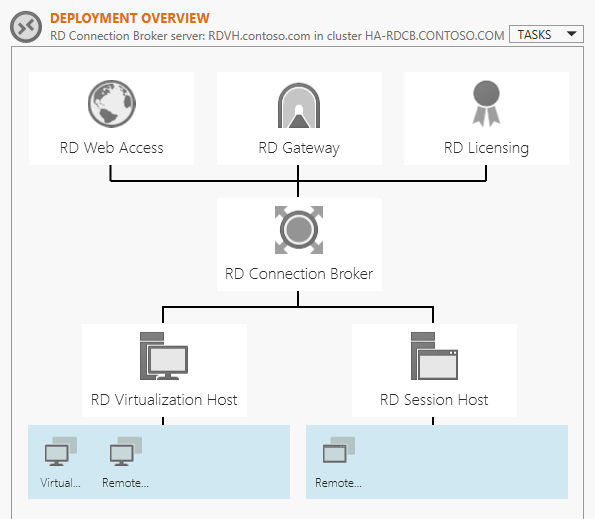
Windows Server "8" Beta の接続ブローカーでは、Windows Server 2008 R2 モデルと比較して、次の点が強化されています。

* 複数のアクティブな接続ブローカーがサポートされるようになった (アクティブ/アクティブ構成)。
* フェールオーバー クラスタリングは使用されなくなったので、セットアップと展開が大幅に簡素化され、ほとんどの構成が自動化されている。
* アクティブな接続ブローカーが複数あるので、接続ブローカー ノードの 1 つに障害が発生しても、クライアントは必ず、機能している接続ブローカーに確実にルーティングされる。

##### アーキテクチャの図

リモート デスクトップ サービス プラグインの [概要] タイルに示されるように、接続ブローカー サーバーはあらゆるリモート デスクトップ環境の主要コンポーネントで、一元化された管理サーバーとして機能します。

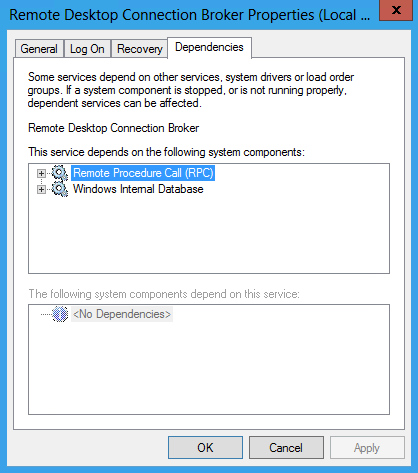
図 49: RDS 展開図



##### 依存関係

リモート デスクトップ接続ブローカー サービスは、RPC および Windows Internal Database に依存します。

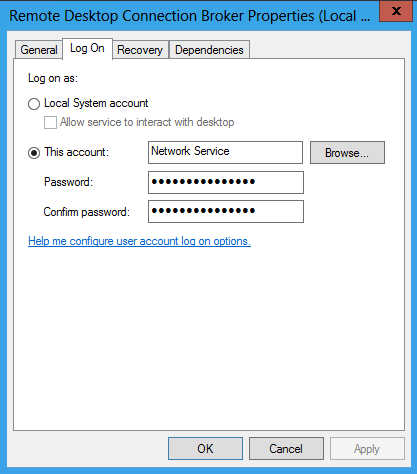
図 50: 接続ブローカーの依存関係



##### サービスの詳細

リモート デスクトップ接続ブローカー サービスは、tssdis.exe という自らのプロセス内で動作します。このサービスは [自動] 開始オプションを使用し、ネットワーク サービス アカウントを使用してログオンするように構成されます。

図 51: 接続ブローカー サービスの詳細



#### リモート デスクトップ Web アクセス

RD Web アクセスによってユーザーは、Windows 8 Consumer Preview を実行するコンピューターのスタート画面から、または Web ブラウザーを使用して、RemoteApp およびデスクトップ接続にアクセスすることが可能になります。RemoteApp およびデスクトップ接続は、RemoteApp プログラムと仮想デスクトップのカスタマイズされたビューをユーザーに提供します。

ユーザーが RemoteApp プログラムを開始すると、RemoteApp プログラムをホストする RD セッション ホスト サーバー上でリモート デスクトップ サービス セッションが開始されます。ユーザーが仮想デスクトップに接続すると、RD 仮想化ホスト サーバー上で実行されている仮想マシンへのリモート デスクトップ接続が作成されます。

RemoteApp およびデスクトップ接続を通して利用可能にする RemoteApp プログラムと仮想デスクトップを構成するには、Windows Server "8" Beta を実行するコンピューター上に RD 接続ブローカー役割サービスをインストールしてから、リモート デスクトップ サーバー マネージャー プラグインを使用してセッション仮想化またはデスクトップ仮想化のコレクションを構成する必要があります。

また、Web ブラウザーを通して RD セッション ホスト サーバー上の RemoteApp プログラムをユーザーに提供するだけの場合も、RD Web アクセスを使用できます。

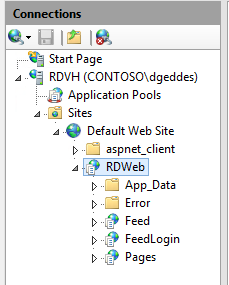
##### 依存関係

RD Web アクセスは Windows Server "8" Beta 上でサービスとして実行されるのではなく、インターネット インフォメーション サービス (IIS) に依存して [RD Web アクセス] ページをホストします。RD Web アクセスをインストールすると、必須コンポーネントとして IIS がインストールされ、RD Web アクセス サイトが自動的にインストールおよび構成されます。

##### RD Web サイト

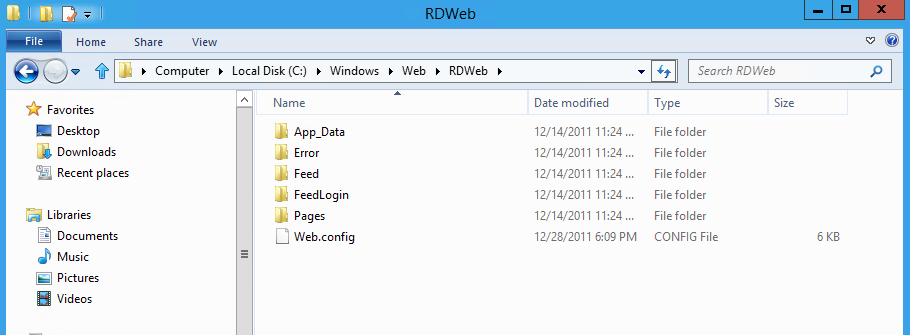
RD Web サイトは、IIS の [既定の Web サイト] の下にインストールされます。

図 52: RD Web サイト



既定では、ローカル ディスク上の Web サイト パスは C:\Windows\Web\RDWeb になります。

図 53: RDWeb パス



RD Web サイトの構成は、RD 接続ブローカー サーバーから RDMS を使用して実行され、IIS マネージャーによって制御された設定を変更する必要はほとんどありません。

|  |  |
| --- | --- |
| 警告: | IIS マネージャーを使用して RD Web サイトの既定の設定を変更すると、RD Web サイトとリモート デスクトップ サービスで予期しない動作が起こる可能性があります。 |

##### RD Web サイトのカスタマイズ

RD Web は、既定のゲートウェイ サーバー設定やリダイレクト設定を制御する機能など、RD Web インターフェイスをカスタマイズするためのオプションを多数備えています。これらの設定は、%SYSTEMROOT%\Web\RDWeb\Pages にある web.config ファイルを編集することで制御できます。

###### ローカル ヘルプの表示

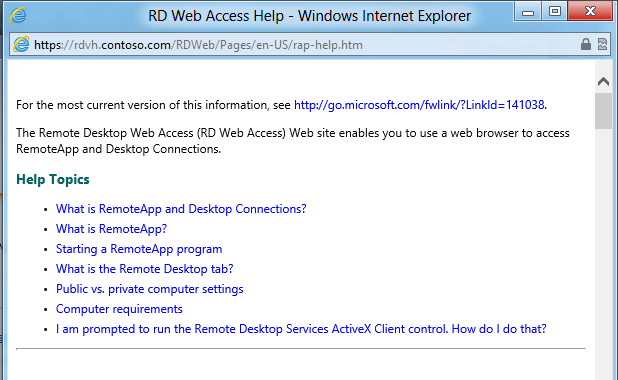
Web ベースのヘルプではなくローカル ヘルプをユーザーに表示するには、LocalHelp 値を編集して、false から true に値を変更します。

<!-- LocalHelp:Displays local help for users, instead of the web-based help. Value must be "true" or "false" -->

<add key="LocalHelp" value="false" />

この値を変更した場合は、ユーザーが RD Web ログイン ページの右上隅にある [ヘルプ] をクリックすると、Web ベースのファイルではなくローカル ヘルプが表示されます。

図 54: ローカル ヘルプを有効にした場合



###### [リモート PC に接続] タブの非表示化

コレクションで構成されたサーバー以外のサーバーへユーザーが RD Web を通して接続するのを防ぐために、RDWeb ページの [リモート PC に接続] タブをユーザーに対して非表示にすることができます。既定では、この設定は true に設定されており、[リモート デスクトップ] タブは表示されます。タブを非表示にするには、値を false に設定します。

<!-- ShowDesktops:Displays or hides the Remote Desktops tab. Value must be "true" or "false" -->

<add key="ShowDesktops" value="true" />

値を false に設定すると、ユーザーが RD Web ページにログオンしたときに、[リモート PC に接続] タブは表示されなくなります。

図 55: [リモート PC に接続] タブの非表示化



###### RD ゲートウェイの設定

[リモート PC に接続] タブが有効な場合は、リモート コンピューターへの接続時にゲートウェイ サーバーを使用するように RD Web を構成できます。ゲートウェイを指定するには、RD ゲートウェイ サーバーの名前を使用して次の値を編集します。

<!-- DefaultTSGateway:Admin can preset this to a given Gateway name, or set to "" for no gateway. -->

<add key="DefaultTSGateway" value="" />

|  |  |
| --- | --- |
| 重要: | Web ページには、ユーザーのためにゲートウェイ名は表示されません。また、RD ゲートウェイ サーバーが使用されていることを示すインジケーターなども表示されません。これらの設定は [リモート PC に接続] タブにのみ適用され、コレクションのゲートウェイ設定は RDMS UI で制御されます。 |

RD ゲートウェイ サーバーの既定の認証方法も、web.config の次のセクションを編集することで構成できます。

<!-- GatewayCredentialsSource:TS Gateway Authentication Type.

Admins can preset this.

0 = User Password

1 = Smartcard

4 = "Ask me later"

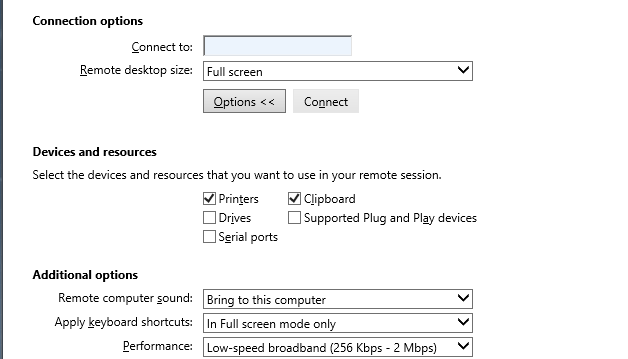
-->

<add key="GatewayCredentialsSource" value="0" />

###### デバイスとリソース

既定では、[リモート PC に接続] タブを使用して作成された接続上では、プリンターとクリップボードのみがリダイレクトされます。ユーザーが [オプション <<] ボタンをクリックすると、特定の接続のリダイレクト設定を変更できます。

図 56: リダイレクト設定



特定のリダイレクト オプションのそれぞれを既定で有効または無効になるように構成するには、web.config ファイルの次のセクションを編集します。

<!-- Devices and resources:Preset the Checkbox values to either true or false -->

<add key="xPrinterRedirection" value="true" />

<add key="xClipboard" value="true" />

<add key="xDriveRedirection" value="false" />

<add key="xPnPRedirection" value="false" />

<add key="xPortRedirection" value="false" />

###### LAN エクスペリエンスの既定の設定

Windows Server "8" Beta RD Web アクセスでは、LAN 接続エクスペリエンスを最適化するためのユーザーが選択可能な新しいオプションを表示できます。このオプションは RD Web ページの下部に表示され、管理者は web.config ファイルの次のセクションを使用して制御できます。

<!-- Checkbox to opt for optimized LAN experience -->

<add key="ShowOptimizeExperience" value="false" />

<add key="OptimizeExperienceState" value="false" />

この値は既定では false に設定されていますが、true に変更すると、Web ページの下部に次のチェックボックスが表示されます。また、この LAN エクスペリエンス チェックボックスは、既定で有効になるように設定することもできます。

図 57: LAN エクスペリエンス チェックボックス



#### リモート デスクトップ ゲートウェイ

リモート デスクトップ ゲートウェイ (RD ゲートウェイ) 役割サービスによって、許可されたリモート ユーザーは、リモート デスクトップ接続 (RDC) クライアントの実行が可能な任意のインターネット接続デバイスから社内ネットワークやプライベート ネットワーク上のリソースに接続できます。この場合、ネットワーク リソースは、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) サーバー、RemoteApp プログラムを実行する RD セッション ホスト サーバー、またはリモート デスクトップが有効に設定されているコンピューターです。

RD ゲートウェイは、RDP over HTTPS を使用して、インターネット上のリモート ユーザーと生産性向上アプリケーションを実行する内部ネットワーク リソースとの間で、セキュリティで保護された暗号化接続を確立します。

##### RD ゲートウェイを使用する理由

RD ゲートウェイは、次のような多数の利点をもたらします。

* RD ゲートウェイによってリモート ユーザーは、仮想プライベート ネットワーク (VPN) 接続を使用することなく、暗号化接続を使用してインターネット経由で内部ネットワーク リソースに接続することが可能になります。
* RD ゲートウェイは、特定の内部ネットワーク リソースに対するアクセスを制御することが可能な、包括的なセキュリティ構成モデルを提供します。RD ゲートウェイは、すべての内部ネットワーク リソースに対するリモート ユーザー アクセスを許可するのではなく、ポイント ツー ポイントの RDP 接続を提供します。
* RD ゲートウェイによってほとんどのリモート ユーザーは、ネットワーク アドレス変換器 (NAT) を越えて、ファイアウォールの内側のプライベート ネットワークにホストされた内部ネットワーク リソースに接続することが可能になります。RD ゲートウェイを使用すると、このシナリオのために RD ゲートウェイ サーバーまたはクライアントの追加構成を実行する必要はなくなります。

Windows Server 2008 のリリース前は、リモート ユーザーがファイアウォールや NAT を越えて内部ネットワーク リソースに接続するのがセキュリティ対策によってよく妨げられていました。この理由は、RDP 接続に使用されるポート 3389 は、通常はネットワーク セキュリティのためにブロックされているからです。RD ゲートウェイは、HTTP Secure Sockets Layer/トランスポート層セキュリティ (SSL/TLS) トンネルを使用して、代わりにポート 443 に RDP トラフィックを送信します。ほとんどの企業はインターネット接続を有効にするためにポートを 443 を開くので、RD ゲートウェイはこのネットワーク設計を利用して、複数ファイアウォールを越えたリモート アクセス接続を提供します。

* リモート デスクトップ ゲートウェイ マネージャーを使用すると、リモート ユーザーが内部ネットワーク リソースに接続するために満たす必要がある条件を定義する承認ポリシーを構成できます。たとえば、次の項目を指定できます。
  + だれが内部ネットワーク リソースに接続できるか (つまり、接続できるユーザー グループ)
  + どのネットワーク リソース (コンピューター グループ) にユーザーが接続できるか
  + クライアント コンピューターは Active Directory セキュリティ グループのメンバーでなければならないかどうか
  + デバイス リダイレクトが許可されるかどうか
  + クライアントはスマート カード認証とパスワード認証のどちらを使用する必要があるか、またはいずれかの方法を使用できるかどうか
* さらにセキュリティを強化するためにネットワーク アクセス保護 (NAP) を使用するように RD ゲートウェイ サーバーおよびリモート デスクトップ サービス クライアントを構成できます。NAP は、Windows Server "8" Beta、Windows Server® 2008 R2、Windows Server® 2008、Windows® 7、Windows Vista®、および Windows® XP Service Pack 3 に含まれる正常性ポリシーの作成、適用、および修復テクノロジです。システム管理者は NAP を使用して、ソフトウェア要件、セキュリティ更新プログラムの要件、必要なコンピューター構成といった正常性要件を適用できます。

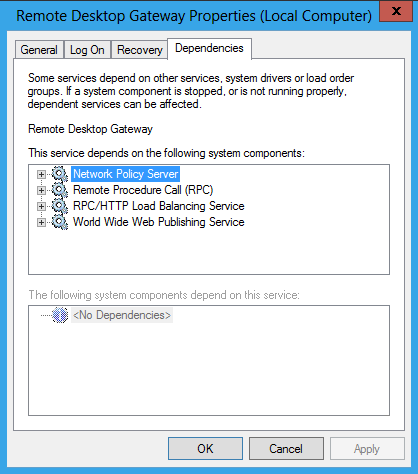
|  |  |
| --- | --- |
| 注意: | RD ゲートウェイが NAP を適用する場合、Windows Server "8" Beta、Windows Server 2008 R2、または Windows Server 2008 を実行しているコンピューターは NAP クライアントとして使用できません。RD ゲートウェイが NAP を適用する場合、NAP クライアントとして使用できるのは、Windows 8 Consumer Preview、Windows 7, Windows Vista、または Windows XP SP3 を実行しているコンピューターのみになります。 |

* RD ゲートウェイ サーバーをMicrosoft Forefront Threat Management Gateway (TMG) サーバーと共に使用することで、セキュリティを強化できます。このシナリオでは、境界ネットワークではなくプライベート ネットワークに RD ゲートウェイ サーバーをホストし、境界ネットワークに TMG サーバーをホストします。リモート デスクトップ サービス クライアントと TMG サーバーの間の Secure Sockets Layer (SSL) 接続は、インターネットに接続する TMG サーバーで終端できます。
* リモート デスクトップ ゲートウェイ マネージャーは、RD ゲートウェイ サーバーの状態とイベントの監視に役立つツールを提供します。リモート デスクトップ ゲートウェイ マネージャーを使用することで、監査のために監視したいイベント (RD ゲートウェイ サーバーへの接続試行の失敗など) を指定できます。

##### 依存関係

RD ゲートウェイ サービスは、ネットワーク ポリシー サーバー、RPC、RPC/HTTP 負荷分散サービス、および World Wide Web 発行サービスに依存します。

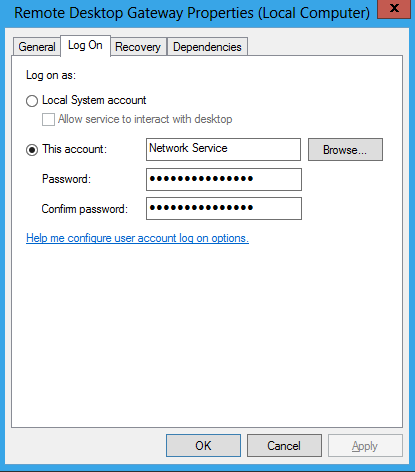
図 58: RD ゲートウェイの依存関係



##### サービスの詳細

RD ゲートウェイ サービスは tsgateway グループの単一の svchost インスタンスで実行されます。この svchost は他のサービスとは共有されません。RD ゲートウェイ サービスは [自動 (遅延開始)] オプションを使用し、ネットワーク サービス アカウントを使用してログオンするように構成されます。

図 59: RD ゲートウェイのログオン



##### データ フロー

次の表に、Windows Server "8" Beta を使用した接続シーケンスおよび動作の詳細を示します。

表 7: RDG UDP 接続シーケンス マトリックス

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | **RDS サーバー — WS2008/R2** | | **RDS サーバー — WS 08** |
| **接続性 (従来の RDG サーバー ファームを使用)** | RDC 7 |  | |  |
| RDC 8 | RDC クライアントは UDP を開始しません。 | | RDC クライアントはエラーを返し、接続は TCP に戻ります。 |
| **接続性 (ws08 RDG ファームを使用)** | RDC 7 |  | |  |
| RDC 8 (ポートがブロックされている場合) | RDC クライアントは UDP を開始しません。 | | RDC クライアントはエラーを返し、TCP に戻ります。 |
| RDC 8 (ポートが開いている場合) | RDC クライアントは UDP を開始しません。 | | UDP 接続は成功します。\* |
| \* 管理者が UDP をオンにした場合のみ成功します。 | | | |
| **UX エクスペリエンス — UDP 成功/失敗シナリオ** | 自動再接続 | |  | サポートされています。 |
| WebSSO | |  | サポートされています。 |
| 接続時間 | |  | 増加しません。 |
| RDweb/シェル/ワークスペースを使用した接続 | |  | サポートされています。 |

管理者は、UDP サポート (ファイアウォール ポートの転送規則や、ネットワーク ロード バランサーが使用されている場合はその IP アフィニティ設定など) を明示的に構成する必要があります。リモート デスクトップ ゲートウェイの管理者エクスペリエンスはシンプルかつシームレスで、メンテナンス オーバーヘッドは低く抑えられています。次の表に、UDP トランスポートの追加によってリモート デスクトップ ゲートウェイの新機能や既存の機能のサポートがどのような影響を受けるかを示します。

表 8: RDG の管理者エクスペリエンス

|  |  |  |  |
| --- | --- | --- | --- |
| **新しいトランスポート** | | **管理者エクスペリエンス** | **UI/向上点** |
| **展開**  **シナリオ** | アップグレード | UDP サポートは既定でオフになっています。UDP 設定ポート、ファイアウォールのポート転送規則、およびロード バランサーの IP アフィニティ設定を明示的に構成する必要があります。 | N/A |
| 新規 | サーバー マネージャーのセットアップ ウィザードから UDP を構成します。 | サーバー マネージャー UI で UDP を構成します。 |
| **機能の 類似性** | 監視 | サポートされています。 | RDG スナップイン UI が進化しています。 |
| アイドル/セッション タイムアウト (マウス/キーボード ストローク) | N/A |  |
| 同意の署名 | N/A |  |
| セキュリティで保護されたデバイス リダイレクト | N/A |  |
| PAA フレームワーク | N/A |  |
| CAP/RAP 承認 | RAP は特定の宛先ポート上で UDP プロトコルをサポートする必要があります。 | UI は UDP ポートをサポートする必要があります。 |
| ブリッジング | N/A |  |
| サーバー認証 | サポートされています。 |  |
| 外部 NIC 上の UDP  リスナーの構成 | サポートされています。 | UI が変更されています。 |
| NAP 修復 | N/A |  |
| ファーム モード | サポートされています。 | 新しいトランスポートの UI はありません。 |
| **サポートされていない機能** | DNS RR 負荷分散 | サポートされていません。 | BPA 警告が表示されます。 |
| IP アフィニティなしの NLB | サポートされていません。 | IP アフィニティが設定されていない場合は、スナップイン警告が表示されます。 |
| **高度な機能セット** | Cookie 負荷分散 | サポートされていません。 |  |
| **RPC 設定** | RPC と項目を開く操作 (M2 で変更予定) | サポートされています。 |  |

## リモート デスクトップ サービスのトラブルシューティング

### リモート デスクトップ サービスのトラブルシューティングの概要

以下のセクションでは、リモート デスクトップ サービスの問題をトラブルシューティングする際に収集する必要があるデータについて説明するほか、利用可能なトラブルシューティング ツールの一部について説明します。トラブルシューティング ツールの使い方のチュートリアルも提供します。

#### RDS ログおよびトレース

Windows Server "8" Beta のリモート デスクトップ サービス コンポーネントに含まれるログ ファイル、トレース ログ、およびイベント ログは、セッション仮想化およびデスクトップ仮想化のシナリオで発生する問題のトラブルシューティングを実行する際に役立ちます。以下の表では、各ログの名前と場所の詳細をまとめます。また、以降のセクションでは、それぞれのシナリオで収集するログと、それらを有効にする方法を詳述します。

##### テキスト ログ ファイル

以下のテキスト ファイルは、リモート デスクトップ サービスの問題をトラブルシューティングする際に役立ちます。

表 9: テキスト ログ ファイル

|  |  |
| --- | --- |
| ログ ファイル名 | パス |
| RDMSDeploymentUI.txt | %windir%\Logs |
| RDMSUI-trace.log | %temp% (通常は \users\<username>\appdata\local\temp) |

##### イベント ログ

以下のイベント ログも、リモート デスクトップ サービスの問題をトラブルシューティングする際に役立ちます。

表 10: イベント ログ

|  |  |
| --- | --- |
| イベント ログ | パス |
| RDMS-UI デバッグ ログ | アプリケーションとサービス ログ\Microsoft\Windows\RDMS-UI\デバッグ |
| ターミナル サービス セッション ブローカー 管理、分析、デバッグ、および操作ログ | アプリケーションとサービス ログ\Microsoft\Windows\TerminalServices-SessionBroker |
| ターミナル サービス セッション ブローカー クライアント管理、分析、デバッグ、および操作ログ | アプリケーションとサービス ログ\Microsoft\Windows\TerminalServices-SessionBroker-Client |
| ターミナル サービス TSV VMHostAgent  管理、分析、デバッグ、および操作ログ | アプリケーションとサービス ログ\Microsoft\Windows\TerminalServices-TSV-VmHostAgent |

#### RDMS UI トレースの有効化

シナリオ ベースのインストールやコレクションの作成で発生した問題をトラブルシューティングする際は、RDMS UI ログを有効にする必要があります。RDMS UI ログは、イベント ビューアーを使用し、SYSTEM 環境変数を接続ブローカー (RDMS) サーバーに追加することで、有効にする必要があります。

RDMS UI ログとイベント ログを有効にする手順は次のとおりです。

1. 管理者権限で コマンド プロンプトを開き、**RDMSUI\_TRACING** という名前のシステム環境変数を作成して、値を **1** に設定します。
2. 「servermanager」と入力してから **Enter** キーを押して、同じ コマンド プロンプト ウィンドウから**サーバー マネージャー**を起動します。
3. イベント ビューアーを開き、メニュー バーで [表示] をクリックしてから [分析およびデバッグ ログの表示] をクリックします。
4. イベント ビューアーで [アプリケーションとサービス ログ\Microsoft\Windows\RDMS-UI\デバッグ] に移動します。デバッグ ログを右クリックして [ログの有効化] をクリックします。

### シナリオ ベースのインストールのトラブルシューティング

シナリオ ベースの展開は、IT 管理者が RDS シナリオを迅速に展開できるように、複数のリモート サーバーへの役割サービスと機能のインストールと構成を簡素化することを目的として設計されています。IT 管理者は新しい Windows Server "8" Beta サーバー マネージャーとサーバー プールの概念を使用することで、1 つのユーザー インターフェイスから複数コンピューター上に役割サービスをインストールおよび構成できるほか、必要に応じて再起動も実行できます。リモート インストールおよび構成機能は、Windows に組み込まれた Powershell およびリモート管理テクノロジに基づいています。また、サーバー マネージャーのシナリオ ベースの展開プロセスでは、インストールおよび構成プロセスの各ステップに対する詳細なログ ファイルを利用します。

#### RDMSDeploymentUI ログの使用

シナリオ ベースの展開時に実行したインストールおよび構成アクション、およびインストール プロセス時に下されたロジックの決定は、すべて RDMSDeploymentUI.txt ファイルに記録されます。このログ ファイルは、次のパスに存在します。

c:\Windows\Logs\RDMSDeploymentUI.txt

このログ ファイルには、管理されているすべてのサーバー、およびインストールおよび構成中の展開の種類が示されます。ログ ファイルの例を以下に示します。

ServerManager.exe Information: 0 : 19/08/2011 18:37:29.94: DeploymentContext: (public)PopulateSMPool...

ThreadId=12

ServerManager.exe Information: 0 : 19/08/2011 18:37:29.94: DeploymentContext: Add Server 'RDMS2.contoso.com' to SMPool.

ThreadId=12

ServerManager.exe Information: 0 : 19/08/2011 18:37:29.94: DeploymentContext: Add Server 'DG-RFX-MAIN.contoso.com' to SMPool.

ThreadId=12

ServerManager.exe Information: 0 : 19/08/2011 18:37:29.94: RDWorkloadWizardPlugin: IRolePlugin.Initialize...

ThreadId=12

ServerManager.exe Information: 0 : 19/08/2011 18:37:29.94: RDWorkloadWizardPlugin: IScenarioBasedPlugin.InitializePluginData...

ThreadId=1

ServerManager.exe Information: 0 : 19/08/2011 18:37:29.94: RDWorkloadWizardPlugin: Tracking service is being registered...

ThreadId=1

ServerManager.exe Information: 0 : 19/08/2011 18:37:29.94: RDWorkloadWizardPlugin: get ServiceProvider...

ThreadId=1

ServerManager.exe Information: 0 : 19/08/2011 18:37:29.94: RDWorkloadWizardPlugin: IScenarioBasedPlugin.PopulateWizard...

ThreadId=1

ServerManager.exe Information: 0 : 19/08/2011 18:37:29.99: RDMS2 is domain joined.

ThreadId=1

ServerManager.exe Information: 0 : 19/08/2011 18:37:29.99: Following RDManagement servers present in the server pool.

ThreadId=1

ServerManager.exe Information: 0 : 19/08/2011 18:37:29.99: RDMS2.contoso.com

ThreadId=1

ServerManager.exe Information: 0 : 19/08/2011 18:37:37.21: Joined nodes count on RDMS2.contoso.com server: 2

ThreadId=13

ServerManager.exe Information: 0 : 19/08/2011 18:37:37.21: Virtual desktop deployment present on RDMS2.contoso.com server? True

ThreadId=13

ServerManager.exe Information: 0 : 19/08/2011 18:37:37.21: Shared desktop present on RDMS2.contoso.com server? False

ThreadId=13

ServerManager.exe Information: 0 : 19/08/2011 18:37:47.37: Web access server RDMS2.contoso.com is present on Rdms server RDMS2.contoso.com

ThreadId=1

ServerManager.exe Information: 0 : 19/08/2011 18:38:24.29: DeploymentContext: (public)PopulateSMPool...

ThreadId=30

ServerManager.exe Information: 0 : 19/08/2011 18:38:24.29: DeploymentContext: Add Server 'RDMS2.contoso.com' to SMPool.

ThreadId=30

ServerManager.exe Information: 0 : 19/08/2011 18:38:24.29: DeploymentContext: Add Server 'DG-RFX-MAIN.contoso.com' to SMPool.

ThreadId=30

ServerManager.exe Information: 0 : 19/08/2011 18:38:24.29: DeploymentContext: Add Server 'RDSH1.contoso.com' to SMPool.

ThreadId=30

ServerManager.exe Information: 0 : 19/08/2011 18:38:24.29: DeploymentContext: Add Server 'RDSH2.contoso.com' to SMPool.

ThreadId=30

ServerManager.exe Information: 0 : 19/08/2011 18:38:24.29: RDWorkloadWizardPlugin: IRolePlugin.Initialize...

ThreadId=30

ServerManager.exe Information: 0 : 19/08/2011 18:38:24.29: RDWorkloadWizardPlugin: IScenarioBasedPlugin.InitializePluginData...

ThreadId=1

ServerManager.exe Information: 0 : 19/08/2011 18:38:24.29: RDWorkloadWizardPlugin: Tracking service is being registered...

ThreadId=1

ServerManager.exe Information: 0 : 19/08/2011 18:38:24.29: RDWorkloadWizardPlugin: get ServiceProvider...

ThreadId=1

ServerManager.exe Information: 0 : 19/08/2011 18:38:24.29: RDWorkloadWizardPlugin: IScenarioBasedPlugin.PopulateWizard...

ThreadId=1

ServerManager.exe Information: 0 : 19/08/2011 18:38:24.31: RDMS2 is domain joined.

ThreadId=1

ServerManager.exe Information: 0 : 19/08/2011 18:38:24.31: Following RDManagement servers present in the server pool.

ThreadId=1

ServerManager.exe Information: 0 : 19/08/2011 18:38:24.31: RDMS2.contoso.com

ThreadId=1

ServerManager.exe Information: 0 : 19/08/2011 18:38:26.19: Joined nodes count on RDMS2.contoso.com server: 2

ThreadId=17

ServerManager.exe Information: 0 : 19/08/2011 18:38:26.19: Virtual desktop deployment present on RDMS2.contoso.com server? True

ThreadId=17

ServerManager.exe Information: 0 : 19/08/2011 18:38:26.19: Shared desktop present on RDMS2.contoso.com server? False

ThreadId=17

ServerManager.exe Information: 0 : 19/08/2011 18:38:30.00: Web access server RDMS2.contoso.com is present on Rdms server RDMS2.contoso.com

ThreadId=1

ServerManager.exe Information: 0 : 19/08/2011 18:38:36.58: RDSH1.contoso.com is domain joined.

ThreadId=34

ServerManager.exe Information: 0 : 19/08/2011 18:38:36.63: The current user is an admin on the server RDSH1.contoso.com

ThreadId=34

ServerManager.exe Information: 0 : 19/08/2011 18:38:36.68: Selected server RDSH1.contoso.com is Win8 server.

ThreadId=34

ServerManager.exe Information: 0 : 19/08/2011 18:38:38.88: Selected server RDSH1.contoso.com don't have pending reboots.

ThreadId=34

ServerManager.exe Information: 0 : 19/08/2011 18:38:38.88: Selected server RDSH1.contoso.com is not a localhost.

ThreadId=34

ServerManager.exe Information: 0 : 19/08/2011 18:38:38.97: RDSH2.contoso.com is domain joined.

ThreadId=34

ServerManager.exe Information: 0 : 19/08/2011 18:38:39.01: The current user is an admin on the server RDSH2.contoso.com

ThreadId=34

ServerManager.exe Information: 0 : 19/08/2011 18:38:39.06: Selected server RDSH2.contoso.com is Win8 server.

ThreadId=34

ServerManager.exe Information: 0 : 19/08/2011 18:38:41.14: Selected server RDSH2.contoso.com don't have pending reboots.

ThreadId=34

ServerManager.exe Information: 0 : 19/08/2011 18:38:41.14: Selected server RDSH2.contoso.com is not a localhost.

ThreadId=34

ServerManager.exe Information: 0 : 19/08/2011 18:38:46.33: User selected paramters for shared desktop scenario deployment.

ThreadId=1

ServerManager.exe Information: 0 : 19/08/2011 18:38:46.33: Is Rdms server already exists: True

ThreadId=1

ServerManager.exe Information: 0 : 19/08/2011 18:38:46.33: Rdms server : RDMS2.contoso.com

ThreadId=1

ServerManager.exe Information: 0 : 19/08/2011 18:38:46.33: Is web access server already exists on Rdms server: True

ThreadId=1

ServerManager.exe Information: 0 : 19/08/2011 18:38:46.34: Web access server : RDMS2.contoso.com

ThreadId=1

ServerManager.exe Information: 0 : 19/08/2011 18:38:46.34: RD Session Host servers :

ThreadId=1

ServerManager.exe Information: 0 : 19/08/2011 18:38:46.34: RDSH1.contoso.com

ThreadId=1

ServerManager.exe Information: 0 : 19/08/2011 18:38:46.34: RDSH2.contoso.com

ThreadId=1ServerManager.exe Information: 0 : 19/08/2011 17:05:10.27: NIC: DG-RFX-MAIN.contoso.com >> Broadcom NetXtreme Gigabit Ethernet

ThreadId=1

ServerManager.exe Information: 0 : 19/08/2011 17:05:13.97: User selected paramters for virtual desktop scenario deployment.

シナリオ ベースの展開の完了後に分析できるように、ログではプレーン テキストと読みやすい情報が使用されます。

##### ログの分析

RDMSDeploymentUI.txt には、シナリオ ベースの展開プロセスで実行されたアクションと下されたロジックの決定がすべて表示されます。ログの先頭には、サーバー マネージャー プールで利用可能なサーバーが検出されたことと、プールの各サーバーで現在どの役割サービスが実行されているかが示されます。

ServerManager.exe Information: 0 : 19/08/2011 18:37:37.21: Joined nodes count on RDMS2.contoso.com server: 2

ThreadId=13

ServerManager.exe Information: 0 : 19/08/2011 18:37:37.21: Virtual desktop deployment present on RDMS2.contoso.com server? True

ThreadId=13

ServerManager.exe Information: 0 : 19/08/2011 18:37:37.21: Shared desktop present on RDMS2.contoso.com server? False

ThreadId=13

ServerManager.exe Information: 0 : 19/08/2011 18:37:47.37: Web access server RDMS2.contoso.com is present on Rdms server RDMS2.contoso.com

ThreadId=1

ServerManager.exe Information: 0 : 19/08/2011 18:38:24.29: DeploymentContext: (public)PopulateSMPool...

ThreadId=30

ServerManager.exe Information: 0 : 19/08/2011 18:38:24.29: DeploymentContext: **Add Server 'RDMS2.contoso.com' to SMPool.**

ThreadId=30

ServerManager.exe Information: 0 : 19/08/2011 18:38:24.29: DeploymentContext: **Add Server 'DG-RFX-MAIN.contoso.com' to SMPool.**

ThreadId=30

ServerManager.exe Information: 0 : 19/08/2011 18:38:24.29: DeploymentContext: **Add Server 'RDSH1.contoso.com' to SMPool.**

ThreadId=30

ServerManager.exe Information: 0 : 19/08/2011 18:38:24.29: DeploymentContext: **Add Server 'RDSH2.contoso.com' to SMPool.**

ThreadId=30

ServerManager.exe Information: 0 : 19/08/2011 18:38:24.29: RDWorkloadWizardPlugin: IRolePlugin.Initialize...

ThreadId=30

ServerManager.exe Information: 0 : 19/08/2011 18:38:24.29: RDWorkloadWizardPlugin: IScenarioBasedPlugin.InitializePluginData...

ThreadId=1

ServerManager.exe Information: 0 : 19/08/2011 18:38:24.29: RDWorkloadWizardPlugin: Tracking service is being registered...

ThreadId=1

ServerManager.exe Information: 0 : 19/08/2011 18:38:24.29: RDWorkloadWizardPlugin: get ServiceProvider...

ThreadId=1

ServerManager.exe Information: 0 : 19/08/2011 18:38:24.29: RDWorkloadWizardPlugin: IScenarioBasedPlugin.PopulateWizard...

ThreadId=1

ServerManager.exe Information: 0 : 19/08/2011 18:38:24.31: RDMS2 is domain joined.

ThreadId=1

ServerManager.exe Information: 0 : 19/08/2011 18:38:24.31: Following RDManagement servers present in the server pool.

ThreadId=1

ServerManager.exe Information: 0 : 19/08/2011 18:38:24.31: RDMS2.contoso.com

ThreadId=1

ServerManager.exe Information: 0 : 19/08/2011 18:38:26.19: Joined nodes count on RDMS2.contoso.com server: 2

ThreadId=17

**ServerManager.exe Information: 0 : 19/08/2011 18:38:26.19: Virtual desktop deployment present on RDMS2.contoso.com server? True**

ThreadId=17

**ServerManager.exe Information: 0 : 19/08/2011 18:38:26.19: Shared desktop present on RDMS2.contoso.com server? False**

それから、プールの各サーバーについて、シナリオ ベースの展開の要件を満たしているかどうかがチェックされます。

ServerManager.exe Information: 0 : 19/08/2011 18:38:36.58: **RDSH1.contoso.com is domain joined.**

ThreadId=34

ServerManager.exe Information: 0 : 19/08/2011 18:38:36.63: **The current user is an admin on the server RDSH1.contoso.com**

ThreadId=34

ServerManager.exe Information: 0 : 19/08/2011 18:38:36.68: **Selected server RDSH1.contoso.com is Win8 server.**

ThreadId=34

ServerManager.exe Information: 0 : 19/08/2011 18:38:38.88: **Selected server RDSH1.contoso.com don't have pending reboots.**

ThreadId=34

ServerManager.exe Information: 0 : 19/08/2011 18:38:38.88: **Selected server RDSH1.contoso.com is not a localhost.**

ThreadId=34

ServerManager.exe Information: 0 : 19/08/2011 18:38:38.97: **RDSH2.contoso.com is domain joined.**

ThreadId=34

ServerManager.exe Information: 0 : 19/08/2011 18:38:39.01: **The current user is an admin on the server RDSH2.contoso.com**

ThreadId=34

ServerManager.exe Information: 0 : 19/08/2011 18:38:39.06: **Selected server RDSH2.contoso.com is Win8 server.**

ThreadId=34

ServerManager.exe Information: 0 : 19/08/2011 18:38:41.14: **Selected server RDSH2.contoso.com don't have pending reboots.**

ThreadId=34

ServerManager.exe Information: 0 : 19/08/2011 18:38:41.14: **Selected server RDSH2.contoso.com is not a localhost.**

次に、ユーザーが選択した展開の種類が記録され、その後、展開に追加中の各サーバーも表示されます。

ServerManager.exe Information: 0 : 19/08/2011 18:38:46.33: **User selected paramters for shared desktop scenario deployment.**

ThreadId=1

ServerManager.exe Information: 0 : 19/08/2011 18:38:46.33: **Is Rdms server already exists: True**

ThreadId=1

ServerManager.exe Information: 0 : 19/08/2011 18:38:46.33: **Rdms server : RDMS2.contoso.com**

ThreadId=1

ServerManager.exe Information: 0 : 19/08/2011 18:38:46.33: **Is web access server already exists on Rdms server: True**

ThreadId=1

ServerManager.exe Information: 0 : 19/08/2011 18:38:46.34: **Web access server : RDMS2.contoso.com**

ThreadId=1

ServerManager.exe Information: 0 : 19/08/2011 18:38:46.34: **RD Session Host servers :**

ThreadId=1

ServerManager.exe Information: 0 : 19/08/2011 18:38:46.34: **RDSH1.contoso.com**

ThreadId=1

ServerManager.exe Information: 0 : 19/08/2011 18:38:46.34: **RDSH2.contoso.com**

ThreadId=1

ServerManager.exe Information: 0 : 19/08/2011 18:38:46.34: Selected server RDSH1.contoso.com is not a localhost.

ThreadId=1

ServerManager.exe Information: 0 : 19/08/2011 18:38:46.34: Selected server RDSH2.contoso.com is not a localhost.

前述の例では、既存の仮想デスクトップ環境が検出され、ユーザーは共有デスクトップ環境の種類を選択しています。RDSH1 および RDSH2 という 2 台のサーバーが環境に追加されています。

その後、各サーバー上で役割サービスがインストールおよび構成され、ログ ファイルには実行された Powershell コマンドレットが示されて、進行および完了状況が報告されます。

ServerManager.exe Information: 0 : 19/08/2011 18:38:48.27: RDManagement\Install-RoleService -PSComputerName System.String[] -**RoleFeatureName RDS-RD-Server** -RestartIfNeeded 1 -SingleReboot 1

ThreadId=24

ServerManager.exe Information: 0 : 19/08/2011 18:39:18.38: CommandLetExecutor: Job Progress Received for cmdlet: RDManagement\Install-RoleService - **Start Installation... - 100% completed**

ThreadId=28

ServerManager.exe Information: 0 : 19/08/2011 18:41:56.42: CommandLetExecutor: Job Progress Received for cmdlet: RDManagement\**Install-RoleService - Complete - 100% completed**

ThreadId=28

ServerManager.exe Information: 0 : 19/08/2011 18:41:56.72: CommandLetExecutor: RDManagement\**Install-RoleService: succeeded**

ThreadId=24

全体的な環境の設定と共に、それぞれのサーバーも構成されます。

ServerManager.exe Information: 0 : 19/08/2011 18:41:56.73: **RDManagement\Set-RDSHDeployment -RDMSServer RDMS2.contoso.com** -RDSHServers System.String[] -RDWebAccessServers System.String[]

ThreadId=24

ServerManager.exe Information: 0 : 19/08/2011 18:41:58.62: CommandLetExecutor: Job Progress Received for cmdlet: RDManagement\Set-RDSHDeployment - Write-Debug - -1% completed

ThreadId=19

ServerManager.exe Information: 0 : 19/08/2011 18:42:01.05: CommandLetExecutor: Job Progress Received for cmdlet: RDManagement\Set-RDSHDeployment - **Configuring RDMS Server** - 0% completed

ThreadId=3

ServerManager.exe Information: 0 : 19/08/2011 18:42:08.99: CommandLetExecutor: Job Progress Received for cmdlet: RDManagement\Set-RDSHDeployment - **Configuring RDWA Server** - 0% completed

ThreadId=12

ServerManager.exe Information: 0 : 19/08/2011 18:42:13.65: CommandLetExecutor: Job Progress Received for cmdlet: RDManagement\Set-RDSHDeployment - **Configuring RDSH Server** - 0% completed

ThreadId=13

ServerManager.exe Information: 0 : 19/08/2011 18:42:16.93: RDManagement\Set-RDPGeneralSetting -PSComputerName RDMS2.contoso.com -RedirectionServer RDMS2.contoso.com -AlternateServer $Null

ThreadId=24

インストールの後で、サーバー マネージャーは RDS プラグインを読み込んで、構成を更新します。

ServerManager.exe Information: 0 : 19/08/2011 18:42:17.28: RDMSContext of 'RDMS2.contoso.com'

ThreadId=28

ServerManager.exe Information: 0 : 19/08/2011 18:42:17.28: ClusterName:

ThreadId=28

ServerManager.exe Information: 0 : 19/08/2011 18:42:17.28: IsInHa: False

ThreadId=28

ServerManager.exe Information: 0 : 19/08/2011 18:42:17.28: State: UnReachable

ThreadId=28

ServerManager.exe Information: 0 : 19/08/2011 18:42:17.28: ActiveServer:

ThreadId=28

ServerManager.exe Information: 0 : 19/08/2011 18:42:17.30: RDMSMachinePool: Non HA single RDMS which is reachable - RDMS2.contoso.com

ThreadId=28

ServerManager.exe Information: 0 : 19/08/2011 18:42:17.30: RDMSContext of 'RDMS2.contoso.com'

ThreadId=28

ServerManager.exe Information: 0 : 19/08/2011 18:42:17.30: ClusterName:

ThreadId=28

ServerManager.exe Information: 0 : 19/08/2011 18:42:17.30: IsInHa: False

ThreadId=28

ServerManager.exe Information: 0 : 19/08/2011 18:42:17.30: State: Alive

ThreadId=28

ServerManager.exe Information: 0 : 19/08/2011 18:42:17.30: ActiveServer:

ThreadId=28

ServerManager.exe Information: 0 : 19/08/2011 18:42:17.30: RDMSHeartbeat: Is 'RDMS' service running? True

ThreadId=28

ServerManager.exe Information: 0 : 19/08/2011 18:42:17.30: RDMSHeartbeat: Is 'WinRM' service running? True

ThreadId=28

ServerManager.exe Information: 0 : 19/08/2011 18:42:17.30: RDMSHeartbeat: Is 'MSSQL$MICROSOFT##WID' service running? True

ThreadId=28

ServerManager.exe Information: 0 : 19/08/2011 18:42:17.30: RDMSHeartbeat: Is 'TScPubRPC' service running? True

ThreadId=28

ServerManager.exe Information: 0 : 19/08/2011 18:42:17.30: RDMSHeartbeat: Is 'WinMgmt' service running? True

ThreadId=28

ServerManager.exe Information: 0 : 19/08/2011 18:42:17.30: RDMSHeartbeat: All the services are running

ThreadId=28

ServerManager.exe Information: 0 : 19/08/2011 18:42:18.25: **RDMachinePool: RefreshMachinePool called with force refresh = True**

ThreadId=17

ServerManager.exe Information: 0 : 19/08/2011 18:42:18.25: RDMachinePool: **Updating RDS Machine Pool Servers ...**

ThreadId=17

ServerManager.exe Information: 0 : 19/08/2011 18:42:18.25: RDMachinePool: Server DG-RFX-MAIN.contoso.com already part of the server machine pool. **Updating role information**

ThreadId=17

ServerManager.exe Information: 0 : 19/08/2011 18:42:18.25: RDMachinePool: RDS Roles/Features installed on server DG-RFX-MAIN.contoso.com

ThreadId=17

ServerManager.exe Information: 0 : 19/08/2011 18:42:18.25: RDMachinePool: RemoteDesktop role installed

ThreadId=17

ServerManager.exe Information: 0 : 19/08/2011 18:42:18.25: RDMachinePool: RDVH role installed

ThreadId=17

ServerManager.exe Information: 0 : 19/08/2011 18:42:18.25: RDMachinePool: Server RDMS2.contoso.com already part of the server machine pool. Updating role information

ThreadId=17

ServerManager.exe Information: 0 : 19/08/2011 18:42:18.25: RDMachinePool: RDS Roles/Features installed on server RDMS2.contoso.com

ThreadId=17

ServerManager.exe Information: 0 : 19/08/2011 18:42:18.25: RDMachinePool: RemoteDesktop role installed

ThreadId=17

ServerManager.exe Information: 0 : 19/08/2011 18:42:18.25: RDMachinePool: CB & RDMS role installed

ThreadId=17

ServerManager.exe Information: 0 : 19/08/2011 18:42:18.25: RDMachinePool: RDWA role installed

ThreadId=17

ServerManager.exe Information: 0 : 19/08/2011 18:42:18.25: RDMachinePool: Finding the RDMS server to use ...

ThreadId=17

RDS プラグインが初期化して RDMS サーバーをチェックします。また、RDS プラグインはハートビートを送信して、展開されているサーバーの状態をチェックします。

ServerManager.exe Information: 0 : 19/08/2011 18:42:18.28: RdsPluginController: Creating serverpage

ThreadId=1

ServerManager.exe Information: 0 : 19/08/2011 18:42:18.28: RDNavigationTree: Create 'SERVERS' node

ThreadId=1

ServerManager.exe Information: 0 : 19/08/2011 18:42:18.28: RdsPluginController: RDMS Machine changed. New RDMS Server: RDMS2.contoso.com

ThreadId=17

ServerManager.exe Information: 0 : 19/08/2011 18:42:18.28: RdsPluginController: RDMS Machine detected: RDMS2.contoso.com

ThreadId=17

ServerManager.exe Information: 0 : 19/08/2011 18:42:18.28: RdsPluginController: Initializing model...

ThreadId=17

ServerManager.exe Information: 0 : 19/08/2011 18:42:18.28: RdsPluginController: RDMS Server: RDMS2.contoso.com

ThreadId=17

ServerManager.exe Information: 0 : 19/08/2011 18:42:18.28: RDMSHeartbeat: StartHeartbeatCheck...

ThreadId=17

ServerManager.exe Information: 0 : 19/08/2011 18:42:18.42: RDMSHeartbeat: Last bootup time: 8/19/2011 4:38:16 PM

ThreadId=17

ServerManager.exe Information: 0 : 19/08/2011 18:42:18.42: RDMSHeartbeat: Minutes since last boot: 124.038421178333

ServerManager.exe Information: 0 : 19/08/2011 18:42:18.44: RDMSHeartbeat: Is 'RDMS' service running? True

ThreadId=17

ServerManager.exe Information: 0 : 19/08/2011 18:42:18.44: RDMSHeartbeat: Is 'WinRM' service running? True

ThreadId=17

ServerManager.exe Information: 0 : 19/08/2011 18:42:18.44: RDMSHeartbeat: Is 'MSSQL$MICROSOFT##WID' service running? True

ThreadId=17

ServerManager.exe Information: 0 : 19/08/2011 18:42:18.44: RDMSHeartbeat: Is 'TScPubRPC' service running? True

ThreadId=17

ServerManager.exe Information: 0 : 19/08/2011 18:42:18.44: RDMSHeartbeat: Is 'WinMgmt' service running? True

ThreadId=17

ServerManager.exe Information: 0 : 19/08/2011 18:42:18.44: RDMSHeartbeat: All the services are running

ThreadId=17

ServerManager.exe Information: 0 : 19/08/2011 18:42:18.44: RDMSHeartbeat: Check Heart beat every 5 minutes

ThreadId=17

ServerManager.exe Information: 0 : 19/08/2011 18:42:18.50: Virtual desktop deployment present on RDMS2.contoso.com server? True

ThreadId=17

ServerManager.exe Information: 0 : 19/08/2011 18:42:18.50: Shared desktop present on RDMS2.contoso.com server? True

ThreadId=17

ServerManager.exe Information: 0 : 19/08/2011 18:42:18.50: RdsPluginController: Creating homepage

ThreadId=1

ServerManager.exe Information: 0 : 19/08/2011 18:42:18.50: RDNavigationTree: Create 'OVERVIEW' node

ThreadId=1

ServerManager.exe Information: 0 : 19/08/2011 18:42:18.50: RdsPluginController: Creating All Collectionpage

展開段階でのトラブルシューティングの最初の方針は、問題を再現して RDMSDeploymentUI.txt ファイルを収集することです。ログを調べることで、展開プロセスが正常に行われなかった場所とその原因を正確に特定するのに役立ちます。

###### RemoteApp 公開のトラブルシューティング

RDMSDeploymentUI.txt ログ ファイルには、コレクションへの RemoteApp の公開のステータスも記録されます。該当するログ セクションを見つけるには、"RemoteApps: Publishing Summary…" というテキストを探します。

ServerManager.exe Information: 0 : 29/09/2011 14:18:44.95: **RemoteApps: Publishing Summary...**

ThreadId=1

ServerManager.exe Information: 0 : 29/09/2011 14:18:44.95: RemoteApps: Collection Id: RemoteApps

ThreadId=1

ServerManager.exe Information: 0 : 29/09/2011 14:18:44.95: RemoteApps: Collection Name: RemoteApps

ThreadId=1

ServerManager.exe Information: 0 : 29/09/2011 14:18:44.95: **RemoteApps: Selected session host server: RDSH2.contoso.com**

ThreadId=1

ServerManager.exe Information: 0 : 29/09/2011 14:18:44.95: RemoteApps: **#Remote Apps: 4**

ThreadId=1

ServerManager.exe Information: 0 : 29/09/2011 14:18:44.95: **RemoteApps: Alias: iexplore**

ThreadId=1

ServerManager.exe Information: 0 : 29/09/2011 14:18:44.95: **RemoteApps: Name: Internet Explorer**

ThreadId=1

ServerManager.exe Information: 0 : 29/09/2011 14:18:44.95: **RemoteApps: Location: %SYSTEMDRIVE%\Program Files\Internet Explorer\iexplore.exe**

ThreadId=1

ServerManager.exe Information: 0 : 29/09/2011 14:18:44.96: RemoteApps: Status: Published

ThreadId=1

ServerManager.exe Information: 0 : 29/09/2011 14:18:44.96: RemoteApps: Alias: wordpad

ThreadId=1

ServerManager.exe Information: 0 : 29/09/2011 14:18:44.96: RemoteApps: Name: WordPad

ThreadId=1

ServerManager.exe Information: 0 : 29/09/2011 14:18:44.96: RemoteApps: Location: %SYSTEMDRIVE%\Program Files\Windows NT\Accessories\wordpad.exe

ThreadId=1

ServerManager.exe Information: 0 : 29/09/2011 14:18:44.96: RemoteApps: Status: Published

ThreadId=1

ServerManager.exe Information: 0 : 29/09/2011 14:18:44.96: RemoteApps: Alias: mspaint

ThreadId=1

ServerManager.exe Information: 0 : 29/09/2011 14:18:44.96: RemoteApps: Name: Paint

ThreadId=1

ServerManager.exe Information: 0 : 29/09/2011 14:18:44.96: RemoteApps: Location: %SYSTEMDRIVE%\Windows\system32\mspaint.exe

ThreadId=1

ServerManager.exe Information: 0 : 29/09/2011 14:18:44.96: RemoteApps: Status: Published

ThreadId=1

ServerManager.exe Information: 0 : 29/09/2011 14:18:44.96: RemoteApps: Alias: calc

ThreadId=1

ServerManager.exe Information: 0 : 29/09/2011 14:18:44.96: RemoteApps: Name: Calculator

ThreadId=1

ServerManager.exe Information: 0 : 29/09/2011 14:18:44.96: RemoteApps: Location: %SYSTEMDRIVE%\Windows\system32\calc.exe

ThreadId=1

ServerManager.exe Information: 0 : 29/09/2011 14:18:44.96: RemoteApps: Status: Published

ThreadId=1

**ServerManager.exe Information: 0 : 29/09/2011 14:18:48.95: RDWizardManager: Wizard for 'Publish remote apps' completed.**

#### 既知の障害のシナリオ

ログ ファイルとイベント ログを分析することで簡単に診断できる既知の問題の一覧を以下に示します。

##### サーバーで再起動が保留になっている

サーバーに修正プログラムが適用されたばかりのときや、役割サービスまたは機能のインストール後に再起動待ちになっている場合、RDMS 環境で互換性チェックに失敗することがあります。RDMSDeploymentUI.txt ログ ファイルには次のように表示されます。

ServerManager.exe Information: 0 : 27/09/2011 16:57:41.77: DG-RFX-MAIN.contoso.com is domain joined.

ThreadId=22

ServerManager.exe Information: 0 : 27/09/2011 16:57:41.81: The current user is an admin on the server RDVH.contoso.com

ThreadId=22

ServerManager.exe Information: 0 : 27/09/2011 16:57:41.86: Selected server RDVH.contoso.com is Win8 server.

ThreadId=22

**ServerManager.exe Information: 0 : 27/09/2011 16:57:42.37: Selected server RDVH.contoso.com has pending reboots.**

この問題を解決するには、サーバーを再起動して、インストールまたはサーバーの保守を完了します。

何回か再起動してもこの問題を解決できない場合は、レジストリに、ファイル名の変更操作が保留になっていることを示すレジストリ キーが含まれている可能性があります。次のレジストリ値が存在する場合、サーバーが再起動待ちになっていることが、サーバー マネージャーによって検出されることがあります。

HKLM\System\CurrentControlSet\Control\Session Manager\PendingFileRenameOperations

この問題を解決するには、示されたモジュールが属するコンポーネントを調べ、このレジストリ値を削除しても安全かどうかを確認します。一部のアプリケーションは、このレジストリ値に書き込みを行い、ファイル名の変更後にこの値を適切に削除しないことがあります。また、インストールされた修正プログラムや更新プログラムに問題があった可能性もあります。このレジストリ キーを削除する前に、このキーのバックアップを取っておき、レジストリ値の削除後にシナリオ ベースの展開ウィザードを再実行することをお勧めします。

### コレクション作成のトラブルシューティング

セッション仮想化またはデスクトップ仮想化のコレクション作成で問題が起きた場合は、以下の手順でトラブルシューティングを実行してください。

**RD 接続ブローカーサーバー上:**

1. 前述の「[RDMSDeploymentUI ログの使用](#_Using_the_RDMSDeploymentUI)」セクションの手順を使用して、**RDMSDeploymentUI.txt** を見つけます。
2. 前述の「[RDMS UI トレースの有効化](#_Enabling_RDMS_UI)」セクションの手順に従って、**RDMSUI-trace.log**、分析ログ、およびデバッグ ログを有効にします。
3. [アプリケーションとサービス ログ]、[Microsoft]、[Windows] の順に展開し、その下の [TerminalServices-SessionBroker] および [TerminalServices-SessionBroker-Client] に移動して、すべてのデバッグ ログを有効にします。

**RD 仮想化ホスト サーバー上:**

1. [アプリケーションとサービス ログ]、[Microsoft]、[Windows] の順に展開し、その下の [TerminalServices-TSV-VmHostAgent] および [TerminalServices-SessionBroker-Client] に移動して、すべてのデバッグ ログを有効にします。
2. [アプリケーションとサービス ログ]、[Microsoft]、[Windows] の順に展開し、その下の Hyper-V 関連ノードに移動して、イベント ログにデータが記録されていることを確認します。
3. サーバー マネージャーを使用して、コレクション作成の問題を再現します。

#### データの収集

**RD 接続ブローカー サーバー上:**

1. イベント ビューアーを開いて、[カスタム ビュー]、[管理イベント] の順に移動し、イベント ログをエクスポートします。
2. デスクトップ仮想化のコレクションを作成する場合は、  
   **%windir%\system32\tssesdir\\*.xml** フォルダーの内容を収集します。
3. RDMSDeploymentUI.txt および RDMSUI-Trace.log ファイルを収集します。
4. [アプリケーションとサービス ログ]、[Microsoft]、[Windows] の順に展開し、その下の [TerminalServices-SessionBroker] および [TerminalServices-SessionBroker-Client] に移動して、ログをエクスポートします。

**RD 仮想化ホスト サーバー上:**

1. イベント ビューアーを開いて、[カスタム ビュー]、[管理イベント] の順に移動し、イベント ログをエクスポートします。
2. [アプリケーションとサービス ログ]、[Microsoft]、[Windows] の順に展開し、その下の [TerminalServices-TSV-VmHostAgent] および [TerminalServices-SessionBroker-Client] に移動して、ログをエクスポートします。
3. [アプリケーションとサービス ログ]、[Microsoft]、[Windows] の順に展開し、その下の Hyper-V 関連ノードに移動して、ログをエクスポートします。
4. 収集したすべてのデータを、問題を再現するために RDMS UI で実行する手順と共に、マイクロソフトのサポート スタッフの解析用に送信してください。

### リモート デスクトップ サービスのトラブルシューティング ツール

以下のセクションでは、新しい RDVDiag ツールの使用シナリオのチュートリアルを始め、リモート デスクトップ サービス環境の問題をトラブルシューティングする際に役立つツールについて説明します。

#### RDVDiag

RDVDiag ツールは、他のトラブルシューティング方法のすべてに失敗したときや、問題の診断用にイベント ログに含まれていないその他のトレース データが必要なときにのみ使用する高度なトラブルシューティング ツールです。セッション仮想化コレクションの作成やコレクションへの接続の問題の大半は、RDVDiag を実行して高度なトラブルシューティングのデータを収集しなくても解決できます。

RDVDiag の機能は次のとおりです。

* 環境内の管理されているすべてのコレクションに関する情報 (仮想マシン別の構成を含む) が表示されます。
* コレクションへの最新の 30 件の接続に関する情報 (接続 GUID を含む) が表示されます。
* 接続ブローカーのデータベースの内容がダンプされます。
* VM プロビジョニング ジョブのレポートが表示されます (前述の「データの収集」を参照)。

##### RDVDiag を使用したデータの収集

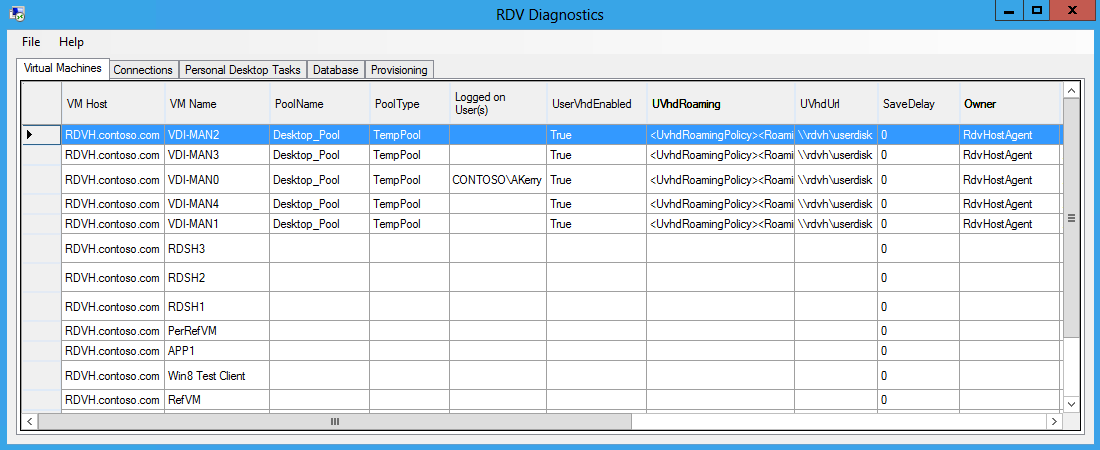
RDVDiag は、RDMS による管理に使用している接続ブローカー サーバー上で実行する必要があります。

RDVDiag を実行してログとトレースを生成する手順は次のとおりです。

1. rdvdiag.exe を右クリックして [プロパティ] をクリックします。
2. [互換性] タブをクリックし、[管理者としてこのプログラムを実行する] チェック ボックスをオンにして [OK] をクリックします。
3. RDVDiag を実行し、診断データが読み込まれるまで 10 秒ほど待ちます。

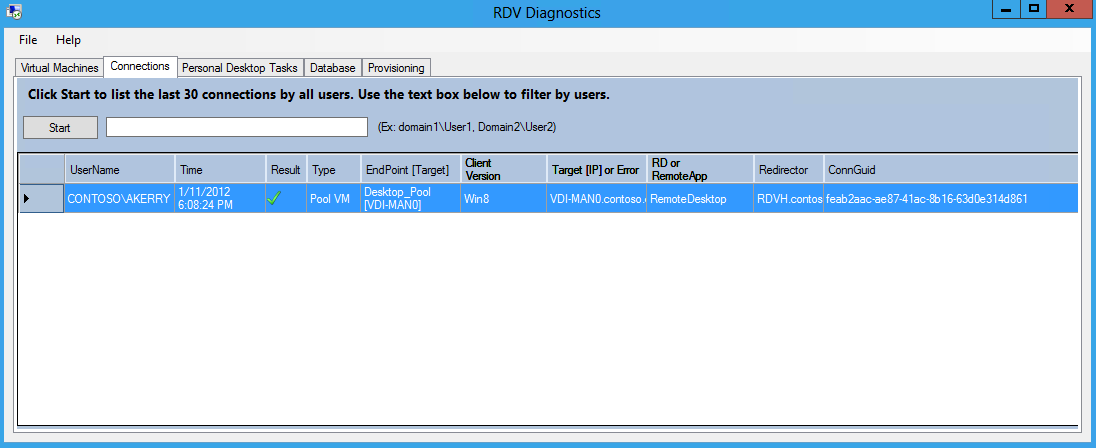
[仮想マシン] タブに、RDVH サーバー上の各仮想マシンに関する情報 (VM ホスト、VM 名、プール名、プールの種類、ログオンしたユーザーなど) の一覧が表示されます。

図 60: RDVDiag の [仮想マシン] タブ



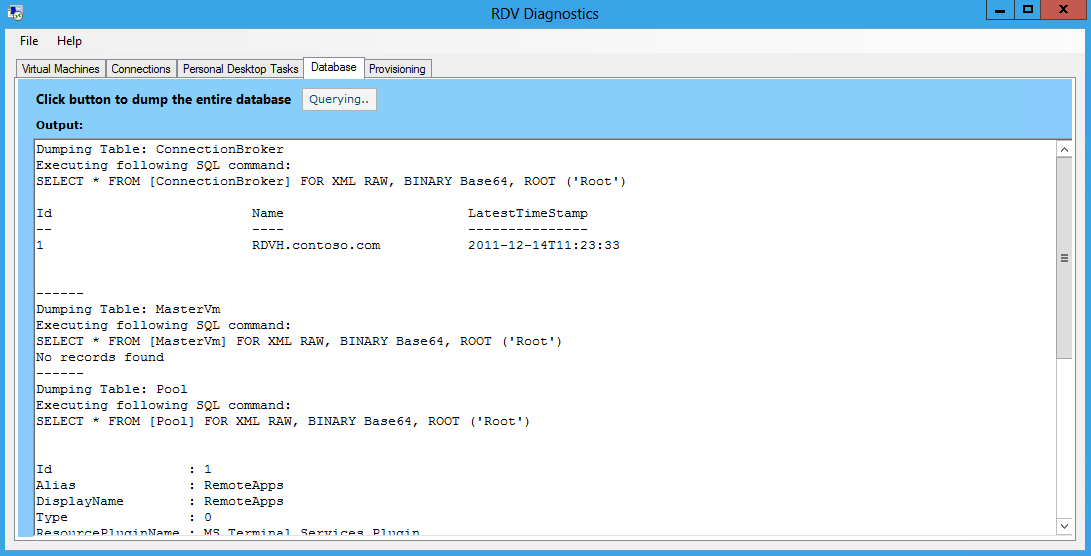
[接続] タブには、環境内のコレクションへのすべての接続の一覧が表示されます。[Start] をクリックすると、最新の 30 件の接続の一覧が表示され、[ConnGuid] フィールドにそれぞれの接続の接続 GUID が表示されます。

図 61: RDVDiag の [接続] タブ



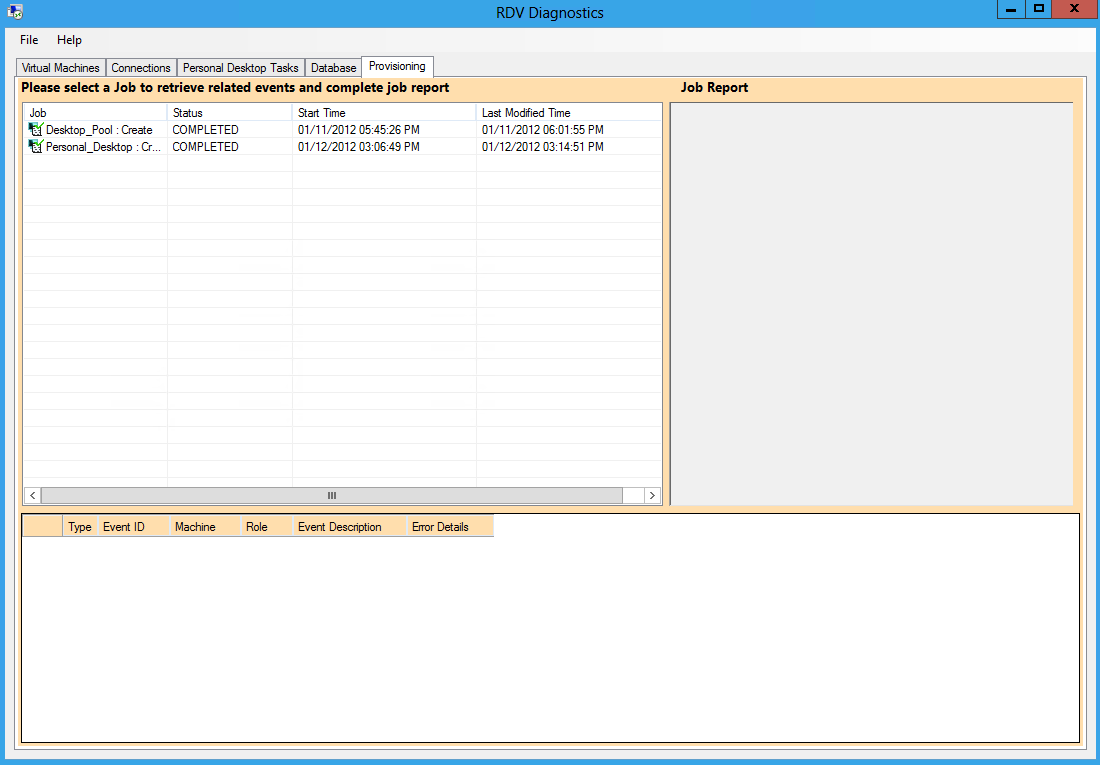
[データベース] タブには、接続ブローカー データベースの内容のダンプが表示されます。

図 62: RDVDiag の [データベース] タブ



[プロビジョニング] タブには、各コレクション作成のイベント ログと VM プロビジョニング レポート ファイルが表示されます。ここに表示されるイベントは、このドキュメントの「イベント ログ」セクションで示したイベントです。

図 63: RDVDiag の [プロビジョニング] タブ

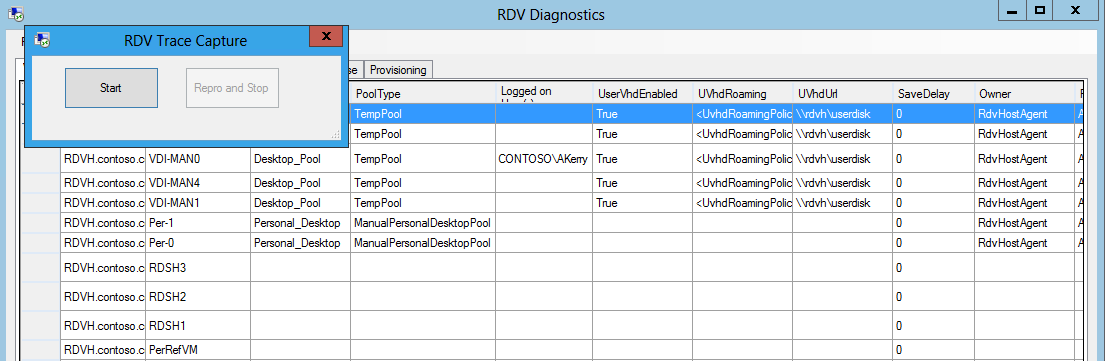


##### トレースの収集

RDVDiag によって、デスクトップ仮想化コンポーネントのトレースを有効にすることもできます。この基本的なプロセスは、次のとおりです。

1. RDVDiag を開いて、トレースを有効にします。
2. トレースを開始してから、問題を再現します。
3. トレースを停止して、マイクロソフトのサポート スタッフにデータを送信します。

図 64: RDVDiag トレース



RDVDiag によって生成される次のファイルは、RDVDiag が実行されているフォルダーに書き込まれます。

* rddb-rdvh.etl
* rdvtrace-rdvh.etl
* RDVDiagOutput.txt

#### RD Web ログの有効化

RD Web ページの問題をトラブルシューティングする際は、RD Web ログを有効にすると役立ちます。このログには、展開されている RD 接続ブローカーへの接続と RD 接続ブローカーとやりとりされたデータに関する有用な情報が含まれており、次のシナリオのトラブルシューティングに役立ちます。

* コレクションが Web ページに表示されない場合
* 一部のコレクションは表示されるのに、他のコレクションは表示されない場合
* ユーザーに対する Web ページの表示で、エラー メッセージが表示されたり、予期しない動作が起きる場合

|  |  |
| --- | --- |
| 警告: | 次の手順を使用して web.config ファイルに変更を加える際は、必ずその前に web.config ファイルのコピーを作成してください。また、トラブルシューティングが完了したら、ログを有効にしたままにしないで、必ず無効にしてください。 |

RD Web ログを有効にする手順は次のとおりです。

1. 管理者として RD Web サーバーにログオンし、管理用の Windows PowerShell プロンプトまたはコマンド プロンプトを開きます。
2. %SYSTEMROOT%\Web\RDweb フォルダーに変更します。
3. web.config ファイルを開き、<system.diagnostics> というセクションを見つけます。
4. TraceTSWA 値を 4 に変更します。

<add name="TraceTSWA" value="4" />

1. コメントは <!-- および --> で示されます。コメントを削除して RD Web ログを有効にするには、次の行を変更してコメントを削除します。

<!-- Uncomment for file tracing

<add name="FileLog"

type="Microsoft.VisualBasic.Logging.FileLogTraceListener,

Microsoft.VisualBasic, Version=8.0.0.0,

Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a,

processorArchitecture=MSIL"

initializeData="FileLogWriter" BaseFileName="RDWeb"

Location="Custom"

LogFileCreationSchedule="Daily"

MaxFileSize="50000000"

CustomLocation="\Windows\Web\RDWeb\App\_Data" />

-->

例:

<add name="FileLog"

type="Microsoft.VisualBasic.Logging.FileLogTraceListener,

Microsoft.VisualBasic, Version=8.0.0.0,

Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a,

processorArchitecture=MSIL"

initializeData="FileLogWriter" BaseFileName="RDWeb"

Location="Custom"

LogFileCreationSchedule="Daily"

MaxFileSize="50000000"

CustomLocation="\Windows\Web\RDWeb\App\_Data" />

1. Web ページを再度読み込んで、問題を再現します。
2. ログ ファイルが %SYSTEMROOT%\Web\RDWeb\App\_Data フォルダーに作成されます。これには、ログ ファイルが書き込まれた日付と時刻のスタンプが含まれます。
3. マイクロソフトのサポート スタッフの分析用に RD Web ログ ファイルを送信します。

##### RD Web ログの分析

RD Web ログ ファイルはテキスト ファイルで、ユーザーのログオン、RD Web アクセス サーバーと接続ブローカーの間の通信、およびユーザーのために Web ページを構築するプロセス (フォルダー、ユーザーのためのアプリケーションのフィルター処理など) を記録します。以下に RD Web ログの例を示し、重要なセクションは太字で表します。

**2012/02/06 15:21:31 [Info] 89 DomainUserName : contoso.com\dgeddes.**

2012/02/06 15:21:31 [Info] 89 UserSid : S-1-5-21-3827296891-200277369-620272553-1107.

2012/02/06 15:21:31 [Verbose] 68 Page Requested : login.aspx, Request Type : GET.

**2012/02/06 15:21:31 [Verbose] 68 Radcm Server Name : RDVH.contoso.com.**

**2012/02/06 15:21:31 [Verbose] 68 RDSH Server Names : .**

2012/02/06 15:21:31 [Info] 68 Connecting to Centralized Publishing Server: RDVH.contoso.com

2012/02/06 15:21:31 [Verbose] 68 Cache TTL is 120 minutes

2012/02/06 15:21:31 [Verbose] 68 Setting up access check.

2012/02/06 15:21:31 [Verbose] 68 :Putting workspace Info into the Cache

**2012/02/06 15:21:31 [Verbose] 68 Workspace ID : HA-RDCB.CONTOSO.COM**

**2012/02/06 15:21:31 [Verbose] 68 Workspace Name : Work Resources**

2012/02/06 15:21:31 [Info] 68 :Cache is not available, downloading information.

2012/02/06 15:21:37 [Info] 82 User Name : dgeddes, DomainName : contoso.com, Password : Non-NullOrEmpty, Private logon : True, LogonUser returned : True.

2012/02/06 15:21:37 [Info] 76 DomainUserName : contoso.com\dgeddes.

2012/02/06 15:21:37 [Verbose] 76 :Workspace Info found in cache, not re-querying, it may be stale!!!

**2012/02/06 15:21:37 [Info] 76 :Attempting to get Applications from the cache**

**2012/02/06 15:21:37 [Info] 76 :No apps found in the cache**

2012/02/06 15:21:37 [Warning] 76 :Program's icon file not available - using default.

2012/02/06 15:21:37 [Info] 76 :App: Personal added, FileExtension: .rdp IsRDP: True

2012/02/06 15:21:37 [Warning] 76 :Program's icon file not available - using default.

2012/02/06 15:21:37 [Info] 76 :App: Virtual Desktops added, FileExtension: .rdp IsRDP: True

2012/02/06 15:21:37 [Warning] 76 :Program's icon file not available - using default.

2012/02/06 15:21:37 [Info] 76 :App: Sessions added, FileExtension: .rdp IsRDP: True

**2012/02/06 15:21:37 [Verbose] 76 :Putting applications into the Cache**

**2012/02/06 15:21:37 [Verbose] 76 Filtering apps for SID: S-1-5-21-3827296891-200277369-620272553-1107**

**2012/02/06 15:21:37 [Verbose] 76 >>>>> Personal Checking Access**

**2012/02/06 15:21:37 [Verbose] 76 ALLOWED access to desktop Personal**

**2012/02/06 15:21:37 [Verbose] 76 >>>>> Virtual Desktops Checking Access**

**2012/02/06 15:21:37 [Verbose] 76 ALLOWED access to desktop Virtual Desktops**

**2012/02/06 15:21:37 [Verbose] 76 >>>>> Sessions Checking Access**

**2012/02/06 15:21:37 [Verbose] 76 ALLOWED access to desktop Sessions**

**2012/02/06 15:21:37 [Verbose] 76 No RDSH servers specified, skipping RDSH app collection**

## 付録

### 付録 A — 新規グループ ポリシーの一覧

以下に、リモート デスクトップ サービスの新しいグループ ポリシーの一覧を示します。これらのポリシーは、このドキュメントを作成した時点のもので、Windows Server "8" Beta および Windows Server "8" Beta Beta にのみ適用されます。

#### リモート デスクトップ接続クライアント

以下のポリシーは、リモート デスクトップ接続クライアントの新しいポリシーです。

表 11: RDC クライアント ポリシー

|  |  |
| --- | --- |
| グループ ポリシー | 説明 |
| Turn off UDP On Client | このポリシー設定では、リモート デスクトップ プロトコルを介してサーバーにアクセスするために UDP プロトコルを使用するかどうかを指定します。  このポリシー設定を有効にすると、リモート デスクトップ プロトコルのトラフィックは TCP プロトコルのみを使用します。  このポリシー設定を無効にした場合、または構成しない場合、リモート デスクトップ プロトコルのトラフィックは TCP プロトコルと UDP プロトコルの両方を使用しようと試みます。 |

#### リモート デスクトップ セッション ホスト

以下のポリシーは、リモート デスクトップ セッション ホスト役割サービスの新しいポリシーで、リモート デスクトップ セッション ホスト接続に適用されます。

表 12: RDSH ポリシー

|  |  |
| --- | --- |
| グループ ポリシー | 説明 |
| Connections — Turn Off Network Detection On Server | このポリシー設定では、リモート デスクトップ プロトコルがネットワーク品質 (帯域幅と遅延時間) の検出を試行するかどうかを指定します。  このポリシー設定を有効にする場合は、[Connect Time Network Detect]、[Continous Network Detect]、または [Connect Time Detect] と [Continous Network Detect] のいずれかを選択する必要があります。[Connect Time Network Detect] を選択すると、リモート デスクトップ プロトコルは接続時にネットワーク品質を判断しようとしないで、このサーバーへの全トラフィックは低速接続から来たものと想定します。[Continous Network Detect] を選択すると、リモート デスクトップ プロトコルは変化するネットワーク品質に対応しようとしなくなります。[Connect Time Detect] と [Continous Network Detect] を選択すると、リモート デスクトップ プロトコルは接続時にネットワーク品質を判断しようとしないで、このサーバーへの全トラフィックは低速接続から来たものと想定します。また、リモート デスクトップ プロトコルは、変化するネットワーク品質に対応しようとしなくなります。  このポリシー設定を無効にした場合、または構成しない場合、リモート デスクトップ プロトコルは最大数秒間を費やして接続前にネットワーク品質を判断しようと試み、ネットワーク品質に継続的に対応しようとします。 |
| Connections — Turn Off UDP On Server | このポリシー設定では、このサーバーに対するリモート デスクトップ プロトコルのアクセスに UDP プロトコルを使用するかどうかを指定します。  このポリシー設定を有効にすると、このサーバーに対するリモート デスクトップ プロトコルのトラフィックは TCP プロトコルのみを使用します。  このポリシー設定を無効にした場合、または構成しない場合、このサーバーに対するリモート デスクトップ プロトコルのトラフィックは TCP プロトコルと UDP プロトコルの両方を使用します。 |
| Remote Session Environment — Configure RemoteFX lossless graphics | 管理者はこのポリシー設定を使用して、リモート デスクトップ セッション ホストまたはリモート デスクトップ仮想化ホスト サーバーの RemoteFX グラフィックスをロスレスに構成できます。  このポリシー設定を有効にすると、RemoteFX グラフィックスはロスレス エンコードを使用します。そして、グラフィックス データの色の完全性が影響を受けることはなくなります。  このポリシー設定を無効にした場合、または構成しない場合、RemoteFX グラフィックスのロスレスのエンコードは使用されません。 |
| Remote Session Environment — Configure RemoteFX Adaptive Graphics | 管理者はこのポリシー設定を使用して、リモート デスクトップ セッション ホストまたはリモート デスクトップ仮想化ホスト サーバーの RemoteFX エクスペリエンスを構成できます。既定では、システムは、利用可能なネットワーク帯域幅に基づいて、最適なエクスペリエンスを選択します。  このポリシー設定を有効にした場合は、次のオプションのいずれかに RemoteFX エクスペリエンスを設定できます。  1. ネットワークの状態に合わせてシステムにエクスペリエンスを選択させる  2. エクスペリエンスのために最適化する (バランス)  3. 最小限のネットワーク帯域幅を使用するように最適化する  このポリシー設定を無効にした場合、または構成しない場合、RemoteFX エクスペリエンスはネットワークの状態に合わせて動的に変化します。 |
| Remote Session Environment — Use the hardware default graphics adapter for all Remote Desktop Services sessions | システム管理者はこのポリシー設定を使用して、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) サーバー上のすべてのリモート デスクトップ サービス セッションのグラフィックス レンダリングを変更できます。  このポリシー設定を有効にすると、RD セッション ホスト サーバー上のすべてのリモート デスクトップ サービス セッションは、既定のアダプターとして Microsoft Basic レンダー ドライバーではなく、ハードウェア グラフィック レンダラーを使用します。  このポリシー設定を無効にした場合、または構成しない場合、RD セッション ホスト サーバー上のすべてのリモート デスクトップ サービス セッションは、既定のアダプターとして Microsoft Basic レンダー ドライバーを使用します。  注意: このポリシー設定は、複数のグラフィックス処理装置 (GPU) が搭載されているコンピューター上の既定の GPU にのみ影響を与えます。他のすべての GPU はセカンダリ アダプターと見なされて、ハードウェア レンダラーとして使用されます。ローカル セッションの GPU 構成は、このポリシー設定の影響を受けません。 |