Parallels Remote Application Server
管理者ガイド

19.3

Parallels International GmbH
Vordergasse 59
8200 Schaffhausen
スイス
Tel：+ 41 52 672 20 30
www.parallels.com/jp

目次

第　1　章

はじめに

アプリケーション、デスクトップおよびデータを仮想化する統合ソリューション、Parallels® Remote Application Server（Parallels RAS）へようこそ。Parallels RAS を使用して、ご利用のネットワーク内であれば場所を問わずどのデバイスに対してもアプリケーションを公開し、リモートの仮想デスクトップを配信できます。

この章の内容

Parallels RAS 19 リリース履歴

次の表に、Parallels RAS 19 のリリース履歴を示します。Parallels RAS ドキュメントは、毎回のリリースごとに更新されます。このガイドは、以下の表から最新の Parallels RAS 19 リリースを参照しています。新しい Parallels RAS リリースまたはバージョンを使用している場合は、https://www.parallels.com/jp/products/ras/resources/ からガイドの現在のバージョンをダウンロードしてください。

Parallels RAS バージョン	リリース	日付
19.0	初回リリース	2022/07/27
19.0	Update 1	2022/08/31
19.0	ホットフィックス 1	2022/09/16
19.0	ホットフィックス 2	2022/09/30
19.0	ホットフィックス 3	2022/10/14
19.1	Update 2	2022/11/15
19.2	Update 3	2023/07/06

19.3	Update 1	2023/11/06

Parallels RAS について

Parallels RAS を使用すると、単一のプラットフォームからバーチャルデスクトップとアプリケーションをベンダーに依存せずに配信できます。Parallels RAS は、プラットフォーム固有のクライアントや、ビルトインの Parallels Web Client などのウェブ対応ソリューションを活用することで、ロケーションを問わずにアクセスできるリモートデスクトップ、アプリケーション、ドキュメントを公開できます。デスクトップの管理性、セキュリティ、パフォーマンスを向上させることができます。

Parallels RAS では、カスタマイズされたシェルと、Microsoft RDP プロトコルを介した仮想チャネル拡張を使用して、Windows リモートデスクトップサービスを拡張しています。Parallels RAS は、Microsoft、VMware、および Nutanix AHV（AOS）や Scale Computing などのハイパーコンバージドソリューションを含むその他のベンダーが提供するすべての主要なハイパーバイザーをサポートしており、さらに、Microsoft Azure や Azure Virtual Desktop（旧名: Windows Virtual Desktop）などのクラウドプラットフォーム/サービスもサポートしています。これらを活用することで、仮想デスクトップとアプリケーションを Parallels Client に公開できるようにします。

この製品には、強力なユニバーサルプリント機能とユニバーサルスキャン機能、およびリソースベースのロードバランス、管理機能が含まれています。

Parallels RAS 用の Parallels デバイスマネージャーモジュールでは、ユーザー接続の他、無料の Parallels Client を使用してシンクライアントに変換された PC を集中管理することもできます。

仕組み

ユーザーがアプリケーションまたはデスクトップをリクエストすると、Parallels RAS により負荷の最も低い RD セッションホスト、または負荷の最も低いプロバイダー上のゲスト VM が検索され、その間の RDP 接続が確立されます。Microsoft RDP プロトコルを使用して、リクエストされたアプリケーションまたはデスクトップがユーザーに提供されます。Parallels RAS は、RD セッションホストと VDI に加えて、Azure Virtual Desktop リソースの構成、管理、および公開にも使用できることに注意してください。

ユーザーは、Windows、Linux、macOS、Android、Chrome、iOS および iPadOS で実行できる無料の Parallels Client を使用して、Parallels RAS に接続できます。また、HTML5 ブラウザーまたは Chromebook を使用して接続することもできます。

Windows の新規バージョンが次々に開発される中、ビジネスの移行コストを抑える必要があります。Parallels RAS がお役に立ちます。デスクトップの置換を使用することで、ハードウェア寿命を延長し、最新 OS への移行をユーザーに最も適した時期まで遅らせることができます。Parallels RAS ソリューションを使用すると、非常に柔軟に対応できます。たとえば、ユーザー側のマシン構成をロックすることで、企業データを極めて安全な場所に配置することができます。また、ユーザーが一部のローカルアプリケーションまたはリモートアプリケーション以外を実行できないようにすることもできます。Parallels Client のデスクトップの置換を使用すると、最もよく使用するローカル構成オプションを無効にすることでローカルマシンの操作性を抑えながら、シンクライアントによって提供されるのと同レベルのサービスとセキュリティを保証できます。しかも、これらをすべて既存の PC から実行できます。

このガイドについて

このガイドは、Parallels RAS をインストール、構成、管理するシステム管理者向けです。このガイドは、Microsoft リモートデスクトップサービスに習熟し、中程度のネットワーク知識を有している読者を想定しています。

新機能

Parallels RAS 19.3.1

> 注: 複数のテンプレートを単一の VDI ホストプールに割り当てている場合は、Parallels RAS 19.3 をアップデートしないでください。

Parallels RAS 19.3.1 には、以下の新機能が追加されました。

- ユーザーのログオフ時にセッションを自動的にリセットする機能（p. 324）。
- Azure Virtual Desktop の強化。

新機能と改善点の詳細なリストについては、リリースノートを参照してください: https://kb.parallels.com/en/129018。

Parallels RAS 19.3

注: 複数のテンプレートを単一の VDI ホストプールに割り当てている場合は、Parallels RAS 19.3 をアップデートしないでください。

Parallels RAS 19.3 には、以下の新機能が追加されました。

- RD セッションホスト、VDI、および Azure Virtual Desktop のテンプレートバージョン作成。以下の機能をご利用いただけます。
  - バージョン管理（p. 583）
  - バージョンタグ（p. 583）
  - RD セッションホスト（p. 123）、VDI（p. 208）Azure Virtual Desktop（p. 262）のホストプールに対してテンプレートバージョンを割り当てる機能。
  - スケジュールによる RD セッションホスト（p. 154）、VDI（p. 222）、Azure Virtual Desktop（p. 266）テンプレートの再作成。
- ホストプールレベルでユーザープロファイルやその他の設定を構成する機能。
- サードパーティの IdP を介したユーザーパスワードの変更機能（p. 348）。
- ドライブリダイレクトキャッシュを構成するための新しいポリシー（p. 522）。
- ユーザー名の保存を禁止する新しいポリシー（p. 534）。
- ワークロードのホストを空にして電源をオフにする機能（p. 115）。
- FSLogix Office コンテナーのサポートと FSLogix の管理強化（p. 140）。
- 動的なプリンターマッピング。
- Azure Virtual Desktop の強化。
- SC//HyperCore プロバイダーに複数のプロバイダーアドレスを追加しました。
- テナントの請求情報を非表示にする機能。
- SC//HyperCore プロバイダー上の既存の MAC アドレスを保持したままホストを再作成する機能。
- TLS 1.3 のサポート。
- FIPS 140-2 準拠（p. 350）。
- 用語の更新:
  - プール/グループに言及される場合、用語は「ホストプール」に標準化されました。

  - デスクトップ/ゲストに言及される場合、用語は「ホスト」に標準化されました。
- 新しい定義済みレポート（p. 550）：
  - セッションアクティビティ
  - 切断の理由

新機能と改善点の詳細なリストについては、リリースノートを参照してください: https://kb.parallels.com/en/129018。

Parallels RAS 19.2.3

Parallels RAS 19.2.f3 には、以下の新機能が追加されました。

- Connection Broker 間における監査データベースの同期を解除する機能（p. 586）
- Parallels Client for macOS によって開始されたセッションにおけるドライブリダイレクトキャッシュのサポート（p. 152）

新機能と改善点の詳細なリストについては、リリースノートを参照してください: https://kb.parallels.com/en/129018。

Parallels RAS 19.2.2

Parallels RAS 19.2.2 には、以下の新機能が追加されました。

- ホストがホストプールに参加した際に、そのライセンスタイプを変更する機能（p. 249）。ホストプール内に存在する任意のホストのライセンスタイプを手動で変更することもできます（p. 263）。
- すべてのユーザーセッションが終了した際にコンピューターをロックまたはログオフする機能（p. 529）。

新機能と改善点の詳細なリストについては、リリースノートを参照してください: https://kb.parallels.com/en/129018。

Parallels RAS 19.2

Parallels RAS 19.2 には、以下の新機能が追加されました。

- AVD 向け MSIX app attach との機能統合（p. 576）。
- VDI（p.182）と AVD（p. 253）におけるディスクストレージコストの最適化。

- Parallels Client と RDSH（p. 131）、VDI（p. 182）、Remote PC（p. 285）上のサーバー間の接続にトランスポートプロトコルを選択する機能。
- シングルセッション(p. 269)およびマルチセッション(p. 273)の AVD ホストに対して RDP Shortpath を使用できるようになりました。
- Parallels Web Client を使用して AVD リソースに接続することができます。（p. 276）。
- ディスプレイ構成を選択するための新しいポリシー（p. 515）。
- クライアントデバイスのホスト名でパーシスタントなホストを割り当てる機能（p. 220）。
- ESXi と vCenter 上で RD セッションホストとホストを元の BIOS UUID で再作成する機能（自動で動作する）。
- Microsoft Azure を TOTP プロバイダーとして追加（p. 368）。

非推奨事項および更新されたシステム要件:

- コンポーネントとクライアントの最新のシステム要件については、「ソフトウェア要件」(p. 30）を参照してください。

新機能と改善点の詳細なリストについては、リリースノートを参照してください: https://kb.parallels.com/en/129018。

Parallels RAS 19.1

Parallels RAS 19.1 には、以下の新機能が追加されました。

- VDI 向け MSIX app attach との機能統合（p. 576）。
- クライアントポリシーの検索（p. 508）。
- AVD ホストプール内のすべてのエージェントを同時にアップデートする機能（p. 256）。
- 公開済みアプリケーションの動的なデスクトップサイズ変更を構成するための新しいポリシー（p. 515）。
- Azure Virtual Desktop でマルチメディアリダイレクトを設定するための新しいポリシー（p. 522）。
- 秘密鍵を使用して RAS テナントブローカーを参加させる際に、パブリックドメインアドレスを登録する機能（p. 408）。
- 秘密鍵を使用して RAS テナントブローカーにテナントを加入させる際に、パブリックドメインアドレスを提供する機能（p. 408）。
- ホストの作成に失敗した場合の詳細を簡単に表示する機能（p. 206）。

- 新しい定義済みレポート（p. 550）:
  - 転送プロトコル（TCP または UDP）
  - ネットワーク遅延
  - 接続品質
  - 帯域幅の可用性

非推奨事項および更新されたシステム要件:

- コンポーネントとクライアントの最新のシステム要件については、「ソフトウェア要件」（p. 30）を参照してください。

新機能と改善点の詳細なリストについては、リリースノートを参照してください: https://kb.parallels.com/en/129018。

Parallels RAS 19.0

Parallels RAS 19.0 には、以下の新機能が追加されました。

- クラウドプロバイダーとして Amazon Web Services をサポートし、EC2 インスタンスが利用できるようになりました（p. 177）
- MSIX app attach との機能統合を実現しました。（p. 576）
- Let's Encrypt 証明書管理（p. 340）。
- 新しい Parallels Client for Windows for ARM64。
- 表現的な記述のクライアントポリシー（p. 508）、公開済みリソースのフィルタリング（p. 317）、MFA（p. 378）の構成。
- 電源管理: スケジュールに従ってサーバーを起動および終了します。RD セッションホストのスケジュール作成（p. 154）、VDI（p. 222）、AVD ホスト（p. 266）
- Parallels Client を使用しているときに RAS リソースにすばやくアクセスできる、メールベースのアカウント検出機能（p. 381）。
- 指定した時間帯に公開済みリソースへのユーザーアクセスを制限できるログオン時間制限（p. 352）。
- テーマごとに異なる MFA プロバイダーを割り当てる機能（p. 357）。
- ローカルエンドユーザーデバイスにリダイレクトする URL を指定したり、リモートセッションで起動する URL を指定したりする機能（p. 573）

- 特定の公開フォルダーを操作するための権限をカスタム管理者に委譲する機能（p. 312）。

非推奨事項および更新されたシステム要件:

- コンポーネントとクライアントの最新のシステム要件については、「ソフトウェア要件」（p. 30）を参照してください。

新機能と改善点の詳細なリストについては、リリースノートを参照してください: https://kb.parallels.com/en/129018。

このガイドで使用される用語と略語

注: Parallels RAS 19 以降、このセクションを含むすべての製品およびドキュメントで、用語が更新されています。用語の変更については、https://kb.parallels.com/en/128943 を参照してください。

用語/略語	説明
RAS Console	Parallels RAS Console。 RAS Console は、Parallels RAS の構成、管理、実行に使用する主要なインターフェイスです。管理者は、RAS Console を使用して、ファーム、サイト、RD セッションホスト、公開済みのリソース、クライアント接続などを管理します。
カテゴリー	RAS Console では、メインウィンドウの左ペインに [カテゴリー] が表示されます。各カテゴリーは、特定のタスクまたは操作に関連するいくつかの設定で構成されます。 カテゴリーには、[開始]、[ファーム]、[ロードバランス]、[公開]、[ユニバーサルプリント]、[ユニバーサルスキャン]、[接続]、[デバイスマネージャー] などがあります。
ファーム	Parallels RAS ファームは、一括管理を目的としたオブジェクトの論理グループです。ファーム構成の情報は単一のデータベースに保存され、ファームを構成するすべてのオブジェクトに関する情報がそこに保存されます。ファームには少なくとも 1 つのサイトが必要ですが、必要な数のサイトで構成することができます（以下の「サイト」を参照）。
サイト	1 つのサイトは、少なくとも 1 つの RAS Connection Broker、RAS Secure Gateway（または複数のゲートウェイ）、および RD セッションホスト、プロバイダー、Windows PC にインストールされた RAS Agent で構成されます。RD セッションホスト、プロバイダー、または PC が、同時に複数のサイトのメンバーになることはできません。
ライセンスサイト	Parallels RAS ファーム内で Parallels RAS ライセンスを管理するサイトです。デフォルトでは、Parallels RAS をインストールするサーバーがライセ

	ンスサイトになります。後で追加のサイトを作成した場合、そのいずれかをライセンスサイトとして指定できます。 1 つのファームに存在できるライセンスサイトは 1 つのみです。他のすべてのサイトはセカンダリサイトと呼ばれます。 注: Parallels RAS のアップデートまたはアップグレードは最初にライセンスサイトに適用する必要があります。
RAS Secure Gateway	RAS Secure Gateway は、アプリケーションで必要とされるすべてのトラフィックを単一のポートでトンネリングして、安全な接続を実現します。
Web Client	Web Client を使用すると、ウェブブラウザーでリモートアプリケーションやデスクトップを表示および起動できます。Web Client 機能は、RAS Secure Gateway の一部です。
公開	リモートデスクトップサーバー、プロバイダー、またはリモート PC にインストールされたアイテムを Parallels RAS 経由でユーザーに提供すること。
RAS Connection Broker	RAS Connection Broker では、公開済みのアプリケーションおよびデスクトップのロードバランスが実行されます。
RAS RD セッションホスト Agent	RAS RD セッションホスト Agent では、Connection Broker で必要とされる情報が Microsoft RDS から収集され、必要に応じて Connection Broker に送信されます。
Remote PC Agent	Remote PC Agent では、Connection Broker で必要とされる情報がリモート PC ホストから収集され、必要に応じて Connection Broker に送信されます。
RAS Guest Agent	RAS Guest Agent では、RAS Connection Broker で必要とされる情報が VDI デスクトップから収集され、必要に応じて Connection Broker に送信されます。
RAS Provider Agent / RAS Provider Agent	RAS Provider Agent では、Parallels RAS Infrastructure から情報が収集され、ネイティブ API を介して VDI が制御されます。RAS Provider Agent は、RAS Connection Broker に組み込まれておりデフォルトで利用可能です。これは、Parallels RAS ファームで複数のプロバイダーを制御するために使用できます。 RAS Provider Agent は、RAS Provider Agent と同じものを指していますが、この用語は Azure Virtual Desktop（この表の最後で説明）のコンテキストで使用されます。
専用 RAS Provider Agent	専用 RAS Provider Agent は、上記の RAS Provider Agent と似ていますが、重要な違いが 1 つあります。これは、Parallels RAS インストーラーからインストールする必要がある別個のコンポーネントであり、単一のプロバイダーのみを制御できます。
RDSH または RD セッションホスト	RDSH は、リモートデスクトッププロトコル（RDP）をサポートするリモートクライアントがアプリケーションと制限のないデスクトップ環境にアクセ

	スできるようにします。Windows 2008 R2 から、ターミナルサービスは RDSH に置き換えられました。
HALB	高可用性ロードバランス（HALB）は、 RAS Secure Gateway に負荷分散を提供するアプライアンスです。Parallels HALB 仮想アプライアンスは次のハイパーバイザーで利用できます。Hyper-V、VMware。異なる HALB デバイスを表す複数の HALB 仮想サーバーを単一のサイトに展開できます。 複数の HALB を配置して同時に実行することができます。その場合、1 つがプライマリとして機能し、その他がセカンダリとして機能します。サイトに配置された HALB が多いほど、ダウンタイム発生の可能性が低くなります。プライマリとセカンダリの HALB 展開では、同じ IP アドレスまたは仮想 IP アドレス（VIP）が共有されます。プライマリの HALB 展開に障害が発生した場合、セカンダリがマスターに昇格し、プライマリの地位を引き継ぎます。
テナントブローカー	テナントブローカーは、共有 RAS Secure Gateway をホストする、特殊な RAS インストールです。RAS マルチテナントアーキテクチャに不可欠な部分です。
テナント	テナントは、テナントブローカー（上記参照）に参加する RAS ファームです。共有 RAS Secure Gateway と HALB を使用するため、別途ゲートウェイや HALB を用意する必要がありません。
RAS 登録サーバー	RAS 登録サーバーは SAML SSO 認証機能に不可欠の構成要素です。Microsoft 認証局（CA）と通信し、Parallels RAS 環境内にある SSO 認証のデジタル証明書のリクエスト、登録、および管理をユーザーに代わって実行します。
RAS PowerShell	Parallels RAS PowerShell では、PowerShell コマンドレットを使用して Parallels RAS の管理タスクを実行できます。コマンドレットは、Windows PowerShell コンソールで実行することも、スクリプトを書いて一般的な Parallels RAS の管理タスクを実行することもできます。Parallels RAS PowerShell の完全ガイドは、その他の Parallels RAS マニュアルとともに Parallels ウェブサイトで入手できます。
RAS REST API	Parallels RAS にはさまざまな API があり、これにより API が統合されたカスタムアプリケーションを開発できます。RAS REST API はその 1 つです。
RAS 管理ポータル	Parallels RAS 管理ポータルは、HTML5 ブラウザーベースのアプリケーションで、これにより Parallels RAS を管理できます。
RAS ウェブ管理サービス	RAS 管理ポータルのユーザーインターフェイスを提供し、RAS REST API（上記を参照）の RESTful ウェブサービスを実装するウェブサービスです。

Azure Virtual Desktop	Azure Virtual Desktop は、Microsoft Azure で実行されるデスクトップおよびアプリの仮想化サービスであり、RD セッションホストおよび VDI へのアクセスを提供します。Parallels RAS 18 は、Parallels RAS の既存の技術的機能に加えて、Azure Virtual Desktop のワークロードを統合、構成、保守、サポートしたり、アクセスを確保したりする機能を提供します。
FSLogix	FSLogix プロファイルコンテナーは、パーシスタントでない環境向けのリモートプロファイルソリューションです。Parallels RAS は、RD セッションホスト、VDI、および Azure Virtual Desktop で FSLogix をサポートします。

第 2 章

Parallels RAS のインストール

この章では、Parallels RAS をインストールし、アクティベートする方法について説明します。

この章の内容

システム要件

Parallels RAS をインストールする前に、ハードウェアとソフトウェアが、以下のハードウェアおよびソフトウェア要件以上であることを確認してください。Parallels RAS は、ワークグループ環境でも使用できますが、Parallels では Active Directory を使用し、グループポリシーを介して、ユーザー、グループ、マシンアカウントを管理することをお勧めしています。

ハードウェア要件

Parallels RAS は、物理プラットフォームおよび仮想プラットフォーム上で広範囲にわたってテストされています。Parallels RAS を実行するうえで認定されたハードウェアの最低要件を以下に示します。

- 物理マシン - デュアルコアプロセッサ、最小 4GB の RAM。
- 仮想マシン - 2 基の仮想プロセッサ、最小 4GB の RAM。

Parallels RAS をインストールおよび構成するためのサーバーハードウェア要件は、エンドユーザーの要件によって異なる可能性があります。

通常、30 ユーザー以下のインストールの場合、1 つの高性能サーバーに Parallels RAS をインストールし、そのサーバーからリソースを直接公開することができます。30 ユーザー以上の場合、複数のサーバーが必要になる可能性があります。

Parallels RAS の展開を計画する段階で、以下の点を考慮する必要があります。

- 複数の CPU コア、高性能のディスク転送速度、および十分な RAM で構成される高性能サーバーを使用する必要があります。
- エンドユーザーに提供するために必要なリソースが適切に用意されている場合は、ハイパーバイザーベースの仮想マシンを使用できます。
- Gateway SSL モードを使用する受信接続では、RAS Secure Gateway が 1 台のサーバーにつき 1200 ユーザーを超えないようにすることをお勧めします。
- HALB の使用量は、HALB アプライアンスごとに 2000 ユーザーセッションを超えてはなりません。https://kb.parallels.com/125229 を参照してください。
- VDI ハイパーバイザーリソースの要件を計画する場合、仮想マシンごとの RAM 使用量、ディスク容量など、追加の要件を考慮する必要があります。

RD セッションホスト、VDI、または Azure Virtual Desktop を構成する場合、ワークロードの種類に応じて、セッションホストを構成する必要があることに注意してください。可能な限り最高のエクスペリエンスを得るには、ユーザーのニーズに応じて展開を拡張する必要があります。次の表は、さまざまなワークロードの種類がセッションホストの構成にどのように影響するかを示しています。

ワークロード	ユーザーの例	アプリの例	vCPU あたりの最大ユーザー数	最小要件
ライト	基本的なデータエントリータスク	データベースエントリーアプリケーション、コマンドラインインターフェイス	6	2 vCPU 8 GB RAM 16 GB ストレージ
ミディアムユーザー	コンサルタントおよびマーケットリサーチ	データベースエントリーアプリケーション、コマンドラインインターフェイス、Microsoft Word、静的ウェブページ	4	4 vCPU 16 GB RAM 32 GB ストレージ
ヘビーユーザー	ソフトウェアエンジニア、コンテンツ作成者	データベースエントリーアプリケーション、コマンドラインインターフェイス、Microsoft Word、静的ウェブページ、Microsoft Outlook、Microsoft PowerPoint、動的ウェブページ	2	4 vCPU 16 GB RAM 32 GB ストレージ
パワーユーザー	グラフィックデザイナー、3D モデルメーカー、機械学習の研究	データベースエントリーアプリケーション、コマンドラインインターフェイス、Microsoft Word、静的ウェブページ、Microsoft Outlook、Microsoft PowerPoint、動的ウェ	1	6 vCPU 56 GB RAM 340 GB ストレージ

		ブページ、Adobe Photoshop、Adobe Illustrator、CAD、CAM		

注: サイズについてのガイドラインは、RDS または Azure Virtual Desktop マルチセッションホストに関する Microsoft の推奨事項に基づいています。

ポートの要件については、「ポート参照」セクションを参照してください。

ソフトウェア要件

RAS Connection Broker および RAS Secure Gateway（64 ビット版のみ）

RAS Connection Broker および RAS Secure Gateway は、次のオペレーティングシステムでサポートされています。

- Windows Server 2012 R2 から Windows Server 2022 まで
- Windows Server 2016、2019 および 2022（Server Core とデスクトップエクスペリエンスインストールの両方がサポート対象）

注: DHCP サーバーを実行しているドメインコントローラーやその他のマシンに RAS Connection Broker や RAS Secure Gateway をインストールしないでください。一般的に、これはどの RAS コンポーネントにも当てはまります。

RAS ウェブ管理サービス

RAS Connection Broker と同じ OS が必要です（上記参照）。なお、大規模環境（同時接続数が 2000 以上）では、専用のサーバーにインストールすることをお勧めします。詳細については、https://kb.parallels.com/en/124988 を参照してください。

また、Windows Server 2012 R2 では、以下のアップデートをインストールする必要があります。ご注意ください。

- Windows Server 2012 R2 - KB2999226

新しいバージョンの Windows Server では特定のアップデートは必要ありません。

RAS RD セッションホスト Agent

RAS RD セッションホスト Agent は、次のオペレーティングシステムでサポートされています。

- Windows Server 2008 R2 から Windows Server 2022 まで
- “デスクトップエクスペリエンス”インストールオプションを使用して Windows Server 2016 以降をインストールする必要があります。
- Windows Server 2012 R2（Server Core のインストールオプションはサポートされていません）

RAS Provider Agent

- Windows Server 2012 R2 から Windows Server 2022 まで

サポートされるプロバイダーのリストについては、「RAS Provider Agent のインストールオプション」（p. 166）を参照してください。

RAS Guest Agent

- Windows Server 2008 R2 から Windows Server 2022 まで
- Windows 7 から Windows 11 まで

Remote PC Agent

- Windows Server 2008 R2 から Windows Server 2022 まで
- Windows 7 から Windows 11 まで

Parallels RAS PowerShell

- Windows Server 2012 R2 から Windows Server 2022 まで
- Windows 7 から Windows 11 まで
- Windows Management Framework 3.0 および .NET Framework 4.5.2 をインストールする必要があります

Parallels RAS Console

- Windows Server 2012 R2 から Windows Server 2022 まで
- Windows 7 から Windows 11 まで

RAS 登録サーバー

- Windows Server 2012 R2 から Windows Server 2022 まで

Parallels Client

Parallels Client は、次のオペレーティングシステムで認定されています（32 ビット版と 64 ビット版がある場合はその両方に対応）。

- Windows 7、8.x、10、11
- Windows Server 2008 R2 から Windows Server 2022 まで
- macOS 12 Monterey から macOS 14 Sonoma まで。Parallels Client は、Intel または Apple M1、いずれのチップを搭載する Mac コンピューター上でもネイティブに動作します。
- iOS および iPadOS 15 以降
- Android 7 以降
- Chrome OS

  注: Parallels Client for Chrome は廃止予定です。代わりに Parallels Web Client を使用することをお勧めします。

Parallels Client for Linux は、次の Linux ディストリビューション（x64 版のみ）をサポートしています。

- Ubuntu 18.04 LTS、20.04 LTS、22.04 LTS
- Debian 11（Bullseye）、Debian 12（Bookworm）
- Fedora 37、38
- Linux Mint 20、21
- ThinOS/ Dell Wyse Thin Clients 2303

Igel、HP、10Zig などのテクノロジーパートナーがサポートするシンクライアントとサポートされるハードウェアのリストについては、次のナレッジベースの記事を参照してください: https://kb.parallels.com/124606。

Microsoft ライセンスの要件

リモートデスクトップサービスクライアントアクセスライセンス（RDS CAL）や仮想デスクトップアクセス（VDA）ライセンスなど、Microsoft のライセンス要件については、付録: Parallels RAS の Microsoft ライセンスの要件（p. 628）を参照してください。

Parallels RAS をインストール

Parallels RAS をインストールするには、以下の操作を実行します。

1 Parallels RAS をインストールしているコンピューターに管理者権限があることを確認します。

2 `RASInstaller.msi` ファイルをダブルクリックし、Parallels RAS のインストールウィザードを起動します。”Parallels RAS のこのバージョンはテスト目的でのみご使用いただけます”で開始されるメッセージが表示された場合、ご利用のバージョンが公式のビルドではなく、本番環境での使用が禁止されていることを意味します。

3 画面上の指示に従います。

> **注:** インストールやアップグレードを行う際には、ライセンス契約に記載されている内容を確認し、同意した上で行ってください。プログラムによる展開の場合は、ライセンス契約の条項をお読みの上同意したものとみなされます。
>
> **注:** メジャーバージョンからアップグレードする場合（たとえば、Parallels RAS 18 から Parallels RAS 19）、新バージョンの各コンポーネントのシステム要件が記載されたメッセージが表示されます。現在の環境ですべてのコンポーネントがアップグレード可能であることを確認するために、これらを注意深くお読みください。システム要件を満たさないシステムにコンポーネントをインストールした場合、そのコンポーネントは動作しないことに注意してください。

4 「インストールタイプの選択」ページに進み、以下の中から選択します。

- Parallels Remote Application Server を指定します。RAS Console、RAS 管理ポータル、RAS Connection Broker、RAS Secure Gateway、RAS RD セッションホストエージェント、RAS PowerShell、および RAS ウェブ管理サービスを同じマシンにインストールするデフォルトのインストール方法です。この方法は、テストや小規模な本番環境に最適です。
- Parallels RAS テナントブローカー: このオプションはテナントブローカーをインストールします。なお、テナントブローカーは、既存の RAS ファームとは別のサーバーにインストールする必要があります。テナントブローカーの詳細については、「RAS マルチテナントアーキテクチャ」の章（p. 397）を参照してください。
- カスタム: 必要なコンポーネントのみを選択してインストールします。[次へ] をクリックした後、個々のコンポーネントを選択できます。現在のサーバーにコンポーネントをインストールできない場合、インストールに利用できないことに注意してください。「ソフトウェア要件」を参照してください。

5 [次へ] をクリックします。

6 [重要なお知らせ] ウィザードページのお知らせを確認します。コンピューターでポートの競合がある場合、情報がここに表示されます。競合は後で解決できます。

7 [次へ] をクリックします。

8 [ファイアウォールの設定] ページで [ファイアウォールルールを自動的に追加] を選択します。これにより、Parallels RAS が適切に動作するようにこのコンピューターでファイアウォールが構成されます。詳細については、「ポート参照」を参照してください。

9 [次へ] をクリックし、[インストール] をクリックします。インストールが終了するまで待って、[完了] をクリックします。

10 RAS のバージョンをアップグレードする場合、コンポーネントをアップグレードするすべてのサーバーの再起動をお勧めします。

別のサーバーに特定の Parallels RAS コンポーネントをインストールする必要がある場合は、もう一度インストールウィザードを実行し、[カスタム] を選択し、インストールするコンポーネントを選択します。

Parallels RAS のログインとアクティベート

Parallels RAS をインストールした後、RAS Console を実行し、新しい Parallels RAS ファームをアクティベートします。

Parallels RAS Console の起動

デフォルトでは、インストールウィザードの最後のページで [完了] をクリックした後、Parallels RAS Console が自動的に起動します。コンソールを手動で起動するには、[スタート] > [アプリ] > [Parallels] に移動して、[Parallels Remote Application Server Console] をクリックします。

Parallels RAS Console の初回起動時に、ログインダイアログが表示されます。ダイアログで、以下の情報を指定します。

- ファーム: 接続先の Parallels RAS ファーム。RAS Connection Broker がインストールされているサーバーの FQDN または IP アドレスを入力します。
- RAS Console をインストールするときに Parallels Single Sign-On コンポーネントをインストールしている場合、[認証タイプ] フィールドが表示され、そこから資格情報を使用してログオンするか、 SSO を使用してログオンするかを選択できます。インストール後に再起動し、SSO を選択する場合は、[Single Sign-On] を選択し、[接続] をクリックします。

RAS ファームへのログインには、Windows 資格情報が使用されます。[資格情報] を選択する場合は、下記のように資格情報を入力します。

- ユーザー名: Parallels RAS がインストールされているサーバーでの管理権限があるユーザーアカウント（通常はドメインまたはローカル管理者）。アカウント名は UPN 形式（例: `administrator@domain.local`）で指定する必要があります。指定したユーザーは自動的に完全なアクセス権がある Parallels RAS 管理者として構成されます。
- パスワード: 指定したユーザーアカウントのパスワードです。
- [認証情報を記憶する] オプションを選択した場合、次に Parallels RAS Console を起動したときにはこのダイアログは表示されません。

[接続を編集する] ボタンをクリックすると、ダイアログが開き、RAS 接続を管理できます。このダイアログは、1 つまたは複数の RAS ファームに接続するのが初めてではない場合に有用です。ダイアログの左ペインには、以前に接続した RAS ファームが表示されます（ファームが不要になった場合、[-] アイコンをクリックしてリストから削除できます）。右ペインには、少なくとも選択したファームのプライマリ Connection Broker が表示されます。ファームにセカンダリ Connection Broker を追加している場合、[+] アイコンをクリックし、そのホスト名または IP アドレスを入力して、このリストに追加できます（エージェントのステータスを確認するには、[リサイクル] アイコンをクリックします）。この方法で、RAS Console はプライマリ Connection Broker に最初に接続を試み、失敗した場合（例: エージェントがオフラインになっている、またはアクセスできない）、セカンダリ Connection Broker への接続を試みます。セカンダリ Connection Broker の詳細については、「Parallels RAS Connection Broker」の章（p. 77）を参照してください。

接続情報の入力が完了したら、[接続] ボタンをクリックして、Parallels RAS ファームに接続します。

Parallels My Account へのサインイン

Parallels RAS をアクティベートするには、Parallels ビジネスアカウントに登録する必要があります。Parallels RAS にログインした後、[Parallels My Account へのサインイン] ダイアログが表示されます。すでにアカウントをお持ちの場合は、アカウントの登録時に使用したメールアドレスとパスワードを入力して、[サインイン] をクリックします。

注: ネットワークで HTTP プロキシサーバーを使用している場合、プロキシサーバーの接続設定を構成するように求めるダイアログが表示されます。[プロキシを設定] ボタンをクリックします。ダイアログが開いたら、次のいずれかを選択します。[システムのプロキシ設定を使用]（Internet Explorer のデフォルトのプロキシ設定が使用されます）または [手動での HTTP プロキシ構成]（設定を手動で

指定します）。プロキシ構成が変更された場合、[管理] > [設定] に移動し、[プロキシを設定] ボタンをクリックして、後から再構成できます。

Parallels ビジネスアカウントをお持ちでない場合は、次のように登録できます。

1. [Parallels My Account へのサインイン] ダイアログで、[登録] をクリックします。[Parallels My Account を登録] ダイアログが開きます。
2. 名前とメールアドレスを入力し、パスワードを選択して入力し、会社情報を入力します（すべて必須フィールドです）。
3. Parallels のプライバシーポリシーとご利用条件へのリンクをご確認ください。それらを読んだ後（そして同意する場合）、[私は Parallels の「個人情報の取り扱いについて」と「ご利用条件」を読み、その内容に同意します] チェックボックスを選択してください。
4. [登録] をクリックして、アカウントを登録します。これで、自分用の個人アカウントと、管理者として割り当てられる組織用のビジネスアカウントが作成されます。

Parallels RAS をアクティベートする

Parallels My Account にサインインした後、[製品をアクティベート] ダイアログが開き、Parallels RAS ファームをアクティベートするように求められます。

Parallels RAS のライセンスキーをすでにお持ちの場合は、[ライセンスキーを使用してアクティベートする] オプションを選択して、表示されているフィールドにキーを入力します。フィールドの横にあるボタンをクリックすると、Parallels My Account に登録されているサブスクリプションと永久ライセンスキーのリストを表示することができます。リストが空の場合は、サブスクリプションまたはライセンスキーがなく、まず初めに購入する必要があります。

注: Parallels RAS Console の [ライセンス] カテゴリーを使用して Parallels RAS ライセンスを管理できます。管理タスクには、ライセンス情報の表示、別の Parallels My Account への切り替え、および別のライセンスキーを使用する Parallels RAS ファームのアクティベートなどがあります。詳細については、「ライセンス」セクション（p. 591）を参照してください。

Parallels RAS ライセンスキーをお持ちでない場合は、以下のオプションが利用できます。

- [ライセンスを購入する] リンクをクリックして、サブスクリプションをオンラインで購入します。
- [トライアルバージョンをアクティベートする] オプションを選択して、Parallels RAS をトライアル版としてアクティベートします。

ライセンスキーを入力した後（またはトライアル版のアクティベートを選択した後）、[アクティベート] をクリックします。Parallels RAS ファームが正常にアクティベートされたことを示すメッセージが表示されます。[OK] をクリックして、メッセージボックスを閉じます。

最初に表示されるダイアログには、公開済みのリソースをホストするために使用できる構成されたサーバーがないことが表示されます。これは、Parallels RAS の使用を開始するには、少なくとも 1 つの RD セッションホスト、プロバイダー、またはリモート PC を構成する必要があるということです。次の章で Parallels RAS ファームの構成について説明します。今のところは、[OK] をクリックして、メッセージボックスを閉じます。その後で [設定を適応する] ダイアログが表示されます。Parallels RAS の初期構成が完了するのを待ち、[OK] をクリックします。Parallels RAS Console のメインウィンドウが表示されます。Parallels RAS ファームの構成を開始できます。

次に、すばやく RD セッションホストを追加する方法、リソースを公開する方法、ユーザーを Parallels RAS に招待する方法について説明します。

第 3 章

Parallels RAS の使用を開始する

この章は、Parallels RAS を使い始める際に役立ちます。Parallels RAS Console の使用方法と簡単な RAS 環境の設定方法について説明します。

この章の内容

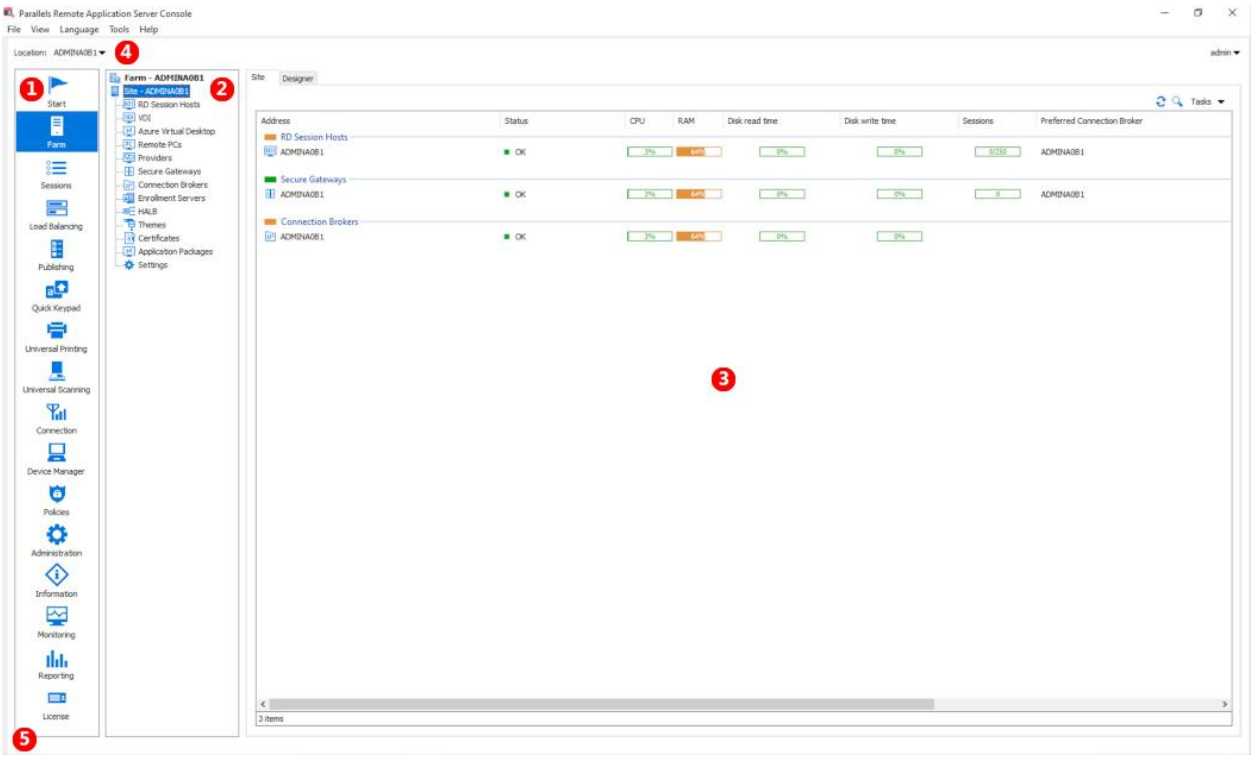
Parallels RAS Console

Parallels RAS Console は、Parallels RAS ファームの構成と管理に使用する Windows アプリケーションです。

Parallels RAS Console を開くには、[アプリ] > [Parallels] に移動し、[Parallels Remote Application Server Console] をクリックします。コンソール内で切り替えることなく 2 つ以上のファームまたはサイトを同時に管理する場合、Parallels RAS Console の複数のインスタンスを同じコンピューターで開くことができます。この機能は、ローカルにインストールされている Parallels RAS Console を使用する場合、また Parallels Client からリモートアプリケーションとして実行する場合に有効となります。

情報: Parallels RAS Console に加えて、Parallels RAS 18 では Parallels RAS 管理ポータルが導入されました。これは Parallels RAS を管理できる HTML5 ブラウザーベースのコンソールです。この記事の執筆時点では、一部の管理機能はまだ開発中であるため、Parallels RAS 管理ポータルがデスクトップ版の RAS Console に完全に取って代わるわけではないことに注意してください。続くリリースで、さらに機能が追加される予定です。詳細については、以下の Parallels ウェブサイトで利用できる「Parallels RAS 管理ポータルガイド」をお読みください: https://www.parallels.com/products/ras/resources/。

次のスクリーンショットと以下の説明は、Parallels RAS Console の概要に関するものです。



Parallels RAS Console は、次の各セクションで構成されています。

1. このセクションにはカテゴリーが一覧表示されます。カテゴリを選択すると、そのカテゴリに関連する要素が右ペインに表示されます。

2. このセクション（中央のペイン）は、[ファーム] カテゴリと [公開] カテゴリの場合のみ利用できるようになります。ナビゲーションツリーでは、選択したカテゴリに関連するオブジェクトを参照できます。

3. このセクションには、ファーム内のサーバー、公開済みのアプリケーションのプロパティなど、選択したオブジェクトやカテゴリのプロパティが表示されます。

4. RAS Console 上部の情報バーには、現在ログインしているサイトの名前が左側（[場所] フィールド）に表示されます。複数のサイトを利用している場合は、ドロップダウンリスト（サイト名）をクリックし、目的のサイトを選択して、サイトを切り替えられます。RAS Console を使用して複数のファームに接続している場合、ドロップダウンリストには他のファーム名も表示されます。これをクリックすると、コンソールがそのファームに接続されます。

   右側には管理者アカウント名が表示されます。名前をクリックするとドロップダウンリストが開き、そこから他の管理者とのチャットを開始したり、現在のセッションを表示したり、RAS Console からログオフしたりできます。

   いずれかのコンポーネントまたはオブジェクトを変更した後、中央（赤色）に新しい設定を確定するには [適用] を押しますというメッセージが表示されます。このメッセージは、変更を有効にするには変更を Parallels RAS に適用する必要があることを通知します。動作について以下に説明します。

   RAS Console で変更を加えた場合、ダイアログで [OK] をクリックするとすぐに変更内容がデータベースに保存されます。このタイミングでコンソールを閉じると、データベースに変更内容が残され、変更内容が失われることはありません。しかし、Parallels RAS プロセスの実行中インスタンスには変更内容がまだ適用されていないため、実行中の RAS ファームに影響はありません。[適用] ボタン（画面下部）をクリックすると、変更内容がランタイムに適用され、すぐに有効になります。

   RAS Console に変更を加える場合は、次のルールに従ってください。小規模な変更を加える場合は、変更を加え終わったらすぐに [適用] をクリックできます。複数の場所にまたがって大規模な修正を加える必要がある場合、すべての変更を加え終えてから [適用] を押すことで、同時にすべての変更内容を適用できます。

5. 最新のコンソール通知は画面下部の情報バーに表示されます（新規の通知がある場合）。

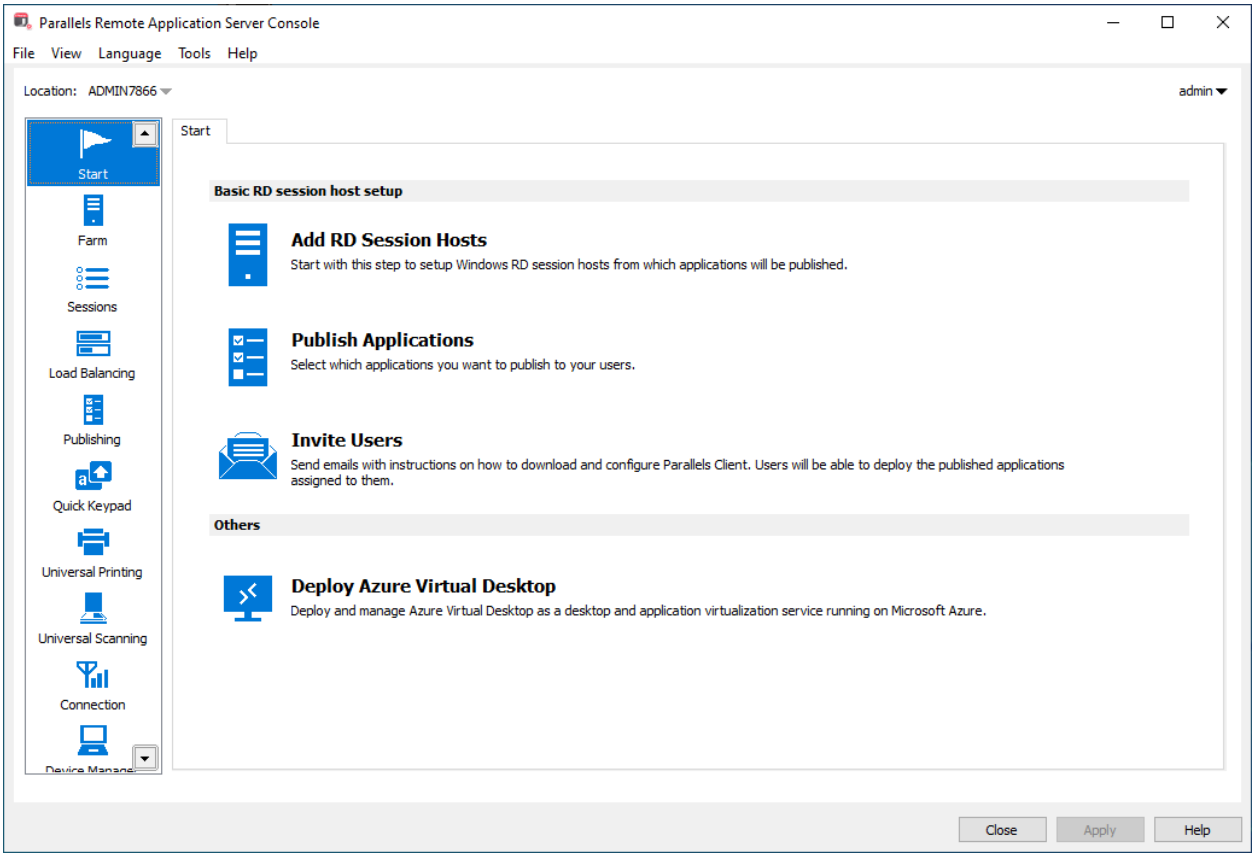
基本的な Parallels RAS ファームを設定する

このセクションでは、必要なコンポーネントすべてが 1 台のサーバーで動作する基本的な Parallels RAS ファームを設定します。

Parallels RAS ファームを設定するには、次の操作を実行します。

1 Parallels RAS Console にログインします。

2 コンソールで、[開始] カテゴリーを選択します。このカテゴリーから 3 つのウィザードにアクセスして、RD セッションホストを追加する、アプリケーションを公開する、Parallels RAS にユーザーを招待するなど、重要なタスクを簡単に実行できます。

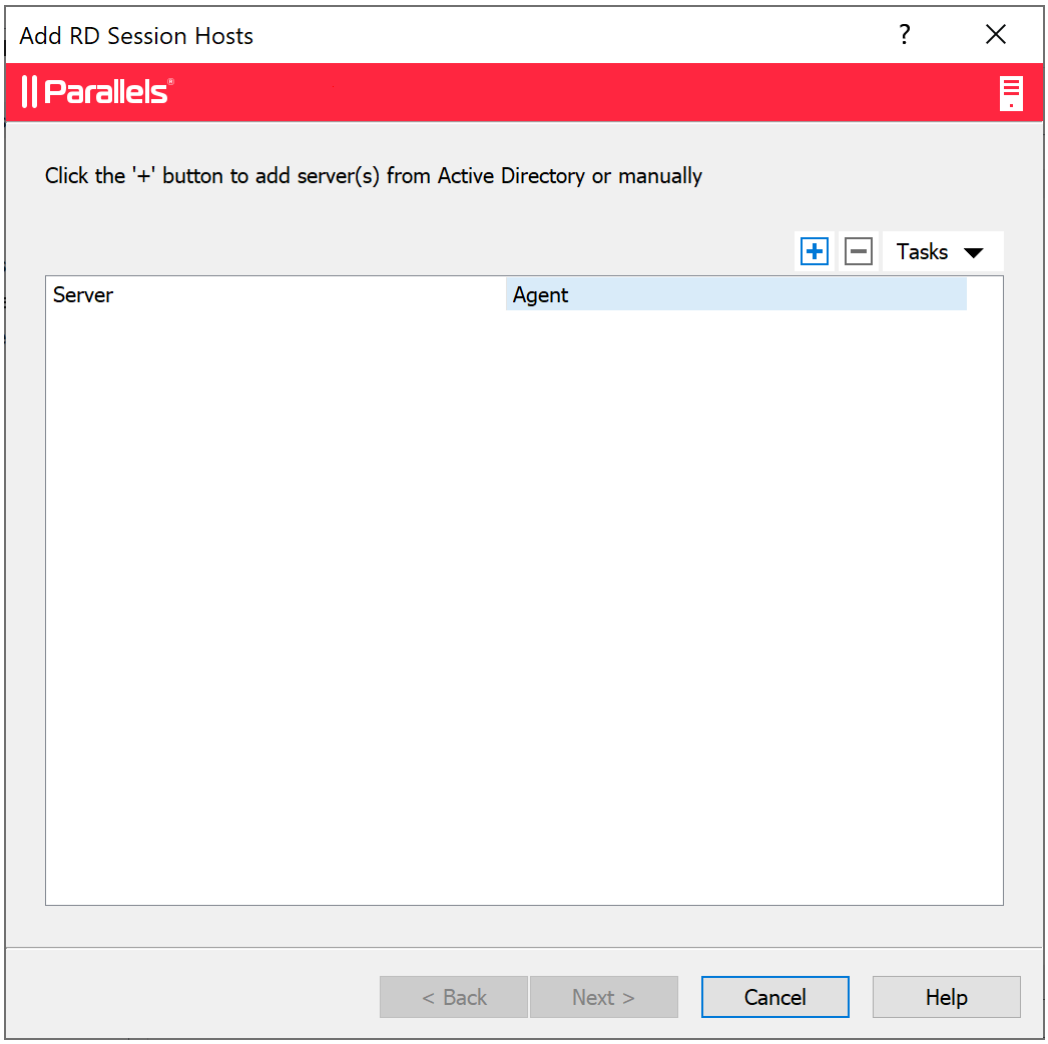


RD セッションホストを追加

最初に、RD セッションホストをファームに追加する必要があります。このチュートリアルでは、Parallels RAS がインストールされるローカルサーバーを追加します。

RD セッションホストをファームに追加するには、次の操作を実行します。

1 [RD セッションホストを追加] をクリックします。[RD セッションホストを追加] ウィザードが開きます。



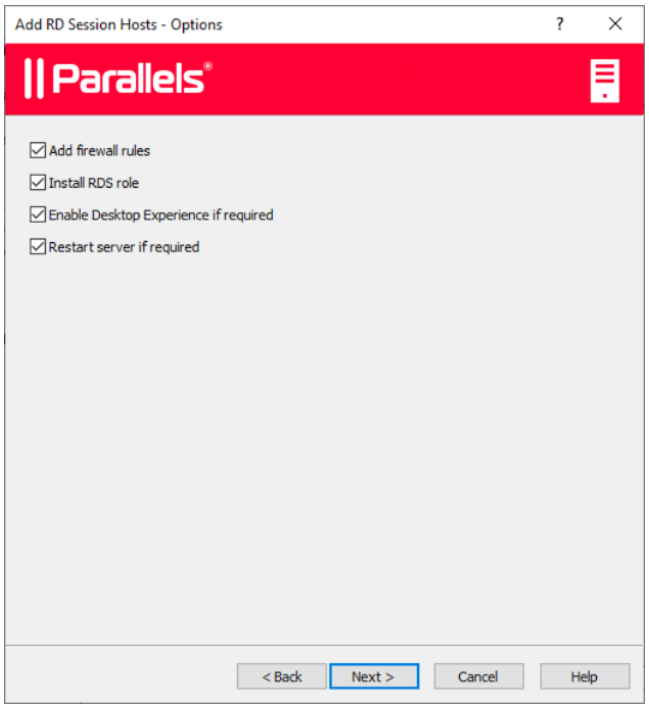
2 [タスク] メニューをクリック（または [+] アイコンをクリック）し、次のいずれかを選択します。

- Active Directory から追加する: Active Directory から RD セッションホストを追加します。
- 手動で追加する: RD セッションホストの FQDN または IP アドレスを入力し、追加します。

サーバーの FQDN を入力すると、他の RAS コンポーネントやクライアントからそのサーバーに接続する主要な方法として使用されることに注意してください。IP アドレスを入力すると、自動的に FQDN に解決されます。ただし、FQDN に解決するグローバルオプションが有効な場合に限ります。このグローバルオプションの現在の設定を確認するには、メインメニューの [ツール] > [オプション] をクリックします。[オプション] ダイアログで、[ホストを追加する場合は、常に完全修飾ドメイン名（FQDN）で解決するよう試みてください] オプションを確認します。このオプションが選択されている場合、その RAS ファーム内のすべてのサーバー/コンポーネントの IP アドレスは、常時 FQDN に解決されます。このオプションの選択を解除すると、サーバーとの通信にはサーバーに指定した内容（IP アドレスまたは名前）がそのまま使用されます。サーバーがクラウド内にホストされている場合のように、IP アドレスではサーバーにアクセスできない場合の展開では、この機能が役立ちます。詳細については、「ホスト名の解決」（p. 568）を参照してください。

3 [次へ] をクリックします。

4 一般設定のページが開きます。



次の設定を行います。

- ファイアウォールルールを追加: サーバー上で実行されている Windows で Parallels RAS が必要とするファイアウォールルールを追加します。詳細については、「ポート参照」を参照してください。
- RDS 役割をインストール: インストールされていない場合は、RDS 役割をサーバーにインストールします。このオプションは常に選択する必要があります。
- デスクトップエクスペリエンスを有効にする: サーバー上で実行されている Windows でデスクトップエクスペリエンス機能を有効にします。このオプションは、[RDS 役割をインストール] オプション（上記）が選択されている場合のみ有効です。このオプションは、デスクトップエクスペリエンス機能がデフォルトで有効にされていない、Windows Server 2008 R2 および Windows 2012 R1/R2 に適用されます。
- 必要な場合にサーバーを再起動: 必要な場合にサーバーを自動的に再起動します。必要に応じて、手動でサーバーを再起動することもできます。

5 [次へ] をクリックします。

6 サーバー（1 台または複数）をホストプールに追加します。必要なホストプールを選択するか、新しいホストプールを作成します。どのホストプールを選択したらよいかわからない場合は、[既定のホストプール] を選択してください。ホストプールについて詳しくは、「ホストプール（RD セッションホスト）の管理」（p. 115）セクションで説明します。

7 [次へ] をクリックします。

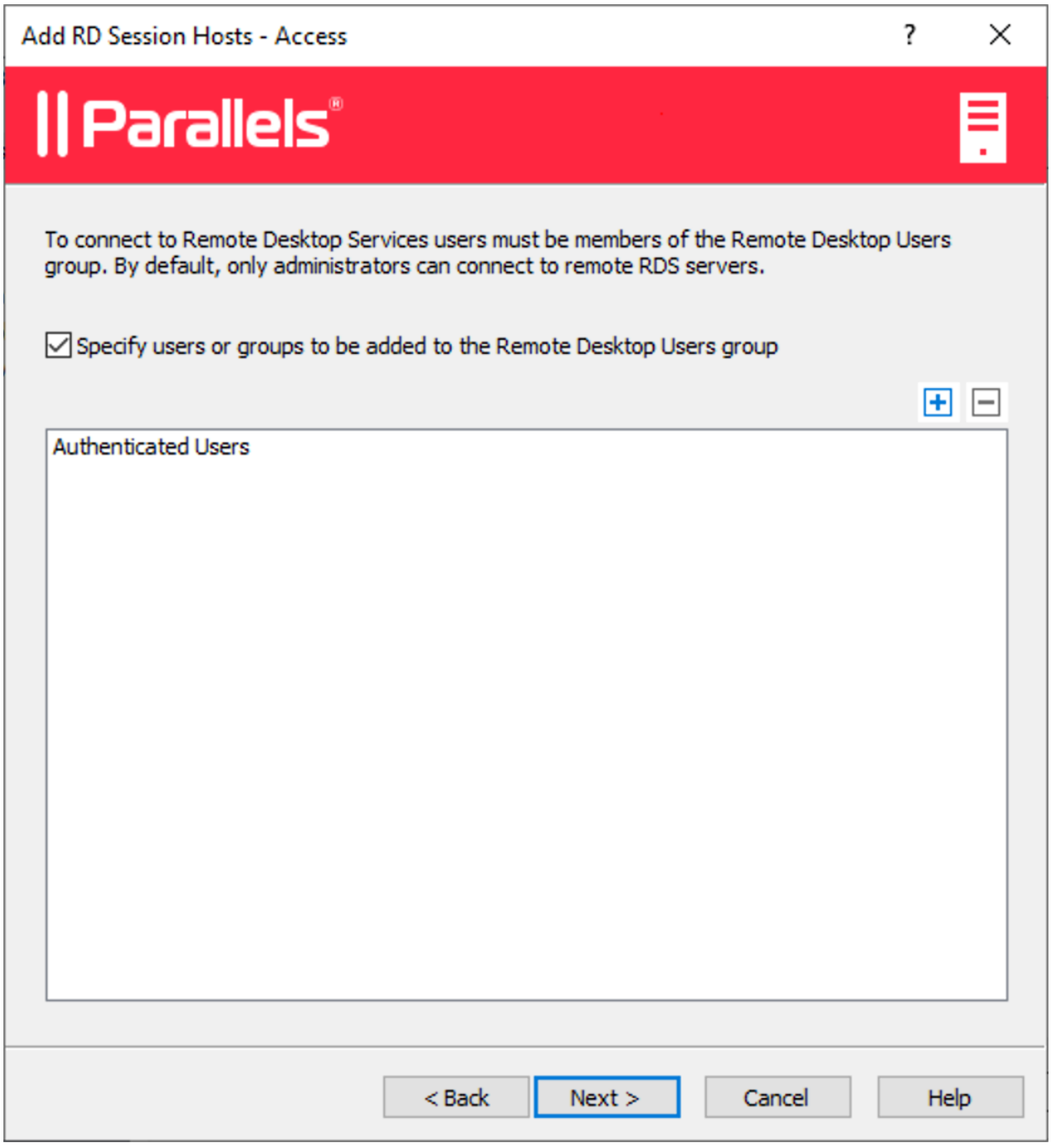
8 エンドユーザーが RD セッションホストで公開されているリソースにアクセスできるようにするには、対象のユーザーをサーバーで実行されている Windows のリモートデスクトップユーザーグループに追加する必要があります。これは、次のいずれかの方法で実行できます。

- 標準の Windows 管理ツールを使用して、各ユーザーまたはグループをサーバーに直接追加します。
- ActiveDirectory 経由でのユーザーまたはグループの追加。
- ユーザーの利便性のために提供されている、以下で説明するウィザードページを使用します。

特定のサーバーのリモートデスクトップユーザーグループにユーザーをすでに追加している場合（または何らかの理由で上記の他の方法のいずれかを使用する場合）、[次へ] をクリックするだけでこのページをスキップできます。

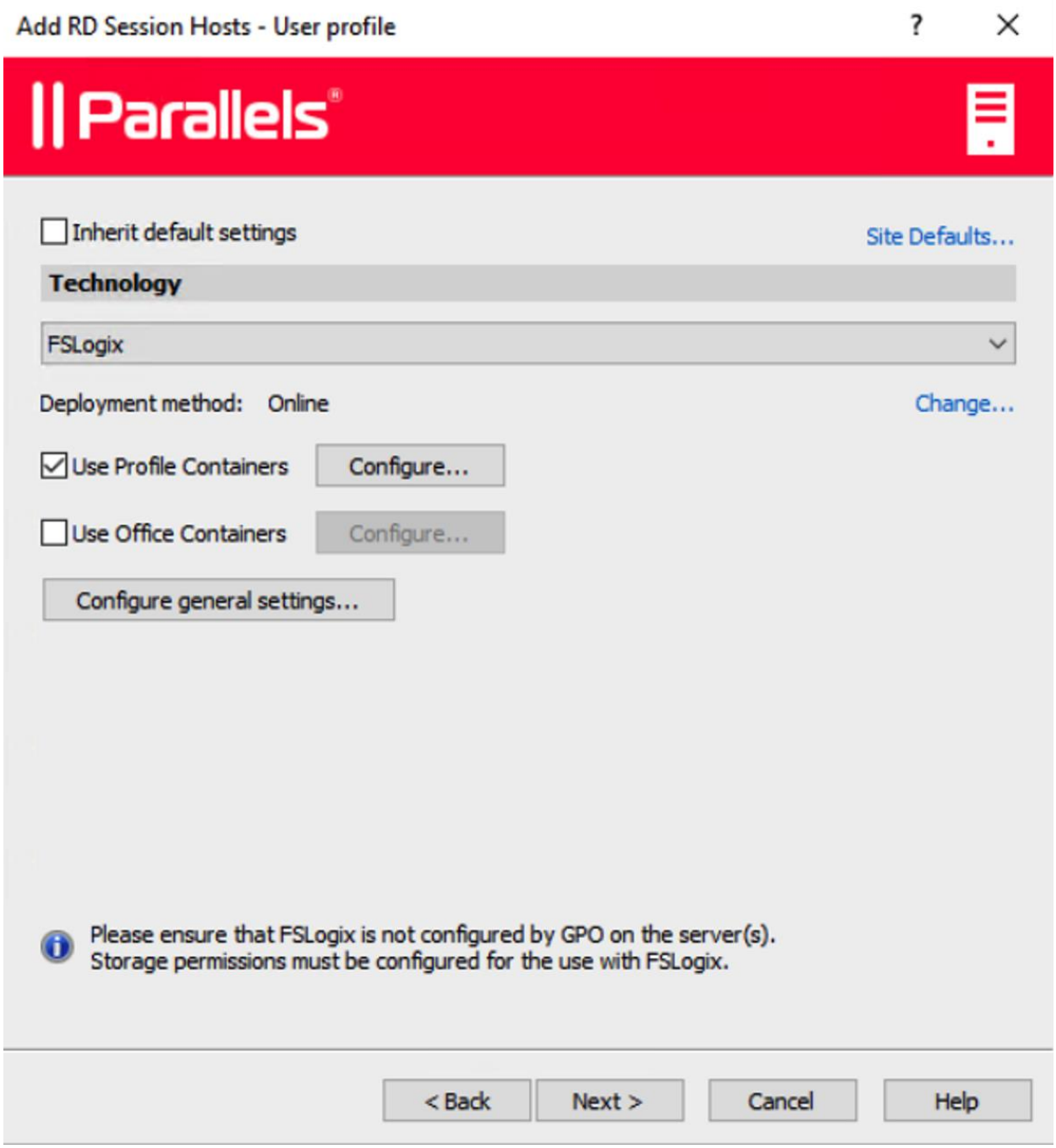
ウィザードを使ってリモートデスクトップユーザーグループにユーザーを追加するには、[リモートデスクトップユーザーグループに追加するユーザーまたはグループを指定] オプシ

ョンを選択し、[+] アイコンをクリックします。[ユーザーまたはグループの選択] ダイアログで、ユーザーまたはグループを指定して、[OK] をクリックします。選択されたユーザー/グループがウィザードページのリストに追加されます。



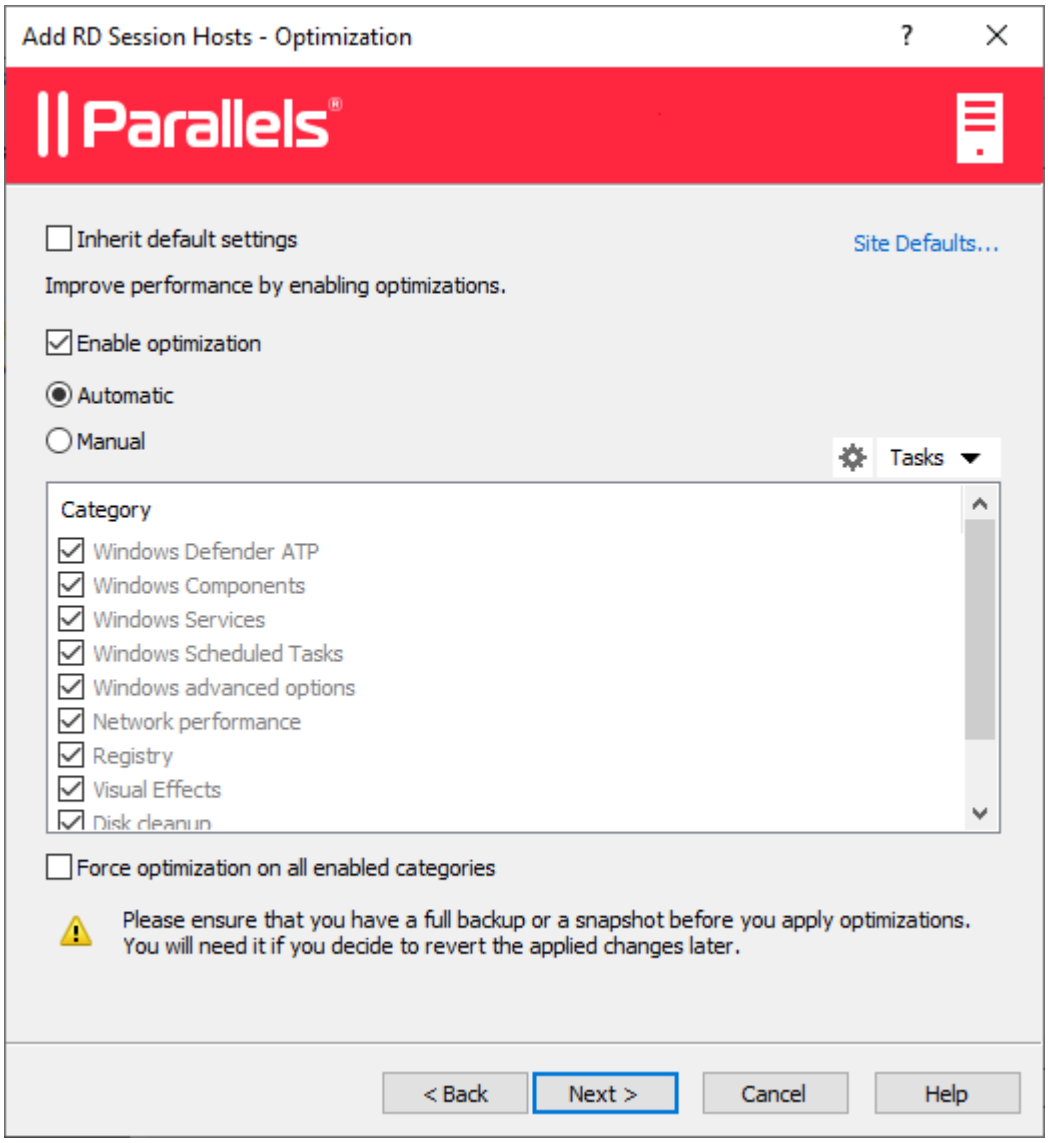
9 [次へ] をクリックします。

10 [ユーザープロファイル] ページでは、ユーザープロファイルを管理するためのテクノロジーを選択できます。



ユーザープロファイルディスクまたは FSlogix のいずれかを選択できます。ユーザープロファイルディスクは、専用のファイル共有にユーザーアプリケーションデータを保存する仮想ハードディスクです。Microsoft FSLogix プロファイルコンテナーは、ローミングプロファイルおよびユーザープロファイルディスク（UPD）の後継技術として利用されることの多いプロファイル管理ソリューションです。これは、パーシスタントでない環境でユーザーコンテキストを維持し、サインイン時間を最小限に抑え、互換性の問題を排除するネイティブプロファイルのユーザーエクスペリエンスを提供できるように構成されています。ここでは、デフォルト設定を維持しても問題ありません。ユーザープロファイルについては、このガイドの後半で詳しく説明します（p. 138）。

11 [最適化] ページでは、Parallels RAS 環境での最高のパフォーマンスを実現するために使用される、RD セッションホストにおける Windows システムの最適化設定を指定できます。



無効化、削除、または最適化の対象となる Windows コンポーネントやサービス、またその他のオプションを選択して、仮想アプリおよびデスクトップの配信の効率性と合理性を向上させ、改善することができます。ここでは、デフォルト設定を維持することも、最適化を変更（不明瞭な場合は無効化）することもできます。最適化については、このガイドの後半で詳しく説明します（p. 146）。

12 次のページで、設定を確認して、[次へ] をクリックします。

13 [RAS RD セッションホスト Agent をインストール] ダイアログが開きます。指示に従って、Agent をインストールします。インストールが完了したら、[完了] をクリックしてダイアログを閉じます。

14 ウィザードに戻り、[完了] をクリックしてウィザードを閉じます。

RD セッションホストがファームに追加されていることを確認するには、[ファーム] カテゴリー（Parallels RAS Console ウィンドウの左ペインの [開始] カテゴリーの下）をクリックし、ナビゲーションツリー（中央のペイン）で [RD セッションホスト] をクリックします。サーバーは、[RD セッションホスト] リストに表示されています。[ステータス] 列に、警告メッセージが表示されることがあります。警告メッセージが表示された場合は、サーバーを再起動します。[ステータス] 列に、”OK”と表示されている場合、RD セッションホストは正常に機能しています。

次に、RD セッションホストからアプリケーションを公開する方法（p. 49）について説明します。

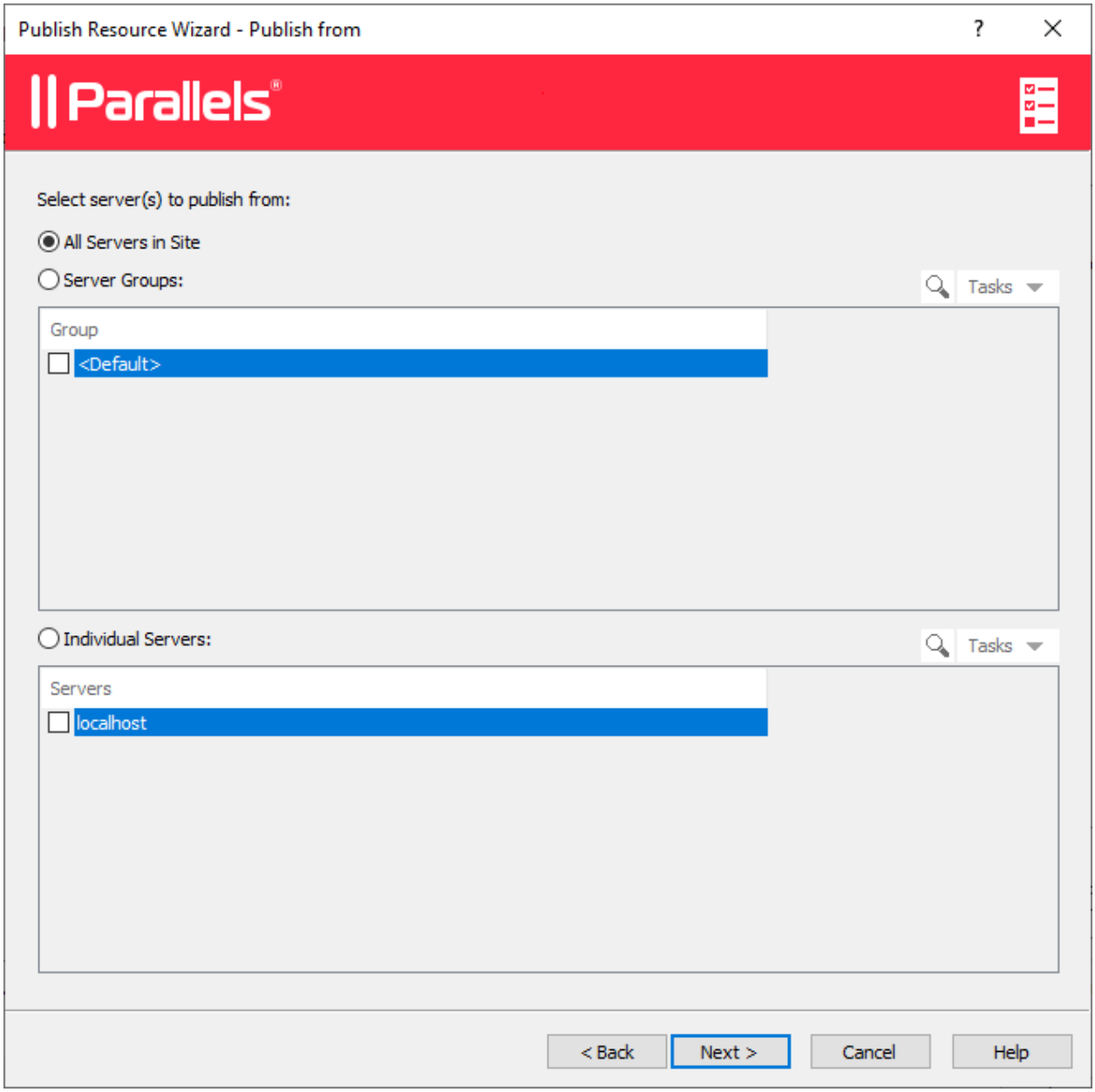
アプリケーションを公開

RD セッションホストを追加すると、ここからアプリケーションを公開できるようになります。

アプリケーションを公開するには、次の操作を実行します。

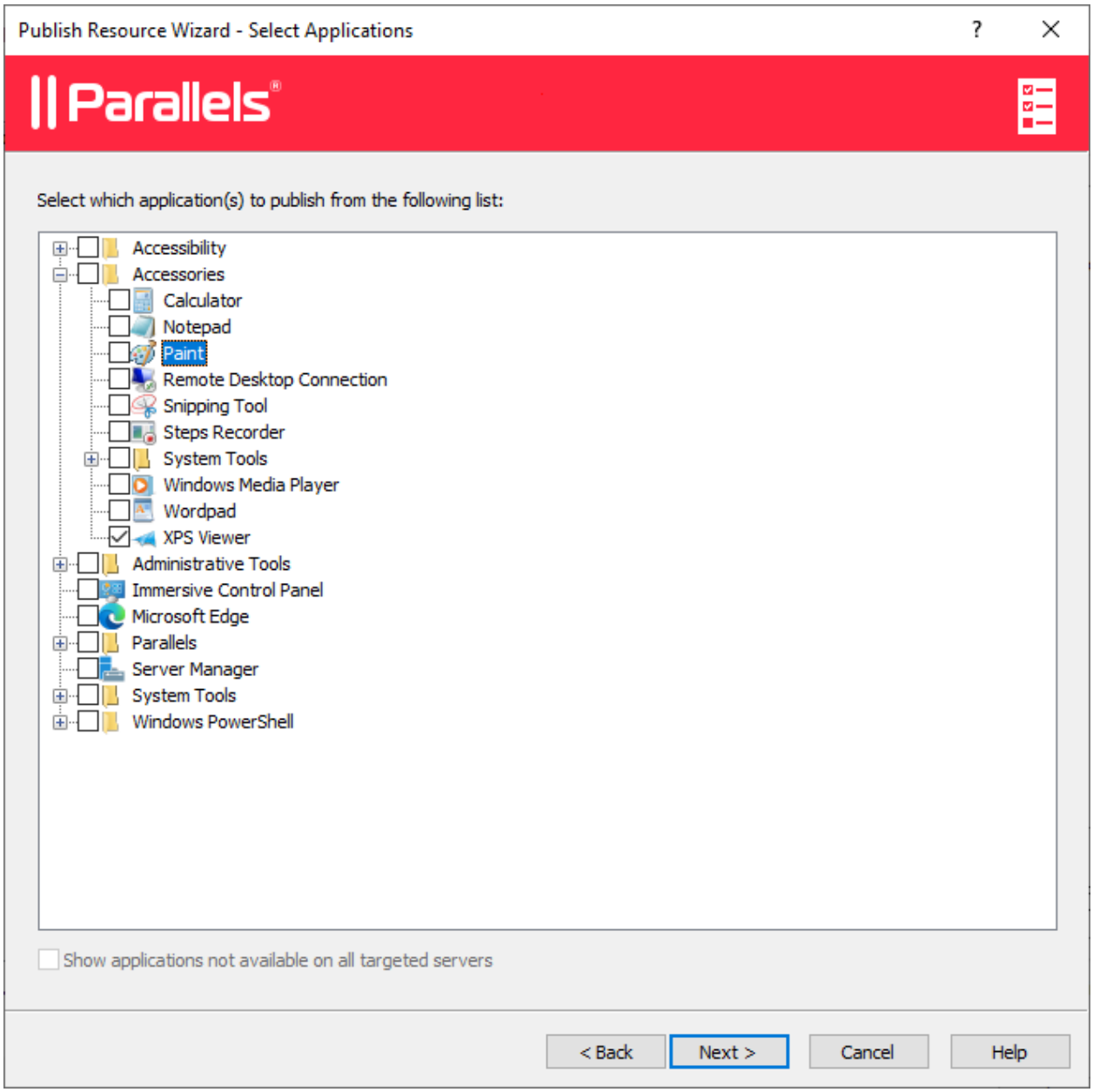
1 Parallels RAS Console で、[開始] カテゴリー選択し、右ペインの [アプリケーションを公開] アイテムをクリックします。

2 [アプリケーションを公開] ウィザードが開きます。最初のページで、アプリケーションのプッシュ元になる、1 つまたは複数のサーバーを選択します。すべてのサーバー、サーバーホストプール、または個々のサーバーを選択できます。



3 [次へ] をクリックします。

4 次のページで、公開するアプリケーションを 1 つ以上選択します。



前の画面でサーバーを 2 台以上選択した場合は、[すべての対象サーバーで使用できないアプリケーションを表示] オプションを選択できるようになります。このオプションをオフにすると（デフォルトはオフ）、フォルダーツリーには、選択したすべてのサーバーで利用できるアプリケーションが表示されます。このオプションをオンにすると、ディレクトリツリーには、一部のサーバーでのみ利用でき、他のサーバーでは利用できない可能性のあるアプリケーションも表示されます。

5 [次へ] をクリックします。概要情報を確認して、[次へ] を再度クリックします。

6 準備が完了したら、[完了] をクリックします。

アプリケーションが正常に公開されたことを確認するには、RAS Console で [公開] カテゴリーを選択します。アプリケーションは、[公開済みのリソース] リスト（中央のペイン）に表示されます。

ユーザーを招待

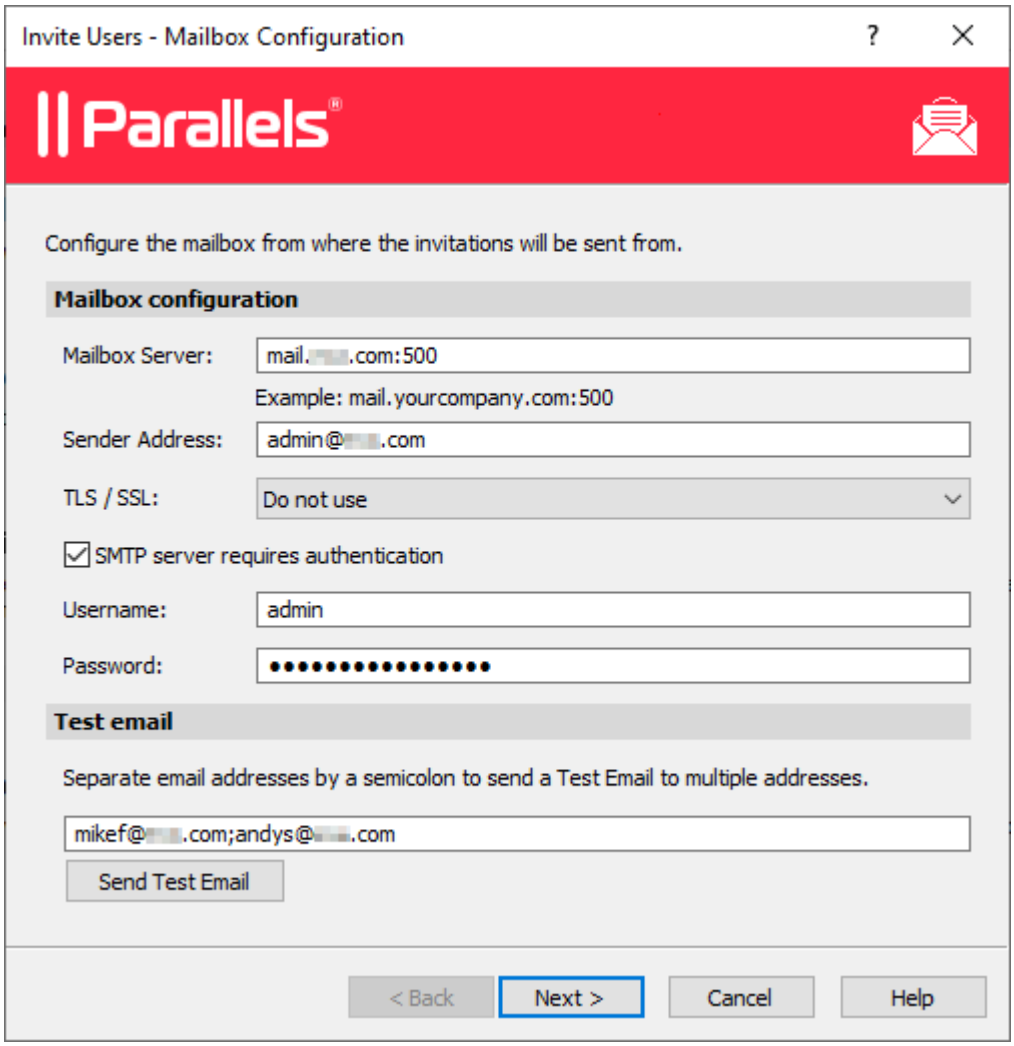
Parallels RAS ファームの準備が完了しました。RD セッションホストと公開アプリケーションを用意できました。必要なのは、Parallels Client ソフトウェアをデバイスにインストールし、Parallels RAS ファームに接続するようユーザーを招待することだけです。

注: Secure Gateway の IP アドレスやホスト名ではなく、ユーザーのメールを使用して公開済みリソースにアクセスできるようにすることを検討してください。その方法については、「メールアドレスにより RAS 接続の検出を許可する」（p. 382）を参照してください。

ユーザーを招待するには、次の手順を実行します。

1 Parallels RAS Console で、[開始] カテゴリーを選択し、[ユーザーを招待] アイテムをクリックします。

2 [ユーザーを招待] ウィザードが開きます。最初のページで、ユーザーに招待メールを送信するときに使用するメールボックス情報を指定します。



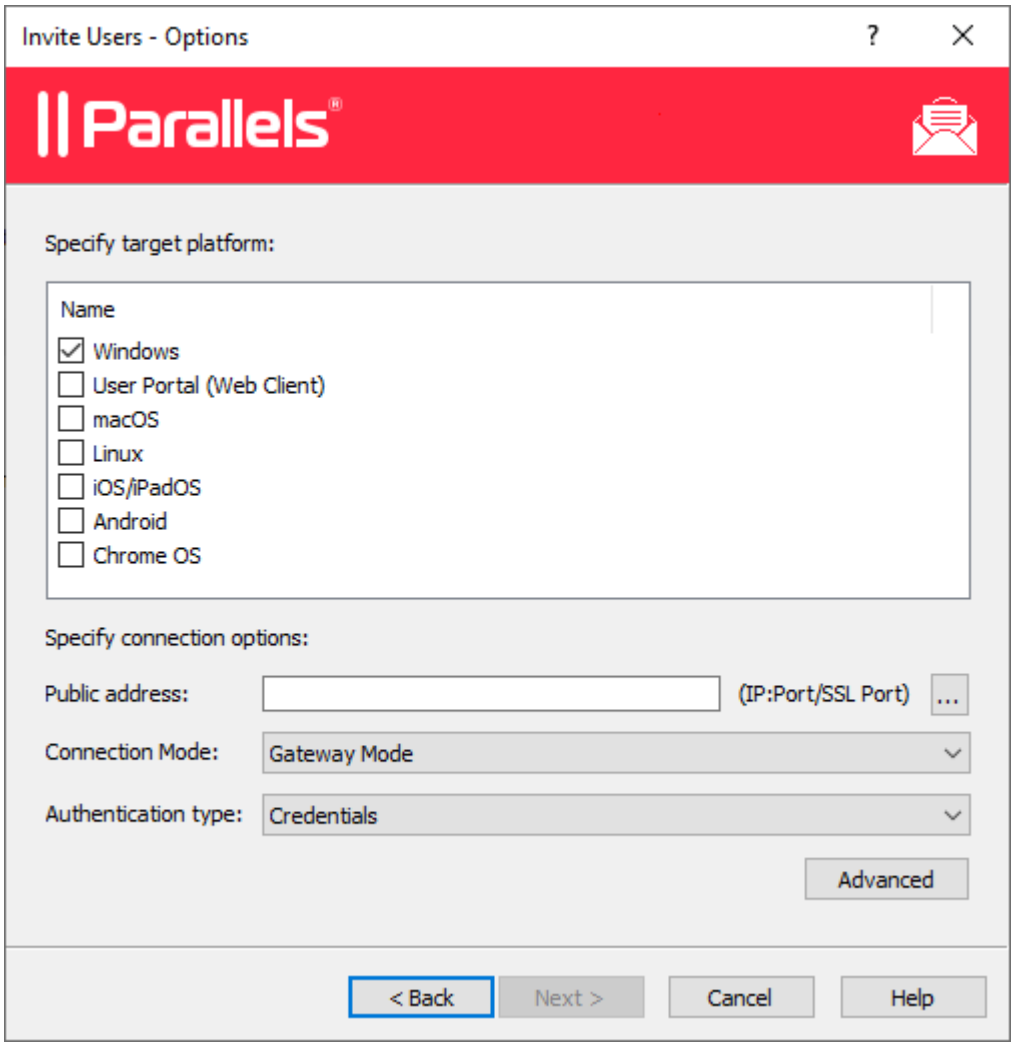
次のオプションを指定します。

- メールボックスサーバー: メールボックスサーバー名を入力します。たとえば、mail.company.com:500 など
- 送信者アドレス: メールアドレスを入力します。
- TLS / SSL: TLS/SSL プロトコルを使用するかどうかを選択します。
- SMTP サーバーは認証をリクエストする: SMTP サーバーが認証を必要とする場合は、このオプションを選択します。選択した場合はさらに、指定されたフィールドにユーザー名とパスワードを入力します。

[テスト E メール] セクションで、テストメールの送信先のメールアドレスを 1 つ以上入力します（複数のアドレスを入力する場合は、セミコロンで区切ります）。[テストメール送信] ボタンをクリックし、E メールを送信します。

3 [次へ] をクリックします。

4 ウィザードの次のページで、送信先のプラットフォームおよび接続オプションを指定します。

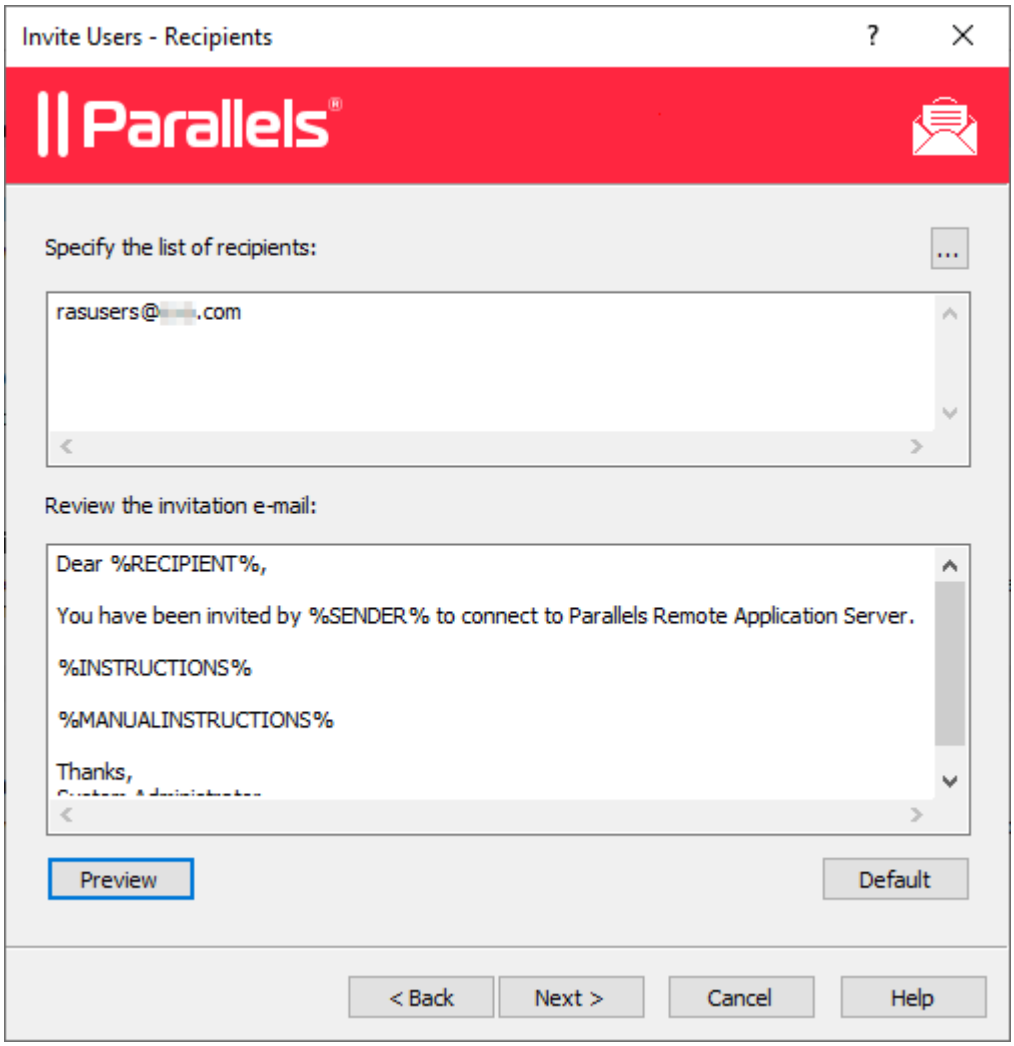


- 送信先デバイスのリストで、招待の送信先となるデバイスのタイプを選択します。特定のタイプの各送信先デバイスに電子メールが送信されます。メールには、そのデバイスタイプで Parallels Client ソフトウェアをダウンロード、インストール、構成するための手順が含まれています。

- [パブリックアドレス] フィールドで、パブリックの FQDN または IP アドレスを指定します。この設定は、クライアントの接続をリダイレクトするために優先ルーティング機能で使用されます。「優先ルーティングを構成」（p. 319）を参照してください。
- [接続モード] ドロップダウンリストで、RAS Secure Gateway 接続モードを選択します。SSL モードの場合は、ゲートウェイで SSL が構成されている必要があります。詳細については、「RAS Secure Gateway の構成」（p. 89）セクションを参照してください。
- [認証モード] ドロップダウンリストで、ユーザーの認証モードを選択します。認証モードのリストについては、「接続」（p.511）セクションの「プライマリ接続」を参照してください。
- 必要に応じて、[詳細] ボタンをクリックして、[詳細設定] ダイアログを開きます。このダイアログで、サードパーティ認証情報プロバイダーのコンポーネントを指定できます。このようなコンポーネントを使用してユーザーを認証する場合は、このダイアログで GUID を指定します。詳細については、「クライアントポリシーオプションの構成」>「Single SignOn」（p. 529）を参照してください。

5 [次へ] をクリックします。

6 次のページで、メールの受信者を指定します。[...] ボタンをクリックし、ユーザーまたはグループを選択します。



7 [招待状メールをレビュー] ボックスに表示された招待メールのテンプレートを確認します。必要に応じて、テンプレートの文章を変更できます。テンプレートでは変数も使用できます（詳細は以下を参照）。

- `%RECIPIENT%` - メールメッセージの受信者の名前を指定します。
- `%SENDER%` - 送信メールサーバーの設定を構成したときにこのウィザードの最初の手順で指定した送信者のメールアドレスです。
- `%INSTRUCTIONS%` - Parallels Client の自動構成用のカスタム URL ハイパーリンクを含みます。URL は Parallels Client の URL スキームを使用しています。詳細については

、「RAS Web Client API および Parallels Client の URL スキーム」（p. 627）を参照してください。

- %MANUALINSTRUCTIONS% - Parallels Client を手動構成するための手順を含めます。

変数は、送信先デバイスのタイプとその他の設定に基づいて動的に定義されます。通常は、これらの情報を常にメッセージに含める必要があります。これで、ユーザーはすべての必要な指示およびリンクを受け取ることができます。変数が含まれていない場合は警告メッセージが表示されますが、すべての変数が必須という意味ではありません。メッセージを確認するには、[プレビュー] ボタンをクリックします。別のウィンドウに HTML バージョンのメッセージが表示されます。これは、ユーザーが受信するメールメッセージです。

8 [次へ] をクリックし、サマリを確認します。[次へ] を再度クリックすると、ユーザーに招待メールが送信されます。

招待メールが届いたら、メールにある手順に従って、お使いのデバイスに Parallels Client をインストールして構成します。手順を終了すると、Parallels RAS に接続して、公開済みリソースを起動することができます。

Azure Virtual Desktop

[開始] カテゴリーの [Azure Virtual Desktop のデプロイ] セクションはオプション機能であり、この機能により、Parallels RAS に Azure Virtual Desktop を導入できます。この機能の詳細については、「Azure Virtual Desktop」の章（p. 241）で説明されています。

まとめ

このチュートリアルでは、1 台の RD セッションホストと 1 つの公開アプリケーションを使用して、シンプルな Parallels RAS ファームを構成しました。次に、送信メール用のメールボックスを構成して、エンドユーザーに招待メールを送信しました。このメールには、Parallels Client のインストール方法、Parallels RAS ファームへの接続方法、公開アプリケーションの実行方法が記載されていました。実質的に、リモートアプリケーションをエンドユーザーに提供する、フル機能の Parallels RAS ファームを作成しました。

必要に応じてチュートリアルを繰り返し、RD セッションホストの追加、アプリケーションの公開、各種デバイスを使用するユーザーへの招待メールの送信を実行できます。方法は基本的に同じです。

このガイドの残りの部分で、Parallels RAS のさまざまな機能の構成方法と使用方法を詳しく説明します。

第 4 章

ファームとサイト

Parallels RAS ファームは、集中管理機能を目的としたオブジェクトの論理グループです。ファーム構成の情報は単一のデータベースに保存され、ファームを構成するすべてのオブジェクトに関する情報がそこに保存されます。サイトは、ファーム階層内での次のレベルのグループです。接続やリモートアプリケーションサービスを提供する、サーバーやその他のオブジェクトが含まれます。

この章の内容

Parallels RAS ファームへの接続

組織内に複数の Parallels RAS ファームがある場合でも、同じ Parallels RAS Console インスタンスを使用して管理できます。Parallels RAS Console は、デフォルトでは他の Parallels RAS コンポーネントをインストールしたのと同じサーバーにインストールされますが、ネットワークの任意のコンピューターにインストールできます。

Parallels RAS ファームへの最初の接続

Parallels RAS Console を初めて開くときには、ログオンダイアログが表示され、以下の項目を指定する必要があります。

- ファーム: 接続先の Parallels RAS ファーム。RAS Connection Broker がインストールされているサーバーの FQDN または IP アドレスを入力します。
- RAS Console をインストールするときに Parallels Single Sign-On コンポーネントをインストールしている場合、[認証タイプ] フィールドが表示され、そこから資格情報を使用して

ログオンするか、 SSO を使用してログオンするかを選択できます。インストール後に再起動し、SSO を選択する場合は、[Single Sign-On] を選択し、[接続] をクリックします。RAS ファームへのログインには、Windows 資格情報が使用されます。[資格情報] を選択する場合は、下記のように資格情報を入力します。

- ユーザー名: Parallels RAS がインストールされているサーバーでの管理権限があるユーザーアカウント（通常はドメインまたはローカル管理者）。アカウント名は UPN 形式（例: administrator@domain.com）で指定する必要があります。指定したユーザーは自動的に完全なアクセス権がある Parallels RAS 管理者として構成されます。
- パスワード: 指定したユーザーアカウントのパスワードです。
- [認証情報を記憶する] オプションを選択した場合、次に Parallels RAS Console を起動したときにはこのダイアログは表示されません。

接続プロパティを入力した後に、[接続] をクリックして、ファームに接続し、RAS Console を開きます。

初回の接続時には、[接続を編集] ボタンを押しても情報が表示されません（これは既存のファームの接続を編集するときに使用します）。このタイミングではこのボタンを無視できます。このボタンの使用方法については、本セクションの終わり近くで触れます。

別の Parallels RAS ファームへの接続

別の Parallels RAS ファームに接続する場合、Parallels RAS Console からいったんログオフし、ログオンダイアログを再度表示する必要があります。このためには、次の操作を実行します。

1. Parallels RAS Console の右上隅に表示されている自分のユーザー名の隣にある矢印アイコンをクリックし、コンテキストメニューで [ログオフ] を選択します。
2. コンソールが閉じられ、RAS ログオンダイアログが開かれます。ダイアログには、現在のファームの接続プロパティが入力されます。
3. 別のファームに接続するには、他のファームが存在するサーバーの FQDN または IP アドレスを入力します。ここでも、そのサーバーに RAS Connection Broker がインストールされている必要があります。
4. ユーザー名とパスワードを指定して、[接続] をクリックします。指定した接続プロパティを使用して、Parallels RAS Console がファームに接続されます。

Parallels RAS ファーム間の切り替え

同じ Parallels RAS Console インスタンスから複数のファームに接続した後、次のようにしてそれらのファームを簡単に切り替えられます。

1. Parallels RAS Console の左上隅（現在のサイト名が表示されているメインアプリケーションメニューの右下）で、[場所] ドロップダウンリストをクリックします。
2. ドロップダウンリストの下部には、過去に少なくとも 1 回接続したことのあるファームの名前が表示されます（上部には、現在のファームのサイト名が表示されます）。目的のファーム名をクリックして接続します。
3. ファーム名をクリックすると、コンソールが瞬時に閉じられ、選択したファームに接続した状態で再度開かれます。

ファームは、コンソールからログオフし、希望のファームを RAS ログオンダイアログの [ファーム] ドロップダウンリストから選択することでも切り替えられます。別の方法として紹介しておきますが、前述の方法のほうが便利です。

Parallels RAS ファーム接続の編集

本セクションの始めで説明したように、RAS ログオンダイアログには [接続を編集] ボタンがあります。これをクリックすると、[Parallels RAS ファームの管理] ダイアログが開きます。

ダイアログ左側の [ファームの接続] ペインに、過去に少なくとも 1 回接続したことのある Parallels RAS ファームが一覧表示されます。すでに必要のない接続がある場合、その接続を選択し、一番上の [-] アイコンをクリックすれば削除できます。接続が削除されると、RAS ログオンダイアログや Parallels RAS Console（[場所] ドロップダウンリスト）に表示されなくなります。

ダイアログ右側の [Connection Broker] ペインに、選択されたファームの接続に対応する RAS Connection Broker が一覧表示されます。デフォルトでは、プライマリ Connection Broker がリストに表示されますが、必要に応じて Connection Broker をさらに追加できます。ファームに接続する際、Parallels RAS Console は最初にプライマリ Connection Broker を試行します。接続が確立できない場合、Parallels RAS Console は [Connection Broker] ペインに一覧表示されている順番で他の Connection Broker を試行します。リストに Connection Broker を追加するには、[+] アイコンをクリックしてから、サーバーの FQDN または IP アドレスを指定します。

サイトについて

Parallels RAS ファームには少なくとも 1 つのサイトが必要ですが、必要な数のサイトで構成することができます。

多くの場合、サイトは管理や場所の機能を分割する目的で使用されます。たとえば、サイトを作成することで、ファームのフル権限を付与することなくサイト管理者に権限を委任できます。また、エンドユーザーか（ニーズによっては）バックエンドサーバーに近い RD セッションホスト、プロバイダー、PC を使用しながら、同じ設定を各サイトにコピーする機能を使用して、別の物理的な場所に独立したサイトを配置できます。このことは、たとえば、データベースサーバーの近くに配置された RD セッションホストで公開されているデータベースにクエリを実行するクライアント/サーバーアプリケーションで意味があります。

各サイトは、同じファーム内の他のサイトと完全に分離されています。ファームは、サイトを論理的にグループ化し、各サイト（および各サイトを構成するオブジェクト）の構成プロパティを単一のデータベースに保存したものです。サイト間で互いに通信することはなく、オブジェクトやデータを共有することもありません。このルールの唯一の例外が、RAS ライセンスサイトです。これは、統計を取得するために他のサイトと定期的に通信します。

1 つのサイト内の個別のオブジェクトの設定を、それ以外のすべてのサイトに複製できます。これは、サイト間で設定が共有されるという意味ではありません。選択した設定が、他のサイトにも適用されるだけです。詳細については「サイト設定の複製」セクション（p. 66）を参照してください。

Parallels RAS をインストールするときには、1 つのサイトを持つファームが自動的に作成されます。この最初のサイトが RAS ライセンスサイトおよびメインの Parallels RAS 構成データベースのホストになります。ファームにさらにサイトを追加すると、追加されたサイトすべてにこのデータベースのデータが自動的に同期されます。特定のサイトに変更が適用されたときは、メインの構成データベースが自動的にアップデートされ、変更内容が反映されます。

各サイトには、エンドユーザーにリモートアプリケーションとデスクトップを公開するため、少なくとも以下のコンポーネントがインストールされていることが必要です。

- プライマリ RAS Connection Broker
- RAS Secure Gateway: あるサイトがテナントとして RAS テナントブローカーに参加する場合、RAS Secure Gateway は不要です。詳細については、「RAS マルチテナントアーキテクチャ」（p. 397）を参照してください。

- RD セッションホスト、VDI、または PC

デフォルトのインストールオプションを使用して Parallels RAS をインストールするとき、プライマリ RAS Connection Broker と RAS Secure Gateway は、インストールを実行するサーバーに自動的にインストールされます。その後、1 つまたは複数の RD セッションホストをサイトに追加して公開済みのリソースをホストできます。必要な場合はファームにさらにサイトを追加し、各サイトに個々のコンポーネントを自由に構成することもできます。

RAS Console でのサイト

Parallels RAS Console で既存のサイトを表示するには、左ペインで [ファーム] カテゴリーを選択します。既存のサイトは右ペインに一覧表示されます。

注: [ファーム] ノードは、そのファームを管理するフル権限を付与されている管理者にのみ表示されます。ファーム/サイトの権限の詳細については、「管理者アカウントの管理」（p. 68）を参照してください。

[ファーム] カテゴリには、一度に 1 つのサイトの構成のみが表示されます。ファーム管理者としてログインした場合、RAS ライセンスサイトの構成が表示されます。特定のサイトへのアクセス権を持つ（しかし、ファームに対するアクセス権はない）管理者としてログインした場合、そのサイトの構成が表示されます。

作業中のサイト

中央ペインにある [ファーム] アイテムをクリックして、利用可能なサイトの一覧を表示します。コンソールに現在構成がロードされているサイトは、[タイプ] 列に“作業中のサイト”としてマークされます。列にはその他のサイト属性も表示されます。"ライセンスサイト/ローカルサイト/作業中のサイト" などです。

各サイト間の切り替え

特定のサイトに切り替えるには、中央ペインで [ファーム] を選択し、右ペインでサイトを右クリックして、[このサイトへ切り替える] を選択します。サイト構成が RAS Console にロードされます。

サイトを切り替える別の方法は、RAS Console 左上の [場所] ドロップダウンリストをクリックすることです。このメニューには現在のファームのサイトが一覧表示されます。この RAS

Console を使用して他のファームに接続した場合、それらのファームも一覧表示されます。詳細については、「Parallels RAS ファームへの接続」（p. 59）を参照してください。

サイト名の変更

サイト名を変更するには、名前を右クリックして、[サイト名の変更] を選択します。

サイト構成と状態のビュー

中央のペインにある [サイト] ノードを選択すると、右ペインにある [サイト情報] タブに、そのサイトに構成された Parallels RAS コンポーネントのリストが表示され、各コンポーネントの対話型パフォーマンスモニタリングメトリクスも表示されます。サイトの構成に応じて、リストには RD セッションホスト、VDI、リモート PC、Secure Gateway、Connection Broker、Azure Virtual Desktop、HALB 仮想サーバーとデバイス、テナントブローカー、ホストプール、および登録サーバーが含まれる場合があります。

コンポーネントグループを折りたたむ、または展開するには、リストの右側にある ”上矢印” または”下矢印”アイコンをクリックします。特定のタイプのサーバーがサイトに追加されていない場合、リストにグループ名は表示されません。

各コンポーネントについて、以下の情報が表示されます（情報は約 2 分間隔で更新されます）。

- アドレス: サーバーの FQDN または IP アドレス。
- ステータス: エージェントソフトウェアがサーバーにインストールされているかどうか、また適切に機能しているかどうかを示します。
- CPU: 現在の CPU 使用率。
- RAM: 現在の RAM 使用率。
- ディスク読み取り時間: ディスク読み取り時間。
- ディスク書き込み時間: ディスク書き込み時間。
- セッション: 現在アクティブなユーザーセッション数。
- 優先 PA: このサーバーで優先的に指定されている RAS Connection Broker の名前。
- オペレーティングシステム: サーバーにインストールされているオペレーティングシステムのバージョン。
- Agent のバージョン: サーバーにインストールされているエージェントのバージョン。

- ハイパーバイザー: サーバーが稼働しているハイパーバイザーです。

このビューは、[タスク] > [監視の設定] をクリックして、カスタマイズできます。異なるパフォーマンスカウンターとその値を表示するためにどの色を使用するかを指定できるダイアログが開きます。

コンポーネント上でのタスクの実行

[サイト情報] タブに表示されているコンポーネント上で多数のタスクを実行できます。これらのタスクについて、以下に説明します。

コンポーネントを構成するには、次のいずれかを実行します。

- [サイト] ノードが中央ペインで選択されているときに、右ペインでコンポーネントを右クリックし、[エディターに表示] を選択します。
- 中央ペインでコンポーネントカテゴリー（例: RD セッションホスト、プロバイダー）を選択します。

コンピューター管理ツールを使用するには、コンポーネント（サーバー）を右クリックし、[ツール] をクリックして目的のツールを選択します。ツールの詳しい説明については、「コンピューター管理ツール」（p. 569）を参照してください。

サイトデザイナーの使用

中央で [サイト] ノードを選択し、右ペインで [デザイナー] タブをクリックします。タブにサイトのインフラストラクチャが視覚的に表示されます。必要に応じて、上部にあるアイコンを使用して、図にコンポーネントを追加します。図にコンポーネントを追加すると、実際にサイトに追加されることに注意してください。対応エディターでコンポーネントを表示して構成するには、そのコンポーネントをダブルクリックします。

ファームへのサイトの追加

ファームにサイトを追加するには、次の操作を実行します。

1 RAS Console の左ペインで、[ファーム] カテゴリを選択し、中央のペインでファームを選択します。

2 [タスク] ドロップダウンリスト（右ペイン、[サイト] リストの上部）で [追加]（または + アイコン）をクリックします。

3 [サイト追加] ダイアログで、次の操作を実行します。

- [サイト] フィールドで、サイト名を指定します。
- [サーバー] フィールドで、プライマリ Connection Broker と Secure Gateway をインストールするサーバーの IP アドレスまたは FQDN を指定します。
- [HTML5 ゲートウェイの有効化] オプションを選択して、自己署名証明書の作成、SSL の有効化、および HTML5 サポートの有効化を自動で行います。詳細については、「ユーザーポータルの構成」（p. 97）を参照してください。

4 [次へ] をクリックします。

5 [サイトプロパティ] ダイアログが開きます。最初に、指定されたサイトサーバーに RAS Connection Broker がインストールされているかどうかが確認されます。インストールされていない場合、インストールされていないことが [ステータス] フィールドに示されます。

6 [インストール] ボタンをクリックして、Agent をインストールします。

7 [RAS Connection Broker のインストール] ダイアログで、RAS Connection Broker をインストールするサーバーの名前を選択します。

8 （オプション）別の資格情報を使用してサーバーに接続し、Agent をインストールするには、[資格情報の上書き] オプションを選択します。

9 [インストール] をクリックして、Connection Broker と Secure Gateway をインストールします。正常にインストールされたら、[完了] をクリックします。

新しいサイトを作成したら、RAS Console でサイトを右クリックし、[このサイトへ切り替える] を選択して、構成を表示および管理できます。

サイト設定の複製

あるサイトに構成したサイト固有の設定を、ファーム内にあるその他のすべてのサイトに複製できます。他のサイトに複製可能な設定の詳細については、以下の表を参照してください。

カテゴリー	セクション	オプション
ファーム	VDI > テンプレート	準備に失敗したホストプールの自動削除タイムアウト
ファーム	[VDI] > [デスクトップ]	自動削除タイムアウト
ファーム	[設定] > [監査]	すべての設定
ファーム	[設定] > [グローバルロギング]	ログ設定

ファーム	[設定] > [URL リダイレクト]	すべての設定
ロードバランス	ロードバランス	すべての設定
ロードバランス	CPU の最適化	すべての設定
公開	アプリケーション	サイトのデフォルト値が複製されます。他の設定（例: 名前、説明、アイコン）はグローバルで、すべてのサイトに共通しています。
公開	ショートカット	すべての設定
公開	拡張	すべての設定
公開	ライセンス	すべての設定
公開	ディスプレイ	すべての設定
公開	フィルタリング（Secure Gateway を除くすべてのタイプ）	すべての設定
ユニバーサルプリント	ユニバーサルプリント	プリンターの名前変更
ユニバーサルプリント	プリンタードライバー	すべての設定
ユニバーサルプリント	フォントマネジメント	すべての設定
ユニバーサルスキャン	WIA	スキャナーの名前変更
ユニバーサルスキャン	TWAIN	スキャナーの名前変更
ユニバーサルスキャン	[TWAIN] > [TWAIN アプリケーション]	スキャンアプリケーション
接続	認証	すべての設定
接続	設定	すべての設定
接続	多要素認証	すべての設定
接続	許可されたデバイス	すべての設定
レポート作成	レポートエンジン	レポートエンジンのタイプ
レポート作成	エンジン固有の設定	すべての設定

サイト設定を他のすべてのサイトに複製するには、[ファーム] > <サイト> > [設定] を選択してから、（[監査] タブの下部にある）[設定を複製する] オプションを選択します。ファーム内にサイトが 1 つしかない場合、このオプションは無効になります。

複製されたサイト設定の上書き

複製設定を有効または無効にする権限を持つ管理者が特定の設定を変更すると、その設定は他のすべてのサイトに複製されます。特定のサイトへのアクセス権のみを持つ管理者が、複製さ

れたサイト設定を変更すると、複製された設定は上書きされ、[設定を複製する] オプションが自動的にオフになります。そのため、その設定は他のサイトに複製されなくなります。

ライセンスサイトの管理

ライセンスサイトは、ファームに別のサイトがある場合でも、常にオンラインであることが必要です。ライセンスサイトがオフラインになった場合、その他のサイトは引き続きサブスクリプションに含まれる個別ライセンスの最大数を 72 時間のみ使用できます。この間に、次のいずれかの手順を実行する必要があります。

- ライセンスサイトを復元します。
- 別のサイトを昇格してファームのライセンスサイトにします（手順については以下を参照）。

ライセンスサイトが 48～72 時間オフラインになってからオンラインに戻る動作が月に 3 回発生した場合、3 回目の後、Parallels RAS ライセンスキーを使用して再アクティベートするように求められます。

セカンダリサイトをファームのライセンスサイトに昇格させるには、次の手順を実行します。

1 RAS Console で [ファーム] > [ファーム] に移動します。

2 右ペインでサイトを選択し、[タスク] > [サイトをライセンスサイトとして設定する] をクリックします。

3 Parallels RAS ライセンスを使用して新しいライセンスサイトをアクティベートするように要求されます。指示に従って、サイトをアクティベートします。

管理者アカウントの管理

Parallels RAS では複数の管理者を設定できます。少なくとも 1 名の管理者（root 管理者と呼ばれます）が常に存在する必要があります。他の管理者には、以下の役割を割り当てることができます。

- root 管理者: Parallels RAS ファームを管理するためのフル権限が付与されています。
- 上級管理者: デフォルトでほとんどの権限を付与されていますが、特定のサイトやカテゴリーを管理するために制限された権限を付与するように構成することもできます。

- カスタム管理者。デフォルトでは権限が付与されていません。Parallels RAS ファームの特定のエリアまたはオブジェクトに表示や修正を行う具体的な権限を付与できます。

続いて、管理者アカウントを作成し、管理する方法について説明します。

管理者アカウントの追加

管理者アカウントを Parallels RAS ファームに追加するには、次の操作を実行します。

1 RAS Console で [管理] > [アカウント] に移動します。

2 [タスク] ドロップダウンリストをクリックし、[追加] を選択します（または [+] アイコンをクリックします）。

3 [アカウントのプロパティ] ダイアログが開きます。

4 [名前] フィールドの横にある [...] ボタンをクリックします。[ユーザーまたはグループを選択] ダイアログで、ユーザーまたはグループを選択します。

5 メールアドレスと携帯電話番号を指定します。これらのフィールドはオプションで、[名前] フィールドで指定されたアカウントがグループである場合、無効にされています。

6 [権限」 ドロップダウンリストで、管理者に割り当てる役割を選択します。

   - root 管理者: 管理者にファームを管理するためのフル権限を付与します。
   - 上級管理者: デフォルトで管理者にフル権限を付与しますが、必要に応じてそれらに制限を加えることもできます。特定の権限を付与または削除するには、[権限の変更] ボタンをクリックします。詳細については、「管理者アカウントの権限」（p. 70）を参照してください。
   - カスタム管理者。この役割にはデフォルトで権限が何も付与されておらず、RAS Console の特定のカテゴリー、エリア、オブジェクトに特化した権限を付与できます。詳細については、「管理者アカウントの権限」（p. 70）を参照してください。

7 [システム通知を受け取る手段] ドロップダウンリストで、[メール] を選択して、すべてのシステム通知を指定のメールアドレスに送信するか、[なし] を選択して、このアカウントのメールのシステム通知を無効にします。

8 [OK] をクリックして、ファームに新しい管理者アカウントを追加します。

管理者アカウントの変更

アカウントを変更するには、リストからアカウントを選択し、[タスク] > [プロパティ] をクリックします。これにより、[アカウントプロパティ] ダイアログが開きます。ここでアカウント情報を変更できます。

アカウントを有効または無効にするには、[アカウントプロパティ] ダイアログの上部にある [アカウントを有効化] オプションを選択するか、オフにします。

管理者アカウントの権限

RAS 管理者の権限を設定するには、次の手順を実行します。

1. RAS Console で [管理] > [アカウント] に移動します。
2. リストで管理者を選択し、[タスク] > [プロパティ] をクリックします。
3. [管理者のプロパティ] ダイアログで [許可の変更] ボタンをクリックします。[権限] フィールドで選択されている内容に応じて、次のようになります。
   - root 管理者: root 管理者にはフル権限が常に付与されているため、[権限の変更] ボタンが無効になります。
   - 上級管理者: [アカウントの権限] ダイアログが開きます。左側のペインで、管理者に権限を付与する 1 つまたは複数のサイトを選択します。右のペインで、特定の権限を選択します。詳細については、以下の「上級管理者の権限」サブセクションを参照してください。
   - カスタム管理者。別の [アカウントの権限] ダイアログが開かれます。このダイアログでは、カスタム権限を設定できます。上級管理者の役割（上記参照）とは異なり、このオプションでは RAS Console のカテゴリ全体または特定エリアやオブジェクトに対して権限（表示、変更、追加など）を付与できます。あるカテゴリやタブの表示権限がカスタム管理者に付与されていなければ、それらのカテゴリやタブは RAS Console に表示されません。カスタム管理者の役割を使用することで、権限を 1 つ以上の特定のタスクに限定できます。詳細については、以下の「カスタム管理者の権限」を参照してください。

上級管理者の権限

次の権限を上級管理者に設定できます。

- サイト情報の表示を許可: 管理者がサイト情報を表示できるかどうか。

- サイトの変更を許可: 次のカテゴリーを変更する権限: [サイト]、[ロードバランス]、[ユニバーサルプリント]、[ユニバーサルスキャン][サイト情報へのアクセスを許可] オプションがクリアされている場合、このオプションは無効です。
- セッション管理を許可: 実行中のセッションを管理する権限。[サイト情報へのアクセスを許可] オプションがクリアされている場合、このオプションは無効です。
- 公開の変更を許可: [公開] カテゴリーを変更する権限。
- 接続の変更を許可: [接続] カテゴリーを変更する権限。
- RAS レポート作成機能の表示を許可: RAS レポート作成機能により生成されるレポートを表示する権限。
- クライアント管理の変更を許可: [デバイスマネージャー] カテゴリーを変更する権限。

[グローバル権限] エリアで、以下を設定します。

- ポリシーの表示を許可: 管理者に [ポリシー] カテゴリーを表示する許可を与えるかどうか。
- ポリシーの変更を許可: 管理者に [ポリシー] カテゴリーを変更する許可を与えるかどうか。

カスタム管理者の権限

カスタム管理者の権限を設定するには、root 管理者または [サイトの変更を許可] 権限が付与されている上級管理者である必要があります。

このタイプの管理者を最初に作成する際、管理者には権限は全くありません。権限を追加するには、左側のペインでサイトを選択してから、[権限の変更] ボタンをクリックします。[アカウントの権限] ダイアログが開きます。ダイアログの左側のペインで、権限の種類を選択します。

権限の種類は次の通りです。

- RD セッションホストグループ: [ファーム] > [RD セッションホスト]の [グループ] タブ。

  注: Parallels RAS 19 以降、サーバー単位の RDSH 権限は非推奨となりました。手動でグループ単位の権限に置き換える必要があります。以前のバージョンから Parallels RAS 19 以降にアップグレードする場合、アップグレード中にプロセスを支援するダイアログが表示されます。
- リモート PC: [ファーム] > [リモート PC] ビュー。
- Secure Gateway: [ファーム] > [Secure Gateway] ビュー。

- Connection Broker: [ファーム] > [Connection Broker]
- HALB: [ファーム] > [HALB] ビュー。
- テーマ: [ファーム] > [テーマ] ビュー。
- 公開: [公開] カテゴリー内の個別フォルダーの権限。
- 接続: [接続] カテゴリー全体。
- デバイスマネージャー: [デバイスマネージャー] カテゴリー全体。
- 証明書: [ファーム] > [証明書] ビュー。
- アプリケーションパッケージ: [ファーム] > [アプリケーションパッケージ] ビュー。

権限の種類を選択した後に、実際の権限を右のペインで設定できます。権限の種類に応じ、権限のセットが異なる場合があります。利用可能なすべての権限を以下のリストに示します。

- 表示: 表示のみ。
- 変更: 表示と変更。
- 追加: 新規オブジェクト（サーバーなど）の表示、変更、追加。
- 削除: オブジェクトの表示、変更、削除。
- コントロール: オブジェクトの表示、コントロール。この権限は、[タスク] > [コントロール] メニューを（利用可能な場合に）有効にします。このメニューには、ログオンの有効化/無効化、保留中の再起動のキャンセル、RDS 役割のインストール、再起動、ならびにいくつかの他のオプションがあります。またこれにより、電源関連の処理（利用可能な場合は起動、停止など）も有効になります。
- セッションの管理: 表示とセッションの管理。

選択した権限の種類に個別のオブジェクトがある場合、右のペインの下部には、個別のオブジェクト（サーバーなど）が一覧表示されます。ここでは、特定のオブジェクトに対して個別の権限を設定できます（タブ全体ではなくインスタンスが対象となります。そうでないとすべての利用可能なオブジェクトが含まれてしまいます）。

右のペインの上部にある [グローバル権限] オプションを利用すると、選択された権限の種類に対して全オブジェクトのすべての権限を有効にできます。

権限の複製

root 管理者（あるいは適切な権限のある上級管理者）として、既存の管理者アカウントの権限を別の既存のアカウントに適用（複製）できます。このようにして、1 つのアカウントに対して権限を構成し、必要とするすべての他のアカウントに同じ構成をすばやく適用できます。

権限を複製するには、複製元の管理者アカウントを選択して、[タスク] > [権限の複製] をクリックします。開いたダイアログで、複製先のアカウントを選択して（複数アカウントも可能）、[OK] をクリックします。

権限の委任

上級管理者がいくつかの権限をカスタム管理者に付与する必要が生じる場合があります。これは、権限を変更しても実行できません。上級管理者が管理者アカウントを直接管理できないためです。代替手段として、特定のサイトについて、権限の一部を選択したカスタム管理者に委任することができます。

たとえば、上級管理者の側からカスタム管理者による特定の RD セッションホストの管理を可能にしたい場合、上級管理者は RAS Console から目的のホストを選択して、[タスク] > [権限を委任] をクリックします。これにより、カスタム管理者を選択した上で、どの権限（表示、変更など）をその管理者に割り当てるべきかを管理者が指定できるダイアログが開きます。[タスク] > [権限を委任] メニューオプションは多くのオブジェクトに対して利用できます。プロバイダー、ホストプール（デスクトップ）、他のいくつかのオブジェクトなどです。オブジェクトでメニューが無効になっている場合、そのタイプのオブジェクトではその機能が利用できないことを意味しています。

管理者アカウントの管理

既存の管理者アカウントを表示するには、RAS Console で [管理者] カテゴリーを選択します。[アカウント] タブには既存のアカウントとそのプロパティが一覧表示されます。このプロパティには以下が含まれます。

- グループまたはユーザー名: アカウント名。ユーザー名またはグループ名が使用できます。
- タイプ: アカウントの種類。低い、普通、良い、最高品質[ユーザー]、[グループ]、[グループユーザー] のいずれかです。[ユーザー] と [グループ] は名称自体が説明になっています。[グループユーザー] は、グループのメンバーシップを介して Parallels RAS の管理者権限を受けるユーザーです。Parallels RAS 管理者のリストに最初にグループを追加するとき、そのメンバーは [アカウント] タブに表示されません。グループのメンバーが Parallels

RAS にログインするとすぐ、[グループユーザー] というアカウント名で管理者のリストに追加され、その状態が維持されます。グループ権限外で個々にこのようなアカウントの Parallels RAS 権限を変更することはできません。

- 権限: 管理者に割り当てられているセキュリティの役割。
- メール: メールアドレス。
- 携帯電話: 携帯電話の番号。
- グループ: グループ名。この列にはグループユーザーの値のみが入ります（上記の [タイプ] 列の説明を参照してください）。
- 最終変更者: Parallels RAS で最後にこのアカウントを変更したユーザーの名前。
- 変更日時: 最終アカウント変更日。
- 作成者: Parallels RAS でこのアカウントを作成したユーザーの名前。
- 作成日時: このアカウントが Parallels RAS に追加された日付。
- ID: Parallels RAS の内部 ID。

アカウントの変更

アカウントを変更するには、次の手順を実行します。

1. アカウントを右クリックし、コンテキストメニューで [プロパティ] を選択します。
2. [管理者のプロパティ] ダイアログを使用して、必要な情報を変更します。詳細については、「管理者アカウントの追加」（p. 69）を参照してください。

ロックされたオブジェクトの処理

管理者がオブジェクト（[RD セッションホストプロパティ] ダイアログのタブなど）を操作しているとき、そのオブジェクトは他のすべての管理者に対してロックされます。従って、他の管理者がロックされているオブジェクトにアクセスしようとすると、オブジェクトがロックされていることを通知するエラーメッセージが表示され、アクセスが拒否されます。

root 管理者（上級管理者やカスタム管理者ではありません）は、次の手順によりオブジェクトのロックを解除できます。

1. [管理] > [アカウント] タブで [タスク] ドロップダウンリストをクリックし、[セッションを表示] を選択します。

2 [セッション] ダイアログで、オブジェクトをロックしている管理者を選択し、[メッセージを送信] アイコン（上部）をクリックします。

3 管理者が応答せず、オブジェクトのロックが解除されない場合、[ログオフ] をクリックしてログオフし、カテゴリーのロックを解除するオプションがあります。

RAS Console のアイドルセッションの構成

複数の管理者が RAS Console を使用して同じファームを管理している場合、RAS Console のアイドルセッションをいつ切断するかを構成できます。デフォルトでは、管理者がコンソールを開いてファームに接続した後にログオフせず立ち去った場合、セッションが無期限にアクティブなままになり、カテゴリのいくつかがロックされて他の管理者が接続できなくなる可能性があります。この状況を変えるために、アイドルセッションの切断までの（カテゴリがロック解除される）時間を指定できます。

アイドルなセッションを構成するには、次の手順を実行します。

1 RAS Console で [管理] > [設定] に移動します。

2 [その他] セクション（一番下）を見つけ、[RAS Console のアイドルセッションをリセットするまでの時間] ドロップダウンリストで目的の期間を選択します。

セッションが指定された期間の近くまでアイドルな状態のままである場合、管理者（セッション所有者）は、セッションが切断される数分前に通知されます。管理者が接続状態の維持を選択した場合は、期間がリセットされます。管理者が何もしない場合、期間終了時にセッションが切断されます。

インスタントメッセージの使用

同じファームにログオンしている Parallels RAS 管理者は、組み込みのインスタントメッセンジャーを使用して互いに通信できます。

インスタントメッセンジャーを使用するには、次の手順を実行します。

1 RAS Console で [管理] カテゴリーを選択します。

2 ユーザー名（コンソール画面の右上隅）の横のドロップダウンリストを展開して、[チャット] をクリックします。

3 [Parallels Remote Application Server チャット] ウィンドウが開きます。

メッセージを送信するには、次の操作を実行します。

1 下部の入力パネルにメッセージテキストを入力します。

2 [ログオン済みの管理者] リストボックスで、個々の管理者にメッセージを送信するには特定の管理者を選択し、ログオンしているすべての管理者にメッセージを送信するには、[全て] を選択します。

3 [送信] をクリックします。

[メッセージ] パネルには、メッセージ履歴が表示されます。履歴を消去するには、[すべてクリア] をクリックします。

チャット履歴に（自分のメッセージだけでなく）すべての管理者間のメッセージをすべて表示することもできます。それには、コンソールで [管理] ノードを選択してから、[チャット履歴] タブを選択します。

カスタマエクスペリエンスプログラムへの参加

Parallels カスタマーエクスペリエンスプログラムは、Parallels RAS の品質と信頼性の向上に役立てられます。プログラムの参加に同意された場合、ユーザーの Parallels RAS の使用状況に関する情報が収集されます。氏名、住所、電話番号、キーボードの入力内容などの個人情報は収集されません。

プログラムに参加するには、次の手順を実行します。

1 RAS Console で [管理] カテゴリーを選択します。

2 右ペインで、[設定] タブをクリックします。

3 [カスタマエクスペリエンスプログラムに参加する] オプションを選択します。

プログラムに参加すると、CEP は、ユーザーが Parallels RAS をどのように使用しているかについて、情報の収集を開始します。皆様から収集した情報は十分に分析され、Parallels RAS の向上に役立てられます。

第　5　章

RAS Connection Broker

RAS Connection Broker では、公開済みのアプリケーションおよびデスクトップのロードバランスが実行されます。RAS Connection Broker は、Parallels RAS のインストール先のサーバーに自動的にインストールされ、プライマリ Connection Broker として指定されます。プライマリ RAS Connection Broker は各サイトに必須ですが、セカンダリ Connection Broker も追加できます。セカンダリ Connection Broker の目的は、プライマリ RAS Connection Broker の障害のためにサービスが中断し、ユーザーに影響を及ぼすのを防ぐことです。この章では、RAS Connection Broker をサイトに追加し、構成する方法について説明します。

この章の内容

RAS Connection Broker の構成

サイトにインストールされた RAS Connection Broker を表示するには、RAS Console で [ファーム] > <サイト> > [Connection Broker] に移動します。右ペインの [Connection Broker] タブに、インストールされた Connection Broker が一覧表示されます。

サイトには、少なくともプライマリ Connection Broker がインストールされている必要があり、その [プライオリティ] 列にはプライマリであることが記されています。冗長性を確保するためサイトにセカンダリ Agent を追加することもできます（次のセクションで説明します）。

Connection Broker の構成を変更するには、Connection Broker を選択してから、[タスク] > [プロパティ] をクリックします（または [プロパティ] を右クリックします）。[プロパティ] ダイアログが開きます。このダイアログでは以下の内容を変更できます。

- サイトでのサーバー有効化: Connection Broker を有効または無効にします。このオプションは、セカンダリ Connection Broker のみで有効になります。プライマリ Connection Broker では無効になっています。

- サーバー: Connection Broker をホストするサーバーの FDQN または IP アドレスを指定します。IP アドレスを自動的に FQDN に解決するには、[名前解決] グローバルオプションを有効にします。詳細については、「ホスト名の解決」（p. 568）を参照してください。
- IP: サーバーの IP アドレスを指定します。[サーバー] フィールドに指定した FQDN を使用して IP アドレスを自動的に取得するには、[解決] ボタンをクリックします。この IP アドレスは、複数の Connection Broker でリアルタイムで情報を共有するために使用されます。
- 代替の IP: 1 つ以上の代替 IP アドレスをセミコロンで区切って指定します。これらのアドレスは、RAS Secure Gateway が、FQDN または [IP] フィールドに指定されたアドレスを使用して RAS Connection Broker に接続できなかった場合に使用されます。これは Secure Gateway が、Active Directory に参加していないネットワークから接続されている場合などに発生する可能性があります。
- 説明: ユーザー定義の説明。
- スタンバイ: 選択されている場合、セカンダリ Connection Broker をスタンバイモードにします。つまり、別の Connection Broker がオフラインになるまで、どのエージェントもこの Connection Broker に接続しません。このオプションは、すでに存在する 3 つを超えるすべての新しいセカンダリ Connection Broker で自動的に有効になります。システムパフォーマンスが低下する可能性があるため、3 つを超えるアクティブな Connection Broker を使用することは推奨されません。このオプションを使用して、3 つを超える Agent を使用することができますが、必要になるまでスタンバイモードにしておきます。詳細については、「セカンダリ Connection Broker」（p. 79）を参照してください。

変更が完了したら、[OK] をクリックして、RAS Console のメインウィンドウで [適用] をクリックします。

[Connection Broker] タブの [タスク] ドロップダウンリストには、以下の項目があります。

- 追加: RAS Connection Broker をサイトに追加します。セカンダリ Connection Broker の追加方法の詳細については、続くセクションを参照してください。
- すべての Agent をアップグレード: Agent を現在のバージョンにアップグレードします。すべての Agent が最新の場合、この項目は無効になります。
- ツール: 標準的なサーバー管理ツールのセットへアクセスできます。
- トラブルシューティング: [Agent をチェック] メニュー項目により、Connection Broker が適切に機能していることを検証します。検証結果を確認し、オプションで Connection Broker をインストール（またはアンインストール）できるダイアログが開きます。[ロギン

グ] メニュー項目を利用すると、ロギングを構成したり、ログファイルを取得/クリアしたりすることができます。詳細については、「ロギング」（p. 608）を参照してください。

- プライマリへの昇格: セカンダリ Connection Broker をプライマリに昇格します。現在のプライマリ Connection Broker はセカンダリになります。
- 更新: Connection Broker リストを更新します。
- 削除: セカンダリ Connection Broker をサイトから削除します。プライマリ Connection Broker を削除するには、まずセカンダリ Connection Broker をプライマリに昇格させる必要があります。
- 設定監査: Connection Broker に加えられた変更を表示できる [設定監査] ダイアログが開きます。詳細については、「設定監査」（p. 586）を参照してください。
- ムーブアップ および ムーブダウン: セカンダリ Connection Broker の優先順位を変更します（優先順位リストで上下に移動します）。
- プロパティ: Connection Broker の [プロパティ] ダイアログが開きます（上記参照）。

RAS Connection Brokers の概要

上記で説明した Connection Broker エディターに加えて、利用可能な RAS Connection Broker についての概要も確認できます。このためには、次の操作を実行します。

1. RAS Console で、[ファーム] > <サイト> に移動します。
2. 利用可能な RAS Connection Broker は、[サイト情報] タブの [Connection Broker] グループに表示されます。
3. Connection Broker エディターに移動するには、RAS Connection Broker を右クリックして、[エディターに表示] を選択します。

詳細については、「RAS Console でのサイト」（p. 63）を参照してください。

セカンダリ Connection Broker

冗長性を確保するためにセカンダリ Connection Broker がサイトに追加されます。これにより、プライマリ Connection Broker に障害が発生しても、セカンダリ Connection Broker がリクエストを処理できるようになります。Connection Broker は、高可用性を確保するために、アクティブ/アクティブ構成で動作します。Connection Broker に障害が発生しても、負荷に対応可能な予備の Agent が常に待機しています。一般的に、N+1 の冗長構成をサイトごとに使用

する必要があります。自動昇格に 3 つを超える Connection Broker を設定することはできません（自動昇格は本セクションで後ほど説明します）。

セカンダリ Connection Broker を 1 つ以上インストールしておけば、ランタイムデータが各 Agent に複製され、サービスに障害が発生した場合にもダウンタイムを最小限に抑えられます。さらに、いずれかのアクティブな Connection Broker が、AD および使用される二要素認証プロバイダーの両方の認証に使用されます。

プライマリ Connection Broker はセカンダリ Connection Broker と同じタスクを実行しますが、それ以外の役割も担います。つまり、単一の Connection Broker による管理が必要な特定のプロセスを管理します。次の表は、プライマリ Connection Broker とセカンダリ Connection Broker によって管理されるプロセスのリストです。

プロセス	プライマリ Connection Broker	セカンダリ Connection Broker
PA（カウンター）のモニタリング	はい	はい
RD セッションホスト（カウンター）のモニタリング	はい	はい
プロバイダー（カウンター）のモニタリング	はい	はい
RDS セッション（再接続）のモニタリング	はい	はい
展開済みの RDS アプリケーションのモニタリング	はい	はい
VDI セッション（再接続）のモニタリング	はい	はい
システム設定の管理	はい	いいえ
ライセンス情報とハートビートの送信	はい	いいえ
CEP 情報の処理および送信	はい	いいえ
レポートサーバーへの情報の送信	はい	いいえ
RDS スケジューラーの管理	はい	いいえ
エンジン情報のレポート	はい	今後のバージョン
シャドーイング	はい	今後のバージョン
メール通知の送信	はい	いいえ

複数の Connection Broker の間で負荷分散がどのように機能するかを示すために、次の例を考えてみましょう。

- Connection Broker が 2 つあるとします。その内訳は、PA1（プライマリ）と PA2（セカンダリ）です。
- また、RD セッションホストが 10 台あるとします。RDS1、RDS2 ...RDS10 です。

発生する負荷は次のように分散されます。

- RDS1、RDS2 ...RDS4 は、PA1 を優先 Connection Broker として使用します。
- RDS5、RDS6 ...RDS10 は、PA2 を優先 Connection Broker として使用します。

セカンダリ Connection Broker のプランニング

同じサイトで実行されている RAS Connection Broker は、相互に通信し、負荷を分担します。1 つの Agent から別の Agent に伝送されるデータ量は膨大なため、信頼性の高い高速通信チャネルが求められます（例: Connection Broker の通信用にサブネットワークを構成できます）。

セカンダリ Connection Broker をサイトに追加して、その IP アドレスを指定します。すべての Agent の IP アドレスが、必ず同じネットワークセグメントに属するようにします。Connection Broker が相互の通信に使用するポートは、TCP 20030 です。

サイトに追加できる Connection Broker の数に物理的制限はありません。ただし、最も優れた結果が得られるのはエージェント数が 2〜3 のときです。特に、プロバイダーが存在し、VDI の高可用性（p. 226）を有効にしたい場合は、エージェント数を 3 個にするシナリオを強くお勧めします。2〜3 を超える数のセカンダリ Connection Broker をサイトに追加すると、逆の効果が生じ、実際にはシステムのパフォーマンスが低下する可能性があります。ただし、これはスタンバイモードのセカンダリ Connection Broker には当てはまりません。スタンバイモードのセカンダリ Connection Broker については、「RAS Connection Broker の構成」（p. 77）で説明されています。

RAS Connection Broker をサイトに追加する

セカンダリ Connection Broker を追加するには、次の操作を実行します。

1. RAS Console で、[ファーム] > <サイト> > [Connection Broker] に移動します。
2. [タスク] ドロップダウンリストをクリックし、[追加] を選択して、[RAS Connection Broker を追加] ウィザードを起動します。

3 [サーバー] フィールドは、RAS Connection Broker をホストするサーバーの FDQN または IP アドレスを指定します。IP アドレスを自動的に FQDN に解決するには、[名前解決] グローバルオプションを有効にします。詳細については、「ホスト名の解決」（p. 568）を参照してください。

4 [IP] フィールドは、サーバーの IP アドレスを指定します。[サーバー] フィールドに指定した FQDN を使用して IP アドレスを自動的に取得するには、[解決] ボタンをクリックします。

5 [代替 IP アドレス] フィールドでは、1 つ以上の代替 IP アドレスをセミコロンで区切って指定します。これらのアドレスは、RAS Secure Gateway が、FQDN または [IP] フィールドに指定されたアドレスを使用して RAS Connection Broker に接続できなかった場合に使用されます。これは Secure Gateway が、Active Directory に参加していない異なるネットワークから接続されている場合などに発生する可能性があります。

6 指定したサーバーに RAS Secure Gateway もインストールする場合は、[Connection Broker を使って Secure Gateway をイントール] オプションを選択します。このオプションを選択すると、[HTML5 ゲートウェイを有効化] オプションを選択することもできます（詳細については、「ユーザーポータルの構成」（p.97）を参照）。

7 サーバー上のファイアウォールを自動的に構成するには、[ファイアウォールルールを追加] オプションを選択します。詳細については、「ポート参照」を参照してください。

8 [次へ] をクリックします。

9 次のページで [インストール] をクリックして、RAS Connection Broker をサーバーにインストールします。[RAS Terminal Server Agent のインストール] ダイアログが開きます。

10 RAS Connection Broker をインストールするサーバーを選択して、[インストール] をクリックします。

11 [完了] をクリックします。

12 [OK] をクリックして、サーバーをファームに追加します。

セカンダリ Connection Broker の管理

セカンダリ Connection Broker を有効または無効にする

サイトでセカンダリ Connection Broker を有効または無効にするには、[Connection Broker] リストから目的の Agent を選択し、行の先頭にあるチェックボックスを選択またはクリアします。

セカンダリ Connection Broker の優先順位の変更

各セカンダリ Connection Broker には優先順位が与えられます。優先順位を変更するには、セカンダリ Connection Broker を選択し、上向き矢印と下向き矢印のアイコン（または [タスク] > [ムーブアップ] または [ムーブダウン]）を使用して、リストの中で上下に移動します。リスト内で上に配置されている Agent ほど、優先順位が高くなります。

セカンダリ Connection Broker をプライマリに昇格します

プライマリ Connection Broker を復元できない場合、次の手順に従って、セカンダリ Connection Broker をプライマリに昇格できます。

1. 昇格する Connection Broker サーバーで RAS Console を開きます（必要なファイルは、サーバーがセカンダリ Connection Broker としてサイトに追加されたときに、すべて自動的にインストールされています）。
2. [ファーム] カテゴリーを選択し、[Connection Broker] ノードに移動します。
3. Connection Broker を選択し、[タスク] > [プライマリへの昇格] をクリックします。
4. プロセスが完了したら、[OK] をクリックします。

自動昇格を構成する

プライマリ Connection Broker がオフラインになった場合、セカンダリ Connection Broker を昇格してプライマリと交代させる必要があります。自動昇格機能は、指定された時間が経過すると、これを自動的に実行します。

デフォルトでは、自動昇格はオフになっています。有効にするには、次の操作を実行します。

1. RAS Console で、[ファーム] > <サイト> > [Connection Broker] に移動します。
2. 右ペインで [自動昇格] タブを選択します。
3. [自動昇格を有効にする] オプションを選択し、次のセカンダリ Connection Broker がプライマリに昇格するまでの時間を指定します。時間は、15 分間～72 時間の間で設定できます（デフォルト値は 30 分です）。
4. 元の Connection Broker が再度オンラインになったらプライマリに戻す場合は、[フェイルバックを有効にする] オプションを選択します。ライセンスサイトではこれにより、フェイルバックが 72 時間以内に発生した場合のライセンスアクティベーションが不要になります。ライセンスアクティベーションカウントダウンは常に RAS Console に表示されているため、管理者は、元のプライマリ Connection Broker がこの時間内に回復するかどうかを確

認できます。元のエージェントが 72 時間を過ぎてからオンラインに戻った場合（かつファームがすでに再アクティベートされている場合）、元の Agent がセカンダリ Connection Broker になります。

注: 自動昇格を有効にするには、サイトに最低 3 つのアクティブな Connection Broker が必要です。3 つ未満の場合、自動昇格は無視されます。

不良な WAN リンクで別々の場所に Connection Broker が分割されている 1 つのサイトの場合、自動昇格は無効にする必要があることにも注意してください。リモートに配置されている Connection Broker の間にリンクがない場合、3 つ目の Connection Broker がスプリットブレインを防止するために監視します。

自動昇格が実行されるとき、RAS 管理者は以下のイベントについてメールを介して通知を受け取ります。

- セカンダリ Connection Broker がプライマリに昇格された。
- セカンダリ Connection Broker の自動昇格が失敗した。
- 自動昇格フェイルバックが完了した。

セカンダリ Connection Broker を削除する

セカンダリ Connection Broker を削除するには、対象の Connection Broker をリストで選択し、[タスク] ドロップダウンリストで [削除] をクリックします。

コンピューター管理ツールの使用

RAS Console から、RAS Connection Broker をホスティングしているサーバーで標準的なコンピューター管理タスクを直接実行できます。このタスクには、リモートデスクトップ接続、リモート PowerShell 接続、コンピューター管理、サービス管理、イベントビューアー、IPconfig、再起動などが含まれます。[ツール] メニューにアクセスするには、サーバーを選択して [タスク] をクリックし、[ツール] をクリックして目的のツールを選択します。要件と使用方法については、「コンピューター管理ツール」（p. 569）を参照してください。

第　6　章

RAS Secure Gateway

RAS Secure Gateway は、すべての Parallels RAS データを 1 つのポート上でトンネリングします。また、RAS Secure Client Gateway は、セキュアな接続を提供し、Parallels RAS へのユーザー接続点となります。

すべてのサイトに対して、最低 1 つの RAS Secure Gateway をインストールし、構成する必要があります。あるサイトがテナントとして RAS テナントブローカーに参加する場合、RAS Secure Gateway は不要です。詳細については、「RAS マルチテナントアーキテクチャ」(p. 397) を参照してください。

要件によっては、複数のゲートウェイが存在する場合があります。この章では、RAS Secure Gateway を追加、構成、管理する方法について説明します。

この章の内容

概要

Parallels RAS が機能するには、少なくとも 1 つの RAS Secure Gateway をインストールする必要があります。RAS サイトに Gateways を追加することで、さらに多数のユーザーやロードバランス接続に対応し、冗長性を実現することができます。

専用サーバーに RAS Secure Gateway をインストールする

専用サーバーに RAS Secure Gateway をインストールする場合、同じサーバーに Parallels RAS Console もインストールできます。コンソールの機能は制限されますが、Gateway で次のような重要な管理作業のいくつかを実行できます。

- Gateway の動作モードの設定（通常モードまたは転送。詳細については、下記を参照してください）。
- Gateway を管理する RAS Connection Broker の割り当て。
- Gateway 通信ポートの設定。
- ホスト OS バージョン、Parallels RAS バージョン、利用可能な IP アドレス、などの Gateway 情報の表示。

このようなインストールシナリオ（RAS ファームではなく、ローカルコンピューターに接続されている場合）では、RAS Console の左ペインで選択できるカテゴリが、[ゲートウェイ] と [情報] の 2 つのみになります。Gateway 設定を管理するには、[ゲートウェイ] を選択し、右ペインで [所有権の変更] をクリックします。情報を表示するには、[情報] カテゴリを選択します。

RAS Console が Parallels RAS ファーム（つまり、RAS Connection Broker が動作しているサーバー）に接続している場合、[ファーム] > <サイト> > [Secure Gateway] に移動して、RAS Secure Gateway を管理できます。

RAS Secure Gateway の仕組み

ここでは、RAS Secure Gateway がユーザーの接続要求を処理する方法について説明します。

1. RAS Secure Gateway は、ユーザーの接続要求を受信します。
2. その後、要求を登録先の RAS Connection Broker に転送します（デフォルトでの推奨 Connection Broker 設定）。
3. RAS Connection Broker は、ロードバランスチェックと Active Directory セキュリティ検索を実行し、セキュリティ権限を取得します。
4. 公開済みのリソースをリクエストしたユーザーが十分な権限を持っている場合、RAS Connection Broker はゲートウェイに応答を返します。応答には、ユーザーがどの RD セッションホストに接続できるかについての詳細が含まれます。

5 クライアントは、接続モードに応じて、ゲートウェイを介して接続するか、ゲートウェイを切断して RD セッションホストサーバーに直接接続します。

RAS Secure Gateway の動作モード

RAS Secure Gateway は、次のいずれかのモードで動作します。

- 通常モード: 通常モードの RAS Secure Gateway は、ユーザー接続リクエストを受け取った後、要求したユーザーにアクセス権があるかどうかを、RAS Connection Broker に確認します。このモードで動作するゲートウェイを使用することで、より多くのリクエストをサポートすることができ、冗長性を向上させることができます。
- 転送モード: 転送モードの RAS Secure Gateway は、ユーザー接続リクエストを、事前に構成されたゲートウェイに転送します。ファイアウォールカスケードを使用する場合は、WAN 接続を LAN 接続から切り離すのに転送モードのゲートウェイが役立ちます。また、転送モードのゲートウェイを使用すると、問題発生時に LAN を中断することなく WAN セグメントを切断できます。

注: 転送モードを構成するには、Parallels RAS ファームに複数の RAS Secure Gateway が必要です。

高可用性のためのプラン

RAS Secure Gateway をサイトに追加する際、ユーザーに提供するサービスが中断しないよう、N+1 の冗長性を構成する必要があります。これは、Connection Broker や RD セッションホストなど、他の Parallels RAS コンポーネントにも当てはまります。

RAS Secure Gateway の追加

RAS Secure Gateway をサイトに追加するには、次の手順を実行します。

1 RAS Console で、[ファーム] > <サイト> > [Secure Gateway] に移動します。

2 右ペインの [Secure Gateways] タブが選択された状態で、[タスク] > [追加] をクリックして、[RAS Secure Gateway の追加] ウィザードを開始します。

3 サーバーの FQDN または IP アドレスを入力します（または [...] ボタンをクリックして、リストからサーバーを選択します）。IP アドレスを自動的に FQDN に解決するには、[名前解決] グローバルオプションを有効にします。詳細については、「ホスト名の解決」（p. 568）を参照してください。

4 [モード] ドロップダウンリストからゲートウェイモードを選択します。

5 上記の手順で [転送先] モードを選択した場合は、[転送先] ドロップダウンリストで転送先のゲートウェイを選択します。ゲートウェイサーバーに複数の IP アドレスがある場合は、[オン IP] ドロップダウンリストで特定の IP アドレスを選択することもできます。

6 [HTML5 ゲートウェイの有効化] オプションを選択して、自己署名証明書の作成、SSL の有効化、および HTML5 サポートの有効化を自動で行います。詳細については、「ユーザーポータルの構成」（p. 97）を参照してください。

7 ゲートウェイをホストしているサーバー上のファイアウォールを自動的に構成するには、[ファイアウォールルールを追加] を選択します。詳細については、「ポート参照」を参照してください。

8 [次へ] をクリックします。

9 次のページで [インストール] をクリックして、RAS Secure Gateway のインストールを開始します。

10 インストールが終了したら、[完了] をクリックします。

手動による RAS Secure Gateway の追加

RAS Secure Gateway を手動でインストールしてファームに追加するには、次の手順を実行します。

1 RAS Secure Gateway をインストールするサーバーに管理者アカウントを使用してログインします。

2 Parallels RAS のインストールファイル（`RASInstaller.msi`）をサーバーにコピーし、そのファイルをダブルクリックして、インストールウィザードを開始します。

3 画面の指示に従って、インストールタイプのページに進みます。[カスタム] を選択し、[次へ] をクリックします。

4 機能ツリーで [RAS Secure Gateway] をクリックし、[このコンピューターのローカルディスクにすべての機能をインストールします] を選択します。

5 選択ツリーで他のすべてのコンポーネントが選択解除されていることを確認し、[次へ] をクリックします。

6 [インストール] をクリックしてインストールを開始します。

7 インストールが完了したら、[完了] をクリックしてウィザードを閉じます。

8 RAS Console を開いて、ゲートウェイを管理する RAS Connection Broker を指定します。

RAS Secure Gateway のステータスの確認

RAS Secure Gateway のステータスを確認するには、リストを右クリックして、コンテキストメニューの [ステータスをチェックする] をクリックします。[RAS Secure Gateway 情報] ダイアログが開きます。

ダイアログには、次のようなゲートウェイ情報が表示されます。

- サーバー: ゲートウェイがインストールされているサーバーの名前。
- Gateway: ゲートウェイの確認ステータス（確認済みなど）。
- バージョン: ゲートウェイソフトウェアのバージョン番号。バージョン番号は、Parallels RAS のバージョン番号と一致している必要があります。
- OS タイプ: オペレーティングシステムのタイプとバージョン。
- ステータス: 現在の RAS Secure Gateway のステータスを表示。ステータスが問題を示している場合は（ゲートウェイが応答しない、ゲートウェイソフトウェアのバージョンが間違っているなど）、[インストール] ボタンをクリックして、サーバーにゲートウェイをプッシュインストールします。インストールが完了するのを待ち、再度ステータスを確認します。

RAS Secure Gateway の構成

RAS Secure Gateway を構成するには、次の操作を実行します。

1 RAS Console で、[ファーム] > <サイト> > [Secure Gateway] に移動します。

2 右ペインで、Secure Gateway を右クリックして、[プロパティ] をクリックします。

3 [RAS Secure Gateway プロパティ] ダイアログが開きます。

RAS Secure Gateway のプロパティを構成する方法については、こちらを参照してください。

Secure Gateway の有効化および無効化

RAS Secure Gateway は、デフォルトで有効になっています。Secure Gateway を有効化/無効化するには、[RAS Secure Gateway プロパティ] ダイアログの [一般] タブで [サイト内の RAS Secure Gateway を有効化] オプションを選択/クリアします。

パブリックアドレスを設定

[一般] タブの [パブリックアドレス] フィールドには、Secure Gateway のパブリック FQDN または IP アドレスを指定します。この設定は、クライアントの接続をリダイレクトするために優先ルーティング機能で使用されます。「優先ルーティングを構成」（p. 319）を参照してください。

クライアント接続用の IP アドレスの設定

Secure Gateway の受信クライアント接続用の IP アドレスは、[一般] タブの [RAS Secure Gateway プロパティ] ダイアログで指定します。RAS Secure Gateway は IPv4 と IPv6 の両方を認識します。デフォルトでは、IPv4 が使用されます。

次の IP オプションを指定できます。

- 次の IP バージョンを使用: 使用する IP バージョンを選択します。
- IP: 1 つ以上の IP アドレスをセミコロンで区切って指定するか、[解決] をクリックして IP アドレスを自動解決します。それらのアドレスを Secure Gateway サーバーで使用できます。クライアント接続で使用する IP アドレスを指定する場合は、[IP にバインド] セクションを使用します（下記参照）。
- IP にバインド: クライアント接続で Secure Gateway が待機する IP アドレス（複数の場合もあり）を指定するには、このセクションを使用します。特定のアドレスを指定できます。または、<利用できるすべてのアドレス>を指定して、[IP] フィールドに指定されたすべての IP を使用することもできます。
- 次の…システムバッファを削除: これらのフィールド（各 IP バージョンに 1 つ）を使用すると、この Secure Gateway と Parallels Client 間の接続で高遅延が発生した場合（インターネットなど）に、トラフィックが最適化されます。このオプションによりトラフィックが最適化され、Parallels Client 側の操作性が向上します。特定のアドレスまたは利用できるすべてのアドレスを選択できます。または、選択しないこともできます。このオプションは、外部ソケットのパフォーマンスにマッチさせるために内部ソケットを遅延させます。内部ネットワークが速く、外部ネットワークが遅い場合、RDP が速い内部ソケットを検出し、大量のデータを送信します。問題は、データを Secure Gateway からクライアントに十分な速度で送信できず、ユーザーエクスペリエンスが悪化することです。このオプションを有効にすると、データのやり取りが最適化されます。

サイトのデフォルト値（Secure Gateway）

RAS Secure Gateway の [プロパティ] ダイアログには複数のタブがあり、それぞれに固有のオプションが含まれています。[プロパティ] タブ以外のタブにはすべて、[デフォルト設定を継承する] という共通のオプションがあります。このオプションを選択すると、そのタブの全フィールドがグレイアウトし、サイトのデフォルト値が設定内容として継承されます。Secure Gateway のサイトのデフォルト値を表示する（必要な場合は変更する）には、上述のタブすべてにある [サイトのデフォルト値] リンクをクリックします。リンクによって、[サイトのデフォルトプロパティ] ダイアログが開きます。このダイアログは、[ファーム] > [サイト] > [Secure Gateway] タブで [タスク] > [サイトのデフォルト] をクリックすることでも開くことができます。

続くセクションでは、それぞれのタブと、Secure Gateway の [プロパティ] ダイアログで使用できるオプションについて説明します。

ゲートウェイモードと転送設定

RAS Secure Gateway は、「通常モードおよび転送モード」（p. 85）で動作します。希望のモードと関連する設定を構成するには、[RAS Secure Gateway プロパティ] ダイアログの [モード] タブをクリックします。

サイトのデフォルト値を使用

サイトのデフォルト設定を使用するには、[デフォルト設定を継承] オプションをクリックします。固有の設定を指定するには、オプションをクリアします。詳細については、「サイトのデフォルト値（ゲートウェイ）」（p. 91）を参照してください。

通常モードの設定

通常モードを設定するには、[ゲートウェイモード] ドロップダウンリストで [通常] を選択します。

[HTTP サーバーにリクエストを転送] オプションを使用すると、RAS Secure Gateway（HTML5 トラフィック、Wyse、および URL スキームを処理するゲートウェイ）に属していないリクエストを転送できます。複数のサーバーを指定するには、それらをセミコロンで区切ります。必要な場合、IPv6 アドレスを使用して HTTP サーバーを指定できます。リクエスト元のブラウザーと同じ IP バージョンが HTTP サーバーでサポートされていることが必要です。

[推奨 Connection Broker] ドロップダウンリストでは、Secure Gateway が接続する必要がある RAS Connection Broker を指定できます。これは、サイトコンポーネントが、WAN で通信する複数の物理的な場所に設置されているときに役立ちます。より適切な Connection Broker を指定することによりネットワークトラフィックを減らすことができます。ゲートウェイで自動的に Connection Broker が選択されるようにするには、[自動] オプションを選択します。

転送モードの設定

転送モードを設定するには、[ゲートウェイモード] ドロップダウンリストで [転送] を選択します。

[RAS Secure Gateway の転送] フィールドで、1 つ以上の転送 Secure Gateway を指定（または選択）します。

注: 転送モードでは、IPv6 を待機する Secure Gateway にデータを転送できます。転送 Secure Gateway は、同じ IP バージョンを使用するように構成することをお勧めします。

ゲートウェイネットワークオプション

[ネットワーク] タブは、RAS Secure Gateway のネットワークオプションの構成に使用します。

サイトのデフォルト値を使用

サイトのデフォルト設定を使用するには、[デフォルト設定を継承] オプションをクリックします。固有の設定を指定するには、オプションをクリアします。詳細については、「サイトのデフォルト値（ゲートウェイ）」（p. 91）を参照してください。

ネットワークの構成

デフォルトでは、RAS Secure Gateway は TCP ポート 80 と 443 上で待機し、すべての Parallels RAS トラフィックをトンネリングします。ポートを変更するには、[RAS Secure Gateway ポート] 入力フィールドで新しいポートを指定します。

負荷分散された基本的なデスクトップセッションを必要とするクライアントでは、RDP ポート 3389 が使用されます。このポート上の接続では、公開済みのリソースはサポートされません。ゲートウェイの RDP ポートを変更するには、[RDP ポート] オプションを選択して、新しいポ

ートを指定します。自分でポートを設定する場合、そのポート番号が標準の [RD セッションホストポート] 設定と重複していないことを確認してください

注: RDP ポートを変更した場合、ユーザーはリモートデスクトップクライアント内の接続文字列にポート番号を追加する必要があります（例: IP アドレス:ポート）。

Secure ゲートウェイのアドレスを伝播する ： このオプションを使用して、Secure Gateway アドレスのブロードキャストを有効にすることができます。これにより、Parallels Client でプライマリゲートウェイを自動的に見つけることができます。このオプションは、デフォルトで有効になっています。

RDP UDP データトンネリングを有効にする : Windows デバイスで UDP トンネリングを有効にするには、このオプションを選択します（デフォルト）。UDP トンネルを無効にするには、このオプションをオフにします。

デバイスマネージャーポート: デバイスマネージャーカテゴリーから Windows デバイスの管理を有効にするには、このオプションを選択します。このオプションは、デフォルトで有効になっています。

RDP DOS アタックフィルターを有効にする: このオプションを選択すると、同一 IP アドレスからの一連の未完了セッションが拒否されます。たとえば、Parallels Client が各セッションで複数の連続したセッションを開始し、ユーザーからの資格情報の提供を待っている場合、Parallels RAS はこれ以上の試行を拒否します。このオプションは、デフォルトで有効になっています。

SSL/TLS 暗号化

Parallels RAS ユーザーと RAS Secure Gateway 間のトラフィックは暗号化できます。[SSL/TLS] タブでは、データ暗号化オプションを構成できます。

サイトのデフォルト値を使用

サイトのデフォルト設定を使用するには、[デフォルト設定を継承] オプションをクリックします。固有の設定を指定するには、オプションをクリアします。詳細については、「サイトのデフォルト値（ゲートウェイ）」（p. 91）を参照してください。

HSTS を適用

HSTS セクションの [構成] ボタンによって、HTTP Strict Transport Security（HSTS）を適用できます。これは、安全な HTTPS 接続のみを使用してウェブブラウザーにウェブサーバーと通信させるメカニズムです。HSTS が RAS Secure Gateway に適用されると、すべてのウェブリクエストが HTTPS を使用するように強制されます。これは特に RAS ユーザーポータル（p. 97）に影響し、セキュリティ上の理由から通常は HTTPS リクエストのみを受け付けます。

[構成] ボタンをクリックすると、[HSTS 設定] ダイアログが開きます。このダイアログでは、次の内容を指定できます。

- HTTP Strict Transport Security（HSTS）を適用する: Secure Gateway に対し、HSTS を有効化または無効化します。
- 最大期間: HSTS の最大期間を指定します。これは、ウェブブラウザーと Secure Gateway との通信に必ず HTTPS が使用されるという設定が適用される（月単位の）期間です。デフォルト値（および推奨値）は 12 か月です。設定可能な値は 4〜120 か月です。
- サブドメインを含む: サブドメインを含めるかどうかを指定します（サブドメインがある場合）。
- 事前読み込み: HSTS の事前読み込みを有効化または無効化します。これは、SSL/TLS をサイトで適用するホストのリストがウェブブラウザーにハードコーディングされるメカニズムです。リストは Google によりコンパイルされ、Chrome、Firefox、Safari、Internet Explorer 11、Edge といったブラウザーにより使用されます。HSTS のプリロードが使用されると、ウェブブラウザーは HTTP を使用してリクエストを送信せず、常に HTTPS が使用されます。以下に重要な注意点がありますのでこちらもお読みください。

注: HSTS のプリロードを使用するには、Chrome の HSTS プリロードリストに含めるドメイン名を送信する必要があります。ドメインはリストを使用するウェブブラウザーにハードコードされます。重要: プリロードリストへ含めるアクションは簡単には取り消せません。サイト全体およびそのすべてのサブドメインで長期的に（通常 1〜2 年）HTTPS をサポートできることが確実な場合にのみ、リクエストを含めてください。

次の要件にも注意してください。

- ウェブサイトに有効な SSL 証明書が存在している必要があります。「SSL サーバー構成」（p. 97）を参照してください。
- すべてのサブドメイン（サブドメインがある場合）が SSL 証明書でカバーされている必要があります。ワイルドカード証明書を要求することを検討してください。

SSL の構成

デフォルトでは、ゲートウェイのインストール時に、自己署名証明書が RAS Secure Gateway に割り当てられます。RAS Secure Gateway ごとに専用の証明書の割り当てが必要です。また、セキュリティ警告を回避するため、クライアント側の信頼できるルート認証局に追加する必要があります。

SSL 証明書は、RAS Console の [ファーム] > [サイト] > [証明書] サブカテゴリーを使用して作成できます。作成された証明書は、RAS Secure Gateway に割り当てることができます。証明書の作成と管理については、「SSL 証明書の管理」（p. 338）の章を参照してください。

Secure Gateway に SSL を構成する方法:

1. [SSL 有効化] オプションを選択し、ポート番号を指定します（デフォルトは 443）。
2. [許可される SSL バージョン] ドロップダウンリストで、RAS Secure Gateway が受け付けられる SSL バージョンを選択します。
3. [暗号強度] フィールドで、希望する暗号強度を選択します。
4. [暗号] フィールドに暗号を指定します。強い暗号を使用すれば、暗号化の強度が増し、破るのに必要な労力も増大します。
5. [サーバー環境に応じて暗号を使用] オプションは、デフォルトで有効になっています。このオプションを無効にすることで、クライアントの環境設定を使用することができます。
6. [証明書] ドロップダウンリストで任意の証明書を選択します。新規証明書の作成方法とリストへの表示方法については、「SSL 証明書の管理」（p. 338）を参照してください。

   [一致する使用方法すべて] オプションでは、構成されたすべての証明書が Secure Gateway によって使用されます。証明書を作成する場合、”ゲートウェイ”、”HALB”またはその両方を選択できる場所で”使用”プロパティを指定します。このプロパティで [ゲートウェイ] オプションが選択されていれば、Secure Gateway に使用できます。このオプションを選択していても、一致する証明書が存在しない場合には、警告が表示され、先に証明書を作成することになります。

Parallels Client の接続の暗号化

デフォルトで、暗号化される接続のタイプは、Secure Gateway とバックエンドサーバーの間の接続だけです。Parallels Client と Secure Gateway の間の接続を暗号化するには、クライアント側でも接続プロパティを構成する必要があります。これを行うには、Parallels Client で、接続プロパティを開き、接続モードを [ゲートウェイ SSL] に設定します。

Parallels Client の構成を簡素化するために、広く利用されているサードパーティの信頼できる認証局によって発行された証明書を使用することをお勧めします。なお、RAS ユーザーポータルに接続する際は、一部のウェブブラウザー（Chrome、Edge など）で Windows 証明書ストアが使用されます。

Parallels Client の構成

証明書が自己署名されている場合、またはエンタープライズ CA によって発行された証明書の場合、Parallels Client は以下のように構成する必要があります。

1. Base-64 でエンコードされた X.509（.CER）形式で証明書をエクスポートします。
2. メモ帳やワードパッドなどのテキストエディターでエクスポートした証明書を開き、内容をクリップボードにコピーします。

クライアント側で信頼できる認証局のリストを含む証明書を追加し、Parallels Client が組織の認証局から発行された証明書と SSL で接続できるようにするには、次の操作を実行します。

1. クライアント側のディレクトリ”C:\Program Files\Parallels\Remote Application Server Client\”に、`trusted.pem` というファイルが存在している必要があります。このファイルには、共通の信頼できる認証局の証明書が含まれています。
2. エクスポートされた証明書の内容を貼り付けます（他の証明書のリストに添付されています）。

RDP-UDP 接続の保護

通常、Parallels Client は RAS Secure Gateway と TCP 接続経由で通信します。最近の Windows クライアントでも、UDP 接続を使用して WAN のパフォーマンスを向上することができます。UDP 接続を SSL で保護するには、DTLS を使用する必要があります。

RAS Secure Gateway で DTLS を使用するには、次の操作を実行します。

1. [SSL/TLS] タブで、[ポートで SSL 有効化] オプションが選択されていることを確認します。
2. [ネットワーク] タブ（p. 92）で、[RDP UDP データトンネリングを有効にする] オプションが選択されていることを確認します。

Parallels Client は、[ゲートウェイ SSL モード] を使用するよう構成する必要があります。このオプションは、クライアント側の [接続設定] > [接続モード] ドロップダウンリストで設定できます。

上記オプションが適切に設定されると、TCP および UDP 接続が SSL 上でトンネリングされます。

SSL サーバー構成

RAS Secure Gateway を構成して、SSL 暗号化を使用するには、発生する可能性のあるトラップやセキュリティの問題を回避するために SSL サーバーの構成方法に注意する必要があります。具体的には、次の SSL コンポーネントをレーティングし、構成が適切であるかどうかを特定する必要があります。

- 有効で信頼できる証明書。
- プロトコル、鍵の交換、暗号がサポートされている必要があります。

SSL について特定の知識がない場合、査定を行うのは困難かもしれません。Qualys SSL Labs の SSL Server Test の使用をお勧めするのはそのためです。これは、公衆インターネットで SSL ウェブサーバーの構成の分析を実行する無料のオンラインサービスです。RAS Secure Gateway でテストを実行するには、公衆インターネットにそれを一時的に移動する必要が生じる場合があります。

テストは次の URL で実行できます。https://www.ssllabs.com/ssltest/

次の URL で、査定に使用されるメソッドについて説明している Qualys SSL Labs の資料を参照できます。https://github.com/ssllabs/research/wiki/SSL-Server-Rating-Guide

ユーザーポータルを構成する

Parallels ユーザーポータルは、RAS Secure Gateway に組み込まれた機能です。この機能を使用すると、ユーザーは Parallels Web Client を使用して Parallels RAS に接続し、ウェブブラウザーから公開リソースを開くことができます。このクライアントは、プラットフォーム別の Parallels Client に似ていますが、ユーザーのコンピューターやデバイスにソフトウェアを追加でインストールしておく必要がありません。必要なのは HTML5 対応のウェブブラウザーだけです。

このセクションでは、Parallels RAS Console でユーザーポータルを構成する方法について説明します。使用方法の詳細については、「Parallels Web Client とユーザーポータル」の章（p. 454）を参照してください。

注: Web Client とユーザーポータルを使用するには、RAS Secure Gateway で SSL を有効にする必要があります。クライアントを有効にする場合は、[SSL/TLS] タブまたはネットワークロードバラン

サーで SSL が有効になっていることを確認してください。[ユーザーポータル] タブは、ゲートウェイモードが”通常”に設定されている場合にのみ使用できます。詳細については、「ゲートウェイモードと転送設定」を参照してください（p. 91）。

ユーザーポータルを構成するには、[RAS Secure Gateway プロパティ] ダイアログで [ユーザーポータル] タブをクリックしてから、続くセクションに記載のオプションを設定します。

Web Client の URL の構成方法と、ウェブブラウザーからクライアントにアクセスする方法については、「ウェブリクエストのロードバランス」（p. 102）を参照してください。

サイトのデフォルト値を使用

[ユーザーポータル] タブでサイトのデフォルト設定を使用するには、[デフォルト設定を継承] オプションをクリックします。固有の設定を指定するには、オプションをクリアします。詳細については、「サイトのデフォルト値（ゲートウェイ）」（p. 91）を参照してください。

ユーザーポータルを有効化または無効化する

ユーザーポータルを有効化/無効化するには、[ユーザーポータルを有効化] オプションを選択/クリアします。これにより、ユーザーポータルが無効になり、ユーザーは Web Client を使用してユーザーポータルに接続できなくなります。

クライアントの設定

[クライアント] セクションでは、Web Client の起動方法やその他の設定を指定できます。

- 以下を使用してセッションを起動: ユーザーがユーザーポータルのウェブページからリソースを開くときに、ウェブブラウザー内にリソースを開くことも、ユーザーのコンピューターにインストールされているプラットフォーム専用の Parallels Client（Parallels Client for Windows など）でリソースを開くことも可能です。このオプションで、どちらのクライアントを使用するかを指定します。ユーザーポータルに比べ、プラットフォーム専用の Parallels Client は機能がさらに豊富で、全体的なユーザーエクスペリエンスにも優れています。次のいずれかを選択します。

  a ブラウザーのみ - ユーザーは Parallels Web Client のみを使用してリモートアプリケーションとデスクトップを実行できます。ユーザーにプラットフォーム固有の Parallels Client をインストールさせたくない場合は、このオプションを使用します。

  b Parallels Client のみ - ユーザーは Parallels Client のみを使用してリモートアプリケーションとデスクトップを実行できます。ユーザーが Parallels Web Client を使用して Parallels RAS に接続すると、リモートアプリケーションとデスクトップを起動する前

に、プラットフォーム固有の Parallels Client をインストールするように求められます。メッセージが表示され、Parallels Client インストーラーをダウンロードするためのリンクがユーザーに表示されます。ユーザーが Parallels Client をインストールした後も、Parallels Web Client でリモートアプリケーションまたはデスクトップを選択できますが、それらは代わりに Parallels Client で開かれます。

c Parallels Client でのブラウザーへのフォールバック - Parallels Client とブラウザー（HTML5）の両方を使用して、リモートアプリケーションとデスクトップを起動できます。Parallels Client が主要な方法になります。何かの理由で公開済みのリソースを Parallels Client では起動できない場合、バックアップ方法として Parallels Web Client が使用されます。Parallels Client でリソースを開くことができなかった場合、ユーザーに通知され、代わりにブラウザーで開くことができます。

- ユーザーが起動方法を選択することを許可: このオプションを選択すると、ブラウザーまたは Parallels Client でリモートアプリケーションを開くかどうかを選択できます。このオプションは、[以下を使用してセッションを起動:] オプション（上記）が [Parallels Client でのブラウザーへのフォールバック] に設定されている場合（つまり両方の方法が許可されている場合）にのみ、有効にできます。
- 新規タブでアプリケーションを開く: 選択されている場合、ユーザーは、ウェブブラウザーの新しいタブでリモートアプリケーションを開くことができます。
- 以前の Windows 2000 ログイン形式を使用: レガシー（Windows 2000 以前）のログインフォーマットを有効化します。
- ユーザーポータルを他のウェブページに埋め込むことを許可: これを選択すると、ユーザーポータルのウェブページを他のウェブページに埋め込むことができます。これは、クリックジャックと呼ばれる攻撃による潜在的なセキュリティ上のリスクになる可能性があることに注意してください。
- ファイル転送コマンドを許可: リモートセッションでのファイル転送を有効化します。ファイル転送を有効にするには、このオプションを選択し、[構成] ボタンをクリックします。開いたダイアログで、[クライアントからサーバーのみ]（クライアントからサーバーへのファイル転送のみ）、[サーバーからクライアントのみ]（サーバーからクライアントへのファイル転送のみ）、[双方向]（双方向のファイル転送）を選択します。詳細については、「リモートファイル転送を構成する」（p. 538）を参照してください。
- クリップボードコマンドを許可: リモートセッションでのクリップボード操作（コピー/ペースト）を有効化します。クリップボードを有効にするには、このオプションを選択し、[構成] ボタンをクリックします。開いたダイアログで、[クライアントからサーバーのみ]（クライアントからサーバーへのコピー/ペーストのみ）、[サーバーからクライアントのみ]（サーバーからクライアントへのコピー/ペーストのみ）、[双方向]（双方向のコピー/ペースト）を選

択します。クリップボードの使用の詳細については、「リモートクリップボードの使用」(p. 479) を参照してください。

- オリジン間リソース共有を許可: オリジン間リソース共有（CORS）を有効化します。CORS を有効にするには、このオプションを選択し、[構成] ボタンをクリックします。開いたダイアログで、リソースへのアクセスを許可する 1 つまたは複数のドメインを指定します。ドメインを指定しない場合、このオプションは自動的に無効になります。[ブラウザーのキャッシュ時間] フィールドで、エンドユーザーのブラウザーでリソースがキャッシュされる時間を指定します。

ネットワークロードバランサーへのアクセス

[ネットワークロードバランサーへのアクセス] セクションは、Amazon Web Services（AWS）の Elastic Load Balancer（ELB）などのサードパーティー製ロードバランサーを使用する展開シナリオでの利用を意図したものです。ネットワークロードバランサー（NLB）で使用する代替ホスト名とポート番号を構成できます。TCP 通信と HTTPS 通信が実行されるホスト名およびポートを別々にしておくことが必要です。AWS ロードバランサーでは、同じポート上で 2 つの個別のプロトコルをサポートすることはないためです。

次のオプションを利用できます。

- 代替ホスト名を使用する: このオプションを選択し、代替ホスト名を指定します。代替ホスト名を有効化すると、プラットフォーム別の Parallels Client では RAS ファームまたはサイトへの接続にそのホスト名が使用されます。
- 代替ポートを使用する: このオプションを選択し、代替ポート番号を指定します。ポート番号は、RAS ファームまたはサイトの他のコンポーネントで使用されていないことが必要です。ポート番号をデフォルトに戻すには、[デフォルト] をクリックします。代替ポートを有効化すると、プラットフォーム別の Parallels Client では RAS ファームまたはサイトへの接続にそのポートが使用されます。Web Client の RDP セッションでは引き続き標準 SSL ポート（443）で接続されることに注意してください。

注: マルチテナント環境では、代替ホストや代替ポートの使用が適切でない点に注意してください。テナントブローカー RAS Secure Gateway はテナント間で共有され、これには別の構成が必要になるためです。

さらに、Parallels Web Client で必要な HTTP/HTTPS トラフィックを処理する AWS アプリケーションロードバランサー（ALB）では、通常自動的に生成される特定の Cookie のみがサポートされています。ロードバランサーは、クライアントからのリクエストを最初に受信すると、リクエストをターゲットにルーティングし、`AWSALB` という Cookie を生成します。これは、選択されたターゲットの情報をエンコードしたものです。ロードバランサーはこの Cookie

を暗号化してクライアントへの応答に含めます。スティッキーセッションが有効になっている場合、ロードバランサーは同じターゲットが正しく登録され、正常な状態にあると想定し、クライアントから受信した Cookie を使用してトラフィックをそのターゲットにルーティングします。デフォルトでは、Parallels RAS は `_SessionId` という名前の専用 ASP.NET Cookie を使用します。ただし、上記のスティッキーセッション用 AWS Cookie を指定して Cookie をカスタマイズすることが必要です。これは、[ウェブリクエスト] タブの [ウェブ Cookie] フィールドを使用して設定できます。この機能は Parallels RAS 17.1 以降で利用できます。

Wyse ThinOS のサポート

Wyse ThinOS を使用してアプリケーションを Parallels RAS からシンクライアントに公開するには、[Wyse] タブで [Wyse ThinOS サポートを有効化する] オプションを選択します。

注: [Wyse] タブは、ゲートウェイモードが [通常] に設定されている場合にのみ使用できます。詳細については、「ゲートウェイモードと転送設定の設定」（p. 91）を参照してください。

このオプションを有効にすると、RAS Secure Gateway が Wyse Broker として機能します。この Secure Gateway からブートしようとしているシンクライアントは、DHCP サーバー上で DHCP オプション 188 がこのゲートウェイの IP アドレスに設定されていることを確認する必要があります。DHCP サーバーを構成したら、[テスト] ボタンをクリックして、DHCP サーバーの設定を確認します。

ホスト名が証明書と一致しないために、RAS Secure Gateway への接続時に Wyse デバイスで SSL 警告が表示される場合、[サーバー証明書認証の警告を表示しない] オプションを選択（有効化）できます。このオプションを選択すると、Secure Gateway は、wnos.ini ファイル内の次のパラメーターを Wyse クライアントに送信します: SecurityPolicy=low TLSCheckCN=no（これにより SSL の確認が無効化）。なお、証明書に以下の項目がある場合、このオプションは必要ありません:

- CNAME が RAS Secure Gateway の FQDN に設定されている。
- SAN が RAS Secure Gateway の IP アドレスに設定されている。

Secure Gateway 上の”C:\Program Files (x86)\Parallels\ApplicationServer\AppData\wnos”フォルダーにあるカスタムの wnos.ini を使用する場合、Secure Gateway が SSL 確認パラメーターを送信することはありません。ご注意ください。

ブローカーアドレスをこの Secure Gateway に設定するように DHCP オプション 188 を構成する場合は、[テスト] ボタンをクリックしてこれを確認できます

Secure Gateway のセキュリティ

Secure Gateway へのユーザーアクセスを MAC アドレスに基づいて許可または拒否できます。これは、[RAS Secure Gateway のプロパティ] ダイアログの [セキュリティ] タブを使用して実行できます。

サイトのデフォルト値を使用

サイトのデフォルト設定を使用するには、[デフォルト設定を継承] オプションをクリックします。固有の設定を指定するには、オプションをクリアします。詳細については、「サイトのデフォルト値（ゲートウェイ）」（p. 91）を参照してください。

セキュリティの構成

許可または拒否する MAC アドレスのリストを構成するには、[セキュリティ] タブで次のいずれかのオプションを選択します。

- 以外を許可: このリストに含まれる MAC アドレスを除き、ネットワーク上のすべてのデバイスが Secure Gateway への接続を許可されます。[タスク] > [追加] をクリックし、デバイスを選択するか、MAC アドレスを指定します。
- のみを許可する: リストに含まれる MAC アドレスを持つデバイスのみが Secure Gateway への接続を許可されます。[タスク] > [追加] をクリックし、デバイスを選択するか、MAC アドレスを指定します。

Secure Gateway の MAC アドレスフィルタリングは ARP に基づいているため、フィルタリングが機能するには、クライアントとサーバーが同じネットワーク上にある必要があります。ネットワークの境界を超えて機能しません。

ウェブリクエストのロードバランス

注: [ウェブ] タブは、ゲートウェイモードが [通常] に設定されている場合にのみ使用できます。詳細については、「ゲートウェイモードと転送設定」（p. 91）を参照してください。

[ウェブ] タブでは、特定のシナリオでロードバランスに必要な設定を微調整できます。ここでウェブリクエストのリダイレクト URL とセッションの Cookie 名を指定して、クライアントとサーバー間のパーシスタンスを維持できます。

リダイレクト URL

元のウェブリクエストは、以下の 2 種類の方法のいずれかでゲートウェイに到達します。

- IP アドレスまたは FQDN を使用して、リクエストがローカルネットワーク経由で直接ゲートウェイに送信される。例: https://192.168.10.10。
- リクエストがファーム内でそのゲートウェイと他のゲートウェイとの負荷を分散する HALB デバイスに送信される。HALB デバイスは多くの場合インターネットに接続している（DMZ 内に位置している）ため、元のリクエスト URL 内ではその DNS 名を使用できる。たとえば、https://ras.msp.com のようになります。その後、HALB デバイスによってリクエストがゲートウェイに分配される。

ゲートウェイは、ウェブリクエストを受信すると、[ウェブ] タブで指定された URL を使用して、リダイレクトするようウェブブラウザーに返送します。

理論的には、ここにはどのような URL でも入力でき、元のウェブリクエストがその URL にリダイレクトされます。ただし、このフィールドの主要な目的はユーザーがウェブブラウザーからユーザーポータルに簡単にアクセスできるようにすることです。その仕組みを説明します。

1. ユーザーがロードバランサーの DNS 名をウェブブラウザーに入力します。たとえば、https://ras.msp.com のようになります。
2. ロードバランサーは、受信したリクエストを負荷の最も小さい RAS Secure Gateway に分配し、処理させます。
3. ゲートウェイは元の URL を受信し、その URL を [デフォルト URL] フィールドで指定された URL に置き換えます。以下の「デフォルトの URL フォーマット」サブセクションを参照してください。
4. 置換後の URL がウェブブラウザーに返送され、ブラウザーはその URL を使ってユーザーポータルのログインページを開きます。

デフォルトの URL フォーマット

デフォルトの URL フォーマットは以下のようになっています。

```
https://%hostname%/userportal
```

- 変数 `%hostname%` は、元のリクエストを受信したサーバーの名前に置き換えられます。この例ではロードバランサーの DNS 名になります。必要であれば、この変数を特定のホスト名や IP アドレス（このゲートウェイや別のゲートウェイなど）に置き換えることもできま

す。（例: `https://192.168.5.5/userportal`）。この方法では、常時ウェブリクエストが指定のホストに転送され、ユーザーポータルがそこで開かれます。ホストをハードコーディングしてしまうことはあまり実用的ではありませんが、そうすることは可能です。

- `userportal` は定数で、ユーザーポータルログインページへのパスになります。

この例では次の URL が、ウェブブラウザーからユーザーポータルへのアクセスに使用される最終的な URL になります。

```
https://ras.msp.com/userportal
```

実際のところ、ユーザーは最初から上記 URL を使うことも可能ですが、リダイレクト機能のおかげで、URL 全体を入力しなくても、サーバーの DNS 名（またはローカルネットワーク上の FQDN/IP アドレス）を入力するだけでアクセスできます。

特定のユーザーポータルのテーマを開く

ユーザーポータルのテーマは、ユーザーのグループに合わせてユーザーポータルのデザインや操作性をカスタマイズできる機能です。テーマの詳細については、「Parallels Web Client とユーザーポータル」（p. 454）を参照してください。

デフォルトのウェブリクエスト URL では、デフォルトのテーマが開きます。特定のテーマを開くようにするには、URL 末尾にテーマ名を追加します。

```
https://%hostname%/userportal/?theme=<theme-name>
```

の `<theme-name>` をテーマの名前に置き換えます。かっこや引用符は不要です。

ユーザーが特定のテーマを開く場合、ウェブブラウザーに入力する URL にテーマ名を含める必要があります。ただし、この場合は次のように非常にシンプルなフォーマットになります。

```
https://<server-name>/<theme-name>
```

上述のロードバランサー DNS 名を例にすると、次のような URL になります。

```
https://ras.msp.com/Theme-E1
```

詳細については、「テーマの構成 > URL」（p. 457）を参照してください。

ウェブ Cookie

ウェブ Cookie フィールドは、セッションの Cookie 名の指定に使用します。RAS Web Client セッションのパーシスタンスは、通常、ユーザーの IP アドレス（ソースアドレス指定）により設定されます。ソースアドレス指定が使用できない環境では（セキュリティポリシーで許可されない場合など）、セッション Cookie を使用して、クライアントとサーバーの間のパーシスタンスを維持できます。そのためには、パーシスタンスにセッション Cookie を使用できるロードバランサーを設定する必要があります。デフォルトの Cookie 名は ASP.NET_SessionId です。Amazon Web Services（AWS）またはその他のサードパーティ製のロードバランサーを使用している場合は、専用の Cookie 名を指定する必要があるかもしれません。詳細については、「ネットワークロードバランサーへのアクセス」（p. 100）を参照してください。

Secure Gateway のトンネリングポリシー

トンネリングポリシーを使用して、RD セッションホストのグループを特定の RAS Secure Gateway または RAS Secure Gateway IP アドレスに割り当てることで、接続を負荷分散することができます。

トンネリングポリシーを構成するには、[ファーム] > <サイト> > [Secure Gateway] に移動し、右ペインの [トンネリングポリシー] タブをクリックします。

<デフォルト> ポリシーは、事前構成済みのルールであり、常に最後のルールになります。これにより、未構成のすべての Secure Gateway IP アドレスが検出され、ファーム内のすべてのサーバー間でセッション負荷が分散されます。<デフォルト> ポリシーを構成するには、<デフォルト> ポリシーを右クリックし、コンテキストメニューで [プロパティ] をクリックします。

新しいトンネリングポリシーの追加

新しいポリシーを追加するには、次の手順を実行します。

1. [タスク] > [追加] をクリックします。
2. Secure Gateway の IP アドレスを選択します。
3. その Secure Gateway に接続しているユーザーをどの RD セッションホスト（複数可）に転送するかを指定します。[なし]（転送なし）を選択する場合は、下の「RDP アクセスの制限」セクションをお読みください。

トンネリングポリシーの管理

既存のトンネリングポリシーを変更するには、そのトンネリングポリシーを右クリックし、コンテキストメニューで [プロパティ] を選択します。

RDP アクセスの制限

トンネリングポリシーを使用して RAS Secure Gateway ポート経由の RDP アクセスを制限できます。そのためには、[トンネリングポリシー] タブの下部にある [なし] オプションを選択します（Parallels RAS の新規インストール時のデフォルト設定です）。これにより、ネイティブ MSTSC がそのポート（デフォルトポートは 80）経由でゲートウェイにアクセスするのを制限できます。結果として、MSTSC を使用して <IP アドレス>:80 へのアクセスを試行しても、拒否されます。Parallels Client からの RDP 接続についても同様です。

RDP アクセスを制限する、いくつかの理由があります。最初の理由は、ユーザーの RAS ファームへの接続を RDP ではなく Parallels RAS 接続のみに制限したい場合です。第 2 の理由は、*DDoS 攻撃を防止する*ためです。

DDoS 攻撃が発生中であることを示す一般的な兆候の 1 つは、特に理由もなくユーザーが RAS ファームにログインできなくなることです。これが発生した場合、Controller.log ファイル（RAS Connection Broker サーバー内の C:\ProgramData\Parallels\RASLogs にあります）を見ると、次のようなメッセージでいっぱいになっています。

- [I 06/0000003E] Mon May 22 10:37:00 2018 - Native RDP LB Connection from Public IP x.x.x.x, Private IP xxx.xxx.xx.xx, on Secure Gateway xxx.xxx.xx.xx, Using Default Rule
- [I 06/00000372] Mon May 22 10:37:00 2018 - CLIENT_IDLESERVER_REPLY UserName hello@DOMAIN, ClientName , AppName , PeerIP xxx.xxx.xx.xx, Secure GatewayIP xxx.xx.x.xx, Server , Direct , desktop 0
- [I 05/0000000E] Mon May 22 10:37:00 2018 - Maximum amount of sessions reached.
- [I 06/00000034] Mon May 22 10:37:00 2018 - Resource LB User 'hello' No Servers Available!
- [W 06/00000002] Mon May 22 10:37:00 2018 - Request for "" by User hello, Client , Address xxx.xxx.xx.xx, was not served error code 14.

これらのメッセージは、RDP ポートに対する DDoS 攻撃が進行中であることを示します。Secure Gateway のトンネリングポリシーによって RDP アクセスを制限することで、この状況の発生を防止できます。

ログの構成

RAS Secure Gateway は監視され、ログは関連情報を含めた状態で作成されます。ログを構成し、既存のログファイルを取得するかクリアする場合、ゲートウェイで右クリックし、コンテキストメニューで [トラブルシューティング] > [ロギング] を選択してから、希望に応じて [構成]、[取得] または [クリア] をクリックします。これらのタスクを実行する方法の詳細については、「ロギング」（p. 608）セクションを参照してください。

Secure Gateway のサマリとメトリクスの表示

すべての利用可能な RAS Secure Gateway の概要を 1 か所に表示するには、次の操作を実行します。

1. RAS Console で、[ファーム] カテゴリーを選択して、中央のペインで [サイト] ノードを選択します。
2. 利用できる RAS Secure Gateway は、右ペインの [ゲートウェイ] グループに表示されます。
3. Gateway のビュー/エディターに移動するには、サーバーを右クリックし、[エディターに表示] を選択します。

RAS Secure Gateway の詳細情報は、Parallels RAS Console で [情報] > [サイト] に移動することによっても表示できます。このページの情報には、OS のバージョン、RAS バージョン、ゲートウェイモードなどの一般情報、ならびに接続、セッション、キャッシュソケット、スレッドのさまざまな種類の情報が含まれています。

コンピューター管理ツールの使用

RAS Console から、RAS Secure Gateway をホスティングしているサーバーで標準的なコンピューター管理タスクを直接実行できます。このタスクには、リモートデスクトップ接続、PowerShell、コンピューター管理、サービス管理、イベントビューアー、IPconfig、再起動などが含まれます。[ツール] メニューにアクセスするには、サーバーを選択して [タスク] をクリック（または右クリック）し、[ツール] をクリックして目的のツールを選択します。要件と使用方法については、「コンピューター管理ツール」（p. 569）を参照してください。

第 7 章

RD セッションホスト

RD セッションホストは、Parallels RAS ファーム内に公開リソース（アプリケーション、デスクトップ、ドキュメントなど）をホストするために使用されます。この章では、RD セッションホストを追加、構成、管理する方法について説明します。

この章の内容

RD セッションホストタイプ

Parallels RAS v16.5 以降では、以下のタイプの RD セッションホストを作成して RAS ファームに追加できます。

- 個々のサーバー: これには、物理サーバーとして扱われる物理マシンまたは仮想マシンを使用できます。これらのタイプのサーバーを作成する方法については、「RD セッションホストを追加する」（p. 109）を参照してください。
- RAS 仮想デスクトップインフラストラクチャ（VDI）の一部である、テンプレートから作成された仮想マシン（VM）。VM を使用する主な利点は、単一の RAS テンプレートから必要な数の VM を作成できることです。これらのタイプのサーバーを作成する方法については、「テンプレートベースの RD セッションホストを追加する」（p. 114）を参照してください。

テンプレートが RAS VDI の一部であることを考慮すると、テンプレートに基づく RD セッションホストの作成、プロビジョニング、管理には、通常の RD セッションホスト（個別サーバ

ー）とは異なる面があります。これらのセクションを読むとき、特定の機能がテンプレートに基づく RD セッションホストにも当てはまるかどうかに注意してください。

RD セッションホストを追加

RD セッションホスト要件

RD セッションホストには、リモートデスクトップサービス（RDS）役割がインストールされている必要があります。本セクションで後述されているように、RAS Console から RDS をインストールできます。

RAS RD セッションホスト Agent をサーバーにプッシュインストールするには、次の要件を満たす必要があります。

- サーバーにファイヤーウォールを構成してプッシュインストールを許可する必要があります。標準の SMB ポート（139 および 445）が開いている必要があります。Parallels RAS が使用するポート一覧については、「ポート参照」を参照してください。
- SMB アクセス。管理共有（\\server\c$）にアクセスできる必要があります。シンプルファイル共有が有効になっている必要があります。
- Parallels RAS 管理者アカウントにはサーバーでリモートインストールを実行する権限が必要です。権限がない場合、権限があるアカウントの資格情報を入力するよう求められます。
- RD セッションホストは AD ドメインへの参加が必要です。参加しない場合、プッシュインストールは機能しないかもしれず、その場合、Agent をサーバーに手動でインストールする必要があります。詳細については、「手動による Agent のインストール」セクションを参照してください（p. 112）。

注: このセクションの残りは、通常の RD セッションホストのみに適用されます。テンプレートに基づく RD セッションホストを追加する方法に関する情報を探している場合は、「テンプレートベースの RD セッションホストの追加」（p. 114）を参照してください。

RD セッションホストを追加

RD セッションホストをサイトに追加するには、次の操作を実行します。

1 RAS Console で、[ファーム] > [サイト] > [RD セッションホスト] に移動します。

2 [タスク] > [追加] をクリックします。[RD セッションホストを追加] ウィザードが開きます。「基本的な Parallels RAS ファームを設定する」(p. 41) で説明したように、[開始] カテゴリーからウィザードを開くこともできます。

3 [タスク] メニューをクリック（または [+] アイコンをクリック）し、次のいずれかを選択します。

- Active Directory から追加する: Active Directory から RD セッションホストを追加します。
- 手動で追加する: RD セッションホストの FQDN または IP アドレスを入力し、追加します。

サーバー名（ホスト名または FQDN）を入力すると、他の RAS コンポーネントやクライアントからそのサーバーに接続する主要な方法として使用されることに注意してください。IP アドレスを入力すると、自動的に FQDN に解決されます。ただし、FQDN に解決するグローバルオプションが有効な場合に限ります。このグローバルオプションの現在の設定を確認するには、メインメニューの [ツール] > [オプション] をクリックします。[オプション] ダイアログで、[ホストを追加する場合は、常に完全修飾ドメイン名（FQDN）で解決するよう試みてください] オプションを確認します。このオプションが選択されている場合、その RAS ファーム内のすべてのサーバー/コンポーネントの IP アドレスは、常時 FQDN に解決されます。このオプションの選択を解除すると、サーバーとの通信にはサーバーに指定した内容（IP アドレスまたは名前）がそのまま使用されます。サーバーがクラウド内にホストされている場合のように、IP アドレスではサーバーにアクセスできない場合の展開では、この機能が役立ちます。詳細については、「ホスト名の解決」(p. 568) を参照してください。

4 [次へ] をクリックします。

5 次のページで、以下のオプションを指定します。

- ファイアウォールルールを追加: サーバー上で実行されている Windows で Parallels RAS が必要とするファイアウォールルールを追加します。詳細については、「ポート参照」を参照してください。
- RDS 役割をインストール: インストールされていない場合は、RDS 役割をサーバーにインストールします。このオプションは常に選択する必要があります。
- デスクトップエクスペリエンスを有効にする: サーバー上で実行されている Windows でデスクトップエクスペリエンス機能を有効にします。このオプションは、[RDS 役割をインストール] オプション（上記）が選択されている場合のみ有効です。このオプションは、デスクトップエクスペリエンス機能がデフォルトで有効にされていない、Windows Server 2008 R2 および Windows 2012 R1/R2 に適用されます。

- 必要な場合にサーバーを再起動: 必要な場合にサーバーを自動的に再起動します。必要に応じて、手動でサーバーを再起動することもできます。
- ホストプールへサーバーを追加します。サーバー（1 台または複数）をホストプールに追加します。このオプションの下にあるリストボックスで希望するホストプールを選択します。どのホストプールを選択したらよいかわからない場合は、[既定のホストプール] を選択してください。ホストプールについて詳しくは、「ホストプール（RD セッションホスト）の管理」（p. 115）セクションで説明します。

6 [次へ] をクリックします。

7 サーバー（1 台または複数）をホストプールに追加します。必要なホストプールを選択するか、新しいホストプールを作成します。どのホストプールを選択したらよいかわからない場合は、[既定のホストプール] を選択してください。ホストプールについて詳しくは、「ホストプール（RD セッションホスト）の管理」（p. 115）セクションで説明します。

8 [次へ] をクリックします。

9 次のページでは、サーバー上で実行されている Windows でリモートデスクトップユーザーグループにユーザーとグループを追加できます。これは、Parallels RAS ユーザーが RD セッションホストでホストされている公開済みのリソースにアクセスするために必要です。ユーザーやグループを指定するには、表示されているオプションを選択し、[+] アイコンをクリックします。[ユーザーまたはグループを選択] ダイアログで、ユーザーまたはグループを指定して、[OK] をクリックします。選択されたユーザー/グループがウィザードページのリストに追加されます。

> **注:** このステップをスキップし、ユーザーが RD セッションホストでリモートデスクトップユーザーグループのメンバーではない場合は、公開されたリソースにアクセスできません。Windows 標準のツールを使って、ユーザーを [リモートデスクトップユーザー] グループに追加したことがある（または後で使いたい）場合、このページはスキップしてください。

10 [次へ] をクリックします。

11 [ユーザープロファイル] ページでは、ユーザープロファイルを管理するためのテクノロジーを選択できます。ユーザープロファイルディスクまたは FSlogix のいずれかを選択できます。ユーザープロファイルディスクは、専用のファイル共有にユーザーアプリケーションデータを保存する仮想ハードディスクです。Microsoft FSLogix プロファイルコンテナーは、ローミングプロファイルおよびユーザープロファイルディスク（UPD）の後継技術として利用されることの多いプロファイル管理ソリューションです。これは、パーシスタントでない環境でユーザーコンテキストを維持し、サインイン時間を最小限に抑え、互換性の問題を排除するネイティブプロファイルのユーザーエクスペリエンスを提供できるように構成されています。詳細な手順については、「ユーザープロファイル」（p. 138）を参照してください。

12 [最適化] ページでは、Parallels RAS 環境での最高のパフォーマンスを実現するために使用される、RD セッションホストにおける Windows システムの最適化設定を指定できます。無効化、削除、または最適化の対象となる Windows コンポーネントやサービス、またその他のオプションを選択して、仮想アプリおよびデスクトップの配信の効率性と合理性を向上させ、改善することができます。詳細な手順については、「最適化」（p. 146）を参照してください。

13 次のページで、設定を確認して、[次へ] をクリックします。

14 [RAS RD セッションホスト Agent をインストール] ダイアログが開きます。指示に従って、Agent をインストールします。インストールが完了したら、[完了] をクリックしてダイアログを閉じます。

15 ウィザードに戻り、[完了] をクリックしてウィザードを閉じます。

RD セッションホストがファームに追加されていることを確認するには、[ファーム] カテゴリー（Parallels RAS Console ウィンドウの左ペインの [開始] カテゴリーの下）をクリックし、ナビゲーションツリー（中央のペイン）で [RD セッションホスト] をクリックします。サーバーは、[RD セッションホスト] リストに表示されています。[ステータス] 列に、警告メッセージが表示されることがあります。警告メッセージが表示された場合は、サーバーを再起動します。[ステータス] 列に、”OK”と表示されている場合、RD セッションホストは正常に機能しています。

次に、RD セッションホストからアプリケーションを公開する方法（p. 49）について説明します。

手動による Agent のインストール

自動でプッシュインストールを実行できない場合は、RAS RD セッションホスト Agent を手動でインストールしなければならないことがあります。たとえば、SMB 共有を利用できない場合や、ファイアウォールルールによってプッシュインストールができない場合があります。

手動での RAS RD セッションホスト Agent のインストール

1 管理者アカウントを使用して RAS RD セッションホスト Agent のインストール先のサーバーにログインし、他のすべてのアプリケーションを閉じます。

2 Parallels RAS のインストールファイル（`RASInstaller.msi`）をサーバーにコピーし、そのファイルをダブルクリックして、インストールを開始します。

3 画面の指示に従って、インストールタイプのページに進みます。[カスタム] を選択し、[次へ] をクリックします。

4 [RAS RD セッションホスト Agent] をクリックし、ドロップダウンリストから [このコンピューターのローカルディスクにすべての機能をインストールします] を選択します。

5 他のすべてのコンポーネントが選択解除されていることを確認し、[次へ] をクリックします。

6 [インストール] をクリックしてインストールを開始します。

7 インストールが終了したら、[完了] をクリックします。

RAS RD セッションホスト Agent は構成を必要としません。エージェントがインストールされたら、RAS Console でサーバー名をハイライトし、[タスク] ドロップダウンリストで [トラブルシューティング] > [エージェントを確認] をクリックして、サーバーのステータスを更新します。

RAS RD セッションホスト Agent のアンインストール

サーバーから RAS RD セッションホスト Agent をアンインストールするには、次の操作を実行します。

1 スタートボタン > [コントロールパネル] > [プログラム] > [プログラムのアンインストール] に移動します。

2 インストールされているプログラムのリストから、[Parallels Remote Application Server] を見つけます。

3 サーバー上に保持する必要がある他の Parallels RAS コンポーネントがない場合、[Parallels Remote Application Server] を右クリックして [アンインストール] をクリックします。手順に従って、プログラムをアンインストールします。以下の手順は省略できます。

4 サーバー上に保持する必要がある他の RAS コンポーネントがある場合、[Parallels Remote Application Server] を右クリックして [変更] をクリックします。

5 [ようこそ] ページで、[次へ] をクリックします。

6 [変更、修復、または削除] ページで [変更] を選択します。

7 次のページで [カスタム] を選択します。

8 [RAS RD セッションホスト Agent] を選択し、その前にあるドロップダウンリストをクリックして、[すべての機能が利用できなくなります] をクリックします。

9 [次へ] をクリックして、ウィザードを完了します。

テンプレートベースの RD セッションホストを追加

テンプレートベースの RD セッションホストは、ハイパーバイザーやクラウドベースのプロバイダー上で動作する仮想マシンのクローンです。テンプレートの作成時には、オペレーティングシステムとアプリケーションがすでにインストールされた、事前構成済みの VM を選択します。その後、個々のホスト（VM）がテンプレートの複製として作成されます。複製は事前に作成することも必要に応じて作成する（テンプレートを作成するときに構成する）こともできます。この機能により、仮想マシンで動作している RD セッションホストを作成および構成し、必要に応じた数のコピーを作成できます。

テンプレートベースの RD セッションホストをサイトに追加するには、次の操作を実行します。

1 「RD セッションホストテンプレートの作成」（p. 122）の説明に従って、テンプレートを作成します。

2 「ホストプールへのテンプレートの割り当て」（p. 123）の説明に従って、テンプレートをホストプールに割り当てます。

3 個々の RD セッションホストをホストプールに追加します。次のいずれかを実行します。

- RD セッションホストを手動で追加する場合は、ホストプールのプロパティで [サーバー] タブを選択し、[タスク] > [追加] をクリック（または [+] アイコンをクリック）します。開いたダイアログで、作成する RD セッションホストの数を選択し、[OK] をクリックします。
- 特定の条件が満たされたときに Parallels RAS に RD セッションホストを自動追加させたい場合は、「ホストプール（RD セッションホスト）の管理」（p. 115）の説明に従って自動スケーリングを構成してください。

RD セッションホストの管理

このセクションでは、Parallels RAS で RD セッションホストコンポーネントを管理する方法を説明します。

ホストプール（RD セッションホスト）の管理

Parallels RAS でリソースを公開するとき、リソースをホストする 1 つまたは複数のサーバーを指定する必要があります。ホストプールは、複数の RD セッションホストを組み合わせ、個々のサーバーを指定する代わりに、ホストプールからリソースを公開できます。

RD セッションホストのホストプールを使用する主な利点は次の通りです。

- 公開済みリソースの管理を簡素化できます。
- テンプレートから作成される RD セッションホストを使用できます。これについてはこのセクションの後半で詳しく説明します。

各 RD セッションホストはホストプールに所属している必要があります。Parallels RAS には、使用可能なホストプール名、<Default> が組み込まれています。1 つの RD セッションホストは 1 つのホストプールのメンバーにしかなれないことに注意してください。同じサーバーを複数のホストプールに追加することはできません。

RD セッションホストをサイト別のホストプールに移動する

RD セッションホストをあるホストプールから別のホストプールへ移動するには、次の操作を実行します。

1. RAS Console で、[ファーム] > <サイト> > [RD セッションホスト] に移動します。
2. RD セッションホストを選択します。
3. [タスク] > [ホストプールに割り当て] をクリックするか、RD セッションホストを右クリックして、コンテキストメニューから [ホストプールに割り当て] を選択します。
4. [ホストプールに割り当て] ダイアログで、任意のホストプールを選択します。

注: 新しいホストプールの設定が、RD セッションホストに適用されます。

自動スケール

ホストプールのプロパティにある [自動スケール] タブの設定により、指定されたテンプレートからどのように RD セッションホストを作成するかを指定します。設定について、以下で説明します。

テンプレート: ホストプールに割り当てられたテンプレートを指定します。

自動スケールの有効化: 自動スケールを有効化します。

構成: 以下の自動スケールの設定を構成します。

- テンプレートからホストプールに追加する最小ホスト数: テンプレートがホストプールに割り当てられたときに、自動的にホストプールに追加されるサーバーの最小数を指定します。利用状況に関わらず、この台数のサーバーがホストプール内に残ります。
- テンプレートからホストプールに追加する最大ホスト数: このオプションでは、合計何台のサーバーをテンプレートからホストプールに追加できるかの上限を設定できます。テンプレートはホストプール間で共有できます。各ホストプールに上限を設定することで、各ホストプールのサーバー数の合計がテンプレートの制限を超えないようにします。次の例を考えてみましょう。
  - テンプレートが 1 つのホストプールに使用されている場合、この数字を最大でテンプレートの [ホスト数の上限] 設定の数にできます。
  - 2 つ以上のホストプールが同じテンプレートを共有する場合、すべてのホストプールの合計がテンプレートの [ホスト数の上限] 設定以下であることが必要です。

  ホストプールを保存するとき、他のホストプール（存在する場合）に対して検証が実行され、数が一致しない場合はエラーメッセージが表示されます。エラーのためにサーバーを作成できないときは、“テンプレートエラー”イベントがトリガーされ、管理者はアラートメッセージを受信します。
- ワークロードが（%）を超えた場合、新規ホストを追加するか、既存ホストの電源を投入します: ワークロードのしきい値をパーセントで指定します。実際のワークロードがこの値を超えると、1 つまたは複数の新しいサーバーが作成され、ホストプールに追加されます（まだ利用できない場合）。ホストプールワークロードの割合は、次の式を使用して計算されます。

  ホストプールワークロード =（現在のセッション数/最大セッション数） x 100

  上の式で、
  - 現在のセッション数は、ホストプール内にある全サーバーの全セッションの合計です。これには、静的（スタンドアロン）サーバーとテンプレートから作成されたサーバー（ホストプール）が含まれます。無効化されているサーバー、空になっているサーバー、または Agent のステータスが [未確認] であるサーバーは、計算に含まれないことに注意してください。
  - [セッション最大数] は、[Agent 設定] タブで指定する設定で（サイトのデフォルト値から継承されるか、このホストプールで上書きされます）、ホストプールに許可されるセッションの最大数です。

次の例を考えてみましょう。

RAS ホストプール 1 - 混合サーバータイプ（静的とホストプール）、異なる Agent のステータスは

- [RDSH-1]、ステータスは[OK]、最大セッション数は 10、現在のセッション数は 2、タイプは静的
- [RDSH-2]、ステータスは[無効]、最大セッション数は 20、現在のセッション数は 0、タイプは静的
- [RDSH-3]、ステータスは[OK]、最大セッション数は 10、現在のセッション数は 4、タイプはホスト
- [RDSH-4]、ステータスは[ドレインモード]、最大セッション数は 10、現在のセッション数は 3、タイプはホスト

上記のホストプールのワークロードは、（現在のセッション数/セッション最大数） x 100 または（（2 + 4）/20） x 100 = 30% として計算されます。

サーバー RDSH-2 と RDSH-4 については、前者は Agent が無効にされていて、後者はドレインモードになっているため、ワークロードに含まれていません。

RAS ホストプール 2 - 混合サーバータイプ（静的とホストプール）、異なる Agent のステータスは

- [RDSH-1]、ステータスは[OK]、最大セッション数は 10、現在のセッション数は 0、タイプはホスト
- [RDSH-2]、ステータスは[OK]、最大セッション数は 10、現在のセッション数は 2、タイプはホスト
- [RDSH-3]、ステータスは[未確認]、最大セッション数は 10、現在のセッション数は 0、タイプはホスト

ホストプールワークロード = （現在のセッション数/最大セッション数） x 100 または（（0 + 2） / 20） x 100 = 10%

ホストプールは、ワークロードが 0% の場合でも、少なくとも 1 台のサーバーが利用できることを常に確認することに注意してください。

- リクエストごとにホストプールに追加するホストの数: ワークロードがこのしきい値を超えたときに作成するサーバーの数を指定します。この設定は、上述の [ワークロードが（%）を超過したらテンプレートからサーバーを追加] 設定と連動します。追加サーバーの作成リクエストがホストプールからテンプレートに送信されると、ここで指定された値によって作成されるサーバーの数が決定されます。

- ワークロードが（%）を下回った場合、ホストプールのホストを空にして電源を切断します: ワークロードのしきい値をパーセントで指定します。実際のワークロードがこの値を下回り、“ワークロードはこのレベル以下にとどまる”フィールドで指定した期間、その状態が続いた場合、過剰なホストは、ドレインモードに変更されるか、電源が遮断されます。期間はドロップダウンリストから選択するか、“週”、“日”、“時間”、“分”、“秒”を単位として使用し、独自の整数値を入力することができます。セッション数が最も少ないサーバーがドレインモードに切り替えられます。すべてのユーザーがサーバーからログオフするとすぐ、ホストプールから割り当て解除されます。その時点で、そのサーバーはオンデマンドで他のホストプールが利用できるようになります。
- ホストを空にして電源を切断してから、ホストプールのホストを削除します: ホストプールから切り離され、電源がオフになったホストを削除するかどうかを指定します。

ヒント: サーバーは、そのサーバー上のすべてのユーザーセッションがログオフされたときにのみ、ホストプールから割り当て解除されます。アイドル状態、アクティブ状態、切断状態など、ユーザーセッションが引き続き存在している場合、自動スケールによるユーザーセッションのログオフは実行されず、ホストプールからのサーバー割り当ては解除されません。

注: Parallels では、ドレインモードを効果的にするために、Windows のホストプールポリシーまたは [サイトのデフォルト値のプロパティ] ダイアログで、アイドル時間と切断されたセッションに実行可能なタイムアウトを設定することをお勧めします。GPO を使用してユーザーセッションを強制的にログオフすることができますが、データの損失が発生する可能性があるため、慎重に使用する必要があります。

ホストプールのデフォルト値を使用する

ホストプールに割り当てられている RD セッションホストには、ホストプールのデフォルト値から継承される様々な設定があります。これにより、各サーバーを個別に構成するのではなく、すべてのサーバーの設定を単一のセットを使用して簡単に構成できます。サイトには、独自のデフォルト設定もあります（サイトのデフォルト値）。さらに、RD セッションホストのホストプールは、これらのサイトのデフォルト値を継承できます。このため、デフォルトの設定を RD セッションホストに継承させる際には、次のような選択肢があります。

- サイトのデフォルト値を構成し、ホストプールにこれらの設定を継承させます。ホストプールに割り当てられている RD セッションホストもサイトのデフォルト値を継承します。新しいホストプールでは、これがデフォルトのシナリオです。サイトのデフォルト値は、[ファーム] > <サイト> > [RD セッションホスト] へ移動し、[タスク] > [サイトのデフォルト値] をクリックすることにより構成できます。

- 対象のホストプールのデフォルト設定を構成します。この方法によって、それぞれが独自にホストプールのデフォルト値（サイトのデフォルト値とは異なる）を持つ、複数のホストプールを設定できます。ホストプールに割り当てられるサーバーは、ホストプールのデフォルト値を継承します。

ホストプールに対してデフォルト設定を構成するには、[ホストプールプロパティ] ダイアログ（[タスク] > [プロパティ]）を開いて、希望のタブ（デフォルト値のない [全般] タブ以外）を選択し、[デフォルト設定を継承] オプションを選択するかクリアします。オプションをクリアすると、独自のデフォルト値を指定できます。このホストプールに割り当てられている（か割り当てられる予定の）全サーバーが、これらの設定を継承します。継承は、[ホストプールプロパティ] ダイアログのそれぞれの個別タブに対して、独立して機能しますので注意してください。

RD セッションホストに対してデフォルト設定を構成する方法の詳細については、「RD セッションホストプロパティの表示と変更」（p. 130）を参照してください。

ホストプール（RD セッションホスト）を追加

ホストプールの作成

RD セッションホストのホストプールを作成するには、次の操作を実行します。

1. RAS Console で、[ファーム] > <サイト> > [RD セッションホストのホストプール] に移動します。
2. [タスク] > [追加] をクリックします（または [+] アイコンをクリックします）。
3. [サイト内のホストプールを有効化] を選択してホストプールを有効化します。新しいホストプールの名前と説明を指定します。
4. [次へ] をクリックします。
5. [プロビジョニング] ページで、このホストプールにテンプレートベースのホストを含めるか、スタンドアロンホストを含めるかを選択します。
   - テンプレート: （テンプレートベースの RD セッションホストのみ）ホストはテンプレートから動的に作成されます。次のステップ以降で、テンプレートを作成するか、既存のテンプレートを選択する必要があります。プロビジョニングタイプとして [テンプレート] を選択すると、均質なホストプールが確保されます。ホストプール全体で一貫したユーザーエクスペリエンスを提供するには、この選択を推奨します。テンプレートベースの RD セッションホストの作成については、「テンプレートベースの RD セッションホストを追加する」（p. 114）を参照してください。

- スタンドアロン: （テンプレートベースおよびスタンドアロンの RD セッションホスト）すでに存在する 1 つまたは複数のホストを選択します。これは、次のステップ、または後のステップでも行うことができます。ホストプールにホストを追加する前に、ホストがドメインに参加し、ドメイン環境のネットワークにアクセスできることを確認してください。スタンドアロンプロビジョニングは、自動スケールなど、機能の一部が欠けているため、「管理対象外」とみなされることに注意してください。

6 [次へ] をクリックします。

7 プロビジョニングページ（前述）での選択内容に応じて、以下のいずれかを実行します。

- スタンドアロン: リストからホストプールに含めるホストを 1 つまたは複数選択します（後からプールにホストを追加することもできます）。
- テンプレート: リストからテンプレートを選択するか、[新規作成] をクリックして新しいテンプレートを作成してからテンプレートの設定を指定します。バージョン: 既存のテンプレートを選択した場合は、そのバージョンのいずれかを選択します。自動スケールの有効化: （マルチセッションホスト）自動スケーリングを有効化して構成します。

8 [次へ] をクリックします。

9 （テンプレートのみ）[全般] ページで、次のオプションを指定します。

- テンプレート名: 選択してテンプレート名を入力します。
- 最大ホスト数: このテンプレートから作成できるホストの最大数を指定します。
- ウィザード完了時にデプロイされるホスト数: テンプレートが作成されたときに展開するホストの数。ホストは一度に 1 つずつ作成されるため、これには時間がかかることに注意してください。
- ホスト名: 新しいホスト名を指定するときに使用するパターン。

10 [次へ] をクリックします。

11 （テンプレートのみ）[追加のプロパティ] ページで、次のオプションを指定します。

- 使用可能なバッファを維持: このテンプレート用に、常に未割り当てでセッションが空いているホストの最小数です。空いているデスクトップと未割り当てのデスクトップの数が設定値を下回るとすぐに、このテンプレートから別のホストを強制的に作成します。テンプレートは、電源の初期状態を含め、ホスト作成のための独自の設定を使用します。
- 準備後のホストの状態: 準備が整ったホストに適用される電源状態を選択します。[使用中]、[停止中]、または [サスペンド] から選択します。電源状態が [停止中] または [サスペンド] に設定されている場合、実行中の（完全に準備が整い、受信接続を待っている）

ホストの数は、[使用可能なバッファを維持] の設定（上記参照）によって制御されます。ホスト数の上限値が 200 に設定され、ウィザード完了時に展開されるゲストホストの数が 100 で、準備後の電源状態が“停止中”であるとします。このような構成の場合、100 の複製が展開され、停止中の状態になります。

- 未使用のホストの削除: リソースを節約するため、未使用のホストを処理する方法を選択します。削除しないように設定するか、削除されるまでの時間を指定します。

12 [次へ] をクリックします。

13 [ユーザープロファイル] ページで、[RAS で管理しない]（ユーザープロファイルは管理されません）または [FSlogix] から選択できます。Microsoft FSLogix プロファイルコンテナーを使用すると、パーシスタントでない環境でユーザーコンテキストを維持し、サインイン時間を最小限に抑え、互換性の問題を排除するネイティブプロファイルのユーザーエクスペリエンスを提供できるように構成されています。詳細な手順については、「ユーザープロファイル」（p. 138）を参照してください。

14 [次へ] をクリックします。

15 [概要] ページでは、テンプレートの概要情報を確認します。必要に応じて、[戻る] ボタンをクリックして情報を修正できます。

16 最後に、[完了] をクリックしてホストプールを作成し、ウィザードを閉じます。

ホストプールを作成し、後でそこからリソースを公開した後、ホストプールを右クリックし、[公開済みのリソースを表示] を選択（または [タスク] > [公開済みのリソースを表示] をクリック）して、リソースの一覧を表示できます。詳細については「RD セッションホストでホストされている公開済みリソースの表示」（p. 162）を参照してください。

テンプレート（RD セッションホスト）の管理

RD セッションホストテンプレートは、特に、仮想マシンで実行されている RD セッションホストを複製できるように設計されています。RD セッションホストテンプレートから作成されたホストは、Parallels RAS によりほぼ通常の RD セッションホストのように扱われます。主な違いは、1 つのテンプレートからホストを必要なだけいくつでも作成でき、必要に応じて RD セッションホストのプロビジョニングを自動化できることです。

RD セッションホストテンプレートは、次の VDI プラットフォームでサポートされています。

- Microsoft Hyper-V
- Microsoft Hyper-V Failover Cluster
- VMware VCenter

- VMware ESXi
- SC//HyperCore
- Nutanix AHV（AOS）
- Microsoft Azure
- Amazon ウェブサービス

RD セッションホストテンプレートは、Windows Server 2008 R2 から Windows Server 2022 までをゲスト OS としてサポートします。通常の RD セッションホスト（p. 108）とは異なり、RD セッションホストテンプレートから作成されたサーバーでは、これより古いバージョンの Windows Server はサポートされません。理由は、これらのサーバーは VM で動作し、RAS Guest Agent がインストールされている必要があるため、ゲスト OS 要件が RAS Guest Agent にサポートされる Windows Server バージョンに制限される、というものです。

RD セッションホストテンプレートを使用した場合は、次の RAS VDI の標準機能を使用できません。

- プール管理
- パーシスタントなホスト
- セッション管理
- 特定のテンプレートから公開
- その他の RAS VDI 固有の機能。

テンプレートから作成された RD セッションホストをプロビジョニングする方法の詳細については、「ホストプール（RD セッションホスト）の管理」（p. 115）を参照してください。

RD セッションホストテンプレートを作成する

要件

このセクションで説明する作業を実行するには、次の要件を満たす必要があります。

- 「VM テンプレートの作成」（p. 194）の「要件」サブセクションで説明されている要件です。
- Network Discovery UDP ポート 137 をゲスト OS のドメインファイアウォールプロファイルで有効にする必要があります。これは、ドメイングループポリシーにより、またはゲスト OS で手動で実行できます。

手動でエージェントをインストール

通常、Parallels RAS Console から直接ソース VM で必要な Agent ソフトウェアをプッシュインストールします。ただし、VM の Windows で Parallels RAS インストーラーを実行して手動でソフトウェアをインストールすることもできます。その際、Custom インストールオプションを使用し、ソース VM にインストールするエージェントコンポーネントとして、RAS Guest Agent と RAS RD セッションホスト Agent を選択します。

テンプレートの作成

RD セッションホストテンプレートを作成するには、次の操作を実行します。

1. 「プロバイダーの追加」（p. 165）で説明されているように、サポートされているプロバイダーのいずれかを追加します。
2. [ファーム] > [サイト] > [RD セッションホスト] > [テンプレート] タブに移動します。
3. [タスク] ドロップダウンメニューで [追加] をクリックします（または [+] アイコンをクリックします）
4. ダイアログが開いたら、テンプレートの作成元になるホストを選択し、[OK] をクリックします。
5. [Parallels テンプレートウィザードを作成] が開きます。各ウィザードページは、画面に表示される順序に従って、下で説明されています。
6. エージェントがインストールされていることを確認し、必要であれば手順 1: の説明に従って手動でインストールします。Agent のチェックとインストール（p. 196）。この手順は、オンプレミスのプロバイダーを使用する場合にのみ表示されます。
7. 手順 2: の説明に従ってテンプレートを構成します。「テンプレートの構成」（p. 197）に進みます。

ホストプール（RD セッションホスト）へのテンプレートの割り当て

RD セッションホストのホストプールを作成する際、ホストプールにテンプレートを割り当てることができます。これは、ホストプールを作成または変更する際に行うか、[テンプレート] タブから行うことができます。

ホストプールにテンプレートを割り当てるには:

1 [ファーム] > [サイト] > [RD セッションホスト] > [テンプレート] タブに移動します。

2 [テンプレート] タブで、テンプレートを選択します。

3 [タスク] > [ホストプールに割り当て] をクリックします。

4 [バージョン] ダイアログで、テンプレートのバージョンを選択します。

5 既存の RD セッションホストのホストプールの一覧を表示するダイアログが開きます。すでにテンプレートが割り当てられているホストプールは、デフォルトではこのリストに表示されません。これらを表示するには、[テンプレートが割り当てられたホストプールを表示する] オプションを選択します。現在使用しているテンプレートが [テンプレート] 列に表示されます。

6 1 つまたは複数のホストプールを選択し、 [OK] をクリックします。

ホストプールからテンプレートを削除するには:

1 テンプレートを選択し、[タスク] > [ホストプールから削除] をクリックします。

2 このテンプレートが割り当てられているすべてのホストプールを一覧表示するダイアログが開きます。

3 テンプレートを削除するホストプールを選択し、[OK] をクリックします。

なお、ホストプールに、削除するテンプレートから作成されたホストがある場合は、それらも削除されます。本当に削除するかどうかを確認するメッセージが表示されます。

テンプレートに基づく RD セッションホストの管理

特定のテンプレートに基づく RD セッションホストの表示

特定のテンプレートに基づく RD セッションホストのリストを表示するには、次の操作を実行します。

1 [ファーム] > [サイト] > [RD セッションホスト] > [テンプレート] に移動します。

2 テンプレートを選択し、[タスク] > [サーバーを表示] をクリックします。

サイトの既定値

テンプレートに基づく RD セッションホストは、テンプレートの設定を引き継ぎます。設定を表示するには、RD セッションホストがどのテンプレートをベースとしているかをメモしてか

ら、そのテンプレートのプロパティを表示します。具体的には、[設定] と [セキュリティ] のタブを確認します。詳細については、「サイトのデフォルト値」(p. 228) を参照してください。テンプレートでは、サイトのデフォルト設定を継承することも、カスタム設定を指定することもできます。

RAS Guest Agent のステータスの確認

テンプレートに基づくゲスト RD セッションホストには、RAS Guest Agent をインストールする必要があり、Agent は Parallels RAS のバージョンと適合している必要があります。テンプレートから RD セッションホストを作成すると、Agent がデフォルトでインストールされます。ネイティブのハイパーバイザーツールを使用して RD セッションホストが作成されている場合は、Agent がインストールされていない可能性があります。この場合、RD セッションホストはリモートデスクトップに対してのみサービスを提供します。サーバーアプリケーションやドキュメントに対するサービスを有効にするには、Agent をご自身でインストールする必要があります。

RAS Guest Agent がインストールされているかどうか、そしてそれが最新であるかどうかをチェックするには、次の操作を実行します。

1 [ファーム] > <サイト> > [RD セッションホスト] > [RD セッションホスト] に移動します。

2 「ホストの管理」(p. 216) のサブセクション、「RAS Guest Agent のステータスの確認」の説明に従って続行します。

RD セッションホストテンプレートには、RAS RD セッションホスト Agent もインストールされている必要があります。

RAS RD セッションホスト Agent がインストールされているかどうか、そしてそれが最新であるかどうかをチェックするには、次の操作を実行します。

1 [ファーム] > [サイト] > [RD セッションホスト] > [テンプレート] に移動します。

2 リストでテンプレートを選択し、[タスク] > [トラブルシューティング] > [Agent をチェック] をクリックします。

テンプレートに基づく RD セッションホストの削除

「ホストの管理」(p. 216) のサブセクション、「ホストの削除」を参照してください。

準備に失敗したテンプレートに基づく RD セッションホストの管理

「ホストの管理」(p. 216)のサブセクション、「準備に失敗したホストの管理」を参照してください。RD セッションホストの場合、[ファーム] > <サイト> > [RD セッションホスト] > [RD セッションホスト] から、[タスク] > [サイトのデフォルト値] をクリックして、サイトのデフォルト値を表示する必要があることに注意してください。

テンプレートに基づく RD セッションホストの再作成

テンプレートに基づく RD セッションホストに問題が発生し、使用不能になった場合、削除して新しいゲスト VM を作成する必要はありません。その代わり、名前、MAC アドレス、その他のプロパティを保持したまま再作成することができます。このようにすれば、サイト設定が破損した RD セッションホストに依存していた場合でも、他のサイト設定は影響を受けません。RD セッションホストを再作成するもう 1 つの理由は、(再作成コマンドを実行せずにメンテナンスを終了するときに)テンプレートに加えられた変更を適用するためです。

なお、再作成された RD セッションホストでは、以下のプロパティが保持されます:

- MAC アドレスは、ESXi、vCenter、Hyper-v、Hyper-v Failover Cluster、Nutanix AHV(AOS)、SC//HyperCore で保持されます。
- BIOS の UUID は、ESXi と vCenter で保持されます。
- DRS グループは vCenter で保持されます。

注: RD セッションホストがテンプレートに基づいて作成され、すでに RD セッションホストのホストプールに割り当てられている場合は、再作成できません。

ゲスト RD セッションホストを 1 つまたは複数作成するには、次の操作を実行します。

1. Parallels RAS Console で、[ファーム] / <サイト> / [RD セッションホスト] > [テンプレート] に移動します。
2. 展開済みの RD セッションホストをすべて再作成するには、[タスク] ドロップダウンリストをクリックして、[すべてのサーバーを再作成] を選択します。
3. 特定のホスト(または複数のホスト)を再作成するには、[タスク] > [サーバーを表示] をクリックします。RD セッションホストの一覧を表示するダイアログが表示されます。1 つまたは複数の RD セッションホストを選択してから、[タスク] > [再作成] をクリックします。

テンプレートに基づく RD セッションホストを再作成するには、次の操作を実行します。

- この手順により RD セッションホストが削除され、同じテンプレートから新しい RD セッションホストが作成されます。
- 新しい RD セッションホストでは、置き換える対象と同じコンピューター名が保持されます。
- RD セッションホストが実行中である場合、そのメモリーの中にある保存されていないすべてのデータが失われます。そのため、重要なデータは外部ストレージに保存する必要があります。

ホスト（RD セッションホスト）の管理

このセクションでは、既存の RD セッションホストを構成および管理する方法について説明します。

その方法についてはこの後説明します。

- RAS RD セッションホスト Agent のステータスの確認（p. 129）
- RD セッションホストサイトの割り当ての変更（p. 130）
- RD セッションホストプロパティの表示と変更（p. 130）
- ログの構成（p. 153）

RD セッションホストの表示

作業中のサイトの RD セッションホストの一覧を表示するには、次の手順を実行します。

1 RAS Console で、[ファーム] > <サイト名> > [RD セッションホスト] に移動します。

2 右ペインの [RD セッションホスト] タブに利用できる RD セッションホストが表示されます。

次のように、[RD セッションホスト] の一覧をフィルタリングすることができます。

1 リストの上のツールバーにある虫眼鏡アイコンをクリックします。

2 リストの上に追加の行が表示されるので、リストのフィルタリングに使用する列に文字列を入力します。複数の列を使用することもできます。

3 たとえば、サーバー名で検索する場合は、[サーバー] 列にテキストを入力します。サーバー名全体を入力することも、一致するサーバーが見つかるまで最初の数文字を入力することも

できます。文字を入力するとリストがフィルタリングされ、一致するサーバーのみが表示されます。

4 2 つ以上の列にフィルター文字列を入力すると、それらの条件が AND 論理演算子で組み合わされます。

5 フィルターを削除してリスト全体を表示するには、虫眼鏡アイコンを再度クリックします。

6 虫眼鏡アイコンをもう一度クリックすると、先ほど指定したフィルターがまだ残っていることがわかります。フィルターを完全に削除するには、列からフィルター文字列を削除します。

RD セッションホストのサマリの表示

上で説明した RD セッションホストのエディターに加えて、利用可能な RD セッションホストに関するサマリも確認できます。このためには、次の操作を実行します。

1 RAS Console で、[ファーム] カテゴリーを選択して、中央のペインで [サイト] ノードを選択します。

2 右ペインの [RD セッションホスト] ホストプールに利用できるサーバーが表示されます。

3 RD セッションホストエディター（上記を参照）に移動するには、サーバーを右クリックして、[エディターに表示] を選択します。

詳細については、「RAS Console でのサイト」（p. 63）を参照してください。

利用可能なメニューオプション

メニューを使用して RD セッションホストで多数のタスクを実行できます。そのためには、[タスク] ドロップダウンリストをクリックして、目的のオプションを選択するかホストを右クリックして、コンテキストメニューからオプションを選択します。

メニューオプションの中には、テンプレートベースの RD セッションホストで利用できないものもあることに注意してください。このホストタイプで利用できないオプションは、無効または非表示にされています。これには以下が含まれます。

- ホストプールに割り当て: テンプレートベースのホストには、ホストプール割り当てが自動的に実行されます。
- 削除: ホスト（VM である）の削除は、テンプレートレベル（[ホストのリスト] ダイアログ）でのみ実行できます。

- プロパティ: このタイプの RD セッションホストには個別のプロパティはありません。一部の重要なプロパティは [デフォルトサーバーのプロパティ] から継承されます（「[RD セッションホストプロパティの表示と変更] > [Agent 設定]」（p. 130）を参照してください）。
- [コントロール]（ログオンコマンド）。ドレインモードは、テンプレートベースのホストが属するホストプールにより自動的に管理されます。

RD セッションホスト Agent のステータスの確認

リモートアプリケーションおよびデスクトップを公開するためには、RD セッションホストに RAS RD セッションホスト Agent がインストールされている必要があります。このほか、リモートデスクトップサービス（以前のターミナルサービス）もインストールされている必要があります。

通常、RD セッションホストをサイトに追加するとき、RD セッションホスト Agent およびリモートデスクトップサービスはデフォルトでインストールされます。しかし、インストールを省略した場合（または Agent や RDS をサーバーからアンインストールした場合）は、必要に応じてステータスを確認することで、適切に対処できます。

RD セッションホスト Agent と RDS のステータスを確認するには、次の手順を実行します。

1 最初に、[RD セッションホスト] リストの [ステータス] 列を確認します。列に”OK” と表示されるはずです。”OK”と表示されている場合は、Agent がインストールされていて正しく機能しています。”OK”と表示されていない場合については、この後説明します。

2 説明に加えて、[ステータス] 列では、色コードを使用して次のように Agent のステータスを示します。

   - 赤 - 未確認
   - オレンジ - アップデートが必要
   - 緑 - 確認済み

3 サーバーを右クリックして、コンテキストメニューの [トラブルシューティング] > [Agent をチェック] をクリックします。[Agent 情報] ダイアログが開きます。

4 サーバーに Agent がインストールされていない場合、画面の [インストール] ボタンをクリックして指示に従います。

Agent のインストール完了後、RD セッションホストの再起動が必要になる場合があります。サーバーを選択し、[タスク] > [コントロール再起動] > [再起動] をクリックして、Parallels RAS Console から直接実行することもできます。

RD セッションホストサイトの割り当ての変更

必要に応じて、RD セッションホストをファーム内の別のサイトに割り当てることができます。この機能は、ファーム内に複数のサイトがある場合にのみ利用できます。

サイトの割り当てを変更するには、次の操作を実行します。

1 RD セッションホストを右クリックして、コンテキストメニューの [サイトの変更] をクリックします。[サイトの変更] ダイアログが開きます。

2 リストからサイトを選択して、[OK] をクリックします。サーバーは、ターゲットサイトの [RD セッションホスト]（[ファーム] > <新規サイト名> > [RD セッションホスト]）リストに移動します。

RD セッションホストプロパティの表示と変更

注: このセクションの情報は、テンプレートに基づく RD セッションホストには適用されません。このタイプのホストには個別のプロパティがなく、テンプレートレベルで管理されます。詳細については、「ホストプール（RD セッションホスト）の管理」（p. 115）および「テンプレート」（p. 192）を参照してください。

RD セッションホストを構成するには、次の手順を実行します。

1 RAS Console で、[ファーム] > <サイト> > [RD セッションホスト] に移動します。

2 サーバーを選択し、[タスク] > [プロパティ] をクリックします。

3 [サーバープロパティ] ダイアログが開きます。このダイアログで RD セッションホストのプロパティを構成できます。

ダイアログについては、本セクションに続くサブセクションで説明します。

デフォルト設定を使用する

[サーバープロパティ] ダイアログには、タブがあり、各タブにはそれぞれに属するプロパティの個別のセットが含まれています。[一般] タブ以外のすべてのタブには、[グループのデフォルト値] または [サイトのデフォルト値] という共通のリンクがあり、サイトのデフォルト設定の表示と変更を行えます。特定のタブのプロパティにデフォルト設定を継承させる場合は、[デフォルト設定を継承] オプションを選択します。その場合、デフォルト設定は以下のいずれかから継承されます。

- グループのデフォルト値: グループについては「RD セッションホストサーバーのグループ化と複製」（p. 115）で説明されています。
- サイトのデフォルト値: グループにはサイトのデフォルトも継承されますが、[グループプロパティ] ダイアログで指定するグループ向けのカスタム設定によって上書きされます。

サイトのデフォルト設定を確認または変更するには、[グループのデフォルト値] または [サイトのデフォルト値] リンクをクリックします。それぞれの個別のタブは他のタブから独立してデフォルト設定を継承できますので注意してください。

RD セッションホストのカスタム設定を指定するには、[既定の設定を継承] オプションを無効にし、任意のタブのコントロールを使用して必要なオプションを設定します。

概要

[サイトでのサーバー有効化] オプションをオンまたはオフにして、サーバーを有効または無効にすることができます。無効にされているサーバーから公開済みのアプリケーションやバーチャルデスクトップをクライアントに提供することはできません。

このタブには、他にも次の要素があります。

- サーバー: サーバーの FQDN または IP アドレスを指定します。
- 説明: サーバーの説明（オプション）。
- ダイレクトアドレス変更: Parallels Client から RD セッションホストへの直接接続を確立するときに使用するダイレクトアドレスを変更する必要がある場合は、このオプションをオンにします。

Agent 設定

ファーム内の各 RD セッションホストには RAS RD セッションホスト Agent がインストールされており、他の Parallels RAS コンポーネントと通信します。Agent を構成するには、[Agent 設定] タブを使用します。

デフォルトの設定を使用するには、[デフォルト設定を継承] オプションを選択します。「デフォルト設定を使用する」（p. 130）を参照してください。

エージェントを構成するには、下記のオプションを設定します。

アプリケーションセッションの痕跡

- アクティブなセッションを中断するまでの時間: ユーザーがリモートアプリケーションを閉じた後、各セッションがバックグラウンドで接続状態を保持する時間を指定します。このオプションを使用して、サーバーへの不必要な再接続を回避します。
- 切断済みセッションをログオフするまでの時間: この設定では、“切断” とマークされた後、セッションのログオフにかかる時間を管理できます。

他の設定

- ポート: サーバーでデフォルト以外のポートが構成されている場合、別のリモートデスクトップ接続ポート番号を指定します。
- セッション最大数: セッションの最大数を指定します。
- 任意の Connection Broker: RD セッションホストが接続する Connection Broker を選択します。これは、サイトコンポーネントが、WAN で通信する複数の物理的な場所に設置されているときに役立ちます。より適切な Connection Broker を指定することによりネットワークトラフィックを減らすことができます。

クライアント URL/メールのリダイレクションを許可

ユーザーがリモートアプリケーションで URL または HTML Mailto リンクを開くと、リンクはクライアントコンピューターにリダイレクトされ、リモートホストのアプリケーションではなく、ローカルのデフォルトアプリケーション（ウェブブラウザーまたはメールクライアント）で開かれます。この機能を有効にするには、このオプションを選択し、[構成] ボタンをクリックします。ダイアログが開いたら、次のいずれかを選択します。

- 登録されたアプリケーションを置き換え: このオプションでは、リンクのリダイレクトの代替メソッドを使用します。これにより、リモートサーバー側でデフォルトの Web ブラウザーとメールクライアントを”ダミー”アプリと置換します。これを行うことで、リンクを開く操作を中断し、クライアントコンピューターにリダイレクトできます。
- Windows シェル URL の名前空間オブジェクトをサポート: シェル URL 名前空間オブジェクトをサポートするということは、Parallels RAS がシェル名前空間 API を使用する公開済みアプリケーションでの操作を中断して、リンクを開くことができるということを意味します。これは多くのアプリケーションでの標準的な動作です。シェル URL 名前領域オブジェクトのサポートを無効する機能は、Parallels RAS の旧バージョンとの互換性のために備えられています。Parallels RAS の旧バージョン（RAS バージョン 16.2 以前）で動作させたい場合、このオプションを無効化できます。

リダイレクトを有効化する場合でも、リダイレクトの除外 URL リストを構成できることにご注意ください。これは、[ファーム] > [サイト] / [設定] > [URL リダイレクト] タブで実行できます。詳細については、「サイト設定」（p. 573）を参照してください。

ドラッグ & ドロップを有効化

ドラッグ & ドロップ機能が Parallels Client 内でどのように機能するかを設定できます。ドラッグ & ドロップを有効化するには、オプションを選択し、[構成] ボタンをクリックして、以下の中から選択します。

- サーバーからクライアントのみ: ローカルアプリケーションへのドラッグ & ドロップです。逆方向には使用できません。
- クライアントからサーバーのみ: ローカルアプリケーションへのドラッグ & ドロップのみです。
- 双方向: Parallels RAS 17.1 以降ではこのオプションが変更されたことに注意してください。それ以前はドラッグ & ドロップを有効化または無効化するチェックボックスであり、[クライアントからサーバーのみ] モードでのみ動作していました。Parallels RAS の以前のバージョンからアップグレードする際、このチェックボックスがオンになっていれば、デフォルトで [クライアントからサーバーのみ] が選択されます。オフになっていた場合は、[無効] オプションが設定されます。必要に応じて、どの新しいオプションに切り替えることも可能です。

注: この文書の作成時点では、ドラッグ・ドロップ機能が利用できるのは Parallels Client for Windows および Parallels Client for Mac のみです。

2XRemoteExec がクライアントにコマンドを送信することを許可

サーバーで実行されているプロセスにより、クライアント側でのアプリケーションの展開をクライアントに指示することを許可するには、このオプションをオンにします。2XRemoteExec の詳細については、このトピックの最後にある「RemoteExec の使用」のサブセクションを参照してください。

RemoteApp を使用（利用可能な場合）

このオプションを有効にすると、シェル関連の問題でアプリが正しく表示されない場合に、リモートアプリを使用できます。この機能は、Windows 用 Parallels Client でのみサポートされています。

RDP 転送プロトコルの管理

Parallels Client とサーバー間の接続に使用されるトランスポートプロトコルを選択します。これを実行するには、このオプションを選択し、[構成] ボタンをクリックします。

アプリケーションの監視を有効にする

サーバーでのアプリケーションの監視を有効または無効にします。アプリケーションのモニタリングを無効にすると、RAS Connection Broker に情報を転送しているときに、サーバーでの CPU 使用率とネットワークの使用率を減らすための WMI モニタリングが停止します。このオプションが有効な場合、収集された情報が対応する RAS レポートに表示されます。このオプションが無効な場合、このサーバーからの情報はレポートに記載されません。

ファイル転送コマンドを許可（Web および Chrome クライアント）:

リモートセッションでのファイル転送を有効化します。ファイル転送を有効にするには、このオプションを選択し、[構成] ボタンをクリックします。詳細については、「リモートファイル転送を構成する」（p. 538）を参照してください。

ドライブリダイレクトのキャッシュを有効化

リダイレクトされたドライブ上でのファイルの参照とナビゲーションをより高速にすることで、ユーザーエクスペリエンスを向上させます。詳細については、「ドライブリダイレクトのキャッシュ」（p. 152）を参照してください。

2XRemoteExec の使用

2XRemoteExec は、サーバーからクライアントへのコマンドの送信を容易に行えるようにするための機能です。そのために、コマンドラインユーティリティ `2XRemoteExec.exe` を使用します。次のコマンドラインオプションが用意されています。

コマンドラインパラメーター	パラメーターの説明
`-s`	2XRemoteExec コマンドを”サイレント”モードで実行するのに使用します。このパラメーターを省略すると、コマンドにより、アプリケーションからのポップアップメッセージが表示されます。このパラメーターを指定すると、メッセージは表示されません。

-t	アプリケーションが開始されるまでのタイムアウトを指定するのに使用します。タイムアウトは 5000 ミリ秒～30000 ミリ秒の値にする必要があります。値の単位は”ミリ秒”である点に注意してください。タイムアウトが発生すると、コマンドはエラーを返します。タイムアウトが発生しても、クライアントでアプリケーションが開始されている場合があります。
-?	2XRemoteExec で使用されるパラメーターのヘルプリストを表示します。
"Path for Remote Application"	サーバーからの要求に従ってクライアントで開始されるアプリケーション。

2XRemoteExec の例:

次のコマンドを実行すると、使用できるパラメーターの説明がメッセージボックスに表示されます。

```
2XRemoteExec -?
```

このコマンドを実行すると、クライアントでメモ帳が起動します。

```
2XRemoteExec C:\Windows\System32\Notepad.exe
```

この例のコマンドを実行すると、クライアントのメモ帳で C:\readme.txt ファイルが開きます。メッセージは表示されず、2XRemoteExec は 6 秒間、またはアプリケーションが起動するまで待機します。

```
2XRemoteExec C:\Windows\System32\Notepad.exe "C:\readme.txt"
```

ユーザープロファイル

このタブでは、ユーザープロファイルの設定を行います。

デフォルトの設定を使用するには、[デフォルト設定を継承] オプションを選択します。「デフォルト設定を使用する」（p. 130）を参照してください。

ユーザープロファイル設定の詳細については、「ユーザープロファイル」（p. 138）を参照してください。

アプリケーションパッケージ

[アプリケーションパッケージ] タブでは、RD セッションホストとグループ上の MSIX アプリケーションパッケージを管理することができます。

デフォルトの設定を使用するには、[デフォルト設定を継承] オプションを選択します。「デフォルト設定を使用する」（p. 130）を参照してください。

RD セッションホストにパッケージを追加する

「MSIX アプリケーションパッケージの使用」（p. 576）、サブセクション「ホストへのパッケージの追加」を参照してください。

VDI プールにパッケージを追加する

「MSIX アプリケーションパッケージの使用」（p. 576）、サブセクション「VDI プールへのパッケージの追加」を参照してください。

MSIX パッケージからインストールされたアプリケーションの管理

[タスク] のドロップダウンリストから、以下の操作を実行できます:

- 追加: RD セッションホストに新しいパッケージを追加します。
- ステージングを再試行: 追加されたすべてのパッケージのステージング再試行を手動でトリガーします。
- 更新: パッケージの一覧を更新します。
- 削除: 選択したパッケージを削除します。

最適化

[最適化] タブでは、RD セッションホストを最適化して、Parallels RAS 環境で最適なパフォーマンスを発揮できるようにするために使用する設定を指定できます。無効化、削除、または最適化の対象となる Windows コンポーネントやサービス、またその他のオプションを選択して、仮想アプリおよびデスクトップの配信の効率性と合理性を向上させ、改善することができます。

デフォルトの設定を使用するには、[デフォルト設定を継承] オプションを選択します。「デフォルト設定を使用する」（p. 130）を参照してください。

詳細な手順については、「最適化」（p. 146）を参照してください。

デスクトップアクセス

[デスクトップアクセス] タブでは、リモートデスクトップへのアクセスを特定のユーザーに制限できます。

デフォルトの設定を使用するには、[デフォルト設定を継承] オプションを選択します。「デフォルト設定を使用する」（p. 130）を参照してください。

デフォルトでは、RD セッションホストでリモートアプリケーションにアクセスできるすべてのユーザーが標準 RDP 接続経由でサーバーにも接続できます。リモートデスクトップへのアクセスを特定のユーザーに制限するには、次の手順を実行します。

1. [デスクトップアクセス] タブで、[直接デスクトップアクセスを次のユーザーに制限する] オプションを選択します。[デフォルト設定を継承] オプションを選択している場合、[デフォルトを編集] リンクをクリックして、デフォルトの構成を表示し（必要な場合は変更し）ます。残りの手順は、[サーバープロパティ] ダイアログおよび [デフォルトサーバーのプロパティ] ダイアログの両方に適用されます。
2. [追加] ボタンをクリックします。
3. 希望するユーザーを選択します。複数のユーザーを含めるには、セミコロンで区切ります。
4. [OK] をクリックします。
5. 選択されたユーザーは、[デスクトップアクセス] タブのリストに表示されます。

このリストのユーザーは引き続き Parallels Client を使用してリモートアプリケーションにアクセスできますが、このサーバーへのリモートデスクトップアクセスは拒否されます。

注: [コンピューターの構成] > [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] > [リモートデスクトップセッションホスト] > [接続] > [ユーザーがリモートデスクトップサービスを使ってリモート接続することを許可する] は、[未構成] に設定されている必要があります。それ以外の場合には、この設定が優先されます。

管理者グループのメンバーは、このリストに含まれている場合でも引き続きリモートデスクトップにアクセスできることに注意してください。

RDP プリンター

[RDP プリンター] タブでは、リダイレクトされたプリンターの名前変更フォーマットを構成できます。フォーマットは、サーバーのどのバージョンと言語を使用しているかによって異なる場合があります。

デフォルトの設定を使用するには、[デフォルト設定を継承] オプションを選択します。「デフォルト設定を使用する」（p. 130）を参照してください。

[RDP プリンター名のフォーマット] ドロップダウンリストでは、構成したサーバーに固有のプリンター名フォーマットを選択できます。

[プリンター名にセッション番号を入れない] および [プリンター名にクライアント名を入れない] を選択すると、対応する情報をプリンター名から除外できます。

ユーザープロファイル

ユーザープロファイルは、特定のユーザーに関する設定とアプリケーションデータの集合です。Parallels RAS などのパーシスタントでないリモート環境では、一貫したユーザーエクスペリエンスを提供するために、ユーザープロファイルを保持する必要があります。ユーザープロファイルデータをネットワーク上の場所に保存して、サインイン時間を最小限に抑え、ホスト、クライアント、およびプロファイルストレージ間のファイル I/O を最適化することで、これを実現できます。

Parallels RAS では、以下のテクノロジーをサポートすることでユーザープロファイルを管理しています。

- ユーザープロファイルディスク（p. 139）: [RD セッションホスト限定] これは、専用のファイル共有にユーザーアプリケーションデータを保存する仮想ハードディスクです。このディスクは、ユーザーがセッションホストにサインインするとすぐにユーザーセッションにマウントされ、ユーザーがログアウトするとアンマウントされます。

  注: Microsoft は、ユーザープロファイルディスクテクノロジーの開発に積極的ではありません。FSLogix（p. 140）のプロファイルを移行することをお勧めします。 [ユーザープロファイルディスク] オプションは旧式化しているため、VDI と Azure Virtual Desktop では使用できません。

- FSLogix（p. 140）: パーシスタントでない環境向けのリモートプロファイルソリューションです。FSLogix プロファイルコンテナーにより、ユーザープロファイル全体をリモートの場所にリダイレクトし、パーシスタントでない環境でユーザーコンテキストを維持し、サインイン時間を最小限に抑え、互換性の問題を排除するネイティブプロファイルのユーザーエクスペリエンスを提供できます。FSLogix プロファイルコンテナーは、ローミングプロファイルおよびユーザープロファイルディスクの後継技術として利用されることの多いプロファイル管理ソリューションです。

ユーザープロファイルは、下記向けに構成できます。

- RD セッションホスト

- VDI
- Azure Virtual Desktop

ユーザープロファイル設定は、サイトレベル（サイトのデフォルト値）で上記向けに構成されます。RAS 管理者が特定のコンポーネントにカスタム設定を使用することを決定した場合は、個別のコンポーネント向けに構成することもできます。

サイトレベルでユーザープロファイルを構成するには、[ファーム] > [サイト] に移動し、[タスク] > [サイトのデフォルト値] メニューをクリックして以下のいずれかを選択します。

- RD セッションホスト
- VDI
- AVD マルチセッションホスト
- AVD シングルセッションホスト

表示された [サイトのデフォルト値] ダイアログで、[ユーザープロファイル] タブを選択します。最適化を構成する場合、上述のいずれについても同一のユーザーインターフェイスが使用されます。

次のセクションでは、ユーザープロファイルの機能を構成する方法について詳しく説明します。

ユーザープロファイルディスク

ユーザープロファイルディスクを構成するには、以下の設定を指定します。

1. このホストに別の設定を指定する場合は、ホストの [プロパティ] ダイアログで、[デフォルト設定を継承] の選択を解除します。
2. [テクノロジー] セクションで、[ユーザープロファイルディスク] を選択します。
3. ドロップダウンリストで、次のいずれかを選択します。
   - 変更しない: 現在のサーバー設定を保持します（デフォルト）。
   - 有効: ユーザープロファイルディスクの機能を有効にします。
   - 無効: この機能を無効にします。
4. [詳細プロファイルディスク設定を構成] ボタンをクリックして、[ユーザープロファイルの詳細設定] ダイアログを開きます。
5. [ディスク] タブで、以下を指定します。

- ディスクの場所: 前の手順で [有効] を選択した場合、ユーザープロファイルディスクが作成されるネットワークロケーションを指定します。Microsoft Windows UNC フォーマットを使用して場所を指定します（例: `\\RAS\users\disks`）。サーバーはディスク共有でフルコントロール権限を持つ必要があることに注意してください。
- 最大サイズ: 許可されている最大のディスクサイズを入力します（ギガバイト単位）。

6 [フォルダー] タブで、以下を指定します。

- すべてのユーザー設定とデータをユーザープロファイルディスクに保存: 除外リストで指定されたフォルダーを除くすべてのフォルダーが、ユーザープロファイルディスクに保存されます。除外リストにフォルダーを追加またはフォルダーから削除するには、[+] ボタンまたは [-] ボタンをクリックします。
- 次のフォルダーのみユーザープロファイルディスクに保存: 包含リストで指定されたフォルダーのみがユーザープロファイルディスクに保存されます。2 つの包含リストがあります。最初のリストには標準のユーザープロファイルフォルダー（デスクトップ、ドキュメント、ダウンロード、など）が含まれ、含めるフォルダーを選択できます。2 番目のリストで追加フォルダーを指定できます。[+] ボタンまたは [-] ボタンをクリックして、フォルダーを追加または削除します。

ユーザープロファイルディスクを有効にする場合、変更を適用するためにサーバーを再起動する必要があります。

FSLogix

注: 既存の FSLogix プロファイルコンテナーがあり、その構成を Parallels RAS で管理したい場合は、「Parallels RAS で既存プロファイルの管理を構成する」（p. 144）の追加説明を参照してください。

サポートされる FSLogix リリース

Parallels RAS は、リリース 2210 hotfix 2 までの FSLogix リリースでテストされています。

インストール方法の構成

特定のサーバーまたはテンプレート向けに FSLogix を構成する（本ガイドで後述します）前に、次のようにサイトレベルで FSLogix のインストール方法を構成する必要があります。

1 [ファーム] > [サイト] > [設定] に移動し、[機能] タブを選択します。ここで、Parallels RAS が FSLogix を個別のホストにインストールするために使用する方法を選択する必要があります。以下のいずれかを選択できます。

- 手動でインストールする: すべてのホストで FSLogix を手動でインストールする場合は、このオプションを選択します。このオプションが選択された場合、Parallels RAS はホストで FSLogix のインストールを試行しません。
- オンラインでインストールする: このオプションを選択すると、FSLogix がインターネットからセッションホストにインストールされます。ドロップダウンリストから、サポートされる FSLogix のバージョンを 1 つ選択するか、[カスタム URL] を選択し、ダウンロード URL を指定します。[最新情報を検出] ボタンをクリックして、最新の FSLogix バージョンの URL を自動で取得します。
- ネットワーク共有からインストールする: ネットワーク共有に FSLogix インストールファイルがあり、その場所を指定する場合はこのオプションを選択します。
- RAS Connection Broker からプッシュする: このオプションを選択すると、FSLogix インストールアーカイブを RAS Connection Broker サーバーにアップロードできます。セッションホストで FSLogix を有効にすると、RAS Connection Broker サーバーからホストにプッシュインストールされます。

2 完了したら、RAS Console で [適用] をクリックして、変更を Parallels RAS に適用します。

FSLogix のアップグレード

上述のダイアログを使用して、FSLogix を新しいバージョンにアップグレードすることもできます。アップグレードするには、次のいずれかを実行します。

- [オンラインでインストールする] を選択し、表示される FSLogix ビルドの 1 つを選択するか、カスタム URL を指定します。[最新情報を検出] ボタンをクリックし、最新の安定した FSLogix ビルドの URL を取得します。
- Microsoft のウェブサイトから新しいバージョンをダウンロードし、ネットワーク共有に配置するか、RAS Connection Broker サーバーにアップロードします。続いて、[ネットワーク共有からインストールする] または [RAS Connection Broker からプッシュする] のいずれか該当する方法を選択します。

FSLogix が 1 つまたは複数のホストにすでにインストールされており、上記のいずれかを実行して新しいバージョンの FSLogix が利用可能になると、FSLogix がインストールされているホストでアップグレードされます。ホストにインストールされているバージョンよりも古いバージョンを指定した場合は、FSLogix はダウングレードされます。

サイトのデフォルト値と FSLogix のホストの構成

サイトのデフォルト値または FSLogix の個別ホストを構成するには、以下のいずれかを実行します。

- サイトのデフォルト値を構成するには、[ファーム] > [サイト] に移動し、[タスク] > [サイトのデフォルト値] > [RD セッションホスト] をクリックします（または、[VDI] をクリックして VDI のデフォルト値を構成するか、[AVD] オプションの 1 つをクリックして Azure Virtual Desktop のサイトのデフォルト値を構成します）。
- 個別のホストを構成するには、[ファーム] > [サイト] > [RD セッションホスト] に移動します。ホストを右クリックし、[プロパティ] を選択します。
- RD セッションホストをファームに追加すると、FSLogix 設定が [ユーザープロファイル] ページで指定されます。

[サイトのデフォルト値] または [プロパティ] ダイアログで、[ユーザープロファイル] タブを選択し、以下のオプションを指定します。

1. ホストの [プロパティ] ダイアログ（もしくは新しいホストまたはテンプレートを追加するウィザード）が表示されている状態で、このホストに対して別の設定を指定するには、[デフォルト設定を継承] オプションの選択を解除します。
2. [テクノロジー] セクションで、[FSLogix] を選択します。
3. [展開の方法] フィールドに、サイトレベルで構成され、現在設定されている展開の方法が表示されます（上記の説明を参照）。[変更...] リンクをクリックして別の方法を選択できます。この操作を行うと、サイトの設定が変更され、サイトのすべてのホストに変更が適用されます。
4. プロファイルコンテナーを使用したい場合は、[プロファイルコンテナーを使用する] オプションを選択します。[構成] ボタンをクリックして、設定を構成します。
   - ユーザーとグループタブ: ユーザーとグループの包含リストと除外リストを指定します。デフォルトでは、すべてのユーザーが FSLogix プロファイルの包含リストに追加されます。一部のユーザープロファイルをローカルのままにする場合は、該当のユーザーを除外リストに追加できます。ユーザーとグループは両方のリストに追加できますが、除外リストが優先されます。
   - フォルダータブ: フォルダーの包含リストと除外リストを指定します。共通フォルダーから選択することも、手動でフォルダーを指定することもできます。フォルダーはユーザープロファイルのパスに配置する必要があります。ご注意ください。

- ディスクタブ: プロファイルディスクの設定を指定します。　場所の種類: プロファイルディスクの場所の種類（SMB の場所、またはクラウドキャッシュ）を選択し、1 つまたは複数の場所を指定します。プロファイルディスクの場所: プロファイルディスクの場所（1 つまたは複数）です。これは、VHD（X）ファイルの場所（FSLogix ドキュメントに記載されている、レジストリ内の VHD の場所の設定）です。プロファイルディスクのフォーマット: 要件に応じて、VHD または VHDX を選択します。VHDX はより新しいフォーマットであり、より多くの機能を備えています。割り当てタイプ: [動的] または [フル] を選択します。この設定は、[デフォルトサイズ] の設定（以下を参照）と一緒に使用して、プロファイルのサイズを管理します。[動的] を選択すると、割り当てられたデフォルトサイズにかかわらず、プロファイルコンテナーは最低限のディスク領域を使用します。ユーザープロファイルにより多くのデータが入力されると、ディスクのデータ量はデフォルトサイズで指定したサイズにまで増加しますが、デフォルトサイズを上回ることはありません。デフォルトサイズ: 新たに作成された VHD（X）のサイズを MB 単位で指定します。
- 詳細タブ: このタブでは、FSLogix の詳細なレジストリ設定を変更できます。設定を変更するには、設定を選択して [タスク] > [編集] をクリックします。デフォルトでは、設定は無効になっています。設定を有効にするには、設定名の前にあるチェックボックスをオンにします。各設定の説明は RAS Console に表示されます。FSLogix プロファイルコンテナーの構成について詳しくは、https://docs.microsoft.com/en-us/fslogix/profile-container-configuration-reference を参照してください。

5 オフィスコンテナーを使用したい場合は、[オフィスコンテナーを使用する] オプションを選択します。[構成] ボタンをクリックして、設定を構成します。

- ユーザーとグループタブ: 上と同様です。
- ディスクタブ: 上と同様です。
- 詳細タブ: 上と同様です。

6 [一般設定を構成する] ボタンをクリックして、すべてのタイプのコンテナーに対して FSLogix の設定を構成できます。

- アプリサービスタブ: このタブでは、FSLogix の詳細なレジストリ設定を変更できます。これらの設定の詳細については、https://learn.microsoft.com/en-us/fslogix/reference-configuration-settings?tabs=profiles#app-services-settings を参照してください。
- クラウドキャッシュタブ: このタブでは、クラウドキャッシュの設定を変更できます。これらの設定の詳細については、

https://learn.microsoft.com/en-us/fslogix/reference-configuration-settings?tabs=ccd#fslogix-settings-profile-odfc-cloud-cache-logging を参照してください。

- ログタブ: このタブでは、プロファイルコンテナーのログ設定を変更できます。これらの設定の詳細については、https://learn.microsoft.com/en-us/fslogix/reference-configuration-settings?tabs=logging#fslogix-settings-profile-odfc-cloud-cache-logging を参照してください。

ホストの再起動

ウィザードの実行中に新しいホストの FSLogix を有効にする場合、追加で行う手順はありません。ウィザードが完了したら、ホストが再起動され、アクティブなロードバランスに追加されます。既存のホストは、[タスク] > [ツール] > [再起動] メニューオプションを使用して手動で再起動する必要があります。

Parallels RAS で既存プロファイルの管理を構成する

このトピックでは、Parallels RAS で既存の FSLogix プロファイルコンテナーの管理を構成する方法について説明します。FSLogix プロファイルコンテナーの構成により、プロファイルをリダイレクトされる場所と方法を定義できます。通常、プロファイルの設定はレジストリ設定や GPO で行います。Parallels RAS では、外部ツールを使用せずに、Parallels RAS Console または RAS 管理ポータルからプロファイルを構成することができます。

ご利用いただく前に

Parallels RAS で FSLogix プロファイルコンテナーを構成する前に、以下の点に注意してください。

- プロファイル自体を変更する必要はなく、既存のプロファイルをそのまま使用できます。
- FSLogix プロファイルコンテナーのロケーションとして、SMB ネットワーク共有やクラウドキャッシュなど、既存のロケーションを引き続き使用できます。

準備

準備として以下の手順を実行します。

1. 既存のプロファイルをバックアップします。プロファイルデータが喪失または破損することはほとんどありませんが、プロファイル構成を変更する前に有効なバックアップを取得しておくことをお勧めします。

2 FSLogix プロファイルコンテナーの GPO 構成をオフにします。GPO からの FSLogix プロファイル管理と Parallels RAS からの管理を同時に有効にすることはできません。それで、この手順が重要になります。

3 RAS ファーム内のホストで FSLogix プロファイルを設定する前に、ホストでユーザーセッションが実行されていないことを確認してください。業務時間外のメンテナンス期間に移行作業を行うことも考慮できるでしょう。

GPO と FSLogix の構成を複製する

Parallels RAS で既存の FSLogix プロファイルコンテナーを構成するには、既存の GPO を Parallels RAS の FSLogix 構成に複製する必要があります。これは、Parallels RAS Console または Parallels RAS 管理ポータルで実行できます。

RAS Console でプロファイルを設定するには:

1 「FSLogix プロファイルコンテナー」セクション（p. 140）の指示に従い、[ディスク] タブを開きます。

2 [プロファイルディスクの場所] リストボックスで、FSLogix プロファイルを保存する既存の SMB またはクラウドキャッシュの場所を指定します。さらに、プロファイルディスクのフォーマット、割り当てタイプ、既定サイズを指定します。

3 ユーザーの除外やフォルダーの除外など、サーバー上にある FSLogix の他の設定を行います。

RAS 管理ポータルでプロファイルを構成するには:

1 [インフラストラクチャ] > [RD セッションホスト] に移動します。

2 リストからホストをクリックして、[プロパティ] をクリックします。

3 中央のペインで [ユーザープロファイル] をクリックします。

4 RAS Console では、上記の手順で設定を行います。

なお、本ガイドの執筆時点で RAS 管理ポータルは、FSLogix プロファイルコンテナーの使用に供する RD セッションホストの構成目的でのみ利用できます。その他のホストタイプの場合は、デスクトップベースの RAS Console をご利用ください。

推奨事項とテスト

前のセクションの手順を実行する場合、RAS ファームに存在する複数の（またはすべての）サーバーをまとめて構成することは避けてください。1 台のサーバー（例: RD セッションホスト

) から着手し、1 人のユーザーを接続した上でテストを行ってください。その後、他のサーバーを設定し、同一ユーザーが複数のサーバーに連続してログインするテストを行います。このテストで、いずれのセッションホストでもプロファイルが読み込まれ、カスタマイズされた機能が利用できることを確認します。特に問題がなければ、他のホスト、ホストプール、またはサイトのデフォルトを構成します。

RAS ユーザーは、Parallels RAS によって集中管理される、既存の FSLogix プロファイルコンテナーを使用して Parallels RAS に接続することが可能です。

FSLogix のウイルス対策の除外項目

FSLogix プロファイルコンテナーの仮想ハードドライブに対し、以下のウイルス対策の除外項目を必ず設定してください。以下の情報は、必ずセキュリティチームに確認してください。

除外対象のファイル:

- %Programfiles%\FSLogix\Apps\frxdrv.sys
- %Programfiles%\FSLogix\Apps\frxdrvvt.sys
- %Programfiles%\FSLogix\Apps\frxccd.sys
- %TEMP%*.VHD
- %TEMP%*.VHDX
- %Windir%\TEMP*.VHD
- %Windir%\TEMP*.VHDX
- \\storageaccount.file.core.windows.net\share**.VHD
- \\storageaccount.file.core.windows.net\share**.VHDX

除外対象のプロセス:

- %Programfiles%\FSLogix\Apps\frxccd.exe
- %Programfiles%\FSLogix\Apps\frxccds.exe
- %Programfiles%\FSLogix\Apps\frxsvc.exe

最適化を構成する際に、Windows Defender ATP カテゴリーで除外するファイルやプロセスを指定できます。詳細については、「最適化」（p. 146）を参照してください。

最適化

バージョン 18 より、Parallels RAS には RD セッションホスト、VDI、Azure Virtual Desktop のワークロード向けの自動最適化機能が組み込まれています。管理者は、マルチセッションホ

スト（RD セッションホストなど）またはシングルセッションホスト（VDI など）向けに事前に構成されたさまざまな最適化機能を手動または自動で選択できます。これにより、仮想アプリと仮想デスクトップの配信の効率性と合理性を向上させ、改善することができます。

事前構成済みの最適化機能は、Microsoft Windows の今後のリリースをサポートするために、簡単に更新できるように設計されています。さらに、ツール内でカスタムスクリプトを使用して、すでに利用可能な最適化機能を Parallels RAS ワークロードのマシンに展開することもできます。

130 を超えるイメージ最適化機能を特別な設定なしに利用できます。これらの最適化機能は、主に以下のカテゴリーに分類されます。

- UWP アプリケーションパッケージ（削除。VDI でのみ利用可能）
- Windows Defender ATP（オンまたはオフの設定、リアルタイムスキャンの無効化、ファイル、フォルダー、プロセス、および拡張子の除外）
- Windows コンポーネント（削除）
- Windows サービス（無効化）
- Windows のスケジュール済みタスク（無効化）
- Windows 拡張オプション（Cortana、システムのリストア、テレメトリ、カスタムレイアウト）
- ネットワークパフォーマンス（タスクのオフロード、ipv6 などの無効化）
- レジストリ（サービス起動のタイムアウト、ディスク I/O のタイムアウト、カスタムなど）
- 視覚効果（最適な外観、最適なパフォーマンス、カスタム）
- ディスクのクリーンアップ（ユーザープロファイルの削除、イメージのクリーンアップなど）
- カスタムスクリプト（.ps1、.exe、.cmd、その他の拡張子/フォーマット）

最適化機能の全カテゴリーとコンポーネントについては、https://kb.parallels.com/125222 を参照してください。

最適化機能は、以下を基盤とする RD セッションホスト、VDI デスクトップ、Azure Virtual Desktop、リモート PC プール（VDI 経由）で利用できます。

- Windows Server 2012 R2 以降
- Windows 7 SP1
- Windows 10

- Windows 11

最適化の構成

最適化は、下記向けに構成できます。

- RD セッションホスト
- VDI
- Azure Virtual Desktop

最適化の設定は、サイトレベル（サイトのデフォルト値）で上記向けに構成されます。RAS 管理者が特定のコンポーネントにカスタム設定を使用することを決定した場合は、個別のコンポーネント向けに構成することもできます。

サイトレベルで最適化を構成するには、[ファーム] > [サイト] に移動し、[タスク] > [サイトのデフォルト値] メニューをクリックして以下のいずれかを選択します。

- RD セッションホスト
- VDI
- AVD マルチセッションホスト
- AVD シングルセッションホスト

表示された [サイトのデフォルト値] ダイアログで、[最適化] タブを選択します。最適化を構成する場合、上述のいずれについても同一のユーザーインターフェイスが使用されます。

注: 最適化を適用する前に、セッションホストの状態が保存されていることを確認してください。最適化を適用した後に変更を元に戻すことはできません。

最適化を構成するには、以下を実行します。

1. ホストの [プロパティ] ダイアログまたはウィザードが表示されている状態で、このホストに対する設定を変更するには、[デフォルト設定を継承] オプションの選択を解除します。
2. [最適化を有効化] オプションを選択します。
3. 最適化の種類を以下から選択します。
   - 自動: 事前に定義された事前構成済みの最適化が自動的に使用されます。
   - 手動: どの最適化オプションを使用するかを完全に制御して、それぞれの最適化を構成できます。このオプションを選択すると、カスタムの最適化スクリプトをホストで実行することもできます。

4 前の手順で [手動] を選択した場合、要件に従って最適化のカテゴリーとコンポーネントを構成します。以下の「最適化の構成」 を参照してください。

5 有効化した全カテゴリーで強制的に最適化する: これは特別なオプションであり、予測できない何らかの理由（ホストが予期せずにオフラインになったなど）によって最適化の一部をホストに適用できなかった場合にのみ使用します。このオプションを選択し、RAS Console で [OK]、続いて [適用] をクリックすると、最適化の構成全体がホストに適用されます。この方法により、最適化コンポーネントに最後に行った変更とホストに適用されなかった変更が、確実に再び適用されます。[有効化した全カテゴリーで強制的に最適化する] オプションの状態（オンまたはオフ）は保存されず、次にダイアログを開くと、オプションは再びオフになっています。それで、この操作は毎回必要になります。変更を行った後にその変更をホストに適用するという標準的なシナリオでは、このオプションを選択する必要はありません。通常は最適化の構成全体を適用するのではなく、変更部分のみを適用するためです。

6 [カテゴリー] リストには、構成できる最適化のカテゴリーが含まれます。最適化にカテゴリーを含めるには、該当するチェックボックスを選択します。個別に構成できる複数のコンポーネントがあるカテゴリーもあれば、設定をカスタマイズできるカテゴリーもあります。カテゴリの設定またはコンポーネントを構成するには、カテゴリーを選択して歯車アイコンをクリックします（または、[タスク] > [プロパティ] をクリックするか、単にカテゴリーをダブルクリックします）。選択したカテゴリーに応じて、以下を実行できます。

- カテゴリー設定を構成します (使用可能なオプションの選択、個々の設定の選択または選択解除、値の指定、エントリーの追加または削除）。
- 基盤となるコンポーネントを追加または削除して、最適化に含めるか、最適化から除外します（プラス記号アイコンとマイナス記号アイコンを使用）。コンポーネントの追加では（利用できる場合）、事前に定義されたリストから選択することも、カスタムコンポーネントを指定することもできます。
- 場合によっては (特にレジストリのエントリーでは）、エントリーをダブルクリックし、そのエントリーに対して複数の値を指定できます。
- 事前定義されたコンポーネントを削除しても、[タスク] > [デフォルトにリセット] をクリックすることで、削除したコンポーネントをいつでもリストに戻すことができます。このメニューを使用して、変更されたカテゴリー設定をデフォルトにリセットすることもできます。
- このリストの最後の最適化カテゴリーはカスタムスクリプトです。カスタムスクリプトを使用して、利用可能な最適化スクリプトを実行できます。詳細については、下記の「カスタムスクリプトの使用」サブセクションを参照してください。

7 終了したら、[OK] をクリックしてダイアログを閉じます。

カスタムスクリプトの使用

最適化カテゴリーのカスタムスクリプトは、対象のホストで最適化スクリプトを実行するために使用されます。このカテゴリーを構成する前に、対象のホストにスクリプトが存在すること、各ホストでパスとファイル名が同一であることを確認します。

最適化カテゴリーのカスタムスクリプトを構成するには、以下を実行します。

1. リストで [カスタムスクリプト] カテゴリーを有効化（チェックボックスを選択）し、強調表示させて [タスク] > [プロパティ] をクリックします。
2. 表示されたダイアログで、実行するコマンド、引数（必要な場合）、初期ディレクトリ、スクリプトの実行に使用される資格情報を指定します。
3. [OK] をクリックします。

最適化をホストに適用するときに、その他の最適化パラメーターを適用する処理の一環として、スクリプトが実行されます。

最適化の適用

ホストで最適化機能を有効化し、RAS Console で [適用] をクリックすると、ホストが Parallels RAS と次に通信したときに次の事象が発生します。

1. ホストのステータスが [最適化を保留中] に変更され、ホストがドレインモードに入ります。この段階では、リストでホストを選択し、[タスク] > [最適化の停止] をクリックすれば、最適化を停止できます。
2. すべてのユーザーがログオフすると、ホストのステータスは [最適化を実行中] に変更されます。
3. 最適化の設定がすべて適用されたら、ホストは再起動されます。
4. 再起動後、ホストは稼働中の状態に戻り、ステータスは [OK] に変更されます。

注: 最適化に失敗しても、最適化完了後にホストが再起動されるように設計されています。

最適化の結果は、ホストのログ（%ProgramData%\Parallels\RASLogs\ImageOptimizer.log）に記録されます。ファイルを開き、次の内容に類似したエントリーを検索します。

- [I 78/00000009/T10C4/P0FD4] 11-30-20 10:09:19 - Image Optimization completed with 98 successful and 0 unsuccessful optimizations（イメージ最適化完了: 98 完了、0 未完了）

注: 設計上、最適化は再起動/無効化よりも優先度が低くなっています。たとえば、スケジュール開始時に、ホストのステータスが”最適化保留”から無効化/再起動に変更されている場合などがあります。

アップグレード

Parallels RAS が古いバージョンからアップグレードされる場合

- 最適化機能は無効化されます。
- 継承はオフになります。

アップグレード後に最適化を利用する場合、管理者は、サイトのデフォルト値またはホストプールの設定から、手動で最適化を有効にする必要があります。

継承

	最適化	継承元
RDSH のサイトのデフォルト値	はい	なし
RDSH ホストプール	いいえ	なし
RDSH スタンドアロン	はい	RDSH のサイトのデフォルト値
RDSH テンプレート	はい	RDSH のサイトのデフォルト値
テンプレートからの RDSH	いいえ	なし
VDI のサイトのデフォルト値	はい	なし
VDI デスクトップスタンドアロン	はい	VDI のサイトのデフォルト値
VDI デスクトップテンプレート	はい	VDI のサイトのデフォルト値
テンプレートからの VDI デスクトップ	いいえ	なし
Azure Virtual Desktop のサイトのデフォルト値	はい	なし
Azure Virtual Desktop ホストプール - テンプレートからのホスト	いいえ	なし
Azure Virtual Desktop ホストプール - スタンドアロンホスト	はい	AVD マルチセッションホストのサイトのデフォルト値、または AVD シングルセッションホストのサイトのデフォルト値

Azure Virtual Desktop テンプレート	はい	AVD マルチセッションホストのサイトのデフォルト値、または AVD シングルセッションホストのサイトのデフォルト値
テンプレートからの Azure Virtual Desktop ホスト	いいえ	なし

追加情報

次の点に注意してください。

- 一部の最適化は、すでに適用されている場合は失敗に終わり警告が生成される可能性があります。
- OS の特性によっては、一部の最適化は失敗に終わり警告が生成される可能性があります。たとえば、UWP アプリの削除は、アプリがすでに存在しないため、失敗に終わる可能性があります。

ドライブリダイレクトのキャッシュ

このトピックでは、RAS RD セッションホスト、VDI、Azure Virtual Desktop、または Remote PC Agent を構成するダイアログで利用できる [ドライブリダイレクトのキャッシュを有効化] オプションについて説明します。このオプションが有効化されている場合、以下で説明するキャッシュのメカニズムがもたらす効果により、リダイレクトされたドライブでフォルダーを参照する速度が向上します。

ドライブリダイレクトを使用する場合、ネイティブの RDP ではファイルやフォルダーを列挙する際の効率性に劣り、ユーザーエクスペリエンスの反応速度が低下し、動作は重くなります。[ドライブリダイレクトのキャッシュを有効化] オプションを有効にすると、セッションホストによってカーネルベースのドライバー（RasRdpFs）が強制的に実行されます。これにより、標準的な RDP と比較して、通信が実行される方法が最適化され、セッションホスト（RDSH、VDI、または Azure Virtual Desktop）のフォルダー構造のキャッシュが追加されます。RAS Console の [適用] によって設定がセッションホストにプッシュされるとすぐに、ドライバーが起動されます。それ以降は、すべての新しいセッションでこの機能が有効化されます。既存のセッションでこの最適化を使用するには、再接続が必要です。

注記

- セッションホストは、64 ビットオペレーティングシステムを実行している必要があります。
- キャッシュはセッションごとであり、ドライバーメモリにページングされます。

- ログオフ時と切断時にキャッシュは消去されます。
- セッションでキャッシュされたフォルダーの数がしきい値を上回り、ユーザーがキャッシュされていない新しいフォルダーにアクセスした場合、最後にアクセスされたフォルダーとそのフォルダーがキャッシュで入れ替わります。
- このオプションがオフになると、現在アクティブなすべてのユーザーセッションはキャッシュを失います（ドライバーは停止され、キャッシュは消去されます）。この処理はユーザーには認識されませんが、ファイルとフォルダーの列挙は低速になります。
- このオプションがオンになっても、現在アクティブなすべてのユーザーセッションでキャッシュが自動的に有効化されることはありません。この機能を使用するには、既存のセッションを再接続する必要があります。

制限事項

- このオプションは、以下のバージョンの Parallels Client によって起動されたセッションにのみ適用できます。
  - Parallels Client for Windows 18 以降
  - Parallels Client for macOS 19 以降
- ネイティブ RDP と同じく、クライアント側（リモートセッション）で変更を加えた場合は、サーバー側のリダイレクトされたフォルダーで手動更新する（F5 キーを押す）必要があります。

ログの構成

RAS セッションホストは監視され、ログは関連情報を含めた状態で作成されます。ログを構成し、既存のログファイルを取得するかクリアする場合、ホストで右クリックし、コンテキストメニューで [トラブルシューティング] > [ロギング] を選択してから、希望に応じて [構成]、[取得] または [クリア] をクリックします。これらのタスクを実行する方法の詳細については、「ロギング」（p. 608）セクションを参照してください。

セッション（RD セッションホスト）の管理

「セッションの管理」（p. 329）を参照してください。

スケジューラー（RD セッションホスト）の使用

[RD セッションホスト] ビューの [スケジューラー] タブでは、スケジュールに従って各種のコマンドを実行できます。

新しいスケジューラータスクの作成または既存のスケジューラータスクの変更を行うには、次の操作を実行します。

1 RAS Console で、[ファーム] > <サイト> > [RD セッションホスト] に移動します。

2 右側のペインで、[スケジューラー] タブを選択します。

3 新しいタスクを作成するには、[タスク] > [追加] をクリックし、以下のオプションのいずれかを設定します。

- ホストを無効化
- ホストプールを無効化
- ホストを再起動
- ホストプールを再起動
- ホストを起動*
- ホストプールを起動*
- ホストプールをシャットダウン
- ホストプールをシャットダウン
- テンプレートからホストを再作成*
- テンプレートからホストプールを再作成*

*テンプレートベースのホストおよびホストプールにのみ適用されます。

[RDSH スケジュールプロパティ] ダイアログが開きます。このダイアログは、以下で説明する 3 つのタブから構成されています。

一般

[概要] タブで、以下を指定します。

- [スケジュールを有効化] を選択してスケジュール済みのタスクを有効にします。
- 名前と説明（オプション）指定します。

- [利用可能] リストで、対象のホストまたはホストプールを選択し、[追加] をクリックします（さらにホストまたはホストプールを追加する場合はこの操作を繰り返します）。すべてのサーバーを追加する場合は、[すべて追加] をクリックします。[対象] リストからサーバーを削除するには、[削除] または [すべて削除] をクリックします。

トリガー

[トリガー] タブで、スケジュール済みのタスクがトリガーされる条件を指定します。

- [日付]、[開始]、[期間] フィールドで、開始日、時間、期間を指定します。
- （ホストプールの再起動のみ）[完了までの時間] フィールドでタスクを完了するまでの時間を指定します。
- [繰り返し] フィールドにタスクの繰り返しについて指定します。[なし] を選択すると、タスクは 1 回のみスケジュールの通りに実行されます。[週の特定の曜日] を選択する場合、週の 1 つ以上の曜日を選択します。

オプション

[オプション] タブで、以下を実行できます。

- スケジュール済みタスクのトリガーの前後（特定のシナリオ）に、ユーザーに対して送信されるメッセージを作成します。メッセージの作成については、このサブセクションで後述します。
- 追加オプションを指定します。オプションは、後述の通りタスクのタイプによって異なることに注意してください。

タスクが [ホストを無効化] または [ホストプールを無効化] の場合、利用可能なオプションは

- [無効時の処理] です。このオプションを使用して、タスクがトリガーされた場合に、どのようなアクティブセッションが処理されるかを指定します。割り当てられたテンプレートでホストプールを無効にすると、ホストプールの RD セッションホストが空になり、削除されることに注意してください。「テンプレートに基づく RD セッションホストのメンテナンス」（p. 159）を参照してください。
- 現在非アクティブの RD セッションホストにスケジュールを適用する: このオプションは、上述のオプションで表示されるリストにアクティブなメッセージが存在する場合に限り、有効になります。オプションが有効化されている場合、現在オフラインの RD セッションホストもモニタリングされます。そのサーバーがスケジュール済みタスクの実行中にオンラインに戻ると、そのタスクも適用されます。

このオプションを有効にした場合、現在非アクティブの RD セッションホストにも、そのホストがオンライン状態に戻ったときにスケジュールが適用されます。このオプションが無効になっている場合（デフォルト）、そのようなサーバーにスケジュールが影響を与えることはありません。サーバーが無効化されている場合やネットワーク経由で到達できない場合（RAS Connection Broker に登録されたもの）、そのサーバーは非アクティブ（オフライン）とみなされることに注意してください。

タスクが [ホストをシャットダウン] または [ホストプールをシャットダウン] の場合、利用可能なオプションは

- 現在非アクティブの RD セッションホストにスケジュールを適用する: このオプションは、上述のオプションで表示されるリストにアクティブなメッセージが存在する場合に限り、有効になります。オプションが有効化されている場合、現在オフラインの RD セッションホストもモニタリングされます。そのサーバーがスケジュール済みタスクの実行中にオンラインに戻ると、そのタスクも適用されます。

  このオプションを有効にした場合、現在非アクティブの RD セッションホストにも、そのホストがオンライン状態に戻ったときにスケジュールが適用されます。このオプションが無効になっている場合（デフォルト）、そのようなサーバーにスケジュールが影響を与えることはありません。サーバーが無効化されている場合やネットワーク経由で到達できない場合（RAS Connection Broker に登録されたもの）、そのサーバーは非アクティブ（オフライン）とみなされることに注意してください。

タスクが [ホストを再起動]、[ホストプールを再起動]、[ホストをシャットダウン]、または [ホストプールをシャットダウン] の場合、利用可能なオプションは

- [ドレインモードを有効化] および [指定した時間の後にサーバーを強制的に再起動] となります。これら 2 つのオプションは組み合わせて使用できます。ドレインモードを選択した場合、次のように動作します。タスクがトリガーされると、サーバーへの新しい接続は拒否されますが、アクティブなセッションは引き続き実行され、再接続されます。すべてのアクティブなユーザーセッションが終了したとき、または指定した時間の後にサーバーを強制的に再起動の時間に到達したときのどちらか早い時点で、サーバーが再起動されます。アクティブユーザーの作業が失われることのないよう、ユーザーに対する作業を保存してログオフすることを促すメッセージを作成します（詳細は後述します）。「RD セッションホストのドレインモードの例」（p. 158）も参照してください。
- 現在非アクティブの RD セッションホストにスケジュールを適用する: このオプションは、[ドレインモードを有効化] オプションが選択されている場合に有効になります。オプションが有効化されている場合、現在オフラインの RD セッションホストもモニタリングされます。そのサーバーがスケジュール済みタスクの実行中にオンラインに戻ると、そのタスクも適用されます。

タスクが [ホストプールを起動] の場合、以下のオプションが利用できます。

- メンバーの割合: このオプションを選択して、各ホストプールで起動する必要のある RD セッションホストの割合を指定します。
- 開始するメンバーの数を指定: このオプションを選択して、各ホストプールで起動する必要のある RD セッションホストの数を指定します。

タスクが [テンプレートからホストを再作成] または [テンプレートからホストプールを再作成] の場合、以下のオプションが利用できます。

- 強制的にホストを再作成するまでの時間（ホストの場合）および強制的にホストプールを再作成するまでの時間（ホストプールの場合）: これらのオプションは、 [ドレインモードを有効化] オプションと連携して動作します（上記を参照）。 タスクがトリガーされると、サーバーへの新しい接続は拒否されますが、アクティブなセッションは引き続き実行され、再接続されます。すべてのアクティブなユーザーセッションが終了したとき、またはこれらのオプションで指定した時間に到達したときのどちらか早い時点で、サーバーが再作成されます。アクティブユーザーの作業が失われることのないよう、ユーザーに対する作業を保存してログオフすることを促すメッセージを作成します（詳細は後述します）。「RD セッションホストのドレインモードの例」（p. 158）も参照してください。

ユーザーに送信するテキストメッセージを作成するには、[タスク] > [追加] をクリックして、以下を指定します。

- [メッセージを有効化] オプションを選択して、メッセージを有効化します。オプションが選択されない場合、メッセージは保存されますが、ユーザーに送信されることはありません。[オプション] タブのリストでチェックボックスを選択したりクリアしたりすることでも、既存のメッセージを有効化または無効化できます。
- メッセージの件名と本文を指定します。ここで、ユーザーの画面に表示されるメッセージを設定します。
- [メッセージを送信] ドロップダウンリストで、メッセージの送信に指定する時間間隔を選択します。デフォルトではこれが、タスクがトリガーされる”前”の時間になります。ただし、[ホストを再起動] と [ホストプールを再起動] タスクの場合は、タスクが発生した”後”の時間になります（つまり、サーバーがドレインモードになります）。これは、スケジュール済みのタスクがすでに進行中でユーザーに対して異なる時間間隔で複数のメッセージを送信したい場合に活用できる有効な機能です。詳細については以下の説明を参照してください。

ユーザーに複数のメッセージを送信

[ホストを無効化] および [ホストプールを無効化] タスクでは、スケジュール済みのタスクがトリガーされる前に限りメッセージを送信できます。それで、メッセージを作成する場合に、メッセージを送信に指定するオプションに”前”のみを選択できます。必要に応じて、2 つ以上のメッセージを作成して、異なる時間間隔で送信できます。それでユーザーはタスク実行の前に、複数回通知を受け取ります。

[ホストを無効化] および [ホストプールを無効化] タスクでは、スケジュール済みのタスクがトリガーされる前または後にメッセージを送信できます。ドレインモードを有効化できるため、これらのタスクに”後”オプションを使用できます。これにより、場合によってはアクティブセッションの実行を維持できます。この時間中、複数のメッセージを送信して、アクティブユーザーに対し、作業を終了してセッションを閉じる必要があることをリマインドできます。”後”オプションを使用するには、[ドレインモードを有効化] オプションを選択する必要があります。”後”の時間間隔と [指定した時間の後にサーバーを強制的に再起動] の設定は、矛盾のないように構成する必要があります。たとえば、”後”の時間が経過する前に強制再起動が発生する場合、アクティブユーザーにメッセージが表示されることはありません。

RD セッションホストのドレインモードの例

例 1: ドレインモードなしでホストプールを再起動するようにスケジュールする

ホストプールには次の 3 つのホストが含まれています。A、B、C

- 日付: 2020/01/24
- 開始時刻: 午前 10:45
- メッセージを送信: 2 分前

ホストの再起動タスクがトリガーされる 2 分前に、アクティブなセッションを持つユーザーに通知が送信されます。

例 2: ドレインモードを有効にしてホストプールを再起動するようにスケジュールする

ホストプールには次の 3 つのホストが含まれています。A、B、C

- 日付: 2020/01/24
- 開始時刻: 午前 10:45
- ドレインモード: 有効

- 強制的にサーバーを再起動するまで後: 1 時間
- メッセージを送信: 2 分前、15 分後、30 分後。

ホストの再起動タスクがトリガーされる 2 分前にセッションユーザーに通知が送信されます。さらにタスクがトリガーされてから 15 分後と 30 分後にも通知が送信されます。ドレインモードが有効化されているため、ユーザーセッションは引き続き実行されます。つまりホストを再起動するまでメッセージの表示は可能であり、セッションを閉じることができます。強制再起動の時間が 1 時間に設定されているため、ユーザーは、タスクのトリガーから 30 分後に送信される最後のメッセージを確認することができます。

タスクがトリガーされたときの動作:

1 ホストでドレインモードが有効になります。

2 ホスト A と B にはアクティブなセッションや切断されたセッションが存在しないため、それらのサーバーは直ちに再起動されます。

3 ホスト C には、開いている/切断されたセッションがまだ存在するため、サーバー C は、すべてのユーザーがセッションを終了するまで引き続き実行されます。1 時間後にまだホストにアクティブなセッションがある場合、セッションは終了されサーバーが再起動されます。

テンプレートに基づく RD セッションホストのメンテナンス

テンプレートから作成された RD セッションホストに対してスケジュールされたメンテナンスを実行する必要がある場合、次の手順に従ってください。

1 メンテナンス期間に合わせて”ホストプールの無効化”スケジュールを作成し、割り当てられたテンプレートで RD セッションホストグループに適用します。

スケジューラーがグループを無効にする場合:

- グループ内のすべてのホストで、Agent のステータスを”無効（スケジューラー）”にして、ログオンステータスは”有効”のままにします。
- 新しいセッションが制限されます。
- 管理者が「無効」のオプションに”すべてのセッションのリセット”を指定した場合、セッションはログオフされますが、テンプレート化された RD セッションホストはグループから削除されません。

2 メンテナンス期間（またはその直前）にテンプレートをメンテナンスモードに切り替えます。その後で必要な変更を適用します。

3 メンテナンスモードの終了時にすべてのホストを再作成したい場合は、[グループ] タブで RD セッションホストグループを無効にする必要があります。これを行うには、グループ名の前（左側）にあるチェックボックスをオフにして、[適用] をクリックします。

グループ（a）を無効にする場合:

- ユーザーセッションが存在しないテンプレート化された RD セッションホストは、グループから削除（割り当て解除）されます。
- テンプレート化された RD セッションホストはどのグループにも属していないため、テンプレートのメンテナンスモードを終了する際に再作成できます。

4 テンプレートをメンテナンスから解放し、すべての複製を再作成するか尋ねられたら、[はい] をクリックします。

5 先に無効化していたグループを有効にします。この時点でグループは、[使用可能なバッファを維持] の設定に従い、再作成されたホストの受け取りを開始します。

6 この時点以降、グループは必要に応じて、更新済みのテンプレート化 RD セッションホストでプロビジョニングされるようになります。

高可用性のためのプラン

RD セッションホストをサイトに追加する際、N+1 の冗長性構成を使用して、ユーザーに提供するサービスが中断しないようにする必要があります。これは、Connection Broker、RAS Secure Gateway やプロバイダーなど、他の Parallels RAS コンポーネントにも当てはまります。

ログオンの管理

ログオン管理機能を使用すると、RD セッションホストからのログオンを有効または無効にすることができます。この機能は、`change logon` コマンドラインユーティリティと同じタスクを実行します。

注: テンプレートに基づく RD セッションホストの場合、ドレインモード（ログオンを無効化）はホストが属するグループにより自動的に処理されます。詳細については、「スケジューラーの使用」（p. 154）を参照してください。

ログオンを管理するには、次の手順を実行します。

1 Parallels RAS Console で、[ファーム] / <サイト> / [RD セッションホスト] に移動します。

2 RD セッションホストを選択し、[タスク] > [コントロール] をクリックして、次のいずれかを選択します。

- ログオンを有効化: コンソールからではなく、クライアントセッションからのログオンを有効にします。このオプションは、`change logon /enable` コマンドと同じアクションを実行します。
- ログオンを無効化: コンソールからではなく、クライアントセッションからのそれ以降のログオンを無効にします。現在ログオンしているユーザーには影響しません。このオプションは、`change logon /disable` コマンドと同じアクションを実行します。
- ドレイン: 新しいクライアントセッションからのログオンを無効にします。ただし、既存のセッションへの再接続は許可します。ドレインは、再起動後も管理者がログオンを許可するまで保持されます。

  なお、ホストがドレインモードになっている場合でも、管理者は物理コンソールにログオンすることができます。また、MSTSC の /admin や /console コマンドラインオプションを使って、リモートでログオンすることもできます。これにより管理者は、[ツール] > [リモートデスクトップ] 経由で、RDS ホストをリモートでメンテナンスできます。
- 再起動までドレイン: コンピューターが再起動するまで、新しいクライアントセッションのログオンを無効にします。ただし、既存のセッションへの再接続は許可します。ドレインはホストが再起動されるまで保持されます。`change logon /drainuntilrestart` コマンドと同じアクションを実行します。

RD セッションホストの現在のログオンコントロールモードを確認するには、[タスク] > [コントロール] をクリックします。チェックアウトされたオプションが、選択した RD セッションホストの現在のログオンコントロールモードを示します。この確認をコマンドラインから実行するには、ホストで `change logon /QUERY` コマンドを実行します。

次の点にも注意してください。

- ホストにログオンコントロールモードを適用する場合、Agent の状態がそれに従って更新されることを確認してください。
- ホストのログオンコントロールオプションは 1 つずつ設定する必要があります。ホストのグループに対してログオン制御オプションを設定する場合は、スケジューラーを使用できます（「スケジューラーの使用」（p. 154）を参照）。
- `/Drain` により新しいクライアントセッションからのログオンを無効にします。ただし、既存のセッションへの再接続は許可します。ドレインは、管理者の介入を必要とするのに対し

、 Drainuntilrestart は再起動後に自動的にログオンを可能にするという点で異なります。

- [コンピューターの構成] / [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] / [リモートデスクトップセッションホスト] / [接続] / [ユーザーがリモートデスクトップサービスを使ってリモート接続することを許可する] は [未構成] に設定されている必要があります。それ以外の場合、この設定が優先されます。

コンピューター管理ツールの使用

RAS Console から、RAS セッションホストをホスティングしているサーバーで標準的なコンピューター管理タスクを直接実行できます。このタスクには、リモートデスクトップ接続、PowerShell、コンピューター管理、サービス管理、イベントビューアー、IPconfig、再起動などが含まれます。[ツール] メニューにアクセスするには、ホストを選択して [タスク] をクリック（または右クリック）し、[ツール] をクリックして目的のツールを選択します。要件と使用方法については、「コンピューター管理ツール」（p. 569）を参照してください。

RD セッションホストからの公開

「公開」（p. 289）を参照してください。

「基本的な Parallels RAS ファームのセットアップ」セクション（p. 41）で説明した通り、[開始] カテゴリーの公開ウィザードを使用してリソースを公開することもできます。[開始] カテゴリーの公開ウィザードは簡易バージョンで、公開するリソースを選択するための使いやすいオプションが用意されています。どちらの方法を使用してもかまいません。ニーズに合った方法を選択してください。

公開済みリソースの表示

サイトから RD セッションホストまたは RD セッションホストグループを削除するとき、ホストまたはホストプール内のにホストされている公開済みリソースのリストを確認したい場合があります。この方法で、どのリソースが影響を受けているか確認できます。これは、次の方法で実行できます。

1 Parallels RAS Console で、[ファーム] \ [RD セッションホスト] を選択します。

2 特定の RD セッションホストの公開済みリソースを表示するには、[RD セッションホスト] タブを選択します。グループの公開済みリソースを表示するには、[グループ] タブを選択します。

3 ホストまたはホストグループを右クリックし、[公開済みのリソースを表示] を選択（または [タスク] > [公開済みのリソースを表示] をクリック）します。

4 [公開済みのリソース] ウィンドウが開き、選択したホストまたはホストプールの公開済みリソースのリストが表示されます。リソース情報には以下が記載されています。

- 名前: リソース名。
- ステータス。有効または無効。
- タイプ: "アプリケーション」 は、公開済みアプリケーション、URL、ネットワークフォルダーなどに使用されます。"デスクトップ" は公開済みデスクトップに使用されます。
- パス: 公開済みアプリケーションの場合は、実行ファイルへのパス、URL、または UNC パスを指定します。
- パラメーター: 公開済みアプリケーションのパラメーター（ある場合）。
- 公開元: サイト、ホストプール、またはホスト。

5 リストを更新するには、F5 を押すか、または [リサイクル] アイコン（右上）をクリックします。

6 リストをフィルタリングするには、Ctrl-F を押すか、または虫眼鏡アイコンをクリックしてから、希望する列にフィルターを指定します。

第　8　章

仮想デスクトップインフラ（VDI）

Parallels RAS VDI（仮想デスクトップインフラストラクチャ）では、ホストの仮想化を使用して、公開済みリソースをホストするために必要な物理ホストプールの数を減らすことができます。Parallels RAS VDI は、ハイパーバイザーやクラウドベースのプラットフォームなど、数多くの仮想化テクノロジーをサポートしています。

Parallels RAS VDI には、テンプレート機能も搭載されています。これは、事前に構成されたホスト（仮想マシン）からテンプレートを作成し、そこからホストと RD セッションホスト VM を自動的に複製する機能を備えています。

この章の内容

サポート対象のプロバイダー

Parallels RAS では、ハイパーバイザーベースのプロバイダーとクラウドベースのプロバイダーがサポートされています。

ハイパーバイザー

以下のハイパーバイザーがサポートされています。

- Microsoft Hyper-V（Windows Server 2012 R2 から Windows Server 2022 まで）

- Microsoft Hyper-V Failover Cluster（Windows Server 2012 R2 から Windows Server 2022 まで）
- VMware vCenter 6.5.0*、6.7.0*、7.x、8.0
- VMware ESXi 6.5.0*、6.7.0*、7.x、8.0
- SC//HyperCore 8.9、9.1
- Nutanix AHV（AOS 5.15、5.20、6.5 LTS）
- リモート PC - リモート PC のプールを作成できる特別なタイプです。「リモート PC プール」（p. 233）を参照してください。

* VMware は、2022 年 10 月 15 日に vSphere 6.5.0 および 6.7.0 のサポートを終了しました。これらのバージョンを Parallels RAS 19 で使用することは可能ですが、長期間のサポートを確保するために vSphere 7.0 へのアップグレードを推奨します。

クラウドプロバイダー

- Microsoft Azure
- Amazon ウェブサービス

プロバイダーの追加

このセクションでは、以下の内容を説明します。

- ハイパーバイザープロバイダーの追加（p. 168）
- クラウドプロバイダーの追加（p. 170）

RAS Provider Agent 情報

プロバイダー（ハイパーバイザーベースまたはクラウドベース）を RAS ファーム内で機能させるには、RAS Provider Agent がファームにインストールされている必要があります。RAS Provider Agent は、他の RAS コンポーネントとプロバイダーの間のインターフェイスとして動作します。RAS Provider Agent は、プロバイダーのネイティブ API によってプロバイダーとのすべての通信を統括します。

Parallels RAS には、ファームにインストールできる次の 2 種類の RAS Provider Agent があります。

- 組み込み: この RAS Provider Agent は、RAS Connection Broker に組み込まれており、Parallels RAS をインストールすると自動的にインストールされます。この Agent は、複数のプロバイダーを処理したり、高可用性向けに構成したりすることもできます。
- 専用: この RAS Provider Agent は手動でインストールされます。単一のプロバイダーのみ処理できます。複数のプロバイダーでこのエージェントタイプを使用する場合は、各プロバイダーに別のインスタンスをインストールする必要があります。

組み込みと専用の RAS Provider Agent はどちらも、Parallels RAS でサポートされるすべてのタイプのプロバイダーと互換性があります。どちらのエージェントをインストールするかは、ご自身の要件のみを考慮して選択できます。高可用性とビジネスの継続性のために、可能な限り常に組み込み Provider Agent を使用することが推奨されます。

次のセクションも参照してください。

- 組み込み RAS Provider Agent を使用するプロバイダーを追加する場合は、「プロバイダーの追加」（p. 165）に進んでください。
- 任意のホストに専用 RAS Provider Agent をインストールする場合は、次のセクション「RAS Provider Agent のインストールオプション」のセクション（p. 166）をお読みください。

RAS Provider Agent のインストールオプション

専用 RAS Provider Agent をインストールしている場合は、最初にインストールする場所を決定する必要があります。プロバイダーのタイプに応じて、以下のオプションが利用できます。

- ハイパーバイザーが動作しているホスト。このオプションは、Microsoft Hyper-V でのみ利用できます。
- 物理マシンまたは仮想マシンで動作している、サポートされているバージョンの Windows Server。サポートされている Windows Server バージョンについては、[ソフトウェア要件] > [RAS Provider Agent] を参照してください。

以下の表は、サポートされる各プロバイダーに対する RAS Provider Agent のインストールオプションのリストです。

プロバイダー	組み込み Agent（PA の一部）	プロバイダー上の Agent	Windows Server（VM または HW）上の Agent
Microsoft Hyper-V	はい	はい	はい*
Microsoft Hyper-V Failover Cluster	はい	いいえ	はい*

VMware VCenter	はい	いいえ	はい*
VMware ESXi	はい	いいえ	はい*
SC//HyperCore	はい	いいえ	はい*
Nutanix AHV（AOS）	はい	いいえ	はい*
リモート PC（下記の注を参照）	はい	いいえ	はい*
Microsoft Azure	はい	いいえ	はい*
Amazon ウェブサービス	はい	いいえ	はい*

* これらの Provider Agent インストールオプションでは、高可用性を利用できません。詳細については、「VDI の高可用性の実現」（p. 226）を参照してください。

注: リモート PC はリモート PC プールをホスト型デスクトップインフラ（HDI）の一部として作成および管理するために使用できる特別なタイプの PC です。このタイプのプロバイダーを追加すると、実際のプロバイダーのように管理できます。ただし、テンプレートの作成ができないことや、その他の VDI 固有の機能が使用できないことなど、いくらかの制限があります。このタイプを使用する場合の主要機能は、HDI ベースのリモート PC（HPE Moonshot System、Atrust Remote PC Array など）のプールを作成し、個々の PC を特定のユーザーに割り当てることで PC をパーシスタントにする機能です。詳細については、[リモート PC プール]（p. 233）を参照してください。

上の表で、使用しているプロバイダータイプを探し、RAS Provider Agent をインストールできる場所を確認します。利用できる選択肢に応じて、次のいずれかを実行します。

- 組み込み Agent: Agent は RAS Connection Broker の一部としてすでにインストールされています。高可用性とビジネスの継続性のために、可能な限り常に組み込み Provider Agent を使用することが推奨されます。
- プロバイダー上の Agent: このオプションは、Microsoft Hyper-V を使用している場合のみ利用できます。「プロバイダーの追加」（p. 165）で説明されているように、ホストにそのまま Agent をインストールできます。
- Windows Server（VM または HW）上の Agent: このオプションを使用する場合、サポートされているバージョンの Windows Server が実行されている物理マシンまたは仮想マシンがあることを確認します。ファームにプロバイダーを追加するときには、FQDN または IP アドレスを指定する必要があります。

ハイパーバイザープロバイダーの追加

このセクションでは、ハイパーバイザーベースのプロバイダー（p. 164）の追加方法について説明します。クラウドベースのプロバイダーの追加方法については、「クラウドプロバイダーの追加」（p. 170）を参照してください。

プロバイダーを追加するには、次の操作を実行します。

1 RAS Console で、[ファーム] > [サイト] > [プロバイダー] に移動します。

2 [プロバイダー] タブで [タスク] > [追加] をクリックし、追加したいプロバイダーを選択します。

3 [仮想化プロバイダーを追加] ウィザードが開きます。

4 [名前] フィールドで、プロバイダーの名前を指定します。

5 [説明] フィールドに、任意の説明を入力します。

6 [アドレス] フィールドで、ホストの FQDN または IP アドレスを指定します。SC//HyperCore では、複数のノードの IP アドレスを指定することができます。

7 ホストにログインするためのユーザー名とパスワードを指定します。

8 [認証情報を管理する] ボタンをクリックして、RAS Agent の展開に使用するアカウントを指定します。

9 [詳細設定] リンクをクリックして、[プロバイダー詳細設定] ダイアログを開きます。このダイアログでは、次のオプションを選択できます。

- 専用 Provider Agent の使用: RAS Provider Agent を自分でインストールする（またはインストールした）場合は、このオプションを選択します。組み込み RAS Provider Agent（p. 165）を使用する場合はオプションをクリアします。
- Agent アドレス: 上にあるオプションを選択すると、このオプションが有効になります。RAS VDI Agent がインストールされている（またはこれからインストールされる）ホストの FQDN または IP アドレスを指定します。物理ボックスまたは仮想マシンのいずれかを指定できます。
- 任意の Connection Broker: このプロバイダーの推奨 Agent にする RAS Connection Broker を選択します。詳細については、「VDI の高可用性の実現」（p. 226）を参照してください。

10 [次へ] をクリックします。

11 ここで、ウィザードは RAS Provider Agent に接続しようとします。前の（オプションの）ステップで [専用 Provider Agent の使用] オプションを指定したものの、まだ Agent をインストールしていない場合は、[インストール] をクリックし、手順に従って指定のホストに Agent をプッシュインストールします。

リモートインストールが機能するには、次の要件を満たす必要があります。

- ホストにファイヤーウォールを構成してプッシュインストールを許可する必要があります。標準の SMB ポート（139 および 445）が開いている必要があります。Parallels RAS が使用するポート一覧については、「ポート参照」を参照してください。
- SMB アクセス。管理共有（\\server\c$）にアクセスできる必要があります。シンプルファイル共有が有効になっている必要があります。
- Parallels RAS 管理者アカウントにはホストでリモートインストールを実行する権限が必要です。権限がない場合、権限があるアカウントの資格情報を入力するよう求められます。
- 対象ホストは AD ドメインへの参加が必要です。

何らかの理由でプッシュインストールを実行できない場合は、インストーラーを使用して手動でエージェントをインストールできます。「インストーラーを使用した RAS Provider Agent のインストール」（p. 185）を参照してください。

12 プロバイダータイプとして Microsoft Hyper-V Failover Cluster を選択した場合、ホストに対する MAC アドレス管理を無効化できるページが開きます。MAC アドレス管理の無効化は、Microsoft System Center Virtual Machine Manager（SCVMM）またはその他のソリューションを使用して MAC アドレスを管理している場合にのみ行います。詳細については以下の説明を参照してください。

Microsoft Hyper-V Failover Cluster をプロバイダーとして使用する場合は、MAC アドレスの管理が必要です。これは、MAC アドレス重複を避けるためです。ホストがクラスターの別のノードに移行され、MAC アドレスがリリースされて元のノードで再利用されると、MAC アドレスの重複が発生する可能性があります。そのような場合は、該当のホストをファームで管理できなくなります。Parallels RAS では、プロバイダーレベルで静的 MAC アドレスのプールを使用して、MAC アドレスを自動的に生成してホストに割り当てます。この方法により、ホストがクラスターの別のノードに移行された場合も、その MAC アドレスは別の VM で再利用されず、MAC アドレスの重複は発生しません。プールには、10,000 の予約済み MAC アドレスがあり、ウィザードページの [MAC アドレスの開始] フィールドと [MAC アドレスの終了] フィールドにその範囲が表示されます。

上で述べたように、すでに SCVMM またはその他のソリューションを使用して MAC アドレスを管理している場合は、[MAC アドレス管理の有効化] オプションをオフにします。

13 [次へ] をクリックします。

14 プロバイダーに [VMware vCenter] を選択した場合、別のページが開きます（他のホストタイプではこのページは開きません）。このページで、vCenter リソースプールを指定できます。これにより、クラスター（ルートリソースプール）またはクラスター内の個別のリソースプールを選択して、VM を列挙できます。リソースプールを選択するには、[指定のリソースプールを使用] オプションを選択してから、[リソースプール] フィールドの隣の [...] ボタンをクリックします。ダイアログが開いたら、希望のリソースプールを選択します。[指定のリソースプールを使用] オプションをクリアしたままにすると、すべての VM が vCenter クラスター全体から取得されます（最大数は 35,000）。完了したら [OK] をクリックします。

15 [完了] をクリックして、ウィザードを閉じます。

クラウドプロバイダーの追加

このセクションでは、クラウドベースのプロバイダー（p. 164）の追加方法について説明します。ハイパーバイザーベースのプロバイダーの追加方法については、「ハイパーバイザープロバイダーの追加」（p. 168）を参照してください。

Microsoft Azure

このセクションでは、以下の内容を説明します。

- 概要と前提条件（p. 170）
- Microsoft Entra ID アプリケーションの作成（p. 171）
- Microsoft Azure をプロバイダーとして追加（p. 175）
- Microsoft Azure とテンプレート（p. 176）

概要と前提条件

はじめに

Microsoft Azure を使用中または検討中の組織は、VDI および RD セッションホストのワークロードのプロビジョニング、スケーリング、管理を Parallels RAS Console から直接実行し、Azure Resource Manager（ARM）を使用して Microsoft Azure 上に展開できます。Parallels RAS は、Azure リソースに必要な権限（サブスクリプションとリソースグループ）を持つサービスプリンシパルを使用して、リソースの認証、プロビジョニング、管理を実行します。

前提条件

Microsoft Azure をプロバイダーとして使用するには、以下の条件を満たしている必要があります。

- 既存の Microsoft Azure アカウントとサブスクリプション。
- 必要な Microsoft Azure プロバイダーが有効化されていること（Microsoft.ResourceGraph、Microsoft.Resources、Microsoft.Compute、Microsoft.Network など）。
- AD サービスに接続可能な、選択したリージョン内の ARM 仮想ネットワークとサブネット。Microsoft Entra ID with Active Directory Domain Services（AADDS）、Azure IAAS 内またはハイブリッドのドメインコントローラー（オンプレミスドメインへの接続を使用できるもの）。
- ハイブリッド RAS 展開を使用する場合、サイト間 VPN または ExpressRoute が必要。
- VDI または RD セッションホストのテンプレートとして使用される、構成済みの VM。

Microsoft Azure をプロバイダーとして追加するには、以下の 2 つのステップがあります。

1. まず、サブスクリプション内のリソースにアクセスするアプリケーションを Microsoft Azure 内に作成する必要があります。このステップについては、「Microsoft Entra ID アプリケーションの作成」（p. 171）セクションで説明されます。
2. アプリケーションの作成と登録が完了したら、Parallels RAS Console 内で Microsoft Azure をプロバイダーとして追加できます。このステップについては、「Microsoft Azure をプロバイダーとして追加」（p. 175）で説明されます。

ここからは、上記のステップを実行する方法について説明します。

Microsoft Entra ID アプリケーションの作成

以下のステップを完了させるには、Microsoft Azure のサブスクリプションとアカウントが必要です。サブスクリプションを所有していない場合、先に購入しておく必要があります。

Microsoft Entra ID アプリケーションの作成

Microsoft Entra ID アプリケーションは、ロールベースのアクセス制御とともに使用されます。サブスクリプション内で Parallels RAS からリソースにアクセスするには、Microsoft Entra ID アプリケーションを作成する必要があります。

Microsoft Entra ID アプリケーションを作成するには

1 Microsoft Azure Portal にログインします。

2 ポータルメニューを開いて、[Microsoft Entra ID] を選択します。

3 左側のペインで、[アプリの登録] を選択します。

4 [新規登録] をクリックします（右側ペイン上部）。

5 [アプリケーションを登録する] ブレードが開きます。

6 [名前] フィールドに、アプリケーションに使用したい名前を入力します。

7 [リダイレクト URI（オプション）] セクションのドロップダウンリストで、[Web] が選択されていることを確認します。[URI] フィールドは空白のままにしておきます。

8 [登録] をクリックします（左下）。

9 新しい Microsoft Entra ID アプリが作成され、そのブレードがポータルに表示されます。

右側のペイン上部に表示される、アプリケーションの以下のプロパティをメモしておきます。

- 表示名
- [アプリケーション（クライアント）ID]*
- [ディレクトリ (テナント) ID] *
- [オブジェクト ID]*

* これらのプロパティをコピーして保存しておきます。後ほど RAS Console で Azure をプロバイダーとして追加するときにこれらを指定する必要があります。

クライアントシークレットの作成

クライアントシークレットは、トークンをリクエストするときにアプリケーションが ID の証明として使用する文字列です。実質的にはアプリケーションのパスワードとして動作します。Azure をプロバイダーとして追加するときに、RAS Console でこの文字列を指定する必要があります。

クライアントシークレットの作成方法:

1 アプリケーションページにいない場合、[ホーム] ページから[Microsoft Entra ID] > [アプリの登録] を選択し、右側のペインでアプリをクリックしてホームに移動します。

2 左側のペインで、[証明書とシークレット] を選択します。

3 右側のペインで、[新しいクライアントシークレット] を選択します。

4 クライアント名を入力し、希望する有効期限オプションを選択します。

5 [追加] をクリックします。[クライアントシークレット] リストに新しいクライアントシークレットが表示されます。

6 重要: クライアントシークレットをコピーして保存します（[値] 欄）。このページでシークレットをコピーしなかった場合、非表示になってしまい、後から取得することができなくなります。

リソースへの読み書きアクセス許可のアプリケーションへの付与

作成された Microsoft Entra ID アプリには、Azure リソースへの読み書きアクセス許可が必要です。以下の手順は、リソースグループの読み書きアクセス許可をアプリケーションに付与する方法を示したものです。特定のリソースへのアクセス許可や、Azure サブスクリプション全体へのアクセス許可を付与することもできます。詳細については、Microsoft Azure のドキュメントを参照してください。

新しい VM の配置先になるリソースグループへの書き込み許可をアプリに付与する場合:

1 Azure のポータルメニューで、[リソースグループ] を選択します。

2 新しい VM の配置先になるリソースグループをクリックします。

3 左側のペインで、[アクセス制御（IAM）] を選択します。

4 右側のペインで、[このリソースにアクセスを付与] ボックスを見つけて、[ロールの割り当てを追加] をクリックします。

5 [ロールの割り当てを追加] ページの [ロール] タブで [特権管理者ロール] を選択し、次に [コントリビューター] ロールを選択します。

6 [次へ] をクリックします。

7 [メンバー] タブで、[ユーザー、グループ、またはサービスプリンシパル] オプションを選択します。

8 [メンバーを選択] リンクをクリックし、[選択] フィールドに以前に作成したアプリケーションの名前を入力します。ドロップダウンリストでアプリケーションを選択し、[選択] をクリックします。

9 [次へ] をクリックします。

10 [レビューと割り当て] タブで、設定が正しいことを確認し、[レビューと割り当て] をクリックします。

アプリにリソースグループへの読み取りアクセス許可を付与する場合:

1 上のリストのステップ 1〜4 を繰り返します。

2 [ロールの割り当てを追加] ページの [ロール] タブで [ジョブ機能ロール] を選択し、次に [読者] ロールを選択します。

3 上のリストのステップ 6〜10 を繰り返します。

注: サブスクリプション全体への読み取り許可をアプリケーションに付与する（特定のリソースグループだけではない）場合、Azure のポータルメニューで [すべてのサービス] を選択してから、[カテゴリ] > [すべて] > [サブスクリプション] に移動し、サブスクリプションを選択します。中央のペインの [アクセス制御（IAM）] を選択し、[ロールの割当の追加] ボックスで [追加] をクリックします。上のリストのステップ 2〜4 を繰り返します。

Microsoft Azure サブスクリプション ID の確認

RAS Console で Microsoft Azure をプロバイダーとして追加する場合、Azure のサブスクリプション ID の指定が必要です。記憶していない場合、Microsoft Azure ポータルで次の方法によって確認できます。

1 ポータルメニューで [すべてのサービス] を選択します。

2 左側のペインで、 [カテゴリー] リストの [全般] をクリックします。

3 右側のペインで、[サブスクリプション] を選択します。

4 サブスクリプションをクリックしてから、[サブスクリプション ID] フィールドの値をコピーし、保存します。

概要

上記のステップを完了させると、RAS Console で Microsoft Azure をプロバイダーとして使用する準備のために以下の値が保存されているはずです。

- アプリケーション (クライアント) ID: アプリケーション ID。
- ディレクトリ (テナント) ID: テナント ID。
- クライアントシークレット: クライアントシークレット（アプリケーションキー）。
- サブスクリプション ID: Microsoft Azure サブスクリプション ID。

RAS Console で Microsoft Azure をプロバイダーとして追加する方法について、引き続きお読みください。

Microsoft Azure をプロバイダーとして追加

Microsoft Azure をプロバイダーとして追加するには、以下の操作を実行してください。

1 RAS Console で、[ファーム] > [サイト] > [プロバイダー] に移動します。

2 [プロバイダー] タブで、[タスク] > [追加] > [Microsoft Azure] をクリックします。

3 [クラウドコンピューティングを追加] ウィザードが開きます。

4 ウィザードで、以下の情報を指定します。

- 名前: プロバイダーの名前です。
- 説明: プロバイダーの説明です。
- 管理資格情報: Parallels Agent の展開に使用する管理者アカウントです。
- 認証 URL: Microsoft 認証サイトの URL が入力された状態になっています。変更が必要な場合や指示された場合を除き、デフォルト値のままにしておきます。
- 管理 URL: Microsoft 管理サイトの URL が入力された状態になっています。変更が必要な場合や指示された場合を除き、デフォルト値のままにしておきます。
- リソース URI: Microsoft Azure のリソース URI が入力された状態になっています。変更が必要な場合や指示された場合を除き、デフォルト値のままにしておきます。
- テナント ID: 先ほど作成した Microsoft Entra ID アプリの [ディレクトリ (テナント) ID] の値。
- サブスクリプション ID: 自分の Microsoft Azure サブスクリプション ID。
- アプリケーション ID: 先ほど作成した Microsoft Entra ID アプリの”アプリ（クライアント）ID”の値（p. 171）。
- アプリケーションキー: 先ほど作成した Microsoft Entra ID アプリの”クライアントシークレット”の値（p. 171）。

5 [詳細設定] リンクをクリックして、以下のオプション設定を構成できるダイアログを開きます。

- 専用 Provider Agent の使用: このオプションがクリアされている場合（デフォルト）、組み込みの RAS Provider Agent が使用されます。専用 RAS Provider Agent を使用する場合は、このオプションを選択し、ホストの FQDN または IP アドレスを指定します。
- Agent アドレス: 上にあるオプションを選択すると、このオプションが有効になります。RAS VDI Agent がインストールされている（またはこれからインストールされる）ホ

ストの FQDN または IP アドレスを指定します。物理ボックスまたは仮想マシンのいずれかを指定できます。

- 任意の Connection Broker: このプロバイダーの推奨 Agent にする RAS Connection Broker を選択します。詳細については、「VDI の高可用性の実現」（p. 226）を参照してください。

6 [次へ] をクリックします。ウィザードには新しいプロバイダーが表示され、RAS Provider Agent のステータスも確認できます。問題がなければ、[完了] をクリックしてウィザードを終了します。問題があれば、[戻る] をクリックし、必要に応じて間違いを修正します。

RAS Console の [プロバイダー] タブに、新しいプロバイダーが表示されます。次の手順に従って、プロバイダーの追加を完了させます。

1 [適用] をクリックして変更を適用します。

2 [ステータス] 列の値を確認します。[OK] 以外の値であれば、プロバイダーを右クリックし、[トラブルシューティング] > [Agent をチェック] を選択します。Agent のステータスを確認し、必要な場合はインストールしてから、[OK] をクリックします。[プロバイダー] タブの [ステータス] 列が [OK] になります。

プロバイダー構成の変更

プロバイダーの構成を表示し、変更するには、テンプレートを右クリックして [プロパティ] を選択します。開いたダイアログを使用して、プロバイダーのプロパティを表示し、変更します。

Microsoft Azure とテンプレート

Microsoft Azure 内での VM 複製用のテンプレートを作成するときには、VM クローンの作成先になる Azure リソースグループを選択する必要があります。Microsoft Entra ID アプリケーションにアクセスを許可したグループでなければならないことに注意してください。VM のサイズ、および複製された VM で使用するディスクの種類を選択する必要もあります。これらの設定は、[テンプレート作成ウィザード] の [詳細] ページで指定されます。

Virtual Desktop と RD セッションホストの両方のテンプレートを、Microsoft Azure をプロバイダーとして作成できます。複製された VM は、RAS Console に表示されます。同時に、Microsoft Azure ポータルにも表示されます。

注: 同じサブスクリプションを使用する複数の RAS インストールが存在する場合、回避方法として、Provider Agent アプリケーションの読み取りアクセスをサブスクリプションレベルからリソースグ

ループレベルまたはリソースグループのセットに変更することができます。このような操作は、Provider Agent が別の Provider Agent アプリケーションのリソースグループのセットと重なってしまう状況を回避するために必要です。

Microsoft Azure の仕様を含むテンプレートの作成と使用に関する包括的な情報については、テンプレートセクション（p. 192）を参照してください。

Amazon ウェブサービス

概要と前提条件

はじめに

Amazon ウェブサービス（AWS）は、最大手のクラウドプラットフォームプロバイダーであり、200 以上のフル機能のサービスを世界中のデータセンターから提供しています。Parallels RAS 19 は、Parallels RAS の既存の技術的機能に加えて、Amazon EC2 のワークロードを統合、構成、保守、サポートしたり、アクセスを確保したりする機能を提供します。

マルチセッション（RDSH）、シングルセッション（サーバーベース VDI）のサーバー OS、およびその他の Microsoft OS（ライセンスを保有している場合）をサポートしています。AWS での Microsoft オペレーティングシステムの使用に関する詳細については、https://aws.amazon.com/windows/faq/ を参照してください。

Parallels RAS Console には、以下のような機能があります。

- Amazon EC2 インスタンスの管理
- テンプレートの作成と管理
- インスタンスプールの作成と管理
- 自動スケーリングの構成
- スケジュールによるインスタンスの有効化、再起動、起動、シャットダウン
- イメージの最適化を構成
- FSLogix プロファイルコンテナーと MSIX app attach を使用
- インスタンスタイプ、ストレージタイプの変更

前提条件

- AWS のアカウント。まだアカウントをお持ちでない方は、aws.amazon.com/ec2/ で無料でアカウントを作成できます。
- Amazon EC2 のクローンインスタンスをドメインに参加させるための Microsoft Active Directory 環境が稼働している。
- 仮想プライベートクラウド（VPC）を仮想ネットワークとして事前構成済みで、セキュリティグループが EC2 インスタンスの仮想ファイアウォールとして機能している。
- Amazon EC2 インスタンスが事前構成済み（後で Parallels RAS テンプレートとして使用、Windows Server 2012 から Windows Server 2022 までの OS で動作）。

設計上の注意点

このセクションでは、Parallels RAS で AWS を使用する際に留意しておきたい設計上のアドバイスを紹介します。

DHCP オプションセット

テンプレートから作成された VM が Active Directory ドメインに参加できるように、AWS DHCP オプションセットを使用して、ドメインコントローラーを示すカスタム DNS の指定が必要になる場合があります。カスタム DNS が設定されていない場合、デフォルトの AWS パブリック DNS が使用され、VM はドメインコントローラーと通信することができなくなります。

DHCP オプションセットの設定方法については、
https://docs.aws.amazon.com/vpc/latest/userguide/DHCPOptionSet.html を参照してください。

ゲストエージェントがブロードキャストを使用してプロバイダーエージェントを検出するためには、プロバイダーエージェントとゲストエージェントが同じサブネット上に存在している必要があります。これが不可能な場合、Provider Agent の IP アドレスを含むレジストリ設定を VM に追加する必要があります: https://kb.parallels.com/en/124157?language=en。

サービスクォータ

ソリューションは、使用状況、呼び出し回数、インスタンス数などに応じて、スケーリングされます。このため、標準的な AWS のサービスクォータの制限に到達する場合があります。

AWS サービスクォータの詳細については、
https://docs.aws.amazon.com/general/latest/gr/aws_service_limits.html を参照してください。

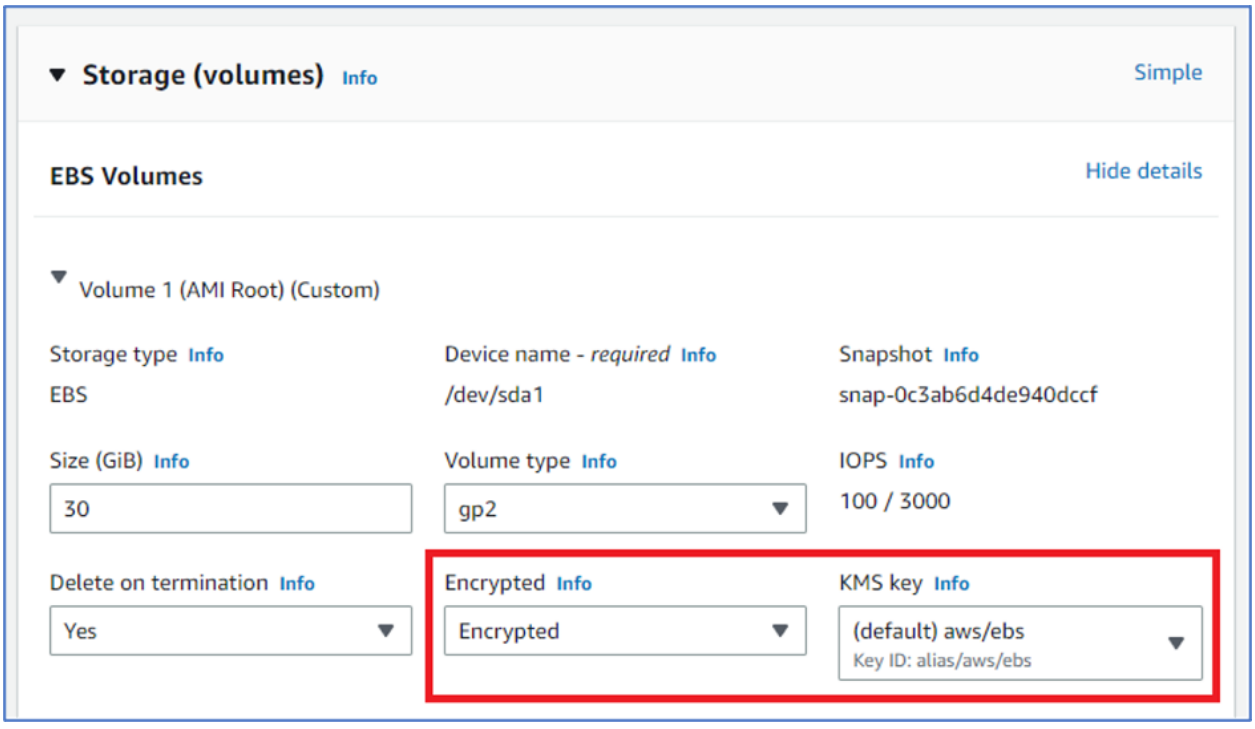
Parallels RAS 統合には、ここで指定された EC2 および EBS のエンドポイント制限が適用されます:

- https://docs.aws.amazon.com/general/latest/gr/ec2-service.html
- https://docs.aws.amazon.com/general/latest/gr/ebs-service.html

ストレージの暗号化

AWS 管理者が AWS Management Console で RAS テンプレートの VM ストレージの暗号化を有効にした場合、RAS テンプレートから作成したクローンのストレージは暗号化されます。

暗号化は、デフォルトで有効にするか、新しい EC2 VM を起動する際に明示的に有効にすることができます:



暗号化の詳細については、
https://aws.amazon.com/blogs/compute/must-know-best-practices-for-amazon-ebs-encryption/
を参照してください。

手順 1: プログラムアクセス用の IAM ユーザーの作成

IAM ユーザーアカウントを作成するには、AWS Management Console、AWS CLI、Tools for Windows PowerShell、AWS API 処理のいずれかを使用します。今回の例では、AWS Management Console を使用します。

1 AWS Management Console にサインインし、console.aws.amazon.com/iam にある IAM ページを開きます。

2 ナビゲーションペインで、[ユーザー] を選択し、[ユーザーを追加] ボタンをクリックします。

3 ユーザーの詳細を設定セクションで、「ParallelsConnector」などのユーザー名を入力します。

4 Parallels RAS Console は API を使用して AWS アカウントと通信するため、[AWS アクセスタイプ] 以下で、[アクセスキー] > [Programmatic access（プログラムによるアクセス）] を選択します。これにより、IAM ユーザーのアクセスキーが作成されます。完了のページに移動すると、アクセスキーを表示したりダウンロードしたりできます。[次へ] をクリックし、権限設定のページに進みます。

5 権限設定のページで、新しい IAM ユーザーが所属するユーザーグループを作成できます。これは必須ではありませんが、管理上の理由で推奨されています。

6 グループを使用しない場合は、[Attach existing policies directly（既存のポリシーを直接アタッチ）] を選択します。アカウント内の AWS マネージドポリシーとカスタマーマネージドポリシーのリストが表示されます。

7 フィルターポリシーで、事前構成済みの AWS マネージドポリシーである AmazonEC2FullAccess を選択し、[次へ] をクリックして次のページに進みます。

8 このページではオプションのタグを使用して、このユーザーのアクセスを整理、追跡、または制御することができます。

9 タグの用意ができたら、[次へ] をクリックすると、ここまでの選択がすべて表示されます。準備ができたら、[ユーザーを作成] をクリックします。

10 ユーザーのアクセスキー ID とシークレットアクセスキーを表示するには、表示したい各パスワードとアクセスキーの横にある [表示] をクリックします。アクセスキーを保存するには、[CSV をダウンロード] を選択し、ファイルを安全な場所に保存してください。

なお、シークレットアクセスキーを表示/ダウンロードできるはこのタイミングのみとなります。

11 ユーザーの新しいアクセスキー ID とシークレットアクセスキーを、次に Parallels RAS Console で使用するため安全な場所に保存します。

注: https://aws.amazon.com/blogs/security/how-to-rotate-access-keys-for-iam-users/ で説明されているように、セキュリティ上の理由から IAM ユーザーのキーを定期的に変更することが推奨されています。

手順 2 に進みます。AWS をプロバイダーとして追加する（p. 181）

手順 2: AWS をプロバイダーとして追加する

Amazon ウェブサービスをクラウドコンピューティングプロバイダーとして設定するには、次の操作を実行します。

1 RAS Console で、[ファーム] > [プロバイダー] に移動します。

2 [タスク] ドロップダウンメニューをクリックし、[追加] を選択します（または [+] アイコンをクリックします）。

3 メニューで、[Amazon EC2] を選択します。[クラウドコンピューティングプロバイダーを追加] ウィザードが開きます。

4 ウィザードで、以下の情報を指定します。

- 名前: プロバイダーの名前です。
- 説明: プロバイダーの説明です。
- 管理資格情報: セッションホスト（Amazon EC2 インスタンス）上の Parallels Agent の展開に使用する管理者アカウントです。現行の RAS 管理者はこのリストにすでに存在していますが、他のアカウントを使用することもできます。
- アクセスキー ID: アクセスキー ID です。
- 秘密アクセスキー: 秘密キーです。

5 [次へ] をクリックします。

6 Parallels RAS 設定の検証が完了するまで待機し、[次へ] をクリックします。

7 使用するリージョンを選択します。多くの場合、最適なリージョンは地理的に近い場所になります。また、[オプトインされたリージョン] オプションを選択してオプトイン AWS リージョンのいずれかを選択するか、[EC2 エンドポイント URL] オプションを選択してカスタム EC2 エンドポイント URL を指定することができます。

8 [完了] をクリックします。

9 「VDI テンプレートの作成」(p. 194) の説明に従って、テンプレートの作成に進みます。テンプレート作成時に、クローン用のインスタンスタイプや、ストレージのタイプ、サイズ、IOPS などを設定できます。また、[ファーム] > [RD セッションホスト] > テンプレートを右クリック > [プロパティ] からも実行できます。

VDI の管理

このセクションでは、Parallels RAS で VDI コンポーネントを管理する方法を説明します。

プロバイダー（VDI）の管理

このセクションでは、Parallels RAS でプロバイダーの構成を変更する方法を説明します。

プロバイダーを構成する

既存のプロバイダーを構成するには、次の操作を実行します。

1 RAS Console で、[ファーム] > [サイト] > [プロバイダー] に移動します。。

2 [プロバイダー] タブでプロバイダーを選択し、[タスク] > [プロパティ] をクリックします。[プロパティ] ダイアログが開きます。

注: 一部のホストでは、以下のいくつかのプロパティを利用できない場合があります。これはプロバイダーの種類によって変化します。

サイトでのプロバイダーの有効化/無効化

デフォルトで、プロバイダーは有効です。プロバイダーを有効または無効にするには、[全般] タブの [サイト内のプロバイダーを有効化] オプションを使用します。

プロパティ: プロバイダーの接続設定の構成

プロバイダーがハイパーバイザーベースかクラウドベースかによって、[全般] タブには異なるプロパティが表示されます。

ハイパーバイザープロバイダー:

- タイプ: プロバイダーの種類です。

- サブタイプ: ハイパーバイザーのバージョン。使用しているハイパーバイザのバージョンが含まれていない場合、[他:] を選択します。
- ホスト: プロバイダーの IP アドレスです。
- ポート: プロバイダーが受信接続を待機しているポート番号です。
- リソースプール: このフィールドは VMware vCenter の場合のみ有効です。プロバイダーの追加時に vCenter リソースプールを指定していた場合、ここにプールが表示されます。[...] ボタンを利用すると、異なるプールを指定できます（または、フィールドが空の場合にプールを選択できます）。ただし、これは、現在のプールからのホストが作成されていないか、いかなる方法でも Parallels RAS で使用されていない場合に限ります。Parallels RAS が現在使用されていることを検出すると、警告メッセージが表示され、変更することはできません。それでも別のリソースプールを選択したい場合は、RAS Console でフルクリーンアップを手動で行い、使用されているものが一切ない状態にする必要があります。
- 説明: オプションの説明。
- 専用 Provider Agent: 別のホストに専用 RAS Provider Agent がインストールされている場合は、このオプションを選択します。ホストの FQDN または IP アドレスを [Agent アドレス] フィールドに入力します。

クラウドベースのプロバイダー:

- タイプ: クラウドベースのプロバイダーの種類（例: Microsoft Azure）です。
- 名前: プロバイダーの名前です。
- 説明: オプションの説明。
- 資格情報: RAS Guest Agent のインストールに使用するアカウントの認証情報です。
- 専用 Provider Agent: 別のホストに専用 RAS Provider Agent がインストールされている場合は、このオプションを選択します。ホストの FQDN または IP アドレスを [Agent アドレス] フィールドに入力します。

Microsoft Azure に関連するその他のプロパティの説明については、「Microsoft Azure をプロバイダーとして追加」（p. 175）を参照してください。

資格情報: ユーザー名とパスワードの構成

プロバイダーがハイパーバイザーベースかクラウドベースかによって、[資格情報] タブには異なるプロパティが表示されます。

ハイパーバイザープロバイダー:

- プロバイダーにログインするためのユーザー名とパスワードを指定します。[認証情報をチェック] ボタンをクリックして、入力した認証情報を確認します。

クラウドベースのプロバイダー:

- 「Microsoft Azure をプロバイダーとして追加（p. 175）または「AWS をプロバイダーとして追加」 （p. 181）を参照してください。

詳細

[詳細] タブでは、プロバイダーの構成を実行して、現在使用していない VM に搭載されているマネージドディスクのタイプを標準 HDD に自動変更するよう設定できます。VM を起動すると、管理ディスクは自動的に元のタイプに変更されます。この機能により、VM の維持にかかるコストを削減することができます。

ディスクストレージのコスト最適化を有効化するには:

1. 一覧からプロバイダーを右クリックして、[プロパティ] を選択します。
2. プロバイダーの [プロパティ] ウィンドウで [詳細] タブを選択します。
3. [ディスクストレージコストの最適化を有効にする] オプションを選択します。
4. [ストレージコストの最適化を有効にする前のタイムアウトを設定] ドロップダウンリストで、必要なオプションを選択します。

MAC アドレス

このタブは、プロバイダーに Microsoft Hyper-V Failover Cluster を使用する場合にのみ表示されます。ホストの MAC アドレス管理を有効または無効にするために使用します。詳細については、「ハイパーバイザーホストの追加」（p. 168）を参照してください（MAC アドレス管理の構成手順の説明をお読みください）。

MAC アドレス管理は Parallels RAS 18 以降で利用できます。新規に Parallels RAS 18 をインストールする場合、この機能は、Microsoft Hyper-V Failover Cluster がプロバイダータイプとしてファームに追加されたときに、デフォルトで有効化されます。それ以前のバージョンの Parallels RAS の場合、この機能は、既存のプロバイダーに対して無効化されており、新しいプロバイダーを追加したときにデフォルトで有効化されます。

インストーラーを使用した RAS Provider Agent のインストール

デフォルトの場合 Provider Agent は、Connection Broker と一緒にインストールされます。ただし、Provider Agent を別のサーバーにインストールしたい場合や、何らかの理由で RAS Console からのプッシュインストールが実行できない場合は、この限りではありません。このような場合は、対象のサーバーで直接インストーラーを実行することで Agent をインストールできます。

注: この手順を使用できるのは、Windows に Provider Agent をインストールする場合のみです。

専用 Provider Agent をインストールするには、次の操作を実行します。

1 管理者アカウントを使用して Provider Agent をインストールするサーバーにログインし、他のすべてのアプリケーションを閉じます。

Parallels RAS の標準インストーラー（RASInstaller.msi）をサーバーにコピーし、実行します。

1 [インストールタイプの選択] ページが表示されたら、[カスタム] を選択し、[次へ] をクリックします。

2 [専用 RAS Provider Agent] をクリックし、ドロップダウンリストから [このコンピューターのローカルディスクにすべての機能をインストールします] を選択します。

3 他のすべてのコンポーネントで選択が解除されている（インストールから除外されている）ことを確認し、[次へ] をクリックします。

4 [インストール] をクリックし、画面上の指示に従って Agent をインストールします。

Provider Agent は構成を必要としません。インストールされたら、RAS Console に戻り、サーバー名を選択し、[トラブルシューティング] > [Agent をチェック] をクリックします。Agent が適切にインストールされている場合、ステータスは“Agent をインストールしました”に変わります。

サーバーから Provider Agent をアンインストールするには、次の操作を実行します。

1 スタートボタン > [コントロールパネル] > [プログラム] > [プログラムのアンインストール] に移動します。

2 インストールされているプログラムのリストから、[Parallels Remote Application Server] を見つけます。

3 サーバー上に保持する必要がある他の Parallels RAS コンポーネントがない場合、[Parallels Remote Application Server] を右クリックして [アンインストール] をクリックし

ます。手順に従って、プログラムをアンインストールします。この指示の残りの部分は省略できます。

4 サーバー上に保持する必要がある他の RAS コンポーネントがある場合、[Parallels Remote Application Server] を右クリックして [変更] をクリックします。

5 [ようこそ] ページで、[次へ] をクリックします。

6 [変更、修復、または削除] ページで [変更] を選択します。

7 次のページで [カスタム] を選択します。

8 [専用 RAS Provider Agent] を選択したら、前面のドロップダウンリストをクリックして、[すべての機能が利用できなくなります] をクリックします。

9 [次へ] をクリックして、ウィザードを完了します。

RAS Provider Agent のステータスの確認

RAS Provider Agent がインストールされていて正常に機能することを確認するには、次の操作を実行します。

1 最初に、[ファーム] > [サイト] > [プロバイダー] リストの [ステータス] 列を見ます。Agent で問題が発生している場合は、その列に該当する説明が表示されます。説明に加えて、[ステータス] 列では、色コードを使用して次のように Agent のステータスを示していることに注意してください。

- 赤 - 未確認
- オレンジ - アップデートが必要
- 緑 - 確認済み

2 ホストを右クリックして、コンテキストメニューの [トラブルシューティング] > [Agent をチェック] をクリックします。

3 [Provider Agent 情報] ダイアログが開き、Provider Agent、VDI サービスに関する情報やその他の関連情報が表示されます。

4 Provider Agent がインストールされていない場合は、[インストール] ボタンをクリックして、画面の指示に従います。詳細については、[RAS Provider Agent のインストールオプション]（p. 166）を参照してください。

複数のファームにおけるプロバイダーの使用

このトピックでは、複数の RAS ファームで同じプロバイダーを同時に使用する方法について説明します。問題と解決策をよりよく理解するために、仮に次のような例を考えてみましょう。

- 2 つの利用可能な仮想マシンを持つハイパーバイザーがあるとします。
- また、2 つのファーム（ファーム 1 とファーム 2）もあります。
- 第 1 のホストを使用してファーム 1 のリソースをホストし、もう 1 つのホストをファーム 2 のテンプレートとして使用することを計画しています。両方のホストはハイパーバイザー上で同時に実行されますが、各ホストはそれぞれのファームでのみ利用可能になります。

ここで問題となるのは、RAS Guest Agent は通常 1 つの RAS Provider Agent と通信できますが、各ファームにはそれぞれ独自の RAS Provider Agent があるため、このままではうまく機能しないことです。解決策は、ホストで実行している RAS Guest Agent が、1 つの特定の RAS Provider Agent のみを認識すると同時に、必要に応じて割り当てを変更できるようにすることです。

割り当ては Windows レジストリを介して行われます。VDI プールに属するすべてのホストとテンプレートから作成されたホストクローンは、RAS Provider Agent の名前またはアドレスを指定する新しい文字列値 `2XVDIAgent` を持つ必要があります。値を追加するには、次の手順に従います。

1. 仮想マシンで実行されている Windows にログインし、レジストリエディター（regedit）を開き、以下のキーを探します。
   - 32 ビットシステム: `HLKM\Software\Parallels\GuestAgent`
   - 64 ビットシステム: `HLKM\Software\WOW6432Node\Parallels\GuestAgent`
2. `2XVDIAgent` という名前の文字列値を追加します。値のデータは、次のように指定する必要があります。
   - 専用の RAS Provider Agent を使用する場合、値には、エージェントがインストールされているサーバーの FQDN または IP アドレスを設定してください。
   - 組み込みの RAS Provider Agent を手動で選択して使用する場合は、値に RAS Connection Broker の FQDN または IP アドレスを設定してください。
   - ビルトイン RAS Provider Agent を使用し、エージェントが自動的に選択される場合（高可用性）、文字列には、すべての RAS Connection Broker の FQDN または IP アドレ

スを、セミコロンで区切って含める必要があります（例: <PA1 アドレス>;<PA2 アドレス>;<PA3 アドレス>）。

手動エージェント選択シナリオ（上記の 2 番目の項目）でも、複数の Connection Broker の名前または IP アドレスを含められることに注意してください。このようにすれば、プロバイダーの推奨 Connection Broker を切り替えるたびに値を変更する必要はありません。

ホストプール（VDI）の管理

大量のホストを管理する場合、特に、ゲストを大規模の企業インフラストラクチャに実装する場合は、プールによって管理者の柔軟性が高まります。RAS Console では、プール管理の包括的な基盤を作成するのに必要なフレームワークとツールを利用できます。プールを管理するには、RAS Console で、[ファーム] > <サイト> > [VDI] に移動してから、[プール] タブをクリックします。

ホストプール（VDI）の追加

ホストプールを追加するには、次の操作を実行します。

1. RAS Console で、[ファーム] > <サイト> > [VDI ホストプール] に移動します。
2. [プール] リストの上にある [タスク] ドロップダウンリストをクリックして、[追加]（またはプラス記号アイコン）をクリックします。[VDI ホストプールを追加] ウィザードが開きます。
3. [サイト内のホストプールを有効化] を選択してホストプールを有効化します。新しいホストプールの名前と説明を指定します。
4. [次へ] をクリックします。
5. [プロビジョニング] ページで、このホストプールにテンプレートベースのホストを含めるか、スタンドアロンホストを含めるかを選択します。
   - テンプレート: ホストはテンプレートから動的に作成されます。次のステップ以降で、テンプレートを作成するか、既存のテンプレートを選択する必要があります。プロビジョニングタイプとして [テンプレート] を選択すると、均質なホストプールが確保されます。ホストプール全体で一貫したユーザーエクスペリエンスを提供するには、この選択を推奨します。
   - スタンドアロン: すでに存在する 1 つまたは複数のホストを選択します。これは、次のステップ、または後のステップでも行うことができます。ホストプールにホストを追加する前に、ホストがドメインに参加し、ドメイン環境のネットワークにアクセスできる

ことを確認してください。スタンドアロンプロビジョニングは、自動スケールなど、機能の一部が欠けているため、「管理対象外」とみなされることに注意してください。

6 プロビジョニングページ（前述）での選択内容に応じて、以下のいずれかを実行します。

- スタンドアロン: リストからホストプールに含めるホストを 1 つまたは複数選択します（後からプールにホストを追加することもできます）。
- テンプレート: リストからテンプレートを選択するか、[新規作成] をクリックして新しいテンプレートを作成してからテンプレートの設定を指定します。バージョン: 既存のテンプレートを選択した場合は、そのバージョンのいずれかを選択します。

7 [次へ] をクリックします。

8 （テンプレートのみ）[全般設定] ページで、次のオプションを指定します。

- テンプレート名: 選択してテンプレート名を入力します。
- 最大ホスト数: このテンプレートから作成できるホストの最大数を指定します。
- ウィザード完了時にデプロイされるホスト数: テンプレートが作成されたときに展開するホストの数。ホストは一度に 1 つずつ作成されるため、これには時間がかかることに注意してください。
- ホスト名: 新しいホスト名を指定するときに使用するパターン。

9 [次へ] をクリックします。

10 （テンプレートのみ）[設定] ページで、次のオプションを指定します。

- 使用可能なバッファを維持: このテンプレート用に、常に未割り当てでセッションが空いているホストの最小数です。空いているデスクトップと未割り当てのデスクトップの数が設定値を下回るとすぐに、このテンプレートから別のホストを強制的に作成します。テンプレートは、電源の初期状態を含め、ホスト作成のための独自の設定を使用します。
- 準備後のホストの状態: 準備が整ったホストに適用される電源状態を選択します。[使用中]、[停止中]、または [サスペンド] から選択します。電源状態が [停止中] または [サスペンド] に設定されている場合、実行中の（完全に準備が整い、受信接続を待っている）ホストの数は、[使用可能なバッファを維持] の設定（上記参照）によって制御されます。ホスト数の上限値が 200 に設定され、ウィザード完了時に展開されるゲストホストの数が 100 で、準備後の電源状態が“停止中”であるとします。このような構成の場合、100 の複製が展開され、停止中の状態になります。
- 未使用のホストの削除: リソースを節約するため、未使用のホストを処理する方法を選択します。削除しないように設定するか、削除されるまでの時間を指定します。

11 [次へ] をクリックします。

12 [ホストプールの設定] ページで、次のオプションを指定します。

- セッション: アクションがトリガーされるタイミングを選択します。
- アクションの実行: アクションを選択します。
- 経過時間: アクションが起動するまでの時間を選択します。

13 [次へ] をクリックします。

14 [ユーザープロファイル] ページで、[RAS で管理しない]（ユーザープロファイルは管理されません）または [FSlogix] から選択できます。Microsoft FSLogix プロファイルコンテナーを使用すると、パーシスタントでない環境でユーザーコンテキストを維持し、サインイン時間を最小限に抑え、互換性の問題を排除するネイティブプロファイルのユーザーエクスペリエンスを提供できるように構成されています。詳細な手順については、「ユーザープロファイル」（p. 138）を参照してください。

15 [次へ] をクリックします。

16 （スタンドアロンのみ）[最適化] ページで、最適化（p.146 を参照）を構成します。

17 [概要] ページでは、テンプレートの概要情報を確認します。必要に応じて、[戻る] ボタンをクリックして情報を修正できます。

18 最後に、[完了] をクリックしてホストプールを作成し、ウィザードを閉じます。

ホストプール（VDI）の削除

ホストプールを削除するには、次の操作を実行します。

削除するプールを右クリックして [削除] をクリックします（またはマイナス記号アイコンをクリックするか、[タスク] > [削除] をクリックします）。

ホストプールメンバーの追加および削除

VDI プールには、さまざまなタイプのメンバーを追加できます。メンバーとして、利用可能なすべてのホスト、特定のホスト、テンプレートから作成されたホストを指定できます。

メンバーをプールに追加する

メンバーをプールに追加するには、次の操作を実行します。

1 [ホストプール] リストでプールをダブルクリックします。

2 [メンバー] タブを選択します。

3 プラス（+）ボタンをクリックし、以下のリストからメンバータイプを選択します:

- プロバイダーのすべてのホスト: 特定のプロバイダーに配置されているすべてのホストです。このオプションをクリックすると、プロバイダーを選択できるようになります。

  注: Parallels はこのタイプを推奨していません。サポートされていない OS（Linux、HALB など）のホストが追加される可能性があるためです。このタイプを使用する必要がある場合は、注意深く操作を行うか、または適切なホスト名を含むワイルドカード（p. 192）を使用してください。

- ホスト: ホストに配置されている特定のゲスト。このオプションをクリックすると、リストからホストを選択できるようになります。
- リソースプール: ハイパーバイザー内でプールとしてネイティブに構成されたホストのグループ。ハイパーバイザーでは、プールに関して別の用語（リソースプールなど）を使用する場合があります。このオプションをクリックすると、リストからリソースプール（利用可能な場合）を選択できるようになります。
- テンプレート: テンプレートから自動的に作成されるホスト。このオプションをクリックすると、テンプレートを選択できるようになります。テンプレートの詳細については、「テンプレート」（p. 192）を参照してください。

4 上記のメニュー項目の 1 つをクリックすると、利用可能なホストまたはテンプレートのリストが表示され、それらを選択できます。

注: メンバーの重複の問題を回避するために、任意のプールに同じタイプのメンバーのみが含まれるように設定できます。たとえば、指定のホストでプールに追加した最初のメンバーがホストの場合、追加のメンバーをすべてホストにするよう設定できますが、テンプレート、リソースプール、全ホストに設定することはできません。異なるタイプのメンバーを使用する場合は、各メンバータイプに対して別のプールを作成する必要があります（ホスト用に 1 つのプール、テンプレート用に別のプールを作成するなど）。この要件は、最初のメンバーをプールに追加してからメンバータイプの選択を無効にすることにより、UI に適用できます。

ホストプールかメンバーを削除する

ホストプールからメンバーを削除するには、次の操作を実行します。

1 [ホストプール] リストでプールをダブルクリックします。

2 [メンバー] タブを選択します。

3 削除するプールメンバーを選択します。

4 マイナス（-）ボタンをクリックします。

メンバーがホストプールから削除されると、そのメンバーは削除されます。

ワイルドカードの使用による VM のフィルタリング

[プール] タブの下部にある [ワイルドカード] 入力フィールドを使用して、ユーザーが利用できるホストを示すワイルドカードを指定できます。VM の名前がワイルドカードと一致すると、その VM が利用可能になります。一致しない場合、ユーザーはそのゲストを使用できません。ワイルドカードを指定するには、アスタリスク演算子（*）を使用します（例: ABC*、*ABC*）。

プールでのホストの管理

プールに属するホスト（および他のホストやデスクトップ）は、[VDI] > [デスクトップ] タブで管理します。このタブでは、標準的なデスクトップ管理操作すべてを [タスク] メニューから実行できます。再作成、削除、全 Agent の更新、割り当て、割り当て解除、セッションの表示、開始、停止、再起動、サスペンド、リセットなどを実行できます。再起動操作（猶予）には 10 分間のタイムアウトがあります。この時間内に操作が完了しない場合は、リセット操作（強制）となります。

デフォルトでは、[デスクトップ] タブには、ファーム内で利用可能なすべてのデスクトップが表示されます（利用可能なすべてのデスクトップを表示するには、リストのスクロールが必要な場合があります）。特定のプールに属するホストだけを表示するには、[プール] タブでプールを選択し、[タスク] > [プール内のホストを表示する] をクリックします。これにより、[デスクトップ] タブに切り替わります。このタブでは、選択されたプールに属する VM だけが表示されるよう、自動的に絞り込まれています。

テンプレート（VDI）の管理

テンプレートは、Parallels RAS でホストの作成と展開を自動化するために使用されます。テンプレートは、Parallels RAS でサポートされるいずれかのハイパーバイザーを使用して作成された既存の仮想マシンに基づきます。テンプレートの準備ができたら、それを使用して、テンプレートのプロパティをすべて継承する複製（ホスト）を作成できます。作成されたホストは、公開済みのリソースをホストするために使用できます。

以下のトピックでは、テンプレートを作成し、使用する方法を説明します。

Virtual Desktop テンプレート

Virtual Desktop テンプレートは、Parallels RAS VDI の重要な部分です。デスクトップ、アプリケーション、ドキュメントなどを公開するためのホストを作成するために使用されます。ゲスト OS サポートは、RAS Guest Agent（VM でインストールする必要があります）のサポートと同じです。「ソフトウェア要件」（p. 30）を参照してください。

バーチャルデスクトップテンプレートから作成されたホストは、通常、シングルユーザーとして機能します。ホストは、パーシスタント VM の作成、VDI セッションの管理、特定の Virtual Desktop テンプレートからのリソースの公開、などの機能を備えた RAS VDI 内から完全に管理されます。

マルチプロバイダーのテンプレート配信

テンプレートを作成すると、通常は単一のプロバイダーによって管理されます。このプロバイダーは、ソースとなる仮想マシンが属するプロバイダーと同じです。複製がテンプレートから展開され、テンプレートの作成に使用されたプロバイダーと同じプロバイダーで実行されます。複製されたホストは、通常はストレージエリアネットワーク（SAN）などの一元化された共有ストレージに保存されます。

Parallels RAS 18 から、管理者はテンプレートを作成し、そのテンプレートを複数の Microsoft Hyper-V ホストに配信できるようになりました。その結果、Parallels RAS Console に表示されるテンプレート構成は、複数の Microsoft Hyper-V ホストで共有され、各ホストのローカルストレージには、テンプレートの独自コピーが配置されます。これにより、複製を一元化された共有ストレージだけでなく、複数の独立した Microsoft Hyper-V ホストのローカルディスクにも展開できます。必要な数の Microsoft Hyper-V ホストをテンプレート配信リストに追加することで、簡単にスケールアウトを実行できます。

テンプレート配信は、[Parallels テンプレートの作成ウィザード]（次のサブセクションで説明）の [配信] ページで構成します。テンプレート配信機能を使用する予定がある場合は、ウィザードを実行する前に、以下の「前提条件」サブセクションをお読みください。

マルチプロバイダーのテンプレート配信の管理について詳しくは、「マルチプロバイダーのテンプレート配信の管理」（p. 214）も参照してください。

前提条件

- テンプレート配信は、スタンドアロンの Microsoft Hyper-V Server 2012R、2016、2019、2022 でサポートされます。

- すべてのターゲットプロバイダーでは次の項目が同一でなければなりません。

  - プロバイダーのタイプとサブタイプ。

  - ホストが配置されるフォルダーのパス。

  - ホストが接続される仮想スイッチの名前。

- Hyper-V ホストは、ドメインに参加している必要があります。現在の実装では、テンプレートの完全な VM コピーを使用して、Hyper-V ライブマイグレーションの仕組みによって、テンプレートを他のホスト（ローカルストレージ）に配信しています。

  注: 完全な複製も、ライブマイグレーションを使用して他のホストに移行できますが、プロセスには時間がかかります（テンプレートの初回コピーと同程度）。

- ソースとなる VM をホストする Microsoft Hyper-V サーバーをターゲットホストとして使用することもできます。

- テンプレートを配信して複製を作成するターゲットホストを選択する前に、利用可能なストレージ領域が十分にあることを常に確認してください。

- Hyper-V 設定では、次のように Kerberos 認証が有効化されており、適切な委任が AD で構成されている必要があります。

  - ホストマシンの [Hyper-V の設定] に移動し、Kerberos を使用したライブマイグレーションを有効にします。

  - [Active Directory ユーザーとコンピューター] に移動し、各 Hyper-V ホストサーバーで、移行先と移行元のすべてのサーバーで“cifs”および“Microsoft Virtual System Migration Service”の委任を有効にします。

注: 認証が機能しない場合は、[任意の認証プロトコルを使う] オプションを変更してみてください。

VM テンプレートの作成

要件

このセクションで説明する作業を実行するには、次の要件を満たす必要があります。

- ハイパーバイザーベースのホストの場合は、ホストにハイパーバイザーツールがインストールされ、実行中であることを確認してください。

- VM に Agent ソフトウェアをプッシュインストールできるアカウントの認証情報がわかっていることを確認します。このような認証情報（ドメイン管理者など）を使用して Parallels RAS Console を実行する場合、Agent のインストール中に認証情報の入力は求められませ

ん。他のアカウントを使用してコンソールを実行する場合は、Agent をインストールするときに認証情報を入力するよう求められます。

- VM で動作しているゲスト OS（Windows）は、DHCP サーバーから IP アドレスを取得するように構成する必要があります。
- ユーザーがホストで公開済みのリソースにアクセスする場合、RDP ポートがローカルに、または VM で動作している Windows のグループポリシー経由で開いている必要があります。デフォルトの RDP ポートは 3389 です。
- RD セッションホストテンプレートの場合、Network Discovery UDP ポート 137 をゲスト OS のドメインファイアウォールプロファイルで有効にする必要があります。これは、ドメイングループポリシーにより、またはゲスト OS で手動で実行できます。

手動でエージェントをインストール

通常、Parallels RAS Console から直接ソース VM で必要な Agent ソフトウェアをプッシュインストールします（このセクション後半で説明します）。ただし、VM の Windows で Parallels RAS インストーラーを実行して手動でソフトウェアをインストールすることもできます。その際、Custom インストールオプションを使用し、RAS Guest Agent を選択して、ソース VM にインストールします。

テンプレートの作成

テンプレートの作成を開始するには、次の操作を実行します。

1. RAS Console で、[ファーム] > <サイト> > [VDI] に移動します。
2. 右側のペインで [テンプレート] タブを選択します。
3. [タスク] ドロップダウンリストで [追加] をクリックします（または [+] アイコンをクリックします）
4. ダイアログが開いたら、テンプレートの作成元になるホストを選択し、[OK] をクリックします。
5. [Parallels テンプレートウィザードを作成] が開きます。各ウィザードページは、画面に表示される順序に従って、下で説明されています。
6. エージェントがインストールされていることを確認し、必要であれば手順 1: の説明に従って手動でインストールします。Agent のチェックとインストール（p. 196）。この手順は、オンプレミスのプロバイダーを使用する場合にのみ表示されます。

7 手順 2: の説明に従ってテンプレートを構成します。「テンプレートの構成」（p. 197）に進みます。

手順 1: Agent のチェックとインストール

この手順は、オンプレミスのプロバイダーを使用する場合にのみ表示されます。Azure Virtual Desktop およびクラウドプロバイダーでは表示されません。

この手順では、選択された VM に RAS Guest Agent がインストールされているかどうかを確認します。チェックの終了を待ち、[ステータス] フィールドを調べます（ページの下部近く）。結果に応じて、次のいずれかを実行します。

- Agent がインストールされている場合は、[次へ] をクリックして、続行します。ここで読むのをやめ、手順 2: 「テンプレートの構成」（p. 197）に進みます。
- Agent がインストールされていない場合は、下記のようにインストールする必要があります。

Agent をインストールするには、最初に [Guest Agent 展開設定をカスタマイズする] リンクをクリックし、ダイアログが開いたらオプションを指定します。強制されるオプションはありません。必要に応じて、オプションを選択またはクリアします。テンプレートタイプにより、下記のようにオプションが異なることに注意してください。

仮想デスクトップ:

- ファイアウォールルールを追加する: ホストで自動的にファイアウォールルールを構成します。
- リモートデスクトップ接続を許可する: VM でリモートデスクトップアクセスを自動的に構成するように選択します。
- リモートデスクトップユーザーグループに追加するユーザーまたはグループを指定: このオプションを選択し、[+] アイコンをクリックして、特定のユーザーをグループに追加します。

RD セッションホスト:

- ファイアウォールルールを追加する: ホストで自動的にファイアウォールルールを構成します。

> **注:** 別のステップで、Network Discovery UDP ポート 137 をゲスト OS のドメインファイアウォールプロファイルで有効にする必要があります。これは、ドメイングループポリシーにより、またはゲスト OS で手動で実行できます。

- RDS 役割をインストール: ホストに RDS の役割をインストールします。
- デスクトップエクスペリエンスを有効にする: Windows でデスクトップエクスペリエンス機能を有効にします。
- 必要な場合にサーバーを再起動: 必要な場合は VM を再起動します。
- リモートデスクトップユーザーグループに追加するユーザーまたはグループを指定: このオプションを選択し、[+] アイコンをクリックして、特定のユーザーをグループに追加します。

オプションの指定が完了したら、[OK] をクリックしてダイアログを閉じます。

次に、[インストール] ボタンをクリックし、画面上の指示に従って、Agent ソフトウェアをインストールします。

ヒント: ホスト名として指定された名前でホストにアクセスできない場合は、ホスト名をダブルクリックして、正しい IP アドレスに変更します。

完了したら、[Agent をチェック] ウィザードページの [ステータス] フィールドを見て、Agent がインストールされていることを確認します。インストールされている場合は、手順 2: について説明している次のセクションに進みます。「テンプレートの構成」（p. 197）に進みます。

手順 2: テンプレートの構成

Agent がインストールされ、[Agent をチェック] ウィザードページの [ステータス] フィールドでインストールが確認できたら、[次へ] をクリックします。VM の電源がオフになります（電源オフ動作が完了するのを待ちます）。VM の電源がオフになったら、テンプレート構成の手順が開始します。

ウィザードの後続のページについては、この後のセクションで説明します。ウィザードのページの多くは、サイトのデフォルト設定の情報を継承していますが、必要に応じて上書きできます。独自の設定を指定するには、[デフォルト設定を継承] オプションをオフにします。デフォルト設定を確認し、編集するには、[デフォルトを編集] リンクをクリックします。詳細については、「サイトのデフォルト値」（p. 228）を参照してください。

プロパティ

[概要] ページで、次のオプションを指定します。

- テンプレート名: 選択してテンプレート名を入力します。

- 複製方法: リンク済みの複製を作成するか、完全複製を作成するか。完全複製は、テンプレートの完全なコピーです。そのため、ソーステンプレートと同じ程度の物理ハードドライブの領域を占有し、作成にも膨大な時間がかかります。リンククローンは、仮想ディスクをソーステンプレートと共有するスナップショットから作成されたテンプレートのコピーです。そのため、使用される物理ハードドライブの領域は少なく、わずか数分で作成されます。

  アプリケーションと OS アップデートが遅い場合は、完全複製を使用する必要があります（完全複製は作成に時間がかかりますが、最高のパフォーマンスが得られます）。それ以外の場合は、アップデートの速度が十分であれば、作成にかかる時間が大幅に短いため、リンク済みの複製を使用します。

注: [リンク複製を作成] オプションがグレーアウトされている場合は、現在のバージョンまたは Parallels RAS が、使用しているプロバイダーによるリンク複製をサポートしないことを意味します。この文書の作成時点では、リンク済みの複製のサポートは、VMware、Microsoft Hyper-V、SC//HyperCore および AHV（AOS）で利用できます。

- （Microsoft Azure のみ）可用性セット: Microsoft Azure 可用性セットを選択します。

配信

このページは、複数の Microsoft Hyper-V ホストへのテンプレート配信を構成するために使用します。このページは、ソース VM が Microsoft Hyper-V マシンの場合にのみ表示されます。この機能と要件の説明については、「マルチプロバイダーのテンプレート配信」（p. 193）を参照してください。

テンプレート配信を構成するには、以下の手順を実行します。

1. [マルチプロバイダーのテンプレート配信を有効化] オプションを選択します。
2. [利用可能] リストで、1 つまたは複数のプロバイダーを選択し、[追加] をクリックします（または [すべて追加] をクリックして利用可能なプロバイダーをすべて追加します）。このリストには、ソースとなる VM と同じタイプとサブタイプのプロバイダーのみが表示されます。
3. [同時配信の対象となるプロバイダーの数] フィールドで、同時配信操作の数を指定します。Hyper-V ライブマイグレーションを使用して、テンプレートがターゲットホストに配信されます（仮想マシンがまずファイルにエクスポートされ、次にそのファイルが移行先ホストに移行されます）。[対象] リストの各ホストで、ライブマイグレーションの操作を実行する必要があります。ここで指定した数は、同時に開始するネットワークコピー操作の数を示しています。この数が大きいほど、必要になるネットワークリソースが多くなります。仮想マシンのエクスポート（ライブマイグレーションの最初のステップ）は、常に 1 度に 1 つの VM で実行されるため、ここで指定する数が影響を与えるのはコピー操作のみです。

注: テンプレートが作成された後に、[マルチプロバイダーのテンプレート配信を有効化] 設定を変更（選択または選択解除）することはできません。オンまたはオフにする（機能を有効または無効にする）ことを後で決定する場合は、テンプレート全体を削除して再度作成する必要があります。ただし、プロバイダーを既存のテンプレートに追加したり、既存のテンプレートから削除したりすることは可能です。

完了したら、[次へ] をクリックしてウィザードの次のページに進みます。

追加情報

マルチプロバイダーのテンプレート配信の管理（p. 214）

詳細設定

[詳細] ページのプロパティは、プロバイダーのタイプによって異なります。相違点について、以下で説明します。

ハイパーバイザーベースのプロバイダー:

- クラスター共有ボリューム（CSV）、ネットワーク共有: Hyper-V Failover Cluster を使用している場合は、この 2 つのオプションが表示されます。ホストが作成されるストレージのタイプを選択できます。任意のオプションを選択して、編集するフィールドの隣にある [...] ボタンをクリックします。選択したオプションに応じて、クラスター共有ボリュームまたはネットワークフォルダーを指定します。共有フォルダーは SMB 3.0 と互換性を持っている必要があります。また、プロバイダーとして Microsoft Hyper-V ホストを登録するために使用した資格情報と同じものを使用して、ホストの SMB ファイル共有にアクセスします。

  以下に重要な注意点がありますのでこちらもお読みください。

  注: この機能を使用するには、Windows PowerShell を使用して、SMB の制約付き委任（リソースベース）を設定する必要があります。重要: Windows Server 2012 フォレスト機能レベルが必要です。

  Windows 2012 R2 以降を実行中のサーバーで、PowerShell を使用して Active Directory PowerShell モジュールをインストールします。Hyper-V ホストや SMB ファイルサーバーでは、このモジュールは必要ありません。

  次のコマンドレットを実行します。

  ```
  Install-WindowsFeature RSAT-AD-PowerShell
  ```

  Hyper-V クラスターのすべてのノードのファイルサーバー（クラスター）で、SMB の委任を行います。たとえば、4 ノードの Hyper-V クラスターを実行中で、仮想マシンのストレージにスケールアウトしたファイルサーバーのクラスター FS-CL01 を使用する場合は、以下を実行します。

```
Enable-SmbDelegation - SmbServer FS-CL01 - SmbClient Hyperv-01
Enable-SmbDelegation - SmbServer FS-CL01 - SmbClient Hyperv-02
Enable-SmbDelegation - SmbServer FS-CL01 - SmbClient Hyperv-03
Enable-SmbDelegation - SmbServer FS-CL01 - SmbClient Hyperv-04
必須: 次のように、適用した設定（実際の委任）を確認します。
Get-SmbDelegation - SmbServer FS-CL01
```

- フォルダー: このオプションは、Hyper-V、VMware VCenter、または AHV（AOS）を使用している場合に利用できます。ホストを作成するフォルダーを指定します。
- LAN アクセスに、別のネットワークインターフェイスを使用します: このオプションは、Hyper-V または VMware プロバイダーのいずれかを使用している場合に利用できます。Connection Broker と Provider Agent が使用するネットワークインターフェイスを指定します。これは、テンプレートに複数のネットワークインターフェイスがあり、Parallels RAS との通信に特定のインターフェイスを使用したい場合に便利です。このオプションを選択した場合、以下の要素も指定する必要があります。
  - アドレス: ネットワークインターフェイスの IP アドレスです。
  - サブネットマスク: IP アドレスのサブネットマスクです。
- リソースプール: VMware リソースプールを指定します。
- 物理的ホスト: VMware vCenter を使用している場合に利用できます。ホストを作成する物理ホストを指定します。
- ハードウェアアクセラレーショングラフィックのライセンスサポートを有効化: このオプションは、VMware vCenter または VMware ESXi を使用している場合に利用できます。このオプションを使用すると、vGPU が有効なホストで、シャットダウン時に vGPU ライセンスの登録をライセンスサーバーから解除できます

Microsoft Azure プロバイダー:

- リソースグループ: VM の複製先になる Azure リソースグループを選択します。Microsoft Entra ID アプリにアクセスを許可したグループでなければならないことに注意してください。詳細については、「Microsoft Entra ID アプリケーションの作成」（p. 171）を参照してください。
- サイズ: 複製された VM に使用する VM のサイズを選択します。
- OS ディスクの種類: 複製された VM に使用するディスクの種類を選択します。

準備

[準備] ページを使用して、イメージの準備ツールを選択し、構成できます。

注: このページでプロパティを指定する際、これらの情報はローカルマシンのパーソナル構成ファイルに保存されます。次回に別のテンプレートを作成する場合、ここにあるフィールドは最後に使用した値を使用して自動的に入力されます。

最初に、RASprep と Sysprep のどちらを使用するかを選択します。RASprep を使用する利点と 2 つのツールの違いは下記で説明されています。

RASprep は、ベースイメージから VM を複製した後、VM で Windows を準備する Parallels RAS ツールです。RASprep は、各新規 VM の初回起動時に次のタスクを実行します。

- 各ホスト用に Active Directory で新しいコンピューターアカウントを作成します。
- ホストに新しい名前を付けます。
- ホストを Active Directory ドメインに参加させます。

Sysprep に比べて、RASprep は変更する構成可能なパラメーターの数が少なく、従って再起動の必要が少なくなるため、はるかに高速で動作します。

注: API の制限により、RASprep は Windows Server 2008 マシンでは使用できません。

次の表には RASprep および Sysprep の主な違いについて説明しています。

オペレーション:	RASprep	Sysprep
ローカルアカウントを削除	いいえ	はい
新しい SID を発行	いいえ	はい
ドメインから親ホストを分離	いいえ	はい
コンピューター名を変更	はい	はい
ドメインへ新しいインスタンスを招待	はい	はい
言語、地域設定、日付と時刻をカスタマイズ	いいえ	はい
再起動の回数	1	2（シール、ミニセットアップおよびドメイン参加）

準備ツールを選択した後に、次のオプションを指定します。

- コンピューター名: コンピューター名を割り当てるために使用する命名パターンです。Windows10-RAS-%ID% などです。

- オーナー名: オーナー名（オプション）。
- 組織: 組織名（オプション）。
- 管理者パスワード: ローカルの Windows 管理者パスワード。
- ドメインに参加: VM が参加するドメイン名。
- 運営管理者: ドメインアカウント。
- パスワード: ドメインアカウントのパスワード。
- ターゲット OU: 組織単位の完全な DN。[...] ボタンをクリックして Active Directory を参照し、OU を選択します。

最適化

[最適化] ページでは、ホストで実行される Windows を最適化して、Parallels RAS 環境で最適なパフォーマンスを発揮できるようにするために使用する設定を指定できます。無効化、削除、または最適化の対象となる Windows コンポーネントやサービス、またその他のオプションを選択して、仮想アプリおよびデスクトップの配信の効率性と合理性を向上させ、改善することができます。詳細な手順については、「最適化」（p. 146）を参照してください。

上記の「最適化」セクションをお読みになり、以下の VDI の特性にも注意してください。

- 新しいテンプレートを作成する場合、最適化はデフォルトで無効になっています。有効化する場合は、ソースとなるホストのバックアップ（完全複製）を作成してから実行する必要があります。最適化を無効にしてテンプレートを作成し、スナップショットを作成してから、最適化を有効にすることもできます。最適化の設定が適用された後はロールバックできないため、バックアップを作成することをお勧めします。
- 既存のテンプレートで最適化を有効にするには、テンプレートがメンテナンスモードでなければなりません。“待機”状態のテンプレートでは、[最適化] タブは無効になっています。
- 既存のテンプレートで最適化が有効になるかまたは変更されていて、テンプレートのメンテナンスモードが終了すると、管理者は既存のホストを再作成するよう求められます。再作成すると、最適化の設定が適用されます。ホストを再作成（その場で、または後から）して、仮想化の設定を受信する必要があります。
- 最適化をテンプレートに適用すると、そのステータスが [最適化を実行中] に変更されます（代表的な変化）。この段階では、リストでテンプレートを選択し、[タスク] > [最適化の停止] をクリックすれば、処理はキャンセルされます。

ライセンスキー

[ライセンスキー] ページで、このテンプレートから作成される仮想マシンのアクティベートに使用するライセンスキー情報を指定します。

まず、自分の組織で使用しているライセンスキーの管理タイプ（KMS または MAK）を選択します。MAK はアクティベーションが制限されているため、Parallels では KMS を使用することをお勧めしています。

キー管理サービス（KMS）: KMS を使用している場合は、[完了] ボタンをクリックして、テンプレート構成情報を保存します。このテンプレートから作成される仮想マシンは、（OS ミニセットアップおよびドメイン参加の最後に）DNS で KMS を探し、それに応じてアクティベートされます。

注: KMS のアクティブ化と RASPrep を使用している場合、そこからテンプレートを作成する前に、KMS を使用してソースホストをアクティブ化する必要があります。別の方法（販売キーまたは MAK）ですでにホストがアクティブ化されている場合、KMS のアクティブ化に変換する必要があります。これを実行する方法の詳細については、Microsoft の記事をお読みください。https://technet.microsoft.com/en-us/library/ff793406.aspx。

マルチライセンス認証キー（MAK）: MAK を使用している場合は、次の操作を実行します。

1. [追加] ボタンをクリックして、[ライセンスキー] フィールドに有効なキーを入力します。
2. [最大ゲスト数] フィールドで、キーの制限を指定します。この制限は、テンプレートの最大ゲスト数（ウィザードの最初のページで設定）より大きいか等しい必要があります
3. [OK] をクリックします。

注: Parallels RAS では、MAK キーが Parallels テンプレートのプロパティで更新された場合、古い MAK キーはホストに保持されません。

概要

[概要] ページでは、テンプレートの概要情報を確認します。必要に応じて、[戻る] ボタンをクリックして情報を修正できます。

最後に、[完了] をクリックしてテンプレートを作成し、ウィザードを閉じます。

ホスト名

このセクションでは、テンプレート作成ウィザードの [プロパティ] ページ（p. 197）で指定したホストの命名パターンについて説明します。

新しいホストが作成されるたびに、その名前が [ホスト名] フィールド（p. 197）で指定したパターンに基づいて自動的に生成されます。完全な名前形式は以下の通りです。

<プレフィックス>%ID:N:S%<末尾>

ここで、

- <プレフィックス> は英数字です。必ず英字（数字ではない）で始めます。
- %ID:N:S% は一意のホスト ID の自動生成に使用される番号パターンです。以下の「番号パターン」セクションをご覧ください。
- <末尾> は自由な形式の英数字文字列です。

番号パターン

VM の名前の中の番号パターンは以下の形式になります。

```
%ID:N:S%
```

上のパターンの構成要素は以下の通りです。

- ID - このまま含めることが必要です。
- N - 使用する番号の桁数です。先行するゼロを含みます。先行ゼロを含めたくない場合、“0”を使用します。
- S - 開始番号。この要素はオプションです。含めなかった場合、番号は 1 から始まります。

例:

- `%ID:3%` - このパターンは、“001”、“002”、“003”～“998”、“999”のように先頭を 0 で埋めた 3 桁の番号を生成します。
- `%ID:3:200%` - このパターンは、“200”、“201”、“202”～“998”、“999”のように 3 桁の数字を 200 から生成します。
- `VDI-R1-%ID:3:100%` - これは英数字プレフィックスに番号パターンを加えた完全名です。次のような名前が生成されます。“VDI-R1-100”、“VDI-R1-101”など。

番号パターンの作成時は、以下の規則に従います。規則が守られなかった場合、エラーメッセージが表示され、修正が必要になります。

- 名前は英字で始めます。数字を最初の文字にすることはできません。
- 英数字部分には、英字、数字、ハイフンを含めることができます。その他の文字は使用できません。
- 名前全体の長さは 15 文字までに制限されています。

- 名前に含めることができる番号パターン（%ID:N:S%）は 1 つだけです。名前の末尾か中間に位置していることが必要です。

指定したパターンは、[ホスト数の上限] フィールドの値に対しても検証されます。パターンがホスト数の上限を網羅していない場合は、エラーが返されるため、パターンを修正する必要があります。

名前の中の VM 番号の再利用

ホストを削除すると、そのホストに割り当てられた数値が未使用になります。次に作成されるホストにはこの番号が付与されるので、通し番号の抜け落ちを回避できます。

Parallels テストテンプレートウィザード

[Parallels RAS テストテンプレートウィザード] は、テンプレートの健全性をテストするために使用されます。このウィザードでは、テンプレートが準備された後のすべてのアクティビティが正常に実行されていることを確認できます。これには、DHCP 設定のチェック、DNS 登録、適切な VLAN、AD ドメインへの参加、適切なターゲット OU などが含まれます。

このウィザードを開くには、Parallels RAS Console でテンプレートを右クリックし、[テスト] を選択します。テストは以下の手順から構成されます。

1. テンプレートは、この目的のために特別に設計された“テスト”モードに一時的に切り替わります。テンプレートがこのモードである間は、テストが完了してテンプレートがテストモードを終了するまで、他のすべての動作がブロックされることに注意してください。
2. ホストは、テストに使用されるテンプレートから複製されます。この VM は、テスト期間中はサーバー上に保持され、その後に削除されます。
3. 一連のテストはホストで実行され、作成元のテンプレートをテストします。
4. テストが完了すると、画面にレポートが表示され、テスト結果が示されます。

ウィザードが開始するとき、次のように動作します。

1. ウェルカムページが開きます。ページに表示されている情報を読み、準備ができたら [次へ] をクリックします。
2. 次のページに、以下を含む、実行される個別のテストのリストが表示されます。
   - ホスト Agent を確認: このテストは、VM にインストールされた RAS Guest Agent との通信を試みます。Agent が応答する場合は、VM が正常に作成され、起動されたことを意味します。

- ドメインのメンバーシップをチェックする: コンピューターが AD ドメインに参加しているかどうかをチェックします。
- ターゲット OU をチェックする: ドメイン資格情報によるコンピューターへの RDP 接続が可能かどうかをチェックします。
- Parallels Client を起動する: このテストでは、Parallels Client を起動し、ホストとの接続を確立します。

3 テストの実行中、進行状況のインジケーターが画面に表示されます。必要に応じて、[キャンセル] ボタンをクリックすると、テストをいつでも中止できます。

4 テストがすべて完了したら、テスト結果を示す以下のページが表示されます。

- 成功: テストがすべて正常に完了したら、一時ホストは削除としてマークされ、テンプレートは通常の動作モードに戻ります。
- 失敗: テストが 1 つでも失敗した場合は、該当する情報が表示され、[ログファイルのダウンロード] リンクをクリックするとログファイルをダウンロードできます。テンプレートをメンテナンスモードに切り替えるオプションもあります。これにより、テンプレートが修正されるまで、テンプレートからホストが作成されるのを防ぐことができます。

5 [完了] をクリックして、ウィザードを閉じます。

テンプレートプロパティの変更

既存テンプレートの構成を変更する必要がある場合は、[テンプレート] リストでテンプレートを選択して、[タスク] > [プロパティ] をクリックします。これにより、[テンプレートのプロパティ] ダイアログが開きます。このダイアログは、「手順 2: 「テンプレートの構成」（p. 197）に進みます。

ホストをテンプレートから作成する方法

テンプレートが作成されると、Parallels RAS はそのテンプレートからホストの作成を開始します。仮想マシンは一度に 1 つずつ作成されます。この時点で作成される VM の数は、[ウィザード完了時に展開されるホストの数] プロパティで決定されます（ここおよびこの後でのすべてのプロパティ名は、前述の [テンプレートウィザードを作成] に言及しています）。

どの時点で利用できる VM の数も、[使用可能なバッファを以下に維持] プロパティで指定されている数を下回ることはありません。このルールを守るため、必要に応じて新しい VM が自動的に作成されます。同時に、VM の総数が [ホスト数の上限] プロパティで指定された数を超えることはありません。

テンプレートから新しいホストを作成するには、しばらく時間がかかります。テンプレートが完全複製を作成するために構成されているときは特にかかります（リンククローンの作成の方が高速です）。ホストが作成の途中であり、他に利用可能な VM がない場合、VM が必要なユーザー（複数可）は VM の準備が整うまで待つ必要があります。

準備段階でホストに（何らかの理由で）問題が発生した場合、その VM は使用不能状態でサーバーに残ります。[ゲスト VM ステータス] 列の「作成に失敗」という値により、このような VM を特定できます。このような VM は、修復または再作成されない限り、サイトのデフォルト値（[ファーム] > <サイト> > [VDI] > [デスクトップ] > [タスク] > [サイトのデフォルト値]）の [準備に失敗したホストを自動削除するまでの時間] フィールドに指定した時間が経過した後に、自動的に削除されます。ホストの作成に失敗した場合の詳細は、[ステータス] 列の [詳細] リンクをクリックするか、列をダブルクリックすることで表示されます。また、同じメニューから [再作成] や [削除] を選ぶこともできます。ホストの再作成方法の詳細については、「テンプレートのメンテナンス」セクション（p. 208）を参照してください。

ホストの自動削除

ホストは、テンプレートのプロパティにある [以下の後に未使用のホストを削除] フィールドで指定した時間より長く使用されないと、自動的に削除されます。

手動によるホストの追加

ホストはテンプレートから自動的に作成されます。1 つまたは複数の追加のホストが必要な場合、それらを手動で追加（作成）できます。

ホストを追加するには:

1. RAS コンソールで、[ファーム] > <Site> > [VDI] > [ホスト] に移動します。
2. リストの上部にある [+] アイコンをクリックします。
3. 開いた [ホストの追加] ダイアログで、新しいホストを作成するテンプレートを選択します。
4. 起動するホストの数を指定します。指定した数値がホストプールプロパティで設定された”ホスト数の上限”の値を超えると（すでに存在する VM の数が考慮されます）、警告メッセージが表示されます。この場合、より小さい数値を設定するか、ホストプールプロパティの [プロビジョニング] タブで、ホスト数の上限値を変更する必要があります。
5. [OK] をクリックして、ダイアログを閉じます。

6 RAS Console で[適用] をクリックすると、新しいホストが [デスクトップ] タブのリストに表示されます。その際、[ステータス] 列には“複製中”と表示されます。複製が完了すると、ユーザーが新しいホストを利用できるようになります。

ホストプール（VDI）へのテンプレートの割り当て

VDI ホストプールを作成する際、グループにテンプレートを割り当てることができます。これは、プールを作成または変更する際に行うか、[テンプレート] タブから行うことができます。

ホストプールにテンプレートを割り当てるには:

1 [テンプレート] タブで、テンプレートを選択します。

2 [タスク] > [プールに割り当て] をクリックします。ウィザードが開きます。

3 [バージョン] ページで、ホストプールに割り当てるテンプレートのバージョンを選択します。

4 （オプション）[ホストプール] ページで、スケジュールで再作成するホストプールを選択し、[次へ] ボタンをクリックします。再作成を予約するダイアログが表示されます。必要に応じてスケジュールを構成し、[次へ] をクリックします。

5 [完了] をクリックします。

ホストプールからテンプレートを削除するには:

1 テンプレートを選択し、[タスク] > [プールから削除] をクリックします。

2 このテンプレートが割り当てられているすべてのホストプールを一覧表示するダイアログが開きます。

3 テンプレートを削除するホストプールを選択し、[OK] をクリックします。

なお、ホストプールに、削除するテンプレートから作成されたホストがある場合は、それらも削除されます。本当に削除するかどうかを確認するメッセージが表示されます。

テンプレートのメンテナンス

テンプレートは、“メンテナンス”と呼ばれる特別なモードに設定することができます。このモードは、主にゲストオペレーティングシステムでソフトウェアのアップデートやインストールを行うために使用されます。このモードでは、テンプレートは、新しいホストの作成といった一般的なタスクを行うことができなくなり、通常の仮想マシンとして起動できるようになります。仮想マシンが実行されたら、ゲスト OS でソフトウェアのインストールやアップデートを行ったり、オペレーティングシステムで管理タスクを実行したりすることができます。

テンプレートが完全複製とリンク複製のどちら向けに構成されているかによって、メンテナンスモードは多少異なる方法で使用されます。以下にその違いを説明します。

完全複製

完全複製を作成するようテンプレートが構成されている場合、次の操作を実行します。

1. テンプレートを選択し、[タスク] > [メンテナンス] をクリックし、メンテナンスを開始するテンプレートのバージョン（p. 583）を選択します。テンプレートが無効になり（グレーで表示される）、そこで行われるすべての操作が一時停止されます。[ステータス] のテンプレートのステータスが、”メンテナンスを開始中”になり、完了すると”メンテナンス”に変わります。
2. ハイパーバイザーのネイティブツールを使用して、通常の仮想マシンとしてテンプレートを起動します。
3. 必要に応じて Windows Update または Windows ソフトウェアをインストールします。
4. 完了したら、仮想マシンをシャットダウンします。
5. RAS Console に戻り、テンプレートを選択して [タスク] > [メンテナンス] を再度クリックし、メンテナンスモードを終了します。新しいバージョンを作成するか、変更を破棄するかを選択するダイアログが表示されます。[新しいバージョンを作成] を選択します。

   注: 1 つのテンプレートに最大 5 つのバージョンを含めることができます。別のバージョンを作成したい場合は、すでに存在するバージョンを削除する必要があります。

6. 「テンプレートバージョンの使用」（p. 583）の「新しいバージョンの作成」サブセクションの説明に従って、新しいテンプレートバージョンを作成します。完全複製テンプレートを更新すると、変更は今後の複製にのみ影響を与えます。既存の複製にこの更新を適用するには、その複製を再作成する必要があります。既存のホストの再作成をこの時点で行うか、後で行うかを選択できます。完全複製の再作成には時間がかかります。また、再作成中に新しいアプリが完全複製の VM にインストールされたり、ユーザープロファイルが変更されたりする場合がありますが、こういった変更はすべて失われます。ユーザーへの影響を最小限に抑えるために、メンテナンス期間をスケジュール設定して、その期間中に複製を再作成することをお勧めします。

リンク複製

リンク複製では仮想ハードディスクがテンプレートのスナップショットと共有されるため、完全複製と比較すると追加の手順が必要になります。

まず、データを保存してログオフするようにホストユーザーに通知する必要があります。これは、テンプレートにインストールするアップデートを既存のホストに反映するために必要になります。すべてのユーザーがログオフしたら、次の操作を実行します。

1 テンプレートを選択し、[タスク] > [メンテナンス] をクリックし、メンテナンスを開始するテンプレートのバージョン（p. 583）を選択します。テンプレートが無効になり（グレーで表示される）、そこで行われるすべての操作が一時停止されます。また、ウィンドウの下部には、操作に関するステータスが表示されます。

2 ハイパーバイザーのネイティブツールを使用して、通常の仮想マシンとしてテンプレートを起動します。

3 必要に応じて Windows Update または Windows ソフトウェアをインストールします。

4 完了したら、仮想マシンをシャットダウンします。

5 RAS Console に戻り、テンプレートを選択して [タスク] > [メンテナンス] を再度クリックし、メンテナンスモードを終了します。新しいバージョンを作成するか、変更を破棄するかを選択するダイアログが表示されます。[新しいバージョンを作成] を選択します。

> 注: 1 つのテンプレートに最大 5 つのバージョンを含めることができます。別のバージョンを作成したい場合は、すでに存在するバージョンを削除する必要があります。

6 「テンプレートバージョンの使用」（p. 583）の「新しいバージョンの作成」サブセクションの説明に従って、新しいテンプレートバージョンを作成します。リンク複製を再作成せずに新しいバージョンを作成した場合、手動で再作成するか、スケジューラーを使用して再作成する必要があることに注意してください。

テンプレート内の RAS Guest Agent の更新

テンプレートには、RAS Guest Agent の最新バージョンがインストールされている必要があります。RAS Guest Agent はテンプレートの作成時にインストールされます。RAS Guest Agent の新しいバージョンが入手できるようになったら、RAS Guest Agent をアップデートする必要があります。Agent を更新するには、上述のメンテナンスモードを使用する必要があります。Parallels RAS では、Agent の更新を簡素化するために、インストール済みのすべての Agent をモニタリングし、更新プログラムが利用可能になると管理者に通知します。

RAS Console の起動時に、インストール済みのすべて Agent がチェックされ、更新が必要な Agent が存在する場合はメッセージが表示されます。これは、RAS インフラストラクチャのサーバーとテンプレートに適用されます。すべてのエージェントを更新するかどうかをユーザーに確認するメッセージが表示されます。[はい] をクリックすると、Agent を更新する必要のあるすべてのサーバーとテンプレートを一覧表示するダイアログが表示されます。サーバー/テン

プレートの選択または選択解除を行い、一括更新の手順にサーバー/テンプレートを含めたり、除外したりできます。選択を行ったら、[OK] をクリックして、更新を開始します。画面の指示に従って、Agent を更新します。

完全複製テンプレートとリンク複製テンプレートの比較: テンプレートの RAS Guest Agent を更新する際には、このテンプレートから作成されたホストの Agent も更新する必要があります。この更新は、完全複製テンプレートとリンク複製テンプレートに対して別々に実行されます。以下に説明する手順をお読みください。

リンク複製テンプレートの Agent を更新する場合、このテンプレートから作成されたすべてのホストを再作成するかどうか確認されます。[はい] をクリックすると、それらはテンプレートに合わせて自動的に再作成されます。

完全複製テンプレートの Agent を更新するときに、自動的に完全複製ホストが再作成されることはありません。再作成するかどうかが確認されます。完全に複製された VM は完全なマシンであるため、再作成には時間がかかります。再作成する場合は注意してください。代わりに、これらの VM の Agent を RAS Console からプッシュインストールすることによって更新できます。これは [VDI] > [デスクトップ] タブで [タスク] > [すべての Agent をアップグレード] をクリックして実行できます。

テンプレート内の RAS Guest Agent のステータスを手動で確認するには、[タスク] > [Agent をチェック] をクリックします。Agent が最新の場合、メッセージボックスに最新であることを確認するメッセージが表示されます。RAS Guest Agent の新しいバージョンが入手できる場合は、更新するかどうかを確認するダイアログが表示されます。上述の、完全複製テンプレートおよびリンク複製テンプレートの更新における違いがこのシナリオにも当てはまりますので注意してください。

テンプレートに基づく RD セッションホストのメンテナンス

テンプレートから作成された RD セッションホストに対してスケジュールされたメンテナンスを実行する必要がある場合、次の手順に従ってください。

1. メンテナンスウィンドウに合わせて対象の RD セッションホストグループを空にするスケジュールを作成します。
2. メンテナンス中（またはその直前）にテンプレートをメンテナンスモードに切り替えます。その後で必要な変更を適用します。
3. スケジュールでは、テンプレートにプロビジョニングされたグループが（メンテナンスウィンドウが継続している間）無効になり、これにより、すべてのホストがグループから削除（割り当て解除）されます。

4 テンプレートをメンテナンスから解放し、すべての複製を再作成するか尋ねられたら、[はい] をクリックします。

5 ステップ 3（上記）で無効にしたグループを有効にします。この時点で、グループは、[使用可能なバッファを以下に維持] 設定に従い、ホストの受け取りを開始します。

6 この時点以降、グループはオンデマンドで VM によりプロビジョニングされます。

テンプレートのステータス

テンプレートが意図した通りに機能していることを確認するには、RAS Console でメインテンプレートリストのステータス（[ステータス] 列）を調べます。テンプレートが適切に機能している場合は、[ステータス] 列に “待機” と表示されます。このステータスは、必要に応じてこのテンプレートからホストを作成できることを意味します。テンプレートが作成中またはメンテナンスモードの場合、またはテンプレートが削除中の場合は、それに応じてステータスが変わります。

表には、テンプレートにインストールされている RAS Guest Agent のステータスを表示する [Agent のステータス] 列もあります。RAS インフラストラクチャのサーバー（Connection Broker、ゲートウェイ、RD セッションホストなど）と比較すると、テンプレート Agent のステータスはテンプレートのステータスほど重要ではありません。テンプレートは通常の仮想マシンではなく、大抵は実行中ではないため、停止している VM の Agent のステータスを確認することにはそれほど意味がないためです。そのため、RAS Console ではテンプレートの Agent のステータスは通常は [利用不可] であり、これはまったく正常なステータスです。[Agent のステータス] に意味のあるステータスが表示されるのは、テンプレートがメンテナンスモードであり、通常の VM と同じように実行中の場合のみです。このような場合は、Agent も実行中であり、Agent のステータスを検証できます。

以下の表では、多様に変化するテンプレートの各状態で、[ステータス] 列と [Agent のステータス] 列に何が表示されるかを示します。

テンプレートの作成

ステータスの色	テンプレートのステータス	Agent のステータス	説明
グレー	利用不可	利用不可	プロバイダーが無効な場合、Provider Agent が切断されている場合、またはテンプレートが存在しない場合。
グレー	適用されません	適用されません	ウィザードの終了後、管理者が RAS Console で [適用] をクリック

			するのを待っています。
オレンジ	作成中	利用不可	Azure Gallery をソースとして使用しています（利用可能な事前作成済みのホストはない）。
オレンジ	Agent のインストール	利用不可の後 OK	新たに作成した VM、またはテンプレートとして利用できる VM に Agent を展開しています。
オレンジ	展開中	最適化を保留中	最適化の適用を待っています。管理者は、この時点で最適化を停止できます。
		最適化を実行中	最適化を実行しています。管理者は、この時点でまだ最適化を停止できます。
		OK の後に利用不可	VM をテンプレートに変換中の内部処理です。変換が完了したら、テンプレートのステータスは“待機”に変わります。
赤	作成に失敗しました	利用不可	問題が発生しました。（クォータの上限到達、Azure でのリソース作成に関する問題など）。管理者は、[タスク] > [直前の処理を再試行] をクリックして処理を再試行できます。
赤	Agent のインストールに失敗しました	利用不可	潜在的なネットワーク問題、ファイル共有の制限、管理者権限の問題など。管理者は、[タスク] > [直前の処理を再試行] で再試行できます。
赤	展開に失敗しました	実際のステータス（OK、利用不可など）	問題が発生しました。（クォータの上限到達、ストレージ領域の問題、プロバイダーからのスナップショット作成に関する問題など）。管理者は、[タスク] > [直前の処理を再試行] で再試行できます。
		FSLogix を使用できません	FSLogix Agent が見つかりません。
		FSLogix が更新されていません	FSLogix Agent の更新が必要です。

本稼働中のテンプレート

ステータスの色	テンプレートのステータス	Agent のステータス	説明

緑	待機	実際のステータス（OK、利用不可など）	テンプレートの準備が完了しました。
緑	複製の作成	実際のステータス（OK、利用不可など）	テンプレートからホストを複製中です。
オレンジ	更新が必要	更新が必要	RAS Guest Agent の更新が必要です。

メンテナンスモードのテンプレート

ステータスの色	テンプレートのステータス	Agent のステータス	説明
オレンジ	メンテナンス	実際のステータス（OK、未確認など）	テンプレートとして使用されているホストが稼働中です。
		最適化を保留中	最適化の適用を待っています。管理者は、この時点で最適化を停止できます。
		最適化を実行中	最適化を実行しています。管理者は、この時点でまだ最適化を停止できます。
		更新が必要	テンプレートとして使用されているホストが稼働中であるが、RAS Guest Agent の更新が必要です。

テンプレートの削除

ステータスの色	テンプレートのステータス	Agent のステータス	説明
グレー	削除マーク	テンプレートとして使用されているホストがまだ実行中の間の実際のステータス（OK、未確認など）	テンプレートが削除中です。

マルチプロバイダーのテンプレート配信の管理

マルチプロバイダーのテンプレート配信の機能について詳しくは、「マルチプロバイダーのテンプレート配信」セクション（p. 193）を参照してください。

配信リストに対するプロバイダーの追加または削除

テンプレートの [プロパティ] ダイアログを使用して、配信リストでいつでもプロバイダーの追加または削除を行えます。このダイアログを開くには、[VDI] > [テンプレート] タブでテンプレートを右クリックし、[プロパティ] を選択します。

テンプレート配信のステータス

[Parallels テンプレートの作成ウィザード] を完了してテンプレートを作成した後や、プロバイダーを既存のテンプレートで追加または削除した場合は、[テンプレート] タブでテンプレートの配信ステータスをモニタリングできます。ステータスは [配信] 列に以下の値で表示されます。

- 配信中 - 配信が進行中（テンプレートをターゲットホストに配信中）です。
- OK - テンプレートは、指定されたすべてのホストに正常に配信されました。
- プロバイダーを削除/プロバイダーを追加 - プロバイダーが追加されています、または削除されました。
- 配信に失敗しました - 配信操作中にエラーが起きたことを示しています。

配信の詳細

[テンプレート] タブの [タスク] > [配信の詳細] メニューで、ダイアログが開き、このテンプレートを使用しているプロバイダーの現時点での配信状態と進捗状況を示すインジケーターが表示されます。

[進行] 列には、メインテンプレートリスト（上記参照）の [配信] 列と同じ値が表示されます。

[状態] 列には、次のいずれかが表示される場合があります。

- 準備完了 - プロバイダーの準備ができました。
- 利用不可 - プロバイダーが応答していません。
- アップデートが必要 - テンプレート配信操作を再度実行する必要があります。このホストのテンプレート配信操作を再度実行するには、[再試行] ボタンをクリックします。

メンテナンスモードの終了

テンプレートのメンテナンスモードを終了すると、通常、「テンプレートが変更されました。すべてのホストを再作成する必要があります。今すぐ再作成しますか？」というプロンプトが表示されます。管理者が [はい] をクリックし、テンプレートがマルチプロバイダー配信を使用している場合、Parallels RAS は各プロバイダーの状態を確認します。プロバイダーが応答しない場合は、管理者に対しプロバイダーの状態を確認するように求めるメッセージが表示されます。プロバイダーをオンライン状態に戻して、ホストを再作成してみてください。この時点でできない場合は、後でホストを再作成することができます。

テンプレートベースのホストの管理

ホストとその他のデスクトップは [VDI] > [デスクトップ] タブで管理します。このタブでは、標準的なデスクトップ管理操作すべてを [タスク] メニューから実行できます。再作成、削除、全 Agent の更新、割り当て、割り当て解除、セッションの表示、開始、停止、再起動、サスペンド、リセットなどを実行できます。再起動操作（猶予）には 10 分間のタイムアウトがあります。この時間内に操作が完了しない場合は、リセット操作（強制）となります。

デフォルトでは、[デスクトップ] タブには、ファーム内で利用可能なすべてのデスクトップが表示されます（利用可能なすべてのデスクトップを表示するには、リストのスクロールが必要な場合があります）。特定のテンプレートに属する VM だけを表示するには、[テンプレート] タブでテンプレートを選択し、[タスク] > [ホストを表示] をクリックします。これにより、[デスクトップ] タブに切り替わります。このタブでは、選択されたテンプレートに属する VM だけが表示されるよう、自動的に絞り込まれています。

詳細については、「ホストの管理」（p. 216）を参照してください。

ホスト（VDI）の管理

Parallels RAS VDI の使用時には、テンプレートベースおよび非テンプレートベースの 2 つの基本的なホストのタイプを利用できます。このトピックは、両方のホストタイプの管理タスクについて説明します。タスクが特定のホストタイプに当てはまる場合はそれを明記します。

ホストリストを表示する

非テンプレートベースのホストのリストを表示するには、[ファーム] > <サイト> > [VDI] > [デスクトップ] を選択します。リストにフィルターを適用していた場合、虫眼鏡アイコンをクリックして解除します。フィルターが適用されていないリストには、RAS ファームで利用できるす

べてのデスクトップが含まれます。ゲスト VM（テンプレートベースおよび非テンプレートベース）、プールからのゲスト VM（RAS またはネイティブ）、およびプールベースのリモート PC が含まれます。従って、[デスクトップ] タブでは、1 か所ですべてのデスクトップを確認できます。ここでは、標準的なデスクトップ管理作業すべてを [タスク] メニューから実行できます。再作成、削除、割り当て、割り当て解除、開始、停止、サスペンド、リセット、セッションの表示などを実行できます。再起動操作（猶予）には 10 分間のタイムアウトがあります。この時間内に操作が完了しない場合は、リセット操作（強制）となります。

テンプレートから作成されたホストのリストを表示するには、[ファーム] > <サイト> > [VDI] > [テンプレート] を選択します。テンプレートを選択し、[タスク] > [ホストを表示] をクリックします。これにより、[デスクトップ] タブに切り替わります。このタブでは、テンプレートに属する VM だけが表示されるよう、自動的に絞り込まれています。上述のように、このタブでは電源の操作を含む標準的なデスクトップ管理操作すべてを実行できます。このセクションで後ほど詳細に説明します。

特定のプールのホストだけを表示するには、[プール] タブでプールを選択し、[タスク] > [プール内のホストを表示する] をクリックします。

[デスクトップ] タブ内のフィルターは、虫眼鏡アイコンをクリックして、リスト最上部に表示されるフィールドにフィルター条件を入力することで、手動でも適用できます。

サイトの既定値

テンプレートから作成されたホストはテンプレートの設定を継承します。設定を表示するには、ホストがどのテンプレートをベースとしているかをメモしてから、そのテンプレートのプロパティを表示します。具体的には、[設定] と [セキュリティ] のタブを確認します。詳細については、「サイトのデフォルト値」（p. 228）を参照してください。テンプレートでは、サイトのデフォルト設定を継承することも、カスタム設定を指定することもできます。

非テンプレートベースのホストには固有の設定があります。一部（具体的には設定とセキュリティです）はサイトのデフォルト値（p. 228）から継承されます。非テンプレートベースの VM の設定を確認するには、[ファーム] > <サイト> > [VDI] > [デスクトップ] に移動します。テンプレートに属していないホストは、[テンプレート] 列の値が空白になります。テンプレートを右クリックし、[プロパティ] を選択します（テンプレートベースのホストにはこのメニューオプションがありません）。

RAS Guest Agent のステータスの確認

ホストには RAS Guest Agent をインストールする必要があり、Agent は Parallels RAS のバージョンと適合している必要があります。テンプレートからホストを作成すると、Agent がデフォルトでインストールされます。ネイティブのハイパーバイザーツールを使用してホストが作成されている場合は、Agent がインストールされていない可能性があります。この場合、ホストはリモートデスクトップに対してのみサービスを提供します。サーバーアプリケーションやドキュメントに対するサービスを有効にするには、Agent をご自身でインストールする必要があります。

RAS Guest Agent がホストにインストールされているかどうか、そしてそれが最新であるかどうかをチェックするには、次の操作を実行します。

1. リストでホストを選択し、[タスク] > [トラブルシューティング] > [Agent をチェック] をクリックします。
2. [Guest Agent の情報] ダイアログが開き、RAS Guest Agent の情報が表示されます。
3. Agent がインストールされていない場合、[インストール] ボタンをクリックして指示に従います。ホスト内で実行されている Windows に Agent がプッシュインストールされます。

ホストを削除する

テンプレートベースのホストを削除するには、該当の VM を選択してから [タスク] > [削除] をクリックします。

重要: ホストは必ず RAS Console から削除する必要があります。ハイパーバイザーのネイティブクライアントやウェブインターフェイスを使用してホストを削除しようとしないでください。実行すると、VM だけでなく、親テンプレートも削除される可能性があります（その結果、このテンプレートからリンク複製として作成された他のすべてのホストも無効になります）。これは、一部のネイティブのハイパーバイザークライアントがリンク複製をスタンドアロン VM として扱うためです。Parallels RAS は、リンク済みの複製をスタンドアロン VM ではなく、複製として処理します。

準備に失敗したホストの管理

準備段階でテンプレートベースのホストに問題が発生した場合、その VM はサーバーに残りますが、使用することはできません。[ゲスト VM ステータス] 列の「作成に失敗」という値により、このような VM を特定できます。このような VM は、修正されない限り、サイトのデフ

ォルト値（p. 228）に指定した時間が経過した後に、自動的に削除されます。サイトのデフォルト値を確認するには、次の操作を実行します。

1 [ファーム] > <サイト> > [VDI] > [デスクトップ] を選択してから、[タスク] > [サイトのデフォルト値] をクリックします。

2 開いたダイアログの [全般] タブで、[準備に失敗したホストを自動削除するまでの時間] オプションを（必要に応じて）表示または変更します。有効な期間は、ドロップダウンリストから選択するか、”8 日間”や”12 時間”などの値を入力することで設定できます。

ホストを再作成する

テンプレートベースのホストに何かが発生し、使用不能になった場合、削除して新しいホストを作成する必要はありません。その代わり、名前、MAC アドレス、その他のプロパティを保持したまま再作成することができます。このようにすれば、サイト設定が破損したホストに依存していた場合でも、他のサイト設定は影響を受けません。ホストを再作成するもう 1 つの理由は、（再作成コマンドを実行せずにメンテナンスを終了するときに）テンプレートに加えられた変更を適用するためです。

なお、再作成された VM では、以下のプロパティが保持されます：

- MAC アドレスは、ESXi、vCenter、Hyper-v、Hyper-v Failover Cluster、Nutanix AHV（AOS）、SC//HyperCore で保持されます。
- BIOS の UUID は、ESXi と vCenter で保持されます。
- DRS グループは vCenter で保持されます。

ホストを 1 つ以上作成するには、次の操作を実行します。

1 Parallels RAS Console で、[ファーム] > <サイト> > [VDI] > [テンプレート] に移動します。

2 展開済みのホストをすべて再作成するには、[タスク] ドロップダウンリストをクリックして、[すべてのホストを再作成] を選択します。

3 特定のホスト（または複数のホスト）を再作成するには、[タスク] > [ホストを表示] をクリックします。これにより、[デスクトップ] タブが開き、ホストのリストが表示されます。1 つまたは複数のホストを選択してから、[タスク] > [再作成] をクリックします。

ホストを再作成する場合:

- この手順により VM が削除され、同じテンプレートから新しい VM が作成されます。
- 新しいホストでは、置き換える対象と同じコンピューター名が保持されます。

- ホストが実行中である場合、そのメモリーの中にある保存されていないすべてのデータが失われます。そのため、重要なデータは外部ストレージに保存する必要があります。

パーシスタントなホスト

ホストは、特定のユーザーまたはデバイスに割り当てられたときに「パーシスタント」となります。ホストをパーシスタントにするには、次の操作を実行します。

1 ホストからのデスクトップまたはリソースの公開を開始します。

2 [バーチャルゲストの設定] オプションを指定する場合、[ホストに対する静的割り当てを有効化] を選択します。

3 公開ウィザードを終了します。

4 これにより、デスクトップやリソースを使用する最初のユーザーやデバイスに VM が割り当てられます。ユーザーとデバイスの割り当てを切り替える方法については、「サイトのデフォルト値（VDI）」（p.228）のサブセクション、「一般」を参照してください。

ホストをユーザーまたはデバイスに手動で割り当てることもできます。このためには、次の操作を実行します。

1 [ファーム] > <サイト> > [VDI] > [デスクトップ] に移動します。

2 ホストを選択し、[タスク] > [割り当てる] をクリックします。ホストをユーザーまたはデバイスに割り当てることもできます。ユーザーとデバイスの割り当てを切り替える方法については、「サイトのデフォルト値（VDI）」（p.228）のサブセクション、「一般」を参照してください。

3 ユーザーに割り当てる場合は、Active Directory に登録されているユーザーを指定します。

4 デバイスに割り当てる場合、以下のオプションのいずれかを選択します:

- [Active Director から追加] では、Active Directory のドメインに参加しているデバイスを追加できます。
- [既知のデバイスから追加] では、RAS デバイスマネージャーで既知となっているデバイスを追加できます。
- [カスタムエントリーを追加] では、デバイス名を手動で入力できます

5 これにより、ホストが選択したユーザーに割り当てられます。

パーシスタントホストを表示するには、[ファーム] > <サイト> > [VD] > [デスクトップ] に移動します。パーシスタントホストは、[割り当て] 列の“パーシスタント”という値により識別されます。

ホストからパーシスタンスを削除するには、次のいずれかを実行します。

- [デスクトップ] タブでホストを選択して、[タスク] > [割り当て解除] をクリックします。
- [ファーム] > <サイト> > [VDI] > [デスクトップ] に移動し、[タスク] > [サイトのデフォルト値] をクリックします。開いたダイアログで、[以下の時間使われていない場合は、自動的にパーシスタントデスクトップを削除する] オプションを使用して、パーシスタンスの自動削除を実行するまでの経過時間を選択します。希望の期間を指定することもできます（例: ”1 週間と 3 日間 “）。

セッション（VDI）の管理

「セッションの管理」（p. 329）を参照してください。

第　9　章

スケジューラーの使用（VDI）

[スケジューラー] タブでは、指定された時間に個々のホストまたはホストプールで実行されるスケジューラータスクを作成することができます。なお、個別のホストのタスクは、テンプレートベースでない場合に限り、特定のスケジュールを設定できます。

ホストまたはプール内のホストを無効にする

ホストまたはプール内のホストを無効にするには、次の操作を実行します。

1. [タスク] > [追加] > [デスクトップを無効化] または [プールを無効化] をクリックします。
2. [一般] タブで、[スケジュールを有効化] オプションを選択します。
3. このスケジュールの名前と説明（オプション）を指定します。
4. [利用可能] リストでホスト、またはプール（選択したアクションに応じて）を選択し、[追加] をクリックします。[対象] リストにホスト（またはプール）が表示されます。
5. [トリガー] タブを選択し、このイベントの開始日、開始時刻、期間、および繰り返しの設定を指定します。これを 1 回限りのイベントにするには、[繰り返し] ドロップダウンリストで [なし] を選択します。
6. [オプション] タブを選択します。以下のオプションが含まれています。
   - メッセージリスト: ここでは、ホストがオフラインになる前にユーザーに送信されるメッセージを構成します。[タスク] > [追加] をクリックして、メッセージのタイトル、本文、送信する期間を指定します。
   - 無効時の処理: スケジュールされたタスクがトリガーされたときに現在のセッションに対して実行する処理を指定します。[無効時の処理] ドロップダウンリストから必要なオプションを選択します。
   - 現在非アクティブのホストにスケジュールを適用する: このオプションは、リストにアクティブなメッセージが存在する場合に限り有効になります。オプションが有効化されている場合、現在オフラインのホストもモニタリングされます。そのサーバーがスケジュール済みタスクの実行中にオンラインに戻ると、そのタスクも適用されます。
7. [OK] をクリックしてスケジュールを保存します。

ホストまたはプール内のホストを再起動する

ホストまたはプール内のホストを再起動するには、次の操作を実行します。

1 [タスク] > [追加] > [デスクトップを再起動] または [プールを再起動] をクリックします。

2 [トリガー] タブで、スケジュールのプロパティは、上述したのと同じ方法で指定します。さらに、”次のオプションを指定します”タスクに以下のオプションを指定します。

- 終了: タスクを完了するまでの時間を指定します。

3 [オプション] タブで、スケジュールのプロパティは、上述したのと同じ方法で指定します。さらに、次のオプションを指定します。

- メッセージリスト: ここでは、ホストが再起動される前にユーザーに送信されるメッセージを構成します。[タスク] > [追加] をクリックして、メッセージのタイトル、本文、送信する期間を指定します。
- [ドレインモードを有効化] および [指定した時間の後にサーバーを強制的に再起動] となります。これら 2 つのオプションは組み合わせて使用できます。[ドレインモードを有効化] オプションを選択すると、タスクが発生したときにホストへの新しい接続は拒否されますが、アクティブな接続は引き続き実行され、再接続されます。すべてのアクティブなユーザーセッションが終了したとき、または指定した時間の後にサーバーを強制的に再起動の時間に到達したときのどちらか早い時点で、サーバーが再起動されます。アクティブユーザーの作業が失われることのないよう、ユーザーに対する作業を保存してログオフすることを促すメッセージを作成します。
- 現在非アクティブのホストにスケジュールを適用する: このオプションは、リストにアクティブなメッセージが存在する場合に限り有効になります。オプションが有効化されている場合、現在オフラインのホストもモニタリングされます。そのサーバーがスケジュール済みタスクの実行中にオンラインに戻ると、そのタスクも適用されます。

4 [OK] をクリックしてスケジュールを保存します。

ホストまたはプール内のホストを起動する

ホストまたはプール内のホストを起動するには、次の操作を実行します。

1 [タスク] > [追加] > [デスクトップを起動] または [プールを起動] をクリックします。

2 スケジュールのプロパティは、上記と同じ方法で指定します。唯一の違いは、[オプション] タブに次のオプションが追加されていることです。。

- すべてのメンバーの電源を投入: 特定のユーザーに割り当てられたすべてのホストを起動するには、このオプションを選択します。
- メンバーの割合: このオプションを選択して、各プールで起動する必要のあるホストの割合が指定します。

- 開始するメンバーの数を指定: このオプションを選択して、各プールで起動する必要のあるホストの数を指定します。

3 [OK] をクリックしてスケジュールを保存します。

ホストまたはプール内のホストをシャットダウンする

ホストまたはプール内のホストをシャットダウンするには、次の操作を実行します。

1 [タスク] > [追加] > [デスクトップをシャットダウン] または [プールをシャットダウン] をクリックします。

2 スケジュールのプロパティは、上記と同じ方法で指定します。唯一の違いは、[オプション] タブに次のオプションが追加されていることです。

- ここでは、ホストがシャットダウンされる前にユーザーに送信されるメッセージを構成します。[タスク] > [追加] をクリックして、メッセージのタイトル、本文、送信する期間を指定します。
- ドレインモードを有効化および指定した時間の後にサーバーを強制的にシャットダウン: これら 2 つのオプションは組み合わせて使用できます。[ドレインモードを有効化] オプションを選択すると、タスクが発生したときにホストへの新しい接続は拒否されますが、アクティブな接続は引き続き実行されます。すべてのアクティブなユーザーセッションが終了したとき、または指定した時間の後にサーバーを強制的にシャットダウンの時間に到達したときのどちらか早い時点で、サーバーがシャットダウンされます。アクティブユーザーの作業が失われることのないよう、ユーザーに対する作業を保存してログオフすることを促すメッセージを作成します。
- 現在非アクティブのホストにスケジュールを適用する: このオプションは、リストにアクティブなメッセージが存在する場合に限り有効になります。オプションが有効化されている場合、現在オフラインのホストもモニタリングされます。そのサーバーがスケジュール済みタスクの実行中にオンラインに戻ると、そのタスクも適用されます。

ホストとホストプールを再作成する

ホストまたはプール内のホストを再作成するには、次の操作を実行します。

1 [タスク] > [追加] > [テンプレートからホストを再作成]、または [テンプレートからホストプールを再作成] をクリックします。

2 スケジュールのプロパティは、上記と同じ方法で指定します。唯一の違いは、[オプション] タブに次のオプションが追加されていることです。

- ここでは、ホストがシャットダウンされる前にユーザーに送信されるメッセージを構成します。[タスク] > [追加] をクリックして、メッセージのタイトル、本文、送信する期間を指定します。
- ドレインモードを有効化、強制的にホストを再作成するまでの時間、強制的にホストプールを再作成するまでの時間: このオプションは組み合わせて使用できます。[ドレインモードを有効化] オプションを選択すると、タスクが発生したときにホストへの新しい接続は拒否されますが、アクティブな接続は引き続き実行されます。すべてのアクティブなユーザーセッションが終了したとき、または [強制的にホストを再作成するまでの時間]/[強制的にホストプールを再作成するまでの時間] オプションで指定した時間に到達したときのどちらか早い時点で、サーバーが再作成されます。アクティブユーザーの作業が失われることのないよう、ユーザーに対する作業を保存してログオフすることを促すメッセージを作成します。
- 現在非アクティブのホストにスケジュールを適用する: このオプションは、リストにアクティブなメッセージが存在する場合に限り有効になります。オプションが有効化されている場合、現在オフラインのホストもモニタリングされます。そのサーバーがスケジュール済みタスクの実行中にオンラインに戻ると、そのタスクも適用されます。

ログの構成

ログの構成、および既存ログファイルの取得やクリアを実行するには、プロバイダーを右クリックして、[トラブルシューティング] > [ログ] を選択してから、行う作業に応じて、[構成]、[取得]、または [クリア] をクリックします。これらのタスクの実行方法については、「ログ」セクション（p. 608）を参照してください。以下に重要な情報がありますのでこちらもお読みください。

プロバイダーの操作ログの記録は、RAS Provider Agent レベルで実行されます。プロバイダーのログを構成するときには、実際にはこのプロバイダーにサービスを提供する RAS Provider Agent の構成を実行することになります。組み込み RAS Provider Agent を使用している場合、ロギング構成はサービスを提供するすべてのプロバイダーに適用されます。次のシナリオについて考えてみましょう。

- 組み込み Provider Agent のサービスを受けている特定のプロバイダーのログファイルを取得すると、その Agent のサービスを受けているすべてのプロバイダーのログがファイルに含められます。
- 特定のプロバイダーのログファイルをクリアする場合、同じ組み込み Provider Agent によりサービスが提供されていると、すべてのプロバイダーのログがクリアされますので注意し

てください。このような共有ログを削除しようとすると、RAS Console にはプロンプト画面が表示されます。

プロバイダーにあるのが専用 Provider Agent であり、サービスの対象がそのホストのみである場合、上記はいずれも当てはまりません。

VDI の高可用性の実現

VDI の高可用性とは、プロバイダーが Provider Agent との接続を失わないようにすることです。接続が切れると、ユーザー接続でホストを利用できなくなります。VDI の高可用性は、最少で 3 個の RAS Connection Broker を設置することで実現されます。このようにすれば、いずれかの Connection Broker が（組み込みの Provider Agent と共に）オフラインになった場合に、プロバイダーは次に使用可能な Connection Broker で実行中の Provider Agent へと自動的に割り当てられます。

VDI の高可用性を構成するには、以下の情報と手順を使用します。

最低 3 個の Connection Broker が必要

最低 3 個の RAS Connection Broker がインストールされ、実行されていることを確認します。サイトの RAS Connection Broker がオンラインになると、自動的に高可用性が有効になります。さらに別の Connection Broker をスタンバイモードにしておくこともできますが、高可用性を機能させるためには、最低 3 個の Agent をアクティブな状態にしておくことが必要です。すべての Connection Broker が相互に通信可能な状態にしておく必要があります。

Agent 数は奇数を推奨

発生の可能性があるスプリットブレインの状況を適正に制御するため、必ず半数を超える利用可能な Connection Broker が、いつでも相互に通信可能な状態にしておく必要があります。次の例を考えてみましょう。

- あるサイトに 3 個の Connection Broker があるとします。それらすべてが相互に通信可能です。1 個の Agent が他の 2 個と通信できなくなった場合、2 個の Agent は自分たちが過半数であることを認識し、その時点で最初の Agent で管理されていたプロバイダーホストを引き継ぎます。
- では、4 個の Connection Broker が存在する状況を考えましょう。1 個が他の 3 個に接続できなくなった場合は、上の例と同じシナリオが発生します。しかし、もし 2 個の Agent が別の 2 個の Agent と接続できなくなった場合、どちらのグループも過半数にならず、プ

ロバイダーホストをどの Agent が引き継ぐかを判断できません。このような状況では、Agent がそれぞれ独立して動作を続けてしまうスプリットブレインシナリオを回避するための手順に従う必要があります。この問題の解決策としては、同時にすべての Agent がすべてのプロバイダーを無視することで、データの損失や他の起こりうる問題の発生を防ぎます。

上に説明した理由から、インストールする Connection Broker の数はいつでも奇数にしておく必要があります。このようにすれば、Agent のグループのいずれかがいつでも過半数となり、すべてのプロバイダーの処理を継続できます。一般的に推奨されるのは（ここで説明されている高可用性の必要性にかかわらず）、1 つのサイトに 3 個の RAS Connection Broker を設定することです。詳細については、「セカンダリ Connection Broker」（p. 79）を参照してください。

スタンバイモード（p. 77）の Connection Broker は、高可用性の処理には関わらないことに注意してください。それらの Agent は、いずれかのアクティブな Connection Broker が完全にオフラインになるまで非アクティブのままです。そのような状況が発生すると、スタンバイモードの Agent がアクティブになり、失われた Agent の代わりになります。この時点以降この Agent は、高可用性セットアップの一部と考えることができます。失われた Agent がオンラインに戻ると、すべてが以前の状態に戻ります。

高可用性向けのプロバイダー構成

Parallels RAS は、以下の方法で高可用性を維持することができます。

- Parallels RAS は、自動的にプロバイダーの Connection Broker を選択します。この Connection Broker が停止した場合、Parallels RAS は残りの Agent のいずれかにワークロードを移動します。
- プロバイダーの Connection Broker は手動で選択します。この Connection Broker が停止した場合、Parallels RAS は残りの Agent のいずれかにワークロードを移動します。

高可用性を実現するには、次のいずれかの方法でプロバイダーを構成します。

- 既存のプロバイダーについては、[プロパティ] ダイアログを開き、[Agent 設定] タブを選択し、[推奨 Connection Broker] フィールドで [自動] を選択するか、手動で任意の Connection Broker を選択します。
- 新しいプロバイダーを追加する場合、ホストタイプとアドレスを指定する 2 番目のウィザードページで、詳細設定リンクをクリックし、[優先 Connection Broker] ドロップダウンリストから [自動] を選択するか、手動で優先する Connection Broker を選択します。3 個以上の Connection Broker を使用できる場合は、[自動] オプションがデフォルトで選択されています。

サイトのデフォルト値（VDI）

サイトのデフォルト値はサイトレベルで定義される設定で、テンプレートとゲスト VM（テンプレートベースのものとテンプレートベースでないものの両方）により使用されます。デフォルトでテンプレート（本章の後半で説明します）にこれらの設定が継承されますが、必要な場合はテンプレートの構成時に上書きできます。デフォルトでは、テンプレートベースでないホストもサイトのデフォルト値の設定を使用します。また、必要に応じてこれらの VM の構成時に上書きすることもできます。

サイトのデフォルト値を表示し、変更するには、次の操作を実行します。

1 [ファーム] > <サイト> > [VDI] に移動します。

2 右側のペインで [パーシスタントゲスト VM] タブを選択します。

3 [タスク] > [サイトのデフォルト値] をクリックします。これにより、後述する [サイトのデフォルトプロパティ] ダイアログが開かれます。

サイトのデフォルト値に加えた変更はすべて、その設定を使用している現在のサイトの全ホストに即座に適用されます。

一般

[一般] タブには次のプロパティが含まれています。

- セッション準備状態のタイムアウト: セッションを確立するのに必要な最大時間を指定します。指定したタイムアウト時間内にセッションの準備ができない場合、ユーザーにはエラーメッセージが表示され、再度ログインを試みる必要があります。
- プロトコル: ホストとの通信に Parallels RAS で使用するプロトコルを指定します。
- 準備に失敗したホストを自動削除するまでの時間: 準備段階でホストに（何らかの理由で）問題が発生した場合、その VM はサーバーに残りますが、使用することはできません。[ステータス] 列（[ファーム] > <サイト> > [VDI] > [デスクトップ]）の「作成に失敗」という値により、このような VM を特定できます。このような VM は、修復されない限り、このフィールドに指定されている時間が経過すると自動的に削除されます。有効な期間は、ドロップダウンリストから選択するか、”8 日間”や”12 時間”などの値を入力することで設定できます。

- デスクトップの割り当てタイプ: パーシスタントなホストを UPN（ユーザーオプション）またはデバイスホスト名（デバイスオプション）のどちらで割り当てるかを指定します。各ホストは、パーシスタントな割り当てが有効な状態で、そこから公開されたリソースを使用する最初のユーザーまたはデバイスに自動的に割り当てられます。また、ホストを手動で割り当てることもできます。詳細については、[パーシスタントゲスト VM]（p. 220）を参照してください。
- ゲストが次の時間使われない場合にパーシスタンスを自動的に削除: パーシスタンスの自動削除を実行するまでの経過時間。希望の期間を指定することもできます（例: ”1 週間と 3 日間“）。

  注: RAS 17 以降、このオプションのデフォルト設定は、[削除しない] です。この点に注意してください。

ユーザープロファイル

「ユーザープロファイル」（p. 138）の説明に従って、このタブを構成します。

アプリケーションパッケージ

「MSIX アプリケーションパッケージの使用」（p. 576）の説明に従って、このタブを構成します。

最適化

「最適化」（p. 146）の説明に従って、このタブを構成します。

処理

アクション: ここにある 2 つのドロップダウンリストにより、セッションの切断またはログオフを実行するためのアクションを指定します。

Nutanix AHV（AOS）についての注意: AHV（AOS）は、VM に対するサスペンド操作をサポートしていません。[アクションを実行] フィールドで [サスペンド] を選択すると、セッションの切断が発生したときに AHV（AOS）VM にはアクションが適用されません（対応するエラーが Provider Agent ログに記録されます）。

セキュリティ

[セキュリティ] タブで、ユーザーにホストでリモートデスクトップに接続する権限を自動的に付与するかどうかを指定できます。次にその仕組みを説明します。リモートデスクトップユーザー（または管理者）グループに各ユーザーを手動で追加する代わりに、このオプションを有効にして、それを自動的に行うことができます。ユーザーがログオンすると、ユーザーは自動的に指定のグループに追加され、これに伴いサーバーでのリモートデスクトップ接続の権限（または管理者のフル権限）が付与されます。ユーザーがログオフすると、ユーザーはグループから削除されます（つまり、グループメンバーシップはセッションの時間中に限り確保されます）。

この機能のさらに重要なメリットを以下に説明します。

- 今後、リモートデスクトップユーザーグループにユーザーを追加する必要はなくなります。これによりユーザーは、Parallels Client の外部のサーバーとリモートデスクトップセッションを確立することができなくなります。
- 管理者グループにユーザーを自動的に追加することにより、ユーザーにアプリケーションをインストールし、他の管理タスクを実行する権限を付与できます。繰り返しになりますが、ユーザーは Parallels Client からはこれを実行することが可能ですが、標準的なリモートデスクトップツールを使用してサーバーに接続してこれを行うことはできません。

設定

[設定] タブには次のプロパティが含まれています。

- アクティブなセッションを中断するまでの時間: ユーザーが公開済みアプリケーションを閉じた後、セッションがログイン状態を保持する時間。デフォルトのタイムアウトは 25 秒です。これは、アプリケーションでのみ機能し、公開済みのデスクトップでは機能しません（ユーザーがデスクトップを閉じるときに、セッションはログオフされます）。このタイムアウトは、ユーザーがあるアプリケーションを閉じてから別のアプリケーションを開く場合に、不要なログインを回避するために使用されます。
- 任意の Connection Broker: このプロバイダーを割り当てる必要のある推奨 Connection Broker を選択します。WAN 経由で通信している複数の物理的な場所にサイトコンポーネントをインストールしている場合、この設定が役立ちます。より適切な Connection Broker を指定することによりネットワークトラフィックを減らすことができます。
- URL/メールのリダイレクトを許可: ユーザーがリモートアプリケーションで URL または HTML Mailto リンクを開くと、リンクはクライアントコンピューターにリダイレクトされ、リモートホストのアプリケーションではなく、ローカルのデフォルトアプリケーション（ウェブブラウザーまたはメールクライアント）で開かれます。このオプションではリダイレク

トを有効化または無効化できます。[構成] ボタンをクリックして、以下のオプションから選択します。

a 有効化（登録済みアプリケーションを置換） - このオプションでは、リンクのリダイレクトの代替メソッドを使用します。これにより、リモートサーバー側でデフォルトの Web ブラウザーとメールクライアントを”ダミー”アプリと置換します。これを行うことで、リンクを開く操作を中断し、クライアントコンピューターにリダイレクトできます。

b Windows シェル URL 名前空間オブジェクトのサポート - シェル URL 名前空間オブジェクトをサポートするということは、Parallels RAS がシェル名前空間 API を使用する公開済みアプリケーションでの操作を中断して、リンクを開くことができるということを意味します。これは多くのアプリケーションでの標準的な動作です。シェル URL 名前領域オブジェクトのサポートを無効する機能は、Parallels RAS の旧バージョンとの互換性のために備えられています。

- ドラッグ & ドロップを有効化: ドラッグ & ドロップ機能が Parallels Client 内でどのように機能するかを設定できます。[構成] をクリックして、[無効]（ドラッグ & ドロップ機能なし）、[サーバーからクライアントのみ]（ローカルアプリケーションへのドラッグ & ドロップのみ）、[クライアントからサーバーのみ]（リモートアプリケーションへのドラッグ & ドロップのみ）、[双方向]（双方向のドラッグ & ドロップ）から選択できます。

  注: この文書の作成時点では、ドラッグ・ドロップ機能が利用できるのは Parallels Client for Windows および Parallels Client for Mac のみです。

- RDP 転送プロトコルの管理: Parallels Client とサーバー間の接続に使用されるトランスポートプロトコルを選択します。これを実行するには、このオプションを選択し、[構成] ボタンをクリックします。
- ファイル転送コマンドを許可（Web および Chrome クライアント）: リモートセッションでのファイル転送を有効化します。ファイル転送を有効にするには、このオプションを選択し、[構成] ボタンをクリックします。詳細については、「リモートファイル転送を構成する」（p. 538）を参照してください。
- ドライブリダイレクトのキャッシュを有効化: リダイレクトされたドライブ上でのファイルの参照とナビゲーションをより高速にすることで、ユーザーエクスペリエンスを向上させます。詳細については、「ドライブリダイレクトのキャッシュ」（p. 152）を参照してください。

RDP プリンター

[RDP プリンター] タブでは、リダイレクトされたプリンターの名前変更フォーマットを構成できます。フォーマットは、サーバーのどのバージョンと言語を使用しているかによって異なる場合があります。構成したサーバーに固有の [RDP プリンター名のフォーマット] オプションを選択します。

- プリンター名（コンピューター名から）内のセッション番号
- セッション番号（コンピューター名から）プリンター名
- プリント名（リダイレクトセッション番号）

利用できる別の RDP 印刷オプションは [プリンター名にセッション数を入れない] です。

コンピューター管理ツールの使用

RAS Console から、サーバーで標準的なコンピューター管理タスクを直接実行できます。このタスクには、リモートデスクトップ接続、PowerShell、コンピューター管理、サービス管理、イベントビューアー、IPconfig、再起動などが含まれます。[ツール] メニューにアクセスするには、サーバーを選択して [タスク] をクリックし、[ツール] をクリックして目的のツールを選択します。詳しい説明については、「コンピューター管理ツール」（p. 569）を参照してください。

プロバイダー概要の表示

この章で説明したプロバイダーのエディターに加えて、利用可能なプロバイダーに関する概要も表示できます。このためには、次の操作を実行します。

1. RAS Console で、[ファーム] カテゴリーを選択して、中央のペインで [サイト] ノードを選択します。
2. 右ペインの [VDI] セクションに、利用できるサーバーが表示されます。
3. プロバイダーのエディターに移動するには、サーバーを右クリックして、[エディターに表示] を選択します。

詳細については、「RAS Console でのサイト」（p. 63）を参照してください。

リモート PC プール

リモート PC プールは、スタンドアロンの（可能ならドメインに参加した）PC のプールを作成するための Parallels RAS の機能です。そのプールを特定のユーザーに割り当てることも可能です。リモート PC プール機能は RAS VDI に統合されていて、ホストプールを処理するインフラストラクチャを利用できるようになっています。

リモート PC プールとリモート PC の比較

リモート PC は、Parallels RAS で公開したリソースをホストするのに使用できるスタンドアロンマシンです（物理マシンまたは仮想マシン）。リモート PC の管理には、Parallels RAS Console の [ファーム] > <サイト> > [リモート PC] セクションを使用します。「リモート PC」の章（p. 279）で、この機能を詳しく取り上げています。ここで取り上げるリモート PC プールは、スタンドアロンのリモート PC とは動作も操作方法も異なっています。リモート PC プールの管理には、RAS Console の [ファーム] > <サイト> > [VDI] セクションを使用します。

このセクションでは、以下の内容を説明します。

- プロバイダーの追加（p. 233）
- 「プロバイダーの構成」（p. 236）
- 「プールへのリモート PC の追加」（p. 236）
- 「プール内のリモート PC の管理」（p. 237）
- パーシスタントリモート PC（p. 239）
- 「RAS RAS Guest Agent のインストールオプション」（p. 239）

プロバイダーの追加

RAS Console でリモート PC プールをセットアップするには、まず [リモート PC] タイプのプロバイダーを追加する必要があります。これは、リモート PC プールの作成と管理のために存在する特殊なタイプです。実際のプロバイダーではないので、ハイパーバイザーをインストールする必要はありません。既存の VDI 機能を使用してコンピュータープールを作成して管理するだけです。このタイプのプロバイダーを追加すると、実際のプロバイダーのように管理できます。ただし、テンプレートの作成ができないことや、その他の VDI（ハイパーバイザー）固有の機能が使用できないことなど、いくらかの制限があります。

リモート PC タイプのプロバイダーを追加する手順は以下の通りです。

1 [ファーム] > <サイト> > [プロバイダー] に移動します。

2 [プロバイダー] タブで、[タスク] > [追加] をクリックします。

3 次のいずれかを選択します。

- リモート PC（動的）: この方法の場合は、Active Directory の情報を使用して PC を割り当てます。この場合に必要な操作は、ホストに割り当てるコンピューターアカウントが入っている組織単位（OU）を指定することだけです。
- リモート PC（静的）: この方法の場合は、リモート PC の FQDN または IP アドレスを（1 つずつ）入力するか、CSV ファイルからリストをインポートすることによって、リモート PC をプロバイダーに割り当てます。

4 ウィザードが開いたら、以下を指定します。

- 名前: プロバイダーの名前です。
- 説明: プロバイダーの説明です。
- アドレス: リモート PC プールを管理するサーバーの FQDN または IP アドレスです。これは、RAS Provider Agent がインストールされているサーバーでなければなりません。RAS Connection Broker サーバーを使用することも可能です。RAS Provider Agent が組み込まれているからです。しかし、専用の RAS Provider Agent を実行するサーバーならどれでも構いません。
- ユーザー名: UPN 形式のアカウント名です（たとえば `administrator@domain.local`）。このアカウントは、以前指定した、サーバー管理者権限を付与されているドメインユーザーアカウントである必要があります。静的 PC 割り当て（下記を参照）を使用する場合に限り、ローカル Windows アカウントを使用することも可能ですが、いくらかの制限があります。ドメインアカウントの使用をお勧めします。
- パスワード: アカウントのパスワードと説明（オプション）です。

5 [認証情報を管理する] ボタンをクリックして、RAS Agent の展開に使用するアカウントを指定します。

6 [詳細設定] リンクをクリックして、[プロバイダー詳細設定] ダイアログを開きます。このダイアログでは、次のオプションを選択できます。

- 専用 Provider Agent の使用: RAS Provider Agent を自分でインストールする（またはインストールした）場合は、このオプションを選択します。組み込み RAS Provider Agent （p. 165）を使用する場合はオプションをクリアします。

- Agent アドレス: 上にあるオプションを選択すると、このオプションが有効になります。RAS Provider Agent がインストールされている（またはこれからインストールされる）サーバーの FQDN または IP アドレスを指定します。物理ボックスまたは仮想マシンのいずれかを指定できます。
- 任意の Connection Broker: このプロバイダーの推奨 Agent にする RAS Connection Broker を選択します。詳細については、「VDI の高可用性の実現」（p. 226）を参照してください。

7 [次へ] をクリックします。

8 ウィザードには新しいプロバイダーが表示され、RAS Provider Agent のステータスも確認できます。問題がなければ、[次へ] をクリックします。

9 手順 3 で [リモート PC（動的] を選択した場合、以下を指定します。

- ターゲット OU: ホストに割り当てるコンピューターアカウントが入っている組織単位（OU）を指定します。[...] ボタンをクリックして Active Directory を参照することも可能です。なお、1 回の AD/OU 検索で、最大 1000 台のリモート PC を検索することができます。

  注: 動的な割り当てを選択する場合は、ドメインに参加している PC をリモート PC にする必要があります。そのような PC をローカル Windows ユーザーアカウントで管理することはできません。

  動的な割り当てを選択する場合は、各 PC に RAS Guest Agent をインストールすることも可能です。そのためには、RAS Guest Agent を展開するためのスクリプトを組み込んだグループポリシーを組織単位に追加します。そのようなスクリプトの例を以下に示します。

  ```
  msiexec /i RASInstaller-<version & build>.msi ADDLOCAL=F_GuestAgent
  /qn+ /norestart
  ```

  その他の Agent のインストールオプションについては、「RAS Guest Agent のインストールオプション」（p. 239）を参照してください。

- サブネットマスク: リモート PC の IP アドレスから有線ブロードキャストアドレスを算出する際に使用するサブネットマスクです。Wake on LAN マジックパケットの指向性ブロードキャストの送信に使用されます。

10 手順 3 で [リモート PC（静的）] を選択した場合、以下のいずれかを実行します。

- [タスク] > [追加] をクリックし、追加する PC の FQDN または IP アドレスを入力します。[...] ボタンをクリックして検索することも可能です。次に、リモート PC の IP アドレスから有線ブロードキャストアドレスを算出する際に使用するサブネットマスク

を指定します。Wake on LAN マジックパケットの指向性ブロードキャストの送信に使用されます。次に、追加するコンピューターの MAC アドレスを入力します。すべてのフィールドが必須です。

- [タスク] > [CSV ファイルからインポート] をクリックし、コンピューターのリストが入っている CSV ファイルを選択します。CSV ファイルには次の 2 つの列が必要です。（1）FQDN または IP アドレス、（2）MAC アドレス。どちらの列も必須であり、有効な値が入っていなければなりません。

Parallels RAS 18（およびそれ以降）は、プロバイダーあたり最大 1000 台のリモート PC をサポートします。

注: ドメインに参加している PC をリモート PC として使用する方が、管理がしやすくなります。ここで説明している静的な割り当てを選択する場合は、ドメインに参加していない PC を追加することも可能ですが、各 PC で同じローカルユーザーアカウントを作成しなければなりません。ドメインアカウントとドメインに参加している PC の使用をお勧めします。

11 [完了] をクリックします。

プロバイダーへのリモート PC の追加

プロバイダーにリモート PC を追加するには、2 種類の方法があります。

- 「VDI ホストの追加」（p. 233）の説明に従ってプロバイダーを追加する際のウィザード
- このセクションで説明したように、プロバイダーを作成した後に利用します。

プロバイダーの作成後に、リモート PC を追加するには、次の操作を実行します。

1. 作成したプロバイダーを右クリックして、[プロパティ] を選択します。
2. [リモート PC] タブを選択します。
3. 「VDI ホストの追加」（p. 233）の手順 9 と 10 に従って、リモート PC を追加します。

プールへのリモート PC の追加

注: リモート PC プールでリモート PC を管理するには、リモート PC に RAS Guest Agent をインストールする必要があります。詳細については、「RAS Guest Agent のインストールオプション」（p. 239）を参照してください。

PC をプロバイダーに割り当てたら、以下の手順でその PC をリモート PC プールに追加できます。

1 [ファーム] > <サイト> > [VDI] で [プール] タブを選択します。

2 新しいプールを追加するために、[プール] ペインで [タスク] > [追加] をクリックします。

3 作成したプールを選択してから、[メンバー] ペインで [タスク] > [追加] をクリックし、以下のいずれかを選択します。

- ホスト内の全ホスト: プロバイダーに割り当てられているすべてのリモート PC を追加します。このオプションをクリックすると、プロバイダーを選択するためのダイアログが表示されます。ホストを選択して、[OK] をクリックします。
- ホスト: 個別のリモート PC を追加します。表示されるダイアログで、対象のリモート PC を選択し、[OK] をクリックします。リモート PC で RAS Guest Agent をアップグレードするかどうかを確認するためのダイアログが表示されることもあります（プールで PC を管理するには、この Agent が必要です）。[OK] をクリックして、Agent をアップグレード（またはインストール）してください。後から 1 つ以上の PC で RAS Guest Agent をアップグレードすることも可能です。その場合は、「RAS Guest Agent のインストールオプション」（p. 239）を参照してください。

1 つ以上のリモート PC をプールに追加すると、その PC が [プール管理] タブと [デスクトップ] タブに表示されます。

ヒント: メンテナンスのためにプールを無効にする必要がある場合は、プール名の前にあるチェックボックスをクリアしてそのプールを無効にできます。

プール内のリモート PC の管理

プール内のリモート PC の管理には、PC を特定のユーザーに割り当てる操作、RAS Guest Agent のアップグレード、PC のプロパティの表示や変更、標準的な管理タスクの実行などが含まれます。

プール内のリモート PC を管理するには、以下の手順を実行します。

1 [ファーム] > <サイト> > [VDI] で [プール] タブを選択します。

2 このタブのリストには、ホストやプール内のリモート PC も含め、管理対象のすべてのデスクトップが表示されます。[プール] 列でリストを並べ替えれば、特定のプールに割り当てられているリモート PC を確認できます。

3 リモート PC を選択し、[タスク] ドロップダウンリストをクリックし、以下のいずれかのオプションを選択します。[タスク] メニューに表示されるすべてのオプションがリモート PC に当てはまるわけではありません。下記のリストでは、プール内のリモート PC で使用できるオプションだけを取り上げています。

リモート PC に当てはまる [タスク] メニューのオプションは以下の通りです。

- すべての Agent をアップグレード: リストに含まれているすべてのリモート PC（とゲスト VM）の RAS Guest Agent をアップグレードします。
- 割り当てる: リモート PC を特定のユーザーに割り当てます（PC をパーシスタントの状態にします）。メニューオプションをクリックして、ユーザーを指定してください。
- 割り当て解除: リモート PC のユーザーの割り当て（パーシスタントの設定）を解除します。
- セッションを表示: [セッション] タブに切り替えて、セッション情報を表示します。
- ツール: 一連の標準的な操作を実行できます。リモートデスクトップ接続の確立、ping、リモート PC の再起動/シャットダウンなどです。電源操作の説明については、以下の「電源操作の実行」を参照してください。
- トラブルシューティング: リモート PC の RAS Guest Agent をチェックして、インストール/アップグレードします。
- プロパティをリセット: リモート PC のプロパティをデフォルト値にリセットします。下の [プロパティ] を参照してください。
- プロパティ: リモート PC の設定を表示したり確認したりするためのダイアログが開きます。[概要] タブでは、プール内のリモート PC を一時的に無効にできます（[このホストを使用しない] オプションを使用します）。PC でメンテナンスタスクを実行する必要があるときに便利なオプションです。リモート PC の表示名、コンピューター名、プロバイダーとの通信で使用するポート番号の表示や変更も可能です。[設定] タブと [セキュリティ] タブの説明については、「サイトのデフォルト値」（p. 228）を参照してください。

電源操作の実行

リモートによる電源操作を行うには、VM 上で動作する Windows で WMI が有効になっており、TCP ポート 30004 および 30005 が開いている必要があります。本ガイドの執筆時点で、この機能は Parallels RAS では自動化されていませんが、以降のバージョンで自動化される予定です。

ホストで電源操作（起動、停止、再起動、サスペンド、リセット）を実行するには、[VDI] > [デスクトップ] のタブを開き、ホストを選択してから、[タスク] をクリックして、実行する操作を選択します（起動と停止の操作は、上部にある該当のアイコンをクリックします）。再起動操作（猶予）には 10 分間のタイムアウトがあります。この時間内に操作が完了しない場合は、リセット操作（強制）となります。

Nutanix AHV（AOS）を使用している場合、サスペンド操作は利用できないことに注意してください（[サスペンド] アイコンは無効になっています）。これは、Nutanix AHV（AOS）では仮想マシンのサスペンド操作がサポートされていないためです。

パーシスタントリモート PC

パーシスタントリモート PC とは、特定のユーザーに割り当てられた PC のことです。PC を割り当てると、他のユーザーはその PC に接続できません。

リモート PC をパーシスタントの状態にするには、2 つの方法があります。

- 公開ウィザードを使用してプール内のリモート PC からリソース（アプリケーションやデスクトップなど）を公開するときに、[バーチャルゲストの設定] セクションで [パーシスタント] オプションを選択できます。そうすると、その公開済みのリソースを最初に開いたユーザーにプール内のリモート PC が割り当てられます。詳細については、「プール内のリモート PC からの公開」を参照してください。
- 手作業でリモート PC をユーザーに割り当てることもできます。そのためには、[ファーム] > <サイト> > [VDI] に移動し、[デスクトップ] タブを選択し、リストからリモート PC を選択して [タスク] > [割り当て] をクリックします。表示されるダイアログで、ターゲットユーザーを指定します。

リモート PC からパーシスタント設定を解除するには、[デスクトップ] タブでその PC を選択し、[タスク] > [割り当て解除] をクリックします。

RAS Guest Agent のインストールオプション

リモート PC プールでリモート PC を管理するには、リモート PC に RAS Guest Agent をインストールする必要があります。そのためには、以下のいずれかのオプションを使用します。

- 1 つのリモート PC をプールに追加する場合は、Agent をアップグレードするかどうかを確認するためのダイアログが表示されます。画面の指示に従って、インストールまたはアップグレードしてください。
- ホスト内のすべてのリモート PC をプールに一括で追加する場合は、まず追加してから、[デスクトップ] タブの [タスク] > [すべての Agent をアップグレード] メニューオプションを使用します。
- Active Directory を使用してリモート PC をプロバイダーに割り当てる場合は、Agent を展開するためのスクリプトを組み込んだグループポリシーを OU に追加できます。「プロバイダーの構成」 > 「動的（VDI サブタイプ）」（p. 236）を参照してください。
- 1 つのリモート PC で Agent をインストール/アップグレードするには、[デスクトップ] タブでその PC を選択し、[タスク] > [トラブルシューティング] > [Agent をチェック] オプションをクリックします。表示されるダイアログで [インストール] をクリックします。
- 最後に、RAS Guest Agent を手作業でインストールすることも可能です。その場合は、リモート PC で Parallels RAS のインストーラーを実行し、RAS Guest Agent コンポーネントのインストールを選択します。

第　10　章

Azure Virtual Desktop

Azure Virtual Desktop（旧称: Microsoft Windows Virtual Desktop）は、Microsoft Azure 上で動作するデスクトップおよびアプリ仮想化サービスであり、Windows 10/Windows 11 Enterprise マルチセッションホストの新機能を含む RD セッションホストおよび VDI へのアクセスを提供しています。Parallels RAS 18 は、Parallels RAS の既存の技術的機能に加えて、Azure Virtual Desktop のワークロードを統合、構成、保守、サポートしたり、アクセスを確保したりする機能を提供します。

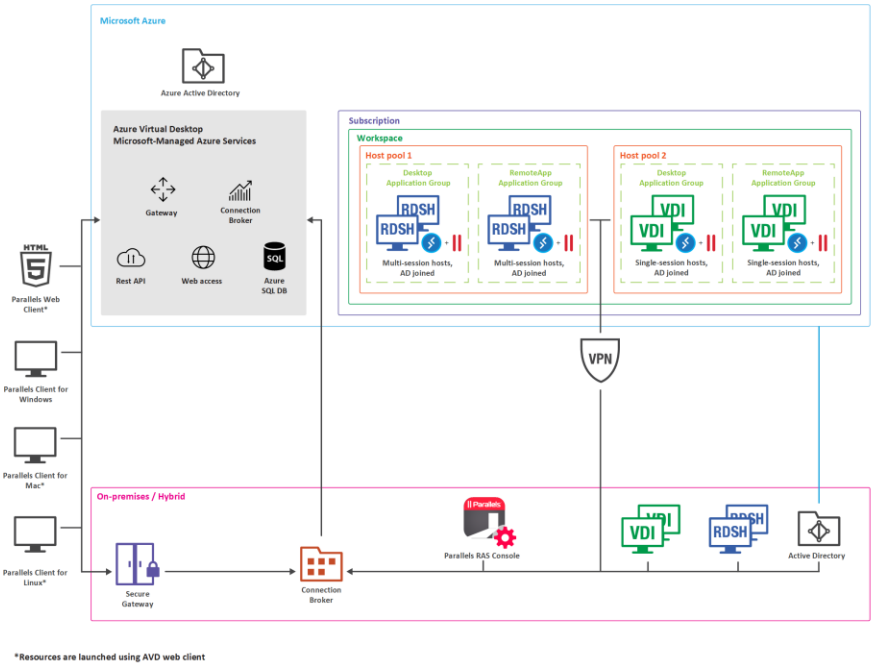
この章の内容

はじめに

次の図は、Parallels RAS と Azure Virtual Desktop のハイブリッド展開を示しています。以下の特徴があります。

- ワークロードホストは、Parallels RAS の標準の展開によるオンプレミスでも、Microsoft Azure 上（サービス経由）でも利用できます。
- ワークスペース、ホストプール、デスクトップ、RemoteApp グループなどの Azure Virtual Desktop オブジェクトは Parallels RAS Console から作成および構成されます。
- Azure Virtual Desktop ホスト（マルチセッションまたはシングルセッション）には、管理と構成のために Azure Virtual Desktop Agent と RAS Agent の両方が含まれています。

- Parallels Client for Windows は Parallels RAS Secure Gateway と Azure Virtual Desktop サービスの両方に接続し、エンドユーザーにリソースの可用性を単一のインターフェイスで提供します。



拡張された価値と機能

- Azure Virtual Desktop のデプロイおよび管理の簡素化と拡張。
- 管理とユーザーエクスペリエンスを一体化 - 一元的なインターフェイス - Parallels Client および Parallels RAS Console。
- ハイブリッドおよびマルチクラウド展開により、柔軟性を備えた上で範囲を拡張。
- 管理ルーチン、Azure Virtual Desktop ワークロードのプロビジョニングおよび管理の自動化と合理化。
- Microsoft Azure やオンプレミスでの組み込み自動スケーリング機能。
- ユーザー、セッション、プロセスの管理。
- RAS ユニバーサルプリントおよびスキャンの使用。
- AI ベースセッションの事前起動により超高速ログオンを実現。
- ドライブリダイレクトのキャッシュを有効にすることで、ファイルのリダイレクトを高速化。

- 統合された自動イメージ最適化と FSLogix プロファイルコンテナー。
- クライアント管理。
- クライアント向けセキュリティポリシー。
- RAS Console からの RAS レポートおよびモニタリングの活用。

前提条件

Azure Virtual Desktop の使用と Parallels RAS 環境における構成に必要な前提条件を以下に列挙します。

Microsoft Azure のサブスクリプション

以下を含む Microsoft Azure のサブスクリプションが必要です。

- Azure テナント ID。
- 十分なクレジットがある Azure サブスクリプション。

Azure Virtual Desktop ユーザーライセンス

以下のライセンスをお持ちのお客様は、Azure のコンピューティング、ストレージ、およびネットワークの使用料の請求を除き、追加料金なしで Azure Virtual Desktop を使用することができます。

Windows 10 および Windows 11 を Azure Virtual Desktop で実行するには、ユーザーごとに次のいずれかのライセンスが必要です。

- Microsoft 365 F3/E3/E5/A3/A5、学生使用特典または Business Premium
- Windows 10 Enterprise E3/E5
- Windows 10 Education A3/A5
- Windows 10 VDA（ユーザー単位）

Windows Server 2012 R2/2016/2019、2022 を実行するには、以下が必要です。

- ユーザーごと、またはデバイスごとに、有効なソフトウェアアシュアランス（SA）を備えたリモートデスクトップサービス（RDS）クライアントアクセスライセンス（CAL）。

詳細については、https://docs.microsoft.com/ja-jp/azure/virtual-desktop/overview の Microsoft ライセンス要件を参照してください。

権限および Azure リソースプロバイダー

サブスクリプションに登録する権限とリソースプロバイダーは以下の通りです。

- Azure サブスクリプションでリソースプロバイダーを有効にし、仮想マシン（VM）を作成するためのパーミッション。
- 必要な Microsoft Azure リソースプロバイダー（[Azure ポータル] > [サブスクリプション] > [リソースプロバイダー]）を有効にする必要があります。Microsoft.ResourceGraph、Microsoft.Resources、Microsoft.Compute、Microsoft.Network、Microsoft.DesktopVirtualization が対象となります。

Microsoft Entra ID アプリケーション

Microsoft Entra ID アプリケーションの作成についての詳細は、「Microsoft Entra ID アプリケーションの作成」（p. 171）を参照してください。

Microsoft Entra ID アプリケーションを作成したら、Microsoft Azure ポータルで以下の API のアクセス許可をアプリケーションに付与します（[Microsoft Entra ID] > [アプリの登録] > [API のアクセス許可] > [アクセス許可の追加] > [Microsoft.Graph] > [アプリケーションのアクセス許可]）。

- [グループ] > [Group.Read.All]
- [ユーザー] > [User.Read.All]

> 注: Graph API のアクセス許可に User と Group を追加するとき、パーミッションタイプが”デリゲート”ではなく”アプリケーション”になっていることを確認してください。

リソースへの読み書きアクセス許可のアプリケーションへの付与。

- 作成した Microsoft Entra ID アプリケーションは、「Microsoft Entra ID アプリケーションの作成」（p. 171）で説明したように、Azure リソースへの読み取りおよび書き込みアクセス許可を持っている必要があります。「リソースへの読み書きアクセス許可のアプリケーションへの付与」を確認してください。

アプリケーションのロールとアクセス許可には、以下を含める必要があります。

- [サブスクリプション] > [アクセス制御（IAM）] からアプリケーションの”ユーザーアクセス管理者”ロール。
- [リソースグループ] > [アクセス制御（IAM）] からのリソースグループレベルの”共同作成者”ロール。

リソースグループの作成が必要な場合は、[サブスクリプション] > [アクセス制御（IAM）] からサブスクリプションレベルの共同作成者ロールも割り当てます。

注: リソースグループ外のリソースの表示や読み取りを行いたい場合は、アプリケーションにもサブスクリプションレベルで読み取り許可が与えられていることを確認してください。

Active Directory

- Active Directory 環境のサーバー、または Azure Active Directory Domain Services（AADDS）。https://azure.microsoft.com/ja-jp/services/active-directory-ds/ を参照してください。
- Azure AD Connect - 使用中の Active Directory と Microsoft Entra ID の間でユーザーを関連付けることができるように、この 2 つは同期している必要があります。
- Microsoft Entra ID に接続されているのと同じ Active Directory に、ユーザーが存在していなければなりません。Azure Virtual Desktop は B2B や MSA のアカウントをサポートしていません。
- Parallels Client で構成されたユーザーが Azure Virtual Desktop リソースにアクセスする場合、セッションホストが参加している Active Directory ドメインに、当該のユーザーが存在している必要があります。

その他

- セッションホストのドメインへの接続を提供する Azure Virtual Network。
- セッションホストは Active Directory のドメインへの参加が必要。
- （オプション）ハイブリッド Parallels RAS 展開を使用する場合、サイト間 VPN または ExpressRoute が必要。
- （オプション） Azure Files または Azure NetApp Files 上で実行される FSLogix プロファイルコンテナーに使用する共有ネットワークの場所。

注: 執筆時点では、Parallels RAS は、Windows 7 を Azure Virtual Desktop セッションホストとしてサポートしていません。

その他の注意事項

異なる RAS ファームと RAS サイトのシナリオでは、以下のプロバイダーと Azure アプリケーションの要件にも注意してください。

- 同じ RAS ファーム、同じ RAS サイト。同じファーム、サイト、アプリケーション ID は VDI と Azure Virtual Desktop の両方で使用することが可能です。Azure Virtual Desktop プロバイダー用の Azure Virtual Desktop タグ付きゲスト VM リストを構築し、Azure プロバイダー用の VDI タグ付きゲスト VM（またはタグなし）を構築します。
- 同じ RAS ファーム、同じ RAS サイト。同じタイプの複数のプロバイダーには、異なる Azure アプリケーションを使用することをお勧めします。つまり、複数の Azure Virtual Desktop や複数のプロバイダーが混在していない場合です。
- 同じ RAS ファーム、異なる RAS サイト、または異なる RAS ファーム。上記と同じ注意が必要です。あるいは、異なる RAS ファームまたはサイトは、共通の VM セットとの通信を行わずに、異なる仮想ネットワークに配置することができます（このケースでは、その必要があります）。

重要: Parallels RAS で管理されている Azure Virtual Desktop オブジェクトは、Parallels RAS Console で管理することをお勧めします。Parallels RAS Console 以外で構成を変更すると、Azure Virtual Desktop オブジェクトが壊れた状態になることがあります。そのような場合、Parallels RAS により、オブジェクトを修復することができます。たとえば、ワークスペースやホストプールの自動作成されたフレンドリー名や関連するタグは Microsoft Azure ポータルからも表示できますが、これらは適切な機能を確保するために使用されるため、編集することはできません。

Azure Virtual Desktop の展開

Parallels RAS での Azure Virtual Desktop の展開は、以下のような一連のウィザードにより行います。

1. 機能を有効化し Azure Virtual Desktop プロバイダーを追加します。
2. Azure Virtual Desktop ワークスペースを追加します。
3. Azure Virtual Desktop ホストプールを追加し、スタンドアロンまたはテンプレートベースのホストをホストプールに追加します。
4. Azure Virtual Desktop リソースを公開します。

単一のデプロイ手順の一部として、[スタート] カテゴリーからすべてを実行できます。その方法についてはこの後説明します。

Azure Virtual Desktop の有効化とプロバイダーの追加

Azure Virtual Desktop の統合は、まず RAS ファームで有効にする必要があります。これは、RAS Console 内の以下の 2 つの場所から行うことができます。

- [スタート] カテゴリーの [Azure Virtual Desktop のデプロイ] ウィザードを使用する。
- [ファーム] > [サイト] > [設定] に移動し、[機能] タブを選択する。

[スタート] カテゴリーから Azure Virtual Desktop を有効化してデプロイする場合は、以下の手順になります。[サイト] > [設定] の [機能] タブには、後述の [機能の有効化] のページと同じ要素があります。

注: RAS ファームで Azure Virtual Desktop をまだ有効にしていない場合、ウィザードページは以下に説明する順番で開きます。Azure Virtual Desktop がすでに有効になっている場合（前にウィザードを実行した場合や、サイト設定から Azure Virtual Desktop を有効にした場合など）、最初の 2 つのページはスキップされ、最初に表示されるページは「Azure Virtual Desktop Provider の追加」となり、そこでプロバイダー情報を入力する必要があります。

デプロイを開始するには、次の操作を実行します。

1. Parallels RAS Console で、[Start] カテゴリーを選択し、[Azure Virtual Desktop のデプロイ] ウィザードを起動します。
2. システムとユーザーの要件: 最初のページで、システムとユーザーの要件を確認します。ページの下部にあるリンクをクリックして、Parallels ナレッジベースの記事を読んで詳細を確認します。[次へ] をクリックします。
3. 機能の有効化: このページでは、RAS ファームの Azure Virtual Desktop を有効にすることができます。まず、Azure Virtual Desktop エージェントとブートローダーを格納する場所を以下のオプションから選択します。
   - Connection Broker: RAS Connection Broker サーバーに保存します。
   - ネットワーク共有: ネットワーク共有を指定または選択します。
4. [エージェントとブートローダーのダウンロード] ボタンをクリックします。ダウンロードが完了するのを待ち、[ステータス] セクションに、「利用可能」と示され、バージョン番号が表示されていることを確認します。Azure Virtual Desktop エージェントの新しいバージョン

が利用可能な場合は、Parallels RAS からデプロイされた新しいサーバーが、アップデートされたバージョンを使用するように、「アップデートが必要」と表示されます。

5 [クライアント機能のセット] の選択では、Parallels Client で公開済みリソースを開いたときに利用できるクライアント機能を指定します。次のオプションから選択します。

- 標準: 標準的な機能のセットです。これは、Azure Virtual Desktop からアプリやデスクトップにアクセスするためのクライアントである Microsoft Windows デスクトップクライアント（リモートデスクトップ（MSRDC）クライアントとしても知られています）を使用して公開済みリソースを開いて実行する場合と同じです。
- アドバンスト: このオプションも Windows デスクトップクライアントを使用しますが、ドラッグ & ドロップなどの Parallels Client のアドバンスト機能が追加されます。
- フォールバック機能付きアドバンスト: このオプションでは、まずアドバンスト機能のセットを使用して公開済みリソースを開こうとします。アドバンスト機能が何らかの理由で動作しない場合は、標準オプションを使用してリソースを開こうとします。

6 これで、RAS ファームの Azure Virtual Desktop を有効にするタスクは完了です。[次へ] をクリックし、次のページに進みます。

7 Azure Virtual Desktop プロバイダーの追加: このページでは、Microsoft Azure のテナント ID、サブスクリプション ID、アプリケーション ID、および秘密鍵を指定する必要があります。これは、Parallels RAS で Microsoft Azure をプロバイダーとして設定するのと似ています。これらのプロパティの指定方法については、「Microsoft Azure をプロバイダーとして追加」（p. 175）を参照してください。サブスクリプション詳細の下にある URI/URL は、プロバイダーの作成中に編集できることに注意してください。[フィード URL] 設定（デフォルトでは https://rdweb.wvd.microsoft.com/api/arm/feeddiscovery）も、Azure Virtual Desktop プロバイダーを作成した後に編集することができます。

8 [次へ] をクリックして、概要を確認し、[完了] をクリックします。プロバイダー作成後に Microsoft Azure アプリのアクセス許可を変更すると、新しいアクセス許可がロードおよび使用されるようにするため、Parallels RAS 冗長サービスの再起動が必要になる場合があることに注意してください。

これで、一連のウィザードのうち、最初の段階が完了しました。最後のページでは、[Azure Virtual Desktop ワークスペースウィザードの起動] オプションがデフォルトで有効になっています。これにより、Azure Virtual Desktop ワークスペースを追加するための次のウィザードが自動的に開きます。

ワークスペースを追加

ワークスペースは、Azure Virtual Desktop のアプリケーショングループの論理グループです。各 Azure Virtual Desktop アプリケーショングループは、ユーザーが公開済みのリモートアプリやデスクトップを表示するために、ワークスペースに関連付けられている必要があります。

ワークスペースを追加するには、次の操作を実行します。

1 新しいワークスペースを作成する、または既存のワークスペースから選ぶのどちらかを選択します。

- 既存のワークスペースを選択するには、[名前] フィールドの横にある [...] ボタンをクリックします。
- 新しいワークスペースを作成するには、名前と説明（オプション）を入力します。既存のリソースグループを選択するか、新しいリソースグループを作成します。場所を指定します。ここで選択した場所は、ワークスペース、ホストプール、アプリケーショングループなど、すべての Azure Virtual Desktop オブジェクトで使用されます。

[フレンドリ名] フィールドで、Azure Virtual Desktop および Parallels RAS でこのワークスペースに使用される名前を指定します。

2 [次へ] をクリックして、概要を確認し、[完了] をクリックします。

ウィザードの最後のページでは、デフォルトで [Azure Virtual Desktop ホストプールウィザードを起動] オプションが選択されています。これにより、[完了] をクリックすると、[Azure Virtual Desktop ホストプールの追加] ウィザードが自動的に開きます。

ホストプールを追加（Azure Virtual Desktop）

ホストプールは、Azure Virtual Desktop 環境内の 1 つまたは複数の同一の仮想マシン（VM）の集合体です。各ホストプールには、ユーザーがアクセスできるアプリケーショングループが含まれています。

ホストプールを追加するには、次の操作を実行します。

1 RAS Console で、[ファーム] > <サイト> > [AVD] > [ホストプール] に移動します。

2 プールリストの上にある [タスク] ドロップダウンリストをクリックして、[追加]（またはプラス記号アイコン）をクリックします。[AVD ホストプールを追加] ウィザードが開きます。

3 新しいホストプールを作成する、または既存のホストプールから選ぶのどちらかを選択します。

- 既存のワークスペースを選択するには、[名前] フィールドの横にある [...] ボタンをクリックします。
- 新しいホストプールを作成するには、[ホストプールの新規作成] を選択し、プロバイダー、ワークスペース、名前、説明、リソースグループ、およびロケーションを選択します。

[フレンドリ名] フィールドで、Azure Virtual Desktop および Parallels RAS でこのホストプールに使用される名前を指定します。

4 [次へ] をクリックします。

5 [構成] ページで、以下を指定します。

- ホストプールの種類: [プール済み]（マルチセッションホスト）または [パーソナル]（シングルセッションホスト）から選択します。
- 公開の種類: プールを使用する目的に応じて、[アプリケーション] または [デスクトップ] から選択します。
- ロードバランサー: ロードバランサーの種類を選択します。幅優先の負荷分散では、ホストプール内のセッションホスト間でユーザーセッションを均等に分散させることができます。深さ優先の負荷分散では、ホストプール内のユーザーセッションで 1 つのセッションホストを飽和させることができます。最初のセッションホストがセッション制限のしきい値に達すると、ロードバランサーは、ホストプール内の次のセッションホストにその制限に達するまで新しいユーザー接続を送ります。
- ホスト上のセッション数の制限: プールのタイプが、プール（マルチセッション）の場合、ホスト上で許可されるセッションの最大数を指定します。
- オンデマンドのホスト稼働: 電源が入っていないホストを、ユーザーが接続しようとしたときに電源を入れるかどうかを指定します。これは、ホストプール内にあるすべてのセッションホストで電源が投入されていない場合に限り適用されることに注意してください。
- デフォルトのライセンスタイプ: Azure ライセンスタイプを選択します。
- サービスアップデートの検証: このホストプールを Microsoft サービス更新の検証環境にする場合は、[検証環境] オプションを選択します。

6 [次へ] をクリックします。

7 [プロビジョニング] ページで、このホストプールにテンプレートベースのホストを含めるか、スタンドアロンホストを含めるかを選択します。

- テンプレート: ホストはテンプレートから動的に作成されます。次のステップ以降で、テンプレートを作成するか、既存のテンプレートを選択する必要があります。プロビジョニングタイプとして [テンプレート] を選択すると、均質なホストプールが確保されます。ホストプール全体で一貫したユーザーエクスペリエンスを提供するには、この選択を推奨します。テンプレートを作成する方法については、「テンプレートの作成」 （p. 261）を参照してください。
- スタンドアロン: すでに存在する 1 つまたは複数のホストを選択します。これは、次のステップ、または後のステップでも行うことができます。ホストプールにホストを追加する前に、ホストがドメインに参加し、ドメイン環境のネットワークにアクセスできることを確認してください。スタンドアロンプロビジョニングは、自動スケールなど、機能の一部が欠けているため、「管理対象外」とみなされることに注意してください。

8 [次へ] をクリックします。

9 プロビジョニングページ（前述）での選択内容に応じて、以下のいずれかを実行します。

- スタンドアロン: リストからホストプールに含めるホストを 1 つまたは複数選択します（後からプールにホストを追加することもできます）。
- テンプレート: リストからテンプレートを選択するか、[新規作成] をクリックして新しいテンプレートを作成してからテンプレートの設定を指定します。バージョン: 既存のテンプレートを選択した場合は、そのバージョンのいずれかを選択します。自動スケールの有効化: （マルチセッションホスト）自動スケーリングを有効化して構成します。テンプレートのプロパティで指定されたサイズを上書き: また、通常はテンプレートのレベルで設定されている仮想マシンのサイズを上書きします。ここで指定したサイズは、このホストプールでのみ使用されます。同じテンプレートを使用している他のホストプールに影響はありません。なお、自動スケール設定により、後でそのようなホストプールから VM が取り出される場合、VM では直近で使用されていたサイズが維持されます。また、別のホストプールには新しく指定されたサイズで参加することができます。利用可能なサイズは、ホストプールのメンバーやテンプレートの場所、サイズ、電源状態によって異なる場合があります。

10 [次へ] をクリックします。

11 （テンプレートのみ）[プロパティ] ページで、次のオプションを指定します。

- テンプレート名: 選択してテンプレート名を入力します。
- 最大ホスト数: このテンプレートから作成できるホストの最大数を指定します。
- ウィザード完了時にデプロイされるホスト数: テンプレートが作成されたときに展開するホストの数。ホストは一度に 1 つずつ作成されるため、これには時間がかかることに注意してください。

- ホストプレフィックス: 新しいホスト名を指定するときに使用するパターン。

12 [次へ] をクリックします。

13 （テンプレートのみ）[設定] ページで、次のオプションを指定します。

- 使用可能なバッファを維持: このテンプレート用に、常に未割り当てでセッションが空いているホストの最小数です。空いているデスクトップと未割り当てのデスクトップの数が設定値を下回るとすぐに、このテンプレートから別のホストを強制的に作成します。テンプレートは、電源の初期状態を含め、ホスト作成のための独自の設定を使用します。
- 準備後のホストの状態: 準備が整ったホストに適用される電源状態を選択します。[使用中]、[停止中]、または [サスペンド] から選択します。電源状態が [停止中] または [サスペンド] に設定されている場合、実行中の（完全に準備が整い、受信接続を待っている）ホストの数は、[使用可能なバッファを維持] の設定（上記参照）によって制御されます。ホスト数の上限値が 200 に設定され、ウィザード完了時に展開されるゲストホストの数が 100 で、準備後の電源状態が“停止中”であるとします。このような構成の場合、100 の複製が展開され、停止中の状態になります。
- 未使用のホストの削除: リソースを節約するため、未使用のホストを処理する方法を選択します。削除しないように設定するか、削除されるまでの時間を指定します。

14 [次へ] をクリックします。

15 [割り当て] ページで、ホストプールのアプリケーショングループに割り当てるユーザーまたはグループを指定します。これは、ユーザーが公開済みのアプリケーションやデスクトップにアクセスできるようにするために必要です。[タスク] > [追加] をクリックして、ユーザーまたはグループを指定します。ウィザードの完了時に、[デスクトップ] または [RemoteApp] （該当する側）のタイプのアプリケーショングループが作成され、ホストプールに自動的に関連付けられます。

16 [ユーザープロファイル] ページで、[RAS で管理しない]（ユーザープロファイルは管理されません）または [FSlogix] から選択できます。Microsoft FSLogix プロファイルコンテナーを使用すると、パーシスタントでない環境でユーザーコンテキストを維持し、サインイン時間を最小限に抑え、互換性の問題を排除するネイティブプロファイルのユーザーエクスペリエンスを提供できるように構成されています。

17 画面の指示に従って、ウィザードを完了します。

18 [概要] ページでは、テンプレートの概要情報を確認します。必要に応じて、[戻る] ボタンをクリックして情報を修正できます。

19 最後に、[完了] をクリックしてホストプールを作成し、ウィザードを閉じます。

注: アドバンストクライアント機能のセットを使用している場合、Parallels のシームレステクノロジーを使用して構成されたデスクトップアプリケーショングループからアプリケーションを公開するため、アプリケーションの公開に RemoteApp グループは必要ありません。

次のステップ

Azure Virtual Desktop のデプロイの確認（p. 278）

Azure Virtual Desktop の管理

このセクションでは、Parallels RAS で Azure Virtual Desktop コンポーネントを管理する方法を説明します。

ここでは、以下を取り上げます。

- プロバイダーの管理（p. 253）
- ワークスペースの管理（p. 255）
- ホストプールの管理（p. 256）
- テンプレートの管理（p. 260）
- ホストの管理（p. 263）
- セッションの管理（p. 265）
- スケジューラーの使用（p. 266）

プロバイダー（Azure Virtual Desktop）の管理

Parallels RAS の Azure Virtual Desktop プロバイダーは、Azure リソースへアクセスするための ID やその他のプロパティの集合体です。プロパティには、テナント ID やサブスクリプション ID などがあります。通常、1 つの組織には Microsoft から 1 つのテナント ID が与えられますが、同じ組織が複数のサブスクリプション ID を所有する場合もあります。テナント ID とサブスクリプション ID の組み合わせごとに、Parallels RAS でプロバイダーを構成する必要があります。

Azure Virtual Desktop プロバイダーを管理するには、[ファーム] > [サイト] > [プロバイダー] に移動し、[プロバイダー] タブを選択します。

新しいプロバイダーを追加するには、[タスク] > [追加] をクリックして [Azure Virtual Desktop] を選択します。このウィザードを完了する方法については、「Microsoft Azure を VDI ホストとして追加」（p. 175）を参照してください。既存のプロバイダーに関するプロパティの一部を表示したり変更したりするには、リスト内のプロバイダーを右クリックして [プロパティ] を選択します。

その他のプロバイダー管理タスクは、[タスク] メニューからアクセスできます。以下のような管理タスクを実行できます。

- プロバイダーのステータスの確認: [タスク] > [トラブルシューティング] > [ステータスをチェック]。
- ログの構成と管理: [タスク] > [トラブルシューティング] > [ログ]。

Active Directory ドメインサービスのタイプを選択する

Parallels RAS 18.3 は、Windows Server Active Directory ドメインサービスおよび Azure Active Directory ドメインサービスに参加する仮想マシンをサポートします。デフォルトでは、Parallels RAS は Windows Server Active Directory ドメインサービスで動作するように設定されていますが、必要に応じて変更できます。

プロバイダーの Active Directory ドメインサービスの種類を選択するには:

1. 一覧からプロバイダーを右クリックして、[プロパティ] を選択します。
2. プロバイダーの [プロパティ] ウィンドウで [資格情報] タブを選択します。
3. [Active Directory ドメインサービスのタイプ] ドロップダウンリストで、Active Directory ドメインサービスのタイプを選択します。
   - Windows Server Active Directory でユーザーを作成し、仮想マシンを Windows Server Active Directory ドメインサービスに参加させる場合は、[Windows Server AD DS] を選択します（デフォルトで選択されています）。
   - Windows Server Active Directory でユーザーを作成し、仮想マシンを Azure Active Directory ドメインサービスに参加させる場合は、[Azure AD DS] を選択します。
   - Microsoft Entra ID でユーザーを作成し、仮想マシンを Azure Active Directory ドメインサービスに参加させる場合は、[Azure AD DS] を選択します。

ディスクストレージコストの最適化

[詳細] タブでは、Azure Virtual Desktop プロバイダーの構成を実行して、現在使用していない AVD ホストに搭載されているマネージドディスクのタイプを標準 HDD に自動変更するよう設定できます。AVD ホストを起動すると、管理ディスクは自動的に元のタイプに変更されます。この機能により、AVD ホストの維持にかかるコストを削減することができます。

ディスクストレージのコスト最適化を有効化するには:

1 一覧からプロバイダーを右クリックして、[プロパティ] を選択します。

2 プロバイダーの [プロパティ] ウィンドウで [詳細] タブを選択します。

3 [ディスクストレージコストの最適化を有効にする] オプションを選択します。

4 [ストレージコストの最適化を有効にする前のタイムアウトを設定] ドロップダウンリストで、必要なオプションを選択します。

ワークスペース（Azure Virtual Desktop）の管理

ワークスペースは、Azure Virtual Desktop のアプリケーショングループの論理グループです。各 Azure Virtual Desktop アプリケーショングループは、ユーザーが公開済みのリモートアプリやデスクトップを表示するために、ワークスペースに関連付けられている必要があります。

Azure Virtual Desktop ワークスペースを管理するには、[ファーム] > [サイト] > [Azure Virtual Desktop] に移動し、[ワークスペース] タブを選択します。

ワークスペースを追加するには、次の操作を実行します。

1 [タスク] > [追加] をクリックして [Azure Virtual Desktop ワークスペース] ウィザードを開きます。

2 ウィザードページの上部にあるプロバイダーの 1 つを選択します（複数のプロバイダーがある場合）。また、このページから直接プロバイダーを新規に作成することもできます。その場合は、[新規プロバイダー] ボタンをクリックして別のウィザードを開きます。詳細については、「プロバイダーの管理」（p. 253）を参照してください。

3 プロバイダーを選択（または作成）したら、「Azure Virtual Desktop ワークスペースの追加」（p. 249）の説明に従ってワークスペースウィザードを完了します。

既存のワークスペースのプロパティを表示するには、そのワークスペースを右クリックして [プロパティ] を選択します。ワークスペースを有効または無効にしたり、ワークスペースの説

明およびフレンドリ名を変更したりできます。その他のプロパティは読み取り専用です。ワークスペースを無効にすると、ホストプールや公開済みのリソースなど、関連付けられたオブジェクトがすべて無効になることに注意してください。

ホストプールを管理（Azure Virtual Desktop）

ホストプールは、Azure Virtual Desktop 環境内の 1 つまたは複数の同一の仮想マシン（VM）の集合体です。各ホストプールには、ユーザーがアクセスできるアプリケーショングループが含まれています。

ホストプールは、使用目的に応じていくつかの異なる方法で構成できます。次の表では、ホストプールを作成する際に選択できる個々のオプションについて説明します。

オプション	説明
個人用とプール	• 個人用ホストプールにはシングルセッションホストが含まれ、それぞれが単一のユーザーに割り当てられます。割り当ては、ユーザーがログオフした後やホストの電源がオフになった後も維持されます。必要に応じて、ユーザーのホストの割り当てを解除し、別のユーザーに割り当てることができます。 • プールホストプールには、特定のユーザーに割り当てられていないマルチユーザーセッションホスト（RD セッションホストまたはマルチセッション Windows 10 マシン）が含まれています。プール内の各ホストは、複数のユーザーに割り当てることができます（マルチセッション）。
アプリケーションとデスクトップ	ホストプールは、アプリケーションまたはデスクトップのみを公開できますが、両方を同時に公開することはできません。ホストプールを作成する際に、公開の種類を [デスクトップ] または [アプリケーション] から選択します。選択に応じて、ホストプールにデスクトップまたは RemoteApp のアプリケーショングループが自動的に作成されます。後から公開の種類を変更できないことに注意してください。変更する場合は、既存のホストプールを削除して新しいホストプールを作成する必要があります。
テンプレートとスタンドアロン	ホストプールを作成する際に、[テンプレート] または [スタンドアロン] から選択する必要があります。ホストプールには、すでに存在するホストを含めること（スタンドアロン）、またはテンプレートを使用することができます。テンプレートは、既存のゲスト VM をベースにしたり、Azure Marketplace または共有イメージギャラリーのイメージからその場で作成したりすることができます。 • テンプレート: ホストは、管理者が手動でテンプレートから作成することも、需要に基づいて自動的に作成することもできます。ホストの自動作成（Parallels RAS では自動スケールと呼ばれています）は、ホストプールのプロパティでオンまたはオフにすることができます。 • スタンドアロン: ホストは、管理者によってホストプールに追加、またはホストプールから削除されます。ホスト（仮想マシン）は、Azure にすでに存

	在し、ドメインに参加している必要があります。

Azure Virtual Desktop ホストプールを管理するには、[ファーム] > [サイト] > [Azure Virtual Desktop] に移動し、[ホストプール] タブを選択します。

ホストプールのプロパティを表示し、変更するには、ホストプールを右クリックして [プロパティ] を選択します。開いたダイアログでタブを選択し、次に説明するようにホストプールのプロパティを表示または変更します。

一般

[一般] タブでは、ホストプールを有効または無効にすることができます。無効にすると、ホストや公開済みのリソースがすべて無効になることに注意してください。

また、ホストプールの説明を変更したり、ホストプールのプロパティ全般を表示したりすることもできます。

[アプリケーショングループ] セクションには、ホストプール用に作成されたアプリケーショングループの名前が表示されます。

[フレンドリ名] フィールドには、Azure Virtual Desktop および Parallels RAS でこのワークスペースに使用される名前を指定します。

構成

[構成] タブで、ホストプールの構成プロパティを確認します。これらのプロパティについては、ホストプールを作成した時点で理解されているはずです。

このページでは、次のプロパティを変更できます。

- ロードバランサー
- ホスト上のセッション数の制限
- オンデマンドのホスト稼働
- 検証環境

構成プロパティの説明については、「Azure Virtual Desktop ホストプールの追加」（p. 249）を参照してください。

自動スケール

このタブは、プロビジョニングタイプとして [テンプレート] が指定されているホストプールに対してのみ表示されます。ホストプールにテンプレートがまだ指定されていない場合は、ここでテンプレートを選択することができます。[新規作成] ボタンをクリックしてウィザードを開き、新しいテンプレートを作成することもできます。テンプレートがない場合、選択可能なのは、ホストを作成するためのテンプレートがないことを示す [なし] だけです。その場合は、まずテンプレートを作成し、そして再度ここで選択する必要があります。「テンプレートの管理」（p. 260）も参照してください。

[自動スケール設定] セクションには、指定したテンプレートからホスト（仮想マシン）を作成する方法の設定が含まれています。これらの設定は、RD セッションホストグループの自動スケール設定と同様に機能します。唯一の違いは、Azure Virtual Desktop ではホストとホストプールを扱うのに対し、RD セッションホストグループではサーバーとグループを扱うことです。それ以外の設定は同様に動作します。詳細については、「RD セッションホストのグループ化と複製」（p. 115）の「自動スケール」サブセクションを参照してください。

[仕様] セクションでは、指定されたホストプールが使用するテンプレートの設定で、指定された仮想マシンのサイズを上書きできます。[テンプレートのプロパティで指定されたサイズを上書き] オプションを選択し、ドロップダウンリストから必要なサイズを選択します。選択したサイズは、このホストプールでのみ使用されます。同じテンプレートを使用している他のホストプールに影響はありません。なお、利用可能なサイズは、ホストプールのメンバーやテンプレートの場所、サイズ、電源状態によって異なる場合があります。また、サイズを上書きするにはホストの再起動が必要になります。ご注意ください。

ホスト

[ホスト] タブには、このホストプールのホストのリストが表示されます。表の値を見ることで、ホストの状態やその他のプロパティを確認できます。

ホストが正常に動作している場合は、[ステータス] 列に“OK”と表示されます。Agent のステータスを確認するには、ホストを右クリックして [Agent をチェック] を選択します。“Agent が応答しませんでした”というメッセージが表示されたら、[インストール] をクリックして Agent をインストールしてみてください。すべてが正常に進めば、Agent が更新され、[ステータス] 列に“OK”と表示されます。[タスク] > [すべての Agent をアップグレード] をクリックしてすべての Agent をアップグレードすることもできます。

新規のホストをプールに追加するには、次の操作を実行します。

1 [タスク] > [追加] をクリックします。

2 ホストプールのプロビジョニングタイプに応じて、次のいずれかを実行します。

- ホストプールのプロビジョニングが、スタンドアロンとして構成されている場合は、リストから 1 つまたは複数のホストを選択します。また、Azure 上の他のホストプールに存在するホストを表示するには、[既存のホストプール内のホストのうち RAS に管理されていないホストを表示する] オプションを選択することもできます。
- ホストプールのプロビジョニングが、テンプレートとして構成されている場合は、ここでホストを手動で追加することはできません。代わりに、Azure Virtual Desktop メインビューの [ホスト] タブを使用します。（p. 263）を使用します。

3 [OK] をクリックします。

アプリケーションパッケージ

「MSIX アプリケーションパッケージの使用」（p. 576）を参照してください。

割り当て

[割り当て] タブには、Microsoft Entra ID オブジェクトに割り当てられた Active Directory ユーザーとグループが表示されます。ユーザーが公開済みのデスクトップやアプリケーションを表示するには、ホストプールで利用可能なアプリケーショングループに割り当てられている必要があります。

新しい割り当てを作成するには、次のいずれかを実行します。

1 [タスク] > [追加] をクリックします。

2 [ユーザーまたはグループの選択] ダイアログで、ユーザーまたはグループを指定して、[OK] をクリックします。

3 画面の指示に従って、割り当てを完了します。[公開] カテゴリーの追加フィルタリングを使用して、Parallels Client での Azure Virtual Desktop リソースの可用性を管理することができます。詳細については、「リソースの公開」を参照してください。

ユーザープロファイル

デフォルトでは、このタブはサイトのデフォルト値を継承します。カスタム設定を指定する場合は、[デフォルト設定を継承] オプションのチェックを外します。ユーザープロファイルの構成については、「サイトのデフォルト値（Azure Virtual Desktop）」（p. 269）を参照してください。

最適化

[最適化] タブでは、Parallels RAS 環境で最高のパフォーマンスが得られるよう、セッションホストを最適化するための設定を指定できます。無効化、削除、または最適化の対象となる Windows コンポーネントやサービス、またその他のオプションを選択して、仮想アプリおよびデスクトップの配信の効率性と合理性を向上させ、改善することができます。デフォルトでは、このタブはサイトのデフォルト値を継承します。カスタム設定を指定する場合は、[デフォルト設定を継承] オプションのチェックを外します。最適化オプションの構成については、「サイトのデフォルト値（Azure Virtual Desktop）」（p. 269）を参照してください。

ホストプールの設定

このタブでは、セッションのタイムアウト、クライアント URL/メールのリダイレクト、ドラッグ & ドロップなどの設定を構成できます。デフォルトでは、このタブはサイトのデフォルト値を継承します。カスタム設定を指定する場合は、[デフォルト設定を継承] オプションのチェックを外します。ホストプール設定の構成については、「サイトのデフォルト値（Azure Virtual Desktop）」（p. 269）を参照してください。

RDP プリンター

[RDP プリンター] タブでは、リダイレクトされたプリンターの名前変更フォーマットを構成できます。 デフォルトでは、このタブはサイトのデフォルト値を継承します。カスタム設定を指定する場合は、[デフォルト設定を継承] オプションのチェックを外します。ユーザープロファイルの構成については、「サイトのデフォルト値（Azure Virtual Desktop）」（p. 269）を参照してください。

テンプレート（Azure Virtual Desktop）の管理

Azure Virtual Desktop テンプレートは、元の VM のクローンとして他の仮想マシンを作成し、セッションホストとしてホストプールに追加される仮想マシンです。

Azure Virtual Desktop テンプレートを管理するには、[ファーム] > [サイト] > [Azure Virtual Desktop] に移動し、[テンプレート] タブを選択します。

このセクションでは、以下の内容を説明します。

テンプレートの作成

テンプレートを作成するには、次の操作を実行します。

1 [テンプレート] タブで、[タスク] > [追加] をクリックします。これにより [Parallels テンプレートウィザードを作成] が開きます。

2 最初のページで、Azure Virtual Desktop プロバイダーを選択します（複数ある場合）。

3 テンプレートタイプを次の中から選択します。

- マルチセッション: Windows Server オペレーティングシステムや Windows 10/Windows 11 Enterprise マルチセッション上で実行される 1 つのホストに対して、複数の同時ユーザーセッションが認められています。
- シングルセッション: シングルユーザーセッションはシングルセッションホストで使用できます。

4 [テンプレートソース] ページで、次の中からソースを選択します。

- カスタムホスト: 既存の仮想マシンのリストが表示されます。
- Azure Gallery: イメージを選択して、そのイメージから新しい仮想マシンを作成できます。マルチセッションまたはシングルセッションのテンプレートタイプに応じて、Windows 10 Enterprise マルチセッションなどの一般的に使用されている Marketplace のイメージがあらかじめ定義されているので、簡単に選択してテンプレートとして作成することができます。場所を選択し、ローカル管理者のユーザー名とパスワードを指定します。[すべてのイメージを参照] ボタンをクリックするとダイアログが開き、Marketplace または共有イメージギャラリーから他のイメージを選択することができます。共有イメージギャラリーからイメージを選択する場合は、発行元、SKU、オファー、その他のオプションのリストから選択します。

5 [ホスト] ページで必要に応じて、あらかじめ定義されている Azure の値から仮想マシンのプロパティを選択します。

- まず、Azure リソースグループを指定します。
- 仮想マシンのサイズを選択します。

  注: 仮想マシンのサイズは、指定されたテンプレートを使用するホストプールの設定で上書きできます。これにより、ホストプールのレベルで異なる VM のサイズを指定することができます。

- ディスクの種類を選択します。
- 仮想ネットワークとサブネットを選択します。

> **注:** テンプレートに高速ネットワークを使用する場合は、高速ネットワークをサポートするセッションホストのホストサイズが適切なものになっていることを確認してください。

6 [概要] ページで、次の設定を指定します。

- テンプレート名: テンプレートの名前です。
- 可用性セットの作成: これを選択すると、テンプレートからホストが可用性セットでデプロイされます。可用性セットでデプロイできるホストの最大数は 200 であることに注意してください（これは Azure の制限です）。200 以上のホストが必要な場合は、このオプションをオフにして、[最大ホスト数] フィールドに独自の値を指定します。

7 [準備] ページでイメージの準備を選択し、必要なオプションを指定します。これは、RAS VDI テンプレートのイメージの準備方法と似ています。細かい違いはありますが、構成手順は基本的に同じです。詳細については、「準備」（p. 201）を参照してください。

8 [最適化] ページで、最適化設定を構成します。これらの設定は、サイトのデフォルト値を継承していますが、必要に応じてカスタム設定を指定することができます。詳細については、「サイトのデフォルト値（Azure Virtual Desktop）」（p. 269）を参照してください。

9 [新しいテンプレートのバージョン] ページで、名前と説明を指定し、バージョンのタグを選択します。タグは、複数選択できます。

10 [サマリ] ページで、設定を確認し、[完了] をクリックしてテンプレートを作成します。

既存のテンプレートの管理

テンプレートの変更

既存のテンプレートを変更するには、テンプレートを右クリックして [プロパティ] を選択します。多くのプロパティは変更できますが、いくつかのプロパティは変更できません。個別のプロパティと設定については、「テンプレートの作成」（p. 261）の説明を参照してください。

テンプレートを削除するには、リストからテンプレートを選択し、[タスク] > [削除] をクリックします。なお、本ガイドの執筆時点で、RAS Console でテンプレートを削除すると、テンプレートと関連するホストが Microsoft Azure から完全に削除されない可能性があるという既知の問題があります。該当のオブジェクトがすべて削除されていることの確認は、Azure ポータルから実行できます。

ホストプール（Azure Virtual Desktop）へのテンプレートの割り当て

ホストプールを作成し、そのプロビジョニングタイプをテンプレートとして設定する際に、既存のテンプレートを割り当てる必要があります。これは、ホストプールを作成または変更する

際に行うことができます。また、[テンプレート] タブでホストプールにテンプレートを割り当てることもできます。

ホストプールにテンプレートを割り当てるには:

1 テンプレートを選択し、[タスク] > [ホストプールに割り当て] をクリックします。

2 [タスク] > [プールに割り当て] をクリックします。ウィザードが開きます。

3 [バージョン] ページで、ホストプールに割り当てるテンプレートのバージョンを選択します。

4 （オプション）[ホストプール] ページで、スケジュールで再作成するホストプールを選択し、[構成] ボタンをクリックします。再作成を予約するダイアログが表示されます。必要に応じてスケジュールを構成し、[次へ] をクリックします。

5 [完了] をクリックします。

ホストプールからテンプレートを削除するには:

1 テンプレートを選択し、[タスク] > [ホストプールから削除] をクリックします。

2 [ホストプールから削除] ダイアログが開き、選択したテンプレートを使用しているすべてのホストプールが一覧表示されます。

3 テンプレートを削除する 1 つまたは複数のホストプールを選択し、[OK] をクリックします。

4 なお、ホストプールにホストがある場合は削除されます。メッセージが表示され、削除に同意する必要があります。

5 1 つまたは複数のホストプールが他の管理者によってロックされている場合、メッセージが表示されます。また、後でプールのロックが解除されたときに同様の操作を再び実行する必要があります。

ホストを管理（Azure Virtual Desktop）

Azure Virtual Desktop ホストを管理するには、[ファーム] > [サイト] > [Azure Virtual Desktop] に移動し、[ホスト] タブを選択します。

利用可能なすべてのホストプールに存在するホストのリストが表示されます。表をフィルタリングして、特定のプールのホストを表示したり、他の基準を使用してホストを表示したりすることができます。フィルタリングするには、虫眼鏡アイコンをクリックして、対象となる 1 つまたは複数の列でフィルターを指定します。

ホストに対して実行できるタスクは、[タスク] メニューからアクセスできます。タスクには、以下が含まれます。

- 追加: 利用可能なホストプールのいずれかにホストを追加します。後述の「ホストの追加」サブセクションを参照してください。
- 割り当て: このオプションは、個人用ホストプールのホストに対して有効です。これにより、選択したホストをユーザーに割り当てることができます。ホストがすでに他のユーザーに割り当てられている場合は、割り当てを変更するかどうかの確認を求められます。尋ねられたら、Microsoft Entra ID ユーザーを選択します。割り当ては Azure で行われるので、処理中はホストのステータスが“割り当て中”に変わります。
- 割り当て解除: 選択したホストからユーザーの割り当てを削除します。上記の「割り当て」を参照してください。このメニューオプションは、現在ユーザーが割り当てられているホストに対して有効です。処理中はホストのステータスが“割り当て解除中”に変わります。
- 検索: フィルタリングにより、リスト内のホストを検索することができます。
- セッションを表示: フィルタリングした [セッション] タブに切り替え、選択したホストのセッションを表示します。
- 公開済みのリソースを表示: 選択したホストから公開されているリソースのリストを表示します。
- アプリケーション情報を表示: 選択したホストに追加された MSIX アプリケーションパッケージが表示されます。
- コントロール: 選択したホストのログオンの有効化または無効化、保留中の再起動のキャンセル（スケジューラーが作成）、無効になっている状態のキャンセル（スケジューラーが作成）などのコントロールオプションを設定します。詳細については、「スケジューラーの使用」（p. 266）を参照してください。
- 起動、停止、リセット、再起動: 選択したホストで実行できる電源操作です。再起動操作（猶予）には 10 分間のタイムアウトがあります。この時間内に操作が完了しない場合は、リセット操作（強制）となります。
- すべての Agent をアップグレード: 必要に応じて、リスト内にあるすべてのホストの Agent をアップグレードします。
- 最適化の停止: ホストに最適化を適用した場合、初期の段階でキャンセルすることができます。詳細については、「最適化」（p. 146）を参照してください。
- ツール: リモートデスクトップ、コンピューターの管理、サービス管理、イベントビューアー、PowerShell などの標準的な RAS ツールがあります。詳しい説明については、「コンピューター管理ツール」（p. 569）を参照してください。

- トラブルシューティング: Agent の状態を確認し、必要に応じて更新することができます。また、ログの管理もできます。
- 詳細: ホストが作成できなかった場合の詳細を表示します。このオプションを選択すると、失敗の理由といくつかの追加情報を表示するダイアログが開きます。
- ライセンスタイプを変更: Azure のライセンスタイプを変更します。
- 再作成: ホストを再作成します。
- 削除: リストおよび所属するホストプールからホストを削除します。ホストプールのプロビジョニングタイプに応じて、ホスト（仮想マシン）自体を保持または削除します。テンプレートから作成されたホストは完全に削除されます。スタンドアロンホストの場合は削除されないので、仮想マシンはそのまま残ります。
- 更新: リストを更新します。

ホストの追加

[ホスト] タブから、ホストをホストプールに追加することができます。このためには、次の操作を実行します。

1 [タスク] > [追加] をクリックします。

2 [ホストの追加] ダイアログで、対象のホストプールを選択します。選択したホストプールに設定されているプロビジョニングタイプに応じて、次の操作を行います。

- スタンドアロン: リストから 1 つ以上のホストを選択します。また、下部のオプションを選択して、Parallels RAS によって管理されていない Azure 上に存在する他の既存ホストプールのホストを表示することもできます。
- テンプレート: テンプレートからプールに追加するホストの数を指定します。

3 [OK] をクリックします。

セッションを管理（Azure Virtual Desktop）

Azure Virtual Desktop セッションを表示および管理するには、[ファーム] > [サイト] > [Azure Virtual Desktop] に移動し、[セッション] タブを選択します。すべてのホストプール内に存在するすべてのホストのセッションがリストに表示されます。

セッションの管理の詳細については、「セッション管理」（p. 329）を参照してください。

スケジューラーを使用する（Azure Virtual Desktop）

[スケジューラー] タブでは、指定した時刻から指定した期間だけオフラインにすることで、1 つまたは複数のホストまたはホストプールのメンテナンス時間枠をスケジュールすることができます。また、1 つまたは複数のホスト/ホストプール全体の再起動、起動、シャットダウンをスケジュールすることもできます。

注: スケジュールされたイベントが発生すると、影響を受けるホストは Parallels RAS で無効化され、そのステータスは“無効（スケジューラー）”または“再起動保留中（スケジューラー）”と表示されます。[ホスト] タブでホストを右クリックし、[コントロール] > [無効になっている状態をキャンセルする（スケジューラー）]、または [コントロール] > [保留中の再起動をキャンセルする（スケジューラー）] を選択することで、これらの状態をキャンセルすることができます。

メンテナンス時間枠を構成するには、以下の操作を実行します。

1. [タスク] > [追加] > [ホストを無効化] または [ホストプールを無効化] をクリックします。どちらのシナリオも同様に構成されます。
2. [一般] タブで、[スケジュールを有効化] オプションを選択します。
3. このスケジュールの名前と説明（オプション）を指定します。
4. [利用可能] リストでホスト、またはホストプール（選択したアクションに応じて）を選択し、[追加] をクリックします。[対象] リストにホスト（またはホストプール）が表示されます。
5. [トリガー] タブを選択し、このイベントの開始日、開始時刻、期間、および繰り返しの設定を指定します。これを 1 回限りのイベントにするには、[繰り返し] フィールドで [なし] を選択します。
6. [オプション] タブを選択します。ここでは、ホストがオフラインになる前にユーザーに送信されるメッセージを構成できます。[タスク] > [追加] をクリックして、メッセージのタイトル、本文、送信する期間を指定します。
   - [オプション] タブの [無効時の処理] オプションでは、スケジュールされたタスクが発生したときに現在のセッションに対して何を実行するかを指定できます。ドロップダウンリストから必要なオプションを選択します。
7. [OK] をクリックしてスケジュールを保存します。

再起動のスケジュールを構成するには、以下の操作を実行します。

1. [タスク] > [追加] > [ホストを再起動] または [ホストプールを再起動] をクリックします。

2 [トリガー] タブで、スケジュールのプロパティは、上述の”ホストを無効化”タスクと同じ方法で指定します。さらに、”ホストプールを再起動”タスクに以下のオプションを指定します。

- 終了: タスクを完了するまでの時間を指定します。

3 [オプション] タブで、スケジュールのプロパティは、上述の”ホストを無効化”タスクと同じ方法で指定します。さらに、次のオプションを指定します。

- [ドレインモードを有効化] および [指定した時間の後にサーバーを強制的に再起動]。これら 2 つのオプションは組み合わせて使用できます。ドレインモードを選択した場合、次のように動作します。タスクが発生すると、ホストへの新しい接続は拒否されますが、アクティブな接続は引き続き実行されます。すべてのアクティブなユーザーセッションが終了したとき、または指定した時間の後にサーバーを強制的に再起動の時間に到達したときのどちらか早い時点で、サーバーが再起動されます。アクティブユーザーの作業が失われることのないよう、ユーザーに対する作業を保存してログオフすることを促すメッセージを作成します。
- 現在非アクティブのホストにスケジュールを適用する: このオプションは、[ドレインモードを有効化] オプションが選択されている場合に有効になります。このオプションを選択すると、活動していないホストも再起動されます。

4 [OK] をクリックしてスケジュールを保存します。

起動のスケジュールを構成するには、以下の操作を実行します。

1 [タスク] > [追加] > [ホストを起動] または [ホストプールを起動] をクリックします。

2 [一般] タブで、スケジュールのプロパティは、”ホストを無効化”タスクと同じ方法で指定します。唯一の違いは、ホストプールの [タイプ] ドロップダウンリストで、追加するホストプールの種類を選択できることです。

3 [トリガー] タブで、スケジュールのプロパティは、上述の”ホストを無効化”タスクと同じ方法で指定します。

4 [オプション] タブで、次のオプションを指定します。

- メンバーの割合: このオプションを選択して、各プールで起動する必要のあるホストの割合が指定します。
- 開始するメンバーの数を指定: このオプションを選択して、各プールで起動する必要のあるホストの数を指定します。

スケジューラーの使用方法の詳細については、「RD セッションホスト」の「スケジューラーの使用」(p. 154) を参照してください。同トピックでは、RD セッションホストでスケジューラーを使用する方法を説明していますが、機能は同じです。

シャットダウンのスケジュールを構成するには、以下の操作を実行します。

1 [タスク] > [追加] > [ホストをシャットダウン] または [ホストプールをシャットダウン] をクリックします。

2 [一般] タブで、スケジュールのプロパティは、”ホストを無効化”タスクと同じ方法で指定します。

3 [トリガー] タブで、スケジュールのプロパティは、上述の”ホストを無効化”タスクと同じ方法で指定します。

4 [オプション] タブで、スケジュールのプロパティは、上述の”ホストを再起動”タスクと同じ方法で指定します。

再作成のスケジュールを構成するには、以下の操作を実行します。

[タスク] > [追加] > [テンプレートからホストを再作成]、または [テンプレートからホストプールを再作成] をクリックします。

1 [一般] タブで、スケジュールのプロパティは、”ホストを無効化”タスクと同じ方法で指定します。

2 [トリガー] タブで、スケジュールのプロパティは、上述の”ホストを無効化”タスクと同じ方法で指定します。

3 スケジュールのプロパティは、[オプション] タブで、上述の”ホストを再起動”タスクと同じ方法で指定します（以下のオプションは除く）。

- 強制的にホストを再作成するまでの時間（ホストの場合）および強制的にホストプールを再作成するまでの時間（ホストプールの場合）：これらのオプションは、 [ドレインモードを有効化] オプションと連携して動作します（上記を参照）。 タスクがトリガーされると、サーバーへの新しい接続は拒否されますが、アクティブなセッションは引き続き実行され、再接続されます。すべてのアクティブなユーザーセッションが終了したとき、またはこれらのオプションで指定した時間に到達したときのどちらか早い時点で、サーバーが再作成されます。アクティブユーザーの作業が失われることのないよう、ユーザーに対する作業を保存してログオフすることを促すメッセージを作成します。

サイトのデフォルト値（Azure Virtual Desktop）

RAS Console で Azure Virtual Desktop コンポーネントとオブジェクトを設定すると、プロパティの一部がサイトのデフォルト値から継承されます。ダイアログまたはタブページに [デフォルト設定を継承] オプションが表示されている場合は、設定をサイトのデフォルト値から継承するか、または特定のオブジェクトにカスタム値を指定できることを意味します。

Azure Virtual Desktop のサイトのデフォルト値を表示および構成するには、[ファーム] > [サイト] に移動し、[タスクメニュー] をクリックして、次のいずれかを選択します。

- AVD マルチセッションホスト: Azure Virtual Desktop の「マルチセッションホストのためのサイトのデフォルト値」（p. 273）を構成するためのダイアログが開きます。
- AVD シングルセッションホスト: Azure Virtual Desktop の「シングルセッションホストのためのサイトのデフォルト値」（p. 269）を構成するためのダイアログが開きます。

各ダイアログの説明は以下の通りです。

シングルセッションホストのためのサイトのデフォルト値

ホストプールの設定

以下の設定を構成します。

- アクティブなセッションを中断するまでの時間: ユーザーが公開済みアプリケーションを閉じた後、各セッションがバックグラウンドで接続状態を保持する時間を指定します。このオプションを使用して、サーバーへの不必要な再接続を回避します。
- 切断済みセッションをログオフするまでの時間: この設定では、“切断” とマークされた後、セッションのログオフにかかる時間を管理できます。
- セッション準備状態のタイムアウト: セッションを確立するのに必要な最大時間を指定します。指定したタイムアウト時間内にセッションの準備ができない場合、ユーザーにはエラーメッセージが表示され、再度ログインを試みる必要があります。
- URL/メールのリダイレクトを許可: ユーザーがリモートアプリケーションで URL または HTML Mailto リンクを開くと、リンクはクライアントコンピューターにリダイレクトされ、リモートホストのアプリケーションではなく、ローカルのデフォルトアプリケーション（ウェブブラウザーまたはメールクライアント）で開かれます。このオプションではリダイレク

トを有効化または無効化できます。[構成] ボタンをクリックして、以下のオプションから選択します。

a 有効化（登録済みアプリケーションを置換） - このオプションでは、リンクのリダイレクトの代替メソッドを使用します。これにより、リモートサーバー側でデフォルトの Web ブラウザーとメールクライアントを”ダミー”アプリと置換します。これを行うことで、リンクを開く操作を中断し、クライアントコンピューターにリダイレクトできます。

b Windows シェル URL 名前空間オブジェクトのサポート - シェル URL 名前空間オブジェクトをサポートするということは、Parallels RAS がシェル名前空間 API を使用する公開済みアプリケーションでの操作を中断して、リンクを開くことができるということを意味します。これは多くのアプリケーションでの標準的な動作です。シェル URL 名前領域オブジェクトのサポートを無効する機能は、Parallels RAS の旧バージョンとの互換性のために備えられています。

- ドラッグ & ドロップを有効化: ドラッグ & ドロップ機能が Parallels Client 内でどのように機能するかを設定できます。[構成] をクリックして、[無効]（ドラッグ & ドロップ機能なし）、[サーバーからクライアントのみ]（ローカルアプリケーションへのドラッグ & ドロップのみ）、[クライアントからサーバーのみ]（リモートアプリケーションへのドラッグ & ドロップのみ）、[双方向]（双方向のドラッグ & ドロップ）から選択できます。

  注: この文書の作成時点では、ドラッグ・ドロップ機能が利用できるのは Parallels Client for Windows および Parallels Client for Mac のみです。

- 2XRemoteExec がクライアントにコマンドを送信することを許可: サーバーで実行されているプロセスにより、クライアント側でのアプリケーションの展開をクライアントに指示することを許可するには、このオプションをオンにします。

- RDP Shortpath を管理: RDP Shortpath を構成します。RDP Shortpath により、リモートデスクトップクライアントとセッションホスト間で UDP ベースの直接接続を確立します。直接接続することで、Azure Virtual Desktop ゲートウェイへの依存度を低下させることができます。これにより、接続の信頼性が向上し、各ユーザーセッションで利用可能な帯域幅が増加します。RDP 接続と RAS 接続に適用されます。この設定を有効にするには、セッションホストの再起動が必要です。

  RDP Shortpath は 2 種類の方法で使用できます。

  - マネージドネットワーク: 仮想プライベートネットワーク（VPN）などのプライベート接続を使用する場合、クライアントとセッションホストとの間で直接接続が確立されます。ネットワークセキュリティの境界を越えて RDP Shortpath のリッスン先へのアクセスを許可するには、Azure ネットワークセキュリティグループを構成して UDP 受信ポー

ト 3390 を許可する必要があります。VPN または ExpressRoute を使用するか、各セッションホストでパブリック IP アドレスを利用する必要があります。

- パブリックネットワーク: パブリック接続を使用する場合、クライアントとセッションホストとの間で直接接続が確立されます。RDP Shortpath のリッスン先へのアクセス許可には、送信ポートが使用されるため、受信ポートは必要ありません。

パブリックネットワークおよびマネージドネットワーク向けの RDP Shortpath のいずれも有効な場合、優先検出アルゴリズムが動作し、当該のセッションで最初に確立された接続が使用されます。マネージドネットワーク向けに RDP Shortpath を設定した場合は、ほとんどのシナリオで RDP Shortpath が優先されます。これは、パブリックネットワーク用の RDP Shortpath のセッションの構築に時間を要するためです。

[構成] ボタンをクリックして、RDP Shortpath を有効にして構成します。

- RDP Shortpath を使用: RDP Shortpath を有効にします。
- デフォルトで狭いポート範囲を使用する: リモートデスクトップクライアントがセッションホストに接続するために使用できるポートの範囲を制限します。デフォルトの範囲は 49152～65535 です。これは、パブリックネットワークの RDP Shortpath にのみ適用されます。

- アプリケーションの監視を有効にする: サーバーでのアプリケーションの監視を有効または無効にします。アプリケーションのモニタリングを無効にすると、RAS Connection Broker に情報を転送しているときに、サーバーでの CPU 使用率とネットワークの使用率を減らすための WMI モニタリングが停止します。このオプションが有効な場合、収集された情報が対応する RAS レポートに表示されます。このオプションが無効な場合、このサーバーからの情報はレポートに記載されません。
- ファイル転送コマンドを許可（Web および Chrome クライアント）: リモートセッションでのファイル転送を有効化します。ファイル転送を有効にするには、このオプションを選択し、[構成] ボタンをクリックします。詳細については、「リモートファイル転送を構成する」（p. 538）を参照してください。
- ドライブリダイレクトのキャッシュを有効化: リダイレクトされたドライブ上でのファイルの参照とナビゲーションをより高速にすることで、ユーザーエクスペリエンスを向上させます。詳細については、「ドライブリダイレクトのキャッシュの説明」（p. 152）を参照してください。
- RemoteApp を使用（ある場合）: このオプションを有効にすると、シェル関連の問題でアプリが正しく表示されない場合に、リモートアプリを使用できます。この機能は、Windows 用 Parallels Client でのみサポートされています。

ユーザープロファイル

[ユーザープロファイル] タブでは、ユーザープロファイルの機能を構成できます。[RAS で管理しない]（ユーザープロファイルは管理されません）または [FSlogix] から選択できます。Microsoft FSLogix プロファイルコンテナーを使用すると、パーシスタントでない環境でユーザーコンテキストを維持し、サインイン時間を最小限に抑え、互換性の問題を排除するネイティブプロファイルのユーザーエクスペリエンスを提供できるように構成されています。詳細な手順については、「ユーザープロファイル」（p. 138）を参照してください。

アプリケーションパッケージ

[アプリケーションパッケージ] タブでは、サイト内のシングルセッションホストで MSIX アプリケーションパッケージを追加/削除したり、その他の管理を実行したりできます。詳細な説明については、「MSIX アプリケーションパッケージの使用」（p. 576）内のサブセクション、「サイトのデフォルト値にパッケージを追加する」を参照してください。

最適化

[最適化] タブでは、Parallels RAS 環境で最高のパフォーマンスが得られるよう、セッションホストを最適化するための設定を指定できます。無効化、削除、または最適化の対象となる Windows コンポーネントやサービス、またその他のオプションを選択して、仮想アプリおよびデスクトップの配信の効率性と合理性を向上させ、改善することができます。詳細な手順については、「最適化」（p. 146）を参照してください。

RDP プリンター

[RDP プリンター] タブでは、リダイレクトされたプリンターの名前変更フォーマットを構成できます。 フォーマットは、サーバーのどのバージョンと言語を使用しているかによって異なる場合があります。

[RDP プリンター名のフォーマット] ドロップダウンリストから以下のいずれかのオプションを選択し、構成したサーバーに固有の RDP プリンター名のフォーマットを設定します。

- プリンター名（コンピューター名から）内のセッション番号
- セッション番号（コンピューター名から）プリンター名
- プリント名（リダイレクトセッション番号）

[プリンター名にセッション番号を入れない] を選択すると、プリンター名からセッション番号が削除され、セッション番号は表示されなくなります。

マルチセッションホストのためのサイトのデフォルト値

ホストプールの設定

以下の設定を構成します。

- アクティブなセッションを中断するまでの時間: ユーザーが公開済みアプリケーションを閉じた後、各セッションがバックグラウンドで接続状態を保持する時間を指定します。このオプションを使用して、サーバーへの不必要な再接続を回避します。
- 切断済みセッションをログオフするまでの時間: この設定では、“切断” とマークされた後、セッションのログオフにかかる時間を管理できます。
- セッション準備状態のタイムアウト: セッションを確立するのに必要な最大時間を指定します。指定したタイムアウト時間内にセッションの準備ができない場合、ユーザーにはエラーメッセージが表示され、再度ログインを試みる必要があります。
- URL/メールのリダイレクトを許可: ユーザーがリモートアプリケーションで URL または HTML Mailto リンクを開くと、リンクはクライアントコンピューターにリダイレクトされ、リモートホストのアプリケーションではなく、ローカルのデフォルトアプリケーション（ウェブブラウザーまたはメールクライアント）で開かれます。このオプションではリダイレクトを有効化または無効化できます。[構成] ボタンをクリックして、以下のオプションから選択します。

  a 有効化（登録済みアプリケーションを置換） - このオプションでは、リンクのリダイレクトの代替メソッドを使用します。これにより、リモートサーバー側でデフォルトの Web ブラウザーとメールクライアントを”ダミー”アプリと置換します。これを行うことで、リンクを開く操作を中断し、クライアントコンピューターにリダイレクトできます。

  b Windows シェル URL 名前空間オブジェクトのサポート - シェル URL 名前空間オブジェクトをサポートするということは、Parallels RAS がシェル名前空間 API を使用する公開済みアプリケーションでの操作を中断して、リンクを開くことができるということを意味します。これは多くのアプリケーションでの標準的な動作です。シェル URL 名前領域オブジェクトのサポートを無効する機能は、Parallels RAS の旧バージョンとの互換性のために備えられています。

- ドラッグ & ドロップを有効化: ドラッグ & ドロップ機能が Parallels Client 内でどのように機能するかを設定できます。[構成] をクリックして、[無効]（ドラッグ & ドロップ機能なし）、[サーバーからクライアントのみ]（ローカルアプリケーションへのドラッグ & ドロップのみ）、[クライアントからサーバーのみ]（リモートアプリケーションへのドラッグ & ドロップのみ）、[双方向]（双方向のドラッグ & ドロップ）から選択できます。

  注: この文書の作成時点では、ドラッグ・ドロップ機能が利用できるのは Parallels Client for Windows および Parallels Client for Mac のみです。

- 2XRemoteExec がクライアントにコマンドを送信することを許可: サーバーで実行されているプロセスにより、クライアント側でのアプリケーションの展開をクライアントに指示することを許可するには、このオプションをオンにします。
- RDP Shortpath を管理: RDP Shortpath を構成します。RDP Shortpath により、リモートデスクトップクライアントとセッションホスト間で UDP ベースの直接接続を確立します。直接接続することで、Azure Virtual Desktop ゲートウェイへの依存度を低下させることができます。これにより、接続の信頼性が向上し、各ユーザーセッションで利用可能な帯域幅が増加します。RDP 接続と RAS 接続に適用されます。この設定を有効にするには、セッションホストの再起動が必要です。ネットワークセキュリティの境界を越えて RDP Shortpath のリッスン先へのアクセスを許可するには、Azure ネットワークセキュリティグループを構成して UDP 受信ポート 3390 を許可する必要があります。VPN または ExpressRoute を使用するか、各セッションホストでパブリック IP アドレスを利用する必要があります。

  [構成] ボタンをクリックして、RDP Shortpath を有効にして構成します。

  - RDP Shortpath を使用: RDP Shortpath を有効にします。
  - デフォルトで狭いポート範囲を使用する: リモートデスクトップクライアントがセッションホストに接続するために使用できるポートの範囲を制限します。デフォルトの範囲は 49152～65535 です。
- アプリケーションの監視を有効にする: サーバーでのアプリケーションの監視を有効または無効にします。アプリケーションのモニタリングを無効にすると、RAS Connection Broker に情報を転送しているときに、サーバーでの CPU 使用率とネットワークの使用率を減らすための WMI モニタリングが停止します。このオプションが有効な場合、収集された情報が対応する RAS レポートに表示されます。このオプションが無効な場合、このサーバーからの情報はレポートに記載されません。
- ファイル転送コマンドを許可（Web および Chrome クライアント）: リモートセッションでのファイル転送を有効化します。ファイル転送を有効にするには、このオプションを選択し、[構成] ボタンをクリックします。詳細については、「リモートファイル転送を構成する」（p. 538）を参照してください。

- ドライブリダイレクトのキャッシュを有効化: リダイレクトされたドライブ上でのファイルの参照とナビゲーションをより高速にすることで、ユーザーエクスペリエンスを向上させます。詳細については、「ドライブリダイレクトのキャッシュの説明」(p. 152)を参照してください。
- RemoteApp を使用(ある場合): このオプションを有効にすると、シェル関連の問題でアプリが正しく表示されない場合に、リモートアプリを使用できます。この機能は、Windows 用 Parallels Client でのみサポートされています。

ユーザープロファイル

[ユーザープロファイル] タブでは、ユーザープロファイルの機能を構成できます。[RAS で管理しない](ユーザープロファイルは管理されません)または [FSlogix] から選択できます。Microsoft FSLogix プロファイルコンテナーを使用すると、パーシスタントでない環境でユーザーコンテキストを維持し、サインイン時間を最小限に抑え、互換性の問題を排除するネイティブプロファイルのユーザーエクスペリエンスを提供できるように構成されています。詳細な手順については、「ユーザープロファイル」(p. 138)を参照してください。

アプリケーションパッケージ

[アプリケーションパッケージ] タブでは、サイト内のマルチセッションホストで MSIX アプリケーションパッケージを追加/削除したり、その他の管理を実行したりできます。詳細な説明については、「MSIX アプリケーションパッケージの使用」(p. 576)内のサブセクション、「サイトのデフォルト値にパッケージを追加する」を参照してください。

最適化

[最適化] タブでは、Parallels RAS 環境で最高のパフォーマンスが得られるよう、セッションホストを最適化するための設定を指定できます。無効化、削除、または最適化の対象となる Windows コンポーネントやサービス、またその他のオプションを選択して、仮想アプリおよびデスクトップの配信の効率性と合理性を向上させ、改善することができます。詳細な手順については、「最適化」(p. 146)を参照してください。

RDP プリンター

[RDP プリンター] タブでは、リダイレクトされたプリンターの名前変更フォーマットを構成できます。 フォーマットは、サーバーのどのバージョンと言語を使用しているかによって異なる場合があります。

[RDP プリンター名のフォーマット] ドロップダウンリストから以下のいずれかのオプションを選択し、構成したサーバーに固有の RDP プリンター名のフォーマットを設定します。

- プリンター名（コンピューター名から）内のセッション番号
- セッション番号（コンピューター名から）プリンター名
- プリント名（リダイレクトセッション番号）

[プリンター名にセッション番号を入れない] を選択すると、プリンター名からセッション番号が削除され、セッション番号は表示されなくなります。

Parallels Client と Azure Virtual Desktop の併用

Parallels RAS に Azure Virtual Desktop をデプロイしてリソースを公開すると、Parallels Client を使用して公開したアプリケーションやデスクトップにアクセスすることができます。このトピックでは、Parallels Client の要件と、公開されたリソースへのアクセスについて詳細を説明します。

要件

Azure Virtual Desktop のアプリやデスクトップを開くための Parallels Client の要件は、以下の通りです。

- Parallels Client for Windows:
  - Parallels Client for Windows バージョン 18 以降 (ベーシックバージョンまたはフルバージョン）。
  - サポートされている Windows のバージョンは次の通りです。Windows 10 および Windows 11 の場合: Windows Server オペレーティングシステムはサポートされていないことに注意してください。
  - 必要な Windows Update は次の通りです。Windows での汎用の C ランタイムの更新プログラム（KB2999226）。Microsoft Windows 10 には、デフォルトで組み込まれています。
  - Microsoft .NET Framework 4.6.0 以降が必要です。Microsoft Windows 10 には .NET Framework 4 が組み込まれており、デフォルトで有効になっています。

- Microsoft Windows デスクトップクライアント（リモートデスクトップ（MSRDC）クライアントとも呼ばれる）がインストールされている必要があります。同クライアントは、Parallels Client から Azure Virtual Desktop リソースを起動すると自動的にダウンロードされ、インストールされます（サポートされている Windows クライアントデバイスにインストールされていない場合）。次のリンクを使用してクライアントをダウンロードすることもできます: https://go.microsoft.com/fwlink/?linkid=2068602。

  注: [標準] クライアント機能セットオプション（p. 247）を選択し、Windows 10/Windows 11 Enterprise Virtual Desktop をデスクトップ OS として使用して、Parallels Client を実行している場合（ネスト化）、管理者は次の記事で Microsoft が明示しているように、デバイスごとのインストールを使用して Windows Desktop クライアントをプリインストールしておく必要があります: https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/clients/windowsdesktop-admin。

- Microsoft Teams サポート: Parallels RAS 19 では、Windows 10 または 11 マルチセッション、Windows 10 または 11 Enterprise を実行している Azure Virtual Desktop ホストから Parallels Client for Windows に音声とビデオをリダイレクトすることが可能になりました。Azure Virtual Desktop ホストに Microsoft Teams をインストールする方法については、https://docs.microsoft.com/en-us/azure/virtual-desktop/teams-on-avd を参照してください。

  注: 高度なクライアント機能セットを使用する公開済みアプリケーションとして Microsoft Teams にアクセスする場合、ビデオフィードは利用できません。

  注: このガイドの執筆時点では、他のプラットフォーム固有の Parallels Client を使用して Azure Virtual Desktop リソースを起動する機能は現在のところ利用できません。ただし、特定の OS では Parallels Web Client から実行できます（下記参照）。

- Parallels Web Client:
  - ユーザーのマシンにインストールされている Windows、Mac、Linux オペレーティングシステム。
  - 「Parallels Web Client とユーザーポータル」（p. 454）に記載されているシステム要件が必要です。

Parallels Client for Windows で Azure Virtual Desktop リソースにアクセスする

Parallels Client for Windows から Parallels RAS に接続すると、Azure Virtual Desktop リソースを含むすべての公開リソースのリストが表示され、ユーザーがアクセスできるようになります。Azure Virtual Desktop リソースは、サポートされているバージョンの Windows で実行されている Parallels Client にのみ表示されることに注意してください（上記参照）。

[クライアント機能セット] オプションが [アドバンスト] または [フォールバック機能付きアドバンスト] に設定されている場合、公開リソースを実行しているときに、RAS ユニバーサルプリントおよびスキャン、セッション事前起動、ファイルリダイレクトの高速化、ドラッグ & ドロップなどの Parallels RAS の高度な機能を使用することができます。このオプションが [標準] に設定されている場合、これらの機能は使用できません。この設定を表示および変更するには、[ファーム] > [サイト] > [設定] に移動し、[機能] タブを選択し、[クライアント機能セット] ドロップダウンリストで必要な設定を選択します。

展開の確認

Azure Virtual Desktop のデプロイを確認するには、次の操作を実行します。

1. [ファーム] > [サイト] > [設定] に移動し、[機能] タブを選択します。[Azure Virtual Desktop 管理の有効化] オプションが選択され、[ステータス] セクションにバージョン番号と共に「利用可能」 と表示されていることを確認します。
2. [ファーム] > [サイト] > [Azure Virtual Desktop] に移動します。次のタブを選択し、対応するコンポーネントが正しく構成され、機能していることを確認します。
   - プロバイダー
   - ワークスペース
   - ホストプール
   - テンプレート（テンプレートを作成した場合は、このタブに表示されます）
   - ホスト（1 つ以上のセッションホストをリストアップする必要があります）

次のステップ

詳細は、「プロバイダーの管理」、「ワークスペースの管理」、「ホストプールの管理」、「テンプレートの管理」（p. 253）を参照してください。

第 11 章

リモート PC

この章の内容

概要

RD セッションホスト、仮想デスクトップ、また Azure Virtual Desktop だけでなく、サポートされているバージョンの Windows（p. 30）を実行しているスタンドアロンのリモート PC からも、リソースを公開できます。リモート PC として、物理マシンや、物理 PC として扱われる仮想マシンを使用できますが、通常は物理コンピューターを使用します。ネットワークに仮想マシンがある場合は、仮想マシンを VDI インフラストラクチャの一部として使用することをお勧めします。「VDI とバーチャルデスクトップ」の章（p. 164）を参照してください。ただし、ゲスト VM のクローン作成機能を必要としない場合や、エンドユーザーが Windows PC 上でカスタマイズのための完全な管理者権限を必要としている場合などは、仮想マシンをリモート PC として使用できます。

注: リモート PC をプールに組み込んでプールのメンバーとして管理することも可能です。リモート PC プールでは RAS VDI インフラストラクチャを使用します。この章で取り上げる単体のリモート PC とは動作が異なります。詳細については、「リモート PC プール」（p. 233）を参照してください。

この章では、リモート PC をファームに追加する方法と、そのリモート PC からリモートアプリケーションおよびデスクトップを公開する方法について説明します。

ファームへのリモート PC の追加

以下のいずれかの方法で、RAS ファームにリモート PC を追加できます。

- 管理者による登録（p. 280）RAS Console から、PC の IP アドレスと MAC アドレスを指定して、RAS Remote PC Agent を PC にインストール（リモートまたは直接）して登録します。
- ユーザー側から、セルフサービスのリモート PC 登録（p. 282）を利用できるようにします。

それぞれの方法については、次のセクションで説明します。

管理者によるリモート PC 登録

要件

RAS ファームにリモート PC を追加するには、RAS Remote PC Agent がインストールされている必要があります。RAS Remote PC Agent を PC にプッシュインストールするための要件は以下の通りです。

- サーバーにファイヤーウォールを構成してプッシュインストールを許可する必要があります。標準の SMB ポート（139 および 445）が開いている必要があります。Parallels RAS が使用するポート一覧については、「ポート参照」を参照してください。
- SMB アクセス。管理共有（\\server\c$）にアクセスできる必要があります。シンプルファイル共有が有効になっている必要があります。
- Parallels RAS 管理者アカウントには PC でリモートインストールを実行する権限が必要です。権限がない場合、権限があるアカウントの資格情報を入力するよう求められます。
- PC は AD ドメインへの参加が必要です。参加しない場合、プッシュインストールは機能しないかもしれず、その場合、Agent を手動でインストールする必要があります。「手動による Remote PC Agent のインストール」を参照してください。

ファームへのリモート PC の追加

次の手順に従って、リモート PC をファームに追加します。

1. RAS Console で、[ファーム] カテゴリーを選択して、ナビゲーションツリーの [リモート PC] ノードをクリックします。
2. [タスク] ドロップダウンリストで [追加] をクリックして、セットアップウィザードを起動します。
3. リモート PC の IP アドレスまたは FQDN を指定します。[MAC アドレス取得] ボタンをクリックして、PC の MAC アドレスを取得します。IP アドレスを自動的に FQDN に解決するには、[名前解決] グローバルオプションを有効にします。詳細については、「ホスト名の解決」（p.568）を参照してください。
4. [次へ] をクリックします。
5. この手順で、Parallels RAS は指定された PC に Remote PC Agent がインストールされているかどうかを確認します。インストールされていない場合は、[インストール] をクリックして、PC に Agent をプッシュインストールします。Remote PC Agent のプッシュインストールが何らかの理由で失敗した場合、手動でインストールすることができます。以下の「手動による Remote PC Agent のインストール」を参照してください。
6. [追加] をクリックして、リモート PC を Parallels RAS ファームに追加します。

手動による Remote PC Agent のインストール

自動のプッシュインストールを何らかの理由で実行できない場合は、Remote PC Agent の手動インストールが必要になる場合があります。このためには、次の操作を実行します。

1. 管理者アカウントを使用して、Remote PC Agent のインストール先の PC にログインし、他のすべてのアプリケーションを閉じます。
2. Parallels RAS のインストールファイル（`RASInstaller.msi`）を PC にコピーし、そのファイルをダブルクリックして、インストールを開始します。
3. 画面の指示に従って、インストールタイプのページに進みます。[カスタム] を選択し、[次へ] をクリックします。
4. [Remote PC Agent] をクリックし、ドロップダウンリストから [このコンピューターのローカルディスクにすべての機能をインストールします] を選択します。
5. 他のすべてのコンポーネントが選択解除されていることを確認し、[次へ] をクリックします。
6. [インストール] をクリックしてインストールを開始します。インストールが終了したら、[完了] をクリックします。

Remote PC Agent は構成を必要としません。Agent をインストールしたら、Parallels RAS Console でリモート PC 名を選択し、[トラブルシューティング] > [Agent をチェック] をクリックします。Agent が適切にインストールされている場合、ステータスは“Agent をインストールしました”に変わります。

Remote PC Agent のアンインストール

Remote PC Agent をサーバーからアンインストールするには、次の手順を実行します。

1. スタートボタン > [コントロールパネル] > [プログラム] > [プログラムのアンインストール] に移動します。
2. インストールされているプログラムのリストから、[Parallels Remote Application Server] を見つけます。
3. サーバー上に保持する必要がある他の Parallels RAS コンポーネントがない場合、[Parallels Remote Application Server] を右クリックして [アンインストール] をクリックします。手順に従って、プログラムをアンインストールします。この指示の残りの部分は省略できます。
4. サーバー上に保持する必要がある他の RAS コンポーネントがある場合、[Parallels Remote Application Server] を右クリックして [変更] をクリックします。
5. [ようこそ] ページで、[次へ] をクリックします。
6. [変更、修復、または削除] ページで [変更] を選択します。
7. 次のページで [カスタム] を選択します。
8. [Remote PC Agent] を選択し、その前にあるドロップダウンリストをクリックして、[すべての機能が利用できなくなります] をクリックします。
9. [次へ] をクリックして、ウィザードを完了します。

セルフサービスのリモート PC 登録

前述した、管理者がリモート PC を登録する方法の代わりに、エンドユーザー側のセルフサービスで、任意の PC を RAS ファームに追加できます。このようにして登録されたコンピューターは、自動的にリモート PC として RAS ファームに追加されます。その後、対応する公開済みデスクトップが作成され、セルフサービスで登録を行ったユーザーのアクセスが許可されます（自動フィルタリング経由）。これによりユーザーは、場所を問わず任意のデバイスからリモート PC にアクセスできるようになります。

注: この機能は、スタンドアロンのリモート PC に適用されます。VDI テクノロジーで構成されたリモート PC には対応していません。

要件

- PC を登録するユーザーは、Parallels RAS Remote PC Agent をインストールするために、Windows のローカル管理者権限を取得している必要があります。
- エンドユーザーに招待メールを送信するには、RAS ファームでメールボックスを構成する必要があります。

セルフサービスの登録を構成

セルフサービスのリモート PC 登録を構成するには:

1. RAS Console で、[ファーム] > [サイト] > [リモート PC] に移動します。
2. 右側のペインで [タスク] メニューをクリックし、[セルフサービスの登録] を選択します。ダイアログが開いたら、以下のオプションを指定します。
3. セルフサービスの登録を有効にするには、[許可] または [次の日時まで許可] を選択します。後者の場合は、日時を指定します。機能を無効にする（一時的になど）場合は、[許可しない] を選択します。
4. [設定] セクションでは、PC が公開済みリソースとして表示される公開フォルダーを指定します。すでに存在するフォルダーを選択するか、新規フォルダーを作成できます。[...] ボタンをクリックし、フォルダーを選択または作成します。
5. [リモート PC 招待ハッシュ] フィールドには、PC を登録する際に指定しなければならないハッシュが含まれています。ハッシュはここからコピーして、スクリプト用として個別に使用することもできます。IT 管理者は、このハッシュを `msiexec` コマンドと一緒に使用することで、ユーザーに代わってリモート PC のインストールと設定をサイレントで実行できます。詳細については、以下の「PC の登録」を参照してください。
6. PC の登録方法を記載した招待メールをユーザーに送信するには、[メールで送信] ボタンをクリックします。
7. 開いたダイアログで、メールアドレスを入力（または貼り付け）して受信者を指定します。[..] ボタンをクリックして、受信者を選択することもできます。
8. [招待メールを確認する] テキストボックスで、メールを確認または（必要に応じて）修正します。メールで使用される変数は内部で設定されており、実際のメールではその値に置き換

えられます。最終的なメールのテキストをプレビューするには、[タスク] > [プレビュー] をクリックします。

9 [送信] をクリックしてメールを送信します。この時点でメールを送信しない場合は、[キャンセル] をクリックして前のダイアログに戻り、[OK] をクリックして変更内容を保存します。

PC の登録

招待メールを受け取ったユーザーは、メールに記載されている指示に従って PC の登録を行います。インストールは以下の手順で行います。

リモート PC にログインします。RASInstaller.msi ファイル（Parallels RAS インストーラー）をダウンロードまたはコピーして、管理者権限で以下のコマンドを実行します（招待メールには、ハッシュ値を含むこのコマンドが記載されています）：

```
msiexec /qb /i <RAS installer> ADDLOCAL=F_PCAgent ADDFWRULES=1 SELFENROLL=<hash key> [OVERRIDEUSER=user@domain] [OVERRIDEPAIP=ip of PA] [OVERRIDEHOST=published name]
```

以下の引数を使うことで、登録内容をカスタマイズできます。リモート PC が Active Directory ドメインに参加していない場合、このような引数が必要になります。

- OVERRIDEPAIP: ファームサイト内に存在するいずれかの Connection Broker の IP アドレスです。システムが検出した IP アドレスを使用して標準インストールの接続が失敗した場合に、これを使用します。
- OVERRIDEUSER: マシンにログインしているユーザーに対してリモート PC を登録したくない場合は、この引数を使用します。
- OVERRIDEHOST: 公開されたアイテム名をリモート PC のホスト名から変更する場合は、この引数を使用します。

インストールが完了したら、Parallels Client を起動して、ローカルマシンの認証情報または OVERRIDEUSER 引数で指定した認証情報によりログインします。公開済みリソースの一覧から、IP アドレス、または OVERRIDEHOST 引数で指定した名前でリモート PC を特定し、デスクトップを起動します。

リモート PC の構成

リモート PC のプロパティを表示するには、ナビゲーションツリーでコンピューターを選択して、[タスク] > [プロパティ] をクリックします。[リモート PC のプロパティ] ダイアログが開きます。

プロパティ

デフォルトでは、PC はファーム内で有効になっています。PC を無効にすると、公開済みのアプリケーションとバーチャルデスクトップをサーバーから提供できなくなります。ファーム内で PC を有効または無効にするには、[リモート PC 有効化] オプションをオンまたはオフします。

リモート PC の IP アドレスまたは MAC アドレスが変更された場合は、[リモート PC] 入力フィールドおよび [MAC アドレス] 入力フィールドを使用して、IP アドレスまたは MAC アドレスを変更します。

[ダイレクトアドレス変更] オプションでは、Parallels Client が PC に直接接続するために使用できる IP アドレスを指定できます。このアドレスはダイレクト接続モードでのみ使用されます。このアドレスには、内部 IP アドレスまたは外部 IP アドレスを使用できます。

注: マシンの自動オンを可能にするには、BIOS の Wake on LAN オプションを有効にする必要があります。仮想マシンを使用している場合、オプションは通常、ハイパーバイザーによってネイティブにサポートされるか、サードパーティのソフトウェア経由でサポートされます。Wake On Lan オプションがオンになっているかどうかをテストするには、[リモート PC のプロパティ] ダイアログを閉じて、[リモート PC] リストの下にある [WOL テスト] ボタンをクリックします。

Agent 設定

ファーム内の各リモート PC には RAS Remote PC Agent がインストールされています。これにより、Parallels RAS と PC 間の通信を実行します。 この Agent は、[Agent 設定] タブページで構成できます。

- アクティブなセッションをログオフするまでの時間: ユーザーが公開済みアプリケーションを閉じた後、セッションがログイン状態を保持する時間。デフォルトのタイムアウトは 25 秒です。これは、アプリケーションでのみ機能し、公開済みのデスクトップでは機能しません（ユーザーがデスクトップを閉じるときに、セッションはログオフされます）。このタイ

ムアウトは、ユーザーがあるアプリケーションを閉じてから別のアプリケーションを開く場合に、不要なログインを回避するために使用されます。

- セッション準備状態のタイムアウト: セッションを確立するのに必要な最大時間を指定します。指定したタイムアウト時間内にセッションの準備ができない場合、ユーザーにはエラーメッセージが表示され、再度ログインを試みる必要があります。
- ポート: 必要に応じて、別のリモートデスクトップ接続のポート番号を指定します。
- 任意の Connection Broker: Remote PC Agent が通信する Connection Broker を選択します。WAN 経由で通信している複数の物理的な場所にサイトコンポーネントをインストールしている場合、この設定が役立ちます。より適切な Connection Broker を指定することによりネットワークトラフィックを減らすことができます。
- URL/メールのリダイレクトを許可: ユーザーがリモートアプリケーションで URL または HTML Mailto リンクを開くと、リンクはクライアントコンピューターにリダイレクトされ、リモートホストのアプリケーションではなく、ローカルのデフォルトアプリケーション（ウェブブラウザーまたはメールクライアント）で開かれます。このオプションではリダイレクトを有効化または無効化できます。[構成] ボタンをクリックして、以下のオプションから選択します。

  a 有効化（登録済みアプリケーションを置換） - このオプションでは、リンクのリダイレクトの代替メソッドを使用します。これにより、リモートサーバー側でデフォルトの Web ブラウザーとメールクライアントを”ダミー”アプリと置換します。これを行うことで、リンクを開く操作を中断し、クライアントコンピューターにリダイレクトできます。

  b Windows シェル URL 名前空間オブジェクトのサポート - シェル URL 名前空間オブジェクトをサポートするということは、Parallels RAS がシェル名前空間 API を使用する公開済みアプリケーションでの操作を中断して、リンクを開くことができるということを意味します。これは多くのアプリケーションでの標準的な動作です。シェル URL 名前領域オブジェクトのサポートを無効する機能は、Parallels RAS の旧バージョンとの互換性のために備えられています。

- ドラッグ & ドロップを有効化: ドラッグ & ドロップ機能が Parallels Client 内でどのように機能するかを設定できます。[構成] をクリックして、[無効]（ドラッグ & ドロップ機能なし）、[サーバーからクライアントのみ]（ローカルアプリケーションへのドラッグ & ドロップのみ）、[クライアントからサーバーのみ]（リモートアプリケーションへのドラッグ & ドロップのみ）、[双方向]（双方向のドラッグ & ドロップ）から選択できます。

  注: この文書の作成時点では、ドラッグ・ドロップ機能が利用できるのは Parallels Client for Windows および Parallels Client for Mac のみです。

- RDP 転送プロトコルの管理: Parallels Client とサーバー間の接続に使用されるトランスポートプロトコルを選択します。これを実行するには、このオプションを選択し、[構成] ボタンをクリックします。
- ファイル転送コマンドを許可（Web および Chrome クライアント）: リモートセッションでのファイル転送を有効化します。ファイル転送を有効にするには、このオプションを選択し、[構成] ボタンをクリックします。詳細については、「リモートファイル転送を構成する」（p. 538）を参照してください。
- ドライブリダイレクトのキャッシュを有効化: リダイレクトされたドライブ上でのファイルの参照とナビゲーションをより高速にすることで、ユーザーエクスペリエンスを向上させます。詳細については、「ドライブリダイレクトのキャッシュ」（p. 152）を参照してください。

RDP プリンター

[RDP プリンター] タブでは、リダイレクトされたプリンターの名前変更フォーマットを構成できます。　フォーマットは、サーバーのどのバージョンと言語を使用しているかによって異なる場合があります。

[RDP プリンター名のフォーマット] ドロップダウンリストから以下のいずれかのオプションを選択し、構成したサーバーに固有の RDP プリンター名のフォーマットを設定します。

- プリンター名（コンピューター名から）内のセッション番号
- セッション番号（コンピューター名から）プリンター名
- プリント名（リダイレクトセッション番号）

[RDP プリンター] タブで指定できるその他の RDP 印刷オプションは次の通りです。

- プリンター名にセッション数を入れない
- プリンター名にクライアント名を入れない

ログの構成

リモート PC はモニターされており、関連情報のログが作成されます。ログを構成して、既存のログファイルを取得したりクリアしたりするには、リモート PC を右クリックし、コンテキストメニューで [トラブルシューティング] > [ロギング] を選択し、[構成]、[取得]、[クリア] のいずれかをクリックします。これらのタスクの実行方法については、「ログ」（p. 608）セクションを参照してください。

リモート PC のサマリの表示

この章で説明するリモート PC のエディターに加えて、利用可能なリモート PC に関するサマリも確認できます。このためには、次の操作を実行します。

1 RAS Console で、[ファーム] カテゴリーを選択して、中央のペインで [サイト] ノードを選択します。

2 右ペインの [リモート PC] グループに利用できるサーバーが表示されます。

3 リモート PC のエディターに移動するには、サーバーを右クリックして、[エディターに表示] を選択します。

詳細については、「RAS Console でのサイトの表示」（p. 63）を参照してください。

コンピューター管理ツールの使用

RAS Console から、サーバーで標準的なコンピューター管理タスクを直接実行できます。このタスクには、リモートデスクトップ接続、PowerShell、コンピューター管理、サービス管理、イベントビューアー、IPconfig、再起動などが含まれます。[ツール] メニューにアクセスするには、サーバーを選択して [タスク] をクリックし、[ツール] をクリックして目的のツールを選択します。要件と使用方法については、「コンピューター管理ツール」（p. 569）を参照してください。

第　12　章

公開

この章の内容

概要

Parallels RAS で公開できるリソースは、以下の通りです。

- 導入されたアプリケーション
- コンテナー化済みアプリケーション
- パッケージアプリケーション
- デスクトップ

- ドキュメント
- ウェブアプリケーション
- ネットワークフォルダー

この章では、Parallels RAS で管理されるサーバーにホストされているリソースを公開する方法と、すでに公開されているリソースに対して実行できる管理タスクについて説明します。ここで説明される公開機能は、RAS Console の [公開] カテゴリーから利用できます。

デスクトップの公開

リモートデスクトップを公開するには、次の操作を実行します。

1 RAS Console で、[公開] カテゴリーを選択し、[公開済みのリソース] ツリーの下にある [追加] アイコンをクリックします。公開ウィザードが開きます。

> **注:** ウィザードのオプションがすべて無効にされている場合、公開元として構成可能なファームにリソース（サーバー）が存在しないことを意味します。

2 ウィザードの最初のステップで、[デスクトップ] を選択し、[次へ] をクリックします。

3 デスクトップタイプの手順で、公開元のサーバーの種類を選択し、[次へ] をクリックします。

> **注:** プールベースのリモート PC から公開する場合は、[仮想ゲスト] オプションを選択します。[リモート PC] オプションは、スタンドアロンのリモート PC 用です。

4 デスクトップを公開する 1 つまたは複数のサーバーを選択します。すべての利用できるホスト、ホストプール、または個々のホストを選択できます。利用可能なサーバーが 1 つのみの場合、このページは表示されません。

5 [次へ] をクリックします。

6 デスクトップの名前と説明（オプション）を入力し、必要に応じてアイコンを変更します。

7 （RD セッションホストのみ）以下の設定を行います。

- ユーザーを管理セッションに接続するには、[管理セッションに接続] オプションを選択します。
- 必要に応じて [セッションの事前起動から除外] を選択します。詳細については、「セッション事前起動の理解」（p. 321）を参照してください。

- ユーザーがログオンしたらすぐにデスクトップを開く場合は、[ユーザーがログオンすると自動的に起動] オプションを選択します。

8 （VDI のみ）[ゲスト VM に対する静的割り当てを有効化] オプションを選択して、ユーザーが最初に接続したときにゲスト VM がパーシスタントとしてマークされるようにします。

9 （リモート PC のみ）[リモート PC の設定] セクションの [...] ボタンをクリックして、アプリケーションの公開元のリモート PC をリストから選択します。開いたボックスで、PC をダブルクリックして選択します。

10 [デスクトップサイズ] ドロップダウンリストを使用して、画面解像度を指定します。カスタムの画面幅および高さを設定するには、[サイズ] ドロップダウンリストで [カスタム] を選択し、提供されたフィールドに値を指定します。

11 [マルチモニター] ドロップダウンリストで、マルチモニターサポートを有効にするか、無効にするか、またはクライアント設定を使用するかを選択します。

12 次のページでは、リソースの初期状態を指定します。[有効]（エンドユーザーがリソースを起動できる）、[無効]（リソースが Parallels Client に表示されない）、[メンテナンス中]（リソースが Parallels Client に表示されるが、ユーザーからは起動できない）から選択します。リソースがメンテナンス中の場合、ユーザーがそのリソースを起動しようとするとメッセージが表示されます。メッセージをカスタマイズするには、[構成] ボタンをクリックします。詳細については、「サイトのデフォルト値（公開）」（p. 314）を参照してください。

13 以上の操作を実行して [完了] をクリックすると、デスクトップが公開されます。

アプリケーションの公開

アプリケーションを公開するには、次の手順を実行します。

1 RAS Console で [公開] カテゴリーを選択し、[公開済みのリソース] ツリーの下にある [追加] アイコンをクリックします（または [公開済みのリソース] ボックス内を右クリックし、コンテキストメニューで [追加] をクリックします）。公開ウィザードが開きます。

> **注:** ウィザードのオプションがすべて無効にされている場合、公開元として構成可能なファームにリソース（サーバー）が存在しないことを意味します。

2 [アイテムタイプの選択] ウィザードページで [アプリケーション] を選択し、[次へ] をクリックします。

3 [サーバータイプを選択] のページで、公開元のサーバーの種類を選択し、[次へ] をクリックします。

> **注:** プールベースのリモート PC から公開する場合は、[仮想ゲスト] オプションを選択します。[リモート PC] オプションは、スタンドアロンのリモート PC 用です。

4 [アプリケーションタイプの選択] ページで、利用可能な以下のいずれかのオプションを選択します。

- 1 つのアプリケーション: 実行ファイルのパスなど、アプリケーション設定をユーザー自身ですべて構成するには、このオプションを選択します。
- 導入されたアプリケーション: サーバーにすでにインストールされているアプリケーションを公開するには、このオプションを選択します。つまり、すべてのアプリケーション設定が自動的に構成されます。
- 既存のアプリケーション: Windows エクスプローラーなど、日常的に使用する Windows アプリケーションを公開するには、このオプションを選択します。
- アプリケーションパッケージ: MSIX アプリケーションパッケージからアプリケーションを公開する場合は、このオプションを選択します。MSIX アプリケーションパッケージからアプリケーションを公開するプロセスについては、「MSIX app attach によるアプリケーションの公開」（p. 295）を参照してください。

5 [次へ] をクリックします。

6 [公開元の選択] ページで、どのホストからアプリケーションを公開するかを指定します。以下のオプションがあります。

- （RDSH の場合）サイト内の全ホスト: 選択すると、サイトで利用可能なすべてのサーバーからアプリケーションが公開されます。
- （RDSH の場合）RD セッションホストのホストプール.このオプションを選択した後、アプリケーションの公開元である個々のホストプールを選択します。
- （RDSH の場合） 各ホスト: このオプションを選択し、アプリケーションの公開元である個々のサーバーを選択します。
- （VDI の場合）ホストプール: アプリケーションの公開元となるホストプールを選択します。
- （AVD の場合）ホストプール: アプリケーションの公開元となるホストプールを選択します。

インストールしているアプリケーションタイプが [既存のアプリケーション] の場合、このページはスキップされます。

7 [次へ] をクリックします。

8 [アプリケーションタイプの選択] ページで選択したアプリケーションタイプに応じて、次に表示されるウィザードページは以下のいずれかになります。

- [1 つのアプリケーション] を選択した場合、[アプリケーション] ページが開きます。このページで、アプリケーションの設定を手動で指定する必要があります（このオプションの詳細については、このセクションの後で説明します）。
- [導入されたアプリケーション] を選択した場合、[導入されたアプリケーション] ページが開きます。このページには、利用可能なアプリケーションのリストが表示されます（アプリケーションは機能別にグループ化されています）。インストールするアプリケーションを選択し、[次へ] をクリックします。指示に従ってウィザードを完了します。
- [既存のアプリケーション] を選択した場合、[既存のアプリケーションの選択] ページが開きます。このページには、利用可能なアプリケーションのリストが表示されます。公開するアプリケーションを選択し、[完了] をクリックします。

9 [アプリケーションタイプの選択] ウィザードページで [1 つのアプリケーション] を選択した場合、[アプリケーション] ページが開きます。アプリケーションの設定を次のように指定します。

最初に「参照」ボタン（[...]）を使用して [ターゲット] フィールドを入力した場合、アプリケーションの [名前]、[説明]、およびアイコンが自動的に選択されます。必要に応じて、これらのオプションを変更できます。

- 名前: 選択して、アプリケーションの名前を入力します。
- 説明: 説明を入力します（オプション）。
- 実行: アプリケーションウィンドウの状態（通常のウィンドウ、最小化、最大化）を選択します。
- セッションの事前起動から除外: 詳細については、「セッション事前起動の理解」（p. 321）を参照してください。
- ユーザーがログオンすると自動的に起動: ユーザーがログオンしたらすぐにアプリケーションを起動する場合はこのオプションを選択します。このオプションは、デスクトップバージョンの Parallels Client でのみ機能します。
- アイコン変更: アプリケーションのアイコンを変更します（オプション）。
- サーバー: アプリケーションの公開元のサーバーごとに、残りのサーバーパラメーターを個々に指定できます。ドロップダウンリストボックスからサーバーを選択し、パラメーターを指定します。リスト内の他のサーバーに対してこれを繰り返します。

- ターゲット: アプリケーションの実行ファイルのパスとファイル名を指定します。
- スタート: [ターゲット] フィールドが有効な場合、このフィールドには値が自動的に入力されます。必要に応じて、独自のパスを指定できます。
- パラメーター: アプリケーションが起動パラメーターを受け付ける場合、パラメーターをこのフィールドで指定できます。

10 （VDI のみ）[ゲスト VM に対する静的割り当てを有効化] オプションを選択して、ユーザーが最初に接続したときにゲスト VM がパーシスタントとしてマークされるようにします。

11 （リモート PC のみ）[リモート PC の設定] セクションの [...] ボタンをクリックして、アプリケーションの公開元のリモート PC をリストから選択します。開いたボックスで、PC をダブルクリックして選択します。

12 次のページでは、リソースの初期状態を指定します。[有効]（エンドユーザーがリソースを起動できる）、[無効]（リソースが Parallels Client に表示されない）、[メンテナンス中]（リソースが Parallels Client に表示されるが、ユーザーからは起動できない）から選択します。リソースがメンテナンス中の場合、ユーザーがそのリソースを起動しようとするとメッセージが表示されます。メッセージをカスタマイズするには、[構成] ボタンをクリックします。詳細については、「サイトのデフォルト値（公開）」（p. 314）を参照してください。

13 以上の操作を実行して [完了] をクリックすると、アプリケーションが公開されます。

App-V アプリケーションの公開

Microsoft Application Virtualization（または App-V）は、Microsoft のアプリケーションストリーミングソリューションです。Parallels RAS v16.5 から、App-V アプリケーション公開のサポートが Parallels RAS Console で利用できます。

この文書の作成時点では、App-V サポートには、App-V コンポーネントによりアプリケーションのプロビジョニングが実行されるシナリオが実装されています。

- アプリケーションは、Microsoft のガイドラインに従って、管理者により配列されます。
- アプリケーションは、管理者が作成するネットワーク共有（SMB、HTTPs）に保存されます。
- App-V 管理および公開サーバーは、特定の AD グループのアプリケーションを公開するために使用されます。この AD グループは、管理者により手動で、App-V アプリケーションの公開に使用される RAS Publishing グループと同期する必要があります。
- App-V クライアントは、管理者により手動でインストールおよび構成されます。

App-V アプリケーションの展開と公開のプロセスは、次のようになります。

1 App-V シーケンサーを使用して、アプリケーションをパッケージします。

2 App-V 管理コンソール、Microsoft SCCM、などを使用して、RD セッションホストにアプリケーションを展開します。

3 アプリケーションをプロビジョニングします。

4 ユーザーが RD セッションホストからアプリケーションを起動できることを確認します。

5 RAS Console からアプリケーションを公開します（手順については、以下を参照してください）。

6 Parallels Client からアプリケーションを起動します。

App-V アプリケーションを公開するには、次の操作を実行します。

1 Parallels RAS Console で [公開] カテゴリーを選択します。

2 右ペインの下部にある [+] 追加アイコンをクリックします。公開ウィザードが開きます。

3 [アイテムタイプの選択] ページで、[App-V アプリケーション] オプションを選択します。

4 [次へ] をクリックします。

5 アプリケーションの公開元にするサーバータイプを選択し、[次へ] をクリックします。

6 公開元のサーバーまたはグループを選択し、[次へ] をクリックします。

7 [インストールされたアプリケーション] ページで、1 つまたは複数の App-V アプリケーションを選択し、[次へ] をクリックします。

8 概要情報を確認して、ウィザードを完了します。

App-V アプリケーションが公開されると、Parallels Client から起動できます。

注: 起動の問題を回避するには、AutoLoad=2 を使用します。詳細は、https://blogs.technet.microsoft.com/technetsto_sup/2013/11/12/autoload-setting-in-app-v-5-0/ を参照してください。

MSIX app attach によるアプリケーションの公開

MSIX アプリケーションパッケージからアプリケーションを公開するには:

1 「MSIX アプリケーションパッケージの使用」（p. 576）に従い、セッションホストにアプリケーションパッケージを追加します。

2 「アプリケーションの公開」（p. 291）に従い、手順 1～2 を実行します。

3 [サーバータイプの選択] ページで [RD セッションホスト] または [仮想ゲスト] または [Azure Virtual Desktop] を選択し、[次へ] をクリックします。

4 [アプリケーションタイプの選択] ページで、[アプリケーションパッケージ] を選択します。

5 「アプリケーションの公開」（p. 291）に従い、手順 5～7 を実行します。

6 [インストール済みのアプリケーション] ページが開きます。このページには、利用可能なアプリケーションのリストが表示されます。公開するアプリケーションを選択し、[次へ] をクリックします。

7 「アプリケーションの公開」（p. 291）に従い、手順 10～11 を実行します。

8 [サマリ] ページが開きます。このページには、公開用に選択したアプリケーションの情報が含まれています。[次へ] をクリックします。

9 [完了] をクリックします。

ウェブアプリケーションの公開

ウェブアプリケーションは、他のアプリケーションと同様、標準のアプリケーション公開機能を使用して公開できます。ただし、ウェブアプリケーションに対する URL リンクをそのまま公開する方法を簡素化するために、別の公開アイテムタイプを利用できます。これにより、最小限の手順数で公開タスクを実行できます。

ウェブアプリケーションを公開するには、次の操作を実行します。

1 RAS Console で [公開] カテゴリーを選択し、[公開済みのリソース] ツリーの下にある [追加] アイコンをクリックします（または [公開済みのリソース] ボックス内を右クリックし、コンテキストメニューで [追加] をクリックします）。公開ウィザードが開きます。

> **注:** ウィザードのオプションがすべて無効にされている場合、公開元として構成可能なファームにリソース（サーバー）が存在しないことを意味します。

2 [アイテムタイプの選択] ウィザードページで、[ウェブアプリケーション] を選択し、[次へ] をクリックします。

3 [サーバータイプを選択] ページで、公開元のサーバーの種類を選択し、[次へ] をクリックします。

> **注:** プールベースのリモート PC から公開する場合は、[仮想ゲスト] オプションを選択します。[リモート PC] オプションは、スタンドアロンのリモート PC 用です。

4 [公開元の選択] ページで、公開元のサーバーを選択します。サーバーが 1 台しかない場合は、[公開元の選択] ページは表示されません。

5 [ウェブアプリケーション] ウィザードページが開いたら、ウェブアプリケーションの名前、説明、ウィンドウ状態、URL を指定します。必要に応じて、[Internet Explorer の使用を強制] オプションを選択します。特定のアプリケーションアイコンを参照するには、[アイコン変更] をクリックします。

6 （VDI の場合のみ）必要に応じて、[パーシスタント] オプションを選択して、ゲスト VM をパーシスタントにします。詳細については、「パーシスタントゲスト VM」を参照してください。

7 （リモート PC のみ）[リモート PC の設定] セクションの [...] ボタンをクリックして、アプリケーションの公開元のリモート PC をリストから選択します。開いたボックスで、PC をダブルクリックして選択します。

8 次のページでは、リソースの初期状態を指定します。[有効]（エンドユーザーがリソースを起動できる）、[無効]（リソースが Parallels Client に表示されない）、[メンテナンス中]（リソースが Parallels Client に表示されるが、ユーザーからは起動できない）から選択します。リソースがメンテナンス中の場合、ユーザーがそのリソースを起動しようとするとメッセージが表示されます。メッセージをカスタマイズするには、[構成] ボタンをクリックします。詳細については、「サイトのデフォルト値（公開）」（p. 314）を参照してください。

9 以上の操作を実行して [完了] をクリックすると、アプリケーションが公開されます。

公開されたウェブアプリケーションは、他のアプリケーションと同様、[公開] > [公開済みのリソース] リストに表示されます。

ネットワークフォルダーの公開

UNC パスを使用してファイルシステムフォルダーを公開し、そのフォルダーを Windows エクスプローラーで開くことができます。構成の手順数を最小限にするため、RD セッションホストからネットワークフォルダーを公開できる特殊な公開アイテムを利用できます。

ネットワークフォルダーを公開するには、次の操作を実行します。

1 RAS Console で [公開] カテゴリーを選択し、[公開済みのリソース] ツリーの下にある [追加] アイコンをクリックします（または [公開済みのリソース] ボックス内を右クリックし、コンテキストメニューで [追加] をクリックします）。公開ウィザードが開きます。

> **注:** ウィザードのオプションがすべて無効にされている場合、公開元として構成可能なファームにリソース（サーバー）が存在しないことを意味します。

2 [アイテムタイプの選択] ウィザードページで、[ファイルシステム上のフォルダー] を選択し、[次へ] をクリックします。

3 [サーバータイプを選択] ページで、公開元のサーバーの種類を選択し、[次へ] をクリックします。

> **注:** プールベースのリモート PC から公開する場合は、[仮想ゲスト] オプションを選択します。[リモート PC] オプションは、スタンドアロンのリモート PC 用です。

4 [公開元の選択] ページで、公開元のサーバーを選択します。サーバーが 1 台しかない場合は、[公開元の選択] ページは表示されません。

5 [UNC フォルダー] ウィザードページで、通常のアプリケーションプロパティを指定します。

6 [UNC パス] フィールドに、公開するフォルダーの UNC パスを入力します。[...] ボタンをクリックしてフォルダーを参照します（[フォルダーの参照] ダイアログが開くまでに時間がかかることがあります）。

7 （VDI の場合のみ）必要に応じて、[パーシスタント] オプションを選択して、ゲスト VM をパーシスタントにします。詳細については、「パーシスタントゲスト VM」を参照してください。

8 （リモート PC のみ）[リモート PC の設定] セクションの [...] ボタンをクリックして、アプリケーションの公開元のリモート PC をリストから選択します。開いたボックスで、PC をダブルクリックして選択します。

9 次のページでは、リソースの初期状態を指定します。[有効]（エンドユーザーがリソースを起動できる）、[無効]（リソースが Parallels Client に表示されない）、[メンテナンス中]（リソースが Parallels Client に表示されるが、ユーザーからは起動できない）から選択します。リソースがメンテナンス中の場合、ユーザーがそのリソースを起動しようとするとメッセージが表示されます。メッセージをカスタマイズするには、[構成] ボタンをクリックします。詳細については、「サイトのデフォルト値（公開）」（p. 314）を参照してください。

10 [完了] をクリックすると、フォルダーが公開され、ウィザードが閉じます。

公開されたネットワークフォルダーは、他のアプリケーションと同様、[公開] > [公開済みのリソース] リストに表示されます。公開されたネットワークフォルダーを選択してから、[アプリケーション] タブをクリックすると、次のアプリケーション設定が表示されます。

- [ターゲット] プロパティは常に `PublishedExplorer.exe` に設定されます。このバイナリは（Agent プッシュによって）自動的に作成されるもので、標準の `explorer.exe` 実行ファイルの単純なコピーです。
- [パラメーター] プロパティには、公開するネットワークフォルダーが指定されます。フォルダーパスは、`explorer.exe` で処理できる任意の形式で指定できます。

この公開アイテムでは、標準のアプリケーションプロパティタブがすべて有効になっていますが、少なくとも次の項目は全く無関係であるため無視してください。

- 公開元
- ファイル拡張子

ドキュメントの公開

ドキュメントを公開するには、次の手順を実行します。

1 RAS Console で [公開] カテゴリーを選択し、[公開済みのリソース] ツリーの下にある [追加] アイコンをクリックします（または [公開済みのリソース] ボックス内を右クリックし、コンテキストメニューで [追加] をクリックします）。公開ウィザードが開きます。

> **注:** ウィザードのオプションがすべて無効にされている場合、公開元として構成可能なファームにリソース（サーバー）が存在しないことを意味します。

2 [アイテムタイプの選択] ウィザードページで [ドキュメント] を選択し、[次へ] をクリックします。

3 公開元にするサーバータイプを選択し、[次へ] をクリックします。

> **注:** プールベースのリモート PC から公開する場合は、[仮想ゲスト] オプションを選択します。[リモート PC] オプションは、スタンドアロンのリモート PC 用です。

4 公開するドキュメントのドキュメントタイプを指定します。事前に定義されたリストからドキュメントタイプを選択するか、[ドキュメントタイプ指定] 入力フィールドにカスタムドキュメントタイプを指定できます。

5 準備が完了したら、[次へ] をクリックします。

6 [公開元の選択] ページで、公開元のサーバーを選択します。サーバーが 1 台しかない場合は、[公開元の選択] ページは表示されません。

7 [アプリケーション] ページで、名前、説明（オプション）、ウィンドウの状態を入力し、必要に応じてアイコンを変更します。

8 [ターゲット] 入力フィールドの横にある [...] ボタンを使用して、ドキュメントを参照します。他のすべてのフィールドのデータは自動的に読み込まれます。自動読み込みフィールドのいずれかを編集するには、該当のフィールドを選択し、必要な詳細情報を入力します。

9 （オプション）[パラメーター] 入力フィールドで、アプリケーションの開始時にアプリケーションに渡すパラメーターを指定します。

> **注:** 特定のサーバー上でドキュメントを異なる方法で構成する場合は、[サーバー] ドロップダウンリストを使用して、その特定のサーバー用の異なるドキュメント設定を指定します。設定は、個別に選択したサーバーごとに保存されます。

10 （VDI の場合のみ）必要に応じて、[パーシスタント] オプションを選択して、ゲスト VM をパーシスタントにします。詳細については、「パーシスタントゲスト VM」を参照してください。

11 （リモート PC のみ）[リモート PC の設定] セクションの [...] ボタンをクリックして、アプリケーションの公開元のリモート PC をリストから選択します。開いたボックスで、PC をダブルクリックして選択します。

12 次のページでは、リソースの初期状態を指定します。[有効]（エンドユーザーがリソースを起動できる）、[無効]（リソースが Parallels Client に表示されない）、[メンテナンス中]（リソースが Parallels Client に表示されるが、ユーザーからは起動できない）から選択します。リソースがメンテナンス中の場合、ユーザーがそのリソースを起動しようとするとメッセージが表示されます。メッセージをカスタマイズするには、[構成] ボタンをクリックします。詳細については、「サイトのデフォルト値（公開）」（p. 314）を参照してください。

13 [完了] をクリックしてドキュメントを公開します。

一般管理タスク

公開済みのリソースを表示するには、Parallels RAS Console で [公開] カテゴリーを選択します。中央のペインで、（折りたたまれている場合は）[公開済みのリソース] ノードを展開し、リソースを確認します。

リソースを右クリックしてコンテキストメニューを開きます。メニューには次のオプションがあります。

- 追加: 公開ウィザードを開始します。このウィザードは、リソースを公開するために使用できます。
- 新しいフォルダー: フォルダーを [公開済みのリソース] ツリーに追加できます。フォルダーについては、「フォルダーの管理」セクション（p. 312）で説明されています。
- 検索: リソースのリストを名前で検索できます。
- 複製: 選択されたリソースを複製します。同じ種類の複数のリソースを公開できますが、ニーズに合わせてそれらをさまざまに構成することができます。
- 削除: 公開済みのリソースを Parallels RAS ファームから削除します。ファームから公開済みのリソースアイテムを削除するだけです。実際のアプリケーションは影響を受けません。不慮の削除を防ぐために、確認用のダイアログボックスが表示されます。
- ステータス: [有効]、[無効]、[メンテナンス中] から選択します。リソースが無効またはメンテナンス中の場合、ユーザーはそのリソースを利用できません。無効にしたリソースは、Parallels Client で使用可能なリソースリストには表示されません。メンテナンス中のリソースは表示されますが、グレーアウトされています（ユーザーポータルでは、リソース名にステータスが表示されています）。ユーザーがリソースを開こうとすると、メッセージが表示されます。このメッセージは、「公開済みリソースのサイトのデフォルト値」（p. 314）でカスタマイズできます。

  なお、公開済みフォルダーのステータスを設定すると、そのフォルダーに含まれるすべてのサブフォルダー（存在する場合）とリソースに親フォルダーのステータスが継承されます。
- 権限の委任: [権限の委任] ダイアログを開き、ユーザーを追加して公開する権限を付与できます。
- 設定監査: 公開済みリソースに最近加えられた変更を確認して、元に戻すことができます。元に戻すことができる変更には、作成、削除、アップデートなどがあります。
- ターゲットの確認: 選択されたリソースに対して指定されたターゲットが有効かどうかを確認します。ターゲットを確認するには、リソースを選択して、[アプリケーション] タブをクリックします。
- フィルターを変換して識別子を保護: リソースのフィルタリングが WinNT または LDAP を使用して指定されている場合は、このオプションを使用してリソースを SID（セキュア識別子）に変換することができます。詳細については、「フィルタールールの使用」（p. 317）を参照してください。

- 実行中のインスタンス: [実行中のプロセス] ダイアログが開きます。ダイアログの詳細については、「セッションの管理」 > 「実行中のプロセスを管理」（p. 153）を参照してください。ダイアログが開くと、プロセスリストにフィルターが適用され、選択された公開済みのリソースのプロセスのみが表示されます（リソース ID は値として使用されます）。リストをさらにフィルタリングして、特定のユーザー（[ユーザー名] 列）のプロセスのみを表示することができます。

画面の下部にある処理アイテムで次の処理を実行できます。

- 追加: 前述の [追加] メニュー項目と同じ処理です。
- 新しいフォルダー: 前述の [新しいフォルダー] メニュー項目と同じ処理です。
- 削除: 前述の [削除] メニュー項目と同じです。
- 上に移動: 選択された公開済みのリソースアイテムをリスト内で上へ移動させます。
- 下に移動: 選択された公開済みのリソースアイテムをリスト内で下へ移動させます。
- 無効: 前述の [無効] メニュー項目と同じです。
- ソート: リソースをアルファベット順でソートします。この処理項目を有効にするには、[公開済みのリソース] ノード（最上位のノード）または個別の項目が含まれるフォルダーを選択する必要があります。
- 検索: 前述の [検索] メニュー項目と同じです。
- 実行中のインスタンス: 前述の [実行中のインスタンス] メニュー項目と同じです。
- 有効なアクセス: 特定のユーザーが利用できる公開済みのリソースを表示できます。詳細については、「有効なアクセスの確認」（p. 322）を参照してください。

公開済みのリソースに変更を加えた後は、必ず [適用] ボタンをクリックして、変更内容を Parallels RAS ファームで確定してください。

公開済みアプリケーションの管理

公開済みアプリケーションの構成

ウィザードを使用してアプリケーションを公開する場合、名前、実行ファイルのパスなど、いくつかのアプリケーションパラメーターを指定します。これらのオプションは、アプリケーションの公開後に変更できます。

公開済みアプリケーションの設定を変更するには:

1 RAS Console で、[公開] カテゴリーを選択し、[公開済みのリソース] ツリーで任意のアプリケーションを選択します。

2 右ペインの各タブを使用して、アプリケーション設定を変更します（詳細は以下のサブセクションを参照）。

[公開元の選択] - アプリケーション公開元のサーバーの構成

[公開元の選択] タブで、アプリケーションの公開元の RD セッションホストのホストプールを指定できます。

[アプリケーション] - アプリケーションとホストサーバー設定の構成

[アプリケーション] タブには、アプリケーションとサーバーの固有の設定が表示されます。

基本的なアプリケーション設定（名前、説明、ウィンドウモード）は必要に応じて変更できます。次のような他の設定があります:

- ステータス: [有効]、[無効]、[メンテナンス中] から選択します。リソースが無効またはメンテナンス中の場合、ユーザーはそのリソースを利用できません。無効にしたリソースは、Parallels Client で使用可能なリソースリストには表示されません。メンテナンス中のリソースは表示されますが、グレーアウトされています（ユーザーポータルでは、リソース名にステータスが表示されています）。ユーザーがリソースを開こうとすると、メッセージが表示されます。このメッセージは、「公開済みリソースのサイトのデフォルト値」（p. 314）でカスタマイズできます。

  なお、公開済みフォルダーのステータスを設定すると、そのフォルダーに含まれるすべてのサブフォルダー（存在する場合）とリソースに親フォルダーのステータスが継承されます。

- ユーザーがログオンすると自動的に起動: このオプションを選択すると、ユーザーがログインすると同時にアプリケーションが起動します。このオプションは、デスクトップバージョンの Parallels Client でのみ機能します。

- セッションの事前起動から除外: このオプションの使い方については、「セッション事前起動の理解」（p. 321）を参照してください。

[サーバー設定] セクションには、構成可能なサーバー固有のオプションがあります。複数のサーバーからアプリケーションが公開されている場合、[サーバー] ドロップダウンリストを使用して個々のサーバーを選択し、特定のサーバーの [ターゲット]、[開始]、[パラメーター] の各値を設定できます。これを行うのは、一例として、異なるサーバーで異なるフォルダーにアプリ

ケーションがインストールされているとき、[ターゲット] および [開始] フィールドの値を各サーバーで有効にするためです。

アプリケーションが MSIX パッケージから公開されている場合、[サーバー設定] セクションは [アプリケーション情報] セクションに置き換えられます。ここでのオプションは、公開用に別のアプリケーションを選択できる [アプリケーションを変更] ボタンを除いて同じです。

現在表示されているサーバー設定をデフォルトとして保存するには、[デフォルトとして保存] ボタンをクリックします。保存したデフォルト設定をサーバーに適用するには、[デフォルト設定使用] ボタンをクリックします。これらの 2 つのボタンにより、カスタム設定またはデフォルトを使用する柔軟性が得られます。設定をデフォルトとして設定すると、Parallels RAS がそのサイトにサーバーごとに設定されたアプリケーションがあるかどうかをチェックし、それらのサーバーで新しいデフォルト設定を使用するかどうかを尋ねるメッセージが表示されます。[いいえ] を選択すると、サーバーは固有の設定を維持します。この場合も、デフォルトは保存されます。

指定した [ターゲット] および [開始] の値がすべてのサーバーで正しいことを確認するには、[ターゲットの確認] ボタンをクリックします。[ターゲット認証ツール] ダイアログが開き、サーバーのリストが表示され、[進行] 列に確認ステータスが表示されます。いずれかのサーバーで、異なるパスにアプリケーションがインストールされている場合、[進行] 列にエラーが示されます。この場合、[ターゲット認証ツール] ダイアログを閉じて、[サーバー] ドロップダウンリストでサーバーを選択します。該当のサーバーに固有の新しい値を [ターゲット]、[開始]、[パラメーター]（必要な場合）の各フィールドに入力します。[適用] をクリックして変更内容を保存します。

[ターゲット認証ツール] ダイアログを使用して、公開したすべてのアプリケーションのターゲットを即座に確認することもできます。これを行うには、[公開済みのリソース]（[公開済みのリソース] ツリーのルートノード）を右クリックし、コンテキストメニューで [ターゲットの確認] をクリックします。このとき、[ターゲット認証ツール] ダイアログには、公開したすべてのアプリケーションと、それらの確認ステータスが含まれます。

フィルタリング

「フィルタールールの使用」（p. 317）を参照してください。

ルーティング

「優先ルーティングを構成」（p. 319）を参照してください。

ショートカット - 公開済みアプリケーションのショートカットオプションの構成

[ショートカット] タブをクリックすると、ユーザーのデスクトップ、および [開始] フォルダーや [オートスタート] フォルダーにアプリケーションのショートカットを作成できます。[オートスタート] オプションを選択すると、コンピューターの起動時にアプリケーションが自動的に起動します。サイトのデフォルト設定を使用するには、[デフォルト設定を継承] オプションを選択します。サイトのデフォルト値を表示または変更するには、[サイトのデフォルト値] リンクをクリックします。詳細については、「サイトのデフォルト値（公開）」（p. 314）を参照してください。

注: ショートカットは、すべてのオペレーティングシステムで利用できるとは限りません。

[ファイル拡張子] – ファイル拡張子の関連付けの構成

特定の公開済みのアプリケーションに対するファイル拡張子の関連付けを変更するには、[ファイル拡張子] タブをクリックします。

項目を追加/削除/変更するには、[ファイル拡張子] オプションを選択します。新しい拡張子をリストに追加するには、[タスク] ドロップダウンリストで [追加] をクリック（または [+] アイコンをクリック）して、拡張子を指定します。

既存の関連付けを変更するには、拡張子を選択し、[タスク] ドロップダウンリストで [プロパティ] をクリック（または [パラメーター] 列をダブルクリック）して、パラメーターを入力します。

[ライセンス] - 公開済みアプリケーションのライセンスオプションの構成

[ライセンス] タブをクリックして、

- セッションの共有を無効にする: このオプションを有効にすると、特定の公開済みアプリケーションを 1 つのセッションに分離することができます。同じアプリケーションを複数回起動する場合、そのアプリケーションのインスタンスは同じセッションを共有することになります。一方、別のアプリケーションの場合は、独自のセッションで起動します。
- ユーザーにアプリケーションの 1 インスタンスのみ開始を許可: このオプションを有効にすると、ユーザーは 1 つのアプリケーションインスタンスのみを起動できます。
- 同時使用ライセンス: このオプションを使用して、アプリケーションが実行できる同時インスタンスの最大数を指定します。たとえば、アプリケーションのライセンスによって、実行できるアプリケーションインスタンスの数が 10 個に限られている場合、[同時使用ライセ

ンス] オプションを 10 に設定します。これにより、この制限に達した場合、他のユーザーが他のインスタンスを実行できなくなります。

- 制限を超えた場合: このドロップダウンリストでは、構成された上記のライセンス制限のいずれかを超えた場合に Parallels RAS で実行するアクションを指定できます。

サイトのデフォルト設定を使用するには、[デフォルト設定を継承] オプションを選択します。デフォルト設定を表示または変更するには、[サイトのデフォルト値] リンクをクリックします。詳細については、「サイトのデフォルト値（公開）」（p. 314）を参照してください。

表示 - 公開済みアプリケーションの表示設定の構成

[表示] タブで、以下のオプションを構成できます。

- アプリケーションの表示前にすべての RAS ユニバーサルプリンターがリダイレクトされるまで待機する: アプリケーションのロード前にプリンターがリダイレクトされるまで待機する場合は、このオプションを有効にします。ユニバーサルプリンターのリダイレクトの最大待ち時間（秒単位）も指定できます。プリンターのリダイレクトには時間がかかる場合もあります。プリンターのリダイレクト中は、進捗状況バーがユーザーに表示されるので、混乱を避けられます。
- 色濃度、解像度、幅、高さ: アプリケーションの表示設定を選択してください。
- モバイルクライアントを使用する場合にアプリケーションを最大化して開始する: このオプションは、モバイルデバイスで実行する Parallels Client だけに当てはまります。このオプションを選択すると、モバイルデバイスでアプリケーションが最大表示の状態で起動します。ユーザーがリモートアプリケーションを操作しやすくなります。また、RAS 管理者は、このオプションを使用してアプリケーションを簡単に最大化できます。追加の手順は不要です。
- WYSE ThinOS をフルスクリーンモードで起動: 選択すると、Wyse ThinOS のフルスクリーンモードでアプリケーションが起動します。場合によっては、アプリケーションの下部がタスクバーの背後に隠れてしまい、アプリケーションのウィンドウ全体が見えなくなることがあります。このオプションを使用すると、タスクバーが非表示になり、アプリケーションウィンドウ全体が表示されるようになります。

表示設定でカスタム値を指定するには、[デフォルト設定を継承] チェックボックスをクリアしておく必要があります。そうしないと、サイトのデフォルト設定が使用されます。サイトのデフォルト値を表示または変更するには、[サイトのデフォルト値] リンクをクリックします。詳細については、「サイトのデフォルト値（公開）」（p. 314）を参照してください。

クイックキーパッド

[クイックキーパッド] セクションでは、このアプリケーションに割り当てるクイックキーパッドテンプレートを選択できます。ドロップダウンリストの下にある [クイックキーパッド] リンクから、コンソールの [クイックキーパッド] カテゴリーに移動できます。ここで、キーパッドテンプレートを構成することができます。詳細については、「クイックキーパッド」セクション（p. 326）を参照してください。

公開済みデスクトップの管理

公開デスクトップの構成

ウィザードを使用してデスクトップを公開する場合、表示サイズなど、デスクトップ設定を指定する必要があります。このオプションは、デスクトップの公開後に変更できます。

公開デスクトップを変更するには、[公開] カテゴリーの [公開済みのリソース] ツリーで公開デスクトップを選択します。

[サイト] – 公開済みのデスクトップにアクセスできるサイトの構成

デフォルトでは、利用可能なすべてのサイトから、公開済みのデスクトップにアクセスできます。特定のサイトまたはサイトグループへのアクセスを制限するには、[公開済みのリソース] ツリーでデスクトップを選択し、右ペインで [サイト] タブをクリックします。どのサイトからデスクトップを利用できるようにするかを選択します。

注: [サイト] タブを利用するには、ファーム内に複数のサイトが存在する必要があります。

[公開元の選択] – デスクトップの公開元の RD セッションホストの構成

RD セッションホストデスクトップを構成する場合、どのサーバーから RD セッションホストデスクトップを公開するかを指定できます。これを行うには、[公開元の選択] タブをクリックし、サーバーを選択します。

[デスクトップ] – デスクトップの名前、サイズおよび他のプロパティの構成

デスクトップの種類に応じて、[デスクトップ]、[リモート PC のデスクトップ]、または [バーチャルデスクトップ] タブをクリックし、デスクトップの名前、説明、アイコン、解像度、ステータス、およびその他の設定を構成します。

- ステータス: [有効]、[無効]、[メンテナンス中] から選択します。リソースが無効またはメンテナンス中の場合、ユーザーはそのリソースを利用できません。無効にしたリソースは、Parallels Client で使用可能なリソースリストには表示されません。メンテナンス中のリソースは表示されますが、グレーアウトされています（ユーザーポータルでは、リソース名にステータスが表示されています）。ユーザーがリソースを開こうとすると、メッセージが表示されます。このメッセージは、「公開済みリソースのサイトのデフォルト値」（p. 314）でカスタマイズできます。

  なお、公開済みフォルダーのステータスを設定すると、そのフォルダーに含まれるすべてのサブフォルダー（存在する場合）とリソースに親フォルダーのステータスが継承されます。
- 管理セッションに接続: ユーザーを管理セッションに接続するには、このオプションを選択します。このオプションを有効にした状態でデスクトップに接続しているユーザーには管理者権限が必要であることに注意してください。この権限がない場合は、"アクセスが拒否されました" エラーがユーザーに表示されます。
- ユーザーがログオンすると自動的に起動: ユーザーがログインしたらすぐにデスクトップを開きたい場合は、このオプションを選択します。[セッションの事前起動から除外] オプションについては、「セッション事前起動を理解する」（p. 321）を参照してください。
- デスクトップサイズ: ドロップダウンリストからデスクトップサイズを選択します。
- マルチモニター: マルチモニターを有効にするか、無効にするか、またはクライアントの設定を使用するかを選択します。

フィルタリング

「フィルタールールの使用」（p. 317）を参照してください。

ルーティング

「優先ルーティングを構成」（p. 319）を参照してください。

ショートカット - 公開済みデスクトップのショートカットオプションの構成

[ショートカット] タブをクリックすると、ユーザーのデスクトップ、および [開始] フォルダーや [オートスタート] フォルダーにショートカットを作成できます。[オートスタート] ショートカットを有効にすると、コンピューターの起動時にアプリケーションが自動的に起動します。サイトのデフォルト設定を使用するには、[デフォルト設定を継承] オプションを選択します。詳細については、「サイトのデフォルト値（公開）」（p. 314）を参照してください。

注: このオプションは、すべてのオペレーティングシステムで利用できるとは限りません。

公開済みドキュメントの管理

公開済みドキュメントの構成

ウィザードを使用してドキュメントを公開する場合は、ドキュメント設定を指定する必要があります。これらのオプションは、ドキュメントの公開後にも変更できます。

公開ドキュメントを変更するには、[公開] カテゴリの [公開済みのリソース] ツリーでそのドキュメントを選択してから、右ペインの各タブを使用して、公開ドキュメントの設定を構成します。

[サイト] – 公開済みのドキュメントにアクセスできるサイトの構成

デフォルトでは、利用可能なすべてのサイトから、公開済みのドキュメントにアクセスできます。特定のサイトまたはサイトグループへのアクセスを制限するには、右ペインで [サイト] タブをクリックします。ドキュメントにアクセスできるサイトを選択します。

注: [サイト] タブを使用できるようにするには、ファーム内に複数のサイトが必要です。

[公開元の選択] – ドキュメントの公開元のサーバーの構成

[公開元の選択] タブをクリックし、ドキュメントの公開元のサーバーを選択します。ドキュメントの公開元のサーバーには、そのドキュメントタイプを開くことができるアプリケーションがインストールされている必要があります。

[アプリケーション] – サーバー固有のドキュメント設定の構成

デフォルトで、[ターゲット] (アプリケーションのパス）、[開始]、[パラメーター] の各フィールドに構成した設定は、ドキュメントの公開元のすべてのサーバーに適用されます。あるドキュメントが、1 つ以上のサーバー上で異なるフォルダーに存在する場合は、そのサーバー向けに上記の設定を個別に指定できます。

このためには、次の操作を実行します。

1. [アプリケーション] タブをクリックします。
2. [サーバー] リストでサーバーを選択します。
3. [ターゲット]、[開始]、[パラメーター]（オプション）の各プロパティを指定します。ここで指定した値は、選択されたサーバーにのみ適用されます。必要に応じて、他のサーバーにも上記の手順を繰り返します。
4. [ターゲットの確認] ボタンをクリックして、このアプリケーションの公開元となるすべてのサーバー上にあるドキュメントのパスを確認します。結果が [ターゲット認証ツール] ダイアログに表示されます。このダイアログで、各サーバーのターゲットが正しいかどうかを確認できます。

フィルタリング

「フィルタールールの使用」（p. 317）を参照してください。

ルーティング

「優先ルーティングを構成」（p. 319）を参照してください。

ショートカット - 公開済みドキュメントのショートカットオプションの構成

[ショートカット] タブをクリックすると、ユーザーのデスクトップ、および [開始] フォルダーや [オートスタート] フォルダーでのショートカットの作成を有効にするかどうかを指定できます。[オートスタート] ショートカットを有効にした場合、ユーザーのコンピューターの起動時にアプリケーションが開始されます。

注: このオプションは、すべてのオペレーティングシステムで利用できるとは限りません。

[ファイル拡張子] – ファイル拡張子の関連付けの構成

特定の公開ドキュメントに対するファイル拡張子の関連付けを変更するには、[ファイル拡張子] タブをクリックします。リストに新しい拡張子を追加するには、[タスク] > [追加] をクリックして、拡張子を指定します。拡張子のパラメーターを変更するには、拡張子を選択して、[タスク] > [プロパティ] をクリックします。

[ライセンス] – 公開済みのドキュメントのライセンスオプションの構成

以下のライセンスオプションを構成するには、[ライセンス] タブをクリックします。

[デフォルト設定を継承] オプションを選択すると、デフォルトが使用されます。独自の設定を指定するには、このオプションをオフにして、次の各オプションを設定します。

- [セッションの共有を無効にする] オプションがあります。このオプションを有効にすると、特定の公開済みアプリケーションを 1 つのセッションに分離することができます。同じアプリケーションを複数回起動する場合、そのアプリケーションのインスタンスは同じセッションを共有することになります。一方、別のアプリケーションの場合は、独自のセッションで起動します。
- ユーザーにアプリケーションの 1 インスタンスのみ開始を許可: このオプションを有効にすると、ユーザーは 1 つのアプリケーションインスタンスのみを起動できます。
- 同時使用ライセンス: このオプションを使用して、アプリケーションが実行できる同時インスタンスの最大数を指定します。たとえば、アプリケーションのライセンスによって、実行できるアプリケーションインスタンスの数が 10 個に限られている場合、[同時使用ライセンス] オプションを 10 に設定します。これにより、この制限に達した場合、他のユーザーが他のインスタンスを実行できなくなります。
- 制限を超えた場合: このドロップダウンリストでは、構成された上記のライセンス制限のいずれかを超えた場合に Parallels RAS で実行するアクションを指定できます。

サイトのデフォルト設定を使用するには、[デフォルト設定を継承] オプションを選択します。詳細については、「サイトのデフォルト値（公開）」（p. 314）を参照してください。

表示 - 公開済みドキュメントの表示設定の構成

公開済みのドキュメントの色濃度、解像度、幅、高さを構成するには、[表示] タブをクリックします。これらのオプションをデフォルト値のままにすると、クライアント指定のオプションが引き継がれます。

また、アプリケーションをロードする前にユニバーサルプリンターのリダイレクトを待機するオプションを有効にすることもできます。このオプションを有効にすると、ユニバーサルプリンターのリダイレクトの最大待ち時間（秒単位）も構成できます。サイトのデフォルト設定を使用するには、[デフォルト設定を継承] オプションを選択します。詳細については、「サイトのデフォルト値（公開）」（p. 314）を参照してください。

フォルダーの管理

フォルダーを使用して、公開済みのリソースを整理できます。また、フィルターオプションを利用することもできます。

Parallels RAS Console の [公開済みのリソース] ツリーには、次の 2 つのタイプのフォルダーを作成できます。

- 管理目的のフォルダー: このタイプのフォルダーは、Parallels RAS 管理者（Parallels RAS Console のユーザー）を対象としています。これらは Parallels RAS Console で公開済みのリソースを論理的に整理するために使用されますが、ユーザーデバイス上の Parallels Client Launchpad には表示されません。これらのフォルダーは、管理者が公開済みのリソースをより効率的に管理するのに役立ちます。
- 一般フォルダー: これらのフォルダーは上記の管理目的のフォルダーと似ていますが、ユーザーデバイスの Launchpad に表示されます。通常は、これらのフォルダーを使用して、タイプごとに公開済みのリソースをグループ化します（オフィスアプリケーション、特定のビジネスアプリケーション、ユーティリティなど）。

フォルダーを作成

新しいフォルダーを作成するには、次のいずれかを実行します。

1. RAS Console で [公開] カテゴリーを選択します。
2. [公開済みリソース] ツリーの任意の場所を右クリックし、[新しいフォルダー] を選択します（または、下部の [+] 新しいフォルダーアイコンをクリックします）。
3. [フォルダー] タブページで、[フォルダー名] と [説明]（オプション）を指定します。
4. 管理目的のフォルダーにするには、[管理目的で使用する] オプションを選択します。通常のフォルダーを公開するには、このオプションをオフにします。2 つのフォルダータイプの詳細については、上記の説明を参照してください。

5 通常のフォルダーを作成するときは、[アイコン変更] ボタンをクリックしてアイコンを変更できます。管理フォルダーは、変更できない組み込みのアイコンを使用します。アイコンは、Parallels RAS Console および Parallels Client の Launchpad（一般フォルダーのみ）の [公開] カテゴリーに表示されます。

6 次のページでは、リソース（フォルダー）の初期状態を指定します。次のオプションから選択します。

- 有効: 該当のフォルダーは、エンドユーザーに対して表示され、エンドユーザーはそのフォルダーに含まれる公開済みリソースを起動できます。
- 無効: このフォルダーは Parallels Client では表示されません。
- メンテナンス中: 該当のフォルダーは Parallels Client で表示されますが、ユーザーはそのフォルダーに含まれるリソースを起動できません。フォルダーにサブフォルダーが含まれている場合、それらは親フォルダーのステータスを継承します。つまり、階層内のどのフォルダーに含まれているリソースも、ユーザー側からはアクセスできないことになります。フォルダーがメンテナンス中の場合、ユーザーが該当のフォルダーからリソースを起動しようとするとメッセージが表示されます。メッセージをカスタマイズするには、[構成] ボタンをクリックします。詳細については、「サイトのデフォルト値（公開）」（p. 314）を参照してください。

7 [完了] をクリックしてフォルダーを作成します。

フォルダーの管理

既存のフォルダーを変更するには、次の操作を実行します。

1 [公開済みのリソース] ツリーでフォルダーを選択します。

2 右ペインの[情報] タブに、フォルダー情報（読み取り専用）が表示されます。

3 [フォルダー] タブでは、フォルダーの名前と説明を表示したり変更したりできます。[管理目的で使用する] オプションを選択したり選択解除したりしてフォルダーのタイプを変更することもできます（上記の説明を参照）。フォルダーのアイコンを変更するには、[アイコン変更] ボタンをクリックします。[管理目的で使用する] オプションが選択されている場合、このボタンは無効になります。

4 [フィルター] タブでフィルターオプションを指定します。これらのオプションを設定すると、そのフォルダー内にある他のすべての公開済みのリソースに設定が継承されます。詳細については、「フィルタールールの使用」（p. 317）を参照してください。

5 ルーティングの詳細については、「優先ルーティングを構成」（p. 319）を参照してください

フォルダーへの公開済みリソースの追加

公開済みのリソースをフォルダーに追加するには、まずルートの場所に追加してから対象のフォルダーにドラッグします。

カスタム管理者への権限の委任

ファームにカスタム管理者がいる場合は、フォルダーを管理する権限をカスタム管理者に委任できます。これは、上級管理者がいくつかの権限をカスタム管理者に付与する必要が生じる場合に特に有効です。フォルダーへの権限を付与するには、次の操作を実行します。

1. [公開済みのリソース] ペイン内の任意の場所を右クリックします。
2. コンテキストメニューで、[権限の委任] を選択します。
3. 表示されるダイアログで、フォルダー権限を付与するユーザーを選択します。[権限の委任 - 公開] ダイアログの右下のペインで、対象ユーザーに付与するフォルダー権限（表示、変更、追加、削除）を選択します。カスタム管理者の詳細については、「管理者アカウントの管理」（p. 68）を参照してください。
4. また、「管理者アカウントの権限の構成」（p. 70）で説明しているように、管理カテゴリー経由で、カスタム管理者にフォルダーへの権限を付与することもできます。

サイトのデフォルト値（公開）

[デフォルト設定] ダイアログでは、公開するためのサイトのデフォルト設定を表示したり確認したりすることができます。公開済みリソースは、次の設定グループにおいて、サイトのデフォルト値を継承できます。

- ショートカット
- ライセンス
- ディスプレイ
- メンテナンス

[デフォルト設定] ダイアログを開くには、[ファーム] > [サイト] に移動します。[タスク] メニューをクリックし、[サイトのデフォルト値] > [公開済みリソース] を選択します。このダイアログは、以下で説明するタブから構成されています。

ショートカット

このタブでは、公開済みのリソースのショートカットをユーザーのコンピューター上に作成するかどうか、またショートカットの作成方法について指定します。次のオプションを利用できます。

- デスクトップにショートカットを作成する: このオプションを選択すると、ユーザーのデスクトップにショートカットが作成されます。
- スタートフォルダーにショートカットを作成する: このオプションを選択すると、[スタート] フォルダーにショートカットが追加されます。表示されるフィールドに、追加先のサブフォルダー名とパスを指定することができます。デフォルト値および %Groups% 変数に限っては、公開済みのリソースをホストするホストサーバーに表示されるので、サブフォルダーを追加できます。たとえば、リソースがホストサーバーの”[Myapps] > [ゲーム]”にある場合、同じフォルダー構造がパスにも追加されます。なお、カスタム変数は一切使用できません。
- オートスタートフォルダーにショートカットを作成する: このオプションを選択すると、コンピューターの起動時に、公開済みのリソースが自動的に起動します。

ライセンス

[ライセンス] タブには、

- [セッションの共有を無効にする] オプションがあります。このオプションを有効にすると、特定の公開済みアプリケーションを 1 つのセッションに分離することができます。同じアプリケーションを複数回起動する場合、そのアプリケーションのインスタンスは同じセッションを共有することになります。一方、別のアプリケーションの場合は、独自のセッションで起動します。
- ユーザーにアプリケーションの 1 インスタンスのみ開始を許可: このオプションを有効にすると、ユーザーは公開済みのリソースのインスタンスを 1 つだけ起動できます。
- 同時使用ライセンス: このオプションを使用して、公開済みのリソースが実行できる同時インスタンスの最大数を指定します。たとえば、アプリケーションのライセンスによって、実行できるアプリケーションインスタンスの数が 10 個に限られている場合、[同時使用ライセンス] オプションを 10 に設定します。これにより、この制限に達した場合、他のユーザーが他のインスタンスを実行できなくなります。
- 制限を超えた場合: このオプションでは、構成された上記のライセンス制限のいずれかを超えた場合に Parallels RAS で実行するアクションを指定します。

ディスプレイ

[表示] タブには、次のオプションがあります。

- アプリケーションの表示前にすべての RAS ユニバーサルプリンターがリダイレクトされるまで待機する: アプリケーションのロード前にプリンターがリダイレクトされるまで待機する場合は、このオプションを有効にします。ユニバーサルプリンターのリダイレクトの最大待ち時間（秒単位）も指定できます。プリンターのリダイレクトには時間がかかる場合もあります。プリンターのリダイレクト中は、進捗状況バーがユーザーに表示されるので、混乱を避けられます。
- 色濃度、解像度、幅、高さ: これらのオプションは、アプリケーションの表示設定を指定します。
- モバイルクライアントを使用する場合にアプリケーションを最大化して開始する: このオプションは、モバイルデバイスで実行する Parallels Client だけに当てはまります。このオプションを選択すると、モバイルデバイスでアプリケーションが最大表示の状態で起動します。ユーザーがリモートアプリケーションを操作しやすくなります。また、RAS 管理者は、このオプションを使用してアプリケーションを簡単に最大化できます。追加の手順は不要です。

メンテナンス

[メンテナンス] タブでは、公開済みリソースをメンテナンス中に起動しようとしたときにユーザーに表示されるメッセージを指定できます。リソースがメンテナンス中の場合、リソースは Parallels Client で表示されますが、グレーアウトされています (ユーザーポータルでは、リソース名にステータスが表示されています) 。ユーザーがリソースを開こうとすると、ここで指定したメッセージが表示されます。変更したメッセージをデフォルトに戻したい場合、任意の言語のメッセージを選択し、[タスク] > [デフォルト値にリセット] をクリックします。すべての言語のメッセージをリセットするには、[タスク] > [デフォルト値にリセット] をクリックします。

前述のサイト設定は、Parallels RAS ファームの他のサイトに複製することができます。複製するには、任意のタブで [設定を複製する] オプションを選択してください。タブ内のすべての設定が複製されます。

フィルタールールの使用

フィルタリングルールを使用すると、特定の公開済みのリソースにどのユーザーがアクセスできるかを制御できます。各ルールは、ユーザー接続に対するマッチングに使用される 1 つまたは複数の条件で構成されています。各条件は、マッチング可能な 1 つまたは複数の特定のオブジェクトで構成されています。

次のオブジェクトのマッチングを実行できます。

- ユーザー、ユーザーが所属するグループ、またはユーザーが接続するコンピューター。
- ユーザーが接続する Secure Gateway。
- クライアントデバイスの名前。
- クライアントデバイスのオペレーティングシステム。
- します。
- IP アドレス。
- ハードウェア ID。ハードウェア ID の形式は、クライアントのオペレーティングシステムに依存します。

ルールについて、次のことに注意してください。

- 条件は AND 演算子で連結されます。たとえばあるルールに、特定の IP アドレスに一致という条件とクライアントデバイスのオペレーティングシステムに一致という条件が含まれる場合、ユーザーの接続が IP アドレスの条件とクライアントオペレーティングシステムの条件の両方に一致する場合に、ルールが適用されます。
- オブジェクトは OR 演算子で接続されます。たとえば、クライアントデバイスのオペレーティングシステムに一致するという条件のみを作成した場合、いずれかのオペレーティングシステムがクライアント接続に一致すれば、ルールが適用されます。
- ルールは、上から順にユーザー接続と比較されます。このため、ルールの優先順位は、ルールリスト内の位置によって異なります。Parallels RAS では、ユーザー接続に一致する最初のルールが適用されます。
- いずれのルールにもマッチしない場合には、デフォルトルールが使用されます。デフォルトルールは、他のルールにマッチしない場合に許可または他のルールにマッチしない場合に拒否のいずれかに設定できますが、条件を利用することはできません。

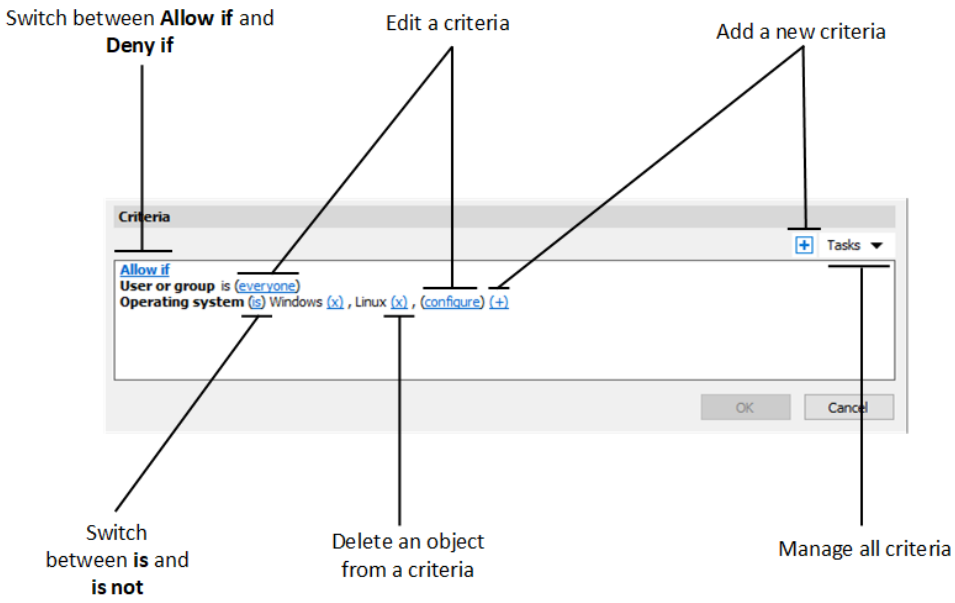
新しいルールを作成するには、次の操作を実行します。

1 RAS Console で、[公開] に移動します。

2 [フィルタリング] タブを選択します。

3 [タスク] ドロップダウンメニューをクリックし、[追加] を選択します（または [+] アイコンをクリックします）。

4 ルールの条件を指定します。以下のコントロールを利用できます。



- Allow if および Deny if: 指定すると、ユーザー接続が条件に一致した場合に、リソースにアクセスできるようになります。これらのオプションは、クリックすると切り替わります。
- （+）：新しい条件を追加します。一致条件として、Secure Gateway、クライアントデバイス名、クライアントデバイスのオペレーティングシステム、テーマ、IP アドレス、ハードウェア ID のいずれかを使用したい場合は、（+）をクリックします。 表示されるコンテキストメニューで、マッチングさせたいオブジェクトの種類を選択し、表示されるダイアログで特定のオブジェクトを追加します。新しい条件が次の行に表示されます。
- （X）：マッチングから特定のオブジェクトを削除します。たとえば、IP アドレス 198.51.100.1 をマッチングから削除したい場合は、その横にある（X）をクリックします。このコントロールは、少なくとも 1 件のオブジェクトが追加されたときに表示されます。条件内のすべてのオブジェクトが削除された場合、その条件は削除されます。

- is および is not: ユーザー接続が条件に一致した場合に、リソースをアクセス可能にするかどうかを指定します。これらのオプションは、クリックすると切り替わります。このコントロールは、少なくとも 1 件のオブジェクトが追加されたときに表示されます。
- configure: マッチさせるオブジェクトのリストを編集します。このリンクをクリックして新しいオブジェクトを追加または削除します。最初の条件（ユーザーまたはグループ）の場合、このリンクは everyone と呼ばれることに注意してください。この条件のオブジェクトを指定すると、構成が変更されます。

優先ルーティングを構成

概要

優先ルーティングは、地理的に異なる展開の Parallels RAS ユーザーが、同じ Parallels RAS ファーム/サイトに接続する場合に便利な機能です。リソースが同じ RAS ファーム/サイト内の別のデータセンターにある場合、共通のアクセスレイヤーの使用（RAS Secure Gateway、HALB、またはサードパーティのロードバランサー）は最適ではありません。この問題を解決するには、特定の公開済みリソースに対して優先的なアクセスレイヤーサーバーを設定します。この場合、ユーザーはデフォルトの Secure Gateway に接続しますが、管理者が設定した近接ルールを使用してリダイレクトされることになります。一般的に、セッションホストに最も近接した Secure Gateway を使用することで、ユーザーエクスペリエンスの向上、内部ネットワークのトラフィックおよび関連コストの削減、リソースの有効活用が可能になります。

注: 優先ルーティングは、Azure Virtual Desktop の公開済みオブジェクトには適用されません。

優先ルーティングは次のように動作します。

1. Parallels Client は、標準的な認証を使用して Secure Gateway との接続を確立します。
2. RAS Connection Broker を通じて、リソースの優先ルート（設定されている場合）が特定されます。
3. Parallels Client は、リソースを起動するための優先パブリックアドレスを受け取ります。
4. Parallels Client はリダイレクトされたアドレスからリソースを起動しようとします。これが失敗すると元のゲートウェイにフォールバックします。

優先ルーティングを構成

公開済みリソースに対して優先ルーティングを構成するには

1 RAS Console で [公開] カテゴリーを選択します。

2 既存の公開済みリソースを選択し、[ルーティング] タブを選択します。

3 [優先ルーティングを有効にする] オプションを選択します。

4 [タスク] > [追加] をクリックします。[優先ルーティングを追加する] ダイアログが開きます。内容をご確認ください。

[優先ルーティングを追加する] ダイアログで、以下の操作を実行します。

1 このルーティングの名前と説明（オプション）を入力します。

2 [タイプ] ドロップダウンリストで、次のいずれかを選択します。

- HALB 仮想サーバー: [タイプ] フィールドの下のリストから、HALB 仮想サーバーを選択します。ここでは HALB サーバーを追加できないため、RAS の HALB 仮想サーバーをリストに表示するには、HALB サーバーでパブリックアドレスを指定する必要があります。
- Secure Gateway: 前述の HALB 仮想サーバーと同様に、ゲートウェイをリストに表示するには、[パブリックアドレス] フィールドに値を指定する必要があります。RAS Secure Gateway を作成または構成する際には、[パブリックアドレス] フィールドを参照してください。
- カスタム: サードパーティのロードバランサーが使用されます。このオプションを選択してから、[タスク] > [追加] をクリックし、フィールドの下のリストでサーバーのプロパティを指定します。プロパティには、名前、説明、パブリックアドレス、ポート、SSL ポートがあります。必要な台数のサーバーを追加し、その中から特定の公開済みリソースに使用するサーバーを選択することができます。

優先ルーティングを設定する際には、以下の点も考慮してください。

- ルーティングに失敗した場合は、発信元アドレスへの自動フォールバックが実行されます。
- RAS Console でルーティングが有効になっているものの未構成の場合、管理者にはエラーメッセージが表示され、構成を実行するか、無効にするように求められます。
- 多くのリソースにルーティングを構成する必要がある場合は、フォルダー（管理目的で構成）を使用することをお勧めします。子オブジェクトでルーティングが有効になっている場合、親フォルダーからルーティングが継承されることはなく、1 つのルーティングセットのみが使用されます。
- RDP トラフィックを同一の RAS サイトにリダイレクトする際には、同じユーザー認証情報が使用されます。ユーザーが認証情報を再入力する必要はありません。

- 既存のセッションが特定の Secure Gateway にトンネリングされており、セッション共有を使用している場合は、構成済みのルーティングにかかわらず、同じセッションのワークフローパスが使用されます（公開済みリソースが同じセッションホストで利用可能な場合）。
- ルーティングは SAML 環境でサポートされています。
- サポートされているクライアントは、Windows、macOS、Linux、Android、iOS、Web です。

ユーザー招待時のパブリックアドレスの指定

[ユーザーの招待] ウィザードでは、対象となるプラットフォームや接続オプションを指定する 2 ページ目で、パブリックアドレスを指定することができます。これにより、特定の地理的ロケーション所在するユーザーのグループに対して、優先ルーティングを設定することができます。詳細については、「ユーザーを招待」（p. 52）を参照してください。

Gateway や HALB の削除と無効化

Gateway や HALB が優先ルーティングとして使用されているときに、管理者がこれを削除しようとすると、そのゲートウェイや HALB を使用しているオブジェクトの情報が画面に表示されます。これにより誤って削除するリスクを回避できます。

セッション事前起動の理解

ユーザーがリモートアプリケーションやデスクトップを開くときには、まずセッションを起動する必要があります。セッションの起動には時間がかかるので、ユーザーはアプリケーションが起動するまで待つことになります。ユーザーエクスペリエンスを改善するため、ユーザーが実際にアプリケーションを開く前に、あらかじめセッションを起動できるようになっています。セッション事前起動はバックグラウンドで実行されるので、ユーザーが画面上でウィンドウやメッセージボックスを見ることはありません。ユーザーがアプリケーションを起動すると、事前に起動されたセッションが使用されるため、非常に早く起動できます。

セッション事前起動の構成方法については、「クライアントポリシー」（p. 511）を参照してください。

セッション事前起動を構成すると、次のオプションが利用できます。

- オフ: セッション事前起動は使用されません。

- 基本: ユーザーがアプリケーションのリストを取得した時点で、セッション事前起動が行われます。数分以内にユーザーがアプリケーションを開くという仮定が、前提になっています。セッションは、10 分間アクティブな状態になります。その時間内にユーザーがアプリケーションを開かないと、クライアントがセッションから切断されます。
- マシンラーニング: ユーザーがアプリケーションのリストを取得すると、その行動に基づいてセッション事前起動が行われます。このオプションを有効にすると、ユーザーが特定の曜日にアプリケーションを起動する行動を Parallels Client が記録して分析します。ユーザーが通常アプリケーションを開く数分前に、セッションを開始します。

セッション事前起動を使用してはならない場合のルールを設定できます。次のオプションを利用できます。

- 事前起動を使用してはならない日付を指定します。
- 公開されているリソースをセッション事前起動の意思決定から除外します。リソースが分析対象から除外される場合、Parallels Client がセッションの事前起動を行うかどうかを判定するときにその対象から除外されます。たとえば、セッション事前起動の対象から除外したいサーバーがある場合、そのサーバーによってホストされているすべての公開済みリソースについて、セッション事前起動の対象から外すためフラグを立てることができます。公開済みリソースをセッション事前起動から除外するには、RAS Console で [公開済みリソース] に移動して、[セッションの事前起動から除外] オプションを選択します。

有効なアクセスの確認

前のセクション（p. 317）で説明したフィルタールールを使用すると、特定の公開済みのリソースにアクセスできるユーザーを設定できます。Parallels RAS ユーザーが Parallels Client で 1 つ以上の公開リソースを参照できない場合、通常は各リソースのフィルター設定をチェックして、特定のユーザー用に公開されていることを確認する必要があります。有効なアクセス機能は、ユーザーが利用できる公開済みのリソースと利用できない公開リソースを 1 か所で表示できるようにすることで、この作業を簡素化します。

[有効なアクセス] ダイアログを開くには、Parallels RAS Console で [公開] カテゴリーを選択し、ウィンドウの下部にあるツールバーの [有効なアクセス] 項目をクリックします（項目が表示されない場合はコンソールウィンドウを最大化します）。また、[公開済みのリソース]ペインのどこかを右クリックし、コンテキストメニューの [有効なアクセス] を選択してダイアログを開くこともできます。

[有効なアクセス] ダイアログでは、ユーザー（およびオプションで追加の条件）を指定し、このユーザーがアクセスできる公開済みのリソースを表示できます。ユーザーを選択するには、次のいずれかを実行します。

- [ユーザー] フィールドにユーザー名を入力するか、その横にある [...] ボタンをクリックし、[ユーザーまたはグループの選択] ダイアログを使用してユーザーを選択します。
- 既知のデバイスのリストからこのユーザーが所有するデバイスを選択します。そのためには、[デバイスを選択] ボタンをクリックしてデバイスを選択します。デバイスがこの Parallels RAS ファームに接続するために使用されたことがない場合、そのデバイスはリストに含まれないことに注意してください。詳細については、「デバイスのモニタリング」セクションを参照してください。（p. 493）デバイスを選択したら、[OK] をクリックして [有効なアクセス] ダイアログに戻ります。選択したデバイスのプロパティを使用して、すべてのフィールドに自動的に入力されます。

ユーザーを指定したら、必要に応じて追加の条件を入力します（[ユーザー] 以外のすべてのフィールドはオプションです）。

- クライアント: デバイスに割り当てられたクライアント名。これは、コンピューター名、FQDN、またはユーザーが Parallels Client に設定したカスタム名です。
- IP アドレス: クライアントの IP アドレス。
- MAC: クライアントの MAC アドレス。
- ゲートウェイ: クライアントがファームに接続するための RAS Secure Gateway の名前。

[グループの管理] ボタンを使用すると、ユーザーが 1 つまたは複数のグループに追加された場合に、ユーザーアクセスがどのように変わるのかをプレビューできます。ボタンをクリックすると、次のようになります。

1. [グループの管理] ダイアログが開き、ユーザーがすでに属しているグループのリストが表示されます。
2. [+] ボタンをクリックして、ユーザーを 1 つまたは複数の追加グループに追加します。これはシミュレーションに過ぎないことに注意してください。ユーザーが実際に追加のグループに追加されることはありません。
3. 「シミュレート」グループを削除するには、下のペインでそのグループを選択し、[-] ボタンをクリックします。
4. [有効なアクセス] ダイアログに戻るには、[閉じる] をクリックします。

最後に、指定したユーザーの有効なアクセス情報を表示するには、[表示] ボタンをクリックします。[有効なアクセス - サマリ] ダイアログが開き、次の情報が表示されます。

- 左ペインには、現在のサイトに公開済みのリソースの完全なリストが表示されます。指定したユーザーがアクセスできるリソースのみを表示するには、[許可された公開済みのリソースのみ表示] オプションを選択します。ユーザーがリソースにアクセスすることを許可されていない場合、リソース名は赤で強調表示されます。
- 右ペインには、ユーザーが左ペインで選択したリソースにアクセスできるかどうか、および選択したリソースに対してフィルターが有効になっているかどうかの情報が含まれています。追加情報には、フィルターの詳細および拡張されたグループメンバーシップが含まれる場合があります。

リソースリストを調べることで、ユーザーがアクセスできるリソースやアクセスできないリソースを確認し、必要に応じて適切なアクションを実行することができます。必要に応じて、有効なアクセス情報を CSV ファイルにエクスポートすることができます。これには、[エクスポート] ボタンをクリックしてファイル名を指定します。CSV ファイルには次の列があります。

- 名前: アプリケーション名。
- ID: アプリケーション ID。
- アクセス可能: ユーザーがアプリケーションにアクセス可能かどうか（ [はい] または [いいえ] ）。
- ルール: フィルタールール。アプリケーションに対してルールが構成されていない場合、列に値が入りません。

クライアント設定の指定

公開済みリソースのクライアント設定を指定するには、[ファーム] > <サイト> > [設定] に移動し、[クライアント設定] タブを選択します。このページで、クライアント側の公開済みアプリケーションアイコンの表示方法や他のオプションを指定できます。

アイコン解像度を選択

公開されたリソースは、アイコンまたはリストとして Parallels Client に表示されます。リソースがアイコンとして表示されるときに使用する解像度を指定できます。次のオプションから選択します。

- [標準解像度の送信] アイコン: 標準解像度のアイコン。

- [高解像度の送信] アイコン: 高解像度のアイコン。このオプションは、より多くのネットワーク帯域幅を使用することに注意してください。

オーバーレイアイコンの有効化、無効化、変更

注: これらの構成の変更は、デスクトップクライアント（Windows、Mac、Linux）にのみ適用されます。モバイルおよび Web Client には影響しません。

このタブのその他のオプションとして、オーバーレイアイコンの有効化、無効化、更新があります。オーバーレイアイコンは標準アプリケーションアイコン上に配置されるので、Parallels RAS が提供するリモートアプリケーションであることが分かります。Parallels Client からリモートアプリケーションを起動すると、アプリケーションアイコンがローカルデスクトップ（Windows ではタスクバー、macOS では Dock）上に表示されます。オーバーレイアイコンを使用すれば、実行中のアプリケーションのうちどれがリモート Parallels RAS アプリケーションで、どれがローカル（または他の種類）であるかを一目で把握することができます。

Parallels RAS ではデフォルトで、Parallels ロゴをオーバーレイアイコンとして使用しています。ただし、管理者はこれを変更して、Microsoft RemoteApp の標準的なオーバーレイアイコンを使用することもできます。Parallels ロゴをオーバーレイアイコンとして使用した場合、ローカルコンピューターのアプリケーションアイコンが次のサンプルアイコンのような外観になります。

ご覧のように、Windows の [電卓] や [ペイント] アプリケーションの標準的なアイコンの上に、Parallels のロゴアイコン（右隅の赤い平行線）が表示されています。オーバーレイの実行中、ユーザーはすぐにこれが Parallels RAS の提供するリモートアプリケーションであって、ローカルの Windows アプリケーションでないことを把握できます。

パスワード有効期限リマインダーを表示する

パスワードの有効期限が近づくと、ドメインパスワードの変更に関するリマインダーを Parallels RAS ユーザーに自動的に表示できます。この機能を有効にするには、[パスワード有効期限リマインダーを表示する] オプションを選択します。有効にすると、パスワードの有効期限が近づいている Parallels Client ユーザーが Parallels RAS に接続した直後に、通知が表示されます。このオプションは、デフォルトでは無効になります。

セッションをリセット

[Parallels Client からのログオフでセッションを強制的にリセット] オプションを選択して、ユーザーログオフ時にユーザーセッションを強制的にリセットします。これは、フリーズしたユーザーセッションをリセットするのに便利です。

クイックキーパッド

Parallels RAS Console でクイックキーパッドカテゴリーを使用すると、カスタムキーを定義して、モバイルデバイス上で実行されている公開済みのアプリケーションで共通のアクションを実行できます。カスタムキーは iOS と Android の標準キーボード上に表示され、仮想キーボードの他のキーと同様にタップできます。

この機能は、公開済みのアプリケーションを電話やタブレットで実行するユーザー向けに設計されています。特定のソフトウェアで特定のメニュー項目やツールバー項目を繰り返し選択する必要がある場合、カスタムキーを使用するとユーザーエクスペリエンスが大幅に向上する場合があります。たとえば、あるユーザーに [ファイル] > [新規] および [ファイル] > [保存] メニュー項目を繰り返し押す必要があるデータ入力タスクがあるとします。これらの操作を実行するために 2 つのカスタムキーを定義すると、ユーザーは iOS または Android の標準キーボードよりも上に表示されます。そのため、アプリケーションのネイティブメニュー項目をタップするのではなく（煩雑になる可能性があります）、これらのキーをタップすることができます。これははるかに簡単で迅速な方法です。

カスタムキーを定義するには、Parallels RAS Console で [クイックキーパッド] カテゴリーを選択します。右ペインの [クイックキーパッド] ビューで、クイックキーパッドテンプレートを作成することができます。テンプレートは、特定のアプリケーション（または同じ UI デザインを持つアプリケーションのグループ）用に作成され、アプリケーション内で共通の操作を実行するためのショートカットを含んでいます。テンプレートが作成されると、それを公開アプリケーションまたはアプリケーショングループに割り当てます。そのため、各アプリケーション（またはグループ）には独自のクイックキーパッドがあります。

クイックキーパッドテンプレートを作成するには、次の操作を実行します。

1. [タスク] ドロップダウンリストをクリックし、[新しいクイックキーパッド] をクリックします（または [+] アイコンをクリックします）。
2. クイックキーパッドのテンプレート名（「オフィスアプリ」など）を指定します。

3 クイックキーパッドは、マルチレベルメニューシステムを使用して整理できます。これを行う場合は、[新規メニュー] 項目をクリックし、メニュー項目名を指定します。サブメニュー項目も追加できます。メニューアイテムをツリーノードにドラッグアンドドロップするだけで、ツリー全体に移動できます。

4 基本的なメニュー構造を定義したら、ショートカットを追加することができます（または、好きな順序で実行できます）。

5 ショートカットを追加するには、[新しいショートカット] 項目をクリックします。

6 [ラベル] フィールドに名前（「新規」など）を入力します。

7 [ショートカット] フィールドをクリックし、ターゲットアプリケーションと同じようにキーボードのショートカットを押します。たとえば、多くのアプリケーションで新しい文書を作成するための標準ショートカットは Ctrl + N です。このショートカットを入力するには、Ctrl キーを押したまま N キーを押します。このショートカットはフィールドに「Ctrl + N」と表示されます。このフィールドには、最大 3 つのショートカットを入力できます。

8 ショートカットをテンプレートに追加するには、[新しいショートカット] 項目をもう一度クリックします。必要なショートカットがすべて定義されるまで繰り返します。

9 [OK] をクリックして、ダイアログを閉じます。クイックキーパッドリストに新しいテンプレートが表示されます。

テンプレートを変更するには、テンプレートを右クリックして [プロパティ] を選択します。

作成したテンプレートをアプリケーション（または複数のアプリケーション）に割り当てる必要があります。このためには、次の操作を実行します。

1 テンプレートを右クリックし、[アプリケーションに割り当て] を選択します（[タスク] ドロップダウンリストを使用するか、[リンク] アイコンをクリックすることもできます）。

2 [クイックキーパッドテンプレートの割り当て] ダイアログで、テンプレートを割り当てるアプリケーションを 1 つ以上選択します。

3 完了したら [OK] をクリックします。

リモートユーザーがモバイルデバイスでアプリケーションを実行し、仮想キーボードを開くと、クイックキーパッドテンプレート用に定義したショートカットに対応する追加のキーが表示されます。キーをタップすると、対応する操作が実行されます（たとえば、Ctrl-N を押すと、新しい文書が開きます）。

クイックキーパッドテンプレートのエクスポートとインポート

クイックキーパッドテンプレートをある Parallels RAS ファームから別の Parallels RAS ファームに簡単に移動するには、インポート/エクスポート機能を使用します。テンプレートをエクスポートするには、テンプレートを右クリックして [エクスポート] を選択します。ファイル名と場所を指定し、[保存] をクリックします。テンプレートをインポートするには、[クイックキーパッド] リストの空白部分を右クリックし、[インポート] を選択します。また、[タスク] ドロップダウンリストを使用してこれらのアクションを実行することもできます。

第　13　章

セッション管理

この章の内容

概要

ユーザーが Parallels RAS に接続してセッションを確立すると、セッション情報が Parallels RAS Console の次の場所に表示されます。

- [セッション] カテゴリー（Parallels RAS 18.1 から新規導入）。
- RD セッションホスト、VDI、および Azure Virtual Desktop ビューの [セッション] タブ（[ファーム] > [サイト] > [RD セッションホスト] > [VDI] > [Azure Virtual Desktop]）

[セッション] カテゴリーには、RD セッションホスト、VDI、Azure Virtual Desktop など、利用可能なすべてのホストタイプのユーザーセッションが表示されます。ここでは、セッションをホストしているサーバーの種類にかかわらず、現在のすべてのセッションを表示できます。各 [セッション] タブには、それぞれのホストタイプのセッションが表示されます。

セッションカテゴリー

メインカテゴリーリストで [セッション] カテゴリーを選択すると、RAS Console の右側ペインに以下の 2 つのタブが表示されます。

- ユーザー: 利用可能なすべてのホストタイプのユーザーセッションを一覧表示します。
- リソース: すべてのタイプのホストで現在実行中の公開済みリソース（アプリやデスクトップ）を一覧表示します。

[タスク] > [検索] をクリック（または虫眼鏡アイコンをクリック）して、1 つまたは複数の列見出しで条件を指定することで、[セッション] カテゴリーのリストをフィルタリングできます。たとえば、[ユーザー] タブのリストをホストタイプでフィルタリングするには [ソース] 列を使用します。この列には次のいずれかの値を含めることができます。

- RDSH: RD セッションホスト
- VDI: 仮想デスクトップ
- リモート PC: VDI 経由のリモート PC
- AVD: Azure Virtual Desktop

セッションタブ

[セッション] タブには、それぞれのホストタイプのセッションが表示されます。特定のホストのセッションを表示するには、ホスト名でリストをフィルタリングします。

[セッション] カテゴリーまたは [セッション] タブを開いたときに、リスト内の列の一部がすぐに表示されない場合があります。これは、これらの値を算出するのに時間がかかるためです。そのような列の例としては、[ログオン時間]、[UX エバリュエーター]、[遅延] などがあります。数秒後にはリストに値が表示されます。

この章で取り上げられている情報のほとんどは、[セッション] カテゴリーと [セッション] タブの両方に共通しています。具体的な内容や違いについては、必要に応じて説明します。

セッション情報

特定のセッションの詳細な情報を表示するには、そのセッションを右クリックして、[情報の表示] を選択します。これにより、[セッション情報] ダイアログが開き、セッションのプロパティが機能別にグループ化されます。

以下のグループが表示されます。

- セッションセットアップ: 一般的なセッション情報が表示されます。
- ログオンの詳細: ログオンプロセスを評価するために使用できるログオンメトリクスが表示されます。
- セッションの詳細: 現在のセッションの状態、ログオン時間、受信/送信データサイズ、および一般的なセッション情報が表示されます。

- 接続の詳細: 接続と認証の詳細を表示します。
- ユーザーエクスペリエンス: ユーザーエクスペリエンスを評価するために使用できるメトリクスが表示されます。
- クライアントの詳細: ユーザーデバイスと Parallels Client のタイプとバージョンに関する情報を表示します。

Parallels RAS 18 では、25 を超える新しいセッション詳細メトリクスが導入されています。以下の表は、これらの新しいメトリクスと既存の重要なメトリクスの概要を示しています。

セッションセットアップ

メトリクス	説明
セッションホスト*	セッションホスト名
ソース*	セッションカテゴリーのみ。 ホストタイプ: RDSH（VDI 経由の場合も含む）、VDI、リモート PC（VDI 経由のみ）、AVD

* Parallels RAS 18.1 で導入された新機能

ログオンの詳細

メトリクス	説明
ログオン期間*	ログオンにかかる時間（UI での待機時間を除く）。
ログオン期間の内訳*	接続時間 認証期間 ホストの準備（負荷分散アルゴリズムを含む） ユーザープロファイルの読み込み時間 RAS ポリシーの検索 グループポリシーの処理時間 デスクトップの読み込み時間 その他
ユーザープロファイル*	使用中のユーザープロファイル形式: FSLogix、ユーザープロファイルディスク、その他（エラーコードなどの付加情報も含む）。

* Parallels RAS 18.0 で導入された新機能

ユーザーエクスペリエンス

メトリクス	説明
UX エバリュエーター*	クライアント側の最初の手順（ユーザーのアクション）から最後の手順（レスポンスの画像表示）までの時間間隔を測定したものです。
接続品質*	接続品質を判定（「悪い」～「非常に良い」）
遅延*	ネットワーク遅延
トランスポートプロトコル*	TCP または UDP（RDP 経由）
帯域幅の可用性*	クライアント側の帯域幅の可用性
再接続*	現在のセッションで開始時に接続不良で再接続した回数（正常接続は除く）
最終再接続*	現在のデバイスのセッションで接続不良で再接続した回数（正常接続は除く）
切断の理由*	最終セッションの切断理由

* Parallels RAS 18.0 の新機能

セッションの詳細*

メトリクス	説明
セッションの状態	アクティブ状態、アイドル状態、切断など
ログオン時間	セッションが確立した日時
セッションの長さ	セッションが確立した時間
アイドル時間	セッションがアイドル状態だった時間
受信データ*	クライアントから受信したデータ量
送信データ*	クライアントに送信したデータ量
解像度	セッションの解像度
色深度	セッションの色深度
帯域幅の使用状況*	クライアントの帯域幅使用状況

* Parallels RAS 18.0 で導入された新機能

クライアントの詳細

メトリクス	説明

デバイス名	セッションが確立されたデバイス名
IP アドレス	クライアントのプライベート IP アドレス
クライアント OS*	クライアントで実行されているオペレーティングシステム
クライアント OS バージョン*	クライアントで実行されているオペレーティングシステムのバージョン
クライアントバージョン*	使用中の Parallels Client のバージョン

* Parallels RAS 18.0 で導入された新機能

セッション情報のエクスポート

セッション情報を CSV ファイルにエクスポートするには、[セッション情報] ダイアログの [エクスポート] ボタンをクリックして、場所とファイル名を指定します。

[タスク] > [エクスポート] をクリックして、メインセッションリストからセッション情報をエクスポートすることもできます。リストで選択する項目に応じて、以下のものがエクスポートされることに注意してください。

- シングルセッション - そのセッションに関する情報がエクスポートされます。
- マルチセッション - 選択したすべてのセッションの情報がエクスポートされます。
- 選択なし - 現在のすべてのセッションに関する情報がエクスポートされます。エクスポートされた CSV には、エクスポートされたセッションの詳細と、以下の形式でエクスポートされた詳細が含まれます。

  %Administrator% により %date% %time% にエクスポートされた Parallels RAS ファーム %Farm name% およびサイト %Site name% からのセッション詳細（RD セッションホストなどの %Server type%）

監視設定

監視設定機能では、しきい値に色の区別を追加して警告レベルと重大性レベルを特定することにより管理者やヘルプデスクのサポート環境が向上します。

監視設定を構成するには、[セッション] カテゴリーまたは [セッション] タブで、[タスク] > [監視の設定] をクリックします。ダイアログが開き、さまざまなセッションメトリクスの設定を構成できます。

1 色分けを有効にしたいメトリクスを選択します。

2 [警告] と [重要] の列にしきい値を指定します。警告のしきい値はオレンジ色で表示されます。重要のしきい値は赤色で表示されます。

3 重要の色（赤）だけを表示したい場合は、両方のしきい値を同じ値に設定します。しきい値に達したときに赤色のみが使用されます。

色分けを有効にしているメトリクスは、指定されたしきい値のいずれかを下回る場合、セッションリストにおいて緑色で強調表示されます。しきい値に達すると、メトリクスの値は、対応するしきい値の色（オレンジまたは赤）で強調表示されます。重要のしきい値は警告のしきい値以上にする必要があることに注意してください。警告と重要の両方の値が等しい場合、重要の色分けには赤色が使用されます。

監視設定はグローバル設定であり、他の RAS 管理者が表示したり変更したりすることができます。

セッションの管理

1 つのセッション（または同時に複数のセッション）を管理するには、1 つまたは複数のセッションを選択し、[タスク] ドロップダウンリストを使用して次の動作から選択します。

- 更新: リストを更新します。
- 切断: 選択したセッションを切断します。
- ログオフ: セッションをログオフします。
- メッセージを送信: [メッセージを送信] ダイアログを開きます。ここにメッセージを入力し、セッション所有者に送信できます。
- リモートコントロール: 選択したユーザーセッションをリモートでコントロールします。接続を確立するには、現在の RAS Console 管理者のドメインまたはローカル Windows アカウントの認証情報（このコンピューターにログインするためにユーザーが使用しているもの）が使用されます。現在のユーザー（特にローカルの Windows ユーザー）が、リモートコンピューターに接続する権限を所有していないこともあるので注意してください。このような場合は、[リモートコントロール（プロンプト）] オプションを使用します（以下に説明があります）。下記の「ユーザーセッションのリモートコントロール」も重要情報がありますので参照してください。
- リモートコントロール（プロンプト）: 上のものと同じですが、認証情報を入力する画面が表示されます。現在のユーザーの認証情報を使用して、セッションをコントロールできない場合に、このオプションを使用します。

- プロセスを表示: 実行中のプロセスを表示して管理します。詳細については以下の「プロセスの管理」を参照してください。

ユーザーセッションのリモートコントロール

[リモートコントロール] メニューオプションと [リモートコントロール（プロンプト）] メニューオプション（上記参照）では、ユーザー RDS セッションをシャドーできます。以下に説明するように制限があります。

- Parallels RAS は Windows 7 および Windows Server 2008 R2 では RDS セッションをシャドーできません。これはネイティブツールでも機能しません。

プロセスを管理

[タスク] > [プロセスを表示] オプションを選択すると、[実行中のプロセス] ダイアログが開き、1 つまたは複数のホストで実行中のプロセスを表示できます。

注: また、メインホストリストでサーバーを右クリックし、[プロセスを表示] を選択して、[実行中のプロセス] ダイアログを開くこともできます。これにより、選択したホストに属するプロセスのみを表示するようにフィルターが適用された [実行中のプロセス] ダイアログが開きます。

[実行中のプロセス] ダイアログで、[以下からプロセスを表示] ドロップダウンリストを使用し、次のオプションを使用してリストをフィルタリングします。

- 選択したセッション: [セッション] リストで選択したセッションのプロセスを表示します。
- 選択したサーバー: 選択したセッションが実行中のサーバーで実行しているすべてのプロセスを表示します。
- すべてのサーバー: 利用できるすべてのサーバーで実行しているすべてのプロセスを表示します。

1 つまたは複数の列に検索条件を指定してリストをフィルタリングすることもできます。これには、虫眼鏡アイコン（右上）をクリックして、1 つまたは複数の列に希望するテキストを入力します。リストは、指定された条件に適合した入力に合わせてフィルタリングされます。

[実行中のプロセス] ダイアログの [タスク] ドロップダウンリストには次のオプションがあります。

- 更新: リストを更新します。
- プロセスの強制終了: 選択したプロセスを強制終了します。

- 公開したアイテムに進む: 実行中の公開済みリソースに属しているプロセスを選択すると有効になります。Parallels RAS Console のメインウィンドウが表示され、対応する公開済みリソースに移動します。
- 切断: セッションを切断します。
- ログオフ: セッションをログオフします。
- メッセージを送信: セッション所有者にメッセージを送信します。
- リモートコントロール: 選択したユーザーセッションをリモートでコントロールします。

リソースタブ

[セッション] カテゴリーの [リソース] タブには、現在実行中の公開済みリソース（アプリやデスクトップ）が表示されます。

注意すべき列をいくつか紹介します。

- ID: 公開済みのリソース ID（[公開] カテゴリーに表示）。
- 公開済みの名前: 公開済みのリソースの名前（[公開] カテゴリーに表示）。
- ユーザー: セッション所有者。
- セッション ID: セッション ID。
- セッションホスト: セッションホスト名。
- ソース: セッションソース（RDSH、VDI、リモート PC、AVD）。

リソースに対してタスクを実行するには、[タスク] メニューをクリックします。次のようなタスクを実行できます:

- 検索: 1 つまたは複数の列（ユーザー、セッション ID、セッションホストなど）を使ってリストをフィルタリングできます。
- ユーザーセッションビュー: [ユーザー] タブに切り替え、フィルターを適用して、選択されたリソースが属するセッションを表示します。
- 公開済みリソースに進む: [公開] カテゴリーに移動し、選択したリソース情報を表示します。
- 情報の表示: リソースサマリー情報とセッション情報を表示します。セッション情報には、「セッション情報」（p. 330）に記載されているものと同じメトリクスが含まれています。

第　14　章

SSL 証明書の管理

Parallels RAS Console には、お使いのすべての SSL 証明書を 1 か所で管理できる、証明書管理インターフェイスが含まれています。

証明書はサイトレベルで管理されます。証明書がサイトに追加されると、その証明書は同じサイト上の RAS Secure Gateway や HALB で使用できるようになります。

証明書を管理するには、RAS Console で [ファーム] > [サイト] > [証明書] に移動します。右ペインの [証明書] タブには、既存の証明書が表示されます。Parallels RAS をインストールすると、<デフォルト> の自己署名証明書が自動的に作成されるので、証明書のリストには少なくともデフォルトの証明書が表示されます。デフォルトの証明書も、自動的にすべての新しい RAS Secure Gateway や HALB に割り当てられます。

後続のセクションでは、証明書管理タスクについて詳しく説明し、証明書に関するその他の情報や指示を取り上げます。

この章の内容

自己署名証明書の生成

自己署名証明書を生成するには、[ファーム] > [サイト] > [証明書] に移動します。[タスク] > [自己署名証明書の生成] をクリックします。ダイアログが開いたら、次のオプションを指定します。

- 名前: 証明書の名前を入力します。このフィールドは入力必須です。
- 説明: オプションの説明。
- 使用方法: 証明書に RAS Secure Gateway と HALB のどちらを使用するか、あるいはその両方を使用するかを指定します。この選択は必須です。
- キーサイズ: 証明書のキーサイズのビット数。ここでは、定義済みの値から選択できます。デフォルト値は、現在の業界標準で必要最小の長さとされる 2048 ビットです。
- 国コード: 国を選択します。
- 有効期限: 証明書の有効期限。
- 都道府県: 都道府県名。
- 市: 市の名前。
- 組織: 組織の名前。
- 部門: 部門名。
- メール: ご利用のメールアドレスです。このフィールドは入力必須です。
- 氏名: コモンネーム（CN）、または完全修飾ドメイン名（FQDN）とも呼ばれるもの。このフィールドは入力必須です。
- 代替名: 1 つまたは複数のサブジェクト代替名（SAN）を指定します。[...] アイコンをクリックして、1 つまたは複数の DNS または IP アドレスを追加します。なお、モバイル機器用の Parallels Client は SAN フィールドをサポートしていないので、共通の名前には大部分のモバイルデバイスで使用される一般的なものを設定するのが安全です。

[保存] をクリックして、証明書を作成します。完了すると、作成した証明書は RAS Console の [証明書] リストに表示され、[ステータス] 列には [自己署名] であることが示されます。

証明書情報を表示するには、証明書情報を右クリックして [プロパティ] を選択します。表示されるダイアログでプロパティを調べてから、[証明書情報の表示] ボタンをクリックして、証明書の信頼性に関する情報、詳細、認定パス、証明書の状態を表示してください。証明書情報は、項目を右クリックして [証明書情報の表示] を選択することによっても表示できます。

証明書署名要求の生成（CSR）

CSR を生成するには、[ファーム] > [サイト] > [証明書] に移動します。[タスク] > [証明書要求の生成] をクリックします。ダイアログが開いたら、必要な情報を指定してください。CSR の

作成に必要な情報は、前述の自己署名証明書（p. 338）で必要な項目とまったく同じです。詳細は、該当のセクションで説明したオプションリストを参照してください。

情報を入力したら、[作成] をクリックしてください。別のダイアログが開いて、作成した証明書署名要求が表示されます。証明書署名要求をコピーしてテキストエディターに貼り付け、記録用にファイルを保存します。このダイアログの時点で、ダイアログからパブリックキーをインポートできるようになります。ここでダイアログを開いたまま、証明書署名要求を証明書認証局に送信して、パブリックキーを取得しインポートしておくことも、または後で行うこともできます。ダイアログを閉じると、証明書は RAS Console に表示され、[ステータス] 列に [リクエスト済み] であることが示されます。

証明書署名要求を証明書認証局に送信し、パブリックキーをインポートするには、次の操作を実行します。

1 証明書署名要求の [プロパティ] ダイアログが閉じている場合は、証明書を右クリックして [プロパティ] を選択し、ダイアログを開きます。ダイアログで、[リクエスト] タブを選択します。

2 証明書署名要求をコピーして認証局のウェブページに貼り付けるか、電子メールで送信（その場合は、後でこのダイアログに戻る必要があります）します。

3 証明書認証局から証明書ファイルを取得します。

4 [パブリックキーのインポート] ボタンをクリックし、キーファイルと証明書ファイルを指定して、証明書の登録を完了します。

Let's Encrypt 証明書

Let's Encrypt 証明書のリクエスト

Let's Encrypt は、グローバルな認証局（CA）です。この組織は非営利団体であり、証明書の発行に費用は一切発生しません。各証明書の有効期限は 90 日間です。RAS Console では、Let's Encrypt の証明書の発行、自動更新、取り消しを行うことができます。

Let's Encrypt 証明書の発行

新しい Let's Encrypt 証明書を発行するには、次の手順を実行します。

1 RAS Console で、[ファーム] > [証明書] に移動します。

2 [タスク] ドロップダウンメニューの左側にある [+] ボタンをクリックし、[Let's Encrypt 証明書を発行] を選択します。

3 [Let's Encrypt EULA を読んで同意しました] オプションを選択します。

4 Lets Encrypt から通知を受領するメールアドレスを、[期限切れのメール] フィールドのリストで指定します。

5 オプションとして、[期限切れの前に自動的に証明書を更新] フィールドで、証明書が自動的に更新される時間を変更できます。

6 [OK] をクリックします。

7 [Let's Encrypt 証明書を発行] ダイアログで、以下を指定します。

- 名前: 証明書の名前です。
- 説明: 証明書の説明です。
- 使用方法: HALB または Secure Gateway を指定できます。
- キーサイズ: キーサイズです。
- 国コード: お住まいの国のコードです。
- 都道府県: お住まいの都道府県です。
- 市: お住まいの市区町村です。
- 組織: 所属している組織の名前です。
- 部門: 所属している組織の部署です。
- メールアドレス: 所属組織のメールアドレスです。
- 氏名: 一般にアクセス可能な HALB または Secure Gateway の有効なドメイン名です。
- 代替名: 一般にアクセス可能な HALB または Secure Gateway 有効なドメイン名です。

8 [保存] をクリックします。

Lets Encrypt 証明書を手動で更新する

Lets Encrypt 証明書を手動で更新するには、次の手順を実行します。

1 RAS Console で、[ファーム] > [証明書] に移動します。

2 更新する Let's Encrypt 証明書を右クリックします。

3 コンテキストメニューで、[制御] > [更新] の順に選択します。

Let's Encrypt 証明書を取り消す

Let's Encrypt 証明書を取り消すには、次の手順を実行します。

1 RAS Console で、[ファーム] > [証明書] に移動します。

2 取り消す Let's Encrypt 証明書を右クリックします。

3 コンテキストメニューで、[制御] > [取り消し] の順に選択します。

4 [証明書を取り消し] ダイアログで、証明書を取り消す理由を選択します。

5 [取り消し] をクリックします。

Parallels RAS が Let's Encrypt に証明書を要求する方法

Parallels RAS を使用して Let's Encrypt 証明書を新規に作成する場合、以下の処理が実行されます。

1 ライセンスロールをホストする Parallels RAS プライマリ Connection Broker が、Let's Encrypt サーバーにアカウントを作成するための最初のリクエストを行います。

2 アカウント作成の確認を受け取ります。Parallels RAS は CSR を作成し、Let's Encrypt サーバーに送信します。

3 チャレンジのリストを受信して、Connection Broker で Let's Encrypt サーバーから送信された HTTP トークンの読み取りが行われます。

4 Secure Gateway または HALB は、Connection Broker からトークンを取得します。

5 準備が整うと、Connection Broker から Let's Encrypt Server に通知が行われます。

6 Let's Encrypt から、Secure Gateway または HALB へのアクセスが行われ、トークンの有無の確認により検証プロセスが開始されます。

7 Secure Gateway または HALB が指定されたドメインに返信できることが確認され、チャレンジが完了します。

8 チャレンジが正常に完了したとの仮定に基づき、Parallels RAS は証明書を要求します。

9 有効な証明書が Let's Encrypt サーバーから Connection Broker にダウンロードされます。

10 Connection Broker から、Secure Gateways または HALB に証明書が配信されます。

証明書のインポート

証明書をファイルからインポートするには、[証明書] タブで、[タスク] > [証明書のインポート] をクリックします。ダイアログが開いたら、以下を指定します。

- 名前: 証明書の名前を入力します。
- 説明: オプションの説明。
- プライベートキーファイル: プライベートキーを含むファイルを指定します。ファイルを参照するには、[...] ボタンをクリックします。
- 証明書ファイル: プライベートキーファイル（上述）を指定し、それに一致する証明書ファイルがある場合、そのファイルがこのフィールドに自動的に挿入されます。そうでない場合は、証明書ファイルを指定してください。
- 使用方法: 証明書に RAS Secure Gateway と HALB のどちらを使用するか、あるいはその両方を使用するかを指定します。

完了したら [OK] をクリックします。インポートした証明書は RAS Console のリストに表示され、[ステータス] 列には [インポート済み] であることが示されます。

証明書情報を表示するには、証明書情報を右クリックして [プロパティ] を選択します。表示されるダイアログでプロパティを調べてから、[証明書情報の表示] ボタンをクリックして、証明書の信頼性に関する情報、詳細、認定パス、証明書の状態を表示してください。証明書情報は、項目を右クリックして [証明書情報の表示] を選択することによっても表示できます。

インポート済みの証明書には、[プロパティ] ダイアログに [中間] という追加のタブがあります。オリジナル証明書に（ルート証明書に加えて）中間証明書が含まれている場合は、そのタブに中間証明書が表示されます。希望する場合は、別の中間証明書をタブに貼り付けることもできます。

証明書のエクスポート

証明書をファイルにエクスポートするには、[証明書] タブで、[タスク] > [証明書のエクスポート] をクリックし、ファイル名を指定してから [保存] をクリックします。その後、[タスク] > [証明書のインポート] をクリックして、[プライベートキーファイル] フィールドで証明書ファイルを指定すれば、エクスポートした証明書を別のファームやサイトにインポートできます。

証明書の Secure Gateway や HALB への割り当て

証明書をサイトに追加した後、作成時に指定した使用方法のタイプに応じて、証明書を RAS Secure Gateway と HALB のどちらか、あるいはその両方に割り当てることができます（この章の始めで説明しています）。証明書の [使用方法] オプションについては、以下に詳しく説明します。

証明書の使用方法

証明書の [使用方法] は、証明書の作成時に指定するオプションです。証明書を RAS Secure Gateway と HALB のどちらで利用するか、あるいはその両方で利用できるようにするかを指定します。このオプションを設定するとき、以下から選択できます。

- Secure Gateway: このオプションを選択すると、RAS Secure Gateway で証明書が利用できるようになります。
- HALB: このオプションを選択すると、HALB で証明書が利用できるようになります。

ゲートウェイと HALB のどちらか、あるいはその両方を選択できます。両方を選択すると、ゲートウェイと HALB の両方で証明書が利用できるようになります。証明書を作成する方法やオプションを選択する方法について詳しくは、「自己署名証明書の作成」（p. 338）および「証明書署名要求（CSR）の作成」（p. 339）を参照してください。

後で RAS Secure Gateway や HALB の SSL を構成する場合は、SSL 証明書を指定する必要があります。その手順の詳細については、「SSL/TLS 暗号化」（p. 93）および「RAS Console での HALB の構成」（p. 390）を参照してください。証明書を選択する際は、[使用方法] オプションが特定の証明書にどのように構成されているかに応じて、次のオプションを利用できます。

- 一致する使用方法すべて: これはデフォルトオプションで、いつでも利用できます。このオプションは、[使用方法] の選択内容がオブジェクトのタイプ（ゲートウェイや HALB）に一致する証明書が使用されるというものです。たとえば、ゲートウェイを構成していて、[使用方法] が「ゲートウェイ」に設定されている証明書がある場合、その証明書が使用されます。証明書の使用方法オプションでゲートウェイと HALB が両方とも選択されている場合も、その証明書は該当のゲートウェイで使用できます。これは、LB SSL ペイロードを構成する際の HALB でも同様です。なお、このオプションがゲートウェイや HALB で選択されているものの、一致する証明書が存在しない場合は、警告メッセージが表示されます。この場合、まず証明書を作成する必要があります。

- [証明書] ドロップダウンリストのその他の項目は個別の証明書ごとに扱われ、証明書の [使用方法] の設定に応じて、リストに表示されたり表示されなかったりします。たとえば、HALB の LB SSL ペイロードを構成していて、[使用方法] オプションが「HALB」に設定されている証明書がある場合、その証明書はドロップダウンリストに表示されます。一方、[使用方法] が「ゲートウェイ」に設定されている証明書はリストに含まれません。

また、1 つの証明書だけですべてのゲートウェイを使用したい場合は、証明書を作成し、その [使用方法] オプションを「ゲートウェイ」に設定する必要があります。その後、各ゲートウェイにこの証明書を使用するように構成するか、[一致する使用方法すべて] の選択内容をデフォルト値のままにすれば、証明書はゲートウェイによって自動的に取得されます。これは HALB についても同様です。

ゲートウェイ

証明書を RAS Secure Gateway に割り当てるには、次の操作を実行します。

1. [ファーム] > [サイト] > [Secure Gateway] に移動します。
2. ゲートウェイを右クリックし、[プロパティ] を選択します。
3. [SSL/TLS] タブを選択します。
4. [証明書] ドロップダウンリストで、作成した証明書を選択します。
5. [OK] をクリックします。

[一致する使用方法すべて] オプションを選択することもできます。そうすると、使用方法がゲートウェイあるいはゲートウェイと HALB の両方に設定されている証明書が使用されることになります。

HALB

証明書を HALB に割り当てるには、[ファーム] > [サイト] > [HALB] に移動します。HALB が有効かつ構成済みで、[LB SSL ペイロード] オプションを選択されていると仮定して、以下の手順に従ってください。

1. [LB SSL ペイロード] オプションの横の [構成] をクリックします。
2. [モード] オプションが [SSL オフローディング] に設定されている場合は、証明書を使用する必要があります。上記と同様、こちらも選択されていると仮定して、次の手順に進んでください。
3. [構成] をクリックします。

4 [SSL] ダイアログで、[証明書] ドロップダウンリストから証明書を選択します。

ゲートウェイの場合と同様、[一致する使用方法すべて] オプションを選択することもできます。そうすると、使用方法が HALB あるいは HALB とゲートウェイの両方に設定されている証明書が使用されることになります。

証明書の監査

証明書に関して実行されるすべてのアクションは監査されており、後で閲覧することができます。証明書に加えた変更を元に戻すことはできませんので注意してください。以前の状態に戻したい場合は、証明書を削除し、新しい証明書を作成する必要があります。

証明書を監査するには、次の操作を実行します。

1 RAS Console で、[ファーム] > [サイト] > [証明書] に移動します。

2 [タスク] > [設定監査] をクリックします。

3 証明書に関して実行されたアクションの履歴を確認できるダイアログが開きます。[元に戻す] ボタンは無効になっていますので注意してください。本セクションの始めで説明したように、証明書に関して実行したアクションについて、元に戻すことはできません。

4 特定の監査エントリの詳細を確認するには、エントリをダブルクリックします。

証明書管理の権限

root 管理者や上級管理者には常に、証明書を管理する権限があります。デフォルトでは、カスタム管理者に証明書を管理する権限はありません。上級管理者に証明書管理の権限を付与する際には、[証明書] のグローバルアクセスを許可する権限タイプが使用されます。

root 管理者や上級管理者は、次のように証明書の権限を設定できます。

1 RAS Console で [管理] > [アカウント] に移動します。

2 カスタム管理者アカウントを選択し、[タスク] > [プロパティ] をクリックします。

3 [アカウントのプロパティ] ダイアログで [権限の変更]をクリックします。

4 [アカウントの権限] ダイアログで、左側のペインでサイトを選択してから [権限の変更] をクリック（または右側のペインの [編集] リンクをクリック）します。

5 左側のペイン（権限タイプ）で [証明書] を選択します。

6 右側のペイン（グローバル権限）で 1 つまたは複数の権限を選択します。

7 完了したら、すべてのダイアログを閉じます。

RAS 管理者も、権限をカスタム管理者に委任することができます。そのためには、[ファーム] > [サイト] > [証明書] に移動し、[タスク] > [権限を委任] をクリックします。表示されるダイアログで、権限を任意のカスタム管理者に委任できます。

旧バージョンの RAS からのアップグレード

Parallels RAS を RAS 17.1 より前のバージョンから RAS 17.1（以降）にアップグレードすると、RAS Secure Gateway や HALB で使用していた証明書はすべて列挙され、一意の証明書のみが [証明書] のサブカテゴリーに追加されます。その後、ゲートウェイや HALB は、アップグレード前に使用していた各証明書に 1 対 1 でリンクされます。

アップグレードに関連したその他のアクションには、以下が含まれます。

- ゲートウェイの [デフォルト値を継承] オプションが、アップグレード後はオフになる。
- アップグレード中にゲートウェイを無効化すると、ゲートウェイが使用する証明書の情報が Connection Broker に残るので、オンラインに復帰した際、ゲートウェイに正しく構成される。
- サイトのデフォルト設定が、デフォルトの自己署名証明書を使用するように構成される。
- サイトのデフォルト値をアップグレード後に変更していない限り、新しいゲートウェイが追加されたときに、デフォルトの自己署名証明書を使用するように構成される。

第　15　章

接続および認証の設定

Parallels RAS 管理者には、ユーザーが Parallels RAS に接続する方法をカスタマイズする能力があります。この章では、組織の要件に従って構成できる接続および認証の設定について説明します。その後、セキュリティレベルを強化するための二要素認証の使用方法について説明します。

この章の内容

RAS Connection Broker の接続設定

RAS Connection Broker の接続設定には、[接続] カテゴリーからアクセスします。

認証タイプの選択

[認証] タブを選択します。[許可された認証タイプ] セクションで次のいずれかのオプションを選択します。

- 資格情報: ユーザー資格情報は RAS が実行されている Windows システムによって認証されます。Windows の認証に使用される資格情報も、RDP セッションにログインするために使用されます。
- スマートカード: スマートカード認証。Windows 認証と同様に、スマートカードの資格情報は、RAS と RDP 間で共有されます。そのため、スマートカードの資格情報を入力する必要があるのは 1 回だけです。Windows 認証と異なり、ユーザーに必要な情報はスマートカードの PIN のみです。ユーザー名はスマートカードから自動的に取得されるため、ユーザーはこれを提供する必要がありません。

- ウェブ（SAML）: SAML SSO 認証。

スマートカードの認証情報が無効の場合、RAS Connection Broker は Local Security Authority Subsystem Service （LSASS）を組み込みません。スマートカード認証は、Parallels Client for Windows/Mac/Linux で使用できます。Parallels Client が RDP セッション内で実行されている場合、スマートカードは認証に使用できないことに注意してください。

スマートカードの証明書

スマートカードを使用するには、ユーザーのデバイスに有効な証明書をインストールしておく必要があります。そのためには、認証局のルート証明書をデバイスの鍵ストアにインポートしなければなりません。

以下の条件を満たした証明書を使用してください。

- ”キー使用法”フィールドにデジタル署名が入っていなければなりません。
- ”サブジェクト代替名”（SAN）フィールドにユーザーのプリンシパル名（UPN）が入っていなければなりません。
- ”拡張キー使用法”フィールドにスマートカードのログオンとクライアント認証が入っていなければなりません。

認証ドメイン

認証ドメインを指定するには、次のいずれかを選択します。

- 特定: このオプションを選択し、特定のドメイン名を入力します。
- 信頼性のある全ドメイン: Parallels RAS に接続するユーザーについての情報がフォレスト内のさまざまなドメインに保存されている場合、複数のドメインに対して認証するには、[信頼性のある全ドメイン] オプションを選択します。
- 指定されたクライアントドメインを使用: このオプションを選択すると、Parallels Client の接続プロパティで指定されたドメインを使用します。クライアント側でドメイン名が指定されていない場合、上記の設定に従って認証が行われます。
- クライアントに NetBIOS 資格情報の使用を強制する: このオプションを選択すると、Parallels Client はユーザー名を NetBIOS ユーザー名で置き換えます。

注: スマートカードの資格情報の“Subject Alternative Name”（SAN）フィールドにユーザープリンシパル名（UPN）がない場合（あるいは、“Subject Alternative Name”フィールド自体がない場合

）、[クライアントに NetBIOS 資格情報の使用を強制する] オプションを無効にする必要があります。

推奨: ドメイン名の変更や、その他の認証関連の変更を行った後は、[設定] タブの [セッション ID のキャッシュを削除する] ボタンをクリックしてください。

ドメインユーザー以外に対する認証

スタンドアロンマシンで指定されたユーザーに対してユーザーセッションを認証するには、ドメイン名の代わりに [ワークグループ名] / [マシン名] を入力する必要があります。ワークグループ WORKGROUP のメンバーである SERVER1 と呼ばれるマシン上のローカルユーザーのリストに対してユーザーを認証する場合、ドメインフィールドには次のように入力します。WORKGROUP/SERVER1

ドメインのパスワードを変更する

ドメインパスワードの変更にカスタム URL を使用するように Parallels Client を構成できます。

ドメインパスワードの変更にカスタム URL を使用するように Parallels Client を構成するには、次の手順を実行します。

1 [”ドメインパスワードを変更”オプションにカスタムリンクを使用する] を選択します。

2 以下のテキストフィールドにリンクを追加します。

リモートセッションの設定

[接続] カテゴリーの [設定] タブで、次のリモートセッションオプションを構成できます。

ユーザーセッションがアイドル状態になるまでの時間

このオプションはレポート統計に影響します。これにより、指定した時間アクティビティがない場合、セッションはアイドル状態として宣言されます。

FIPS 140-2 暗号化

[FIPS 140-2 暗号化] プロパティでは、FIPS 暗号化接続が許可されるかどうか、または RAS Secure Gateway で適用されるかどうかも指定できます。暗号化を許可（または適用）するとき

、Gateway では FIPS 140-2 暗号化モジュールが使用されます。次のオプションから選択できます。

- 無効: FIPS 140-2 暗号化は、RAS Secure Gateway では無効にされています。
- 許可: RAS Secure Gateway は、FIPS 暗号化および FIPS 以外の暗号化接続の両方を受け入れます。
- 強制: RAS Secure Gateway は、FIPS 暗号化接続を受け入れ、FIPS 以外の暗号化接続を切断します。

注: FIPS 140-2 暗号化が機能するには、FIPS に準拠した証明書を各 RAS Secure Gateway にインストールする必要があります。

FIPS 140-2 暗号化を有効にすると、RAS Console の [情報] > [サイト] タブに暗号化ステータスが表示されます。RAS Secure Gateway の [暗号化] プロパティを探します。

注: FIPS を使用する場合、TLS の最小要件のバージョンは自動的に 1.2 に設定されます。

FIPS 140-2 暗号化は、以下を除くすべてのバージョンの Parallels Client でサポートされています。

- Windows 8.1 以降にインストールされた Parallels Client for Windows
- Parallels Client for Android
- Parallels Client for iOS
- Web Client

注: Parallels Client for ARM64 では FIPS 140-2 はサポートされていません。

また、FIPS 140-2 暗号化が適用される場合は、特定のファームにおけるすべてのユーザーが対象となることに注意してください。あるユーザーグループには FIPS を強制的に適用し、別のユーザーグループには強制しない設定が必要な場合、この処理のために別個のファームを導入する必要があります。

アイドル状態のクライアントを自動的にログアウトさせる

アイドル状態のクライアントをログアウトするまでの時間を指定します。接続をログアウトすると、ユーザーは Parallels RAS から切断され、ログアウトしたことを通知するために、そのユーザーには Parallels Client で [接続] ダイアログが表示されます。必要に応じて、このダイ

アログを使用して再度ログオンできます。Parallels Client の接続は、最後のユーザーセッションが切断またはログオフされた後はアイドル状態とみなされます。

キャッシュされた認証トークンのタイムアウト

セッションをキャッシュしている時間を指定します（時間が長いほど AD トランザクションが少なくなります）。

キャッシュされた認証トークンをクリア（ボタン）

キャッシュされたセッション情報をすべてクリアします。

ログオン時間の設定

注: この機能は、バージョン 19 より前の Parallels Client および Parallels Client for Chrome ではサポートされていません。ログオン時間ルールを作成すると、これらいずれかのクライアントによって（サイト内の）公開済みリソースに接続する機能が制限されます。

ログオン時間制限は、柔軟な表現的記述で設定できるルールにより、指定された時間帯について公開済みリソースへのユーザーアクセスを制限する機能です。

前提条件

タイムゾーンのリダイレクト機能を任意の方法で動作させるには、サーバー上で設定する必要があります。

グループポリシー設定 [タイムゾーンリダイレクトを許可] を有効化するには、次の操作を実行します。

1 Active Directory サーバーで、グループポリシー管理コンソールを開きます。

2 ドメインとグループポリシーオブジェクトを展開します。

3 グループポリシー設定用に作成した GPO を右クリックし、[編集] を選択します。

4 グループポリシー管理エディターで、[コンピューターの構成] > [ポリシー] > [管理テンプレート] > [Windows コンポーネント] > [リモートデスクトップサービス] > [リモートデスクトップセッションホスト] > [デバイスとリソースのリダイレクト] に移動します。

5 設定 [タイムゾーンリダイレクトを許可] を有効化します。

新しいログオン時間のルールを追加する

新しいログオン時間のルールを追加するには、次の手順を実行します。

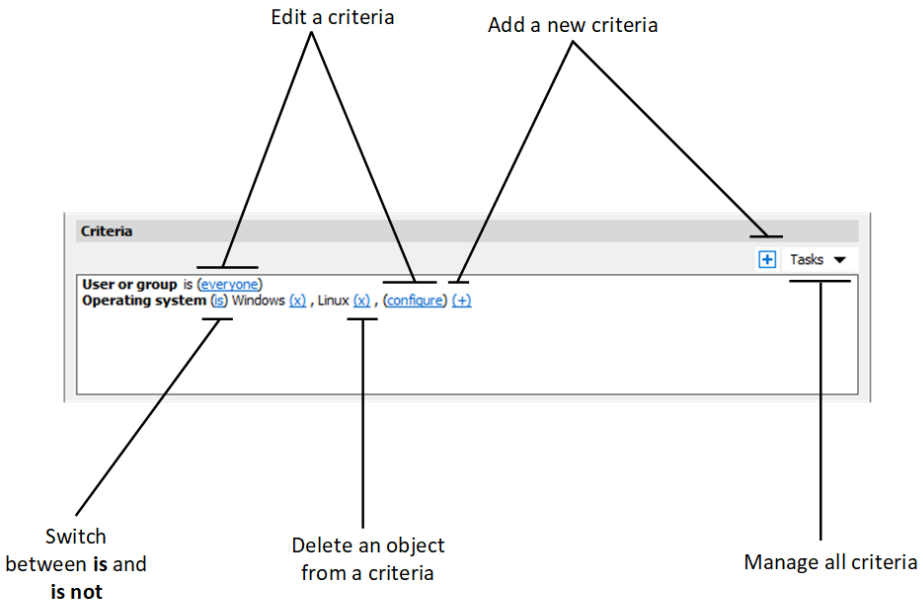
1 RAS Console で、[接続] > [ログオン時間] タブを選択します。

2 [タスク] > [追加] をクリックします（または [+] アイコンをクリックします）。

3 [名前] フィールドで、ルールの名前を指定します。

4 [説明] フィールドで、ルールの説明を追加します

5 [条件] セクションで、ルールの条件を指定します。以下のコントロールを利用できます。



- （+）：新しい条件を追加します。一致条件として、Secure Gateway、クライアントデバイス名、クライアントデバイスのオペレーティングシステム、IP アドレス、ハードウェア ID のいずれかを使用したい場合は、（+）をクリックします。 表示されるコンテキストメニューで、マッチングさせたいオブジェクトの種類を選択し、表示されるダイアログで特定のオブジェクトを追加します。新しい条件が次の行に表示されます。
- （X）：マッチングから特定のオブジェクトを削除します。たとえば、IP アドレス 198.51.100.1 をマッチングから削除したい場合は、その横にある（X）をクリックします。このコントロールは、少なくとも 1 件のオブジェクトが追加されたときに表示されます。条件内のすべてのオブジェクトが削除された場合、その条件は削除されます。

- is および is not: ユーザー接続が条件に一致した場合に、ログオン時間ルールを適用するかどうかを指定します。これらのオプションは、クリックすると切り替わります。このコントロールは、少なくとも 1 件のオブジェクトが追加されたときに表示されます。
- configure: マッチさせるオブジェクトのリストを編集します。このリンクをクリックして新しいオブジェクトを追加または削除します。最初の条件（ユーザーまたはグループ）の場合、このリンクは everyone と呼ばれることに注意してください。この条件のオブジェクトを指定すると、構成が変更されます。

6 [ログオン時間] では、ユーザーのログオンが許可される時間帯を指定します。特定の曜日や時間帯のログオンを拒否するには、任意の曜日や時間帯を選択し、表の右側にある [ログオン拒否] ボタンをクリックします。

7 [OK] をクリックします。

8 [適用] をクリックします。

注: ログオン時間のルールが指定されていない場合は、公開済みリソースへのアクセスは制限されません。ルールが指定されていても、ユーザー接続がそのいずれにも一致しない場合、ユーザーのアクセスは拒否されます。

また、ログオン時間ルールには、以下の設定を追加することもできます。

- ログオンが許可されている時間外に Parallels Client の接続を許可しない: このオプションが選択されると、Parallels Client はサイト上で公開されているリソースに接続できなくなります。
- 時間が超過した場合にユーザーセッションを切断: このオプションが選択されている場合、セッションが切断される際に通知がユーザーに表示されます。このオプションが選択されている場合、以下の項目を設定できるようになります。
  - 切断の前にユーザーに通知: クライアントをファームから切断する際、Parallels RAS からユーザーに対して前もって通知する時間を設定します。
  - セッション時間の延長を許可: このオプションが選択されている場合、セッションを延長できるようになります。

これらの設定を指定するには、以下の手順を実行します。

1 RAS Console で、[接続] > [ログオン時間] タブを選択します。

2 構成するルールを選択します。

3 [タスク] メニューの左側にある歯車のアイコンをクリックします。[オプション] ダイアログが開きます。ここから、必要なオプションを選択します。

Parallels Client の種類とビルド番号によるアクセスの制限

Parallels Client による Parallels RAS ファームへの接続や公開済みのリソースの一覧表示を可能にするため、Parallels Client の種類とバージョン番号に関して最低要件を指定することができます。さらに、Parallels Client のセキュリティパッチレベルを設定することができます（このセクションで後述）。

Parallels Client の要件を指定するには、次の操作を実行します。

1 RAS Console で、[接続] カテゴリーを選択し、[許可されたデバイス] タブを選択します。

2 [最新のセキュリティパッチを適用したクライアントのみ許可する] オプションは、Parallels Client のセキュリティパッチレベルを指定します。このオプションを選択すると、最新のセキュリティパッチを適用したクライアントのみが Parallels RAS への接続を許可されます。通常、このオプションは、脆弱性から環境を保護するために選択する必要があります。セキュリティパッチがインストールされていない古いバージョンの Parallels Client を使用する必要がある場合のみ、このオプションをオフにしてください。詳細については、次のナレッジベースの記事を参照してください: https://kb.parallels.com/en/125112。

3 [モード] ドロップダウンリストで、次のオプションを選択します。

- すべてのクライアントにシステムへの接続を許可: 制限はありません。Parallels Client のすべての種類とバージョンにフルアクセスが許可されます。
- 選択したクライアントのみにシステムへの接続を許可: Parallels RAS ファームへの接続を許可する Parallels Client の種類とバージョンを指定できます。[クライアント] リストで、希望する Parallels Client の種類を選択します。[最小ビルド番号] の値を設定するには、クライアントタイプを右クリックして、[編集] を選択します。[最小ビルド番号] 列にバージョン番号を直接入力します。
- 選択したクライアントのみに公開した項目の一覧表示を許可: 公開済みのリソースをリストに表示できる Parallels Client の種類と番号を指定できます。上記のオプションと比較して、このオプションでは、Parallels Client から Parallels RAS への接続は制限されません。このオプションを選択したら、[クライアント] リストで、希望する Parallels Client の種類を選択します。[最小ビルド番号] の値を設定するには、クライアントタイプを右クリックして、コンテキストメニューで [編集] を選択します。[最小ビルド番号] 列にバージョン番号を直接入力します。

制限が設定され、ある Parallels Client がリストから除外された場合、このクライアントを実行しているユーザーには該当するエラーメッセージが表示され、システム管理者に問い合わせるように勧められます。

多要素認証

Parallels RAS では、アクセス制御に多要素認証を使用できます。多要素認証が使用される場合、ユーザーはアプリケーションリストを取得するために連続する 2 つのステージを経て認証することが必要になります。第 1 レベルの認証は、常にネイティブ認証（Active Directory/LDAP）を使用しますが、第 2 レベルの認証では、次のいずれかのソリューションを使用できます。

- RADIUS（p. 357）
  - Azure MFA（RADIUS）
  - Duo（RADIUS）
  - FortiAuthenticator（RADIUS）
  - TekRADIUS
  - RADIUS
- TOTP（p. 365）
  - Google Authenticator
  - Microsoft Authenticator
  - TOTP（時間ベースのワンタイムパスワード）
- Deepnet
- SafeNet（p. 377）

多要素認証では、標準のユーザー名とパスワードを使用する代わりに、静的ユーザー名と、トークンによって生成された一時パスワードを使用するので、さらに強固なセキュリティを提供します。

MFA プロバイダーを追加する方法については、「MFA プロバイダーの追加」（p. 357）を参照してください。

「MFA ルールの構成」（p. 378）も参照してください。

MFA プロバイダーを追加する

MFA プロバイダーを追加するには、次の手順を実行します。

1 RAS Console で、[接続] > [多要素認証] タブを選択します。

2 [タスク] > [追加] をクリックします（または [+] アイコンをクリックします）。

3 任意の MFA プロバイダーを選択します。ウィザードが開きます。

4 ウィザードウィンドウで、以下のパラメーターを指定します。

- 名前: プロバイダーの名前です。
- 説明: プロバイダーの説明です。
- [テーマ] テーブルで、この MFA プロバイダーを使用するテーマを選択します。

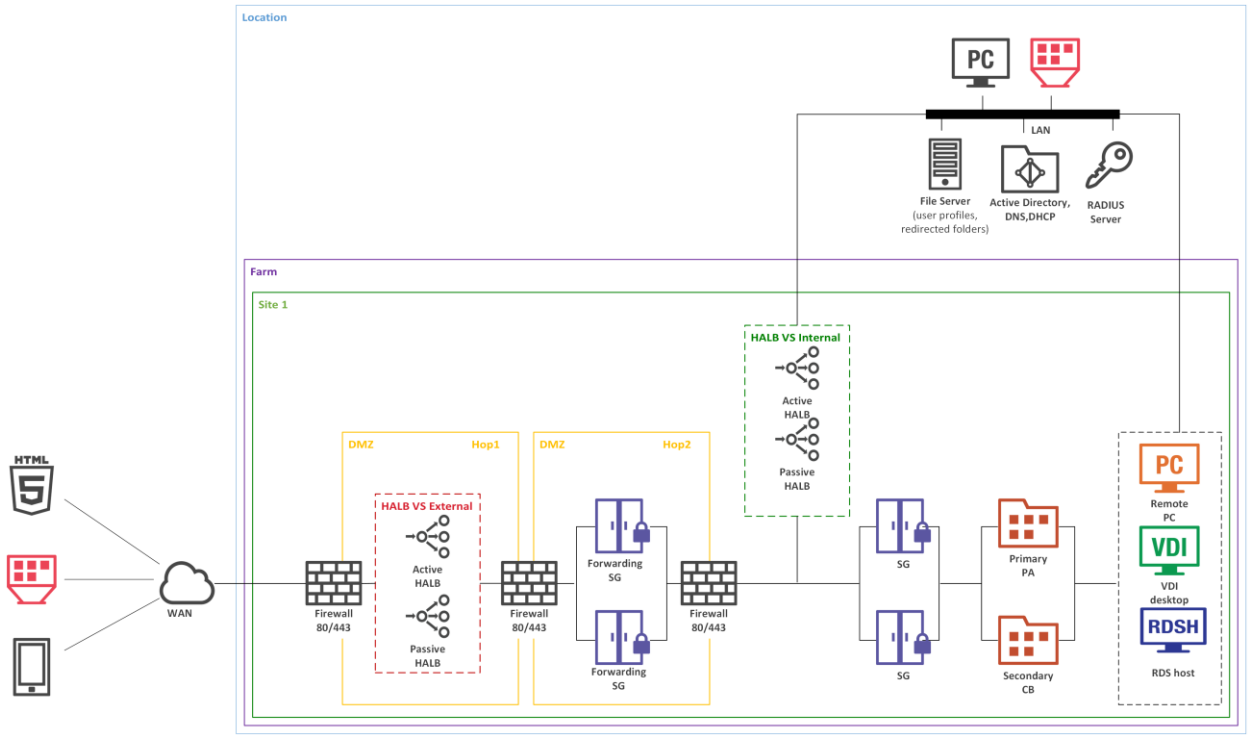
5 [次へ] をクリックします。

6 次のいずれかを実行します。

- RADIUS を使用する場合は、「接続」（p. 358）の説明に従って設定を行い、[完了] をクリックします。
- Deepnet DualShield を使用する場合は、「DualShield 認証プラットフォームを使用するための Parallels RAS の構成」(p. 373)の説明に従って構成を実行します。DualShield 認証プラットフォームの構成については、「DualShield 5.6+ 認証プラットフォームの構成」（p. 369）を参照してください。
- SafeNet を使用する場合は、「SafeNet の構成」（p. 377）に従って構成を実行します。
- Google Authenticator を使用する場合は、「Google Authenticator の構成」（p. 366）に従って構成を実行します。
- Google Authenticator 以外の TOTP プロバイダーを使用する場合は、「TOTP の構成」（p. 365）に従って構成を実行します。

RADIUS の使用

次の図は、RAS Connection Broker が RADIUS サーバーに接続された状態での、境界ネットワークのダブルホップシナリオを示しています（RADIUS はイントラネット内にありますが、DMZ に配置可能です）。



RADIUS のプロパティを構成するには、次の手順を実行します。

1 Parallels RAS Console で、[接続] > [多要素認証] に移動します。

2 構成する MFA プロバイダーをダブルクリックします。

次に、RADIUS プロバイダーの設定を構成する方法について説明します。

接続

[接続] タブでは、以下のオプションを指定できます。

- 表示名: クライアント側のログオン画面に表示される OTP 接続タイプの名前を指定します。ユーザーにとって理解しやすい名前を指定する必要があります。
- プライマリサーバーおよびセカンダリサーバー: この 2 つのフィールドでは、構成に含める RADIUS サーバーを 1 台または 2 台指定できます。2 台のサーバーを指定すると、RADIUS ホストの高可用性を構成することができます（下記参照）。ホスト名または IP アドレスを入力してサーバーを指定するか、[...] ボタンをクリックして Active Directory 経由でサーバーを選択します。

- RADIUS サーバーが 2 台指定されている場合は、[HA モード] ドロップダウンリストから次の高可用性モードのいずれかを選択します。[アクティブ - アクティブ（パラレル）] は、コマンドが両方のサーバーに同時に送信され、最初に応答した方が使用されます。[アクティブ - パッシブ（フェイルオーバー）] は、フェイルオーバー動作を意味し、タイムアウトが 2 倍になり、Parallels RAS は両方のホストからの応答を待ちます。
- HA モード: 上記のプライマリサーバーおよびセカンダリサーバーを参照してください。プライマリサーバーのみを指定した場合、このフィールドは無効になります。
- ポート: RADIUS サーバーのポート番号を入力します。デフォルト値を使用するには、[デフォルト] ボタンをクリックします。
- タイムアウト: パケットタイムアウトを秒単位で指定します。
- 再試行: 接続の確立を試みる場合の再試行回数を指定します。
- 秘密鍵: 秘密鍵を入力します。
- パスワードのエンコード: RADIUS サーバーで指定した設定に従って [PAP]（パスワード認証プロトコル）または [CHAP]（チャレンジハンドシェイク認証プロトコル）から選択します。

[接続の確認] ボタンをクリックして、接続を検証します。接続が適切に構成されている場合、確認メッセージが表示されます。

必要に応じて追加のプロパティを指定します。

- RADIUS サーバーにユーザー名のみを送る: 必要に応じてこのオプションを選択します。
- 最初のパスワードを Windows 認証プロバイダーに転送する: このオプションを選択すると、パスワードを 2 回入力するプロンプトを回避できます（RADIUS と Windows AD）。Azure MFA サーバーでは、このオプションは常に有効にされていて、解除できないことに注意してください。
- 選択した RADIUS ソリューションに固有の特定の設定を提案している、ダイアログ（利用可能な場合）の一番下にある注記もお読みください。

属性

RADIUS ソリューションに構成属性が要求されている場合は、[属性] タブをクリックして [追加] をクリックします。開いたダイアログで、事前設定されている任意のベンダーと属性を選択します。

- [ベンダー] ドロップダウンリストでベンダーを選択します。

- [属性] リストでベンダー属性を選択します。
- [値] フィールドに、選択した属性タイプ（数値、文字列、IP アドレス、日付など）に応じた値を入力します。

特定のシナリオでは、このダイアログに表示されていないベンダーや属性を追加する必要があるかもしれません。ベンダーや属性を追加する方法については、以下のナレッジベースの記事を参照してください: https://kb.parallels.com/en/125576。

[OK] をクリックし、再度 [OK] をクリックしてすべてのダイアログを閉じます。

自動化

RADIUS [プロパティ] ダイアログの [自動化] タブでは、MFA ログインプロセス中に RADIUS サーバーに送信するセキュリティ検証方法とカスタムコマンドを構成して、Parallels Client ユーザーの OTP エクスペリエンスをカスタマイズできます。さまざまなセキュリティ検証方法に優先順位を割り当て、自動的に使用されるように構成できます。

この機能を構成すると、ユーザーは、プッシュ通知、電話のコールバック、SMS、メール、カスタムなど、事前に定義され構成可能なリストから好みのセキュリティ検証方法を選択することができます。これらの方法は、Parallels Client の OTP ダイアログにクリック可能なアイコンとして表示されます。ユーザーがアイコンをクリックすると、RADIUS サーバーにコマンドが送信され、対応する検証方法が使用されます。

検証方法（このダイアログや Parallels RAS Console では“アクション”とも呼ばれます）を構成するには、[自動化] タブで [タスク] ＞ [追加] をクリックします。この [アクションを追加] ダイアログで次のプロパティを指定します。

- アクションを有効化: アクションを有効または無効にします。
- タイトル: Parallels Client のクリック可能なアイコンに表示されるテキスト（例: “プッシュ”）。
- コマンド: Parallels Client でアクションアイコンがクリックされたときに使用する OTP コマンド。コマンドの仕様については、MFA プロバイダーにお問い合わせください。
- 説明: マウスポインターがアクションアイコンの上に移動されたときに、ユーザーの画面に吹き出しとして表示される説明。
- アクションメッセージ: 接続の進捗状況ボックスに表示されるメッセージ。
- 画像を選択: 提供されたギャラリーから画像を選択します。画像は Parallels Client の OTP ダイアログのアクションアイコンとして使用されます。

完了したら、[OK] をクリックして、アクションを保存します。他のアクションについても、上記の手順を繰り返します。

注: 最大 5 つのアクションを作成することができます。5 つすべてが作成されると、[タスク] > [追加] メニューは無効になります。

[自動化] タブのアクションは、リストの中で上または下に移動できます。この操作により、Parallels Client にアクションアイコンが表示される順序が決まります。

自動送信

アクションのために構成できるオプションがもう 1 つあります。それは [自動送信] と呼ばれているものです。このオプションは 1 つのアクションに対してのみ有効にでき、デフォルトのアクションとなって、ユーザーの操作なしで自動的に使用されます。

[自動送信] オプションを有効にするには、[自動化] タブでアクションを選択し、[タスク] > [自動送信] をクリックします。このオプションを無効にするには、同じメニューをもう一度クリックします。あるアクションで [自動送信] を有効にすると、以前のアクションでは自動的に無効になります。

以下の 2 つの方法により、Parallels Client でアクションを自動的に実行させることができます。

- クライアントが初めてアクションアイコンの構成を受信するとき、そのうちの 1 つのアクションの [自動送信] を有効にします。
- [ポリシー] > [セッション] > [接続] > [多要素認証] で [前回使用した手法を記憶] オプションを有効にします。このオプションを有効にし、Parallels Client がポリシーを受信すると、ユーザーが最後に使用したメソッドがデフォルトの自動メソッドになります。

Parallels Client

ユーザーが MFA を介して Parallels RAS にログインすると、Parallels Client に OTP ダイアログが表示され、アクションアイコンが OTP フィールドの上に配置されます。ユーザーがアイコンをクリックすると、事前に定義されたアクションに従って認証が行われます。たとえば、ユーザーが“プッシュ”アイコンをクリックすると、プッシュ通知がユーザーのモバイルデバイスに送信され、“承認”をタップするだけで認証が行われます。または、“メール送信”アイコンがある場合は、テキストがワンタイムパスワード付きでユーザーの携帯電話に送信されます。アクションの 1 つが [自動送信] オプションを有効にしている場合、そのアクションが自動的に使用されます。

ユーザーが常に同じ認証方法を使用している場合は、それをデフォルトの認証方法にすることができます。そのためには、ユーザーは、接続プロパティの [多要素認証] セクションで [前回使用した手法を記憶] オプションを有効にします。各プラットフォームで、このオプションは以下の場所にあります。

- Parallels Client for Windows/Linux: [接続の詳細設定] > [多要素認証]
- Parallels Client for Mac: [詳細] > [多要素認証]
- Parallels Client for Chrome: 詳細設定
- Web Client: 設定
- Parallels Client for iOS: [接続設定] > [多要素認証]
- Parallels Client for Android: [設定] > [多要素認証]

前述したように、[前回使用した手法を記憶] は、RAS Console のクライアントポリシーでも構成できます。このオプションは、デフォルトで有効になっています。

詳細設定

[詳細] タブでは、RADIUS サーバーが送信するエラーメッセージのうち、Parallels Client で表示されないものを指定できます。これは、エラーメッセージがユーザーを混乱させたり、ユーザーエクスペリエンスを阻害したりする場合に有効です。

デフォルトでは、無視するメッセージのリストに「New SMS passcodes sent.」が追加されています（DUO Radius 向け）。これは、SMS による認証をよりシンプルにするために設定されています。このメッセージを無視対象のリストから削除することはお勧めしません。

無視するメッセージのリストに新しいメッセージを追加するには、次の操作を実行します。

1. [詳細] タブで、[タスク] > [追加] をクリックします（または [+] アイコンをクリックします）。
2. 無視させたいエラーメッセージの正確なテキストを入力します。メッセージの大文字と小文字は区別されません。なお、RADIUS サーバーから送信されるテキストのみを指定する必要があります。たとえば、Parallels Client で”Code [01/00000003] Logon using RADIUS failed.エラー: New SMS passcodes sent.”というエラーが発生した場合、「New SMS passcodes sent.」を追加する必要があります。

Azure MFA の構成

このセクションをお読みになる前に、以下の重要なお知らせをご確認ください。

注: 2019 年 7 月 1 日より、Microsoft は新規の展開用の MFA サーバーの提供を取りやめます。ユーザーの多要素認証を必要とする新しいお客様は、クラウドベースの Azure Multi-factor Authentication を使用する必要があります。7 月 1 日より前に MFA サーバーをアクティベートした既存のお客様は、これまでどおり最新バージョンのプログラムや今後のアップデートをダウンロードしたり、ライセンス認証の資格情報を生成したりできます。
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfaserver-deploy。

新規の展開用には、RAS で、Azure の NPS 拡張機能（https://docs.microsoft.com/ja-jp/azure/active-directory/authentication/howto-mfa-nps-extension）や、Azure MFA サービスを SAML 構成とともに使用されることをお勧めします。

Azure MFA の構成

ユーザーロケーションに応じて、クラウド MFA サービスには 4 つのシナリオがあります。

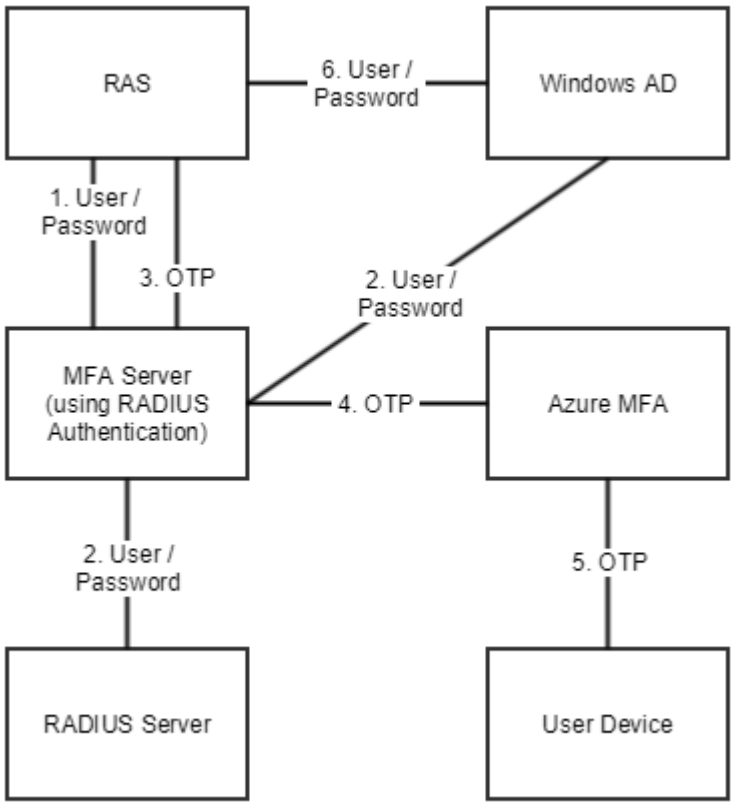
ユーザーロケーション	クラウド内の MFA	MFA サーバー
Microsoft Entra ID	はい	
Microsoft Entra ID と AD FS とのフェデレーションを使用するオンプレミス AD（SSO に必須）	はい	はい
Microsoft Entra ID と DirSync を使用するオンプレミス AD、Azure AD Sync、Azure AD Connect - パスワードなしの同期	はい	はい
Microsoft Entra ID と DirSync を使用するオンプレミス AD、Azure AD Sync、Azure AD Connect - パスワードありの同期	はい	
オンプレミス Active Directory		はい

MFA サーバーをダウンロードしてアクティベートするには、グローバル管理者の役割のある Azure アカウントが必要です。オンプレミスでのみ動作する MFA サーバーを設定するために、Microsoft Entra ID との同期（AD Connect 経由）またはカスタム DNS ドメインは必要ありません。

ユーザーを MFA サーバーにインポートし、MFA 認証が得られるように構成する必要があります。

Parallels RAS は、RADIUS 二要素認証プロバイダーを使用して、MFA サーバーでユーザーを認証します。このため、RAS サーバーからの RADIUS クライアント接続を許可するように MFA サーバーを構成する必要があります。

認証プロセスは、以下のステージを通過します。



ステージ 2 では、RADIUS または Windows AD を使用して、ユーザーを認証できます。パスワードを転送するオプションを有効にすることにより、資格情報を 2 回（ステージ 1 と 6）入力するように求めるプロンプトを回避できます。

Duo の構成

Duo RADIUS で Parallels RAS を構成する方法については、次の Parallels KB 記事を参照してください。https://kb.parallels.com/124429。

TOTP の使用

ここでは、TOTP MFA プロバイダーを Parallels RAS に統合する方法について説明します。

TOTP の構成

TOTP 設定を構成するには、以下の手順を実行します。

1 次の要素を指定します。

- 表示名: この場合のデフォルト名は TOTP です。その名前は、Parallels Client の登録ダイアログの”TOTP アプリを iOS または Android のデバイスにインストールしてください”という部分に表示されます。名前を変更すると、指定した名前が使用され、”<new-name> アプリを iOS または Android のデバイスにインストールしてください”と表示されます。
- ユーザーの登録セクションでは、必要に応じてユーザー登録を制限できます。すべてのユーザーが制限なしで登録できるようにしたり（ [許可] オプション）、指定した日時までに限り登録できるようにしたり（[次の日時まで許可]）、登録を完全に無効にしたり（[許可しない] オプション）できます。有効期限が切れていたり、[許可しない] オプションが選択されていたりして、登録が無効になっている場合にユーザーがログインを試みると、登録が無効化されていることを示すエラーメッセージが表示され、システム管理者に問い合わせるよう促されます。登録を制限したり無効にしたりしても、Google 認証機能や他の TOTP プロバイダーを使用することができますが、それ以上のユーザーの登録を許可しないようなセキュリティが追加されています。これは、危殆化した認証情報を持つユーザーが MFA に登録する可能性を軽減するためのセキュリティ対策です。
- [認証] セクションでは、TOTP の許容範囲を構成することができます。時間ベースのワンタイムパスワード（TOTP）を使用する場合、RAS Connection Broker とクライアントデバイス間で時間を同期させる必要があります。同期は、グローバル NTP サーバー（time.google.com など）に対して実行される必要があります。[TOTP 許容範囲] ドロップダウンリストを使用して、認証の実行中に許容すべき時間差を選択できます。ドロップダウンリストを展開し、事前に定義された値（秒数）のいずれかを選択します。時間差の許容範囲の変更は、セキュリティトークンの有効時間の拡大を意味し、不正に利用できる時間枠が広くなりセキュリティ上の影響があるため、注意して行う必要があります。

> **注:** TOTP プロバイダーを使用する場合、Connection Broker とクライアントデバイスの両方の時間をグローバル NTP サーバー（time.google.com など）と同期させる必要があります。TOTP の許容範囲を追加すると、ワンタイムパスワードの有効性が拡大し、セキュリティに影響を及ぼす可能性があります。

- [ユーザー管理] セクションの [ユーザーをリセット] フィールドでは、ユーザーが TOTP プロバイダーを使用して Parallels RAS に初めてログインしたときに受け取ったトークンをリセットできます。ユーザーをリセットすると、ユーザーは登録手続きを再び実行しなければならなくなります（Google Authenticator でこれを実行する方法については、「Parallels Client での Google 認証の使用」（p. 366）を参照）。特定のユーザーを検索することも、すべてのユーザーをリセットすることも、ユーザーのリストを CSV ファイルからインポートすることも可能です。

2 [完了] をクリックします。

また、TOTP 有効時間は、デフォルトの 30 秒 + 過去の x 秒 + 未来の x 秒として計算されることに注意してください。

Google Authenticator を構成する

Google Authenticator を構成するを構成するには、以下の手順を実行します。

1 次の要素を指定します。

- 表示名: この場合のデフォルト名は Google Authenticator です。その名前は、Parallels Client の登録ダイアログの”Google Authenticator アプリを iOS または Android のデバイスにインストールしてください”という部分に表示されます。名前を変更すると、指定した名前が使用され、”<new-name> アプリを iOS または Android のデバイスにインストールしてください”と表示されます。技術面からすると、どの認証アプリでも使用できますが（つまり、名前を変更することも可能ですが）、この資料の執筆時点では Google Authenticator アプリだけが正式にサポートされています。
- ユーザーの登録セクションでは、必要に応じて Google 認証経由のユーザー登録を制限できます。すべてのユーザーが制限なしで登録できるようにしたり（ [許可] オプション）、指定した日時までに限り登録できるようにしたり（[次の日時まで許可]）、登録を完全に無効にしたり（[許可しない] オプション）できます。有効期限が切れていたり、[許可しない] オプションが選択されていたりして、登録が無効になっている場合にユーザーがログインを試みると、登録が無効化されていることを示すエラーメッセージが表示され、システム管理者に問い合わせるよう促されます。登録を制限したり無効にしたりしても、Google 認証機能や他の TOTP プロバイダーを使用することができますが、それ以上のユーザーの登録を許可しないようなセキュリティが追加されています。これは、危殆化した認証情報を持つユーザーが MFA に登録する可能性を軽減するためのセキュリティ対策です。
- [認証] セクションでは、TOTP の許容範囲を構成することができます。時間ベースのワンタイムパスワード（TOTP）を使用する場合、RAS Connection Broker とクライアント

デバイス間で時間を同期させる必要があります。同期は、グローバル NTP サーバー（time.google.com など）に対して実行される必要があります。[TOTP 許容範囲] ドロップダウンリストを使用して、認証の実行中に許容すべき時間差を選択できます。ドロップダウンリストを展開し、事前に定義された値（秒数）のいずれかを選択します。時間差の許容範囲の変更は、セキュリティトークンの有効時間の拡大を意味し、不正に利用できる時間枠が広くなりセキュリティ上の影響があるため、注意して行う必要があります。

> 注: 時間ベースのワンタイムパスワード（TOTP）プロバイダーを使用する場合、Connection Broker とクライアントデバイスの両方の時間をグローバル NTP サーバー（time.google.com など）と同期させる必要があります。TOTP の許容範囲を追加すると、ワンタイムパスワードの有効性が拡大し、セキュリティに影響を及ぼす可能性があります。

- [ユーザー管理] セクションの [ユーザーをリセット] フィールドでは、ユーザーが Google 認証を使用して Parallels RAS に初めてログインしたときに受け取ったトークンをリセットできます。ユーザーをリセットすると、ユーザーは登録手続きを再び実行しなければならなくなります（詳細については、下記の「Parallels Client での Google 認証の使用」を参照）。特定のユーザーを検索することも、すべてのユーザーをリセットすることも、ユーザーのリストを CSV ファイルからインポートすることも可能です。

2 [完了] をクリックします。

また、TOTP 有効時間は、デフォルトの 30 秒 + 過去の x 秒 + 未来の x 秒として計算されることに注意してください。

Parallels Client での Google 認証の使用

> **重要:** Google Authenticator やその他の TOTP プロバイダーを使用するには、ユーザーのデバイスと RAS Connection Broker サーバーの間で時間を同期する必要があります。そうしないと、Google 認証は失敗します。

Google Authenticator は、サポートされているいずれのプラットフォームで実行している Parallels Client でも利用できます（モバイル、デスクトップ、ウェブの各クライアントでサポートされています）。

Google 認証を使用するには、ユーザーが認証アプリを自分の iOS デバイスまたは Android デバイスにインストールしなければなりません。Google Play または App Store にアクセスして、アプリをインストールしてください。認証アプリをインストールしたら、二要素認証を使用して Parallels RAS に接続する準備が整ったことになります。

Parallels RAS に接続するには、以下の手順を実行します。

1 Parallels Client または Web Client を開き、自分の資格情報を使用してログインします。

2 多要素認証ダイアログが開き、バーコード（QR コード）と秘密鍵が表示されます。

3 モバイルデバイスで Google 認証アプリを開きます。

- 初めて使用する場合は、[開始] をタップし、[バーコードをスキャンする] をタップします。
- Google 認証の別のアカウントを持っている場合は、プラス記号のアイコンをタップし、[バーコードをスキャンする] を選択します。

4 Parallels Client のログインダイアログに表示されているバーコードをスキャンします。

何かの理由でうまくスキャンできない場合は、アプリに戻り、[秘密鍵を入力する] を選択し、アカウント名と Parallels Client のログインダイアログに表示されている秘密鍵を入力します。

5 アプリで [アカウントを追加する] をタップすると、アカウントが作成され、ワンタイムパスワードが表示されます。

6 Parallels Client に戻り、[次へ] をクリックし、[OTP] フィールドにワンタイムパスワードを入力します。

その後のログインでは、資格情報（[パスワードの保存] オプションが選択されている場合は不要）と、Google 認証アプリで取得したワンタイムパスワードを入力するだけで十分です（アプリによって新しいパスワードが生成されます）。RAS 管理者がユーザーをリセットすると（このセクションの最初にある [ユーザーをリセット] フィールドの説明を参照）、ユーザーが上記の登録手順を繰り返さなければならなくなります。

Microsoft Authenticator を構成する

「TOTP を構成する」（p. 365）を参照してください。

Deepnet DualShield の使用

このセクションでは、Deepnet DualShield 認証プラットフォーム 5.6 以降を Parallels RAS と統合する方法を説明します。

このセクションでは、以下の内容を説明します。

- DualShield 認証プラットフォームを使用するための Parallels RAS の構成（p. 373）
- RAS ファームへの接続（p. 376）

DualShield 認証プラットフォームについては、次のドキュメントも参照してください。

- DualShield 認証プラットフォーム - インストールガイド
- DualShield 認証プラットフォーム - クイックスタートガイド
- DualShield 認証プラットフォーム - 管理ガイド

サポートされているトークン

以下は Parallels RAS がサポートするトークンの一覧です。

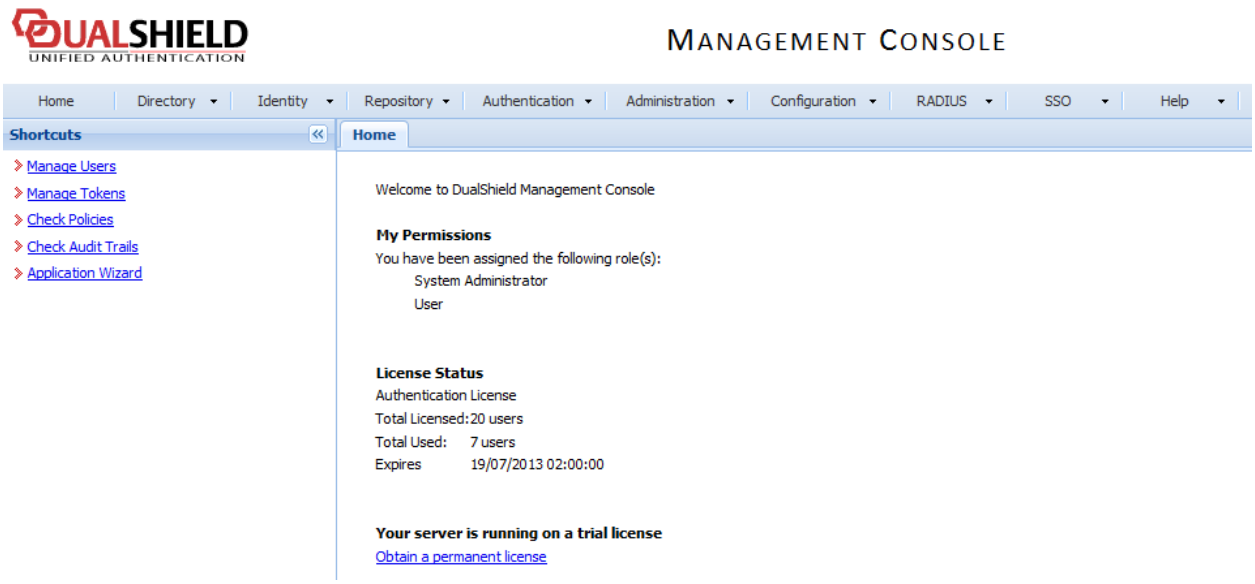
- MobileID（FlashID は MobileID と統合されません）
- QuickID
- GridID
- SafeID
- SecureID（RSA）
- DigiPass（Vasco）

SafeID などのハードウェアトークンを使用する場合は、提供された XML ファイルを使用して、最初にトークン情報をインポートする必要があります。[インポート] をクリックして、提供された XML ファイルを参照します。XML ファイルがインポートされたら、各ハードウェアトークンをユーザーに割り当てる必要があります。

DualShield 5.6+ 認証プラットフォームの構成

「DualShield 認証プラットフォーム - インストールガイド」で指定されているすべての手順に従うと、インターネットブラウザー（http://LOCALHOST:8073）で自動的に URP が開き、DualShield の管理コンソールにログインできます。

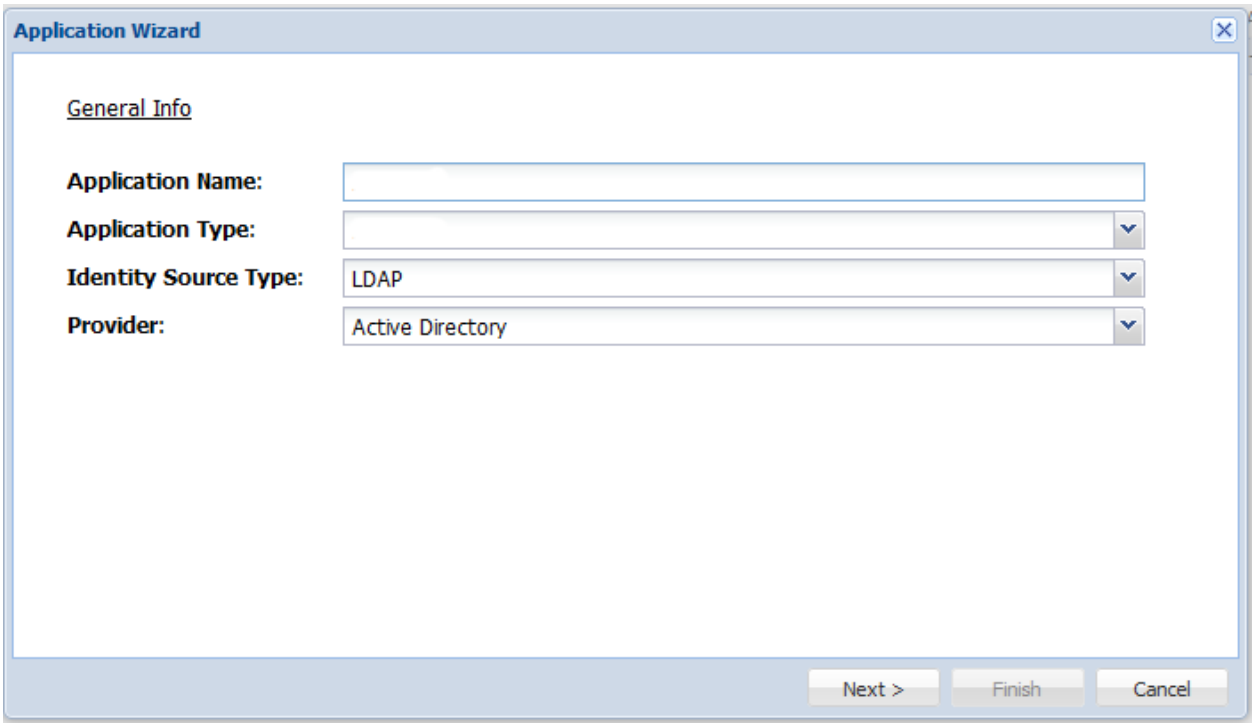
デフォルトの資格情報（ユーザー: sa、パスワード: sa）を使用して、DualShield の管理コンソールにログインします。デフォルトのパスワードを変更するように要求されます。



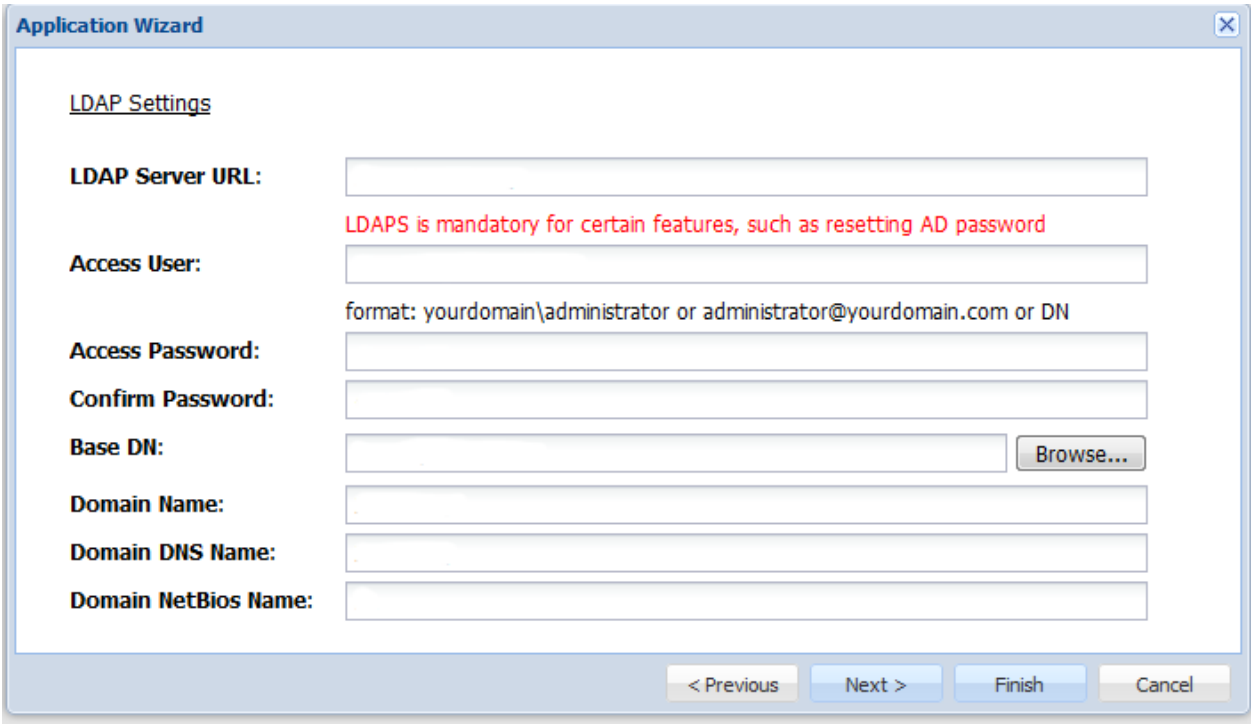
アプリケーションへのアクセスが許可されるユーザーのドメインがレルムに含まれているため、アプリケーションはレルムへの接続を提供するように設定されます。

レルムは、複数のドメインユーザーが同じアプリケーションにアクセスできるように設定されます。

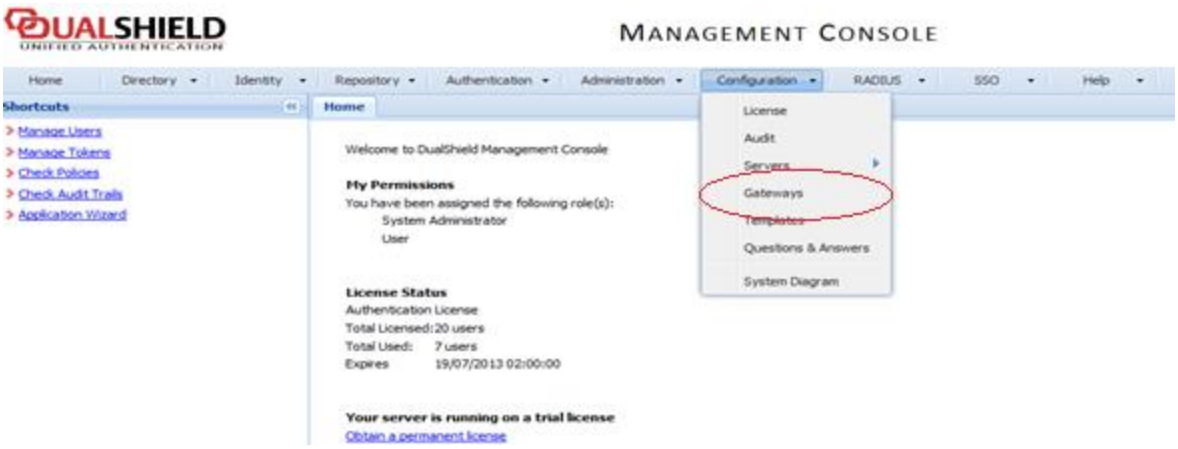
Parallels RAS が通信するアプリケーションを作成する必要があります。[確認証明] > [アプリケーションウィザード] をクリックして、以下に表示される情報を入力し、[次へ] を押します。



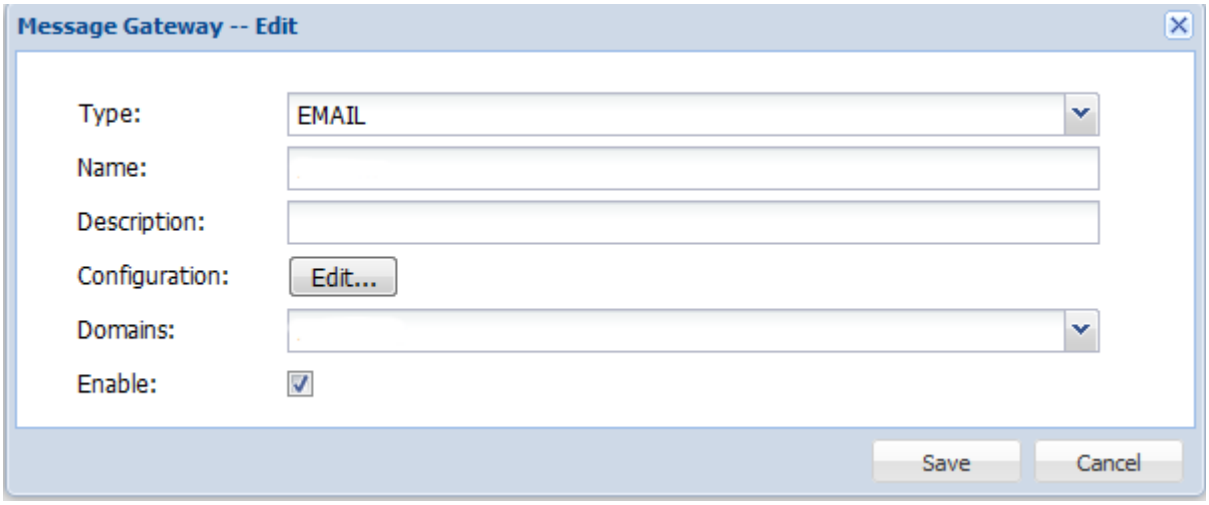
以下に表示される LDAP サーバーの設定を指定して、[完了] を押します。



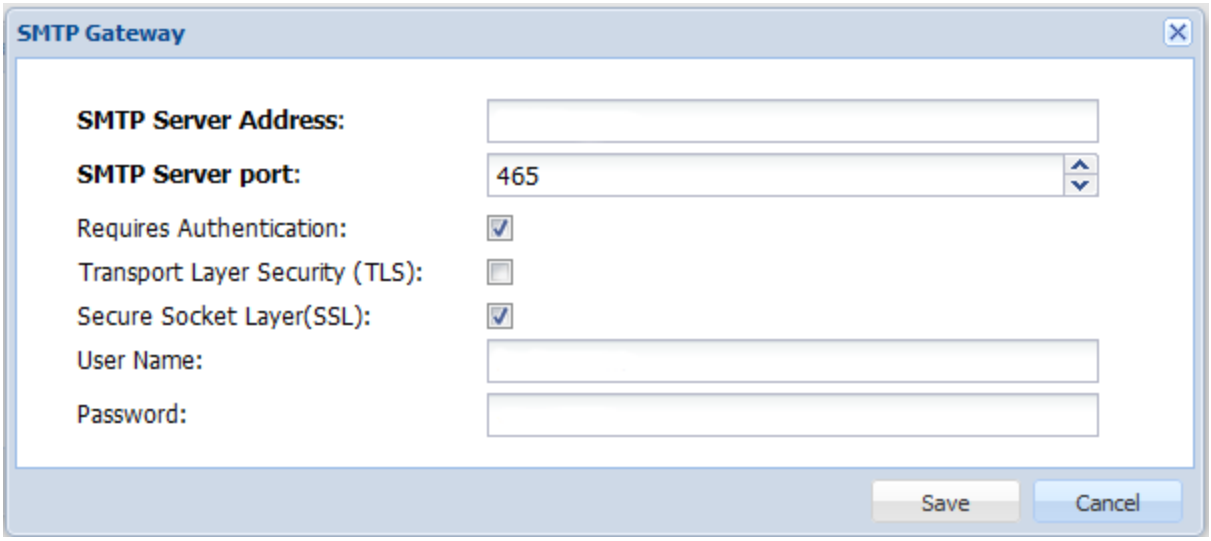
アプリケーションの構成後に、DualShield サーバーとエンドユーザーが通信するために使用する電子メールゲートウェイまたは SMS ゲートウェイを構成する必要があります。このドキュメントでは、電子メールゲートウェイを使用します。[構成] メニューの [ゲートウェイ] を選択します。



電子メールゲートウェイを構成します。



[編集] をクリックして、SMTP サーバー情報を入力します。



DualShield 認証プラットフォームを使用するために Parallels RAS を構成する

Deepnet DualShield の構成を実行するには、次の操作を実行します。

1 次の要素を指定します。

- サーバー: Deepnet サーバーのホスト名です。

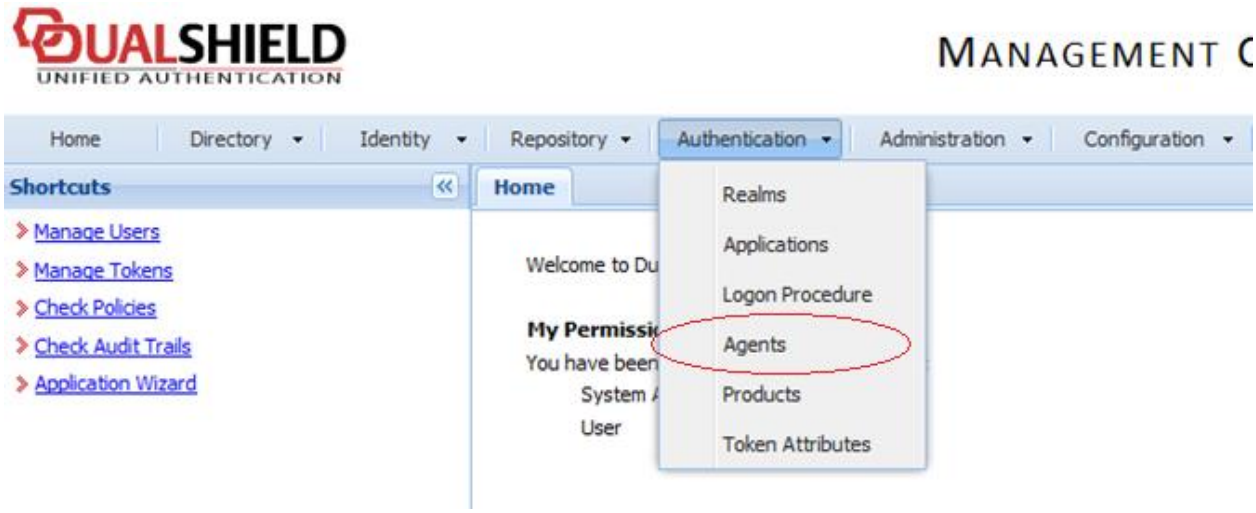
- SSL を有効にする: Deepnet サーバーへの接続時に SSL を使用するかどうかを指定します。
- ポート: Deepnet サーバーへの接続に使用されるポートです。
- Agent: 登録時に使用される Agent の名前です。

2 [接続の確認] ボタンをクリックし、認証サーバーにアクセスできることをテストして、RAS Console が DualShield Agent として登録されていることを確認します。”DeepNet サーバーが有効ではありません”というメッセージが表示された場合、以下のような原因が考えられます。

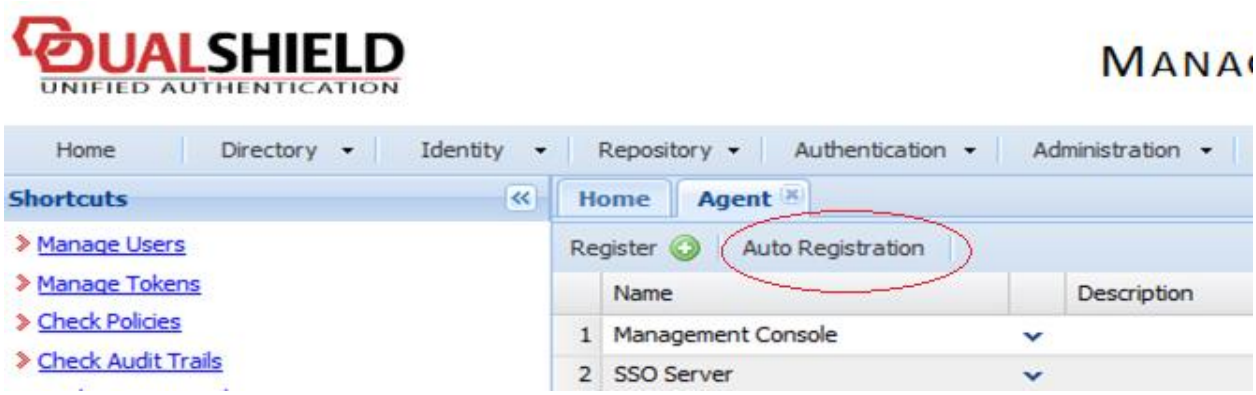
- 指定したサーバーの情報が正しくない。
- DualShield エージェントとして Parallels コンポーネントの自動登録を許可する必要がある。

3 DualShield エージェントとして Parallels コンポーネントの自動登録を許可する必要がある場合は、次の操作を実行します。

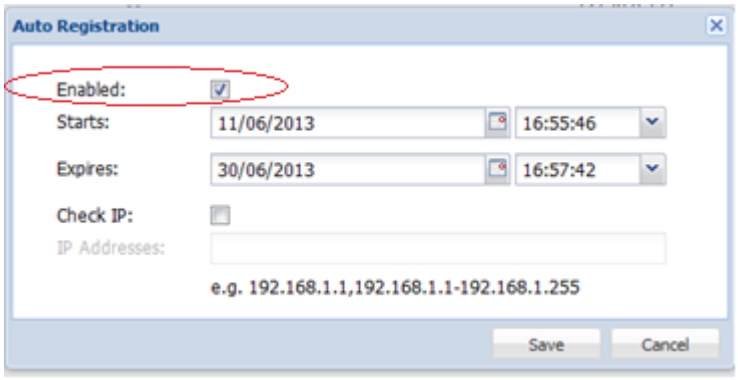
1. DualShield 管理コンソールに戻り、次のように [確認証明] メニューから [Agent] を選択します。



2. [自動登録] を選択します。



3. [使用可能] オプションを選択し、日付範囲を設定します。



4. Agent の自動登録を設定したら、RAS Console に戻って [はい] を選択します。Dual Shield Agent が正常に登録されたことを示すメッセージが表示されます。

   すべての RAS Connection Broker を Deepnet DualShield サーバーに登録する必要があります。セカンダリ Connection Broker を使用している場合は、開いているすべてのウィンドウを閉じる必要があります。すべてのウィンドウを閉じると、RAS Console で [適用] を押せるようになります。これにより、すべての Agent に、DualShield Agent として自己登録するよう通知されます。

4 RAS Console に戻り、[次へ] をクリックします。

5 次の要素を指定します。

- アプリケーション: 「DualShield 5.6+ 認証プラットフォームの構成」（p. 369）で作成したアプリケーションの名前です。

- 既定のドメイン: ユーザー、テーマのプロパティ、または接続設定でドメインが指定されていない場合に使用されるドメインです。

6 [モード] ドロップダウンリストで、ユーザーをどのような方法で認証するかを選択します。

- [すべてのユーザーに必須です] を選択すると、システムを使用するすべてのユーザーが二要素認証を使用してログインする必要があります。
- [ドメイン認証されたユーザーのトークンを作成] を選択すると、ドメイン認証されたユーザーのソフトウェアトークンを Parallels RAS が自動的に作成することができます。ドロップダウンリストからトークンのタイプを選択します。このオプションは、QuickID や MobileID などのソフトウェアトークンでのみ機能します。
- [DualShield が付いているアカウントのみ利用できます] を選択すると、DualShield アカウントを持たないユーザーは二要素認証を使用してログインしなくてもシステムを使用できます。

7 [チャンネルの許可] セクションで、ユーザーへのワンタイムパスワード送信に使用するチャンネルを選択します。

8 [完了] をクリックします。

RAS ファームへの接続

Parallels Client

DualShield を有効にすると、ユーザーに二要素認証が適用されます。QuickID などのソフトウェアトークンを使用すると、管理者はユーザーごとにトークンを作成する必要はありません。ユーザーが最初にログインを試みたときに、RAS Connection Broker がトークンを自動で作成します。

ユーザーが Parallels Client から RAS 接続へのアクセスを試みると、まず Windows ユーザー名とパスワードの入力を求められます。資格情報が受け付けられると、RAS Connection Broker は DualShield サーバーと通信を行い、そのユーザーに固有のトークンを作成します。

MobileID または QuickID を使用する場合は、該当のソフトウェアをどこでダウンロードできるかに関するメールがユーザーに送信されます。

QuickID トークンを使用する場合、アプリケーションは、メールまたは SMS で送信された一時パスワードを要求します。

OTP を求められた場合は、ワンタイムパスワードを入力して Parallels Application Server XG ゲートウェイにログインします。

SafeNet の使用

SafeNet トークン管理システムは、セキュアトークンを使用して高価値の保護を提供します。これにより、SafeNet トークン管理システム製品は、Parallels RAS での二要素認証用の完璧なツールとして機能します。

このセクションでは、以下の内容を説明します。

SafeNet の構成

SafeNet 設定を構成するには、以下の手順を実行します。

1 [接続] セクションで、[OTP 用 URL] フィールドに有効な URL を入力します。OTP サービスとの接続を確立できることを確認するには、[接続の確認] ボタンをクリックします。

> **注:** RAS Connection Broker は SafeNet トークン管理システムサーバーと通信します。セキュリティ上の理由から、認証サーバーをファイアウォールの内側に配置することを強くお勧めします。

2 [確認証明] タブをクリックします。

3 [モード] ドロップダウンリストで、ユーザーをどのような方法で認証するかを選択します。

次のモードを利用できます。

- [すべてのユーザーに必須です:] を選択すると、システムを使用するすべてのユーザーが二要素認証を使用してログインする必要があります。
- ドメイン認証されたユーザーのトークンを作成: ドメイン認証されたユーザーのソフトウェアトークンを Parallels RAS で自動作成することができます。ドロップダウンリストからトークンのタイプを選択します。このオプションは、ソフトウェアトークンでのみ機能します。
- Safenet が付いているアカウントのみ利用できます: SafeNet アカウントを持たないユーザーは二要素認証を使用してログインしなくてもシステムを使用できます。

1 [TMS Web API URL] フィールドに SafeNet API URL の場所を入力します。

2 [ユーザーリポジトリ] フィールドにユーザーリポジトリの宛先を入力します。

3 [完了] をクリックします。

Parallels Client

Parallels Client の [新しいアカウント情報] ダイアログで、次の手順を実行します。

1 [OTP PIN] 数字フィールドに任意の 4 桁の数字を入力します（これらの数字はプロセスの後で必要になります）。

2 メールアドレスを入力し、[OK] をクリックします。

3 メールアカウントにログインして、SafeNet 認証をアクティベートするために必要な情報が記載されている電子メールを取得します。この電子メールの例を以下に示します。

アクティベーションキー: YZQHoczZWw3cBCNo

トークンシリアル番号: 4F214C507612A26A

MobilePASS クライアントを http://localhost:80/TMSService/ClientDownload/MobilePASSWin.exe からダウンロードします。

** ドメイン資格情報でログインします。*

**MobilePASS クライアントと同じフォルダーに添付のシードファイルを保存してください。*

ワンタイムパスワードを入力して、RD セッションホスト接続にログインします。

アプリケーション PIN: 4089

4 電子メールに記載されている URL から MobilePASS クライアントをダウンロードします。

5 SafeNet の電子メールに記載されているアクティベーションキーを入力します。

6 次に、電子メールに記載されているアプリケーション PIN を [MobilePASS PIN] フィールドに入力します。

7 [このゲスト OS の] をクリックして eToken 番号を生成し、[コピー] をクリックします。

8 OTP PIN と eToken を次の順番で組み合わせます。OTP + eToken

9 この値を Parallels Client に入力し、[OK] をクリックしてログインします。

多要素認証（多要素認証）ルールの構成

多要素認証（MFA）は、すべてのユーザー接続に対して有効または無効にできますが、特定の接続に対してはより複雑なルールを構成できますこの機能を使用すると、同じユーザーでも、ど

の場所およびどのデバイスから接続しているかに応じて MFA を有効にしたり無効にしたりできます。各 MFA プロバイダーには、ユーザー接続に対するマッチングに使用される 1 つまたは複数の条件で構成されるルールがあります。各条件は、マッチング可能な 1 つまたは複数の特定のオブジェクトで構成されています。

次のオブジェクトのマッチングを実行できます。

- ユーザー、ユーザーが所属するグループ、またはユーザーが接続するコンピューター。
- ユーザーが接続する Secure Gateway。
- クライアントデバイスの名前。
- クライアントデバイスのオペレーティングシステム。
- IP アドレス。
- ハードウェア ID。ハードウェア ID の形式は、クライアントのオペレーティングシステムに依存します。

ルールについて、次のことに注意してください。

- 条件とオブジェクトは OR 演算子で接続されます。たとえばあるルールに、特定の IP アドレスに一致という条件とクライアントデバイスのオペレーティングシステムに一致という条件が含まれる場合、ユーザーの接続が IP アドレスの条件またはクライアントオペレーティングシステムの条件のいずれかに一致する場合に、ルールが適用されます。

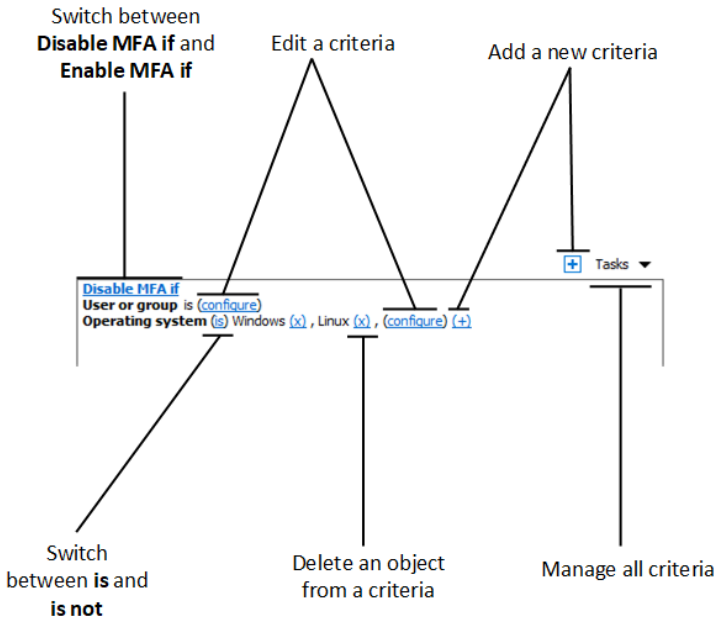
ルールを構成するには、次の操作を実行します。

1 RAS Console で、[接続] > [多要素認証] タブを選択します。

2 ルールを作成したいプロバイダーをダブルクリックします。

3 [制限] タブを選択します。

4 ルールの条件を指定します。以下のコントロールを利用できます。



- Enable MFA if および Disable MFA if: ユーザー接続がすべての条件に一致する場合に、MFA プロバイダーを有効化するかどうかを指定します。これらのオプションは、クリックすると切り替わります。
- （+）：新しい条件を追加します。一致条件として、Secure Gateway、クライアントデバイス名、クライアントデバイスのオペレーティングシステム、IP アドレス、ハードウェア ID のいずれかを使用したい場合は、（+）をクリックします。　表示されるコンテキストメニューで、マッチングさせたいオブジェクトの種類を選択し、表示されるダイアログで特定のオブジェクトを追加します。新しい条件が次の行に表示されます。
- （X）：マッチングから特定のオブジェクトを削除します。たとえば、IP アドレス 198.51.100.1 をマッチングから削除したい場合は、その横にある（X）をクリックします。このコントロールは、少なくとも 1 件のオブジェクトが追加されたときに表示されます。条件内のすべてのオブジェクトが削除された場合、その条件は削除されます。
- is および is not: ユーザー接続が条件に一致した場合に、MFA プロバイダーを有効化するかどうかを指定します。これらのオプションは、クリックすると切り替わります。このコントロールは、少なくとも 1 件のオブジェクトが追加されたときに表示されます。
- configure: マッチさせるオブジェクトのリストを編集します。このリンクをクリックして新しいオブジェクトを追加または削除します。最初の条件（ユーザーまたはグループ）

の場合、このリンクは everyone と呼ばれることに注意してください。この条件のオブジェクトを指定すると、構成が変更されます。

ドメインパスワードの変更許可

ユーザーは Parallels Client から直接ドメインパスワードを変更できます。ユーザーは、ドメインパスワードの変更を強制される場合があります（パスワードの有効期限が迫っている場合など）。パスワードを変更する際には、ユーザー名を UPN 形式（例: user@domain.com）で指定する必要があります。

Parallels Client にドメイン名を渡す

ユーザーは自分のドメイン名を知らない場合があります。Parallels RAS では、ドメイン名をクライアント側に自動的に渡すように構成することで、ユーザーがドメイン名を入力する必要がなくなります。

ドメイン名は、RAS Console の以下の場所で指定することができます。

- 1 つは、[接続] > [認証] タブです。同タブページについては、このセクションですでに説明しました（p. 348）。クライアント側にドメイン名を強制的に指定するには、[特定] オプションを選択してドメイン名を指定します。
- もう 1 つは、[テーマのプロパティ] ダイアログです。テーマについては、このガイドの「テーマの構成」（p. 455）のセクションで後述します。テーマにドメイン名を指定すると、[認証] タブページ（上記参照）で指定したドメイン名よりも優先されます。テーマのドメイン名を指定するには、テーマのプロパティダイアログを開き、[一般] カテゴリーを選択し、[認証ドメインを上書き] オプションを選択し、ドメイン名を指定します。

Parallels Client が Parallels RAS に接続すると、上記で指定したドメイン名が Parallels Client に引き渡されます。ユーザーが Parallels Client でダイアログを開いてドメインパスワードを変更すると、ドメイン名は自動的にユーザー名に追加され、ユーザー名フィールドはグレーアウトされます。これにより、ユーザーはドメイン名を指定する必要がなくなります。

カスタムリンクを使用してドメインのパスワードを変更する

ユーザーが Azure Active Directory ドメインサービスまたはサードパーティの IdP を使用して Parallels RAS に接続する場合は、カスタムリンクを使用してドメインパスワードを変更するように構成する必要があります。リンク先は、サービスのパスワードを変更できるページにする必要があります。

ドメインパスワードを変更するためのカスタムリンクを指定するには、次の手順を実行します。

1 [接続] > [認証] > [ドメインのパスワードを変更] を開きます。

2 [”ドメインパスワードを変更”オプションにカスタムリンクを使用する] を選択します。

3 下のテキストフィールドに、ドメインを変更するためのカスタムリンクを指定します。

ユーザーがメールアドレスで RAS 接続を検出できるようにする

ユーザーのメールアドレスによる RAS ファームへのログインを可能にします。これにより、ユーザーはサーバーのアドレスやホスト名を知らなくても、ファーム上で公開されているアプリケーションやデスクトップにアクセスできるようになります。すべてのネイティブ Parallels Client で、メールアドレス入力による Parallels RAS ファームの検索がサポートされるようになりました。

ユーザーが自分のメールアドレスを使用してファームに接続するには、まず、利用中の DNS サーバー上でユーザーが使用するドメインの前方参照ゾーンに新しい TXT レコードを作成する必要があります。具体的な方法は、DNS サーバーの構成によって異なります。

TXT レコードの構文は以下の通りです。

ホスト: `_prlsclient`

Text: `hostname:port/theme;connmode=X;authmode=X`

テキストフィールドには、以下のパラメーターが用意されています。

- `hostname`: Secure Gateway が存在するサーバーのホスト名です。このパラメーターは必須項目です。
- `port`: Secure Gateway が受信接続を待機しているポートです。このパラメーターはオプションです。
- `theme`: します。このパラメーターはオプションです。
- `connmode`: 接続モードです。このパラメーターはオプションです。指定できる値は、`0`、`1`、`2`、`3` で以下の意味を持ちます。

  - 0: ゲートウェイモード
  - 1: ダイレクトモード
  - 2: ゲートウェイ SSL
  - 3: ダイレクト SSL
- authmode: 認証タイプです。このパラメーターはオプションです。指定できる値は、0、1、2、3 で以下の意味を持ちます。
  - 0: 認証情報
  - 1: SSO
  - 2: スマートカード
  - 3: SAML

入力する文字列の例:

```
hostname

hostname:port

hostname:port/theme

hostname;connmode=2;authmode=1
```

DNS レコードの設定後、ユーザーは自分のメールアドレスを使ってログインできるようになります。特定のクライアントでこれを行う方法については、「Parallels Client ガイド」を参照してください。

第　16　章

ロードバランスと HALB

この章では、Parallels RAS で使用できるロードバランスのオプションについて説明します。

この章の内容

リソースベースのロードバランスおよびラウンドロビンのロードバランス

Parallels RAS のロードバランサーは、Parallels Clients からの RD セッションホスト接続を適切に負荷分散することを目的として設計されています。

次の種類のロードバランスを利用できます。

- リソースベース: 各サーバーのビジー状態に応じて、セッションが各サーバーに分配されます。新しい受信セッションは、ビジー状態の程度が最も低いサーバーに常にリダイレクトされます。
- ラウンドロビン: セッションが順番にリダイレクトされます。たとえば、ファームに 2 つの RD セッションホストがあるとします。最初のセッションはサーバー 1 にリダイレクトされ、2 番目のセッションはサーバー 2 にリダイレクトされ、3 番目のセッションは再度サーバー 1 にリダイレクトされます。

次のサブセクションでも、この 2 つの方法について説明します。ロードバランスのオプションは、RAS Console の [ロードバランス] カテゴリーで設定できます。

ロードバランス方法の選択

サイト内に利用できるサーバーが複数ある場合、ロードバランスはデフォルトで有効になっています。デフォルトのロードバランス方法はリソースベースのロードバランスです。ロードバランス方法は、[方法] ドロップダウンリストから選択できます。

リソースカウンターの構成

リソースベースのロードバランスでは、次のカウンターを使用して、特定のサーバーが他のサーバーよりも負荷が高いかどうかを判断します。

- ユーザーセッション: セッション数の最も少ないサーバーにユーザーをリダイレクトします。
- メモリ: RAM の「空き/使用中」比率が最も高いサーバーにユーザーをリダイレクトします。
- CPU: CPU 時間の「空き/使用中」比率が最も高いサーバーにユーザーをリダイレクトします。

すべてのカウンターが有効になっている場合、ロードバランサーは各カウンターの比率を合計し、最も適切な合算比率のサーバーにセッションをリダイレクトします。

等式からカウンターを削除するには、[カウンター] セクションでカウンター名の横にあるチェックボックスをクリアします。

セッションのオプション

接続解除されたセッションを再接続する: このオプションを有効にすると、受信ユーザーセッションは、すでに切断されたセッションのうち同じユーザーが所有していたセッションにリダイレクトされます。

クライアント IP のみでのセッションの再接続: 切断されたセッションに再接続するときに、Parallels RAS は、再接続を要求するユーザー名と、切断されたセッションのユーザー名を照合し、セッションを一致させます。このオプションを有効にした場合、Parallels RAS は、ソース IP を照合し、切断されたどのセッションにセッションを再接続するかを決定します。

各ユーザーをデスクトップごとに 1 セッションと限定する: このオプションを有効にすると、同一ユーザーが複数のセッションを開くことができなくなります。このオプションが機能するには、1 ユーザーにつき 1 セッションに制限するように、RD セッションホストを構成する必要があります。Windows Server 2012（R2）では、[ローカルグループポリシー] \ [リモートデスクトップサービス] \ [リモートデスクトップセッションホスト] \ [接続] の [リモートデスクトップサービスユーザーに対してリモートデスクトップサービスセッションを 1 つに制限する] オプションがこれに該当します。

Microsoft RD Connection Broker を無効にします:: このオプションが有効な場合、Microsoft RD Connection Broker は、RAS Connection Broker がインストールされている場合に実行される

RAS のやり取りに干渉しません。このオプションは、Windows Server 2012 以上でのみ機能することに注意してください。

Agent のタイムアウトと更新時間

サーバー上で実行している RAS Agent のデフォルトのタイムアウトと更新時間を変更することもできます。Agent 応答の待ち時間が長すぎる場合や、逆にタイムアウトが早すぎる場合は、独自の値を指定することができます。

デフォルトのタイムアウトを変更するには、以下の操作を実行します。

1. [構成] ボタンをクリックします。
2. 開いたダイアログで、[エージェントがレスポンスしない場合] フィールドで、秒単位で期間を指定します。この期間内に Agent が応答しない場合、サーバーはロードバランサーから除外されます。
3. [エージェント更新時間] フィールドでは、エージェントに接続可能かどうかを確認するのに必要な秒数を指定します。

CPU 最適化の構成

CPU 最適化機能では、必要に応じて CPU のロードバランスを最適化することができます。CPU ロードバランサーを構成すると、プロセスによる CPU の使用率が指定値を超えた状態が、指定した秒数の間継続した場合、そのプロセスの優先度が下げられます。そのプロセスの使用率が一定の割合以下になってから一定の秒数が経過すると、ロードバランサーにより、優先度が元のレベルに戻されます。

CPU の最適化を構成するには、[CPU 最適化を有効にする] オプションを選択して、以下のように値を指定します。

開始

CPU の最適化を有効にするタイミングを指定します。[合計 CPU 使用率のしきい値] フィールドで、システム全体の CPU 使用率をパーセントで指定します。

CPU 条件

特定のプロセスが指定された CPU パーセンテージを超えるか下回る場合のプロセスごとのしきい値を指定します。ここでは、[クリティカル] と [アイドル] の値を指定できます。CPU ロードバランサーは、これらの値を基準に他の優先順位を調整します。

CPU 使用率の値は、[ロードバランス] タブ（p. 384）で設定した Agent の更新時間に基づいて減衰および計算されることに注意してください。

除外

[除外] リストを使用して、CPU 最適化から除外するプロセスを指定します。[タスク] > [追加] をクリックしてプロセスを選択します。リストからプロセスを削除するには、削除するプロセスを選択して、[タスク] > [削除] をクリックします。

クリティカル/アイドルの値が不適切な場合、問題（不適切な構成によりプロセスがアイドルになる）が発生する可能性があります。CPU 使用率カウンターの取得に問題がある場合は、最適化を適用できません。

ログファイルは %ProgramData%\Parallels\RASLogs\cpuloadbalancer.log にあります。しきい値を確認するためにログを使用してください。Windows では、CPU 使用率パフォーマンスカウンターを確認することができます。

注: クリティカル/アイドルのしきい値は、プロセスの CPU 使用率が最も高いもの（絶対的な CPU 使用率ではない）を基準に計算されるため、優先順位を変更してもログには反映されません。

絶対的な CPU 使用率とは、合計 CPU 使用率のことです。たとえば、2 つのプロセスがそれぞれ 30% ずつ使用している場合、合計の CPU 使用率は 60% となります。CPU ロードバランサーが起動する使用率のしきい値は 25%（デフォルト）です。

最大のプロセス CPU 使用率とは、最も多くの CPU を使用しているプロセスの CPU 使用率です。たとえば、3 つのプロセスがあり、2 つのプロセスが 10%、3 つ目が 40% の場合、最大の CPU 使用率は 40% です。

高可用性ロードバランス（HALB）

Parallels RAS の高可用性ロードバランス（HALB）は、RAS Secure Gateway の負荷分散を行う機能です。Parallels HALB アプライアンスは、ロードバランサーが組み込まれている仮想マ

シンで、オペレーティングシステムがインストールされ、関連するすべての設定が事前に構成されています。

Parallels HALB アプライアンスは次のハイパーバイザーで利用できます。

- Microsoft Hyper-V
- VMware

他のハイパーバイザーを使用することも可能ですが、サポートはベストエフォートとして提供されることに注意してください。Parallels RAS HALB アプライアンスは、さまざまなハイパーバイザーが標準でサポートしている Open Virtualization Platform（OVA）フォーマットを使用します。

HALB はサイトレベルの Parallels RAS で展開されます。サイトごとに複数の HALB 構成を持つことができ、これを仮想サーバーと呼びます。各仮想サーバーは、固有の IP アドレス（仮想 IP または VIP と呼ばれる）を持ち、実際のロードバランスを実行する 1 つ以上の HALB アプライアンス（仮想サーバーコンテキストでは HALB デバイスとも呼ばれる）が割り当てられます。HALB 仮想サーバーは、HALB デバイスを仮想的に表現したものです。HALB デバイスが適切に設定されている場合、HALB デバイスにトラフィックを分配します。特定の仮想サーバーの IP アドレスは、クライアントソフトウェアにとって唯一の接点であるため、仮想サーバーごとに 2 つ以上の HALB デバイスを用意して冗長性を確保することをお勧めします。

1 台の仮想サーバーに割り当てられた複数の HALB デバイスを同時に実行し、1 台をプライマリ、他の 1 台をセカンダリとして動作させることができます。仮想サーバーに割り当てられた HALB デバイスが多いほど、ダウンタイム発生の可能性が低くなります。仮想サーバーにはプライマリ HALB デバイスの IP アドレスが割り当てられ、セカンダリ HALB デバイスと共有されます。プライマリ HALB デバイスに障害が発生した場合、セカンダリがプライマリに昇格し、クライアント接続用に同じ IP アドレスを使用してプライマリの機能を引き継ぎます。

注: セカンダリ HALB デバイスがプライマリに昇格するとき、最大 2 回の切断が発生する可能性があることに留意してください。最初の切断は、1 つの HALB デバイスがダウンするときに発生します。2 回目の切断は、そのデバイスがオンラインに戻るときに発生する可能性があります。仮想 IP アドレスをダウンした HALB デバイスから別の HALB デバイスに転送する必要があるため、この切断を回避することはできません。つまり、最初のデバイスは、この IP アドレスでの通信を停止せざるを得ず、他のデバイスが通信を開始するまでの間、通信は切断されます。切断してもユーザーセッションには影響しないことに注意してください。ユーザーはセッションに再接続することができ、ユーザーデータが失われることはありません。

高可用性ロードバランスのセットアップは次の手順で実行します。

1 1 つまたは複数の Parallels HALB アプライアンス（デバイス）を展開します。

2 RAS Console で 1 つまたは複数の仮想サーバーを構成します。

次に、Parallels HALB アプライアンスをダウンロードし展開する方法について説明します。

前提条件

HALB を使用するために必要な前提条件を以下に示します。

- クライアント機器のソース IP を保持するように構成された HALB より手前に設置されるファイアウォールまたはルーター

Parallels HALB アプライアンスを展開する

Parallels HALB アプライアンスをダウンロードするには、
https://www.parallels.com/products/ras/download/links/ をご覧ください。

Parallels Remote Application Server をダウンロードのウェブページで、オプションのサーバーコンポーネントをダウンロードの表まで下にスクロールし、Parallels Remote Application Server HALB アプライアンスの行をご覧ください。行には次のダウンロードリンクが記載されています。

- HALB アプライアンス OVA
- HALB アプライアンス VHD
- HALB アプライアンス VMDK

ダウンロードする必要があるアプライアンスタイプは使用されているハイパーバイザーによって異なります。以下の指示に従って、ハイパーバイザーのタイプを確認します。

VMware

VMware の場合、OVA アプライアンスファイルまたは zip 形式の VMDK アプライアンスファイルを使用して、アプライアンスをインポートできます。OVA ファイルを使用して展開する場合、構成済みの VM が作成されます。

また、VMDK ファイルを使用する展開では、事前構成された仕様なしで VM が展開されます。この VM の最小仕様を以下に示します。

- 1 x CPU
- 256 MB RAM

- 1 x ネットワークカード

Microsoft Hyper-V

Microsoft Hyper-V の場合、VDH ファイルを使用して、このアプライアンスをインポートする必要があります。

Parallels HALB アプライアンスを展開する

Parallels HALB アプライアンスはダウンロード後、Parallels RAS と同じローカルネットワークに接続されている独立したマシン上で動作しているハイパーバイザーにインポートする必要があります。仮想アプライアンスのインポート方法について詳しくは、ハイパーバイザーのマニュアルを参照してください。

HALB 仮想サーバーの追加

HALB 仮想サーバーを追加するには:

1 RAS Console で、[ファーム] > <サイト> > [HALB] に移動します。

2 右ペインの [仮想サーバー] タブで [タスク] > [追加] をクリックします。[HALB 構成] ウィザードが開きます。

3 [HALB を有効化] オプションが選択されていることを確認します。

4 この仮想サーバーの名前と説明（オプション）を入力します。

5 [パブリックアドレス] フィールドに、このサーバーのパブリック FQDN または IP アドレスを入力します。これは、クライアントの接続をリダイレクトするために優先ルーティング機能で使用されます。「優先ルーティングを構成」（p. 319）を参照してください。

6 [仮想 IP] セクションで、後でこの仮想サーバーに割り当てる HALB デバイスが受信クライアント接続に使用する、仮想 IP アドレスのプロパティを指定します。

7 [設定] セクションで、以下から 1 つまたは複数のオプションを選択します。少なくとも 1 つの“LB”オプションを選択する必要があることに注意してください。この時点でオプションをスキップした場合は、後で仮想サーバーのプロパティダイアログで追加できます。

   - LB ゲートウェイペイロード: 通常の（セキュアでない）ゲートウェイ接続のロードバランスを有効にします。
   - LB SSL ペイロード: SSL 接続のロードバランスを有効にします。

- クライアント管理: HALB を介して接続された Windows クライアントデバイスの管理を有効にします。

8 [次へ] をクリックします。

ここから先は、前のステップで選択したペイロードに応じて、ペイロードのプロパティを構成できるウィザードページが開きます。これらのページについて、以下に説明します。

LB ゲートウェイペイロード

通常接続時のロードバランスを構成します。

1 HALB デバイスが RAS Secure Gateway にトラフィックを転送するために使用するポート番号を設定します。ポートはゲートウェイで構成します。デフォルトのポートは 80 です。

2 [ゲートウェイ] リストで、負荷分散する RAS Secure Gateway を選択します。ゲートウェイごとに使用できる IP アドレスは 1 つのみであることに注意してください。同じゲートウェイで異なる IP アドレスのエントリーが複数ある場合は、1 つだけを選択できます。

LB SSL ペイロード

SSL 接続時のロードバランスを構成します。

1 HALB デバイスが RAS Secure Gateway に SSL トラフィックを転送するために使用するポート番号を設定します。ポートはゲートウェイで構成します。デフォルトのポートは 443 です。

2 SSL モードを [パススルー] または [SSL オフローディング] から選択します。デフォルトでは、SSL 接続はゲートウェイに直接トンネリングされ（パススルーとも呼ぶ）、そこで SSL 暗号化解除プロセスが実行されます。

[SSL オフローディング] モードでは、SSL 証明書を HALB に割り当てる必要があります。選択したら、[構成] をクリックし、以下のように指定します。

- 許可される SSL バージョン: SSL バージョンを選択します。
- 暗号強度: 必要な暗号強度を選択します。カスタムの暗号を指定するには、[カスタム] を選択して、[暗号] フィールドで暗号を指定します。
- [サーバー環境に応じて暗号を使用] オプションは、デフォルトで有効になっています。このオプションを無効にすることで、クライアントの環境設定を使用することができます。

- 証明書: 必要な証明書を選択します。新規証明書の作成方法とリストへの表示方法については、「SSL 証明書の管理」(p. 338) を参照してください。

  <すべてのマッチングを試用> オプションにより、構成済みの任意の証明書が使用されます。これは HALB で使用されます。証明書を作成する場合、”ゲートウェイ”、”HALB”またはその両方を選択できる場所で”使用”プロパティを指定します。このプロパティで”HALB”オプションが選択されている場合、HALB で使用できます。このオプションを選択していても、一致する証明書が存在しない場合には、警告が表示され、先に証明書を作成することになります。

3 負荷分散するゲートウェイを選択します。ゲートウェイごとに使用できる IP アドレスは 1 つのみであることに注意してください。

デバイスマネージャー

Windows クライアントデバイス管理を構成し、Windows クライアントデバイスを管理するゲートウェイを選択します。ゲートウェイごとに使用できる IP アドレスは 1 つのみであることに注意してください。

デバイス

HALB デバイスを仮想サーバーに割り当てるには、以下の操作を実行します。

1 [タスク] > [追加] をクリックし、HALB デバイスを選択、または指定します。HALB デバイス (アプライアンス) をまだ展開していない場合でも、仮想サーバー構成を保存して、後から HALB デバイスを割り当てることができます。仮想サーバーごとに最低 2 台の HALB デバイスを割り当てることを推奨します。詳細については、「高可用性ロードバランス (HALB)」(p. 387) を参照してください。HALB デバイスの優先度は、リスト内のデバイスの位置によって設定されます。一番上のデバイスがプライマリ HALB デバイスです。その下のデバイスはセカンダリ HALB デバイスです。デバイスをプライマリに昇格させるには、単純にデバイスをリストの一番上に移動します。

2 最後に、[完了] をクリックして仮想サーバーの設定を保存し、ウィザードを閉じます。

RAS Console のリストに、新しい仮想サーバーが表示されます。

仮想サーバーの変更と詳細オプションの設定

仮想サーバーの設定を変更するには、仮想サーバーを右クリックして [プロパティ] を選択します。[プロパティ] ダイアログのタブには、上記のウィザードページと同じオプションがあります。唯一の違いは、以下で説明する [詳細] タブだけです。

仮想サーバーの詳細オプションを表示して設定するには、[詳細] タブを選択します。このタブに表示されるオプションは、仮想サーバーに割り当てられたすべての HALB デバイスに適用されます。このリストを使用すると、仮想マシンに直接ログインしなくても HALB デバイスのオプションに簡単にアクセスできます。これらの値を変更すると、予期しない結果になる可能性があることに注意してください。必ず特定のネットワーク要件に応じて変更する必要があります。

次の詳細設定を使用できます。

オプション	既定値	説明
RDP UDP トンネリングを有効化	有効	RDP クライアントが RDP を HALB デバイス経由で UDP トラフィックに転送できるようにします。
TCP 最大接続数	2000	最大同時 TCP 接続数を設定します。
クライアントの非アクティブタイムアウト（秒）	150	クライアント側の最大非アクティブ時間（秒）。
ゲートウェイの接続タイムアウト（秒）	30	ゲートウェイへの接続試行成功までにかかる最大時間（秒）。
クライアントの接続キュータイムアウト（秒）	30	デバイスの TCP 最大接続数に達すると、以降の接続はこのタイムアウト（秒）の間、キューで保留中となります。
ゲートウェイの非アクティブタイムアウト（秒）	150	ゲートウェイの最大非アクティブ時間（秒）を設定します。
1 秒あたりの TCP 接続量	1000	HALB デバイスで 1 秒あたりに受け入れる新規接続数の上限を設定します。
ゲートウェイヘルスチェックの間隔（秒）	5	2 つの連続するヘルスチェックの間隔（秒）を設定します。
VRRP 仮想ルーター ID	15	同じネットワーク上で実行される複数の VRRP インスタンスを区別するために使用されます。
VRRP 認証パスワード	-	フェイルオーバーの同期のために使用される HALB デバイス間の VRRP 通信に、パスワード認証を設定します。
VRRP ブロードキャストの間隔（分）	1	デバイスがアクティブな状態で ARP の重複確認を行う更新の最短間隔（分）。
VRRP ヘルススクリプトをチェックする間隔（秒）	2	ローカルの HALB サービスを起動し稼働させるためのスクリプトを呼び出す間隔（秒）を設定します。
VRRP ヘルススクリプトのチェックタイムアウト（秒）	10	ローカルの HALB サービスを起動し稼働させるためのスクリプトの実行タイムアウト（秒）。

VRRP 広告の間隔（秒）	1	同一の VRRP グループの HALB デバイス間に広告パケットを送信する間隔（秒）。
OS アップデートの有効化	無効	HALB デバイスで OS パッケージが自動的に更新されるようにします。
既存のロードバランスの設定を保持	無効	現在デバイスにあるロードバランスの構成を保持し、新しい設定を上書きしません。
既存の VRRP やキープアライブ設定を保持	無効	現在デバイスにある VRRP やキープアライブの構成を保持し、新しい設定を上書きしません。

HALB デバイスステータスとバージョン番号

HALB デバイスのステータスとバージョン情報は、RAS Console 内の以下の 2 つの場所で確認できます。

サイトタブ

RAS Console の [サイト] タブで、HALB デバイスと関連する情報を確認できます。確認するには [ファーム] > [サイト] に移動します。[エージェント] と [エージェントのバージョン] 列に注意してください。2 つの列について次に説明します。

[エージェント] 列には次の値が表示されます。

- 未検証（赤） - エージェントは検証されておらず、通信を行えません。この状態の場合は、エージェントを検証してください。
- アップデートが必要（黄） - Agent は正常に動作していますが、古いバージョンです。この場合、Agent を最新バージョンにアップデートする必要があります。
- エージェント OK（緑） - エージェントは正常に動作しています。必要な措置はありません。

[エージェントバージョン] 列には、Parallels RAS のバージョンとビルド番号を含む実際のエージェントのバージョンが表示されます。

また、HALB デバイスを右クリックして [ツール] > [ホストに Ping を実行] を選択すると、HALB デバイスに対して ping を打つことができます。[ツール] メニューおよび [Ping] ツールの使用方法については、「コンピューター管理ツール」（p. 569）を参照してください。

デバイスタブ

HALB デバイスエージェントのステータスとバージョンは、メイン HALB サブカテゴリにも表示されます。これを確認するには、[ファーム] > [サイト] > [HALB] に移動し、[デバイス] タブを選択します。ここに表示されるエージェントの情報は、上述の [サイト] タブに表示されるものと同様です。

HALB のメンテナンス

HALB デバイス（仮想マシン）を交換または修理する必要がある場合は、単に仮想サーバー構成から HALB デバイスを削除した後、修理したデバイスまたは新しいデバイスを追加します。仮想サーバー設定からすべての HALB デバイスを一時的に削除する必要がある場合も、この方法を行うことができます。

また、メンテナンス中に仮想サーバーを無効にするには、仮想サーバーのプロパティダイアログの [一般] タブで [HALB を有効化] オプションをオフにします。

HALB 接続とセッション情報

HALB デバイスごとの TCP 接続数を確認するには、[HALB] > [デバイス] に移動し、デバイスリストの [TCP 接続] 列を確認します。リストを更新するには、[タスク] > [更新] をクリックします。

仮想サーバーごとのセッション情報を表示するには、[ファーム] > [サイト] に移動します。各仮想サーバーのセッションカウントが [セッション] 列に表示されます。

HALB アプライアンスのパスワードの変更

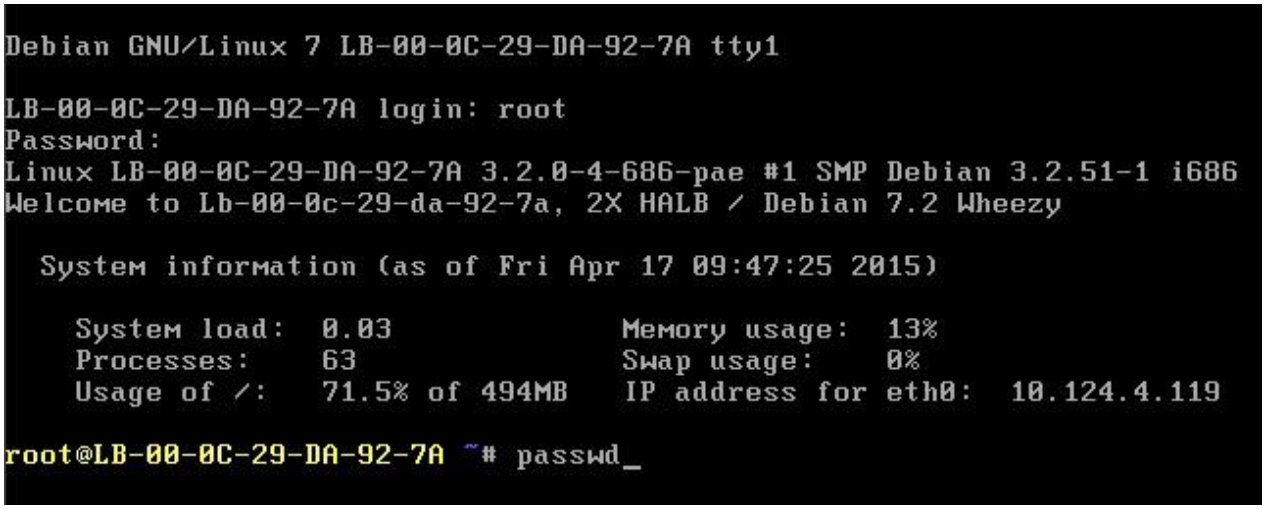
HALB アプライアンスのパスワードを変更するには、以下の操作を実行します。

1 アプライアンス（仮想マシン）を起動します。

2 <ALT> キーと <F1> キーを同時に押します。ログインプロンプトが表示されます。

3 次の資格情報を入入力します。

- ログイン: `root`
- パスワード: `Pa$$w0rd`（“0”はゼロで、文字の “O”ではありません）。



4 ログインしたら、パスワード変更コマンドを実行して、新しいパスワードを入力します。

完了すると、新しいパスワードで HALB デバイスにログインすることができます。

第　17　章

RAS のマルチテナントアーキテクチャ

この章の内容

概要

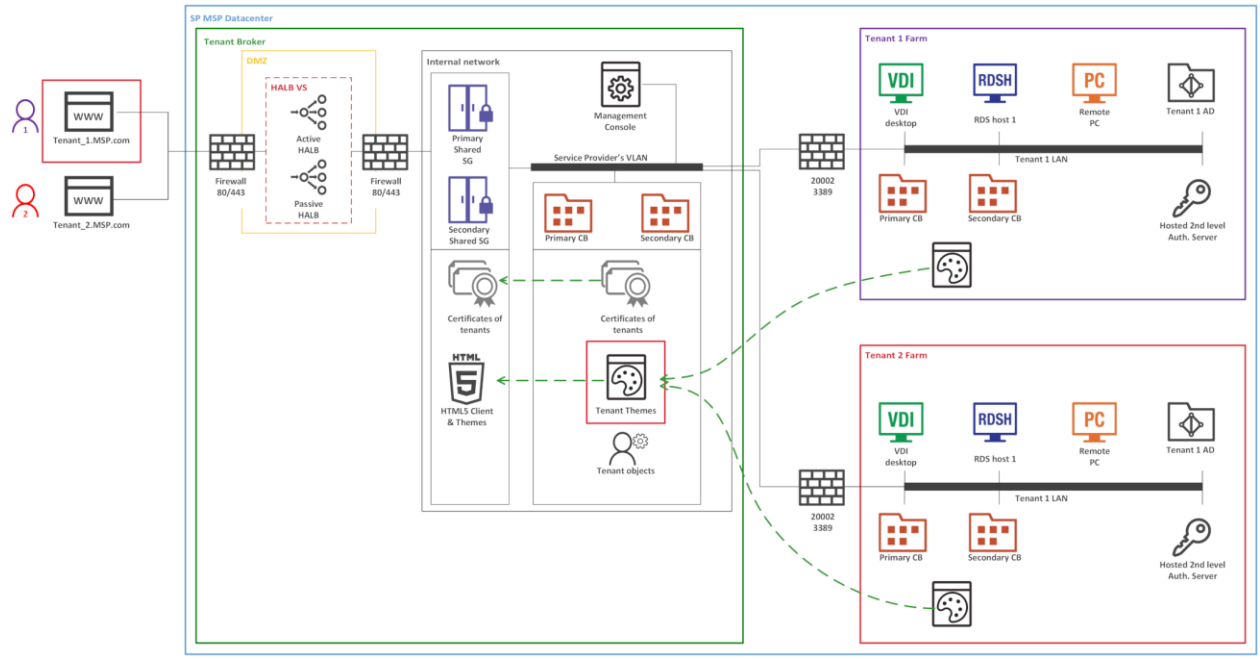
RAS 17.1 で Parallels RAS のテナントブローカーが追加され、マルチテナントアーキテクチャが導入されました。その結果、組織ではさまざまなテナントの間で同じ RAS インフラストラクチャのコンポーネントを共有したり、クライアントデータを分離してコストを低減したりできるようになります。

RAS のマルチテナントアーキテクチャには、サービスプロバイダーと組織にとって以下のメリットがあります。

- RAS Secure Gateway と高可用性ロードバランサー（HALB）の数を減らし、リソースの使用率や統合を最大化することで、コストを削減できます。
- 新しいテナント/顧客のオンボーディングを迅速化できます。
- マルチテナント環境をシンプルに集中管理できます。
- どんな規模の組織でも、インフラストラクチャの共有によってコストのスケーリングを実現し、運営コストを削減し、市場訴求力を増大できます。

アーキテクチャの説明

RAS マルチテナントアーキテクチャを使用した標準的な Parallels RAS の展開環境を以下の図にまとめます。



- ファイアウォールと HALB は DMZ にインストールされていて、各テナントが共有します。
- テナントブローカーは、共有の RAS Secure Gateway と HALB をホストするための特別な RAS インストールであり、RAS のアクセスレイヤーも使用できます。テナントブローカーをインストールするには、Parallels RAS インストーラーで [Parallels RAS テナントブローカー] オプションを使用します。テナントブローカーは、専用ドメインにインストールすることも、ドメインの外にインストールすることもできます。
- テナントファームは、オンプレミスの RAS 環境の場合と同じように展開され、テナントブローカーに接続します。各テナントファームには、独自の RAS Connection Broker と、公開リソース（VDI、RD セッションホスト、リモート PC）をホストするサーバーがあります。ローカルの RAS Secure Gateway と HALB は不要です（サードパーティのロードバランサーも不要です）。
- テナントをテナントブローカーに接続すると、各テナントがテナントブローカーでテナントオブジェクトとして表示されます。

- Parallels Client （プラットフォーム固有の Client または Web Client のいずれも）は、テナントブローカーで共有ゲートウェイに接続します。クライアントがユーザーポータルに接続すると、クライアントの所属先の対応するテナントのテーマが常に使用されます。

実装の概要

RAS のマルチテナントアーキテクチャ実装の概要を以下にまとめます。

- 各テナントは、別々のファームまたはサイトとして展開されます。テナントをファームとして展開する場合は、各テナントが完全に独立していて、相互に通信することはまったくありません。テナントをサイトとして展開する場合は、各サイトが別々にテナントブローカーに接続する必要があります。
- RAS Secure Gateway（ユーザーポータルも含む）や高可用性ロードバランサー（HALB）などは、共有リソースになります。
- テナントファームには、独自の RAS Secure Gateway や HALB は不要です。ただし、内部接続のためにゲートウェイや HALB が必要なら、ゲートウェイや HALB を組み込んだ展開も可能です。例えば、内部接続と外部接続のために別々のポリシーを用意している場合は、ローカルユーザーに対応するためにゲートウェイや HALB をインストールできます。
- テナントのネットワーク構成では、テナントの Connection Broker からテナントブローカーの Connection Broker への接続が必要になります。さらに、共有の RAS Secure Gateway も、公開リソースをホストしているサーバーやテナントの Connection Broker と通信する必要があります。ネットワークアーキテクチャの実装によっては、VLAN と VLAN の接続や VPN などが必要になることもあります。そのような通信については、ごく限られた数のポートを開くだけで十分です。完全なリストについては、「通信ポート」（p. 421）を参照してください。
- テナントドメインとの通信は、常にローカルテナントの Connection Broker から実行され、テナントブローカーのインフラストラクチャから実行されることはありません。
- 各テナントには、固有のパブリックドメインアドレスが必要です。そのアドレスを割り当てる方法はいろいろあります。例えば、サーバープロバイダーがサブドメイン（Tenant1.Service-Provider.com など）を登録し、そのドメインをテナントに割り当てる、といった方法があります。また、プライベートドメインアドレス（RAS.Tenant1.com など）を使用し、テナントブローカーでそのルーティング先を RAS Secure Gateway にする、といった方法も考えられます。別々のパブリックドメインアドレスを同じ IP アドレスに解決することが必要なら、そうすることも可能です。
- テナントをテナントブローカーに接続すると、共有の RAS Secure Gateway がテナントとテナント構成を認識し、テナントの RAS Connection Broker に接続できる状態になります

。インターネットから RAS Secure Gateway （または HALB）に届くテナントの着信トラフィックのためのルートをテナントブローカーで設定する必要があります。

- テナントブローカーには専用の RAS Console が付属しています。そのコンソールで、共有リソースやテナントオブジェクトや証明書を管理したり、テナントのパフォーマンスを監視したり、標準的な RAS 管理タスクを実行したりできます。
- すべてのテナントのテーマがテナントブローカーで使用できるようになります。ユーザーが共有の RAS Secure Gateway を経由してテナントブローカーに接続すると、対応するテナントのテーマがユーザーに表示されます。
- テナントごとに別々の SSL 証明書を使用することも可能です。

ライセンス

テナントブローカーにライセンスは要りません。ライセンスはテナントレベルで管理されています。

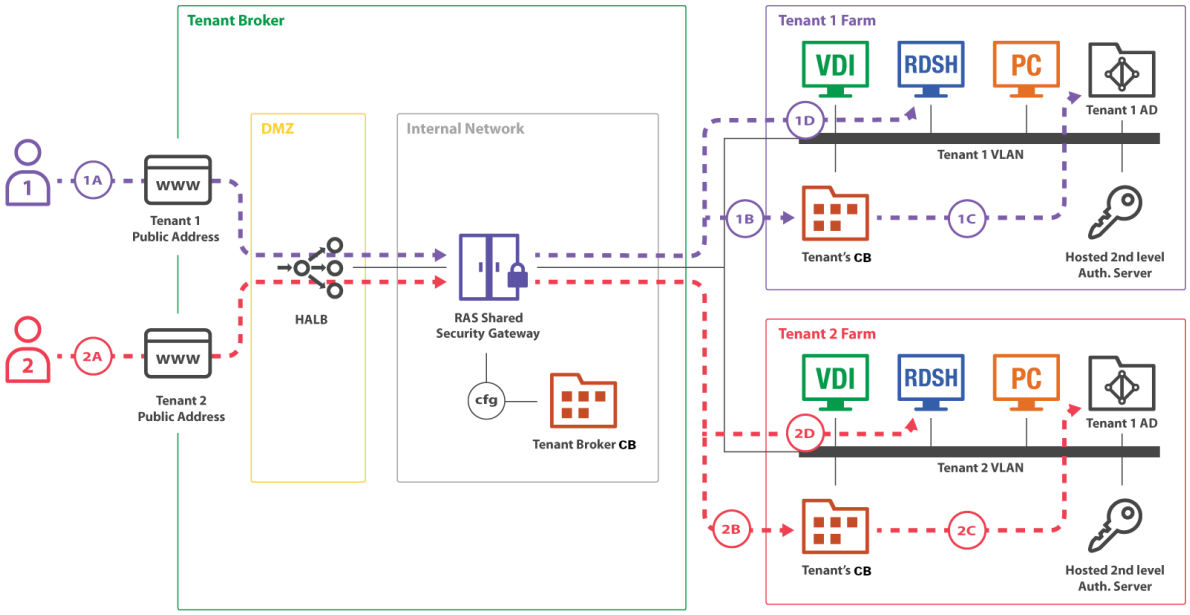
RAS バージョンの互換性

Parallels RAS のマルチテナントアーキテクチャは、Parallels RAS 17.1 以降で使用できます。それよりも古いバージョンの Parallels RAS を使用する場合は、以下の制限があります。

- RAS 17.1 より古いバージョンの Parallels Client は、共有ゲートウェイとの互換性がないので、そのクライアントからテナントブローカー経由でテナントファームに接続することはできません。
- RAS 17.1 より古いバージョンの Parallels RAS インストール環境は、テナントブローカーとの互換性がないので、テナントとして接続できません。

ユーザー接続の流れ

テナントブローカーを経由した RAS ユーザー接続の流れを以下の図にまとめます。



テナントブローカーにインストールされている共有の RAS Secure Gateway は、複数のテナントファームで複数のユーザーセッションを同時に処理できます。上の図では、2 人のユーザー（1 と 2）が別々のテナントファーム（テナント 1 ファームとテナント 2 ファーム）に接続しています。どちらの接続も同じゲートウェイでトンネリングされていますが、それぞれが正しいテナントファームに送られています。

この接続は以下の流れで進んでいきます。

1 （1A）、（2A） - ユーザーが、テナントブローカーに登録されているパブリックアドレスへの RAS 接続を開始します。（1A）接続はテナント 1 のパブリックアドレスに向かい、（2A）接続はテナント 2 のパブリックアドレスに向かいます。

2 （1B）、（1C） - 共有ゲートウェイが、最初の接続（1A、2A）で使用されていたホスト名に基づいて、ユーザー接続の転送先を決定します。その後、各クライアントが、それぞれのテナントファームの Connection Broker との RAS セッションを確立します。テナントの Connection Broker が、テナントの Active Directory に照らしてユーザーを認証します。その後、ユーザーが、自分で利用できる公開アプリケーションのリストを受け取ります。

3 （1D）、（2D） - ユーザーが、公開アプリケーションとのリモートユーザーセッションを開始します。共有ゲートウェイが、テナントの Connection Broker に対して、リモートセッション転送先のサーバーのアドレスを要求し、そのアドレスにセッションを転送します。

パブリックアドレスとテナントのマッピングは、テナントブローカーの Connection Broker が共有ゲートウェイで設定します。

テナントブローカーとテナントの展開

Parallels RAS のマルチテナントアーキテクチャを展開するための標準的なシナリオは、以下のようになります。

1 テナントブローカーを展開します。

2 従来の RAS ファームをテナントとして運用できるように展開します。

3 テナントブローカーとテナントのネットワーク接続を設定して、以下の接続を可能にします。

- 共有の RAS Secure Gateway とテナントの RAS Connection Broker の接続。
- 共有の RAS Secure Gateway とリソースホストの接続。
- テナントの RAS Connection Broker からテナントブローカーの RAS Connection Broker への接続。

ポート番号については、「通信ポート」（p. 421）を参照してください。

4 テナントブローカーのコンソールで、テナントオブジェクトとそれに対応する招待ハッシュを作成するか、または秘密鍵を作成します（この章の後の方で詳しく説明します）。

5 招待ハッシュまたは秘密鍵を使用して、テナントをテナントブローカーに接続します。

6 テナントにパブリックドメインアドレスを割り当てます。この作業は、この時点で（つまりテナントの接続後に）行うことも、後から行うこともできます。どちらにしても、この作業は必須です。そうしないと、クライアントがテナントファームに接続できません。

7 インターネットから共有の RAS Secure Gateway と HALB に入ってくるテナントの着信トラフィックのルーティングをセットアップします。

8 テナントの証明書を設定します。デフォルトでは、インストール時に作成される自己署名証明書が使用されます。

9 クライアント接続をテストします。

以下のサブセクションで、それぞれの手順を詳しく説明します。

テナントブローカーの展開

最初に、テナントブローカーを専用サーバーにインストールする必要があります。テナントブローカーをインストールするコンピューターに Parallels RAS がすでにインストールされている場合は、まずそれをアンインストールすることが必要です。2 つのインストールバージョンを同じマシンに共存させることはできません。

テナントブローカーをインストールするには、以下の手順を実行します。

1 標準の Parallels RAS インストーラーを実行します。

2 [インストールタイプの選択] ページで [Parallels RAS テナントブローカー] を選択します。

3 [次へ] をクリックし、画面上の指示に従います。

インストールが完了したら、Parallels RAS Console を起動します。

コンソールが起動すると、標準の RAS Console とは別のカテゴリや管理対象オブジェクトが表示されます。テナントブローカーコンソールの目的は、共有リソースとテナントを管理することです。RD セッションホストや VDI などの標準 RAS リソースを管理するためのものではありません。そうしたリソースは、テナントファームごとに展開して管理します。

テナントブローカーコンソール

テナントブローカーコンソールでは、以下のカテゴリとオブジェクトを管理できます。

- ファーム: このカテゴリーでは、テナント、ゲートウェイ、Connection Broker、HALB、証明書を管理できます。[設定] サブカテゴリーでは、グローバルログやテナントブローカー自体を管理できます。
- 管理: 標準の RAS Console と同じような管理タスクを実行できます。アカウント、設定、メールボックス、レポート、設定監査などです。
- 情報: テナントブローカーで実行されているサービスやコンポーネントの状況を確認できます。

標準の RAS Console の場合と同じく、いずれかのオブジェクトを変更したら、その変更を構成データベースに保存するために [適用] ボタンをクリックしてください。

RAS Secure Gateway のインストール

デフォルトでは、テナントブローカーに RAS Secure Gateway はインストールされません。ゲートウェイを追加するには、テナントブローカーコンソールにログインし、[ファーム] > [Secure Gateway] に移動し、[タスク] > [追加] をクリックします。どの RAS ファームでも使用されていない RAS Secure Gateway 1 つ以上あれば、そのゲートウェイをテナントブローカーに追加することも可能です。ただし、既存の RAS Secure Gateway のインストール環境は、RAS バージョン 17.1 以降でなければなりません。それより古い RAS バージョンのゲートウェイは、共有ゲートウェイとして使用できません。

新しいゲートウェイをインストールするには、対象のサーバーで Parallels RAS インストーラーを実行し、[カスタム] を選択し、[RAS Secure Gateway] コンポーネントを選択します。インストールが完了したら、テナントブローカーコンソールに戻って、そのゲートウェイをテナントブローカーに追加します。

テナントの展開

テナントファームの展開方法は、従来の Parallels RAS ファームの展開方法とほぼ同じです。唯一の違いは、ファームをインストールするときに、RAS Secure Gateway をインストールする必要はないということです。

注: ローカルの（プライベートの） RAS Secure Gateway を（ローカル接続などのために）テナントファームにインストールすることは可能ですが、テナントブローカーの HALB やゲートウェイとテナントファームの HALB やゲートウェイを混在させることはできません。テナントブローカーにインストールされる HALB アプライアンスは、そのようなシナリオをサポートしていません。

Parallels RAS ファームをテナントとして使用できるようにセットアップするには、以下の手順を実行します。

1. Parallels RAS インストーラーを実行します。
2. [インストールタイプの選択] ページで、[カスタム] を選択します。
3. [次へ] をクリックします。
4. インストール対象として以下のコンポーネントを必ず選択してください。
   - RAS Connection Broker
   - Parallels RAS Console（ただし、別のマシンにインストールすることも可能）

その他のコンポーネントはオプションです。この時点でインストールすることも、後からインストールすることも可能です。

5 [次へ] をクリックし、画面上の指示に従ってインストールを実行します。

テナントをテナントブローカーに接続する方法

テナントファームが稼働するようになったら、その中にある 1 つ以上のサイトをテナントブローカーに接続できます。

注: テナントとは、個別に展開する Parallels RAS ファームにあるサイトのことです。テナントをテナントブローカーに接続すると、サイトを接続することになります。ファーム全体を接続する場合は、サイトを 1 つずつ接続していきます。もちろん、ファームにサイトが 1 つしかなく、サイトを増やす計画もない場合は、そのサイトを接続するとファーム全体を接続したことになります。

テナントを接続するには、2 つの方法があります。（1）招待ハッシュを使用する方法と、（2）共有秘密鍵を使用する方法です。2 つの方法の違いは以下の通りです。

- 招待ハッシュ: 招待ハッシュとは、1 つのテナントをテナントブローカーに接続するのに使用できる自動生成暗号文字列のことです。招待ハッシュは、テナントオブジェクトのプロパティでもあるので、テナントブローカーコンソールで作成できます。そのハッシュをテナントファーム管理者にメールで送ると、管理者がそのハッシュを使用してテナントをテナントブローカーに接続できるようになります。1 度使用した招待ハッシュを別のテナントで再利用することはできません。
- 共有秘密鍵: 共有秘密鍵も招待ハッシュとよく似ていますが、1 つの重要な違いがあります。共有秘密鍵の場合は、接続できるテナントの数に制限がありません。秘密鍵に対応するテナントオブジェクトは、テナントブローカーで事前に作成されません。そうではなく、秘密鍵を使用してテナントを接続するときにオブジェクトが作成されます。秘密鍵には使用制限がないので、テナントブローカー管理者だけが共有秘密鍵にアクセスできるようにしてください。このシナリオは、複数のテナントがあって、そのすべてを同じテナントブローカー管理者が管理する場合に便利です。

ここでは、招待ハッシュのシナリオを説明します。秘密鍵のシナリオについては、「秘密鍵による接続」（p. 408）を参照してください。

まず、招待ハッシュを生成することと、テナントブローカーの側でテナントオブジェクトを作成することが必要です。

1 テナントブローカーにログインします。

2 RAS Console で [ファーム] > [テナント] に移動します。

3 [タスク] > [追加] をクリックします。

4 [テナントのプロパティ] ダイアログで、以下のように指定します。

- 名前: テナント名を入力します（どのような名前でも構いません）。
- パブリックドメインアドレス: そのテナントにすでにパブリックドメインアドレスを割り当ててある場合は、そのアドレスを指定してください。そうでない場合は、ブランクのままにしておきます。そのアドレスは、テナントをテナントブローカーに接続するときには必要ありません。ただし、ここでアドレスを指定しておかないと、エンドユーザーがテナントに接続できないので、いずれにしても後から指定することが必要になります。詳細については、「パブリックドメインアドレスの割り当て」（p. 411）を参照してください。
- ゲートウェイモードのクライアントは、サーバー IP により公開済みのテナントリソースに接続します: このオプションを選択すると、クライアントは DNS 名の代わりにテナント IP アドレスを使用します。このオプションは、テナントファームがテナントブローカーファームと同じ DNS プロバイダーを共有していない場合に使用できます。
- 請求情報を表示しない: これを選択した場合、テナントのライセンスカテゴリー（p.591）に課金情報が表示されなくなります。
- 説明: 説明を入力します（オプション）。
- Connection Broker: このフィールドは無効になっています。テナントがテナントブローカーに接続すると、値が自動的に設定されます。詳細については、「テナントの構成」（p. 413）を参照してください。
- テナント招待ハッシュ: テナントファーム管理者がテナントブローカーに接続するときに、このハッシュが必要になります。このダイアログを開くと、ハッシュが自動的に生成されます。新しいハッシュを作成するには、[新しいハッシュを作成] をクリックします。
- 電子メールで送る: 招待ハッシュをテナント管理者に直接渡すことも、このボタンを使用して電子メールで送ることも可能です。このボタンをクリックすると、ダイアログが表示されます。そのダイアログで受信者を入力し、電子メールメッセージを確認したり変更したりできます。デフォルトでは、テナントブローカーに接続する方法がそのメッセージに記されています。ただし、電子メールオプションを使用するには、RAS Console で SMTP 設定を構成しておく必要があります。まず SMTP を構成してから、この画面に戻って操作を実行してください。

5 [OK] をクリックして、[テナントのプロパティ] ダイアログを閉じます。新しいテナントがコンソールの [テナント] リストに表示されます。この時点では、テナントはまだ接続されていません。接続の方法についてこの後説明します。

テナントをテナントブローカーに接続するには、以下の手順を実行します。

1 テナントファームにログインします。

2 RAS Console で [ファーム] > [サイト] に移動します。ここでは、ファーム全体ではなく 1 つのサイトをテナントブローカーに接続します。複数のサイトがある場合は、1 つずつ接続する必要があります。

3 [タスク] > [テナントブローカーに参加する] をクリックします。

4 [テナントブローカーに参加する] ダイアログで、前の手順でテナントブローカーから取得した招待ハッシュ（テナントファーム管理者なら、招待メールで受け取った招待ハッシュ）を入力します。

5 [接続] をクリックします。

接続が成功すると、テナントブローカーに接続できたことを示すメッセージが表示されます。テナントファームのプライマリ Connection Broker がテナントブローカーにアクセスできない場合は、その趣旨のエラーメッセージが表示されます。テナントの RAS Connection Broker を実行しているマシンからテナントブローカーのコンピューターにアクセスできることを確認してください。

テナントブローカーの IP アドレスの上書き

テナントブローカーの IP アドレスは、招待ハッシュ（または秘密鍵）の生成時に自動的に検出され、ハッシュに埋め込まれます。テナントがそのアドレスでテナントブローカーにアクセスできない場合は、以下のようにしてアドレスを上書きできます。

1 テナントブローカーにログインします。

2 RAS Console で、[ファーム] > [設定] に移動し、[テナントブローカー] タブをクリックします。

3 [テナント招待ハッシュと秘密鍵のテナントブローカーアドレスを上書きする] オプションを選択します。

4 対象のフィールドに IP アドレスを入力します。

招待ハッシュまたは秘密鍵の生成時に自動的に検出されたアドレスの代わりに、ここで指定した IP アドレスが使用されます。テナント側からそのハッシュを使用してテナントブローカーに接続するときに、そのアドレスでテナントブローカーに接続することになります。

テナント側でそのアドレスを使用すると、招待ハッシュによってテナントファームがテナントブローカーのテナントオブジェクトにバインドされ、テナントの関係が有効になります。

秘密鍵による接続

招待ハッシュではなく秘密鍵を使用してテナントをテナントブローカーに接続することも可能です。前述の（p. 405）通り、秘密鍵を使用する場合は、同じテナントブローカーに接続できるテナントの数に制限がありません。

秘密鍵を作成するには、以下の手順を実行します。

1. テナントブローカーコンソールにログインします。
2. RAS Console で [ファーム] > [設定] に移動します。
3. [テナントブローカー] タブを選択します。
4. [秘密鍵によって RAS ファームをテナントブローカーに登録する操作を許可する] を選択します。
5. オプションで、[課金情報を表示しない] を選択すると、秘密鍵で参加したテナントの [ライセンス] カテゴリーの課金情報が非表示になります。
6. 秘密鍵が自動的に生成されます。別の鍵を生成する場合は、[生成] をクリックします。
7. テナントをサブドメインとして登録したい場合、[ドメイン] フィールドでホスト名のドメイン部分を指定してください。たとえば、テナントのホスト名として”subdomain.domain.com”を使用するには、”domain.com”を指定します。

鍵が生成されたら、その鍵を使用して 1 つ以上のテナントをテナントブローカーに接続できます。

注: 秘密鍵には使用制限がないので、テナントブローカー管理者だけが共有秘密鍵にアクセスできるようにしてください。秘密鍵は、テナントブローカー管理者がテナントファームを管理している場合に便利です。テナントごとにハッシュを生成する代わりに、1 つの秘密鍵ですべてのテナントをテナントブローカーに接続できます。

秘密鍵を使用してテナントを接続するには、以下の手順を実行します。

1. テナントにログインします。
2. RAS Console で [ファーム] > [サイト] に移動します。
3. [タスク] > [テナントブローカーに参加する] をクリックします。
4. [テナントブローカーに参加] ダイアログで、以下のように指定します。
   - 最上部のフィールドにシークレットキーを入力します。テナントからテナントブローカーにアクセスできる場合、[テナントブローカー] フィールドに自動入力されます。

- [テナント名] フィールドは、現在のサイト名に基づいて自動的に入力されますが、任意のテナント名を指定することもできます。ここで入力する名前が、対応するテナントオブジェクトの名前としてテナントブローカーで使用されます。
- [パブリックドメインアドレス] フィールドでは、テナントへのアクセスに使用されるパブリックドメインアドレスを指定できます。この構成はオプションです。[ドメイン] フィールドがテナントブローカー設定（上記参照）で構成されている場合、完全なドメインアドレスではなく、サブドメインのみを入力できます。

5 [接続] をクリックします。

接続が成功すると、テナントブローカーに接続できたことを示すメッセージが表示されます。テナントファームのプライマリ Connection Broker がテナントブローカーにアクセスできない場合は、その趣旨のエラーメッセージが表示されます。プライマリ Connection Broker を実行しているマシンからテナントブローカーのコンピューターにアクセスできることを確認してください。

テナントブローカーの IP アドレスの上書き

テナントブローカーの IP アドレスは、秘密鍵の生成時に自動的に検出され、秘密鍵に埋め込まれます。テナントがそのアドレスでテナントブローカーにアクセスできない場合は、以下のようにしてアドレスを上書きできます。

1 テナントブローカーにログインします。

2 RAS Console で、[ファーム] > [設定] に移動し、[テナントブローカー] タブをクリックします。

3 [テナント招待ハッシュと秘密鍵のテナントブローカーアドレスを上書きする] オプションを選択します。

4 対象のフィールドに IP アドレスを入力します。

接続状況の確認

テナントをテナントブローカーに接続したら、操作が成功したかどうかを確認します。

まず、テナントコンソールでテナントブローカーの状況を確認してください。

1 テナントファームにログインします。

2 RAS Console で、[ファーム] > [サイト] に移動し、右ペインの [サイト] タブを選択します。

3 [テナントブローカー] セクションの [ステータス] 列が [OK] になっていることを確認します。ステータスが [未確認] になっている場合は、テナントブローカーが稼働しているかどうかを確認してください（テナントブローカー管理者でない場合は、テナントブローカー管理者に連絡してください）。

テナントブローカーを右クリックして [プロパティ] を選択すると、テナントブローカーの追加情報を表示できます。以下のような情報です。

- 名前: テナントブローカー名。
- プライマリアドレス: プライマリ RAS Connection Broker のアドレス。
- セカンダリアドレス: セカンダリ RAS Connection Broker のアドレス（利用可能な場合）。

次に、テナントブローカーコンソールでテナントの状況を確認してください。

1 テナントブローカーにログインします。

2 RAS Console で [ファーム] > [テナント] に移動します。

3 [テナント] タブで対象のテナントを見つけて、[ステータス] 列を確認します。テナントが正常に接続されていれば、[OK] になっているはずです。[ステータス] 列に表示される他の値については、「テナントの構成」（p. 413）を参照してください。

ネットワークの構成

テナントを展開したら、以下の通信を可能にするために、テナントブローカーとテナントのネットワーク接続を構成する必要があります。

- テナントの Connection Broker > テナントブローカーの Connection Broker: ポート 20003
- テナントブローカーのゲートウェイ > テナントブローカーの Connection Broker: ポート 20002
- テナントブローカーのゲートウェイ > テナントの Connection Broker: ポート 20002
- テナントブローカーのゲートウェイ > 公開リソースをホストしているサーバー: ポート 3389

上記のポートはどれも標準の RAS ポートです。詳細については、「ポート参照」セクションを参照してください。

パブリックドメインアドレスの割り当て

エンドユーザーがテナントブローカー経由でテナントに接続するには、各テナントが固有のパブリックドメインアドレスを持っていなければなりません。どのテナントにも固有のパブリックドメインアドレスが必要ですが、各テナントが固有の IP アドレスを持つ必要はありません。テナントブローカーの共有ゲートウェイにアクセスするために、別々のパブリックドメインアドレスが同じ IP アドレスに解決されるように構成することも可能です。その場合もテナントブローカーは、エンドユーザーから要求されるホスト名に基づいて、正しいテナントにトラフィックを転送できます。

パブリックドメインアドレスを選択する方法は、いろいろあります。例えば、サーバープロバイダーがサブドメイン（Tenant1.Service-Provider.com など）を登録し、そのドメインをテナントに割り当てる、といった方法があります。また、プライベートドメインアドレス（RAS.Tenant1.com など）を使用し、テナントブローカーでそのルーティング先を RAS Secure Gateway にする、といった方法も考えられます。テストのために IP アドレスを使用することも可能です。

[パブリックドメインアドレス] は、テナントブローカーコンソールに表示されるテナントオブジェクトのプロパティでもあります。テナントをテナントブローカーに接続したら、そのプロパティに正しいアドレスが入っていることを確認してください。そうでないと、エンドユーザーは、テナントブローカー経由でテナントに接続できません。

テナントのパブリックドメインアドレスを確認するには、以下の手順を実行します（必要に応じて設定することも可能です）。

1. テナントブローカーにログインします。
2. RAS Console で [ファーム] > [テナント] に移動します。
3. テナントを右クリックし、[プロパティ] を選択します。
4. [プロパティ] ダイアログの [パブリックドメインアドレス] フィールドに正しいアドレスが入っていることを確認します。

SSL 証明書の構成

テナントに割り当てるパブリックドメインアドレスには証明書が必要です。テナントブローカー管理者がテナントブローカーコンソールで各テナントの証明書を作成しなければなりません。その後、その証明書を使用するように共有の RAS Secure Gateway を構成する必要があります。Parallels RAS でテナントの証明書を作成したり管理したりする方法は、他の証明書の場合と同じです。[ファーム] > [サイト] > [証明書] サブカテゴリーを使用してください。証明書を作

成して RAS Secure Gateway や HALB に割り当てる方法の詳細については、「SSL 証明書の管理」の章（p. 338）を参照してください。

ユーザーがテナントのパブリックドメインアドレスに接続すると、対象のパブリックドメインアドレスに対応する共通名の証明書が接続のたびに自動的に選択されます。利用可能な最初の証明書が使用されますが、自己署名証明書でない場合もあります（すでに削除されている場合など）。

対応する証明書が見つからない場合は、デフォルトの自己署名証明書が使用されますが、ウェブブラウザーに証明書に関する警告が表示されます。

着信トラフィックのルーティングのセットアップ

テナントをテナントブローカーに接続した後に、もう 1 つ実行しなければならない作業があります。それは、インターネットから共有の RAS Secure Gateway や HALB に届く着信トラフィックのルートをセットアップする作業です。

ユーザー認証

RAS マルチテナントアーキテクチャのユーザー認証は、テナントファームで稼働している RAS Connection Broker が行います。Connection Broker は、共有の RAS Secure Gateway によってランダムに選択されます。利用可能な Connection Broker がない場合は、その趣旨のマークが設定され、一定の時間、同じ共有ゲートウェイからの通信が行われなくなります。ゲートウェイは、周期的に Connection Broker の状況を確認し、利用可能になったらすぐに通信を再開します。

テナントブローカーからの切断

テナントをテナントブローカーから切断するには、以下の手順を実行します。

1. テナントファームにログインします。
2. RAS Console で [ファーム] > [サイト] に移動します。
3. [タスク] > [テナントブローカーから離脱する] をクリックします。

テナントがテナントブローカーから切断されます。その結果、テナントユーザーは、テナントブローカー経由でテナントファームに接続できなくなります。

テナントの管理

このセクションでは、以下の内容を説明します。

テナントの構成

テナントブローカーコンソールで既存のテナントのリストを表示するには、[ファーム] > [テナント] を選択します。

[ステータス] 列でテナントの状況を確認できます。値は以下のいずれかです。

- [OK] - テナントはすでに接続していて、確認済みです。
- [未参加] - テナントに対応するテナントオブジェクトはすでに作成されていて、招待ハッシュも生成されていますが、テナントがまだテナントブローカーに接続していません。
- 未確認 - テナントはすでに接続していますが、テナントの RAS Connection Broker との接続がまだ確立されていません。通常、テナントがテナントブローカーに接続した直後は、1 分ほどこのステータスが表示されます。接続が確立されると、状況が [OK] に変わります。

  このステータスは、テナントブローカーがテナントのプライマリ Connection Broker との接続を失ったときにも表示されます。共有ゲートウェイが接続を処理できるのは、テナントの Connection Broker との通信を自力で行える場合に限られます。共有ゲートウェイは、テナントブローカーの Connection Broker からは独立していますが、ユーザー認証のためにテナントの Connection Broker が必要です。
- [無効] - テナントはテナントブローカーの構成で無効になっています。テナントオブジェクトを有効/無効にする方法については、以下の説明を参照してください。

テナントのプロパティを確認したり変更したりするには、[タスク] > [プロパティ] をクリックするか、テナントを右クリックして [プロパティ] を選択します。[プロパティ] ダイアログが表示されます。このダイアログで以下のプロパティを確認したり変更したりできます。

- テナントの有効化: テナントブローカーでテナントオブジェクトを有効/無効にできます。
- 名前: テナント名（一意でなければなりません）。

- パブリックドメインアドレス: エンドユーザーが外部から接続する時の接続先になる固有のアドレス（RAS.tenant.com、tenant1.MSP-FARM.com など）。詳細については、「パブリックドメインアドレスの割り当て」（p. 411）を参照してください。
- ゲートウェイモードのクライアントは、サーバー IP により公開済みのテナントリソースに接続します: このオプションを選択すると、クライアントは DNS 名の代わりにテナント IP アドレスを使用します。このオプションは、テナントファームがテナントブローカーファームと同じ DNS プロバイダーを共有していない場合に使用できます。
- 請求情報を表示しない: （インビテーションハッシュで参加したテナントのみ）これを選択した場合、テナントのライセンスカテゴリー （p.591）に課金情報が表示されなくなります。
- サーバーの IP を使用してゲートウェイ経由のトンネリングでテナントセッションを転送する: 公開リソースをホストしているサーバーにクライアントセッションを転送するときに、サーバー名（FQDN、ホスト名）と IP アドレスのどちらかを使用できます。このオプションを選択すると（デフォルト）、セッションの転送のために内部で IP アドレスが使用されます。このオプションをクリアすると、構成されているホスト名が使用されます。
- 説明: テナントの説明（オプション）。テナントの説明は、テナントブローカーコンソールでだけ閲覧できるプロパティです。
- Connection Broker: テナントファームにインストールされている 1 つ以上の RAS Connection Broker の IP アドレス。これは読み取り専用フィールドです。
- テナント招待ハッシュ: テナントをテナントブローカーに接続したときに使用したハッシュ。これは読み取り専用フィールドです。

テナントオブジェクトの削除

テナントオブジェクトはいつでも削除できます。オブジェクトを削除するには、[タスク] > [削除] をクリックするか、オブジェクトを右クリックして [削除] を選択します。この操作によって、共有の RAS Secure Gateway からテナント構成が削除されるので、ゲートウェイからそのテナントへの RDP セッションを確立できなくなります。テナントの RAS Console では、テナントブローカーのステータスが [切断] と表示されます。テナントブローカーへの参照を完全に削除するには、テナント管理者がテナントブローカーからテナントを切断する（p. 412）必要があります。

テナントコンソールの起動

テナントブローカー管理者は、テナントブローカーコンソールからテナントコンソールを起動できます。そのためには、[ファーム] > [テナント] に移動し、テナントを右クリックして [テナントコンソールを開く] を選択します。RAS Console の新しいインスタンスが起動し、テナントファームにログインするための画面が表示されます。テナントファームでは、リモートコンソール接続を許可する設定を行っておく必要があります。つまり、対応するポートがテナントの Connection Broker で開くようにしておかなければなりません。テナントファーム管理者の資格情報も必要になります。

テナントブローカーコンソールからテナントにログインすると、テナントファームが [ロケーション] ドロップダウンリスト（RAS Console ウィンドウの左上隅）に自動的に追加されるので、[ロケーション] リストから選択するだけでテナントに接続できるようになります。

共有ゲートウェイ

テナントブローカーに存在する RAS Secure Gateway はすべて、テナント間で共有されます。共有ゲートウェイの動作は、標準の RAS Secure Gateway の動作とほぼ同じですが、違いがいくつかあります。その違いを次に説明します。

トンネリングポリシー

トンネリングポリシーを設定できます。トンネリング接続は、使用するパブリックアドレスにマッピングされているテナントファームに送られます。ただし、このポリシーは、[なし] と [サイト内の全サーバー] に限られています。

WYSE

WYSE はサポートされていません。

セッションカウンター

テナントブローカーコンソールでは、共有ゲートウェイごとにセッションカウンターが表示されます。ゲートウェイが実行しているセッションの数を確認するには、[ファーム] > [サイト] に移動し、[ゲートウェイ] セクションの [セッション] 列を調べます。

クライアント接続ルーティング

各共有ゲートウェイは、それぞれの既存テナントの構成を認識していて、テナントファームで稼働している正しい RAS Connection Broker にクライアント接続をルーティングできます。このルーティングは以下の流れで進みます。

1 新しいクライアント接続が確立されます。

2 共有ゲートウェイが、テナントの構成に基づいて、クライアントの所属先のテナントを判別します。

3 この接続のために、テナントファーム内の正しい RAS Connection Broker が選択されます。

4 選択された RAS Connection Broker に二要素認証とアプリケーションリストの要求が転送されます。その後のクライアント操作も、その Connection Broker によって行われます。「ユーザー認証」（p. 412）も参照してください。

共有ゲートウェイの保守

共有の RAS Secure Gateway を保守作業のためにオフラインにする必要があるときには、従来の Parallels RAS ファームの場合と同じ要領でその操作を実行できます。ゲートウェイを無効にしてから、アクティブセッションがなくなるのを待ちます。ゲートウェイのアクティブセッションの数を確認するには、[ファーム] > [サイト] に移動します。セッションカウントが [セッション] 列に表示されます。

共有ゲートウェイを安全にオフラインにできます。Parallels Client は、同じセッションに自動的に再接続します。

サードパーティのネットワークロードバランサー

サードパーティのネットワークバランサーを共有の RAS Secure Gateway と併用する方法は、従来の（共有ではない） RAS Secure Gateway と併用する場合と同じです。

Web Client とテーマ

RAS マルチテナントアーキテクチャの重要な機能の 1 つは、テーマの使用に関する機能です。共有のユーザーポータル（RAS Secure Gateway の一部）をすべてのブラウザーベースの接続で使用しながら、テナント側で定義されているテナント固有の Web Client テーマを使用できるようになっています。従ってサービスプロバイダーは、テナントごとに固有のカスタムテーマを作成してホワイトレーベルを実装できます。

Web Client テーマは、テナントファームで作成します。ユーザーインターフェイスや機能は、従来の Parallels RAS ファームの場合と同じです。テナントがテナントブローカーに接続すると、そのテナントの RAS Connection Broker からテーマが取り込まれ、それぞれの共有の RAS Secure Gateway の構成にそのテーマが追加されます。

Web Client 経由でテナントファームに接続する場合は、ゲートウェイのアドレスではなくテナントのパブリックドメインアドレスを入力する必要があります。そうすると、共有ゲートウェイによって正しいテーマが使用されます。

- ユーザーがデフォルトの URL（https://<public-tenant-address>）を入力した場合は、デフォルトのテナントテーマが使用されます。
- ユーザーがテナントのアドレスの後にテーマ名を追加した場合は（https://<public-tenant-address>/<Theme-name>）、そのテーマが使用されます。

Web Client の構成

Web Client は通常、RAS Secure Gateway のレベル（ゲートウェイの [プロパティ] ダイアログの [ユーザーポータル] タブ）で構成します。テーマを構成するときに、テナントファーム内で特定のテーマのゲートウェイ設定を指定して、ゲートウェイ設定を上書きすることも可能です。そのためには、テナントの RAS Console でテーマを選択し、プロパティを開いて、[ゲートウェイ] カテゴリを選択します。そのカテゴリで独自の設定を指定できます。詳細については、「Web Client テーマ設定」 >「Secure Gateway」（p. 459）を参照してください。

テナントブローカーでのテナントテーマの表示

テナントブローカー管理者は、テナントブローカーコンソールからテナントテーマを表示できます。

1 テナントブローカーコンソールで [ファーム] > [テナント] を選択します。

2 テナントを選択し、[タスク] > [テナントのテーマを表示する] をクリックします。

3 表示されるダイアログでテーマを表示できます。テナントから取り込まれて、テナントブローカーのすべての RAS Secure Gateway の構成に追加されたテーマです。

この機能を使用すれば、テナントブローカーの側ですべてのテナントテーマを正しく同期できます。そうすれば、ユーザーがテナントブローカー経由でテナントに接続するときに、正しいテーマが使用されます。

テナントの監視

Parallels RAS Performance Monitor は、Parallels RAS の展開環境のボトルネックやリソース使用状況を分析するための RAS コンポーネントです。RAS Performance Monitor を使用すれば、テナントブローカーコンソールでテナントを監視して、それぞれのパフォーマンスメトリックを表示できます。

テナントの情報を収集できるように RAS Performance Monitor を構成するには、以下の手順を実行します。

1 RAS Performance Monitor をインストールします。方法については、「Parallels RAS Performance Monitor」の章（p. 559）を参照してください。

2 テナントブローカーコンソールにログインします。

3 コンソールで [管理] > [報告] に移動します。

4 [RAS Performance Monitor を有効にする] オプション（[RAS Performance Monitor の構成] セクション）を選択します。

5 [サーバー] フィールドと [ポート] フィールドで、RAS Performance Monitor のインストール先のサーバーの名前または IP アドレスを指定します。

6 [適用] をクリックします。

7 テナントコンソールを開いて、上記の手順 3 から 6 を繰り返し、テナントブローカーとテナントの両方が同じ RAS Performance Monitor を使用するように構成します。そうすれば、テナントがパフォーマンスデータを RAS Performance Monitor に送信したときに、テナントブローカーの側でもそのデータを確認できます。

テナントが統計データを RAS Performance Monitor に送信すると、テナントブローカーコンソールでそのデータを表示できます。RAS Performance Monitor ダッシュボードでデータを表示

するときには、ファームとサイトを切り替えて特定のテナントを選択し、そのテナントのパフォーマンスメトリックを確認することも可能です。

テナントブローカーの互換性と更新

Parallels RAS を新しいバージョンに更新する場合、RAS マルチテナントアーキテクチャには次のルールが適用されます。

- Parallels RAS テナントブローカーは、最大で 2 つ前の RAS メジャーバージョンまで、古いテナントをサポートします。たとえば、RAS テナントブローカーを RAS 17 から RAS 18（または利用可能になった次のメジャーバージョン）にアップグレードすると、Parallels RAS 17 を実行しているテナントがサポートされます。
- 更新を行うときは、最初にテナントブローカーを更新して、RAS マルチテナントのインストールが完全に機能するようにする必要があります。テナントは、後で独自のメンテナンスウィンドウで更新できます。

旧バージョンの RAS からのアップグレード

RAS v16.x を実行する既存のファームをテナントとしてテナントブローカーに接続するには、以下の手順を実行します。

1. ファームを RAS 17.1 以降にアップグレードします。
2. ファームをテナントとしてテナントブローカーに接続する方法については、「テナントブローカーとテナントの展開」セクション（p. 402）を参照してください。
3. ローカル接続のためにローカルの RAS Secure Gateway を使用する計画がなければ、ファームの接続後に削除して構いません。その他の情報については、「実装の概要」（p. 399）を参照してください。

通知の構成

システムイベント通知は、システムイベントをメールによって RAS 管理者に知らせる機能です。[ファーム] > [サイト] > [設定] > [通知] でシステムイベント通知を構成できます。この機能の詳細については、「システムイベント通知」（p. 594）を参照してください。このセクションでは、テナントブローカーとテナントに関する通知を取り上げます。

テナントイベント通知

テナントブローカー管理者は、以下のテナントイベントに関する通知を受け取れます。

- 新しいテナントの登録: 新しいテナントがテナントブローカーに登録されたときに発生します。
- テナントがブローカーから離脱: 登録済みのテナントがテナントブローカーから離脱したときに発生します。
- テナントステータスのアラート: テナントファームの RAS Connection Broker がオフラインになったときに発生します。

テナントイベントが発生すると、テナントブローカー管理者は、以下の情報を含むメールを受け取ります（情報はイベントのタイプによって異なります）。

- テナント名。
- テナントブローカー名。
- テナントの登録方法（招待ハッシュまたは秘密鍵）。
- テナントのステータス。
- 日付。

テナント通知を有効にするには、以下の手順を実行します。

1. テナントブローカーにログインします。
2. RAS Console で、[ファーム] > [サイト] > [設定] > [通知] に移動します。
3. [通知ハンドラー] セクションで、[タスク] > [新規] > [テナントイベント] をクリックします。
4. [テナントイベント通知ハンドラーのプロパティ] ダイアログで以下の項目を指定します。
   - [一般] タブで [RAS 管理者にメールを送信] オプションを選択し、メールアドレスを指定します。複数指定する場合は、セミコロンで区切ってください。
   - [設定] タブで、[デフォルト設定を使用] オプションを選択するか（サイトのデフォルトを使用する場合）、そのオプションをクリアして独自の設定を指定します。
5. [OK] をクリックし、設定を保存してダイアログを閉じます。

テナントブローカーイベント通知

テナントファーム管理者は、テナントブローカーが使用不可の状態になったときに通知を受け取れます。その状態になるのは通常、テナントブローカーの RAS Connection Broker がオフラインになったときです。この通知ハンドラーの構成方法は上記の方法と同じですが、この場合はテナントブローカーではなくテナントファームで構成します。

共通のイベント通知

テナントイベントのハンドラー以外に、共通のイベント（CPU 使用率、メモリ使用率、RAS Agent イベントなど）に関する通知も構成できます。ただしテナントブローカーになる際の制限として、テナントブローカーでは、限られたシステムイベントの通知ハンドラーしか構成できないというものがあります（この後に記す使用可能なハンドラーのリストを参照）。テナントブローカーには、RD セッションホスト、プロバイダー、ライセンス制限、公開リソースなどがないからです。一方、テナントファームには通知ハンドラーが完全にそろっているので、テナント管理者はその種の通知ハンドラーも構成できます。

テナントブローカーでは以下の通知ハンドラーを使用できます。

- CPU 使用率
- メモリ使用率
- ゲートウェイでトンネリングされたセッション数
- ゲートウェイでトンネリングされたセッションの失敗
- RAS Agent イベント

その他の情報については、「システムイベント通知」（p. 594）を参照してください。

通信ポート

テナントブローカーとテナントは、以下のポートを使用して相互に通信します。

- テナントの Connection Broker > テナントブローカーの Connection Broker: ポート 20003
- テナントブローカーのゲートウェイ > テナントブローカーの Connection Broker: ポート 20002
- テナントブローカーのゲートウェイ > テナントの Connection Broker: ポート 20002

- テナントブローカーのゲートウェイ > 公開リソースをホストしているサーバー: ポート 3389

上記のポートはどれも標準の RAS ポートです。詳細については、「ポート参照」セクションを参照してください。

第　18　章

SAML SSO 認証

Parallels RAS 17.1 以降では、Security Assertion Markup Language（SAML）認証メカニズムがサポートされています。SAML は XML ベースの認証です。組織同士の間でシングルサインオン（SSO）機能を利用できるので、ローカルの ID データベースを共有しないでユーザー認証を行うことが可能になります。

この SAML SSO プロセスでは、新しい RAS 登録サーバーが Microsoft 認証局（CA）と通信し、ユーザーに代わってデジタル証明書をリクエストしたり登録したり管理したりするので、ユーザーが認証のために自分の Active Directory 資格情報を入力する必要はありません。サービスプロバイダーも、多くの子会社を抱える大企業も、内部の ID 管理ソリューションを維持したり、ドメイン/フォレストの複雑な信頼関係を構築したりする必要はありません。サードパーティの ID プロバイダーとの統合によって、顧客やパートナーがエンドユーザーに快適な SSO 環境を提供することも可能になります。

この章の内容

はじめに

Security Assertion Markup Language（SAML）は XML ベースの認証です。組織同士の間でシングルサインオン（SSO）機能を利用できるので、ローカルの ID データベースを共有しないでユーザー認証を行うことが可能になります。Parallels RAS 17.1 以降では、SAML 認証メカニズムがサポートされています。

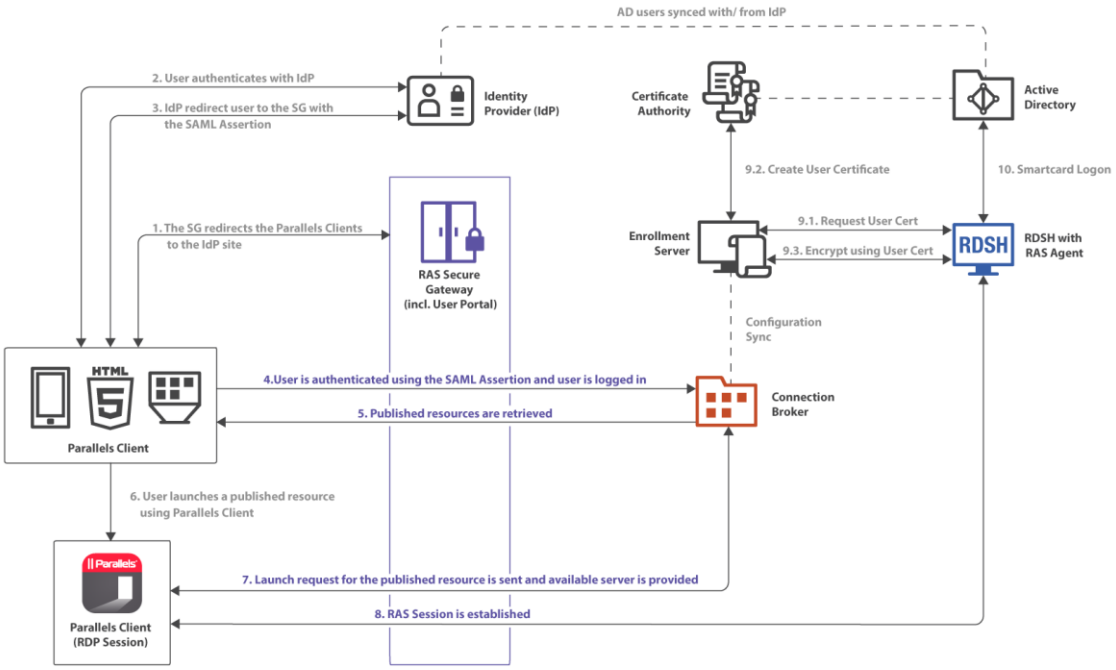
Parallels RAS 17.1 で導入された SAML（2.0）SSO は、HTML5 を介した認証をサポートし、Web Client または Parallels Client for Windows を使用できます。Parallels RAS 18 は、OS 標準のブラウザー、または Parallels Client に組み込まれたブラウザーの使用など SAML 認証を開始するクライアントのサポートを拡張します。

この SAML SSO プロセスでは、新しい RAS 登録サーバーが Microsoft 認証局（CA）と通信し、ユーザーに代わってデジタル証明書をリクエストしたり登録したり管理したりするので、ユーザーが認証のために自分の Active Directory 資格情報を入力する必要はありません。サービスプロバイダーも、多くの子会社を抱える大企業も、内部の ID 管理ソリューションを維持したり、ドメイン/フォレストの複雑な信頼関係を構築したりする必要はありません。サードパーティの ID プロバイダーとの統合によって、顧客やパートナーがエンドユーザーに快適な SSO 環境を提供することも可能になります。

サポートされている提供オプションは以下の通りです。

- Web Client
- Windows の Web Client で SAML を起点として利用する
- Mac および Linux の Web Client で SAML を起点として利用する
- Android、iOS および iPadOS の Web Client で SAML を起点として利用する
- Parallels Client for Windows で SAML 認証を起点として利用する
- Parallels Client for Mac で SAML 認証を起点として利用する
- Parallels Client for Linux で SAML 認証を起点として利用する
- Parallels Client for iOS/iPadOS で SAML 認証を起点として利用する
- Parallels Client for Android で SAML 認証を起点として利用する

以下の概要レベルの論理ダイアグラムは、Parallels RAS 環境内の SAML 認証およびログインプロセスを示しています。



上図の SAML 認証およびログインの手順は以下の通りです。

1 RAS Secure Gateway は Parallels Client のログイン要求を IdP サイトにリダイレクトします。

2 ユーザー認証が IdP で行われます。

3 IdP はユーザーを SAML アサーションを使用して RAS Secure Gateway にリダイレクトします。

4 SAML アサーションを使用してユーザーが認証され、ユーザーはログインします。

5 利用可能な RAS の公開済みリソースのリストを取得します。

6 ユーザーは公開済みリソースを選択し、Parallels Client から起動します。

7 ユーザーからの起動要求がサーバー側に送信され、利用可能なサーバー上でリソースが起動されます。

8 Parallels RAS セッションが確立されます。

9 ユーザーの証明書が次のように処理されます。

- 証明書が要求されます。
- 証明書が作成されます。
- 証明書を使用して暗号化が行われます。

10 スマートカードでログオンします。

システム要件

RAS 登録サーバー

- Windows Server 2012 R2 から Windows Server 2022 まで

RD セッションホスト

- Windows Server 2012 R2（x64 ビットバージョン）から Windows Server 2022 まで

デスクトップオペレーティングシステム（ゲスト VM とリモート PC）

- Windows 7 から Windows 11 まで

32 ビットのオペレーティングシステムはサポートされていません。

Parallels Client

- Parallels Client バージョン 18 または 19 が必要です。
- サポート対象プラットフォームは Windows、Mac、Linux、iOS、Android です。

SAML の基礎

Security Assertion Markup Language（SAML）は、ID プロバイダーとサービスプロバイダーが認証情報をやりとりするための標準規格です。SAML 認証はシングルサインオンのメカニズムであり、中央の ID プロバイダー（IdP）がユーザー認証を行う一方で、サービスプロバイダー（SP）は、認証の結果に基づいてアクセス制御だけを行うという仕組みです。

SAML 認証の主なメリットを以下にまとめます。

- サービスプロバイダーが独自のユーザーデータベースを維持する必要はありません。ユーザー情報は、ID プロバイダー側の中央データベースで保管されます。ユーザーの追加や削除が必要になった場合でも、1 つのデータベースで操作を行うだけで十分です。
- サービスプロバイダーは、ユーザー確認を独自に行わなくてよいので、 サービスプロバイダーの側でセキュアな認証を実装する必要がありません。
- シングルサインオンなので、ユーザーのログオンは 1 回だけで済みます。その後のサインオン（ユーザーが別のアプリケーションを起動するときのサインオン）はすべて自動的に行われます。
- サインインのときにユーザーが資格情報を入力する必要はありません。
- ユーザーがパスワードを記憶したり更新したりする必要はありません。
- 脆弱なパスワードが存在しません。

シングルサインオンのプロセス

SAML シングルサインオンは、サービスプロバイダーの側からも、ID プロバイダーの側からも開始できます。その 2 つのシナリオを以下にまとめます。

サービスプロバイダーの側から SAML シングルサインオンのプロセスを開始する場合は、以下のような流れになります。

1. ユーザーは Parallels Client（サポートされているバージョンのいずれか）（p. 426）を開き、サービスプロバイダーに接続します。
2. サービスプロバイダーが ID プロバイダーにメッセージを送り、ユーザー認証を依頼します。
3. ID プロバイダーがユーザーにユーザー名とパスワード入力を求めます。
4. ユーザーの資格情報が正しければ、認証応答（アサーション）がクライアントに送られ、その後サービスプロバイダーに渡されます。その応答には、ユーザーのログインが成功したことや、ID プロバイダーがアサーションに署名したことを示すメッセージが含まれています。
5. ユーザーに公開アプリケーションのリストが表示されます。ユーザーがアプリケーションを起動するときに、資格情報を入力する必要はありません。

ID プロバイダーの側からシングルサインオンを開始する場合の基本的な流れは、以下の通りです。

1 ユーザーがウェブブラウザーから ID プロバイダーにログインすると、社内向けアプリケーション（Parallels RAS など）のリストが表示されます。

2 Parallels RAS を選択すると、アサーションがクライアントに送られ、その後 Parallels RAS で設定されているサービスプロバイダーに渡されます。

3 ユーザーに RAS の公開アプリケーションのリストが表示されます。

4 ユーザーがアプリケーションを起動するときに、資格情報を入力する必要はありません。

SAML の構成

このセクションでは、以下の内容を説明します。

前提条件

Parallels RAS で SAML を構成するには、以下のものが必要です。

1 以下の 2 つのユーザーアカウントが存在する Microsoft Active Directory。

- 登録エージェントユーザー: 認証ユーザーの代わりに RAS 登録サーバー（ES）によって証明書を登録するときに使用します。
- NLA ユーザー: RD セッションホストや VDI ゲストとの NLA 接続を開始するときに使用します。

必要な権限や委任については、「Active Directory のユーザーアカウントの設定」（p. 434）を参照してください。Azure Active Directory Domain Services（AADDS）は、SAML SSO との併用には対応していないことに注意してください。

2 以下のテンプレートが含まれている Microsoft エンタープライズ認証局（CA）。

- 登録エージェント証明書テンプレート
- スマートカードログオン証明書テンプレート

3 サードパーティの ID プロバイダー（IdP）（Azure、Okta、Ping Identity、Gemalto SafeNet など）。ここでユーザーアカウントが保管されます。IdP にあるユーザーアカウントは、Microsoft Active Directory 環境と同期していなければなりません。ユーザーを正しく同期する方法については、プロバイダーに問い合わせてください。

4 ドメインコントローラーには、ドメインコントローラー証明書が必要です。ドメインコントローラーにある証明書は、スマートカード認証をサポートしていなければなりません。証明書を作成するときには、”ドメインコントローラーの認証”という名前の Microsoft CA 証明書テンプレートを使用します。手動で作成したドメインコントローラー証明書は、正しく機能しないことがあります。”要求はサポートされていません”というエラーが表示される場合は、ドメインコントローラー証明書を再作成しなければならない可能性があります。信頼されているルート認証局のストアに含まれている CA から発行されたルート証明書が RD セッションホストと VDI にあることを確認してください。

5 64 ビットの OS で稼働する RD セッションホストや VDI のワークロードがある Parallels RAS ファーム。

6 セキュリティ上の理由から、RAS 登録サーバーを専用のホストにインストールすることをお勧めします。ホストは、他のコンポーネントやロールがインストールされていないスタンドアロンのサーバーでなければなりません。

7 SAML の構成と RAS 登録サーバーの構成はどちらも、RAS 環境内のサイトごとの設定になります。RAS 管理者は、”サイト情報の表示を許可”と”サイトの変更を許可”の権限の委任を受けていなければなりません。

注: 上記のタスクの中には、Microsoft Active Directory とグループポリシーの設定に関する知識が必要になるタスクもあります。

Azure Active Directory Domain Services（AADDS）および Azure Virtual Desktop へのアクセスは、現在 Parallels RAS SAML SSO でサポートされていません。

IdP 側の構成

ID プロバイダーの側では、以下の手順を実行する必要があります。

1 対象の IdP プラットフォームにログインし、Parallels RAS 環境で使用する SAML ベースの汎用のアプリケーションまたは RAS 固有のアプリケーションを作成します。

2 そのアプリケーションを構成し、後で Parallels RAS に追加する以下の構成プロパティをメモします。

- エンティティ ID
- ログオン URL
- ログアウト URL
- 証明書（base64）

3 あるいは、メタデータファイルをエクスポートして Parallels RAS にインポートするという方法もあります。詳細については、「IdP の例とヒント」を参照してください。

SP 側の構成（RAS 側）

サービスプロバイダー側（Parallels RAS 側）では、ウェブ（SAML）認証を有効にして、ID プロバイダーを RAS ファームに追加する必要があります。

ウェブ（SAML）認証の有効化

1 RAS Console で [接続] > [認証] に移動します。

2 [許可された認証タイプ] セクションで [ウェブ（SAML）] オプションを選択します。

IdP を RAS ファームに追加する方法

IdP を追加するには、以下の手順を実行します。

1 RAS Console で [接続] > [SAML] に移動します。タブページが無効になっている場合は、ウェブ（SAML）が有効になっていることを確認してください上記を参照してください。

2 [タスク] > [追加] をクリックします。

3 [ID プロバイダーの追加] ウィザードでプロバイダーの名前を指定します。

4 [テーマと一緒に使用する] ドロップダウンリストで、IdP に割り当てる [テーマ]（p. 455）を選択します。まだテーマがない場合は、デフォルトのテーマを使用するか、[<使用しない>] を選択して後からテーマを指定できます。同じ RAS ファームに複数の IdP を構成することは可能です。ただし、1 つのテーマには 1 つの IdP しか割り当てられません。

5 ウィザードで IdP 情報を取得するための方法を選択してください。

- 公開済み IdP メタデータのインポート: インターネット上に公開されている XML 文書からインポートします。IdP 側の構成から取得した文書の URL を指定してください。

- ファイルから IdP メタデータをインポートする: IdP アプリケーションからダウンロードしたローカル XML ファイルからインポートします。該当するフィールドでファイル名とパスを指定してください。
- IdP 情報を手動で入力します: このオプションを選択すると、ウィザードの次のページで情報を手入力できます。

6 [次へ] をクリックします。

7 前の手順で構成をインポートした場合は、XML ファイルから取得したデータが次のページに取り込まれます。IdP データを手動で入力するオプションを選択した場合は、次の値を自分で入力してください。

- IdP エンティティ ID: ID プロバイダーのエンティティ ID。
- IdP 証明書: ID プロバイダーの証明書データ。このフィールドに値を設定するには、IdP 側から証明書をダウンロードし、ダウンロードしたファイルを開き、その内容をコピーしてこのフィールドに貼り付けます。
- ログオン URL: ログオン URL。
- ログアウト URL: ログアウト URL。

必要に応じて、[暗号化されていないアサーションを許可する] オプションを選択します。

注: デフォルトでは、[暗号化されていないアサーションを許可する] オプションは無効になっています。IdP 構成でアサーションの暗号化が設定されていることを確認するか、RAS 構成内でデフォルト設定を変更してください。

8 この時点で、IdP 側（IdP ポータル）でインポートするサービスプロバイダー（SP）の構成を行います。今すぐに行うことも、後で行うこともできます。今すぐに行うには、以下の手順に従います。後で実行するには、[完了] をクリックし、必要になったときに、ID プロバイダーオブジェクトのプロパティを開き、[SP] タブを選択して、以下に説明するのと同じ手順を実行します。

9 SP の設定を行うには、[サービスプロバイダー情報] ボタンをクリックします。

10 ダイアログが開いたら、ホストアドレスを入力してください。IdP がそのアドレスにリダイレクトされるので、そのアドレスは、エンドユーザーのブラウザーからアクセスできるアドレスでなければなりません。

11 その他のフィールド（[SP エンティティ ID]、[リプライ URL]、[ログオン URL]、[ログアウト URL] など）には、ホストアドレスに基づく値があらかじめ設定されています。SP 証明書が自動生成されます。

12 次に、上記の値に基づいて IdP 構成を完成させます。値を手動でコピーすることも、メタデータファイル（XML）としてエクスポートすることも可能です。[SP メタデータをファイルにエクスポート] リンクをクリックします。メタデータを XML ファイルとして保存します。その XML ファイルを IdP にインポートします。

13 ダイアログを閉じて、[完了] をクリックします。

ユーザーアカウントの属性の構成

IdP でユーザー認証が実行されると、Active Directory にあるユーザーアカウントの属性が、IdP のユーザーデータベースにある対応属性と比較されます。どの属性を比較するかを構成できます。その方法については、下記の説明を参照してください。

使用可能な属性を次の表にまとめます。

RAS 名	SAML 名 *	AD 名	説明
UserPrincipalName	NameID	userPrincipalName	ユーザープリンシパル名（UPN）は、電子メール形式のシステムユーザー名です。
Immutable ID	ImmutableID	objectGUID	UUID（Universally Unique Identifier）。
SID	SID	objectSid	ObjectSID には、ドメインを一意に識別するドメインプレフィックス ID と、ドメイン内のセキュリティプリンシパルを一意に識別する相対 ID （RID）が含まれています。
sAMAccountName	sAMAccountName	sAMAccountName	sAMAccountName 属性は、旧バージョンの Windows（Windows NT 4.0 など）のクライアントとサーバーをサポートするために使用するログオン名です。
カスタム	メールアドレス	メール	カスタム属性を使用して、SAML 属性名を AD 属性値にマッチングできます。デフォルトではメールアドレスになります。

* [SAML 名] 列の属性は編集可能で、使用している IdP に基づいてカスタマイズできます。

属性を構成するには、以下の手順を実行します。

1 RAS Console で、前の手順で追加した IdP を右クリックします。

2 IdP の [プロパティ] ダイアログで [属性] タブを選択します。このタブで、比較用の属性を選択したりクリアしたりできます。カスタム属性を作成することも可能です。

- 選択した属性が比較されます。
- 必要に応じて、あらかじめ構成されているどの SAML 属性（IdP 側）の名前も、AD 属性に合わせて変更できます。
- カスタム属性を使用して、任意の SAML 属性名をどの AD 属性値に対してもマッチングできます。デフォルトではメールアドレスになります。

3 必要に応じて、IdP 側で構成されている属性に基づいて対象の属性を構成して有効にします。

4 [OK] をクリックして、ダイアログを閉じます。

注 1: 属性が複数ある場合は、表示順で使用されます。1 つの属性が失敗した場合は、次に構成されている属性が使用されます。属性は 1 つずつ（「どちらか 1 つ」という方法で）使用されます。

注 2: 複数の AD ユーザーで同じ AD 属性が構成されていると、ユーザーのマッチングが失敗します。例えば、メールアドレス属性を選択した場合に、複数の AD ユーザーが同じメールアドレスを持っていると、IdP アカウントと AD ユーザーアカウントの間の属性のマッチングは失敗します。

属性の構成に関するヒント

- 可能なら、Active Directory と IdP の間のユーザー同期のために自動処理機能（Azure IdP 構成用の Microsoft Azure AD Connect など）を使用して、ユーザー識別管理のオーバーヘッドを最小化してください。
- 使用中の環境で固有のユーザー識別属性を選択します。可能なら、ユーザープリンシパル名（UPN）や Immutable ID（ObjectGuid）を使用してください。メールアドレスなどの固有の識別情報を使用することも可能です。その場合は、AD でユーザーオブジェクトの [メールアドレス] フィールドが構成されていることを確認してください。Microsoft Exchange Server を使用している場合は、[Exchange アドレス] タブと Exchange ポリシーを使用してください。
- UPN を属性として使用する場合は、代替 UPN サフィックスも構成できます。この構成は、[Active Directory ドメインと信頼関係] で作成可能です（root ＞ 右クリックで [プロパティ] ダイアログを開く）。新しい代替 UPN サフィックスを作成した後、Active Directory ユーザーとコンピューターから、ユーザーオブジェクトのプロパティで、UPN を変更できます。

アカウントの写真を追加する

Single SignOn でユーザーがログインする際に Windows ログオン画面に表示されるカスタムアカウント画像を追加して、パーソナライズ機能を強化できます。手順の詳細については、https://kb.parallels.com/en/129028 を参照してください。

Active Directory のユーザーアカウントの構成

Microsoft Active Directory で登録エージェントユーザーと NLA ユーザーを作成する必要があります。ここでは、それらのユーザーの作成方法を説明します。

登録エージェントユーザーアカウント

登録エージェントユーザーアカウントは、認証ユーザーの代わりに RAS 登録サーバーによって証明書を登録するために必要です。登録エージェントのユーザーには、RAS 登録サーバーエージェントがインストールされているマシンのログオン権限が必要です。

NLA ユーザーアカウント

NLA ユーザーは、RD セッションホストや VDI ゲストとの NLA 接続を開始するときに必要になります。NLA ユーザーには、セッションホストへのログオン権限が必要です。

NLA ユーザーは、Remote Desktop Users グループのメンバーでなければならず、このユーザーには [リモートデスクトップサービスを使ったログオンを許可] の権限を与える必要があります。その一方で、NLA ユーザーに対して、リモートデスクトップサービスを使ったログオンを禁止しなければなりません。

NLA ユーザーアカウントを除外するために、ユーザー権限、[リモートデスクトップサービスを使ったログオンを拒否] をそのアカウントに割り当ててください。

その両方の目的を達成するために、ローカルまたはドメインの GPO（OU またはドメイン全体にリンクした GPO）を使用できます。

このポリシー設定を有効にするために、デバイスを再起動する必要はありません。アカウントのユーザー権限の割り当てを変更すると、そのアカウントの所有者が次回ログオンしたときに、その変更が有効になります。

グループポリシー設定は、GPO によって以下の順序で適用され、その結果、グループポリシーの次回の更新時にローカルコンピューターの設定が上書きされます。

1 ローカルポリシー設定

2 サイトポリシー設定

3 ドメインポリシー設定

4 OU ポリシー設定

以下のようにして、新しい GPO を作成するか、既定のドメインポリシー GPO を使用します。

1 グループポリシー管理コンソール（GPMC）を開きます。

2 RDSH オブジェクトまたは VDI オブジェクトが入っている OU にリンクされている GPO を開くか、作成します。

3 [コンピューターの構成] > [Windows の設定] > [セキュリティの設定] > [ローカルポリシー] > [ユーザー権利の割り当て] に移動し、[リモートデスクトップサービスを使ったログオンを許可] オプションを開きます。

4 ユーザーまたはグループを追加し、NLA ユーザーを追加し、[OK] をクリックします。

注: このオプションによって既定の設定が上書きされるので（ワークステーションとサーバーでは管理者とリモートデスクトップユーザー、ドメインコントローラーでは管理者）、ローカル管理者グループやドメイン管理者グループなどを忘れずに追加してください。

5 [コンピューターの構成] > [Windows の設定] > [セキュリティの設定] > [ローカルポリシー] > [ユーザー権限の割り当て] に移動し、[リモートデスクトップサービスを使ったログオンを拒否] オプションを開きます。

6 ユーザーまたはグループを追加し、NLA ユーザーを追加し、[OK] をクリックします。

認証局テンプレートの構成

このセクションでは、以下の内容を説明します。

- 「登録エージェントテンプレートの作成」（p. 435）
- 「スマートカードログオン証明書テンプレートの作成」（p. 440）

登録エージェントテンプレートの作成

登録エージェントテンプレートを作成するには、以下の手順を実行します。

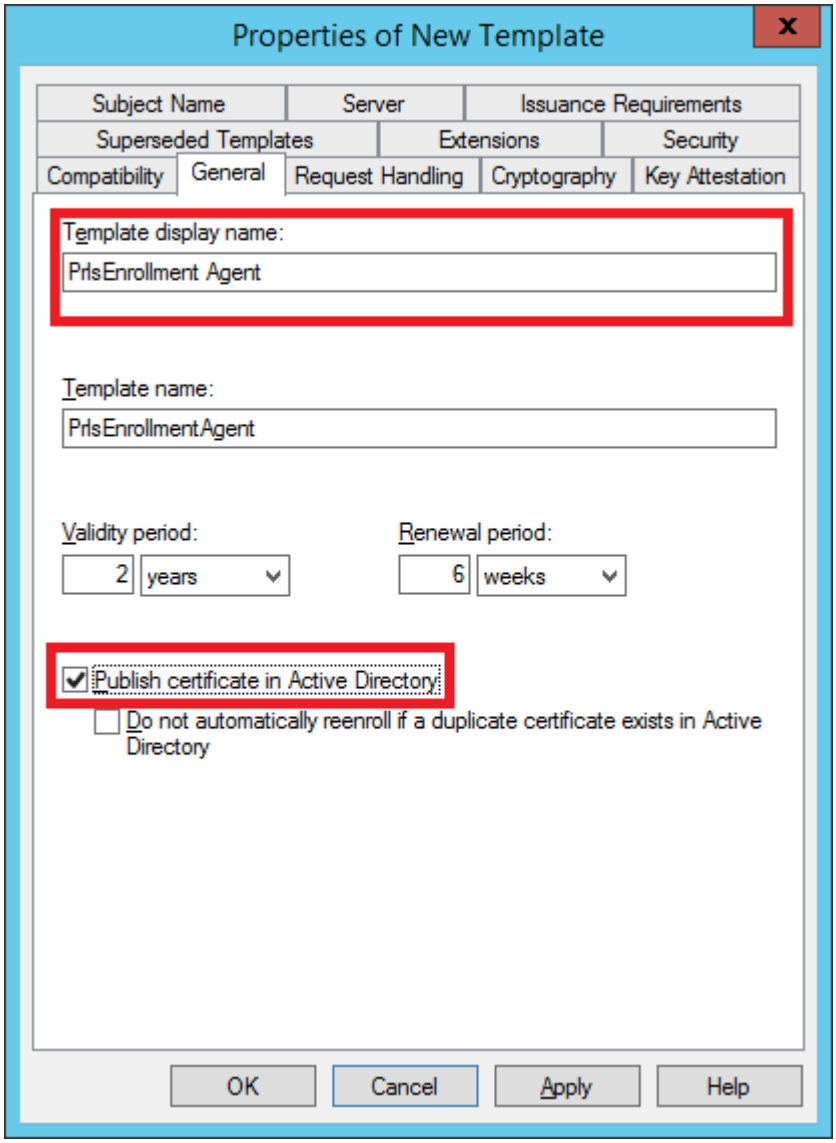
1 認証局サーバーの管理ツールから認証局管理コンソール（MMC）を起動します。

2 CA を展開し、[証明書テンプレート] フォルダーを右クリックし、[管理] を選択します。

3 登録エージェントテンプレートを右クリックして [テンプレートの複製] を選択します。新しいテンプレートプロパティウィンドウが表示されます。[全般] タブで以下のプロパティを構成します。

- テンプレート表示名: PrlsEnrollmentAgent
- テンプレート名: PrlsEnrollmentAgent
- 有効期間: 2 年以内
- 更新期間: 6 週間
- Active Directory の証明書を発行する: ON
- Active Directory に重複する証明書がある場合、自動的に再登録しない: OFF

注: 表示名はどんな名前でも構いませんが、テンプレート名は上記の名前にする必要があります。



4 [暗号化] タブを選択して、以下の値を設定します。

- プロバイダーのカテゴリ: レガシ暗号化サービスプロバイダー（読み取り専用）
- アルゴリズム名: CSP によって設定
- 最小キーサイズ: 2048

[要求で使用できる暗号化サービスプロバイダーを選択してください] セクションで [以下のプロバイダーのうちいずれか 1 つ] を選択します。以下のプロバイダーリストに含まれて

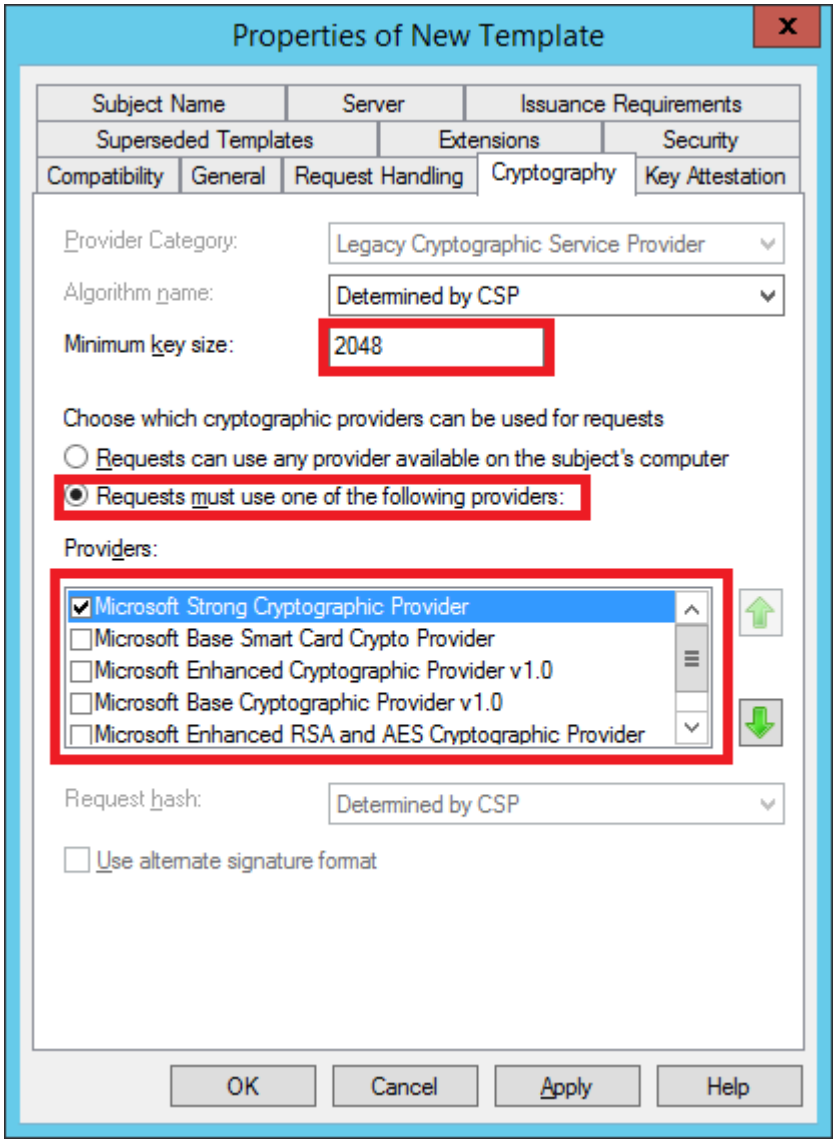
いる [Microsoft Strong Cryptographic Provider] 以外のすべてのオプションをクリアし、そのプロバイダーを優先プロバイダーとして設定します。

[X] Microsoft Strong Cryptographic Provider

[ ] Microsoft Enhanced Cryptographic Provider v 1.0

[ ] Microsoft Base Cryptographic Provider v 1.0

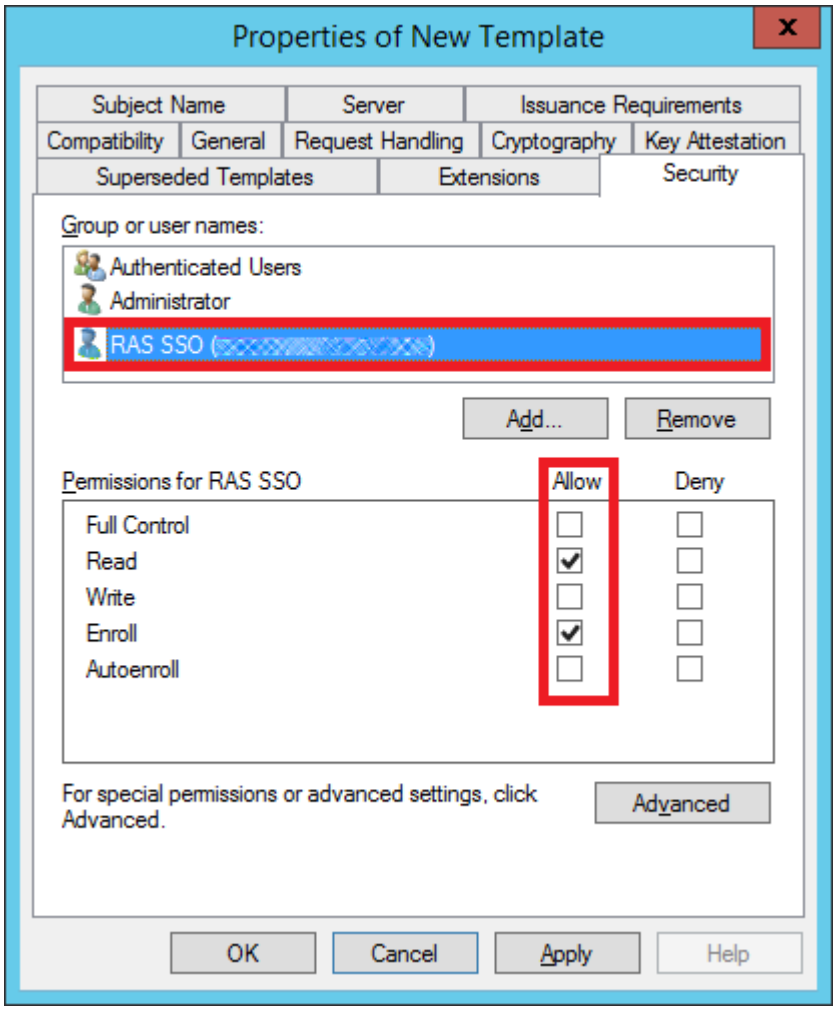
[ ] Microsoft Enhanced RSA and AES Cryptographic Provider



5 [セキュリティ] タブを選択して、以下の手順を実行します。

- [追加] をクリックします。

- 登録エージェントユーザーアカウントを追加します。
- ”読み取り”と”登録”のアクセス許可を選択します。[適用] をクリックし、[OK] をクリックします。



証明書テンプレートの発行

作成した証明書テンプレートを発行するには、以下のようにします。

1 認証局を再び実行し、[証明書テンプレート] を右クリックして [発行する証明書テンプレート] をクリックします。

2 前の手順で作成した証明書テンプレート（Prls Enrollment Agent）を選択して、[OK] をクリックします。

3 その証明書テンプレートが [証明書テンプレート] リストに表示されます。

注: 登録エージェントテンプレートとスマートカードログオンテンプレート（後述）を作成したら、Windows で [Active Directory 証明書サービス] サービスを再起動する必要があります。

スマートカードログオン証明書テンプレートの作成

スマートカードログオン証明書テンプレートを作成するには、以下の手順を実行します。

1 認証局サーバーの管理ツールから認証局管理コンソール（MMC）を起動します。

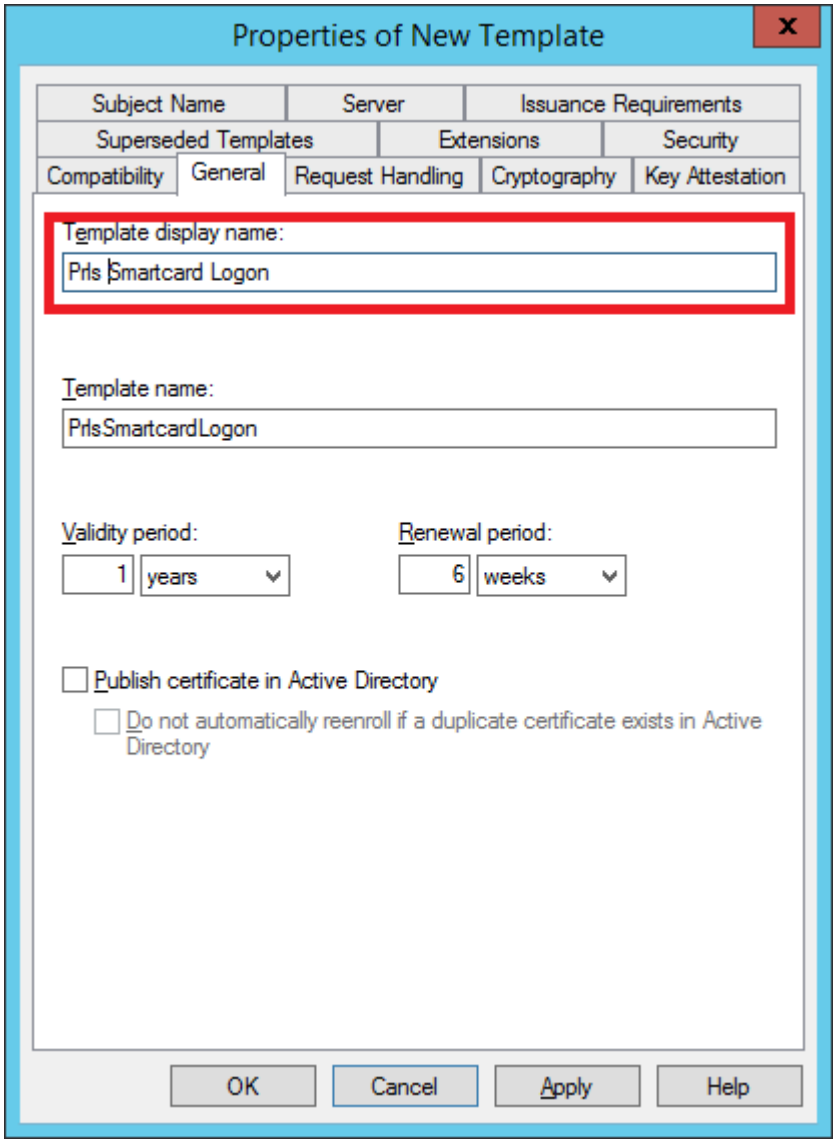
2 CA を展開し、[証明書テンプレート] フォルダーを右クリックし、[管理] を選択します。

3 ”スマートカードログオン”証明書テンプレートを右クリックして [複製] を選択します。

4 新しいテンプレートプロパティが [全般] タブに表示されます。テキストボックスにテンプレート名を入力します。スペースのない実際の名前が 2 番目のテキストボックスに自動的に表示されます。その名前を覚えてください。後で SAML 機能を構成するときにその名前が必要になります。このタブのオプションを以下のように構成してください。

- テンプレート表示名: PrlsSmartcardLogon
- テンプレート名: PrlsSmartcardLogon
- 有効期間: 1 年以内
- 更新期間: 6 週間
- Active Directory の証明書を発行する: OFF
- Active Directory に重複する証明書がある場合、自動的に再登録しない: OFF

注: 表示名はどんな名前でも構いませんが、テンプレート名は上記の名前にする必要があります。



5 [暗号化] タブを選択して、以下の値を設定します。

- プロバイダーのカテゴリ: レガシ暗号化サービスプロバイダー（読み取り専用）
- アルゴリズム名: CSP によって設定
- 最小キーサイズ: 2048

[要求で使用できる暗号化サービスプロバイダーを選択してください] セクションで [以下のプロバイダーのうちいずれか 1 つ] を選択します。以下のプロバイダーリストに含まれて

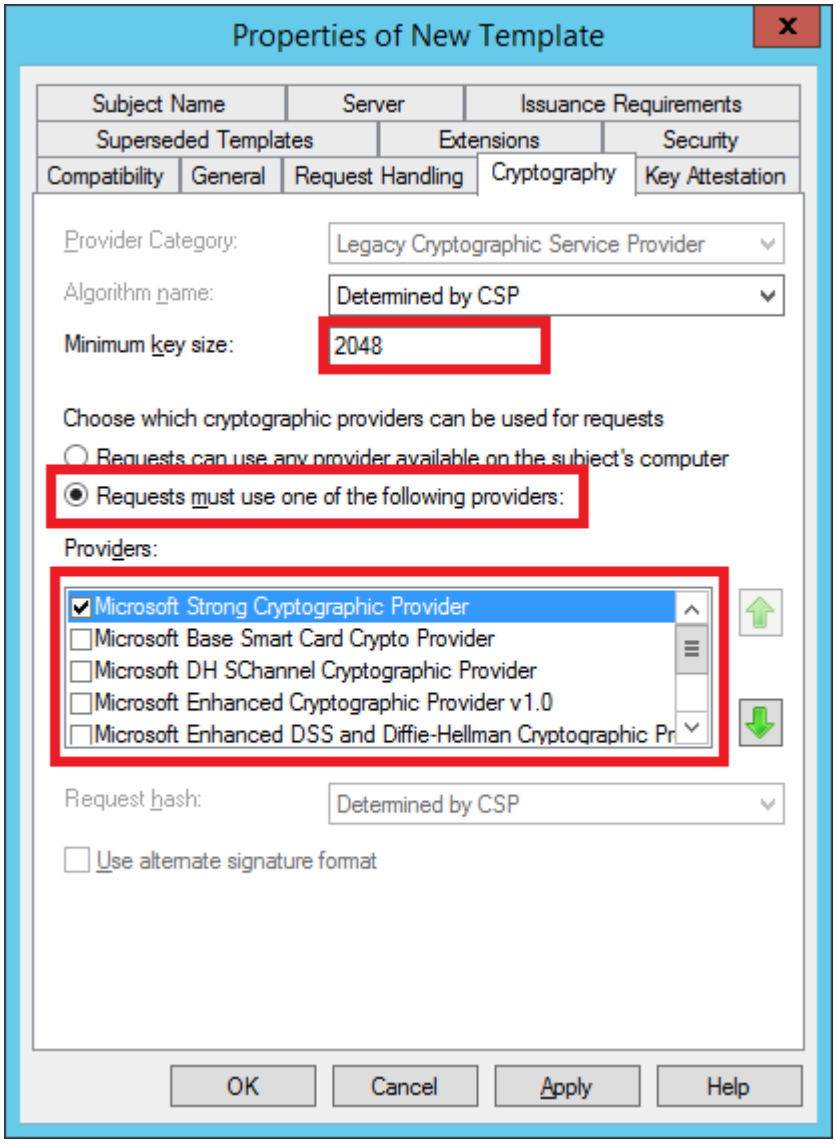
いる [Microsoft Strong Cryptographic Provider] 以外のすべてのオプションをクリアし、そのプロバイダーを優先プロバイダーとして設定します。

[X] Microsoft Strong Cryptographic Provider

[ ] Microsoft Enhanced Cryptographic Provider v 1.0

[ ] Microsoft Base Cryptographic Provider v 1.0

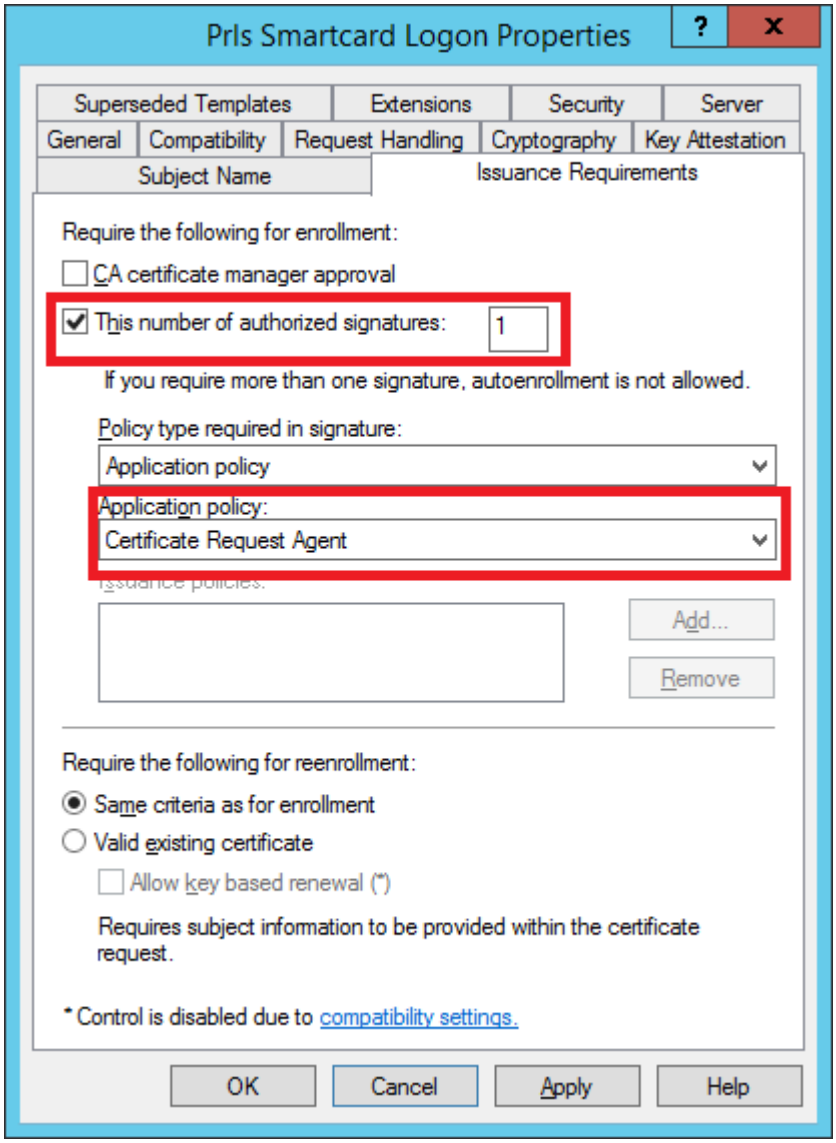
[ ] Microsoft Enhanced RSA and AES Cryptographic Provider



6 [発行の要件] タブを選択して、以下の値を設定します。

- CA 証明書マネージャーの許可: OFF

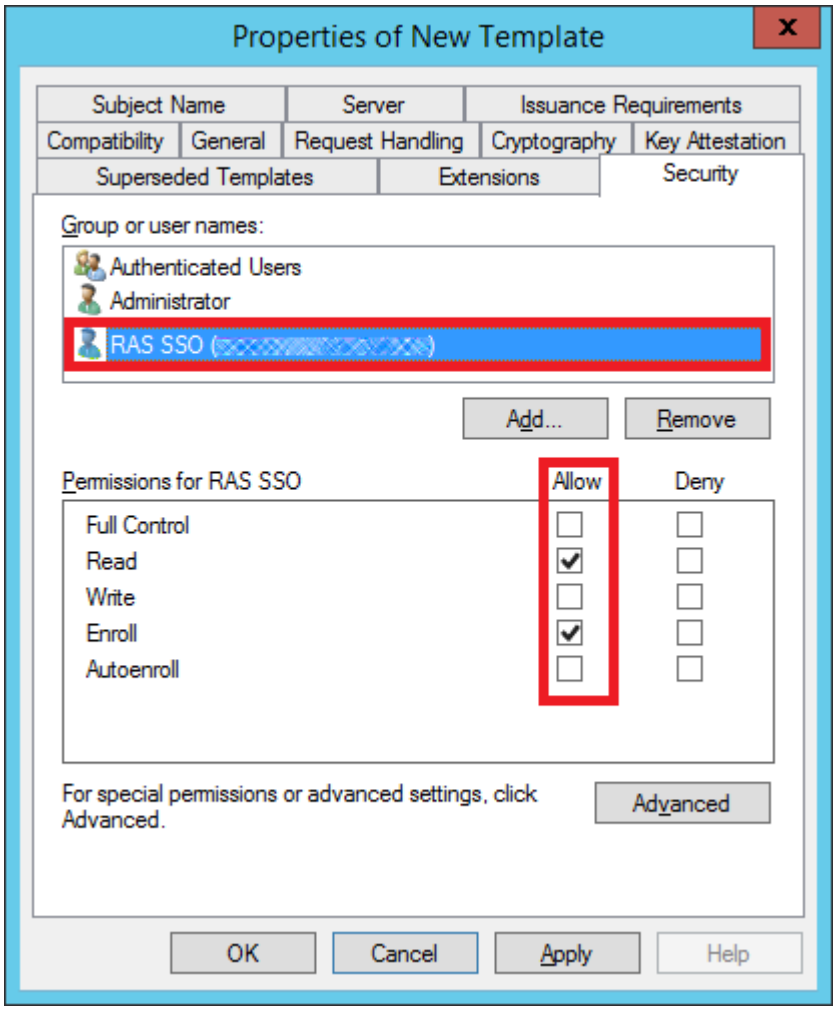
- 次の数の認証署名: 1
- 署名に必要なポリシーの種類: アプリケーションポリシー
- アプリケーションポリシー: 証明書の要求エージェント
- 登録と同じ要件: ON



7 [セキュリティ] タブを選択して、以下の手順を実行します。

- [追加] をクリックします。
- 登録エージェントユーザーアカウントを追加します。

- ”読み取り”と”登録”のアクセス許可を選択します。[適用] をクリックし、[OK] をクリックします。



証明書テンプレートの発行

作成した証明書テンプレートを発行するには、以下のようにします。

1 認証局を再び実行し、[証明書テンプレート] を右クリックして [発行する証明書テンプレート] をクリックします。

2 前の手順で作成した証明書テンプレート（Prls Smarcard Logon）を選択して、[OK] をクリックします。

3 その証明書テンプレートが [証明書テンプレート] リストに表示されます。

注: スマートカードログオンテンプレートと登録エージェントテンプレート（前述）を作成したら、Windows で [Active Directory 証明書サービス] サービスを再起動する必要があります。

RAS 登録サーバーの構成

RAS 登録サーバーは、Parallels RAS 環境で Microsoft 認証局（CA）と通信し、ユーザーに代わって SSO 認証のデジタル証明書をリクエストしたり登録したり管理したりします。

注: セキュリティ上の理由から、RAS 登録サーバーは、Active Directory ドメインコントローラーや認証局と同じように、他の Parallels RAS コンポーネントがインストールされていないセキュアな専用サーバーにインストールしてください。

RAS 登録サーバーのセットアップと構成

RAS Console を使用して、RAS 登録サーバーエージェントを指定のサーバーにリモートからインストールできます。対象のサーバーで標準の RAS インストーラーを実行してエージェントをインストールすることも可能です。

RAS 登録サーバーをリモートからインストールするには、以下の手順を実行します。

1. RAS Console で、[ファーム] > [サイト] > [登録サーバー] に移動します。
2. [タスク] > [追加] をクリックします。
3. RAS 登録サーバーエージェントをインストールするサーバーの FQDN または IP アドレスを指定します。
4. [次へ] をクリックします。
5. [登録サーバーエージェント情報] ダイアログで [インストール] をクリックし、画面上の指示に従います。

Parallels RAS インストーラーを使用して RAS 登録サーバーをインストールするには、以下の手順を実行します。

1. RAS 登録サーバーエージェントをインストールするサーバーで Parallels RAS インストーラーを実行します。
2. [インストールタイプの選択] ページで、[カスタム] を選択し、[次へ] をクリックします。
3. Parallels RAS 登録サーバーコンポーネントを選択し、他のコンポーネントをすべてクリアします。

4 [次へ] をクリックし、画面上の指示に従います。

5 RAS 登録サーバーをインストールしたら、RAS Console を開いて、[ファーム] > [サイト] > [登録サーバー] に移動します。

6 [タスク] > [追加] をクリックします。

7 登録サーバーの FQDN または IP アドレスを入力して、[次へ] をクリックします。

8 画面上の指示に従って、サーバーをファームに追加します。

登録キーの取得とコピー

RAS インストーラーを使用して手動でインストールを実行する場合は、登録サーバーのホストに登録キーファイルを配置する必要があります。RAS Console を使用して RAS 登録サーバーエージェントをリモートから展開した場合は、この手順は不要です。

まず、以下の手順を実行して登録キーファイルを取得する必要があります。

1 RAS Console を開いて、[ファーム] > [サイト] > [登録サーバー] に移動します。

2 [タスク] > [登録キーをエクスポート] をクリックします。

3 *registration.crt* という名前のファイルにキーを保存します。

registration.crt ファイルを作成したら、RAS 登録サーバーのインストール先になっているサーバー上のフォルダーにそのファイルをコピーします。デフォルトでは以下のパスになります。

```
C:\Program Files (x86)\Parallels\ApplicationServer\x64
```

注: 登録キーファイルの名前は必ず”registration.crt”にしてください。

AD 統合の構成

RAS Console で RAS 登録サーバーを追加したら、以下のようにして AD 統合を構成する必要があります。

1 RAS Console で、[ファーム] > [サイト] > [登録サーバー] に移動します。

2 [AD 統合] タブを選択します。

3 [認証局（CA）] セクションで、新しい証明書テンプレート（PrlsEnrollmentAgent と PrlsSmartcardLogon）を作成したエンタープライズ CA の構成文字列を指定します。以下の形式で指定してください。

```
CAhostname.domain\issuing CA name
```

[...] ボタンをクリックして CA を選択することも可能です。構成の詳細については、「認証局テンプレートの構成」(p. 435) を参照してください。

4 [登録エージェント] セクションで、登録エージェントのユーザー名とパスワードを指定します。構成の詳細については、「Active Directory のユーザーアカウントの設定」(p. 434) を参照してください。

5 [NLA ユーザー] セクションで、NLA のユーザー名とパスワードを指定します。構成の詳細については、「Active Directory のユーザーアカウントの設定」(p. 434) を参照してください。

6 [AD 統合設定の検証] ボタンをクリックして、入力情報が有効かどうか確認してください。

コンピューター管理ツールの使用

RAS Console から、RAS 登録サーバーホストをホスティングしているサーバーで標準的なコンピューター管理タスクを直接実行できます。このタスクには、リモートデスクトップ接続、PowerShell、コンピューター管理、サービス管理、イベントビューアー、IPconfig、再起動などが含まれます。[ツール] メニューにアクセスするには、[タスク] をクリックし、[ツール] をクリックして目的のツールを選択します。要件と使用方法については、「コンピューター管理ツール」(p. 569) を参照してください。

RAS 登録サーバーの高可用性

高可用性のために、各サイトに複数の登録サーバー (ES) を追加できます。有効になっている確認済みのすべての ES がアクティブ/アクティブモードで使用されます。ユーザーのログオン時には、ワークロード VM (RD セッションホストや VDI など) からの要求が、使用可能な ES の間で均等に分散されます。1 つの ES で障害が発生すると、次に使用可能な ES が選択され、SAML SSO 認証プロセスが続行されます。複数の ES の手動展開が必要な場合は特に、同じサイトにあるすべての ES が同じ登録キーを共有することを覚えておいてください。その登録キーは、「RAS 登録サーバーの構成」(p. 445) セクションで説明されているパスに配置する必要があります。

注: 複数の ES が共通の証明書リポジトリストアを共有することはありません。ES ごとにすべての証明書が分離されています。従って、複数の ES がある場合は、同じユーザーでも、ES ごとに別々の証明書を使用することが可能になります。

SAML 統合の例とヒント

各種認証プロバイダーと Parallels RAS を統合する事例については、Parallels のウェブサイト（https://www.parallels.com/jp/products/ras/resources/）で利用できる、「SAML SSO 認証の例」ガイドを参照してください。

ユーザーアカウントの属性

IdP でユーザー認証が実行されると、Active Directory にあるユーザーアカウントの属性と IdP にある属性がそれぞれ比較されます。IdP 側でも RAS Console でも比較対象の属性を構成できます。詳細については、「SP 側の構成（RAS 側）」（p. 430）を参照してください。

セキュリティのヒント

セキュリティ上の理由から、CA で登録エージェントの制限を構成し、ユーザーの代わりに証明書を登録する権限を、新しく作成した登録エージェントユーザーだけに与えるようにしてください。そのためには、以下の手順を実行します。

1. 認証局スナップインを開き、CA の名前を右クリックして [プロパティ] をクリックします。
2. [登録エージェント] タブをクリックし、[登録エージェントを制限する] をクリックし、表示されるメッセージで [OK] をクリックします。
3. [登録エージェント] の下にある [追加] をクリックし、前の手順で作成した登録エージェントユーザーの名前を入力し、[OK] をクリックします。[すべてのユーザー] をクリックし、[削除] をクリックします。
4. [証明書テンプレート] の下にある [追加] をクリックし、作成したテンプレート（PrlsEnrollmentAgent と PrlsSmartcardLogon）を選択し、[OK] をクリックします。証明書テンプレートの名前を追加する作業が終わったら、<すべて> をクリックし、[削除] をクリックします。
5. [権限] の下にある [追加] をクリックし、名前またはグループ（SAML を使用して RAS 環境にログインするユーザーまたはグループ）を入力し、[OK] をクリックします。[すべてのユーザー] をクリックし、[削除] をクリックします。
6. 他のユーザーやコンピューターやグループの証明書を登録エージェントが管理できないようにブロックする場合は、[アクセス許可] の下でそのユーザーやコンピューターやグループを選択し、[拒否] をクリックします。
7. 登録エージェントの制限の構成が完了したら、[OK] または [適用] をクリックします。

注: 登録エージェントの制限が適用されているユーザーやグループは、登録エージェントの制限付きのアクセス許可が構成されていてもいなくても、CA の有効な登録エージェント証明書を持っていなければ、登録エージェントとして機能できません。

Parallels Client の構成

Parallels Web Client

追加の構成は必要ありません。

Parallels Client for Windows

「Windows 用 Parallels Client ユーザーガイド」を参照してください。

Parallels Client for Mac

SAML SSO 認証用に Parallels Client for Mac を構成するには：

1. 接続を選択（または新しい接続を作成）して、そのプロパティを開きます。
2. [接続] タブの [ログイン] セクションで、認証タイプとして [ウェブ] を選択します。
3. [詳細] タブを選択して、[既定の OS ブラウザーを使用] オプション（[ウェブ認証]セクション）を有効または無効にします。このオプションを有効化すると、SAML SSO のログインダイアログが既定のブラウザーで開きます。このオプションを解除すると、Parallels Client に組み込まれているブラウザーが使用されます。
4. ダイアログを閉じて、接続のプロパティを保存します。

Parallels RAS に接続すると、ウェブブラウザーでダイアログが開き、資格情報を入力するように求められます。これは、ID プロバイダーによって検証されます。資格情報が有効な場合、公開されたアプリケーションのリストが Parallels Client に表示されます。

Parallels Client for Linux

SAML SSO 認証用に Parallels Client for Linux を構成するには：

1. 接続を選択（または新しい接続を作成）して、そのプロパティを開きます。
2. [接続] タブの [ログイン] セクションで、認証タイプとして [ウェブ] を選択します。

3 追加で構成する場合は、次の操作を実行します。

1. QtWebEngine ライブラリをインストールします。
2. [詳細設定] タブを選択し、[接続の詳細設定] ボタンをクリックします。
3. [Web 認証] セクションの [既定の OS ブラウザーを使用] オプションを選択またはクリアします。このオプションを有効化すると、SAML SSO のログインダイアログが既定のブラウザーで開きます。このオプションを解除すると、Parallels Client に組み込まれているブラウザーが使用されます。
4. ビルトインのブラウザーを使用している場合は、[ウェブ認証] セクションの [ブラウザーのウィンドウを開いてログアウトを完了] オプションを選択またはクリアしてください。このオプションを選択すると、SAML からのログアウトを実行するための URL が開きます。デフォルトでは、この Web ページは表示されませんが、ブラウザーでの操作が必要な場合は、このオプションを有効にすることができます。

4 ダイアログを閉じて、接続のプロパティを保存します。

Parallels Client ポリシーの構成

クライアント側で直接 SAML SSO オプションを指定するができます。また RAS Console の Parallels Client ポリシーを介してそれらを設定することもできます。このためには、次の操作を実行します。

1 RAS Console で [ポリシー] カテゴリーを選択します。

2 ポリシーのプロパティを開き、[セッション] > [接続] > [プライマリ接続] に移動します。

3 [認証タイプ] ドロップダウンリストで [ウェブ] を選択します。

4 [セッション] > [接続] > [ウェブ認証] に移動します。

5 [既定の OS ブラウザーを使用] オプションを有効または無効にします。このオプションを有効化すると、SAML SSO のログインダイアログがクライアント側の既定のブラウザーで開きます。このオプションを解除すると、Parallels Client に組み込まれているブラウザーが使用されます。

> **注:** Parallels RAS Console 19.3 以降を使用している場合、内蔵ブラウザーで SAML SSO ログインダイアログを起動するには、Parallels RAS Client for Windows 19.3 以降を使用します。

「Parallels Client の構成」（p. 449）も参照してください。

SAML SSO の展開のテスト

構成済みの SAML SSO 認証がある場合、次に説明する手順でテストを実行することができます。

サービスプロバイダーが認証を開始しました

1. ウェブブラウザーを使用して、RAS Web Client を開き（またはプラットフォームに対応する Parallels Client を使用して）、割り当てた ID プロバイダーのテーマを指定します。
2. 公開済みのアプリケーションを起動します。アプリケーションセッションが正常に起動したことを確認します。
3. もう一度テーマを作成し、IdP プロバイダーを追加してから、指定している新しいテーマに接続します。別のアプリケーションを起動します。

ID プロバイダーが認証を開始しました

1. ウェブブラウザーを使用して ID プロバイダーのポータルに接続します。
2. 公開済みのアプリケーションを起動します。アプリケーションセッションが正常に起動したことを確認します。

エラーメッセージ

SAML SSO 認証に何らかの問題があった場合、ウェブブラウザーにエラーメッセージが表示されます。

HTML5 事前読み込み

エラーメッセージ	注記
SAML アサーションをパースできません	SAML アサーションのパースと検証でエラーが発生しました。詳細については、HTML5 のログを参照してください。 一般的に次の原因が考えられます。 このユーザーに関する SAML 返信は有効ではありません。この問題の原因として、IDP の設定に問題があること（特にエンティティ ID URL）が考えられます。アサーションのエンティティ ID URL が、SP SAML 設定が提供するエンティティ ID と一致しません。

	1 つのアサーションまたは 1 つの暗号化済みアサーションが予想されます。返信にアサーション/暗号化済みアサーションのタグが見つかりませんでした。IDP が非暗号化アサーションを送信している間、Web Client は、暗号化済みのアサーションについて待機します。これは、IDP 設定を変更して暗号化済みのアサーションを送信するか、[RAS Console] > [接続] > [SAML] > [IDP 設定] から [暗号化されていないアサーションを許可する] のチェックボックスにチェックを入れることで修正できます。 SAML 返信がまだ有効になっていません。この問題は、RAS Gateway がインストールされているサーバーの時間が正しくなく、インスタンスが 4 秒間遅延している場合に発生する可能性があります。この場合アサーションのパースの前に、アサーションが作成されます。 SAML 返信が有効になりません。この問題は、RAS Gateway がインストールされているサーバーの時間設定が正しくない場合に発生する可能性があります。後で手動で設定する場合、アサーションの検証時に、未検証と見なされる可能性があります。
SAML アサーション本文が空です	返信に SAML アサーションが見つかりませんでした。詳細については、HTML5 のログを参照してください
SAML ログアウトリクエストを作成できません	SAML ログアウトリクエストの作成中にエラーが発生しました。詳細については、HTML5 のログを参照してください。
SAML ログアウトレスポンスを作成できません	ログアウト返信の作成中にエラーが発生しました詳細については、HTML5 のログを参照してください。

HTML5 事後読み込み

エラーコード	エラーメッセージ	注記
0x00000029	SAML IdP 設定が見つかりません。IdP Id:'xxx'	ID プロバイダーの設定を確認してください。IdP メタデータが正しくインポートされていることを確認してください。
0x0000002A	SAML IdP 情報キーの読み込みに失敗しました。IdP Id:'xxx'	IdP 設定に IdP 証明書が存在していることを確認してください。
0x0000002B	SAML テーマに整合性がありません	IdP 設定のテーマが正しく設定されていることを確認してください。
0x0000002C	SAML を使用するログオンに失敗しましたエラー: 0x00001	次のエラーが表示されます
0x00000029	利用可能な登録サーバーがありません	登録サーバーのステータスを確認してください
0x0000002A	NLA ユーザー構成が見つかりません	NLA ユーザーの詳細を入力します
0x00000003	SAML を使用するログオンに失敗しましたエラー:	IdP プロパティの属性設定が正しいこと

	AD ユーザーのマッチングに失敗しました 0x00000006	を確認してください。
0x00000003	SAML を使用するログオンに失敗しましたエラー: 返信の検証および復号に失敗しました 0x00000009	IdP 設定に IdP 証明書が存在していることを確認してください。
0x00000003	SAML を使用するログオンに失敗しましたエラー: アサーションが暗号化されませんでした 0x0000001C	ログオンリクエストの IdP 設定が正しいことを確認してください。
0x00000003	SAML を使用するログオンに失敗しましたエラー: アサーションの復号に失敗しました 0x0000001D	IdP 設定の SP 証明書が正しく設定されていることを確認してください。
0x00000003	SAML を使用するログオンに失敗しましたエラー: アサーションの検証に失敗しました 0x0000001F	IdP 設定に IdP 証明書が存在していることを確認してください。

アプリケーションまたはデスクトップの起動後

エラーメッセージ	説明と参照資料
ユーザー名またはパスワードが無効です	ユーザーの証明書は有効ですが、ドメインコントローラーの承認を受けられませんでした。ドメインコントローラーの Kerberos ログオンを確認してください。
ユーザーがシステムにログオンできません。お使いの資格情報を検証できませんでした。	ドメインコントローラーとの接続性、および適切な証明書がインストールされていることを確認してください。
リクエストはサポートされていません	”ドメインコントローラー”およびドメインコントローラーの”ドメインコントローラー認証”証明書は、すでに利用可能な状態であっても登録する必要があります。
ユーザーがシステムにログオンできません。認証に使用するスマートカード証明書の信頼性を確認できませんでした。	エラーが表示されたマシンに、中間証明書および root 証明書がインストールされていません。CA root 証明書およびすべての中間証明書を、ローカルコンピューターアカウントの”信頼済み root 証明書”に追加する必要があります。
ユーザーのアカウントでスマートカードログオンがサポートされていないため、ログオンできません。	ユーザーアカウントでの、スマートカードカードログオンの構成が不完全です。
有効なスマートカード証明書が見つかりませんでした。	PrIsSmartcardCertificate の構成を確認してください。拡張子が正しく設定されていないか、または RSA キーが 2048 ビットに満たない可能性があります。
不正なリクエスト	PrIsSmartcardCertificate の構成を確認してください。拡張子が正しく設定されていないか、または RSA キーが 2048 ビットに満たない可能性があります。

第　19　章

Parallels Web Client とユーザーポータル

Parallels Web Client は、ウェブブラウザーで動作するクライアントアプリケーションです。ユーザーは、Parallels Web Client を使用してユーザーポータルにアクセスして、ウェブブラウザーからリモートアプリケーションやデスクトップを表示したり起動したりできます。

Parallels Web Client は、プラットフォーム固有の Parallels Client（Windows 用 Parallels Client、iOS 用 Parallels Client など）と比較して、エンドユーザーがコンピューターやモバイルデバイスに追加ソフトウェアをインストールする必要はありません。機能的なプラットフォーム固有の Parallels Client は、Parallels Web Client よりもより多くのオプションをユーザーに提供します。それでも、Parallels Web Client は、Parallels RAS を使用して公開されたリモートリソースを使用して、代替方法をエンドユーザーに提供する、フル機能を備えたプラットフォームに依存しないクライアントです。

システム要件

Secure Gateway（ユーザーポータルとウェブクライアントをホストする）。

- Windows Server 2012 R2 以降

クライアント側:

- HTML5 対応のウェブブラウザー（Internet Explorer を除く）。

この章の内容

Web Client の構成

Web Client は、RAS Secure Gateway の一部です。エンドユーザーが使用するには、「ユーザーポータルの構成」(p. 97) の説明に従って、RAS Console でユーザーポータルを有効にして構成する必要があります。

クッキーに基づくセッションのパーシスタンス

RAS Web Client セッションのパーシスタンスは、通常、ユーザーの IP アドレス（ソースアドレス指定）により設定されます。環境でソースアドレス指定が使用できない場合（セキュリティポリシーで許可されない場合など）、セッションクッキーを使用して、ユーザーとサーバーの間のパーシスタンスを維持できます。そのためには、パーシスタンスにセッションクッキーを使用できる負荷分散機能を設定する必要があります。使用する必要があるクッキーは、ASP.NET_SessionId です。ASP.NET を使用しないロードバランサーを使用している場合、RAS Secure Gateway の [プロパティ] ダイアログの [ウェブリクエスト] タブで、別の Cookie を指定できます。詳細については、「ウェブリクエストのロードバランス」を参照してください（p. 102）。

テーマの構成

Parallels RAS のテーマには次のような機能があります。

- 指定されたユーザーグループに適用される特定のテーマプロパティを構成して、該当のグループにテーマへのアクセスを許可できます。この機能は、利用可能なすべてのプラットフォームの Parallels Client でサポートされています。
- ユーザーポータルの外観をカスタマイズします。これにより、さまざまなユーザーグループに対してユーザーポータルのカスタムブランドを実装できます。この機能は、RAS Web Client および Parallels Client for Windows でのみ利用可能です。

テーマを管理するには、Parallels RAS Console で、[ファーム] > <サイト> > [テーマ] に移動します。右ペインの [テーマ] ビューには、利用可能なテーマが表示されます。このリストには、少なくとも 1 つのデフォルトのテーマが表示されます。このテーマは削除できませんが、必要に応じてカスタマイズできます。デフォルトのテーマの他に、独自のテーマを作成できます。

新しいテーマの作成や既存のテーマの変更を行うには、次の操作を実行します。

- [タスク] > [新規テーマ] をクリック（または [+] アイコンをクリック）して、新しいテーマを作成します。
- 既存のテーマをダブルクリックします（または、既存のテーマを右クリックして [プロパティ] を選択します）。

[テーマのプロパティ] ダイアログが開きます。このダイアログを使用して、新しいテーマの作成や既存のテーマの変更を行います。後続のセクションの手順は、両方の場合に該当します。

一般的なテーマ設定

以下で説明するテーマ設定は、利用可能なすべてのプラットフォームの Parallels Client に適用されます。

一般

左ペインの [一般] を選択して、以下のテーマプロパティを指定します。

- テーマを有効化: テーマを有効または無効にします（デフォルトのテーマを無効にすることはできません）。
- 名前: テーマの名前を指定します。
- 説明: テーマの説明を指定します（オプション）。
- 認証ドメインを上書き: Parallels Client に渡されるドメイン名を指定できるため、ユーザーがドメイン名を手動で入力する必要がなくなります。この設定は、[接続] > [認証] のドメイン名設定を上書きします。詳細については、「ユーザーによるドメインパスワードの変更を許可する」（p. 381）を参照してください。
- このテーマへのアクセスをこれらの Active Directory グループのメンバーに制限する: このオプションをオフにすると、すべての Parallels RAS ユーザーが URL を利用して無制限にこのテーマにアクセスできるようになります。特定の 1 グループ（または複数のグループ）にアクセスを制限するには、このオプションをオンにして、[タスク] > [追加] をクリック（または [+] アイコンをクリック）して、グループを選択します。
- MFA プロバイダー: テーマの MFA プロバイダーを選択します。

メッセージ

左ペインの [メッセージ] で、ログオン後メッセージを指定します（最大 500 文字）。ログオン後メッセージは、ユーザーが正常にログインした直後に、メッセージボックスとして表示され

ます。メッセージは Web Client と Windows クライアントで個別に上書きできます（各クライアントについては、後続のセクションの「メッセージ」を参照してください）。

Web Client テーマ設定

[ユーザーポータル（Web Client）] カテゴリーでは、ユーザーポータルのテーマ設定を行うことができます。これらの設定は、ウェブブラウザーでのユーザーポータルの外観と動作に影響します。

注: ダイアログの左下隅にある [ユーザーポータルをプレビュー] ボタンをクリックすると、いつでも Web Client テーマの外観を確認できます。

URL

[URL] カテゴリーでは、テーマのログインページの URL を指定したり、ユーザーポータルページにアクセスする別の URL を追加したりできます。

- テーマのログインページ: テーマのログインページの URL の接尾部を指定します。テーマを保存すると、このフィールドにテーマの名前が自動的に入力されますが、任意の名前を指定することも可能です。テーマのログインページの完全な URL は、”https://<host-name>/”にこのフィールドで指定した名前を追加した形式になります。<host-name> に必要な形式の詳細については、「ウェブリクエストのロードバランス」（p. 102）を参照してください。

  たとえば、テーマに”Theme-S1”と命名する場合、完全な URL は https://<host-name>/Theme-S1 になります。テーマを保存すると、RAS Console の [テーマ] タブ（[ユーザーポータル URL] 列）に URL が表示されます。

  上記の URL は短縮名で、覚えるのも使用するのも簡単です。完全なバージョンは次のようになります。

  https://<host-name>/userportal/?theme=<team-name>

  短いバージョンも長いバージョンも同じように有効です。

- Parallels Client のダウンロード URL を表示: 選択すると、ユーザーには Web Client ページに [Client をダウンロード] リンクが表示され、このリンクを使用して、ユーザーのコンピューターで Parallels Client をダウンロードしたり、インストールしたり、構成したりできるようになります。
- ブランド化した Parallels Client（Windows）用のダウンロード URL を上書きする: Windows ユーザーが Parallels Client for Windows をダウンロードする場所を指定します。デフォル

トでは、Parallels Client は Parallels ウェブサイトからダウンロードされます。ブランド化されたバージョンの Parallels Client を使用する場合、このフィールドでその場所を指定できます。

- フッター URL: このオプションを使用して、Web Client のフッターに配置するカスタム URL を指定できます。URL を追加するには、[タスク] > [追加] をクリックして、URL、ページフッターに表示されるテキスト、ツールヒントのテキストを指定します。類似する URL を入力するときに、既存の URL を複製するには、既存の URL を右クリックして [複製] を選択します（または、エントリを選択して [-] アイコンの隣にある [複製] アイコンをクリックします）。複数の URL を追加している場合、上矢印または下矢印アイコンをクリックするか [タスク] メニューの [上] または [下] アイテムを選択して並べ替えることができます。URL はフッターにリスト内の順番で表示されます（[HTML4 テーマをプレビュー] ボタンをクリックして内容を確認することができます）。

ブランディング

[ブランディング] カテゴリーでは、ユーザーポータルページの外観をカスタマイズできます。

以下のプロパティをカスタマイズできます。

- ウェブページのタイトル: ウェブページに表示するタイトルを指定します。任意のタイトルを入力できます。
- ログイン先: ユーザーポータルのログインダイアログに表示する名前を指定します。たとえば、”ABC”と入力すると、ログインページに”ABC にログイン”と表示されます。ここで使用できる事前定義の変数が 2 つあります。%FARM%（実際のファーム名でこれがデフォルト値）および %SITE%（ライセンスサイト名）。
- 会社のロゴ: ユーザーポータルのページヘッダーに表示されるイメージを表示します。イメージを変更するには、[参照] を選択し、イメージファイルを指定します。ロゴ画像を変更すると、ページヘッダーからデフォルトの [Remote Application Server] の部分も削除されることに注意してください。
- Favicon アイコン: 現在設定されている Favicon アイコンを表示します。アイコンを変更するには、[参照] をクリックし、アイコンファイルを選択します。

色

ユーザーポータルの各種要素（ヘッダー、フッター、作業領域、ボタンなど）の色を指定します。

色を変更するには、次のいずれかを実行します。

- [色の変更] ボタンをクリックして、色を選択します。
- HEX 列の”鉛筆”アイコンをクリックして、任意の色の HEX 値を入力します。

言語バー

ユーザーポータルページの言語セレクターに表示する言語を選択します。セレクターは、ページヘッダーのユーザー名の右側に言語の旗のアイコンとして表示されます。

メッセージ

このペインではログオン前およびログオン後のメッセージを指定できます。

- ログオン前メッセージは、[ログイン] ページに表示されます。
- デフォルトのログオン後メッセージ（このトピックの冒頭にある「メッセージ」を参照）を削除するには、[ログオン後メッセージを上書きする] オプションを選択し、メッセージを入力します。

メッセージの長さは 500 文字以内でなければなりません。

入力プロンプト

ログインページにここで指定された入力プロンプトが表示され、ユーザーが対応するフィールドにユーザー名とパスワードを正しく入力できるようにしますたとえば、デフォルトの user@domain ログインプロンプトは、ログインフィールドに薄い灰色のテキストとして表示され、UPN 形式で名前を入力する必要があることをユーザーに示します。サポートされているすべての言語に対して、事前定義された入力プロンプトが提供されます。必要に応じて、独自のプロンプトを指定できます。

ゲートウェイ

[Secure Gateway] カテゴリーを使用して、RAS Secure Gateway で構成済みのデフォルトのユーザーポータル設定を上書きできます。従来型の Parallels RAS Farm を実行していて、サイトで単一のテーマを利用している場合、通常ゲートウェイ設定を上書きすることはできません。設定を上書きする必要があるのは、次のような場合です。

- 異なるユーザーグループ向けに複数のテーマを使用していて、アプリケーション起動方法の条件と制限に応じ、別個のテーマを動作させたい場合。

- テナントブローカーで RAS Secure Gateway が実行されており、個別のファームであるテナントによって共有されている、RAS の複数のテナントアーキテクチャを使用している場合。この種類の展開のテーマは、テナントレベルで定義されます。それで各テナントの Web Client の外観および使用感は、それぞれ独自のものになります。ゲートウェイはテナントによって共有されるため、テナントのテーマレベルの設定は、論理的に構成されます。これが [Secure Gateway] カテゴリーで実行可能な操作です。テナントブローカーおよびテナントの詳細な説明については、「RAS マルチテナントアーキテクチャ」の章（p. 397）を参照してください。

RAS Secure Gateway の設定を上書きするには、[テーマの Secure Gateway 設定を上書き] オプションを選択して、任意の設定を指定します。これらの設定を構成する方法の詳細については、「Web Client の構成」（p. 97）を参照してください。

リーガルポリシー

Cookie 使用の同意確認

[Cookie 使用の同意確認] オプションを選択すると、ユーザーの初回使用時にユーザーポータルの Cookie ポリシーに関連した通知が表示されます。これにより、ユーザーは Cookie の使用に関する情報を得て、それに同意するかどうかを選択することができます

エンドユーザー許諾契約書

[EULA の有効化] オプションを選択すると、ユーザーの初回使用時に Parallels エンドユーザーライセンス契約（EULA）が表示されます。ログインプロセスを完了するには、契約を読んで同意するというユーザーの操作が必要になります。

Parallels Client for Windows のテーマ設定

[Windows クライアント] 見出しの下にあるペインでは、Parallels Client for Windows のテーマ設定を構成できます。Windows クライアントのテーマを構成すると、これがお客様の組織のクライアントであることがエンドユーザーにはっきり伝わります。

ブランディング

[ブランディング] ペインで、次を指定します。

- 会社名: 次のスタートメニュー階層を作成するために使用されます。[スタート] \ [会社名] \ [アプリ名]。
- アプリケーション名: アプリキャプションやスタートメニューのエントリ名に表示されます。
- 接続バナー: 接続が確立されるときに表示されます。
- アプリケーションアイコン: スタートメニューとメインのアプリウィンドウで使用されるアプリケーションアイコンです。

メッセージ

デフォルトのログオン後メッセージを削除するには、[ログオン後メッセージを上書きする] オプションを選択し、メッセージを入力します。

カスタムメニュー

[カスタムメニュー] ペインでは、ホワイトレーベルの Windows 用 Parallels Client の [ヘルプ] メニューに項目を追加できます。たとえば、[メニュー項目] フィールドに“&Notepad”と入力し、[コマンド] フィールドに“notepad.exe”と入力すると、このファームに接続するすべてのホワイトレーベルの Parallels Client for Windows の [ヘルプ] メニューに新しいメニュー項目が表示されます。その項目は [Notepad] という名前になり（“N”がショートカットになります）、クリックすると Notepad.exe アプリケーションが開きます。[コマンド] フィールドには、実行可能ファイルの名前や URL や、Windows マシンで正常に実行できる任意のコマンドを入力できます。例えば、ヘルプデスクソリューションの URL を指定したメニュー項目を追加すると、ユーザーが必要なときに簡単にヘルプデスクにアクセスできるようになります。

大量配布用の Windows クライアントパッケージを作成する

Windows クライアントテーマを構成した後、次の手順に従って一括配布に対応する Windows クライアント向けパッケージを作成することもできます。

1 [テーマプロパティ] ダイアログの Windows クライアントセクションが表示されている状態で、[Windows 用クライアントパッケージを生成] ボタンをクリックします。

2 ダイアログが開いたら、次のオプションを指定します。

- パッケージが作成されるローカルコンピューター上のターゲットフォルダーを指定します。

- 必要に応じて、”操作完了時に Windows Explorer でフォルダーを開く" オプションを選択またはクリアします。

3 [生成] をクリックします。ClientDownloader.exe ファイルが作成されます。このファイルを実行すると、最新バージョンの Parallels Client for Windows インストーラー（MSI）がダウンロードされ、カスタムテーマが適用されます。

これで、インストーラーをエンドユーザーに配布できるようになります。エンドユーザーがインストーラーを実行すると、テーマで指定されているように、Parallels Client for Windows とすべてのカスタマイズ（スタートメニューのショートカット、デスクトップのショートカット、イメージおよびアイコン）がインストールされます。将来的に、インストールされた Parallels Client for Windows のコピーを新しいバージョンにアップグレードする必要がある場合、上記で説明されている手順を繰り返す必要はありません。古いバージョンをアップグレードするだけで、ブランディング機能はそのまま残ります。

一般テーマタスク

テーマのカスタマイズが完了したら、[OK] をクリックして保存し、Parallels RAS Console に戻ります。

Parallels RAS Console の [テーマ] タブでは、以下の操作も実行できます。

- テーマを複製する - テーマを右クリックして [複製] を選択します（または、テーマを選択して [タスク] > [複製] をクリックします）。
- ユーザーポータルをプレビューする - テーマを右クリックして [ユーザーポータルをプレビュー] を選択します（または [タスク] > [プレビュー...]）を選択します。
- テーマを削除する - テーマを右クリックして [削除] を選択します（または [タスク] > [削除]）を選択します。

テーマの作成または変更が完了したら、Parallels RAS Console で [適用] をクリックして、Parallels RAS に変更をコミットします。これで、HTML5 対応のウェブブラウザーでその URL を開いて、テーマをテストできるようになりました。

セッション管理権限の委任

組織に複数のユーザーグループがあり、すべてのグループで一元管理の Parallels RAS リソースを共有している場合は、特定のグループの管理者にセッション管理権限を委任できます。そ

のようにした場合、管理者は、そのグループに属するユーザーの Parallels RAS セッションだけを表示したり管理したりできます。

この機能の仕組みは以下の通りです。

1 グループごとに別々のテーマを作成します。テーマのセッション管理権限をカスタム管理者に委任します（「管理者アカウントの管理」（p. 68）を参照）。

2 カスタム管理者が Parallels RAS Console にログインすると、管理権限を持っている 1 つ以上のテーマに属するセッションだけが組み込まれた限定的なユーザーインターフェイスが表示されます。

このセクションの残りの部分で、この機能の構成と使用の方法を説明します。

テーマの作成とセッション管理権限の委任

ユーザーグループのテーマがない場合は、テーマを作成する必要があります。この章の前の部分（p. 455）で取り上げた手順を実行します。セッション管理権限を委任するには、以下の手順を実行します。

1 [一般] ページで設定を指定するときに、[このテーマへのアクセスをこれらの Active Directory グループのメンバーに制限する] オプションを選択して、1 つ以上のグループを追加します。

2 テーマの作成または構成が終わったら、[テーマのプロパティ] ダイアログを閉じ、リスト内の任意の場所を右クリックして、[権限の委任] を選択します。

3 使用したいカスタム管理者アカウントがすでにあれば、そのアカウントがリストに表示されます。アカウントがない場合は、以下のようにして作成します。

   a [タスク] > [追加] をクリックします。

   b [アカウントのプロパティ] ダイアログで、[名前]の横にある [...] ボタンをクリックして、アカウントを作成します。

   c [権限] フィールドは読み取り専用で、[カスタム管理者]（ここで使用するタイプの管理者）に設定されています。

   d 必要に応じて、その他のフィールド（電子メール、モバイルなど）を設定します。

   e [OK] をクリックします。

4 [権限の委任] ダイアログに戻り、左ペインで管理者を選択します。

5 右ペインの下側で、対象のテーマに関する権限（表示、変更、セッション管理）を選択します。右ペインの上側で権限を設定することもできますが、その設定はすべての既存のテーマに適用されます（この操作では基本的に対象外です）。

6 [OK] をクリックします。

セッションの管理

上記の作業が完了したら、カスタム管理者が指定のテーマに属するセッションを管理できるようになります。セッションを管理するには、次の操作を実行します。

1 Parallels RAS Console を実行し、カスタム管理者の資格情報を使用してログインします。

2 対象のテーマに割り当てられているグループのメンバーに属するセッションが右ペインに表示されます。

3 セッションを管理するには、そのセッションを選択し、[タスク] ドロップダウンリストをクリックして、オプション（切断、ログオフ、メッセージの送信など）を選択します。

設定監査

管理者権限の変更は設定監査に記録されます。作成、更新、削除の操作が可能です。変更内容を表示するには、[管理] > [設定監査] または [ファーム] > [テーマ] > [設定監査] に移動します。

Parallels Client for Windows でのテーマの使用

ユーザーが対象のテーマを使用できるようにするには、接続プロパティを正しく設定する必要があります。このためには、次の操作を実行します。

1 Windows 用 Parallels Client で接続を右クリックし、[接続プロパティ] を選択します。

2 [接続] タブで、サーバー名の後にスラッシュを入れてテーマ名を付記する必要があります（`Server-name/Theme-name` のように）。

管理者は、RAS Console でセッションを表示するときに、[テーマ] 列にあるテーマ名から、そのテーマを使用しているクライアントを確認できます。

Parallels Web Client を開く

ウェブブラウザーで Parallels Web Client を開くには、ユーザーの設定に応じてウェブブラウザーから次のいずれかを入力します。

- HALB デバイスまたは HALB 仮想サーバー（使用中の場合）の DNS 名。たとえば、https://ras.msp.com のようになります。
- 特定の RAS Secure Gateway の FQDN または IP アドレス。たとえば、https://ras-gw1.company.dom のようになります。

Web Client の URL の詳細については、「ウェブリクエストのロードバランス」（p. 102）を参照してください。

ウェブブラウザーで Web Client を開くと、ログインページが表示されます。

注: デフォルトでは、ユーザーが初めてウェブブラウザーで Web Client を開くと、GDPR 規則に従って、Cookie 使用への同意を求めるメッセージがページの上部に表示されます。Parallels Cookie ポリシーを読み取るには、ユーザーは提供されたリンクをクリックします。ユーザーがポリシーに同意する場合、 [同意する] をクリックします。これによりメッセージを閉じてから続行します。RAS 管理者は、[テーマ設定] ダイアログ（p. 460）で、Cookie 使用への同意を求めるメッセージを無効化できます。

Parallels RAS にログインするには、UPN 形式（username@domain.com）でユーザー名とパスワードを指定し、[ログイン] をクリックします。

注: Parallels RAS がセカンドレベルの認証プロバイダーとして、Google 認証を使用して構成されている場合、ユーザーが QR コードをスキャンするか、またはシークレットキーを使用することでワンタイムパスワード（OTP）を生成できる、追加のダイアログが開きます。詳細については、「Google 認証の使用」（p. 366）を参照してください。

ユーザーがログインすると、Web Client がサーバー側でどのように構成されているかに応じて、以下に示すシナリオのいずれかが進行します。詳細については、「Web Client の構成」（p. 97）を参照してください。

Parallels Client でアプリを起動しブラウザーにフォールバックする

サーバー側でこのオプションを構成すると、ウェブブラウザーでダイアログが開き、次のオプションが表示されます。

- Client を検出: Parallels Client を検索して開きます。Parallels Client が見つからない場合は、Parallels Client のインストールページが開きます。指示に従って Parallels Client をインストールします。

  注: このコンピューターで管理権限を持っていない場合は、そのことを知らせるダイアログが表示されます。そのダイアログには 2 つのボタンがあります。[Client のフルインストール] と [基本的

な Client のインストール] です。このコンピューターの管理アカウントの資格情報を知っている場合は、[Client のフルインストール] をクリックし、資格情報が求められたら入力します。その資格情報に基づいてインストールが行われ、フルバージョンの Parallels Client がインストールされます。資格情報が分からない場合は、[基本的な Client のインストール] をクリックしてください。基本バージョンの Parallels Client を使用できますが、実行できない機能もあります。

インストール後、使用できる公開済みのリソースが Parallels Web Client に表示されます。画面の左下隅にあるリンクに、Parallels Client のバージョンとビルド番号も表示されます。

これで、リモートアプリケーションとデスクトップを Parallels Client または Parallels Web Client で実行できるようになりました。アプリケーションとデスクトップのデフォルトの実行方法は Parallels Client です。リモートアプリケーションまたはデスクトップを Parallels Web Client で実行するには、右クリックして（または、モバイルデバイスでタップし、ホールドして）、Parallels Web Client を選択します。

- ウェブブラウザーを使用: このダイアログを閉じて、Parallels Web Client のメイン画面を開きます。リモートアプリケーションまたはデスクトップがウェブブラウザーで起動されます。次に Parallels Web Client を開いたときに、同じダイアログと同じオプションが再度表示されます。

Parallels Client のみ

サーバー側でこのオプションを構成すると、ダイアログが開き、Parallels Client のインストールを確認するプロンプトが表示されます。指定されたリンクをクリックして Parallels Client のダウンロードおよびインストールのページを開き、指示に従います。Parallels Client をインストールした後に、ユーザーポータルのメイン画面が開き、使用できる公開済みのリソースが表示されます。ここでリソースをダブルクリックまたはタップすると、Parallels Client でそのリソースが起動されます。

ブラウザーのみ

このオプションを構成すると、追加のプロンプトは表示されずに、ユーザーポータルのメイン画面が開きます。リモートアプリケーションとデスクトップはウェブブラウザーで起動されます。

メインメニューのオプション

Parallels ユーザーポータルのメインメニューを開くには、右上に表示されている [ユーザー] アイコンをクリックまたはタップします。下記のメニューオプションから選択できます。

設定

次の設定を構成できます。

- クリップボードのリダイレクト: リモートセッションでのクリップボードの動作を有効化または無効化します。次のオプションから選択します。[双方向]（双方向でのコピーが可能）、[サーバーからクライアントのみ]、[クライアントからサーバーのみ]、[無効]（いずれの方向へもコピー禁止）。
- サウンド: ローカルコンピューターでサウンドを再生するには、[このコンピューターで開く] オプションを選択します。ブラウザーがサウンドに対応していない場合、このメニューは無効になり、該当するテキストメッセージがその下に表示されます。
- リモートオーディオの録音: ローカルコンピューターからリモートアプリケーションへのサウンド入力のリダイレクトを有効または無効にします。たとえば、Skype または類似の電話会議用アプリでマイクを使用したい場合、ユーザーポータルのオーディオの録音を有効にする必要があります。[このコンピューターから録音] を選択して録音を有効にするか、[録音しない] を選択して録音を無効にします。

  注: オーディオ入力は Chrome、Firefox、Edge、Safari 11 に対応しています。お使いのブラウザーがオーディオ入力に対応していない場合、この設定は無効になり、代わりにテキストメッセージが表示されます。

- リンクをリダイレクト: リダイレクトオプションを次の中から選択します。[リダイレクトしない]、[URL のリダイレクト]、[メールのリダイレクト]、[すべてリダイレクト]。リダイレクトを有効にすると、ローカルコンピューターでリンクが開きます。
- ペン入力とタッチ入力: 筆圧感知をサポートしたペン入力のリダイレクトを有効または無効にします。消しゴムボタンには対応していませんのでご注意ください。

  注: ペン入力のリダイレクトは、以下のソフトウェアをサポートしています: Windows 8.1 以降で動作する Chromium ベースのブラウザー、Chrome OS で動作する Google Chrome。この機能の動作確認は Chrome OS 97.X と 98.X で行われました。

- プリンターをリダイレクト: プリンターのリダイレクトオプションを次の中から選択します。[RAS ユニバーサルプリンター]（RAS ユニバーサルプリントテクノロジーを使用）または [リダイレクトしない]（プリンターはリダイレクトされない）。
- キーボードモード: [ユニバーサルキーボード] または [PC キーボード] から選択します。特定の文字の入力で問題が発生した場合は、[PC キーボード] を選択して、[キーボードレイアウト] ドロップダウンリスト（以下を参照）で適切なレイアウトを選択してみてください。

- キーボードレイアウト: キーボードレイアウトを選択します（例: 英語（US）、英語（UK）、日本語）。このドロップダウンリストを有効にするには、[キーボードモード] オプションを [PC キーボード] に設定する必要があります。
- 自動ログイン: ユーザーポータルで自動ログインを有効または無効にします。このオプションが有効になっていて、ユーザー資格情報が以前に保存されている場合、ユーザーはそれらを再度入力する必要はありません。このオプションが無効になった状態でクライアントポリシーが適用されている場合、このオプションが使用できない可能性があります。自動ログインオプションは、最新の Chromium ベースのブラウザー（Google Chrome や Microsoft Edge など）でサポートされています。詳細については、「自動ログイン」（p. 472）を参照してください。
- 接続タイムアウト（秒）: 接続タイムアウトを指定します。
- MFA: 前回使用した方法を記憶: 多要素認証を使用する場合は、このオプションを有効にして、最後に使用した方法が記憶されるようにします。この方法がデフォルトで使用されます。
- アプリケーションを起動する際に、常に認証を要求する: このオプションを有効にすると、セッションがアクティブであっても、アプリケーションの起動時に認証情報の入力が求められます。このオプションは、許可されていないユーザーがアプリケーションにアクセスすることを防ぐための追加のセキュリティとして使用できます。たとえば、ユーザー側でセッションを切断する場合、他のユーザーがセッションを引き継いでリモートアプリケーションを実行することはできません。別の例として、ユーザーがアプリ一覧を表示したユーザーポータルを開いたままデバイスの使用を終了する場合（RDP セッションを実行しているかどうかに関わらず）、いずれかのユーザーが新しいアプリケーションや実行中のアプリケーションで別のインスタンスを開こうとすると、認証情報を入力するよう求められます。なお、この機能を有効にするには、[自動ログイン] オプション（上述）を無効にする必要があります。それ以外の場合は、保存された認証情報が自動的に使用されます。

パスワード変更

ドメインのパスワードをリモートで変更できます。パスワードを変更しようとすると、パスワードの条件が画面に表示されます。有効なパスワードを指定するには、その条件を満たす必要があります。サードパーティの ID プロバイダーを使用している場合は、RAS Connection Broker の接続設定（p. 348）により、パスワードの変更にカスタム URL を使用するようにユーザーポータルを構成できます。これらのオプションは、[クライアントポリシー] から無効にできます（[コントロールの設定] > [パスワード] > [パスワードの変更を禁止]）。

Client を検出

ローカルコンピューターに Parallels Client がインストールされているかどうかを確認します。Parallels Client がインストールされていない場合は、インストールのオプションと、今後のログオン時に Parallels Client の自動検出をスキップするオプションが表示されます。

Client をダウンロード

Parallels Client をダウンロードしてインストールする方法が記載されたウェブページが表示されます。

ログアウト

Parallels RAS でセッションを終了し、ユーザーのログアウトを行います。

リモートアプリケーションとデスクトップの実行

ユーザーポータルでリモートアプリケーションまたはデスクトップを起動するには、次のいずれかを実行します。

- アプリケーションまたはデスクトップのアイコンをダブルクリックします（または、モバイルデバイスでタップします）。リソースは、サーバー側のユーザーポータルの構成（[RAS Secure Gateway プロパティ] > ユーザーポータル > [以下を使用してセッションを起動] オプション）に従って、ウェブブラウザー内または Parallels Client で開きます。
- アプリケーションまたはデスクトップのアイコンを右クリックして（または、モバイルデバイスでタップし、ホールドして）、コンテキストメニューを表示します。このメニューが表示されるのは、RAS Console の [RAS Secure Gateway プロパティ] > [ユーザーポータル] タブで、[ユーザーが起動方法を選択することを許可] と [新規タブでアプリケーションを開く] のいずれかまたは両方のオプションが選択されている場合に限られます。このメニューを使用すると、リソースを Parallels Client と Parallels Web Client のどちらで開くかを選択でき（上記の設定により異なります）、またアプリケーションをウェブブラウザーの同じタブで開くか新しいタブで開くかを選択できます。
- エラーが原因で Parallels Client でリソースを開くことができない場合は、メッセージと共に、代わりにウェブブラウザーでリソースを開くオプションが表示されます。

Parallels Client で HTML5 ページからリソースを開く場合、カスタム URL スキームが使用されます。HTML5 ページのリソースをダブルクリックすると、同 URL スキームを実行して Parallels Client に引き渡し、Parallels Client が同 URL の手順に従ってリソースを開きます。詳細については、「RAS Web Client API および Parallels Client の URL スキーム」（p. 627）を参照してください。

ドラッグアンドドロップ機能の使用

Parallels Web Client では、リモートアプリケーションおよびデスクトップを実行するとき、ドラッグアンドドロップ機能がサポートされます。

注: ドラッグアンドドロップ機能が動作するには、Gateway 上で [ファイル転送コマンドを許可] オプションを有効にする必要があります。「Web Client の構成」（p. 97）を参照してください。

次に、リモートアプリケーションでの作業時にドラッグアンドドロップを使用する方法を説明します。

1. ローカルコンピューターでファイルを選択します。
2. 選択したファイルをアプリにドラッグアンドドロップします。[名前を付けて保存] ウィンドウが表示されます。
3. ファイルに名前を入力し、保存します。ファイルは、アプリをホストしているサーバーに保存されます。

異なるホストを実行している 2 つのリモートアプリの間でもファイルをドラッグアンドドロップできます。

次に、リモートデスクトップでドラッグアンドドロップを使用する方法を説明します。

1. ローカルコンピューターでファイルを選択します。
2. 選択したファイルをリモートデスクトップにドラッグアンドドロップします。[名前を付けて保存] ウィンドウが表示されます。
3. ファイルに名前を入力し、保存します。ファイルは、デスクトップをホストしているサーバー上のデスクトップに保存されます。

ネイティブなクリップボードの使用感

Parallels RAS 18.2 以降では、ローカルデバイスとリモートセッションの間でプレーンテキストを双方向にコピー & ペーストすることができます。Ctrl+C/Cmd+C でコピー（Ctrl+X/Cmd+X でカット）して、Ctr+V/Cmd+V でペーストするだけです。この機能は、Chromium ベースのブラウザー（Chrome、Edge Chromium、Opera）および Internet Explorer で完全にサポートされています。Firefox では、サーバー側からクライアント側へのコピー/ペーストのみサポートされています。他のウェブブラウザーはこの機能をサポートしていません。

その他の便利な機能

ユーザーポータルのメイン画面の便利な機能には、他に次のようなものがあります。

- お気に入りリスト: リモートアプリケーションまたはデスクトップは、お気に入りリストに追加すると見つけやすくなります。そのためには、アプリケーションまたはデスクトップをポイントまたはタップして、"星形" のアイコンをクリックまたはタップします。リストを表示するには、リストの上部にある [お気に入り] タブを選択します。このリストからリソースを削除するには、リソースをポイントして、[X] アイコンをクリックします（または、リソースのアイコンをポイントまたはタップして、[X] アイコンをクリックまたはタップします）。
- 検索: リソースを検索するには、ツールバーにある [検索] ボックス（右上）にその名前を入力します。入力内容に従ってリストが絞り込まれ、名前が一致するリソースのみが表示されます。
- リスト表示: 検索ボックスの下にあるアイコンをクリックすると、グリッド表示とリスト表示を切り替えることができます。リスト表示では、公開済みリソースの説明を見ることができます。
- グリッド表示で説明を表示: グリッド表示でリソースの説明を表示するには、マウスポインターをリソースの上に移動します。ツールヒントとして説明が表示されます。1 つ以上のリソースが同じ名前を使用して公開されたときにこの機能は役立つことがあります。説明を読むことで、それらを区別できるからです。
- タスクバー: リモートアプリケーションまたはデスクトップを起動すると、そのアイコンが、画面の下部にあるタスクバーに追加されます。タスクバーが満杯のときは、同じ種類のアイテムがグループ化され、スペースが節約されます。グループをクリックまたはタップして、実行中のインスタンスをすべて確認したり切り替えたりすることや、特定のインスタンスを閉じることができます。

自動ログイン

RAS ユーザーポータルの自動ログインでは、ユーザーに自動ログインオプションが提供されます。この機能により、ユーザーの介入を必要とせずに、ユーザー資格情報が入力されるようになるため、ポータルを頻繁に使用する場合の煩雑さが軽減されます。自動ログインが有効にされている場合、ユーザーがユーザーポータルを開くと直ちに自動ログインが作動します。管理者が利用を許可したリソースのリストを確認し、それに応じてリソースを起動できます。このエクスペリエンスは、Web Client 設定から構成することも、RAS ポリシー（p. 511）から集中管理することもできます。ユーザーが、Parallels ユーザーポータルへのログインを求められる回数が減少することで、ユーザーのログインを高速化し、ユーザーエクスペリエンスを向上させるように設定されています。

この機能を使用するには、次の要件を満たしている必要があります。

- ユーザーポータルおよび Web Client をホストする Secure Gateway には、有効かつ（エンドポイントデバイスから）信頼できる証明書が必要です。
- 指定されたドメイン（サブドメインを含む）に保存済みの有効な認証情報のセットは 1 つのみです。共有デバイスを使用している場合、複数のユーザーアカウントが同じ Parallels RAS 環境にアクセスしているため、自動ログインは適用されません。
- シークレットモードを使用していないこと - シークレットモードを使用していると、使用可能な認証情報が 1 つしかない場合でもログインがポップアップ表示されます。このため、ユーザーの操作なしに自動ログインすることはできません。
- 自動ログインは、最新の Chromium ベースのブラウザー（Google Chrome や Microsoft Edge など）でサポートされています。

構成

次の設定により、自動ログイン機能を制御します。

- ユーザーがユーザーポータルに初めてログインする場合、パスワードの保存を求められたときに [保存] をクリックする必要がありますこの場合、[パスワードを保存するよう提示] および [自動ログイン] オプションをブラウザーで有効にする必要があります（これらは Chromium ベースのブラウザーにおけるデフォルト設定です）。
- 資格情報が頻繁に要求されることのないよう、ユーザーによる確認が必要になります。これにより、自動ログインオプションが有効になります。

- RAS 管理者は、RAS ポリシーを使用して、自動ログインを強制的に適用（有効/無効）することもできます。これは、[ポリシー] > [セッション] > [接続] > [プライマリ接続] > [自動ログイン] から実行できます。
- セキュリティ上の理由により、[自動ログイン] オプションで 60 日の有効期限が有効化されています。

自動ログインの使用

自動ログインの動作について以下に説明します。

1. ユーザーはブラウザーでユーザーポータルのウェブページを開き、ログインします。「ダイレクトアプリアクセスもサポートされています」（p. 473）を参照してください。
2. ユーザーポータルは、最初のログイン時に、ユーザーに対して自動ログインを有効にするように促します。
3. ユーザーがユーザーポータルを開いたとき（またはアプリのダイレクトリンクを使用したとき）は、資格情報を入力するプロンプトは表示されません。

ユーザーポータルの自動ログイン設定を表示するには、右上のユーザーアイコンをクリックしてから、[設定] をクリックします。[自動ログイン] 設定を確認します。

ダイレクトアプリアクセス

Parallels RAS 18 で公開されている特定のリソースには、RAS Web Client を介して直接アクセスできます。これは、新しいパラメーター、*appid* を導入することで実現できます。これにより、管理者はリンクを使用して公開されたリソースに直接アクセスできるようになります。これにより、ユーザーは、ブラウザーのショートカットやブックマーク、または Azure My Apps Portal などのサードパーティポータルを使用して、Parallels RAS で公開されたリソースにアクセスするためにより柔軟で簡単な方法を利用できるようになります。ここでいうリソースには、独立した SAAS アプリケーションや Parallels RAS 仮想アプリ/デスクトップが含まれます。

公開されたリソースを直接起動するには、次のいずれかの形式を使用して URL を指定する必要があります。

URL のフォーマット	説明
https://FQDN?appid=	この形式では、テーマ名が省略され、デフォルトの

	Web Client テーマが使用されます。 ”appid”パラメーターは、RAS Console の [公開] カテゴリーに示されているのと同様の、公開済みリソース ID を指定します。ID は、リソースが公開されるときに自動的に生成されます。これは、公開済みリソースを選択した上で、[情報] タブの [アプリケーション] フィールドから確認できます。例、#5: Microsoft Office Word - ここで Microsoft World のアプリケーション ID は 5 です。
https://FQDN/<Theme-name>?appid=<app-ID>	この形式は上述の形式と似ていますが、テーマ名を指定します。
https://FQDN/userportal?theme=&appid=	この形式は上述の形式と同じですが、完全な URL を指定します。参照用としてここに掲載します。

サポートされるパラメーター:

パラメーター	説明
appid	起動する公開済みアイテム（アプリケーションまたはデスクトップ）です。
overrideparams	（オプション）: 公開済みアプリケーションに渡される必要のあるエンコード済み URL のオーバーライド引数です。

例:

https://FQDN?appid=14&overrideparams=C%3A%2Ftest.txt

ダイレクトリンクを使用して公開済みリソースを開く場合、設定に応じて、「自動ログイン」オプション（p. 472）も使用されます。

ツールバーの使用

ユーザーポータルには、リモートアプリケーションまたはデスクトップを起動したときに利用できるようになる、特別なツールバーが搭載されています。ツールバーは、リモートデスクトップとリモートアプリケーションでは異なって表示されます。ツールバーの機能も、デスクトップコンピューターとモバイルデバイスでは多少異なります。その違いについては、次のトピックで説明します。

このセクションでは、以下の内容を説明します。

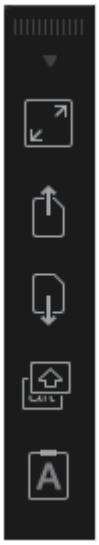
- 「デスクトップコンピューターでのツールバーの使用」（p. 475）
- 「モバイルデバイスでのツールバーの使用」（p. 477）

- 「リモートクリップボードの使用」(p. 479)
- 「ツールバーアイテムを非表示」(p. 480)

デスクトップコンピューターでのツールバーの使用

リモートデスクトップのツールバー

デスクトップまたはラップトップコンピューターのウェブブラウザーでリモートデスクトップを起動すると、次のようなツールバーが表示されます。



ツールバーの最上部の領域は、ツールバーを上下にドラッグするときに使用します。ここをクリックしてホールドし、ツールバーを目的の位置にドラッグします。矢印アイコンは、ツールバーのアイテムを表示または非表示にするときに使用します。

ツールバーの主なアイテムは以下の通りです（上から下に説明します）。

- フルスクリーン: リモートデスクトップが、ローカルコンピューターにフルスクリーンで表示されます。
- ファイルをアップロードする: ローカルコンピューターからリモートサーバーにファイルをアップロードします。このアイテムをクリックした後に、2 つのダイアログが続けて表示されます。1 番目のダイアログで、アップロードするファイルをローカルコンピューターから選択します。2 番目のダイアログで、そのファイルを保存するリモートサーバーの場所を選択します。

- ファイルをダウンロードする: リモートサーバーからローカルコンピューターにファイルをダウンロードします。このアイテムをクリックした後に、リモートサーバーからダウンロードするファイルを選択します。ウェブブラウザーの構成によっては、ダウンロードが自動的に始まったり、ローカルコンピューターでフォルダーを選択するようにメッセージが表示されたりします。
- ショートカット: [ショートカット] メニューを表示します（このメニューの詳細については後で説明します）。
- クリップボード: リモートクリップボードを表示します。詳細については、「リモートクリップボードの使用」（p. 479）を参照してください。

[ショートカット] メニューを使用すると、キーストロークとキーシーケンスをリモートデスクトップに送信できます。

- Escape: “Escape”キーストロークをリモートデスクトップに送信します。
- Tab: “Tab”キーストロークを送信します。
- Backspace: “Backspace”キーストロークを送信します。
- Print screen: “Print Screen”キーストロークを送信します。画面がリモートデスクトップのクリップボードに出力されるため、同じリモートコンピューターで実行されているアプリケーション（Paint など）に貼り付けることができます。
- Windows キー: "Windows ロゴキー" のキーストロークを送信します。
- Control+Alt+Delete: "Ctrl+Alt+Delete" キーシーケンスを送信します。

リモートアプリケーションのツールバー

リモートアプリケーションを起動すると、ツールバーがページフッターに埋め込まれ、デフォルトでは折りたたまれています。ツールバーを展開するには、右下隅にある "上矢印" アイコンをクリックします。

ツールバーのアイテムは以下の通りです（上から下に説明します）。

- ダウンロード: リモートサーバーからローカルコンピューターにファイルをダウンロードします。このアイテムをクリックした後に、リモートサーバーからダウンロードするファイルを選択します。ウェブブラウザーの構成によっては、ダウンロードが自動的に始まったり、ローカルコンピューターでフォルダーを選択するようにメッセージが表示されたりします。
- アップロード: ローカルコンピューターからリモートサーバーにファイルをアップロードします。このアイテムをクリックした後に、2 つのダイアログが続けて表示されます。1 番目のダイアログで、アップロードするファイルをローカルコンピューターから選択します。2 番目のダイアログで、そのファイルを保存するリモートサーバーの場所を選択します。
- クリップボード: リモートクリップボードを表示します。詳細については、「リモートクリップボードの使用」（p. 479）を参照してください。

モバイルデバイスでのツールバーの使用

リモートデスクトップのツールバー

モバイルデバイスのウェブブラウザーでリモートデスクトップを起動すると、次のようなツールバーが表示されます。

上部にある小さい矢印アイコンは、ツールバーのアイテムを表示または非表示にするときに使用します。

ツールバーの主なアイテムは以下の通りです（上から下に説明します）。

- ファイルをアップロードする: ローカルデバイスからリモートサーバーにファイルをアップロードします。iOS では、Photos フォルダーからのみアップロードできることに注意してください。
- ファイルをダウンロードする: リモートサーバーからローカルデバイスにファイルをダウンロードします（iOS では利用できません）。
- ショートカット: [ショートカット] メニューを表示します（このメニューの詳細については後で説明します）。
- クリップボード: リモートクリップボードを表示します。詳細については、「リモートクリップボードの使用」（p. 479）を参照してください。
- キーボード: ネイティブキーボードを表示します。モバイルデバイスのネイティブキーボードが開き、リモートデスクトップのアプリケーションで入力できます。
- 矢印: 矢印アイコンは、利用可能な 2 つのマウス入力モードを切り替えるときに使用します。

  モード 1: 1 番目のモード（矢印アイコンが白色）では、画面上のユーザーの指の動きを追って、ユーザーがタップした場所でリモートデスクトップがクリックされます。

  モード 2: 2 番目のモード（矢印アイコンが赤色）では、リモートデスクトップに仮想マウスポインターが表示され、ユーザーは自分の指を使って正確な位置にポインターを移動できます。画面のどこかをタップすると、仮想マウスポインターの正確な位置で、リモートデスクトップがクリックされます。

[ショートカット] メニューを使用すると、キーストロークとキーシーケンスをリモートデスクトップに送信できます。

- Escape: “Escape”キーストロークをリモートデスクトップに送信します。
- Tab: “Tab”キーストロークを送信します。
- Backspace: “Backspace”キーストロークを送信します。
- Print screen: “Print Screen”キーストロークを送信します。画面がリモートデスクトップのクリップボードに出力されるため、同じリモートコンピューターで実行されているアプリケーション（Paint など）に貼り付けることができます。
- Windows キー: "Windows ロゴキー" のキーストロークを送信します。
- Control+Alt+Delete: "Ctrl+Alt+Delete" キーシーケンスを送信します。

リモートアプリケーションのツールバー

リモートアプリケーションを起動すると、ツールバーがページフッターに埋め込まれ、デフォルトでは折りたたまれています。ツールバーを展開するには、右下隅にある "上矢印" アイコンをクリックします。

ツールバーのアイテムは以下の通りです（上から下に説明します）。

- ダウンロード: リモートサーバーからローカルデバイスにファイルをダウンロードします（iOS では利用できません）。
- アップロード: ローカルデバイスからリモートサーバーにファイルをアップロードします。iOS では、Photos フォルダーからのみアップロードできることに注意してください。
- クリップボード: リモートクリップボードを表示します。詳細については、「リモートクリップボードの使用」（p. 479）を参照してください。
- キーボード: ネイティブキーボードを表示します。モバイルデバイスのネイティブキーボードが開き、リモートデスクトップのアプリケーションで入力できます。

リモートクリップボードの使用

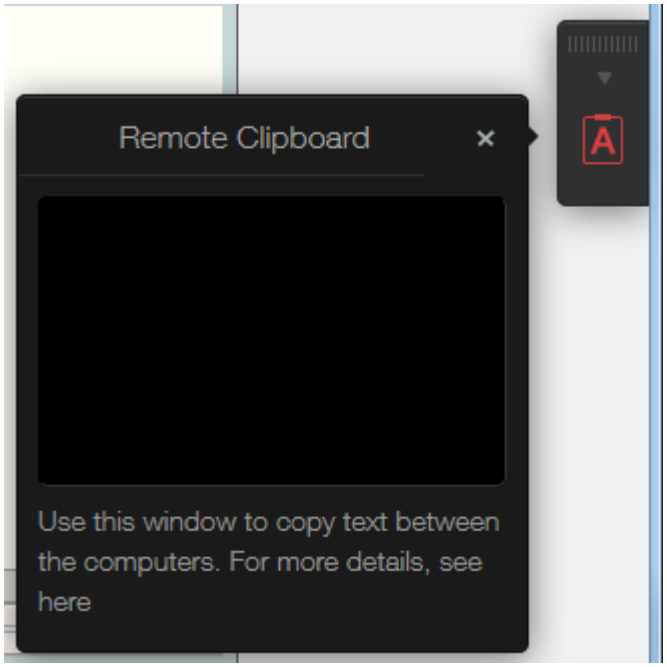
リモートクリップボードにより、ローカルのクライアントシステムと、リモートのアプリケーションやデスクトップの間でテキストをコピー & ペーストできます。クリップボードはツールバーからアクセスできます。

注: Parallels RAS 18.2 以降では、リモートクリップボードを使用せずに、ローカルデバイスとリモートセッション間でプレーンテキストをコピー & ペーストできます。詳細については、「ネイティブなクリップボードの使用感」（p. 471）を参照してください。

クリップボードを使用するには、次の操作を実行します。

1 ツールバーを展開し、[A] アイコンをクリックします。

2 [リモートクリップボード] ウィンドウが開きます。下にあるスクリーンショットには、リモートデスクトップツールバーが表示されています。リモートアプリケーションツールバーは外観が異なりますが、機能はまったく同じです。



3 テキストをローカルコンピューターからリモートアプリケーションにコピーするには、テキストを [リモートクリップボード] ウィンドウに入力します（または貼り付けます）。テキストは、自動的にリモートコンピューターのクリップボードに保存されるため、標準の貼り付けコマンド（Ctrl+V など）を使用して、リモートアプリケーションに貼り付けることができます。

4 テキストをリモートアプリケーションから [リモートクリップボード] ウィンドウにコピーするには、テキストを選択して、標準のコピーコマンド（Ctrl+C など）を使用します。テキストは [リモートクリップボード] ウィンドウに表示され、そこからローカルアプリケーションにコピーできます。

ツールバーアイテムを非表示

セキュリティリスクがあるとお考えの場合、ツールバーのクリップボードおよびファイル転送アイテムを非表示にすることができます。クリップボードは RAS Secure Gateway またはクライアントポリシーレベルで無効にすることができます。

Secure Gateway のクリップボードを無効にするには、次の操作を実行します。

1. Parallels RAS Console で、[ファーム] > <サイト> > [Secure Gateway] に移動します。
2. RAS Secure Gateway を右クリックして、[プロパティ] を選択します。
3. [ユーザーポータル] タブを選択し、[制限] セクションの [クリップボードコマンドを許可] オプションを消去します。

クライアントポリシーレベルでクリップボードを無効にすることもできます。これにより、所定のユーザーあるいはユーザーグループが接続しているゲートウェイであればどのゲートウェイでもクリップボードを無効にできます。

1. Parallels RAS Console で [ポリシー] カテゴリーを選択します。
2. ポリシーを右クリックし、[プロパティ] を選択します。
3. 左ペインで [接続プロパティ] アイテムを選択し、右ペインで [ローカルリソース] タブを選択します。
4. [ローカルデバイスおよびリソース] セクションで、[クリップボード] オプションを消去します。

注: クライアントポリシーレベルでクリップボードを有効あるいは無効にすると、デスクトップおよびモバイルバージョンの Parallels Client のクリップボード機能にも影響します。これは、クリップボードを無効にした場合、デスクトップおよびモバイルデバイスのユーザーはリモートアプリケーションの使用時に、ローカルクリップボードを利用することができなくなるということです。

ツールバーでファイルアップロードおよびファイルダウンロードを無効にすることもできます。詳細については、「リモートファイル転送の構成」セクション（p. 538）を参照してください。

第　20　章

ユニバーサルプリント

プリンターリダイレクトでは、ユーザーは印刷ジョブをリモートアプリケーションまたはデスクトップからローカルプリンターにリダイレクトできます。ローカルプリンターは、ユーザーのコンピューターに接続することも IP アドレス経由で接続したローカルネットワークプリンターとして使用することもできます。RAS ユニバーサルプリントでは、クライアント側の特定のローカルプリンターのプリンタードライバーをリモートサーバーにインストールする必要をなくすることで、印刷プロセスを簡素化し、プリンタードライバーのほとんどの問題が解決します。そのため、ユーザーはローカルでどのプリンターをインストールしたかに関係なく印刷でき、RAS 管理者はローカルネットワークに接続されたそれぞれのプリンターにプリンタードライバーをインストールする必要がありません。

この章の内容

ユニバーサルプリント設定の管理

RAS ユニバーサルプリントを構成するには、RAS Console の [ユニバーサルプリント] カテゴリーを選択します。

デフォルトでは、ユニバーサルプリントドライバーは、RD セッションホスト Agent、VDI Guest VM Agent、または Remote PC Agent とともに自動的にインストールされます。そのため、サーバーをファームに追加すると、ユニバーサルプリントはすでに有効になっています。ユニバーサルプリントドライバーには、32 ビット版と 64 ビット版が用意されています。

ユニバーサルプリントサポートの有効化および無効化

サーバーでユニバーサルプリントサポートを有効または無効にするには、[サイト内のサーバー] リストでそのサーバーを右クリックして、コンテキストメニューで [有効] または [無効] をクリックします。

プリンター名の変更パターンの構成

デフォルトでは、Parallels RAS は次のパターンを使用してプリンター名を変更します。`%PRINTERNAME% for %USERNAME% by Parallels`。例えば、Alice という名前のユーザーに Printer1 という名前のローカルプリンターがあるとします。Alice がリモートアプリケーションまたはデスクトップを起動すると、プリンターは `Printer1 for Alice by Parallels` という名前になります。

プリンターのデフォルトのリネームパターンを変更するには、[ユニバーサルプリント] カテゴリを選択します。[ユニバーサルプリント] タブの [プリンターのリネームパターン] フィールドでパターンを指定します。使用できる事前定義変数を表示するには、入力フィールドの横にある [...] ボタンをクリックします。変数は次の通りです。

- `%CLIENTNAME%` – クライアントコンピューターの名前。
- `%PRINTERNAME%` - クライアント側のプリンターの名前。
- `%SESSIONID%` - RAS セッション ID。
- `%USERNAME%` - RAS に接続しているユーザーの名前。
- `<2X Universal Printer>` - これはレガシーモードで、RDP セッションでプリンターオブジェクトが 1 つだけ作成されます。

プリンターの名前変更パターンで他の特定の文字を使用することもできます。たとえば、次の一般的に使用されるパターンを定義できます。`Client/%CLIENTNAME%#/%PRINTERNAME%`。このパターン（および上記の例の Alice という名前のユーザー）を使用すると、ローカルプリンターの名前は `Client/Alice's Computer#/Printer1` になります

[サイト内のサーバー] リストにある各サーバーに異なるプリンター名変更パターンを指定できます。

注: リダイレクトされたプリンターにアクセスできるのは、管理者とプリンターをリダイレクトしたユーザーのみです。

プリンターの保持

クライアント定義のプリンターがリモートセッションにリダイレクトされると、処理に時間がかかり、セッション確立の全体的な動作に影響が及びます。ユーザーエクスペリエンスを改善するために、以前に作成したユーザーのプリンターを使用できます。その場合、[ユニバーサルプリント] タブで [プリンターの保持] オプションを [オン] に設定します。

ユニバーサルプリントドライバー

システム管理者は、クライアント側のプリンタードライバーのリストを管理できます。プリンタードライバーに対して、ユニバーサルプリントのリダイレクト権限を許可または拒否することができます。

この機能を使用すると、次のことが可能になります。

- 不要なプリンターリダイレクトによるサーバーリソースのオーバーロードを回避します。ユーザーの大半はすべてのローカルプリンターをリダイレクトするため（デフォルトの設定）、多数のリダイレクトされたデバイスを実際には使用していないサーバー上に作成します。これは主に、PDFCreator、Microsoft XPS Writer、または各種の FAX デバイスのようなさまざまなペーパーレスのプリンターが関係します。
- 特定のプリンターが原因でサーバーが不安定になることを回避します。プリンターによってはサーバーが不安定になることがあるため（スプーラーサービスコンポーネント）、その結果、概してすべての接続ユーザーがプリントサービスを使用できなくなる場合があります。プリントサービスの継続して使用するために、管理者がそのようなドライバーの”拒否”リストを作成できることは重要です。

プリンタードライバーを指定するには、次の操作を実行します。

1 Parallels RAS Console で、[ユニバーサルプリント] > [プリンタードライバー] に移動します。

2 [モード] ドロップダウンリストで、リダイレクトを許可するプリンターを次のオプションから選択します。

   - 任意のドライバーを使用するプリンターのリダイレクトを許可（デフォルト）: このオプションは、リダイレクト権限を使用するためにプリンターが使用しているドライバーの種類を制限しません。
   - 次のいずれかのドライバーを使用するプリンターのリダイレクトを許可: [モード] フィールドの下のボックスに一覧表示されているドライバーを使用しているプリンターのみにリダイレクトを許可します。リストにドライバーを追加するには、 [タスク] > [追加]（または + アイコン）をクリックして、表示される編集フィールドにプリンタードライバーの名前を入力します。

- [次のいずれかのドライバーを使用するプリンターのリダイレクトを拒否]：おそらくこれが、この機能において最も便利なオプションです。リストに指定されているドライバーを使用するプリンターのリダイレクト権限を拒否します。その他のすべてのプリンターについてリダイレクトの使用を許可します。リストにドライバーを追加するには、 [タスク] > [追加]（または + アイコン）をクリックして、表示される編集フィールドにプリンタードライバーの名前を入力します。

3 リストからドライバーを削除するには、[タスク] > [削除] をクリックするか、マイナス記号のアイコンをクリックします。

4 変更が完了したら、[適用] ボタンをクリックして、変更を保存します。

次の点を確認してください。

- プリンタードライバーをリストに追加するときは、プリンター名ではなく、*ドライバー*名を入力してください。
- ドライバー名は、大文字と小文字を区別し、完全一致する必要があります（名前の一部や、ワイルドカードは使用できません）。
- このタブで指定した設定は、個々のサーバーだけでなくサイト全体に影響します。

フォントマネジメント

フォントを埋め込む必要があります。ユニバーサルプリントを使用してドキュメントを印刷する場合、ドキュメントがクライアントマシンのローカルスプーラーにコピーされ印刷されます。クライアントマシンにフォントが存在しない場合、印刷が正しく出力されません。

印刷ジョブ内でフォントの埋め込みを制御するには、[フォントマネジメント] タブページを使用して、[フォントを Embed する] オプションをオンまたはオフにします。

フォントの埋め込みの除外

特定のフォントタイプを埋め込まないようにするには、[以下のフォントの Embed を除外する] セクションの [タスク] > [追加] をクリックし、リストからフォントを選択します。

サーバーとクライアントへのフォントの自動インストール

サーバーとクライアントに特定のフォントタイプを自動的にインストールするには、[自動的にインストールされるフォント] セクションで [タスク] > [追加] をクリックし、リストからフォントを選択します。

注: デフォルトでは、自動インストールリストに追加されているフォントは埋め込みリストから除外されます。そのようなフォントは Windows クライアントにインストールされているため、埋め込む必要はありません。[フォントの選択] ダイアログで [自動的にフォントを除外する] オプションをクリアすると、フォントは埋め込みリストから除外されません。

除外するフォントのリストをデフォルトにリセット

除外するフォントのリストをデフォルトにリセットするには、[タスク] > [デフォルトにリセット] をクリックします。

ユニバーサルプリント圧縮ポリシーも指定できます。詳細については、[クライアントポリシー] > [エクスペリエンス]（p. 525）を参照してください。

第 21 章

ユニバーサルスキャン

スキャナーのリダイレクトによって、リモートデスクトップに接続しているユーザーや公開済みのアプリケーションにアクセスしているユーザーは、クライアントマシンに接続されたスキャナーを使用してスキャンを行うことができます。この章では、RAS ユニバーサルスキャンサービスを構成し、使用する方法について説明します。

この章の内容

ユニバーサルスキャンの管理

ユニバーサルスキャンでは、TWAIN および WIA リダイレクトが使用されます。これにより、このどちらかのテクノロジーを備えたハードウェアを使用する任意のアプリケーションをクライアントデバイスに接続し、スキャンを行うことができます。ユニバーサルスキャンでは、サーバーに特定のスキャナードライバーをインストールする必要がありません。

注: RD セッションホストで WIA と TWAIN の両方のスキャンを有効にするには、「デスクトップエクスペリエンス」というサーバー機能が必要です。

ユニバーサルスキャンを構成するには、RAS Console の [ユニバーサルスキャン] カテゴリーを選択します。

デフォルトでは、ユニバーサルスキャンドライバーは、RD セッションホスト、ゲスト VM、リモート PC Agent とともに自動的にインストールされます。そのため、サーバーをファームに追加すると、ユニバーサルスキャンがインストールされます。

スキャナー名の変更パターンの構成

デフォルトでは、Parallels RAS は次のパターンを使用してスキャナー名を変更します。`%SCANNERNAME% for %USERNAME% by RAS`。たとえば、ローカルで SCANNER1 を設置しているユーザーである Lois が、リモートデスクトップまたは公開済みのアプリケーションに

接続した場合、このユーザーのスキャナー名は "SCANNER1 for Lois by RAS" に変更されます。

スキャナー名の変更パターンを変更するには、[スキャナー名の変更パターン] 入力フィールドに新しいパターンを指定します。名前の変更のために使用できる変数は次の通りです。

- %SCANNERNAME% - クライアント側のスキャナー名。
- %USERNAME% - サーバーに接続しているユーザーのユーザー名。
- %SESSIONID% - アクションセッションの ID。

リストのサーバーごとに異なる名前変更パターンを構成できます。

注: リダイレクトされたスキャナーにアクセスできるのは、管理者と、スキャナーをリダイレクトしたユーザーのみです。

ユニバーサルスキャンサポートの有効化および無効化

特定のサーバーについて、WIA または TWAIN のユニバーサルスキャンサポートを有効または無効にするには、[WIA] タブまたは [TWAIN] タブをクリックしてから、サーバーを右クリックし、コンテキストメニューで [有効] または [無効] をクリックします。

スキャンアプリケーションの追加

スキャンアプリケーションの追加

ユニバーサルスキャン機能を使用する TWAIN アプリケーションを、[TWAIN] タブから [TWAIN アプリケーション] ボタンを選択して追加する必要があります。これにより、TWAIN アプリケーションで Twain ドライバーを使用できるようになるため、管理者は TWAIN アプリケーションを容易にセットアップできます。

アプリケーションをスキャンアプリケーションのリストに追加するには、以下の操作を実行します。

1 RAS Console で [ユニバーサルスキャン] カテゴリーが選択された状態で、[TWAIN] タブをクリックします。

2 （[サイト内のサーバー] リストの下にある）[TWAIN アプリケーション] ボタンをクリックしてから、[追加] をクリックします。

3 [TWAIN アプリケーション] ダイアログで、[タスク] > [追加] をクリックし、アプリケーションの実行ファイルを参照します。実行ファイルを選択し、[開く] をクリックします。

注: アプリケーションによっては、異なるまたは複数の実行ファイルが使用される場合があります。必要なすべての実行ファイルがスキャンアプリケーションのリストに追加されていることを確認してください。

スキャンアプリケーションの削除

リストからスキャンアプリケーションを削除するには、削除するアプリケーションを選択して、[タスク] > [削除] をクリックします。

注: リストからアプリケーションを削除しても、アプリケーションのインストールは影響を受けません。

ユニバーサルスキャン圧縮ポリシーも指定できます。詳細については、[クライアントポリシー] > [エクスペリエンス]（p. 525）を参照してください。

第　22　章

ユーザーデバイス管理とクライアントポリシー

この章では、デスクトップコンピューター、スマートフォン、タブレットなどのユーザーデバイスを管理するために Parallels RAS 管理者が実行できるタスクについて説明します。

この章の内容

Parallels RAS に接続するようにユーザーを招待する

Parallels RAS は、デスクトップ PC や MAC コンピューターからモバイルデバイスや ChromeApps にいたるまで、多くのプラットフォームをサポートします。招待メール機能は、インストールやクライアントのロールアウトプロセスに伴う複雑さを軽減することを目的として設計されています。この機能により、管理者はクライアントのインストール手順および自動構成手順をエンドユーザーに Parallels RAS Console から直接送信することができます。

続行する前に、メールボックスを適切に構成していることを確認します（「メール通知の SMTP サーバー接続を構成する」（p. 601）を参照）。招待メールをユーザーに送信するには、RAS Console の [開始] カテゴリーを使用します。詳細については、「ユーザーを招待」（p. 52）を参照してください。

ユーザーデバイスの一括構成

組織内の複数のデバイスにインストールされている Parallels Client を構成する必要がある場合は、以下の一括構成オプションのいずれかを使用して手順を簡略化できます。

- Parallels Client の設定をファイルにエクスポートしてから、他のすべての Parallels Client のインストール環境にインポートします。
- Parallels Client の URL スキームを使用します。

Parallels Client 設定のエクスポートとインポート

Parallels Client に組み込まれているエクスポート/インポート機能を使用すれば、RAS や RDP の接続設定をファイルにエクスポートしてから、他のデバイスで実行している Parallels Client にインポートできます。この機能は、どのプラットフォームでも利用できます。デスクトップバージョンとモバイルバージョンの両方の Parallels Client でサポートされています（Chrome 版の Parallels Client アプリだけが例外です）。Parallels Client のエクスポート/インポート機能には以下のようにしてアクセスします。

- Windows、Mac、Linux: メインメニューで [ファイル] > [設定のエクスポート] または [ファイル] > [設定のインポート] をクリックします。
- iOS/iPadOS: 接続設定をエクスポートするには、右上隅の [...] アイコンをタップし、[接続を共有] を選択します。インポートするには、エクスポートしたファイルを選択し、Parallels Client で開くオプションを選択します。
- Android: 接続設定をエクスポートするには、右上隅のメニューアイコン（3 つの点が横に並んでいるアイコン）をタップし、[接続を共有] を選択します。インポートするには、エクスポートしたファイルを選択し、Parallels Client で開くオプションを選択します。

接続設定のエクスポートとインポートの詳細については、対象のプラットフォームの「Parallels Client ガイド」を参照してください。

Parallels Client の URL スキームの使用

Parallels RAS では、URL スキームを使用して、ユーザーデバイスにインストールされている Parallels Client で操作を実行します。具体的には、URL スキームを使用して、事前定義設定に基づく RAS と RDP の接続を構成できます。URL スキームの詳細については、「RAS Web Client API および Parallels Client の URL スキーム」（p.627）を参照してください。

招待メールで URL スキームを使用して、Parallels Client をユーザーのデバイスにインストールするためのメールを送信できます。Parallels Client の URL スキームを使用する完全な URL のリンクを招待メールに組み込みます。ユーザーデバイスに Parallels Client を一括インストールする場合は、招待メールをユーザーに送信するだけです（p. 52）。Parallels Client の既存のインストール環境を再構成する必要がある場合に、招待メールを送信したくなければ、以下の手順を実行します。

1 必要なすべてのプラットフォームを対象にした構成プロファイルを組み込んだ招待メールを作成して、自分に送信します。

2 そのメールを開いて、Parallels Client の構成 URL をローカルポータルにコピーします。

3 ユーザーにその URL を知らせます。

4 ユーザーが対象のプラットフォームの URL をクリックするだけで、Parallels Client を構成できます。それぞれのデバイスで Parallels Client が自動的に構成されます。

ヘルプデスクサポートの有効化

Parallels Client を使用すると、ユーザーは問題報告と合わせて、ヘルプリクエストを組織のヘルプデスクに送信できます。

注: この文書の作成時点では、この機能が利用できるのは Parallels Client for iOS および Parallels Client for Android のみです。その他のクライアントのサポートは今後のリリースで追加されます。

ヘルプデスクサポートを有効化するには、次の手順を実行します。

1 RAS Console で [機能] カテゴリーを選択します。

2 [Parallels Client でヘルプデスク機能を有効にする] オプションを選択し、表示されているフィールドでヘルプデスクのメールアドレスを指定します。このメールアドレスは、ユーザーが Parallels Client から Parallels RAS に接続するたびに Parallels Client で更新されます。

ヘルプデスクは、Parallels Client の [ヘルプ] セクション（またはメニュー）からアクセスできます。ユーザーが [ヘルプデスクからサポートを要請する] アイテムを選択すると、ローカルメールクライアントが開きます。次の情報がメールに事前に入力されます。

- ヘルプデスクメールアドレス（RAS Console で設定したアドレス）。
- アプリケーション名。

- スクリーンショット。
- ユーザー名。
- アプリケーションのバージョン。
- オペレーティングシステムのバージョン。

ユーザーはリクエストの独自の説明を記入できます。

デバイスのモニタリング

デバイスのモニタリングでは、ファームに接続している、または過去に少なくとも 1 回接続を確立したことがあるデバイスを表示できます。デバイスをモニターするには、Parallels RAS Console で [デバイスマネージャー] カテゴリーを選択し、右ペインにある [デバイスマネージャー] タブをクリックします。デバイスの情報には以下が含まれます。

- デバイス名
- IP アドレス
- 状態（状態のリストは下記を参照してください）
- 最後のユーザー（デバイス使用者）
- MAC アドレス
- OS のバージョン
- Parallels Client のバージョン
- グループ（デバイスがデバイスグループのメンバーである場合）
- ゲートウェイ名（デバイスが接続している RAS Secure Gateway）
- ゲートウェイの IP アドレス

デバイスの状態

Parallels RAS に接続されたデバイスの状態は次のいずれかになっています。

- オフ: デバイスはオフになっています。
- 接続済み: デバイスは接続されています。
- ログオン済み: デバイスはシステムにログオン済みです。

- スタンドアロン: デバイスは Parallels RAS に接続済みですが、Parallels Client が使用されていないため、このデバイスを管理できません。
- サポートされていません: デバイスは Parallels RAS でサポートされていません。
- 外部管理: ファームに接続していますが、別のファームによって管理されています。
- 管理できません: クライアントバージョンに対応していないか、インストールされていないコンポーネントがあるため、クライアントを管理できません。
- ロック済み: デバイスにロック済みステータスのアクティブなセッションがあります。
- ペアを保留中: 接続はクライアント側で更新する必要があります。ポート UDP 20009 はクライアントからゲートウェイ方向はブロックされています。クライアント管理ポートはゲートウェイでは無効にされています。

デバイスモニタリングをオフにする

サードパーティのエンドポイント管理ソリューションを使用しており、Parallels RAS デバイスモニタリングが必要ない場合は、[デバイスマネージャー] > [オプション] タブで機能を無効化できます。機能を無効化することで、コンピューティングリソースが節約され、RAS Console のパフォーマンスが向上する場合があります。

デバイスモニタリングをオフにするには:

1 RAS Console で、[デバイスマネージャー] > [オプション] に移動します。

2 [デバイスマネージャーを有効化] オプションのチェックを外します。

3 [はい] そして [適用] の順にクリックします。I

デバイスモニタリングをオフにすると、RAS Console による接続デバイスの追跡は停止され、[デバイスマネージャー] > [デバイスマネージャー] タブに表示されているデバイス接続履歴が削除されます。オフにした後でも、[セッション] カテゴリーから接続に関する最新の情報を確認できます。

追加のデバイス情報を取得する

詳細なデバイス情報を表示するには、デバイスを右クリックし、コンテキストメニューで [デバイス情報を入手] を選択します。開いたダイアログで次のプロパティを確認します。

- 名前: デバイス名。
- IP: デバイス IP アドレス（該当する場合は複数のアドレス）。

- MAC アドレス: MAC アドレス。
- 状態: 状態（状態のリストは下記を参照してください）。
- 最後のユーザー: このデバイスから最後にログインしたユーザー。
- 最終ログオン時間: 最後のログオン時間。
- OS のバージョン: デバイスで動作しているオペレーティングシステムのバージョン。Windows ポータブルおよび U3 クライアントは "ポータブル" とマークされます。
- Client のバージョン: デバイスにインストールされている Parallels Client のバージョン。
- ゲートウェイ IP: RAS Secure Gateway の IP アドレス（クライアントが使用しているゲートウェイ）。
- Secure Gateway: RAS Secure Gateway の名前。
- 最後のアクティビティ: このデバイスから何らかのアクティビティが検出された日時。

Windows デバイスグループ

[Windows デバイスグループ] タブ（[デバイスマネージャー] カテゴリー）を使用すると、管理対象の Windows デバイスをグループ化してまとめて管理できます。

Windows デバイスグループの作成

Windows デバイスグループを作成するには、次の操作を実行します。

1. [デバイスマネージャー] カテゴリーの [Windows デバイスグループ] タブに移動し、[タスク] > [追加] をクリックします。
2. [メイン] タブページで、[グループ名] と [説明]（オプション）を指定します。
3. [OS 設定] タブで以下のオプションを設定します。
   - リムーバブルドライブを無効にする。管理対象の Windows デバイスでリムーバブルドライブのマウントを無効にします。
   - プリントスクリーンを無効にする: [プリントスクリーン] キーを無効にします。
   - デスクトップを置換: この機能は、Windows コンピューターをシンクライアントのように動作させます。この機能を有効にすると、ユーザーはシステム設定の変更や新しいアプリケーションのインストールを制限されます。管理者は、Parallels RAS から公開済みのリソースに加えて、ローカルアプリ（コンピューターにすでにインストールされている

もの）をアプリリストに追加できます。このオプションを選択する場合、[管理者モードパスワード] フィールド（下記）で、コンピューターのユーザーモードと管理者モードを切り替えるために使用する管理者パスワードを指定します。

- キオスクモード: キオスクモードを有効にします。これにより、グループ内のコンピューターでの電源の再投入機能（再起動、シャットダウン）が無効にされます。コンピューターを管理者モードに切り替えても、電源機能は使用できます。
- クライアントをデスクトップとして使用。このオプションが選択されている場合、Parallels Client はフルスクリーンモードで実行されます。ユーザーはスクリーンを最小化できません。Parallels Client が Windows 8.x でキオスクモードから抜け出す問題に対処するには、このオプションを選択します。この問題は、タイルベースの UI で、または "ドラッグして閉じる" 機能を使用中に明らかになる場合があります。
- 管理者モードパスワード: Windows デスクトップが置換されたとき、ユーザーモードと管理者モードを切り替えるためのパスワードを指定します（上記の「デスクトップを置換」を参照してください）。

4 [ファイアウォールの設定」] タブで、ファイアウォールを有効/無効にしたり、必要に応じて受信ポートを追加したりします。

5 Windows デバイスユーザーのデスクトップをリモートで制御する前にそのユーザーにプロンプトを表示するために、[シャドーイング] タブで [承認要請] オプションを選択します。有効にすると、ユーザーは接続を拒否できます。詳細については、「Windows デバイスの管理」（p. 497）を参照してください。

グループへの Windows デバイスの追加

Windows デバイスをグループへ追加するには、次の操作を実行します。

1 [デバイスマネージャー] > [デバイスマネージャー] タブに移動します。

2 1 つ以上のデバイスを選択し、[タスク] をクリック（または右クリック）し、[グループに移行] を選択します。

3 グループを選択し、[OK] をクリックして設定を保存します。

これで、管理者は、デバイスのグループで、標準的な Windows の電源操作（電源オン、電源オフ、再起動、ログオフ）を実行できます。

Windows デバイスの管理

デバイスマネージャー機能を使用すると、管理者は、Windows 7 から Windows 11 までを実行する Windows デバイスをシンクライアントのような OS に変換できます。Windows デバイスを管理対象にするには、Windows 用 Parallels Client の最新バージョンが Windows デバイスで実行されている必要があります。

以下の手順では、Parallels Client を Windows コンピューターで設定する方法および Parallels RAS で登録し、管理する方法について説明します。

Parallels Client を Windows コンピューターにインストールする

Windows 用 Parallels Client をインストールおよび構成するには、以下の手順を実行します。Parallels Client のインストールおよび構成方法に関する詳細については、「Windows 用 Parallels Client ユーザーガイド」も参照してください。

1. https://www.parallels.com/products/ras/download/client/ から Windows 用 Parallels Client をダウンロードします。
2. `RASClient.msi` または `RASClient-x64.msi` をダブルクリックし、画面に表示される手順に従ってインストールウィザードを実行します。
3. [ファイル] > [新しい接続を追加] をクリックして、新規 Parallels RAS 接続を作成します。https://www.parallels.com/products/ras/download/client/
4. [Parallels Remote Application Server] を選択して [OK] をクリックします。
5. 次に、以下の接続プロパティを構成します。
   - プライマリ接続 - Parallels RAS の FQDN または IP アドレスを指定します。
   - ユーザー認証情報 - ユーザー名、パスワード、ドメインを入力します。
6. [OK] をクリックすると接続が作成され、その接続をダブルクリックすると Parallels RAS に接続されます。

完了すると、Windows デバイスが [デバイスマネージャー] > [デバイス] の Parallels RAS Console に表示されます。

Windows デバイスの登録

Parallels RAS を構成して Windows デバイスを自動的に登録することも、手動での実行を選択することもできます。

Parallels RAS で Windows デバイスを手動で登録するには、次の手順を実行します。

1 RAS Console で、[デバイスマネージャー] > [デバイス] に移動します。

2 [デバイス] タブでデバイスを選択します。

3 [タスク] > [デバイスの管理] をクリックします。

デバイスが再接続されるまでデバイスの状態が [ペアを保留中] に変わります。[デバイスマネージャーポート] オプションが、ゲートウェイで有効になっていることを確認します。これを確認するには、次の手順を実行します。

1 [ファーム] > <サイト> > [Secure Gateway] に移動します。

2 ゲートウェイを選択し、[タスク] > [プロパティ] をクリックします。

3 [ネットワーク] タブをクリックして、[デバイスマネージャーポート] オプションが選択されていることを確認します。

デバイスが再接続されると、登録プロセスが完了し、デバイスの状態が [ログオン済み] にアップデートされます。これは、デバイスが Parallels RAS の管理対象になったことを示します。Windows PC で Parallels Client を実行しているユーザーは、メインの Parallels Client メニューで [ヘルプ] > [バージョン情報] をクリックして、PC が管理されていることを確認することもできます。この情報には、Parallels Client が Parallels RAS と通信するために使用する RAS Secure Gateway の情報が含まれています。

また、Windows デバイスを自動管理するように Parallels RAS を設定することもできます。このためには、次の操作を実行します。

1 RAS Console で、[デバイスマネージャー] カテゴリーを選択します。

2 [オプション] タブをクリックします。

3 [Windows デバイスを自動的に管理する] を有効にします。

これで、管理者はデバイスの状態を確認し、電源オン、電源オフ、再起動、ログオフなどの電源操作を実行できるようになります。

注: 一部の古いバージョンの Parallels Client を実行しているデバイスを管理することはできません。そのようなデバイスには”サポートされていません”と表示されます。

Windows デバイスをロックする

アクティブなセッションがある Windows デバイスをロックするには、リストで選択し、下部にあるツールバーの [ロック] 項目をクリックします。[ロック] アイコンは、選択したデバイスが [ログオン済み] 状態の場合のみ有効にされることに注意してください。

また、スケジューラーを使用してデバイス（またはデバイスグループ）をロックすることもできます。これについては、「Windows デバイスおよびグループの電源サイクルのスケジューリング」セクション（p. 505）で説明されています。

Windows デバイスをシャドーする

Windows デバイスをシャドーすることで、デバイスで Windows デスクトップに対するフルアクセスを取得し、ローカルアプリケーションとリモートアプリケーションを制御できます。

Windows デバイスをシャドーするには、次の操作を実行します。

1. RAS Console で、[デバイスマネージャー] > [デバイス] に移動します。
2. デバイスを選択し、下部にあるツールバーの [シャドー] アイテムをクリックします。

Windows ユーザーは、管理者によるデバイスの制御を許可するように要求され、アクセスの拒否を選択することもできます。管理者は、[承認要請] プロンプトを無効にすることができます。このためには、次の操作を実行します。

1. Parallels RAS Console で、[デバイスマネージャー] カテゴリーを選択して、右ペインの [Windows デバイスグループ] タブをクリックします。
2. グループを右クリックし、[プロパティ] を選択します。
3. [Windows デバイスグループ] ダイアログで、[シャドーイング] タブを選択し、[承認要請] オプションをクリアします。

デスクトップの置換

[デスクトップを置換] 機能を有効にすると、ユーザーはシステム設定の変更や新しいアプリケーションのインストールを制限されます。この機能が有効になっていると、Windows デスクトップが Parallels Client に置換され、シンクライアントのような OS に変換されます。実際の

オペレーティングシステムの置換は不要です。この場合、ユーザーはアプリケーションを Parallels Client 以外から展開できないので、管理者が接続先のデバイスを高いレベルで制御できるようになります。

さらに、キオスクモードの場合は、ユーザーがデバイスの電源再投入の操作を実行できません（管理者モードでは電源操作を実行できます。下記の詳細を参照してください）。

[デスクトップを置換] 機能を有効にするには、次の操作を実行します。

1 [デバイスマネージャー] カテゴリーで [Windows デバイスグループ] タブを選択します。

2 グループを右クリックし、[プロパティ] を選択します。

3 [OS 設定] タブをクリックします。

4 [デスクトップを置換] オプションを有効にし、オプションで [キオスクモード] オプションを有効にします。

5 [OK] をクリックします。

注: この機能を使用するには、Windows デバイスでユーザーモードから管理者モードに切り替えるための管理パスワードを設定する必要があります。

管理者モードへの切り替え

ユーザーモードの場合、ユーザーは、管理者が提供するアプリケーションしか使用できません。システム設定を変更するには、デバイスを管理モードに切り替える必要があります。

管理者モードに切り替えるには、システムトレイアイコンを右クリックし、[管理者モードに切り替え] を選択します。パスワードの入力を求めるメッセージが表示されたら、パスワードを入力します。

管理者モードとユーザーモードで利用できる機能を以下の表にまとめます。

機能	ユーザーモード	管理者モード
Parallels Client グローバルオプション		x
Parallels Client ファーム接続プロパティ		x
ローカルアプリケーションの構成		x

新しい RAS 接続の追加		x
新しい RDP 接続の追加		x
標準 RDP 接続とフォルダーの管理		x
ディスプレイの設定	x	x
マウスの設定	x	x
プリンターの設定		x
タスクマネージャー		x
コントロールパネル		x
コマンドプロンプト		x
Windows エクスプローラー		x
設定のインポート/エクスポート		x

Parallels Client の代替デスクトップを使用する場合のローカルアプリケーションの構成

管理者は、リモートアプリケーションまたはリモートデスクトップを展開し、ネイティブの OS を使用してリモート接続に必要なソフトウェアを展開する目的の場合に限り、[デスクトップを置換] オプションを有効にしてください。ただし、場合によってローカルアプリケーションが必要になることもあります。管理者は Parallels Client の代替デスクトップ内にローカルアプリケーションを表示するように構成することもできますが、その前に管理者モードに切り替える必要があります。

ローカルアプリケーションを公開するには、次の手順を実行します。

1. ユーザーのセッションをシャドーするか、ユーザーデバイスステーションを直接使用します。
2. Parallels Client 代替デスクトップを管理者モードに切り替えます。
3. [ファイル] > [新しいアプリケーションを追加] をクリックします。
4. アプリケーションの情報を入力します。

5 追加されたアプリケーションはアプリケーションランチャーに表示されます。

6 必要なすべてのアプリケーションを構成したら、ユーザーモードに戻ります。

Windows デスクトップの置換

このセクションでは、[デスクトップを置換] オプションが有効な場合の動作と、このオプションが管理者にとって役に立つ理由を説明します。

有効な場合、デスクトップを置換する機能により、管理者はオペレーティングシステムを置換することなく、標準デスクトップをシンクライアントのような制限のあるデバイスに変換できます。

エンドユーザーには、Windows エクスプローラー、タスクバー、または通常新しいアプリケーションのインストールやシステム設定の変更を可能にするその他の Windows コンポーネントへのアクセス権が付与されません。ユーザーは、リモートアプリケーション、リモートデスクトップ、およびローカルで構成されたアプリケーションを含む、Parallels Client 内で構成されたアプリケーションのみ展開できます。ローカルアプリケーションが許可されているため、特定のアプリケーション（たとえば、特定の周辺機器と通信するソフトウェア）が必要だがそれをリモートで使用できない場合でも、ユーザーはそれを展開できます。

[デスクトップを置換] オプションが有効な場合、以下の機能が、対応するバージョンの Windows （7、8、8.1、10、11）に適用されます。

機能	7	8	8.1	10	11
デスクトップを Parallels Client で置換	x	x	x	x	x
スタートボタンの無効化	x	x	x	x	なし
コントロールパネルへのアクセスを制限	x	x	x	x	x
Windows キーの無効化	x	x	x	x	x
タスクマネージャーの無効化	x	x	x	x	x
クイックアクセスツールバーの無効化	なし	なし	なし	なし	なし
セキュリティマネージャー/アクションセンターの通知の無効化	x	x	x	x	x
タスクバーのロック	x	x	x	x	x

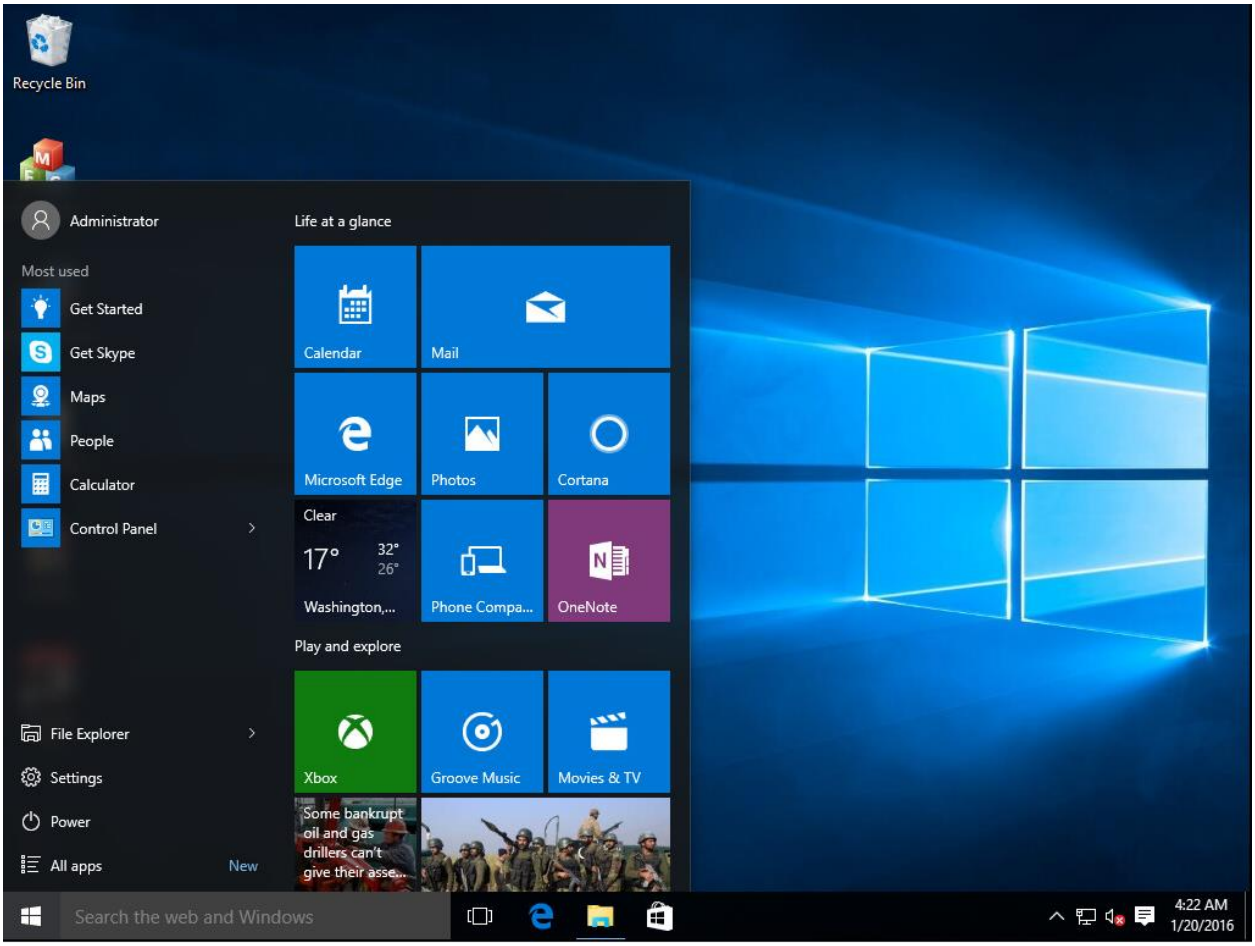
ピン留めされたアプリケーションの削除	x	x	x	x	x
メトロ画面の無効化（ユーザーは直接デスクトップ画面へ）	なし	x	x	x	x
ホットコーナーの無効化	なし	x	x	x	x
チャームヒントの無効化	なし	x	x	x	x
ヘルプの無効化	なし	x	x	x	x
Windows サイドバーの無効化	x	なし	なし	なし	なし

このモードでは、ユーザーはマウスと画面のコントロールパネルのアプレットにアクセスすることもできます。ユーザーは、Parallels Client のグローバルオプションおよび、クライアントファーム接続オプションを変更することができません。デバイスを管理モードに切り替えると、詳細管理機能が有効になります。

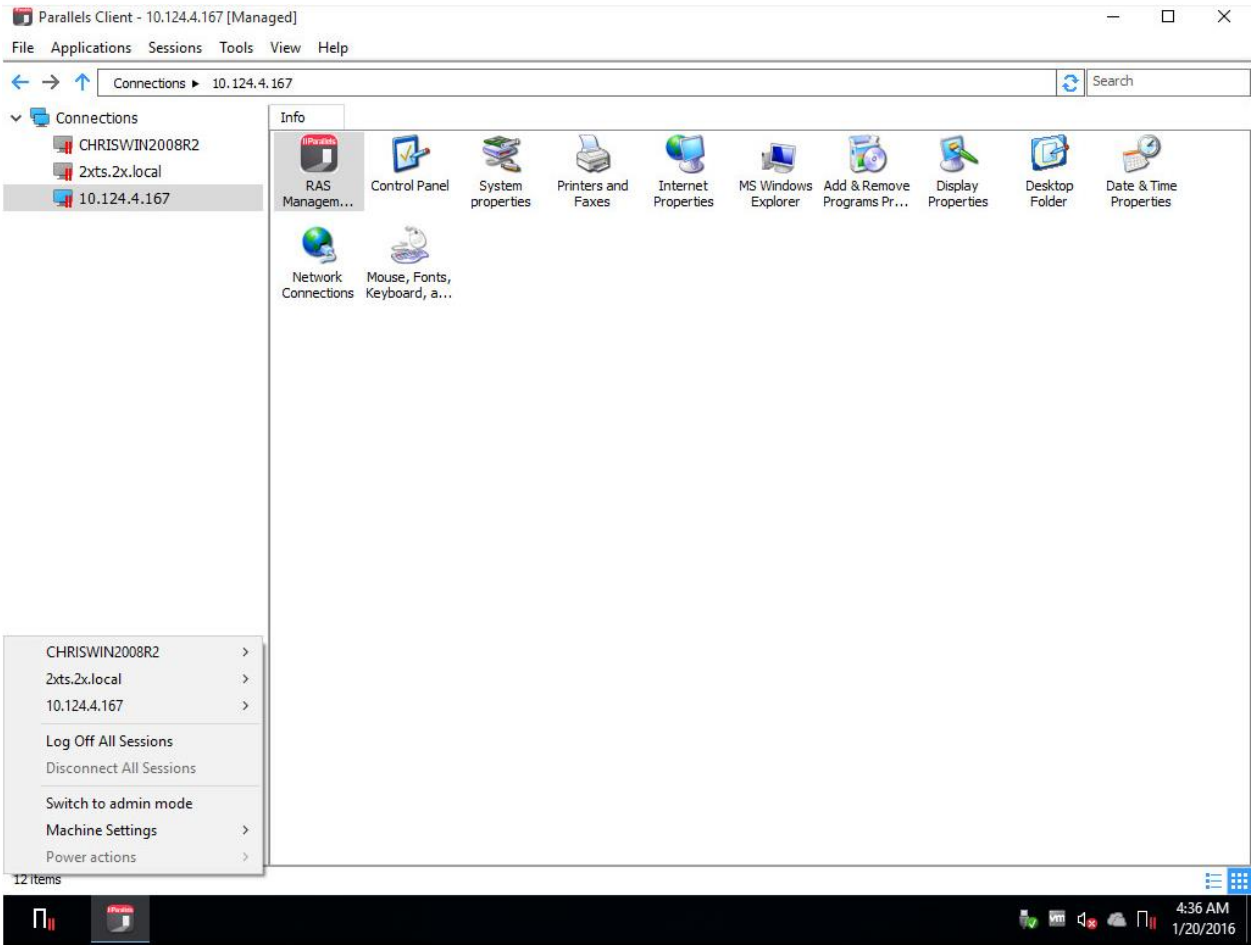
Windows デスクトップの置換機能がオフの場合、すべての制限が解除され、ユーザーは標準のデスクトップを使用できます。

以下のスクリーンショットは、[デスクトップを置換] オプションを有効にする前と後の Windows 10 デスクトップを示しています。

前


Recycle Bin
Administrator
Most used
Get Started
Get Skype
Maps
People
Calculator
Control Panel
File Explorer
Settings
Power
All apps
New
Life at a glance
Calendar
Mail
Microsoft Edge
Photos
Cortana
Clear
17°
32°
26°
Washington,...
Phone Compa...
OneNote
Play and explore
Xbox
Groove Music
Movies & TV
Some bankrupt oil and gas drillers can't give their asse...
Search the web and Windows
4:22 AM
1/20/2016

後



Windows デバイスおよびグループの電源サイクルのスケジューリング

[デバイスマネージャー] カテゴリーの [スケジューラー] タブで、デバイスに対する自動電源操作のスケジュールを設定できます。

新しいスケジュールタスクの追加

タスクをスケジュールするには、次の操作を実行します。

1 [スケジューラー] タブで、[タスク] > [追加] をクリックして、[デバイススケジューラーのプロパティ] ダイアログを開きます。

2 [このスケジュールエントリーを有効にする] オプションを選択します。

3 [アクション] ドロップダウンメニューでアクションを選択します。

- デバイスグループの電源投入
- デバイスグループのログオフ
- デバイスグループの電源オフ
- デバイスグループのリブート
- デバイスグループのロック

4 [ターゲット] ドロップダウンリストでデバイスグループを選択します。

5 タスクの開始日と開始時刻を指定します。

6 次の選択肢の中から、[リピート] オプションを選択します。

- [使用しない]（タスクは、[開始] および [時刻] フィールドで指定された日時に 1 回だけ実行されます）
- 毎日
- 毎週
- 2 週間毎
- 毎月
- 毎年
- 週の特定の曜日。このオプションを選択する場合は、週の曜日（複数可）を選択してください。

7 [説明] フィールドにタスクの説明を入力します。

8 [OK] をクリックしてタスクを作成します。

スケジュール済みタスクの管理

既存のタスクを修正するには、[スケジュールリスト] でタスクを右クリックし、コンテキストメニューで [プロパティ] をクリックします。

イベントを有効または無効にするには、イベントを右クリックして、[プロパティ] をクリックした後、[このスケジュールエントリーを有効にする] オプションをオンまたはオフにします。

スケジュール済みタスクをすぐに実行するには、タスクを右クリックし、コンテキストメニューから [実行してください] をクリックします。

タスクを削除するには、タスクを右クリックし、[削除] をクリックします。

クライアントポリシー

[ポリシー] カテゴリでは、ファームに接続するユーザーを対象とする Parallels Client ポリシーを管理できます。クライアントポリシーを追加することで、ユーザーをグループ化し、ユーザーのデバイスにさまざまな Parallels Client 設定をプッシュし、組織の必要に応じて機能させることができます。

ユーザーデバイスに適用できる設定には、RAS 接続プロパティ、表示、印刷、スキャン、オーディオ、キーボード、デバイスなどの設定があります。ポリシーを作成し、クライアントデバイスにプッシュすると、デバイスのユーザーはポリシーによって適用される設定を変更できません。Parallels Client では、これは非表示または無効にされた接続プロパティおよびグローバル環境設定として明らかになります。

サポートされている Parallels Client のバージョン

すべてのプラットフォーム向けの Parallels Clients がサポートされています。

注: Parallels RAS v16.5 から、クライアントポリシーを管理するために新しいアプローチが使用されています。旧バージョンでは、クライアントポリシーにより、パラメーター一式が適用され、クライアント設定を置き換えて、適用されたカテゴリを完全に非表示にします。RAS v16.5 以降では、クライアントポリシー設定が小さいグループに分割されていて、クライアント側で各グループを個別に構成してポリシーを適用できます。これが、旧バージョンの Parallels RAS で作成された既存のクライアントポリシーにどのように影響するかについては、「クライアントポリシーの後方互換性」（p. 536）を参照してください。

このセクションでは、以下の内容を説明します。

- 新しいクライアントポリシーの追加（p. 508）
- セッション設定の構成（p. 511）
- クライアントポリシーオプションの構成（p. 529）
- コントロールの設定の構成（p. 534）

- ゲートウェイリダイレクトの構成（p. 535）
- クライアントポリシーの後方互換性（p. 536）

新しいクライアントポリシーの追加

新しいクライアントポリシーを追加するには、次の手順を実行します。

1 [ポリシー] カテゴリを選択し、右ペインで [タスク] > [追加] をクリックします。[ポリシーのプロパティ] ダイアログが開きます。

2 左ペインに含まれるナビゲーションツリーを使用して、構成するオプションのグループを選択できます。ダイアログの左上にある [検索] フィールドを使って、オプションを検索できます。複数の選択肢がある場合は、矢印で移動できます。

3 [ポリシー] ノードが選択されていることを確認し、ポリシー名と説明（オプション）を指定します。

4 [ポリシーの適用先] セクションで、[タスク] > [追加] を選択（またはプラス記号アイコンをクリック）して、ポリシーが適用されるオブジェクトを定義するルールを指定します（以下を参照）。

クライアントポリシーのルールを構成する

デフォルトでは、どのような場合も、構成済みのユーザーとコンピューターとグループにクライアントポリシーが適用されます。オプションで、ポリシーを適用するタイミングを定義するルールを指定できます。この機能を使用すると、同じユーザーやコンピューターに対して複数のポリシーを作成し、ユーザーがどの場所のどのデバイスから接続しているかに応じてポリシーを適用することが可能になります。各ルールは、ユーザー接続に対するマッチングに使用される 1 つまたは複数の条件で構成されています。各条件は、マッチング可能な 1 つまたは複数の特定のオブジェクトで構成されています。

次のオブジェクトのマッチングを実行できます。

- ユーザー、ユーザーが所属するグループ、またはユーザーが接続するコンピューター。
- ユーザーが接続する Secure Gateway。
- クライアントデバイスのオペレーティングシステム。
- IP アドレス。
- ハードウェア ID。ハードウェア ID の形式は、クライアントのオペレーティングシステムに依存します。

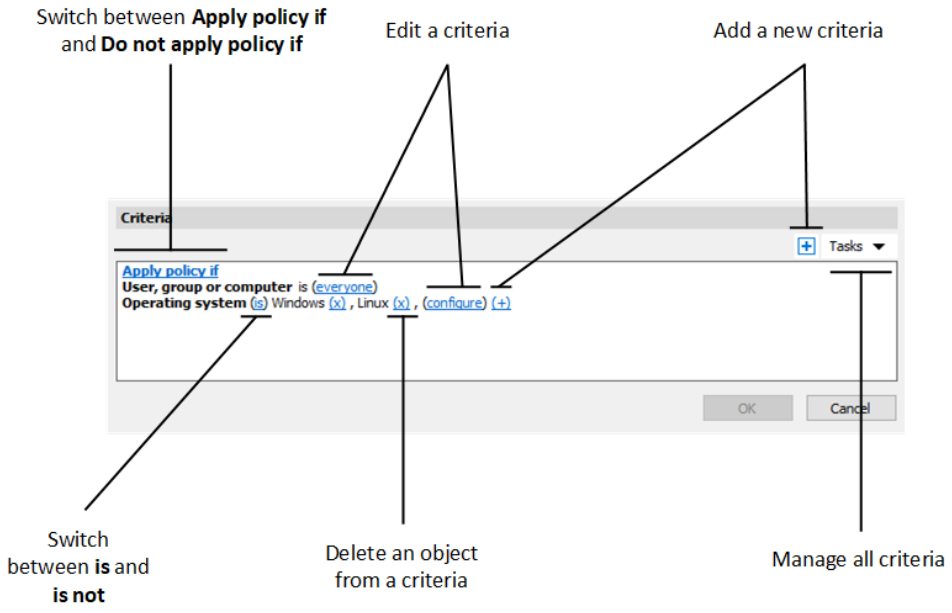
ルールについて、次のことに注意してください。

- 条件は AND 演算子で連結されます。たとえばあるルールに、特定の IP アドレスに一致という条件とクライアントデバイスのオペレーティングシステムに一致という条件が含まれる場合、ユーザーの接続が IP アドレスの条件とクライアントオペレーティングシステムの条件の両方に一致する場合に、ルールが適用されます。
- オブジェクトは OR 演算子で接続されます。たとえば、クライアントデバイスのオペレーティングシステムに一致するという条件のみを作成した場合、いずれかのオペレーティングシステムがクライアント接続に一致すれば、ルールが適用されます。
- ルールは、上から順にユーザー接続と比較されます。このため、ルールの優先順位は、ルールリスト内の位置によって異なります。Parallels RAS では、ユーザー接続に一致する最初のルールが適用されます。
- いずれのルールにもマッチしない場合には、デフォルトルールが使用されます。デフォルトルールは、他のルールにマッチしない場合に適用または他のルールにマッチしない場合に適用しないのいずれかに設定できますが、条件を利用することはできません。

新しいルールを作成するには、次の操作を実行します。

1. ポリシーノードを選択します。
2. [ポリシーの適用先] セクションで、[タスク] > [追加] をクリックします。[新規ルールのプロパティ] ダイアログが開きます。
3. ルールの名前と説明を指定します。

4 [条件] セクションで、ルールの条件を指定します。以下のコントロールを利用できます。



- Apply policy if および Do not apply policy if: ユーザー接続がすべての条件に一致する場合に、ポリシーを適用するかどうかを指定します。これらのオプションは、クリックすると切り替わります。
- （+）：新しい条件を追加します。一致条件として、Secure Gateway、クライアントデバイスのオペレーティングシステム、IP アドレス、ハードウェア ID のいずれかを使用したい場合は、（+）をクリックします。　表示されるコンテキストメニューで、マッチングさせたいオブジェクトの種類を選択し、表示されるダイアログで特定のオブジェクトを追加します。新しい条件が次の行に表示されます。
- （X）：マッチングから特定のオブジェクトを削除します。たとえば、IP アドレス 198.51.100.1 をマッチングから削除したい場合は、その横にある（X）をクリックします。このコントロールは、少なくとも 1 件のオブジェクトが追加されたときに表示されます。条件内のすべてのオブジェクトが削除された場合、その条件は削除されます。
- is and is not:: ユーザー接続が条件に一致する場合に、ポリシーを適用するかどうかを指定します。これらのオプションは、クリックすると切り替わります。このコントロールは、少なくとも 1 件のオブジェクトが追加されたときに表示されます。
- configure: マッチさせるオブジェクトのリストを編集します。このリンクをクリックして新しいオブジェクトを追加または削除します。最初の条件（ユーザー、グループ、コン

ピューター) の場合、このリンクは everyone と呼ばれることに注意してください。この条件のオブジェクトを指定すると、構成が変更されます。

セッション設定の構成

[ポリシーのプロパティ] ダイアログの [セッション] ノードの下にある項目には、接続、表示、印刷、ネットワーク、および定義され、有効にされている場合にクライアントで適用されるその他の設定が含まれます。

クライアントデバイスに特定の設定のグループを適用するには、選択（チェック）する必要があります。選択されていないグループは適用されないため、エンドユーザーは自分で構成できます。たとえば、[接続] ノードをチェックし、その下にある [プライマリ接続] グループと [セカンダリ接続] グループのみをチェックすることができます。これにより、選択した 2 つのグループの設定のみがクライアントデバイスに適用されます。

このセクションでは、以下の内容を説明します。

接続

接続プロパティを構成するには、[接続] ノードを選択し、それぞれの子ノードを調べ、対応するプロパティを構成します。

プライマリ接続

プライマリ接続は常にプライマリ RAS Secure Gateway がデフォルト設定になりますが、以下の接続プロパティを変更できます。

1 この接続のフレンドリ名を指定します。

2 自動ログイン: RAS ユーザーポータルで自動ログインを有効または無効にします。このオプションを無効にすると、ユーザーポータルで自動ログインが無効になり、ユーザーはそれを変更できなくなります。詳細については、「自動ログイン」（p. 472）を参照してください。

3 [認証タイプ] ドロップダウンリストで、使用する認証方法を選択します。

- 資格情報: ログオンするために資格情報を入力しなければなりません。
- シングルサインオン: Parallels Client のインストール時に [Single SignOn] モジュールをインストールした場合のみ、このオプションがリストに含まれます。ユーザーがログオン時に使用した資格情報が、リモートサーバーへの接続で使用されます。
- スマートカード: スマートカードを使用して認証を行う場合、このオプションを選択します。リモートサーバーに接続するとき、ユーザーはカードリーダーにスマートカードを挿入し、要求されたときに PIN を入力する必要があります。
- ウェブ: このオプションを選択すると、クライアント側の SAML SSO ログインダイアログがデフォルトのブラウザーで開きます。詳細については、[SAML SSO 認証]（p. 423）を参照してください。

注: 許可された認証タイプを RAS Console の [接続] > [認証] で指定する必要があります。

4 必要に応じて、[パスワードの保存] を選択またはクリアします（資格情報が認証に使用される場合）。これは、クライアントにこの接続のパスワードの保存を強制するという意味です。

5 ドメイン名を指定します（資格情報が認証に使用される場合）。

セカンダリ接続

複数の RAS Secure Gateway がある場合、セカンダリ接続を定義できます。プライマリゲートウェイの接続に失敗した場合のバックアップ接続として、セカンダリ接続を使用します。

セカンダリ接続を追加するには、次の操作を実行します。

1 [セカンダリ接続] 項目を選択します。

2 [セカンダリ接続] ペインで [タスク] > [追加] をクリックし、サーバー名または IP アドレスを指定します。

3 [接続モード] を選択し、必要に応じてデフォルトのポート番号を変更します。

複数のセカンダリ接続がある場合は、リスト内で上下に移動できます。プライマリ接続を確立できない場合、Parallels Client はリスト内の順番でセカンダリ接続を使用します。

再接続

このペインでは、接続が切れた場合の対応を指定します。

- 接続が切れた場合、再接続する: このオプションを選択すると、接続が切れた場合に Parallels Client が再接続を試みます。[接続リトライ回数] プロパティで、リトライの回数を指定します。
- 接続が確立されない場合にバナーを表示するまでの時間: Parallels Client で接続バナーが表示されるまでの時間を秒数で指定します。接続バナーが表示されると、ユーザーは接続が切れたことを知って、自分で対応策を講じるようになります。

コンピューター名

リモートデスクトップセッション中にコンピューターが使用する名前を指定します。このオプションが設定されている場合は、デフォルトのコンピューター名が上書きされます。[コンピューター名を上書きします] 設定は、サーバー側の管理者が設定したフィルターで使用されます。

詳細設定

- 接続タイムアウト: Parallels Client の接続タイムアウトの値。
- 接続が確立されない場合にバナーを表示するまでの時間。接続バナーが表示されるまでの時間を秒数で指定します。接続バナーが表示されると、ユーザーは接続できないことを知って、自分で対応策を講じるようになります。
- アプリケーションに接続できない場合にデスクトップを表示するまでの時間: 公開されたアプリケーションが、このフィールドに指定された時間内に起動しない場合は、ホストサーバーのデスクトップが表示されます。これは、アプリケーションの起動中にサーバー側でエラーが発生した場合に役立ちます。サーバーのデスクトップが表示されるので、ユーザーはエラーメッセージを確認できます。

ウェブ認証

- [既定の OS ブラウザーを使用] オプションを有効または無効にします。このオプションを有効化すると、SAML SSO のログインダイアログがクライアント側の既定のブラウザーで開きます。このオプションを解除すると、Parallels Client に組み込まれているブラウザーが使用されます。

  注: Parallels RAS Console 19.3 以降を使用している場合、内蔵ブラウザーで SAML SSO ログインダイアログを起動するには、Parallels RAS Client for Windows 19.3 以降を使用します。

- ビルトインのブラウザーを使用している場合は、[ブラウザーのウィンドウを開いてログアウトを完了] オプションが使用されます。この場合、SAML のログアウトを制御することはできません。それでこのオプションを選択すると、SAML からのログアウトを実行するための URL が開きます。デフォルトでは、この Web ページは表示されませんが、ブラウザーでの操作が必要な場合は、このオプションを有効にすることができます。

詳細については、[SAML SSO 認証]（p. 423）を参照してください。

セッション事前起動

ユーザーがリモートアプリケーションを開くときには、まずセッションを起動することが必要です。セッションの起動には時間がかかるので、ユーザーはアプリケーションが起動するまで待つことになります。ユーザーエクスペリエンスを改善するため、ユーザーが実際にアプリケーションを開く前に、あらかじめセッションを起動できるようになっています。

セッションの事前起動を有効（または無効）にするには、[モード] ドロップダウンリストで以下のいずれかを選択します。

- オフ: セッション事前起動は使用されません。
- 基本: ユーザーがアプリケーションのリストを取得した時点で、セッション事前起動が行われます。数分以内にユーザーがアプリケーションを開くという仮定が、前提になっています。セッションは、10 分間アクティブな状態になります。その時間内にユーザーがアプリケーションを開かないと、クライアントがセッションから切断されます。
- マシンラーニング: ユーザーがアプリケーションのリストを取得すると、その行動に基づいてセッション事前起動が行われます。このオプションを有効にすると、ユーザーが特定の曜日にアプリケーションを起動する行動を Parallels Client が記録して分析します。ユーザーが通常アプリケーションを開く数分前に、セッションを開始します。

セッション事前起動はバックグラウンドで実行されるので、ユーザーが画面上でウィンドウやメッセージボックスを見ることはありません。ユーザーがアプリケーションを起動すると、事前に起動されたセッションが使用されるため、非常に早く起動できます。

セッション事前起動を使用してはならない場合のルールを設定できます。次のオプションを利用できます。

- [セッションの事前起動を行わない] リストを使用して、事前起動を使用しない日付を指定できます。プラス記号のアイコンをクリックして、日付を選択してください。このリストに複数の項目を組み込めます。
- 公開済みのリソースをセッション自動起動スキームから完全に除外することもできます。このようにすれば、リソースは分析対象から除外され、Parallels Client がセッションの事前起動を行うかどうかを判定するときにその対象から除外されます。たとえば、セッション事前起動の対象から除外したいサーバーがある場合、そのサーバーによってホストされているすべての公開済みリソースについて、セッション事前起動の対象から外すためフラグを立てることができます。公開済みリソースをセッション事前起動から除外するには、RAS Console で [公開済みリソース] に移動して、[セッションの事前起動から除外] オプションを選択します。

ローカルプロキシアドレス

ここでは、ローカルの RDP プロキシをどの IP アドレスにバインドするかを設定します。[VPN のシナリオでゲートウェイモードを使用する場合は IP アドレス 127.0.0.1 を使用する] オプションを選択します。この設定を有効にする必要があります。この設定を無効にすると、VPN を使用しているときにユーザーがアプリケーションやデスクトップを開くことができなくなる可能性があります。この設定は、Windows 用 Parallels Client のみに適用されます。

ディスプレイ

ディスプレイ設定を構成するには、[ディスプレイ] ノードを選択し、下記のグループの設定を構成します。

設定

希望するビデオアクセラレーションモードと色深度を選択します。

マルチモニター

複数のモニターがユーザーのコンピューターに接続されている場合、どのモニターをセッションに使用するかを指定します。

次のオプションを利用できます。

- すべて: すべてのディスプレイです。
- プライマリ: プライマリのディスプレイを使用します。
- 選択済み: ユーザーは、1 つまたは複数のディスプレイを手動で選択できます。公開済みデスクトップでこのオプションを使用するには、[公開] カテゴリで [フルスクリーン] を選択し、公開済みデスクトップを選択してから、[デスクトップ] タブ > [デスクトップサイズ] を選択する必要があります。

公開アプリケーション

以下のオプションを指定します。

- プライマリデスクトップのみ使用: プライマリモニターで公開済みアプリケーションを開始するには、このオプションを選択します。ユーザーのコンピューターに接続されている他のモニターは使用されません。
- 動的なデスクトップのサイズ変更を使用する: 公開済みリソースにローカルデスクトップの表示設定を適用したい場合は、このオプションを選択します。

デスクトップオプション

[デスクトップオプション] を次のように指定します。

- スマートサイズ: スマートサイズオプションを選択します。[スケール（ウィンドウに合わせる）] オプションでは、リモートデスクトップが接続ウィンドウに合わせてスケーリングされます。[サイズ変更（解像度の更新）] オプションでは、ウィンドウサイズに応じて解像度が動的に更新されます（再接続の必要はありません）。スマートサイズを無効にするには、[無効] を選択します。
- ランチャーの中のデスクトップ: Parallels Client 内の公開デスクトップにアクセスするには、このオプションを有効にします。
- マルチモニターを有効にする: 公開済みデスクトップを接続されたすべてのモニターに分散して表示するには、このオプションを有効にします。

- 接続バーをフルスクリーン表示フルスクリーンモードで接続するとき、接続バーをピン留め、固定解除、または非表示にするかどうかを指定します。

ブラウザー

このセクションは、Parallels Web Client のみが対象です。リモートアプリケーションをデフォルトでウェブブラウザーの同じタブで開くか新しいタブで開くかを指定します。

印刷

[ポリシーのプロパティ] ダイアログの [印刷] ノードでは、印刷オプションを構成できます。

[テクノロジー] セクションで、プリンターをリモートコンピューターにリダイレクトする際に使用するテクノロジーを選択します。

- なし: プリンターリダイレクトを使用しません。
- RAS ユニバーサルプリントテクノロジー: RAS ユニバーサルプリントテクノロジーを使用する場合は、このオプションを選択します。
- Microsoft ベーシックプリントリダイレクトテクノロジー: Microsoft Basic 印刷テクノロジーを使用する場合は、このオプションを選択します。
- RAS ユニバーサルプリントと Microsoft ベーシックリダイレクトテクノロジー: Parallels RAS と Microsoft のテクノロジーを両方使用する場合は、このオプションを選択します。

注: RAS HTML 5 Client で印刷を使用する場合、以下のルールが適用されます。[なし] または [Microsoft ベーシックプリント] が選択されている場合は、リモートセッションで印刷のリダイレクトを行うことはできません。[RAS ユニバーサルプリント] または [RAS ユニバーサルプリントおよび Microsoft ベーシックプリント] が選択されている場合は、リモートセッションで RAS ユニバーサルプリントが使用されます。

RAS ユニバーサルプリント

[RAS ユニバーサルプリントテクノロジー] を選択した場合、[リダイレクトプリンター] ドロップダウンリストを使用して、クライアント側にあるすべてのプリンターがリダイレクトされるか、デフォルトプリンターのみがリダイレクトされるか、指定したプリンターのみがリダイレクトされるかを指定します。

上記のステップで [指定したもののみ] を選択した場合は、[タスク] > [追加] をクリックします。プリンター名を入力し、[オプション] ボタンをクリックします。ダイアログが開いたら、以下の設定を指定します。

[フォーマットの選択] ドロップダウンリストで、印刷のデータフォーマットを選択します。

- Portable Document Format（PDF）を印刷します: Adobe PDF。このオプションでは、PDF 文書を印刷できるローカルアプリケーションをインストールする必要はありません。必要なすべてのライブラリは、すでに Parallels Client と共にインストールされています。
- 外部アプリケーションで PDF を表示します: このオプションを使用するには、PDF 文書を表示できるローカルアプリケーションがインストールされている必要があります。サポートされないアプリケーションもありますのでご注意ください。たとえば、Windows に組み込まれている PDF ビューアーはサポートされていないため、Adobe Acrobat Reader（または同様のアプリケーション）をインストールしておく必要があります。
- 外部アプリケーションで PDF を印刷します: このオプションは、上記の [PDF の表示] オプションと同様に機能します。また、PDF 文書を印刷できるアプリケーションもローカルにインストールしておく必要があります。
- Enhanced Meta File（EMF）: ベクター形式と組み込みフォントを使用します。
- Bitmap（BMP）: ビットマップ画像。

[クライアントプリンターの設定] セクションで次のいずれかを選択します。

- すべてのプリンターにサーバーの環境設定を使用: このオプションが選択されている場合、ユーザーがリモートアプリケーションで [印刷] をクリックすると、一般的なプリンター環境設定のダイアログが表示されます。このダイアログでは最低限のオプションのみを選択できます。
- すべてのプリンターにクライアントの環境設定を使用: このオプションが選択されている場合、ユーザーがアプリケーションで [印刷] をクリックすると、ローカルプリンター環境設定のダイアログが表示されます。このダイアログには、ユーザーがローカルコンピューターにインストールした特定のプリンターのすべてのオプションが含まれています。複数のプリンターをインストールしている場合、印刷に使用する特定のプリンターのネイティブ環境設定のダイアログが開きます。
- 次のプリンターにクライアントの環境設定を使用: このオプションは、[すべてのプリンターにクライアントの環境設定を使用] オプション（上記）と同様に機能しますが、どのプリンターでこのオプションを使用するかを選択できます。このオプションを選択してから、下に表示される一覧で 1 台以上のプリンターを選択します。プリンターを選択しない場合、このリストの最初のオプションと同様に、一般的なプリンター環境設定ダイアログが使用されます。

デフォルトプリンターの設定

デフォルトのプリンター設定を構成するには、[デフォルトプリンターの設定を変更] ボタンをクリックします。

デフォルトのプリンターリストには、クライアントからリモートコンピューターにリダイレクトできるプリンターが表示されます。

- デフォルトのプリンターを無効にするには、[<なし>] を選択します。
- デフォルトのローカルプリンターをリダイレクトするには、[<デフォルトのローカルプリンター>] を選択します。
- [<カスタムプリンター>] を選択した場合、カスタムプリンターを指定できます。[カスタム] フィールドに挿入したプリンター名に一致する最初のローカルプリンターが、リモートコンピューターでデフォルトのプリンターとして設定されます。

[実際のプリンター名と合致すること] を選択すると、[カスタム] フィールドに挿入された名前が完全一致で検索されます。リモートプリンター名は元のプリンター名と一致しない可能性があるため、注意してください。サーバーの設定またはポリシーによっては、ローカルプリンターがリダイレクトされないこともあります。

[強制デフォルトプリンター] オプションは、プリンターがデフォルトとして強制される期間を指定します。接続が確立された後、この時間内にデフォルトのプリンターが変更された場合、そのプリンターの設定はデフォルトに戻されます。

[ローカルのデフォルトプリンターが変更される場合、リモートのデフォルトプリンターを更新します] オプションを選択すると、ローカルのデフォルトプリンターが変更された場合にリモートのデフォルトプリンターも自動的に変更されます。新しいプリンターは事前にリダイレクトされている必要があります。

Windows 10 および 11 に関するメモ

Windows 10 および 11 には、最近使用されたプリンターまたは頻繁に使用されるプリンターを自動的にデフォルトのプリンターに設定する機能があります。これにより、RD セッションホスト、ゲスト VM、リモート PC でのデフォルトのプリンター制御が失敗する場合があります。この問題を解決するには、Windows 10 および 11 のデフォルトのプリンター管理を無効にする必要があります。グループポリシーを使用してこの機能を無効にするには、次の手順を実行します。

1 グループポリシーエディターを開きます。

2 [ユーザー構成] > [管理用テンプレート] > [コントロールパネル] > [プリンター] に移動します。

3 [Windows での通常使うプリンターの管理を無効にします] ポリシーを見つけ、有効にします。

4 ドメインに接続されているすべてのコンピューターにグループポリシーを適用します。

GUI またはレジストリエディターを使用して、Windows 10 および 11 でデフォルトのプリンター管理をローカルで無効にすることもできます。

1 Windows 10 または 11 コンピューターで、[スタート] をクリックし、次に "歯車" アイコンをクリックして、[設定] ページを開きます。

2 [プリンターとスキャナー] タブで、[Windows で通常使うプリンターを管理する] オプションを [オフ] に設定します。

レジストリエディターを使用する場合は、以下の手順を実行します

1 レジストリエディター（regedit）を開きます。

2 HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows に移動します。

3 新しい DWORD 項目を作成し、LegacyDefaultPrinterMode と名前を付けます。

4 項目の [値] データを 16 進に変更し、値のデータ [1] に設定します。

デフォルトのプリンター管理を無効にすることに加え、[従量制課金接続でのダウンロード] オプションを [設定] > [デバイス] > [プリンターとスキャナー] で有効にする必要があります。

スキャン

[ポリシーのプロパティ] ダイアログの [スキャン] ノードでは、公開済みのアプリケーションでスキャナーが必要な場合に使用するスキャナーを指定できます。

- 使用: スキャンテクノロジーを選択できます。RAS ユニバーサルスキャンでは、TWAIN または WIA リダイレクトが使用されます。これにより、アプリケーションでは、ローカルコンピューターに接続されているハードウェアタイプに応じて、どちらかのテクノロジーが使用されます。[なし] を選択すると、スキャンは無効になります。
- スキャナーをリダイレクト: コンピューターに接続されているスキャナーをリダイレクト対象として選択します。[すべて]（接続されているすべてのスキャナーがリダイレクトされる）または [指定したもののみ]（表示されるリストで選択したスキャナーのみがリダイレクトされる）を選択できます。

オーディオ

[ポリシーのプロパティ] ダイアログのノードでは、リモートオーディオの再生と録音の設定を構成できます。

[リモートオーディオの再生] セクションの [場所] ドロップダウンリストで、以下のリモートオーディオ再生オプションのいずれかを選択します。

- このコンピューターで開く。リモートコンピューターからのオーディオがローカルコンピューターで再生されます。
- 再生しない: リモートコンピューターからのオーディオがローカルコンピューターで再生されず、リモートコンピューターでもミュートされます。
- リモートコンピューターで再生する: オーディオはローカルコンピューターでは再生されませんが、リモートコンピューター上では通常どおりに再生されます。

音質を調整するには、[音質] ドロップダウンリストを使用します。

- 利用可能な帯域幅に基づいて動的に調整: このオプションでは、接続速度に応じて音質が上下します。接続が速いほど高い音質設定が使用されます。
- 常に中程度の音質を使用: 音質は中程度のレベルに固定されます。可能な限り最高の音質が必要なく、利用可能な帯域幅をむしろグラフィックに使用する場合、このオプションを利用できます。
- 常に圧縮した音質を使用: 音質は最高のレベルに固定されます。接続が非常に高速で、可能な限り最高の音質が必要な場合は、このオプションを選択します。

[録音を有効化（該当する場合）] オプションでは、リモートコンピューターでオーディオの録音を有効にできます。たとえば、ローカルコンピューターでマイクに向かって話し、リモートコンピューター上の録音アプリケーションを使用して自分の声を録音できます。

キーボード

[ポリシーのプロパティ] ダイアログの [キーボード] ノードで、押すキーの組み合わせ（Alt+Tab など）を適用する方法を選択します。

- ローカルコンピューター上: キーの組み合わせはローカルコンピューター上で実行されている Windows に適用されます。
- リモートコンピューター上: キーの組み合わせはリモートコンピューター上で実行されている Windows に適用されます。

- フルスクリーンモードのみ: キーの組み合わせは、フルスクリーンモードのときのみリモートコンピューターに適用されます。

必要に応じて、[Unicode 文字を送信] を選択またはクリアします。

ローカルデバイスおよびリソース

[ポリシーのプロパティ] ダイアログの [ローカルデバイスおよびリソース] ノードを使用して、リモートセッションでローカルリソースをどのように使用するかを構成します。

クリップボード

リモートセッションでのクリップボードの動作を有効化または無効化します。右側のペインで、以下のクリップボードリダイレクトオプションのいずれかを選択します。

- クライアントからサーバーのみ: クライアントからサーバーアプリへのコピー & ペーストのみです。
- サーバーからクライアントのみ: サーバーアプリからクライアントへのコピー & ペーストのみです。
- 双方向: 双方向にコピー & ペーストします。
- 無効: クリップボードを無効にします。

注: このオプションをオフにすると、Parallels Web Client の影響を受けるユーザー用のリモートクリップボード機能も無効になります。詳細については、「リモートクリップボードの使用」（p. 479）を参照してください。

ディスクドライブとフォルダー

[ディスクドライブとフォルダーのリダイレクトを許可] オプションを選択し、リダイレクトするローカルドライブを選択するか、 [利用できるすべてのディスクドライブを使用] を選択します。

[後でプラグインするディスクドライブも使用します] オプションを選択する場合、後でローカルコンピューターに接続するディスクドライブはリモートセッションで自動的に利用できるようになります。このオプションは、Windows 用 Parallels Client のみに適用されることに注意してください。

[キャッシュ] ドロップダウンリストで、リダイレクトされたドライブ上のファイル参照やナビゲーションをより高速にするドライブリダイレクトキャッシュハットを有効にするかどうかを選択できます。

- 無効: ドライブリダイレクトのキャッシュが無効になっています。
- 有効: ドライブリダイレクトのキャッシュが有効になっています。
- 高速モード: 上述したのと同様ですが、より高速なブラウジングを優先するため、ファイルエクスプローラーの特定のデコレーション機能が無効になっています。

> **注:** このオプションは、Parallels Client for Windows のみに適用されます。

デバイス

このペインでは、ローカルデバイス一般をリダイレクトするかどうか、利用できるすべてのデバイスを使用するかどうか、また後でプラグインするデバイスも使用するかどうかを指定します。

リダイレクト可能なローカルデバイスには、サポートされているプラグアンドプレイデバイス、メディア転送プロトコル（MTP）に基づくメディアプレーヤー、画像転送プロトコル（PTP）に基づくデジタルカメラが含まれます。

ディスクドライブとスマートカードは、専用の [ディスクドライブとフォルダー] と [スマートカード] オプションを使用してリダイレクトされることに注意してください。

ビデオキャプチャデバイス

ビデオキャプチャデバイスを指定して、ユーザーデバイスからリモートセッションにリダイレクトします。これは高レベルのリダイレクトであり、マイク付きのウェブカメラなどのコンポジット USB デバイスをリダイレクトできます。

- デバイスのリダイレクトを許可: どのビデオキャプチャデバイスをリダイレクトするか選択できます。
- 利用できるすべてのデバイスを使用: すべての利用可能なデバイスをリダイレクトします。
- 後で接続するデバイスも使用する: また、セッション開始後に接続するデバイスも使用されます。なお、このオプションを無効にした場合、新たに接続されたデバイスを利用可能にするためには、セッションを再起動する必要があります。

ポート

LPT ポートと COM ポートをリダイレクトするかどうかを選択します。

スマート カード

スマートカードをリダイレクトするかどうかを選択します。[プライマリ接続] ペインでスマートカードを認証タイプとして選択している場合は、スマートカードリダイレクトが自動的に有効になり、このオプションがグレーアウトされます。

ペン入力とタッチ入力

以下の機能を有効または無効にします:

- 筆圧感知をサポートしたペン入力のリダイレクト。

  注: リモートデスクトップペン入力のリダイレクトは、以下のオペレーティングシステムをサポートしています: Windows Server 2016 から Windows Server 2022 まで、Windows 10 バージョン 1607 から Windows 11 まで。

- Windows のタッチ入力のリダイレクト。Windows のタッチ入力をリダイレクトすると、ユーザーはタッチ対応デバイスから、タッチ、ホールド、リリースの操作といった Windows のネイティブのタッチジェスチャーを使用できます。これらの操作は、リモートのアプリケーションやデスクトップに、対応するマウスクリックとしてリダイレクトされます。このオプションを使用すると、アプリの互換性の問題が発生した場合に、タッチ入力のリダイレクトを無効化できます。

注: このポリシーは、Parallels Client for Windows および Parallels Web Client にのみ適用されます。

AVD 向けのマルチメディアリダイレクト

リモートの Azure Virtual Desktop ホスト上のブラウザーで再生されるビデオコンテンツを視聴できるようにします。この機能を使用するには、AVD ホストでリダイレクトを設定する必要もあります（https://learn.microsoft.com/en-us/azure/virtual-desktop/multimedia-redirection?tabs=edge#requirements を参照）。

注: このポリシーは、Parallels Client for Windows 10（1909 以降）/Windows 11 にのみ適用できます。

注: アドバンスドクライアント機能セットを使用する場合、Azure Virtual Desktop 上のマルチメディアリダイレクトは使用できません。

注: Azure Virtual Desktop のマルチメディアリダイレクト機能は、現在プレビュー版です。マルチメディアリダイレクトをサポートするウェブサイトのリストについては、https://learn.microsoft.com/en-us/azure/virtual-desktop/multimedia-redirection-intro を参照してください。

ファイル転送

リモートセッションでのファイル転送を有効化します。ファイル転送を有効にするには、このノードを選択し、右側のペインにある [ファイル転送を許可する] ドロップダウンリストで必要なオプションを選択します。詳細については、「リモートファイル転送を構成する」（p. 538）を参照してください。

エクスペリエンス

[ポリシーのプロパティ] ダイアログの [エクスペリエンス] ノードでは、接続速度と圧縮の細かい設定を行えます。

パフォーマンス

パフォーマンスを最適化するために接続速度を選択してください: 状況に応じて接続タイプを選択してから、有効にするエクスペリエンスオプションを選択します。通常、100 Mbps 以上のローカルネットワーク上でリモートサーバーに接続する場合、すべてのエクスペリエンスオプションを有効にすることをお勧めします。[接続品質を自動的に検出] を選択している場合は、エクスペリエンスオプションがデフォルトで有効になります。ただし、一部のオプションは実際の速度次第で自動的に無効になる場合があります。

ウィンドウの移動/サイズ変更の強化: デスクトップ上でリモートアプリケーションウィンドウを移動またはサイズ変更しているときにユーザーの環境にグラフィックスアーチファクト（暗い色の正方形）が表示される場合は、このオプションを有効にします。この問題は、リモートアプリケーションが Windows Server 2016、2019 または 2022 にホストされているときと、[ドラッグ時にウィンドウの内容を表示] オプションが有効なときに発生する場合があります。この問題は他のバージョンの Windows では発生しません。

圧縮

圧縮を有効にして、接続効率を向上することをお勧めします。選択可能な圧縮オプションには次のようなものがあります。

RDP 圧縮を有効にする: RDP 接続のために圧縮を有効にします。

ユニバーサルプリント圧縮ポリシー: 圧縮タイプは、環境の仕様に基づいて選択する必要があります。次のオプションから選択できます。

- 圧縮が無効にされました: 圧縮は使用されません。
- 最速のスピード（より少ない CPU を使用）: 圧縮は最速のスピードに最適化されます。
- 最適なサイズ（より少ないネットワークトラフィックを使用）: 圧縮はネットワークトラフィックを節約するように最適化されます。
- 接続速度に応じて: 接続速度が速いほど、圧縮レベルが低くなり、圧縮するデータサイズが最小になります。

ユニバーサルスキャン圧縮ポリシー: このドロップダウンリストには上記のユニバーサルプリント圧縮と同じオプションがあります。環境の仕様に応じて圧縮タイプを選択します。

ネットワーク

[ポリシーのプロパティ] ダイアログの [ネットワーク] ノードを使用して、Parallels Client 用のプロキシサーバーを構成します。

[プロキシサーバーの使用] オプションを選択し、次のリストからプロトコルを選択します。

- SOCKS4: ネットワークファイアウォールのサービスを透過的に使用するには、このオプションを有効にします。
- SOCKS4A: 接続できないクライアントが宛先ホストの名前を解決してホスト名を指定できるようにするには、このオプションを有効にします。
- SOCKS5: 認証を使用して接続できるようにするには、このオプションを有効にします。
- HTTP 1.1: 標準の HTTP 1.1 プロトコル接続を使用して接続するには、このオプションを有効にします。

プロキシホストのドメイン名または IP アドレスとポート番号を指定します。

SOCKS5 および HTTP 1.1 プロトコルの場合は、[プロキシは認証を必要] オプションを選択します。認証については、[ユーザーのログイン情報を使用する] オプションを選択するか、所定のフィールドでユーザー名とパスワードを指定します。

サーバー認証

[ポリシーのプロパティ] ダイアログの [サーバー認証] ノードを使用して、RD セッションホスト、リモート PC、またはゲスト VM の認証に失敗した場合の対応を指定します。

[認証に失敗した場合] ドロップダウンリストで、次のオプションのいずれかを選択します。

- 接続: ユーザーは、サーバーの認証情報を無視して、接続を続けることができます。
- 警告: ユーザーは認証情報について警告を受けますが、接続するかどうかの選択肢は残されています。
- 接続しない: ユーザーは接続できません。

詳細設定

[ポリシーのプロパティ] ダイアログの [詳細設定] ノードを使用すると、デフォルトの動作または Parallels Client をカスタマイズできます。

次のプロパティを指定できます。

- クライアントのシステムカラーを表示する: リモートデスクトップで指定されているカラーではなく、クライアントのシステムカラーを使用する場合は、このオプションを有効にします。
- クライアントシステム設定を使用: RD セッションホストで指定されている設定ではなく、クライアントのシステム設定を使用する場合は、このオプションを有効にします。
- サーバーで構成されたショートカット作成: 公開されたアプリケーションごとに、管理者はクライアントのデスクトップおよびスタートメニューに作成できるショートカットを構成できます。ショートカットを作成するには、このオプションをオンにします。ショートカットを作成しない場合は、このオプションをオフにします。
- サーバーから関連付けられたファイルの拡張子を登録する: 公開されたアプリケーションごとに、管理者はファイル拡張子の関連付けを作成できます。このオプションを使用して、関連付けられたファイル拡張子を登録するかどうかを指定します。
- クライアントデバイスに URL をリダイレクト: 'http:' リンクを開くときにローカルのウェブブラウザーを使用する場合は、このオプションを有効にします。

- クライアントデバイスに MAILTO をリダイレクト: 'mailto:' リンクを開くときにローカルのメールクライアントを使用する場合は、このオプションを有効にします。
- アプリケーションを起動する際に、常に認証を要求する: このオプションを有効にすると、セッションがアクティブであっても、アプリケーションの起動時に認証情報の入力が求められます。このオプションは、許可されていないユーザーがアプリケーションにアクセスすることを防ぐための追加のセキュリティとして使用できます。たとえば、ユーザー側でセッションを切断する場合、他のユーザーがセッションを引き継いでリモートアプリケーションを実行することはできません。別の例として、ユーザーがアプリ一覧を表示したユーザーポータルを開いたままデバイスの使用を終了する場合（RDP セッションを実行しているかどうかに関わらず）、いずれかのユーザーが新しいアプリケーションや実行中のアプリケーションで別のインスタンスを開こうとすると、認証情報を入力するよう求められます。なお、この機能を有効にするには、[自動ログイン] オプション（p. 511）を無効にする必要があります。それ以外の場合は、保存された認証情報が自動的に使用されます。
- クライアントが実行するコマンドのサーバーからの送信を許可: サーバーから受け取るコマンドをクライアントが実行できるようにするには、このオプションを有効にします。
- 実行する前にサーバーコマンドを確認: このオプションが有効になっている場合は、コマンドがサーバーから実行される前にコマンドを確認するメッセージが、クライアントに表示されます。
- ネットワークレベルの認証: ネットワークレベルの認証を有効にするには、このオプションをオンにします。この場合、クライアントは、サーバーへの接続前に認証を行う必要があります。
- POS デバイスをリダイレクト: ローカルコンピューターに接続されているバーコードスキャナーや磁気読取装置などの Point of Service（POS）デバイスを、リモート接続で使用できるようにします。
- Windows 2000 以前のログイン形式を使用: このオプションが選択されている場合は、レガシー（Windows 2000 より前）のログイン形式を使用できます。
- ゲートウェイ接続の RDP-UDP を無効にする: クライアント側で RDP UDP データトンネリングを無効にします。このオプションは、RAS Secure Gateway（ゲートウェイの [プロパティ] ダイアログの [ネットワーク] タブ）で RDP UDP データトンネリングが有効な場合に一部のクライアントでランダムな切断が発生し、他のクライアントでは発生しない場合に使用できます。
- ドライブリダイレクトのダイアログを表示しない: このオプションは、Parallels Client for Mac に影響を与えます。Mac ユーザーが Parallels RAS に接続すると、デフォルトで、[ホームフォルダーへのアクセス権を付与] （ドライブリダイレクト）ダイアログが自動的に開きます。このオプションが無効のときや、クライアントポリシーがまったく存在しないとき

にこのようになります。ユーザーは、このダイアログを使用して、ローカルディスクドライブのどのフォルダーをリモートアプリケーションで利用できるようにするかを構成できます。このオプションを有効にすると、ユーザーにこのダイアログが表示されなくなります。詳しい説明については、下記を参照してください。

ドライブリダイレクトはクライアントポリシー経由で構成できないため、Mac ユーザーは自分自身でこれを行う必要があります。ダイアログを自動的に表示することで、ローカルフォルダー構成手順の作業をユーザーに促すことができます。一方、ユーザーがローカルドライブをリダイレクトする必要がない場合は、ダイアログの自動表示を無効にできます。なお、このダイアログは、Parallels Client for Mac から [接続プロパティ] > [ローカルリソース] を開き、[ディスクドライブ] オプションを選択し、[構成]をクリックすることで、今までどおりいつでも手動で実行できます。

このオプションが無効の場合（またはクライアントポリシーが定義されていない場合）は、ユーザーが Parallels RAS に初めて接続するときにダイアログが少なくとも 1 回表示されます。このときに、ユーザーはローカルフォルダーを構成するか、[今後確認しない] オプションを選択することができます。どちらの場合も、このダイアログは今後ユーザーに表示されません。Mac ユーザーは、[接続プロパティ] > [詳細] を選択し、[ドライブリダイレクトのダイアログを表示しない] オプションをクリアすることで、[今後確認しない] の選択をリセットできます。

クライアントポリシーオプションの構成

[クライアントオプション] ノードでは、クライアントポリシーオプションを構成できます。ノードを選択し、下記のように、その下にある個別の項目を選択して構成します。

接続

[接続] ペインで、次のオプションを指定します。

- 接続バナー: 接続を確立中に表示するバナーを選択します。
- 接続済み RAS Connection の更新間隔: このオプションを選択して、接続を自動的に更新する間隔を指定します。これにより、Parallels Client の [公開済みのリソース] リストが更新されます。
- すべてのセッションが終了している場合。すべてのユーザーセッションが終了している場合の動作を指定します:
  - 何もしない。何も起こりません。
  - ワークステーションをロック。コンピューターがロックされます。

- ワークステーションからサインアウト。現在のユーザーがアカウントからサインアウトされます。

> 注: ワークステーションをロックオプションは、キオスクモードで管理されているデバイスではサポートされていません(p. 497)。

ログ

Parallels Client のログレベルを指定します。次のオプションから選択します。

- 標準
- 拡張
- 詳細

通常は [標準] ロギングを使用してください。Parallels Client で問題が発生した場合、[拡張] または [冗長] を選択し、開始日時、期間を設定することで、一時的にロギングレベルを上げることができます。なお、開始日時は、ローカルクライアントのタイムゾーンに対応しています。ロギングを実行するには、Parallels Client が起動している必要があります。[拡張] レベルまたは [冗長] レベルがすでに有効であるときに Parallels Client が起動した場合、指定したレベルは元の設定時間の残時間に限り有効となります。この間にポリシーが変更されると、それに応じて実際のロギングレベルの設定が再度適用されます。

アップデート

Parallels Client の起動時にアップデートをチェックする場合は、[起動時にアップデートをチェックする] オプションを選択し、アップデート URL を指定します。URL は、Parallels ウェブサイトをポイントすることができ、またアップデートをローカルネットワークに保存して、このローカル URL を使用することもできます。ローカルアップデートサーバーを構成する方法の詳細については、https://kb.parallels.com/123658 を参照してください。

> **注:** このオプションは、Windows 用 Parallels Client でのみ機能します。Mac 用 Parallels Client は、App Store からのみアップデートできます。Linux 用 Parallels Client ではこの機能はサポートされていません。

PC キーボード

特定のキーボードを強制使用するには、[PC キーボードを強制使用] を選択し、ドロップダウンリストからキーボードのレイアウトを選択します。選択したレイアウトは、この特定のレイ

アウトをサポートする Parallels Client のバージョンでのみ使用でき、また使用されることに注意してください。

Single SignOn

Windows 用 Parallels Client は、インストールして Parallels RAS にサインインするために使用できる独自の SSO コンポーネントを搭載しています。Windows コンピューターですでにサードパーティの認証情報プロバイダーコンポーネントを使用している場合は、まず、シングルサインオンを設定なしですぐに利用できるかどうかを試してみる必要があります。利用できない場合は、Parallels RAS と Parallels Client を構成して、サードパーティの認証情報プロバイダーコンポーネントのラッパーとして機能するように Parallels RAS SSO コンポーネントを使用する必要があります。

Parallels RAS SSO をラッパーとして使用するには、サードパーティコンポーネントを指定して、[サードパーティの認証情報プロバイダーコンポーネントを強制的にラップする] オプションを選択し、所定のフィールドでコンポーネントの GUID を指定します。GUID は、Parallels Client で次のように取得できます。

1. サードパーティコンポーネントがインストールされているコンピューターに Parallels Client をインストールします。
2. Parallels Client で、[ツール] > [オプション] > [Single SignOn]（タブページ）に移動します。
3. [...を強制的にラップする] オプションを選択し、ドロップダウンリストでプロバイダーを選択します。
4. [GUID をクリップボードへコピー] ボタンをクリックして、コンポーネントの GUID を取得します。

また、RAS Console で招待メールを設定するときにもコンポーネントの GUID を指定する必要があります。招待メールを設定していない場合は、次の手順に従って設定できます。

1. RAS Console で、[開始] カテゴリーを選択し、右ペインの [ユーザーを招待] アイテムをクリックします。
2. ウィザードの 2 ページ目（ターゲットプラットフォームおよび接続オプション）で、[詳細] ボタンをクリックします。
3. 開いたダイアログで、[サードパーティの SSO コンポーネントを強制的にラップする] オプションを選択し、コンポーネントの GUID を指定します。

詳細については、「ユーザーを招待」セクション（p. 52）を参照してください。

Windows コンピューターでポリシーが適用された後に、Parallels Client は、指定されたサードパーティ認証情報プロバイダーを使用するように自動的に構成されます。

詳細

このペインを使用して、Advanced Client オプションを指定します。詳細については以下で説明します。

グローバル

- 常に手前に表示: この機能が有効な場合、他のアプリケーションがランチャーを隠すことはありません。
- 接続ツリーを表示: 接続ツリーを表示します。
- 閉じる/エスケープキーでトレイに最小化する: [閉じる] ボタンをクリックするかエスケープキーを押したときに Parallels Client をシステムトレイに配置するには、この機能を有効にします。
- グラフィックアクセラレーションを有効化（Chrome クライアント）:
- サーバーの証明書が認証されていなくても警告を発しない: SSL 経由で RAS Secure Gateway に接続するとき、証明書が認証されていなければ、警告メッセージが表示されます。このオプションを有効にすると、この警告メッセージを無効にすることができます。
- マウスボタンの入れ替え: この設定を有効にすると、リモートコンピューターでマウスボタンが切り替えられます。
- DPI 対応: クライアントの DPI 設定に応じて、公開されたアプリケーションが強制的に DPI 対応になります。この機能は、Windows 8.1 以降で動作します。
- ウェブまたはショートカット項目の開始時に RAS 接続を自動的に追加する: このオプションでは、まだリストに表示されていない接続に含まれる項目を開始すると、接続設定が Parallels Client に追加されます。
- RAS に自動接続する際、プロンプトメッセージを表示しない: 接続の自動追加時にプロンプトメッセージを無効にするには、このオプションを有効にします。
- エラーメッセージを自動的に閉じる: エラーが原因でセッションが切断されると、エラーは 15 秒後に自動的に削除されます。
- 終了時にセッションの Cookie を削除する: ユーザーがログオンするとき、Parallels RAS のログオンクッキーはクライアント側に保持されます。これによりユーザーは、再認証をし

なくても、Parallels RAS に再接続できます。ユーザーが Parallels Client を閉じるときにクッキーを削除するには、このオプションをオンにします。

- 拡張ロギングを有効化: 拡張ロギングを有効化します。
- Client で UDP をオフにする: Parallels Client for Windows からの UDP トラフィックをオフにします。

言語

Parallels Client が使用する言語を指定します。[デフォルト] オプションでは、クライアントのオペレーティングシステムで使用される主な言語を使用します。

印刷

- 足りないフォントを自動インストール: サーバーに自動フォントがインストールされている場合は、セッションの接続時に自動フォントが利用できるようになります。
- RAW プリント対応: この設定を有効にすると、RAW 形式でデータを送信するアプリケーションでプリントできます。
- 配布不能フォントデータをイメージへ変換: RAS ユニバーサルプリント中に、ドキュメントに配信不能なフォントが含まれていると、各ページが画像に変換されます。
- キャッシュプリンターハードウェア情報: プリンターのハードウェア情報をローカルにキャッシュすると、RAS ユニバーサルプリンターのリダイレクトが速くなります。
- 30 日ごとにプリンターのハードウェア情報を更新: プリンターのハードウェア情報のキャッシュは、30 日間に変更がなかった場合でも強制的に更新されます。このオプションをオフにすると、キャッシュは、既知の変更があった場合のみ更新されます。
- キャッシュ（RAS Universal Printing）埋め込みフォント: 埋め込みフォントをローカルにキャッシュすると、RAS ユニバーサルプリントの処理時間が短くなります。

Windows クライアント

- アプリケーションの起動時にクライアント画面を表示しない: このオプションが有効な場合、アプリケーションが起動されたら、ランチャーはシステムトレイ内で最小化されます。
- Windows の起動時、自動的に起動する: このオプションにより、クライアントのスタートメニューフォルダーにショートカットが作成され、Windows 起動時に Parallels Client が自動的に開始されます。

RemoteFX USB リダイレクト

- その他のサポートされている RemoteFX USB デバイスからすべてのユーザーへの RDP リダイレクトを許可します。この設定は、Windows 用 Parallels Client のみに適用されます。Parallels RAS の外部で標準の RemoteFX USB リダイレクト機能を動作させるには、グループポリシーを介して有効化する必要があります。この画面で [RDP リダイレクトを許可する...] オプションを選択すると、GPO と同じように実行され、クライアントマシン上で Windows の対応するレジストリ設定が更新されます。Parallels Client for Windows で USB デバイスをリダイレクトするには、この機能を Windows レジストリで有効化する必要があります。この設定を含むポリシーがクライアントマシンに適用されると、ユーザーには RemoteFX USB リダイレクトが有効になったこと、また Windows を再起動する必要があるということを示すメッセージが表示されます。

コントロールの設定の構成

[コントロールの設定] オプションを使用すると、クライアント側でのさまざまなアクションを制御できます。これらのオプションは、以下の Parallels Client に影響します。

- Windows
- Linux
- Mac
- Android
- iOS

接続

[接続] ペインで、以下のオプションを選択（またはクリア）します。

- RAS 接続の追加を禁止: ユーザーが [接続の追加] ボタンを押すと、常に RDP 接続が作成されます。
- 標準の RDP 接続の追加を禁止: ユーザーが [接続の追加] ボタンを押すと、常に RAS 接続が作成されます。

パスワード

[パスワード] ペインで、次のオプションを指定します。

- ユーザー名の保存を禁止: Parallels Client では、最後にログインしたユーザーのユーザー名が表示されません。このオプションを選択すると、[パスワードの保存を禁止] オプションが自動的に有効になります。
- パスワードの保存を禁止: この特定の接続用のユーザーには、パスワードを保存するためのオプションが表示されません。パスワードはディスクに一切保存されませんが、ユーザーがアプリケーションを閉じるまでメモリに保持されます。
- パスワードの変更を禁止: この特定の接続用のコンテキストメニューには、パスワードを変更するためのオプションが表示されません。

インポートとエクスポート

[インポートとエクスポート] ペインでは、以下のオプションを指定します。

- 設定のインポートを禁止: このオプションを選択した場合、ユーザーは接続設定を Parallels Client にインポートできなくなります。
- 設定のエクスポートを禁止: このオプションを選択した場合、ユーザーは接続設定を Parallels Client からエクスポートできなくなります。

ゲートウェイリダイレクトの構成

[リダイレクト] オプションを使用すると、既存のユーザーを同じファーム内の RAS Secure Gateway 間で移動することや、さらには、ユーザーを別のファームのゲートウェイにリダイレクトすることまで可能になります。

注: ゲートウェイリダイレクトを設定するときに、ゲートウェイ基準（[基準] ノード）がこれの構成と競合していないことを確認してください。その説明については、このセクションの末尾にある「ゲートウェイ基準」サブセクションをお読みください。

リダイレクトオプションを構成するには、次の操作を実行します。

1 [ポリシーのプロパティ] ダイアログの左ペインの [リダイレクト] ノードを選択します。

2 右ペインで、新しい接続プロパティを以下のように指定します。
   - ゲートウェイのアドレス
   - 接続モード
   - ポート番号
   - 代替アドレス

このポリシーをユーザーのデバイスに適用すると、以下のことが起こります。

- 各デバイスで、Parallels Client の接続設定が自動的に更新されます。
- Parallels Client が新しい接続をテストします。結果が正常だった場合、現在の接続ポリシーが削除され、新しいポリシーが追加されます。
- Parallels Client が、新しい設定を使用して Parallels RAS に接続できない場合、アプリケーションリストは表示されず、リダイレクトポリシーの適用に失敗したことを伝えるエラーメッセージが表示されます。ユーザーは、システム管理者に問い合わせるように勧められます。

ゲートウェイ基準

ポリシーで、[リダイレクト] と [基準] の設定が両方とも有効で構成済みの場合、クライアント側でポリシーが適用されると無限ループが発生し、その結果エラーになることがあります。この状況で考えられる次のシナリオについて検討してください。

- Parallels Client がゲートウェイ”A”に接続してポリシーを適用します。このポリシーによって Parallels Client はリダイレクトされてゲートウェイ”A”に戻ります。Parallels Client が中断してユーザーにエラーが表示されるまで、このループが続きます。エラーの内容は、”リダイレクトポリシー...の適用に失敗しました....” です。
- Parallels Client がゲートウェイ“A”に接続してポリシー“P1”を適用します。このポリシーによって Parallels Client はリダイレクトされてゲートウェイ“B”に移動します。予想どおり、Parallels Client がゲートウェイ“B”に接続してポリシー“P2”を適用します。このポリシーによって Parallels Client はリダイレクトされて、すべての始まりであるゲートウェイ“A”に戻ります。同様に、Parallels Client が中断して上述の同じエラーメッセージが表示されるまで、このループが続きます。

繰り返しになりますが、これが発生する可能性があるのは、[基準] ノードが有効で、指定したゲートウェイが相互に競合する場合のみです。これを回避するには、[基準] ペインの [ゲートウェイ基準] オプションが [クライアントが以下のゲートウェイの 1 つに接続される場合] に設定されていることと、Parallels Client が新しいゲートウェイにリダイレクトされるときに再度同じポリシーが適用されないことを確認します。

クライアントポリシーの後方互換性

Parallels RAS v16.5 から、クライアントポリシーを管理するために新しいアプローチが使用されています。旧バージョンでは、クライアントポリシーにより、パラメーター一式が適用され、クライアント設定を置き換えて、適用されたカテゴリを完全に非表示にします。RAS v16.5

（以降）では、クライアントポリシー設定が小さいグループに分割されていて、クライアント側で各グループを個別に構成および適用できます。たとえば、管理者がポリシーを再設計し、クリップボードのリダイレクトのみを無効にして、残りのローカルデバイスとリソース設定はエンドユーザーが制御できるように残したい場合があります。以前のバージョンでは、これはできませんでした。新しい設計により、管理者はこの目標を容易に達成できます。

このセクションでは、古いクライアントとの後方互換性を達成する方法と新しいクライアントが古いサーバー側のインストールとの互換性を保持する方法について説明します。

新しいクライアントポリシーの実装は、次のように互換性の問題を処理します。

- 古いポリシーのすべての設定は、古い Parallels RAS サーバーから送信されるかのようにクライアントに送信されます。クライアントがポリシーを受信すると、[接続プロパティ] と [オプション]/[環境設定] の設定が、古い設計の観点から正しく設定されます。ただし、ユーザーが一切変更できないようにポリシーが構成されている場合、タブ全体が非表示になります（すべてが無効である場合、オプションを表示する必要がないため）。
- Parallels RAS Console では、古いスタイルのポリシー設定を新しいかのように処理し、アップデートされたグラフィカルユーザーインターフェイスを使用して表示します。
- ポリシーに関しては、Parallels RAS v16.5 クライアントが以前のバージョンの Parallels RAS に接続するとき、クライアントは通常どおりに動作し続け、すべてのポリシー設定は正常に機能します。

Parallels Client に関するポリシー情報

ポリシーがユーザーのデバイスに適用されると、そのポリシーに関する情報が Parallels Client に表示されます。この情報を使用して、正しいポリシーがユーザーのデバイスに配信されたことを確認できます。次の情報が含まれています。

- ID: ポリシー ID は、RAS Console の [ポリシー] リストの [ID] フィールドに表示されます。
- バージョン: ポリシーのバージョン番号は、RAS Console の [ポリシー] リストの [バージョン] フィールドに表示されます。
- RAS 接続: ポリシーが配信された接続の名前です。モバイルデバイスと Web Client にのみ表示されます。

ユーザーのデバイスで実行されている Parallels Client に関する上述の情報と、RAS Console の情報を比較することで、ユーザーのデバイスに適用されたポリシーを確認できます。

接続に適用されたポリシー情報を表示するには次の操作を実行します。

- Parallels Client for Windows/Mac/Linux で、[接続プロパティ] ダイアログを開きます。この情報は、ポリシーが適用されたタブページの下部に表示されます。
- Parallels Client for Android の場合、情報は [設定] 画面の下部に表示されます
- Parallels Client for iOS の場合、RAS 接続の編集画面を開き、[適用されたサーバーポリシーを表示] をタップします（下で説明）。
- RAS Web Client の場合、情報は [設定] ダイアログに表示されます。

Parallels Client のすべての接続プロパティがクライアントポリシーによって管理されている場合でも、ユーザーは、[接続プロパティ] ダイアログを開くことができます。この場合、ダイアログには単一のタブが存在し、そこに適用されたポリシー情報が表示されます。一部の接続プロパティのみがポリシーを介して管理されている場合、ユーザーはそれらのタブとともに、それらに含まれる適用されたポリシー情報を表示できます。

ポリシーにグローバルポリシーオプションが含まれている場合、Parallels Client で適用されたポリシー情報は、次の手順によって表示できます。

- Parallels Client for Windows/Linux の場合、[オプション] ダイアログ（[ツール] > [オプション]）を開きます。
- Parallels Client for Mac の場合、[環境設定]（[Parallels Client] > [環境設定]）を開きます。

適用されたポリシー情報は、接続の場合に表示される情報と同様に、ダイアログの下部に表示されます。

リモートファイル転送を構成する

Parallels RAS を使用して、エンドユーザーはリモートでファイルをリモートサーバーに転送またはリモートサーバーから転送することができます。

注: この文書の作成時点では、ファイル転送が利用できるのは、Parallels Web Client および Parallels Client for Chrome のみです。双方向のファイル転送は、Parallels Web Client でのみサポートされています。Parallels Client for Chrome では、ファイル転送を有効または無効にする設定操作のみ行えます。

リモートファイル転送機能を柔軟に設定できるように、Parallels RAS では以下の 3 つのレベルを設定することができます。

- 「RD セッションホスト、プロバイダー、またはリモート PC」（p. 539）
- RAS ユーザーポータル（p. 540）
- 「Web Client のゲートウェイ設定」（p. 459）
- 「クライアントポリシー」（p. 540）

各レベルで設定したファイル転送設定の優先順位は、上述の順序になります。たとえば、ファイル転送をユーザーポータルで有効にし、RD セッションホストで無効にしている場合、所定のユーザーポータルから所定の RD セッションホストに接続するすべてのユーザーについて、ファイル転送が無効になります。また、RD セッションホストでファイル転送を有効にし、特定のクライアントポリシー（またはユーザーポータル）で無効にすることもできます。このように、ファイル転送を利用できるクライアントと利用できないクライアントを制御することが可能になります。

後続のセクションでは、各レベルでファイル転送を構成する方法について説明します。

サーバーのファイル転送を構成

RD セッションホスト、プロバイダー、リモート PC でリモートファイル転送を構成するには、次の手順を実行します。

1. Parallels RAS Console で、[ファーム] カテゴリーを選択して、中央のペインでサーバータイプ（RD セッションホスト、プロバイダー、リモート PC）を選択します。
2. 右ペインでサーバーを右クリックして、[プロパティ] を選択します。
3. [Agent 設定] タブを選択します。
4. [ファイル転送コマンドを許可] オプションを選択し、[構成] ボタンをクリックします。ダイアログが表示され、以下のようにリモートファイル転送のオプションを指定できます。
5. [方向] ドロップダウンリストで、次のいずれかを選択します。
   - クライアントからサーバーのみ: クライアントからサーバーへのファイル転送のみ。
   - サーバーからクライアントのみ: サーバーからクライアントへのファイル転送のみ。
   - 双方向: 双方向のファイルを転送が可能。
6. [ロケーション] フィールドには、デフォルトのアップロード先として使用するフォルダーの UNC パスを指定します。ここで指定されたパスは、ユーザーがリモートサーバーからファイルをダウンロードしようとしたときの、デフォルトのソースロケーションとしても使用されます。ドロップダウンリストであらかじめ定義されているロケーションから選択するか、

独自のロケーションを指定することができます。Windows の標準的な環境変数である、%USERNAME%、%USERDOMAIN%、%USERPROFILE% を使用することができます。アップロードまたはダウンロードの実行中にロケーションが見つからない場合は、標準（デフォルト）のダウンロードロケーションが使用されます。

7 [位置情報の変更を許可しない] オプションにより、[ロケーション] フィールドで指定された UNC パスをユーザーが変更することを禁止します。このオプションを有効にすると、ファイルのアップロードまたはダウンロードを行う際に、ユーザーが別のロケーションを選択できなくなります。このオプションを無効にすると、ユーザーは別のロケーションを指定できるようになります。

重要: なお、[位置情報の変更を許可しない] オプションでは、ユーザーが指定したリモートロケーションへの直接的なアクセスを禁止することはできません。たとえば、ユーザーがファイルをアップロードしようとするときに、デフォルトのロケーションの UNC パス（自分がアクセスできるパス）をメモし、ファイルエクスプローラーで該当のファイルを開き、プロファイルの任意のフォルダーにコピーすることができます。このような操作を防止するために、ここで指定したロケーション以外のロケーションも制御できるようにする追加の方法を導入する必要があります。

ユーザーポータルでファイル転送を構成する

ユーザーポータルでリモートファイル転送を構成するには、次の手順を実行します。

1 Parallels RAS Console で、[ファーム] > <サイト> > [Secure Gateway] に移動します。

2 右ペインで RAS Secure Gateway を右クリックして、[プロパティ] を選択します。

3 [ユーザーポータル] タブを選択します。

4 [ファイル転送コマンドを許可] オプションを選択し、[構成] ボタンをクリックします。ダイアログが開いたら、次のいずれかを選択します。

- クライアントからサーバーのみ: クライアントからサーバーへのファイル転送のみ。
- サーバーからクライアントのみ: サーバーからクライアントへのファイル転送のみ。
- 双方向: 双方向のファイルを転送が可能。

ユーザーポータルの構成については、「ユーザーポータルの構成」（p. 97）を参照してください。

クライアントポリシーのファイル転送の構成

クライアントポリシーでリモートファイル転送を構成するには、次の手順を実行します。

1. RAS Console で [ポリシー] カテゴリーを選択します。
2. 右ペインでポリシーを右クリックし、[プロパティ] を選択します。
3. 左側のペインで、[セッション] > [ローカルデバイスおよびリソース] に移動します。
4. [ファイル転送] ノードを選択します。
5. 右側のペインの [ファイル転送を許可する] ドロップダウンリストで、以下のいずれかを選択します。
   - クライアントからサーバーのみ: クライアントからサーバーへのファイル転送のみ。
   - サーバーからクライアントのみ: サーバーからクライアントへのファイル転送のみ。
   - 双方向: 双方向のファイルを転送が可能。

クライアントポリシーの詳細については、「クライアントポリシー」（p. 507）を参照してください。

第 23 章

レポート作成

Parallels RAS Reporting は Parallels RAS 管理者が定義済みおよびカスタムの Parallels RAS レポートを実行および表示するのに使用するオプションのコンポーネントです。定義済みのレポートにはユーザーおよびグループのアクティビティ、デバイス情報、セッション情報、アプリケーション使用率が含まれます。独自の基準を使用してカスタムレポートを作成することもできます。この章では、Parallels RAS Reporting をインストールして構成する方法について説明します。

この章の内容

システム要件

オペレーティングシステム要件

Parallels RAS Reporting は、次のいずれかのバージョンの Windows Server を実行するサーバーにインストールする必要があります。

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

.NET Framework 3.5 および .NET Framework 4.5 以降をインストールする必要があります。

Microsoft SQL Server 要件

Parallels RAS Reporting は、次のバージョンの Microsoft SQL Server で使用できます。

- Microsoft SQL Server 2019
- Microsoft SQL Server 2017
- Microsoft SQL Server 2016

RAS 17.1 以降では、SQL Server Reporting Services（SSRS）と SQL Server データベースエンジンを別々のホストに展開できます。

Microsoft SQL Server 2017 および 2019 の使用

Microsoft SQL Server 2017 および 2019 以降を利用することにより、データベースエンジンや SQL Server Reporting Services（SSRS）を異なるホストにインストールできます。Parallels RAS 17.1（およびそれ以降）では、この展開シナリオがサポートされています。つまり、別々のホストにインストールされた SQL Server Reporting Services と、SQL Server データベースエンジンを使用する機能が提供されています。

インストールロケーション

RAS Reporting は、SQL Server Reporting Services が実行されているのと同じサーバーにインストールする必要があります。SSRS とデータベースエンジンが異なるホストにインストールされている場合は、SSRS がインストールされている場所に、RAS Reporting をインストールする必要があります。ご注意ください。

RAS と SQL Server のバージョン互換性情報、また RAS Reporting をインストールするのに使用する必須コンポーネントの場所を次の表に示します。

RAS レポートバージョン	SSRS バージョン	SQL サーバーのバージョン	インストールロケーション
17.1、18.0、19.0	2019	2019	SSRS - RAS Reporting と同一のホスト SQL Server - 別のホストが可能
17.1、18.0、19.0	2017	2019	SSRS - RAS Reporting と同一のホスト SQL Server - 別のホストが可能
17.1、18.0、19.0	2017	2019	SSRS - RAS Reporting と同一のホスト SQL Server - 別のホストが可能
17.1、18.0、19.0	2017	2017	SSRS - RAS Reporting と同一のホスト SQL Server - 別のホストが可能
17.1、18.0、19.0	2017	2016	SSRS - RAS Reporting と同一のホスト

			SQL Server - 別のホストが可能

Microsoft SQL Server は、名前付きのインスタンスとしてインストールする必要があります（デフォルトまたは名前がないインスタンスではありません）。これは、RAS Reporting の動作に、インスタンス名が必要だからです。インスタンス名は、Microsoft SQL Server のインストール時（またはマルチインスタンスの場合は新規に SQL Server インスタンスを作成する際）に指定することができます。詳細については、この後の「Microsoft SQL Server のインストール」セクションを参照してください。

Microsoft SQL Server のインストール

注: 複数のサーバーで実行する Parallels RAS のインストールの場合、Microsoft SQL Server を専用サーバーにインストールすることをお勧めします。

このセクションでは、以下の内容を説明します。

- Microsoft SQL Server 2016 かそれ以前のバージョンをインストール（p. 544）
- Microsoft SQL Server 2017 または 2019 をインストール（p. 547）

Microsoft SQL Server 2016 かそれ以前のバージョンをインストール

SQL Server インスタンス（SQL Server 2016 以前）をインストールするには:

1. Microsoft SQL Server のインストールプログラムを実行し、[カスタム] インストールを選択します。必要なファイルがコンピューターにダウンロードされるのを待ちます。
2. ファイルのダウンロードが完了すると、SQL Server インストールセンターウィンドウが開きます。
3. [インストール] ページで、[新規の SQL Server をスタンドアロンインストールするか既存のインストールに機能を追加する] を選択します。
4. [次へ] をクリックし、画面の指示に従って [機能選択] ページに移動します。
5. [機能選択] ページで、少なくとも以下の SQL Server 機能がインストール用に選択されていることを確認します。
   - データベースエンジンサービス
   - Reporting Services - ネイティブ
6. [次へ] をクリックします。

7 [インスタンスの構成] ページで、[名前付きインスタンス] オプションを選択し、インスタンス名を入力します。インスタンスの名前を付ける際には、以下のオプションがあります:

- Parallels RAS Reporting が使用するデフォルトのインスタンス名である”RASREPORTING”を入力する。この名前を使用すると、後から RAS Console で RAS Reporting をインストールおよび構成する際に指定する必要がなくなります。これは推奨オプションです。
- 別の名前を使用することもできますが、RAS Reporting をインストールして構成する際には、この名前を使用する必要があります。RAS Reporting のインストール手順（本章で後述）には、インスタンス名を指定しなければならない場所が示されているので、手順通りに進めれば見落とすことはありません。なお、インスタンス名には、ダッシュやドットなどの文字は使用できません。

  インスタンス名を入力したら、[インスタンス ID] フィールドにもその名前が設定されていることを確認してください。

8 [次へ] をクリックして、[データベースエンジンの構成] ページに進みます。

9 [データベースエンジンの構成] ページで、[サーバー構成] タブを選択し、以下のユーザーを SQL Server の管理者リストに追加します。

- ローカル管理者（例: Administrator）
- AD 管理者（ローカルサーバーで Parallels RAS Reporting をテストするだけの場合は、このアカウントを除外することができます）。
- SYSTEM（[追加] をクリックしてから、”SYSTEM”と入力し、[名前の確認] をクリックして [OK] をクリックすると、アカウントが”NT AUTHORITY\SYSTEM”としてリストに表示されます）。

10 残りのページでは、デフォルト設定を変更せずにウィザードを完了します。

11 SQL Server のインストールが完了するのを待ちます。[完了] ページで、インストールが成功したことを確認し、ウィザードを終了します。

SQL Server 管理ツールのインストール

また、SQL Server 管理ツール、特に SQL Server Management Studio をインストールする必要があります。これは RAS Reporting で必須とされるツールではありませんが、利便性があり、SQL Server の管理ツールとしては欠かせないものです。これまで SQL Server Management Studio を使用したことがなく、必要かどうかわからない場合は、インストールしておくことをお勧めします。これにより、たとえば、RAS Reporting データベースのテーブル、制約、ストアドプロシージャを表示することができます。また RAS Reporting データベース設計の理解を

深めることができます。インストール用のリンクは、SQL Server インストールセンターウィンドウに表示されます。

Microsoft SQL Server 2016 以前のバージョンを構成

Microsoft SQL Server 2016 以前のバージョンを使用する場合、次の手順を実行してリモート接続向けの構成を実行する必要があります。

1 Microsoft SQL Server Management Studio を開きます。

2 サーバーを右クリックし、[プロパティ] を選択します。

3 [接続] に移動し、[リモートを許可する] を選択します。

4 SQL Server 構成マネージャーを開き、RAS Reporting の[SQL Server ネットワーク構成] > [プロトコル] へ進みます。

5 [TCP/IP] を右クリックし、[プロパティ] を選択します。

6 [有効] プロパティが [はい] に設定されていることを確認します。

7 [IP アドレス] タブを選択して、[IPALL] セクションに移動します。[TCP 動的ポート] フィールドを空にして、[TCP ポート] フィールドを”1433”に設定します。

8 SQL Server を再起動します。これを実行するには、SQL Server の構成マネージャーで SQL Server サービスを右クリックして、[再起動] を選択します。

9 再起動後、SQL Server の構成マネージャーで [SQL Server ブラウザー] を右クリックして、[プロパティ] を選択します。

10 [サービス] タブを選択して、[起動モード] プロパティを [自動] に設定します。

11 SQL Server ブラウザーを起動します。

Microsoft SQL Server Reporting Services の構成

Microsoft SQL Server Reporting Services を設定するには、次の手順を実行します。

1 Reporting Services 構成マネージャーを実行します（[スタート] > [アプリ] > [Microsoft SQL Server 2016] > [Reporting Services 構成マネージャー]）。

2 [Reporting Services 構成接続] ダイアログが開いたら、次の手順を実行します。

- [サーバー名] フィールドに、SQL Server インスタンスをホストしているサーバーの名前が入力されていることを確認します。

- [レポートサーバーインスタンス] フィールドに、先に作成した SQL Server インスタンス名が入力されていることを確認します。デフォルトの Parallels RAS 名を使用した場合は、このフィールドに”RASREPORTING”と表示されます。別のインスタンス名を使用した場合は、その名前を選択してください。

3 [接続] をクリックします。接続に成功すると、[Reporting Services 構成マネージャー] ウィンドウが開きます。

4 左側ペインでウェブサービス URL カテゴリー（ウェブポータル URL とは異なります）を選択し、右側ペインで以下のプロパティを設定します。

- 仮想ディレクトリ: ディレクトリ名が”ReportServer_RASREPORTING”になっていることを確認します。SQL Server インスタンスに別の名前を使用している場合は、”RASREPORTING”の部分に、その名前が表示されるはずです。
- TCP ポート: ポート番号を 8085 に設定します。

5 [適用] ボタンをクリックして、設定を適用します。

6 左側ペインでウェブポータル URL カテゴリーを選択し、次の手順を実行します。

- [仮想ディレクトリ] フィールドが”Reports_<InstanceName>”に設定されていることを確認します。”InstanceName”は SQL Server インスタンスの名前です。デフォルトの Parallels RAS 名は”Reports_RASREPORTING”となります。
- [URL] フィールドを調べます。サーバー名の後のポート番号が 8085 になっていることを確認してください。そうでない場合は、[詳細] ボタンをクリックして、ポート番号を変更してください。

7 [ウェブポータル URL] ページで URL をクリックして、Reporting Services ウェブポータルにアクセスできることを確認します。これにより、ウェブブラウザーで SQL Server Reporting Services のホームページが表示されます。

8 [終了] をクリックして Reporting Services 構成マネージャーを終了します。

Microsoft SQL Server 2017 または 2019 をインストール

Microsoft SQL Server 2017 および 2019 以降を利用することにより、データベースエンジンや SQL Server Reporting Services (SSRS) を個別のホストにインストールできます。Parallels RAS 17.1（およびそれ以降）では、この展開シナリオがサポートされています。つまり、別々のホストにインストールされた SQL Server Reporting Services と、SQL Server データベースエンジンを使用する機能が提供されています。

Parallels RAS Reporting Services と SQL Server 2019 および Microsoft SSRS 2019 をインストールして構成する方法の詳細な手順については、次の Parallels ナレッジベースの記事をお読みください。

- Microsoft SQL Server 2017 および 2019 単一のサーバーのインストール: https://kb.parallels.com/125164。
- Microsoft SQL Server 2017 および 2019 複数のサーバーのインストール: https://kb.parallels.com/125156。

Parallels RAS Reporting のインストール

Parallels RAS Reporting をインストールするには:

1 Microsoft SQL Server Reporting Services がインストールされているサーバーにログインします。使用しているアカウントに管理者特権（AD）が付与されていることを確認してください。

> **注:** 前述したように SQL Server 2017 以降を利用することにより、SQL Server データベースエンジンや SQL Server Reporting Services（SSRS）を異なるホストにインストールできます。SSRS をインストールしたサーバーにログインする必要があります。

2 Parallels RAS Reporting の最新バージョンを https://www.parallels.com/products/ras/download/links/ からダウンロードします。

3 ダウンロードしたら、`RASReporting-xxx.msi` ファイルをダブルクリックして、インストールウィザードを実行します。

4 画面の指示に従って、「データベース接続」のページに進みます。SQL Server データベースエンジンのロケーションを指定する:

- ロケーション: SQL Server データベースエンジンと SSRS をローカルサーバーにインストールしている場合、[ローカルホスト] を選択します。SQL Server が異なるサーバーにインストールされている場合、[リモート] を選択して、サーバー接続のプロパティを指定します（以下を参照）。
- サーバー: [リモート] を選択する場合、SQL Server がインストールされたサーバーの FQDN または IP アドレスを指定します。
- ユーザー名: SQL Server にログインするためのユーザー名を指定します。
- パスワード: パスワードを指定します。

5 同じページで SQL Server のインスタンス名を指定します。デフォルトのインスタンス名は RASREPORTING です。別のインスタンスを使用したくない場合は、このページでインスタンスを指定できます。インスタンスが存在しない場合は、最初に作成する必要があります。

6 [次へ] をクリックします。

7 [レポートユーザーの表示] ページでは、RAS レポートデータベースへのアクセス権限を付与する Active Directory ユーザーを指定する必要があります。デフォルトのユーザーは”rasreportingview”です（なお、ここで使用する前に、Active Directory でユーザーを作成する必要があります）。必要に応じて別の Active Directory ユーザーを指定することもできますが、レポートを表示する前に RAS Console のレポート設定を変更する必要があります（この変更については、本章の後半で RAS のレポート設定について扱う際に説明します）。

8 [次へ] をクリックして Parallels RAS Reporting をインストールします。

RAS Console での RAS Reporting の構成

Parallels RAS Reporting を構成するには:

1 Parallels RAS Console にログインします。

2 [管理] カテゴリーを選択し、右ペインの [報告] タブをクリックします。

3 [報告] タブで、[RAS Reporting を有効化] オプションを選択します。

4 [サーバー] フィールドでは、SQL Server インスタンスをホストするサーバーの FQDN または IP アドレスを指定します。[ポート] フィールドの値は、RAS Connection Broker からのデータ受信サービスに使用されます。デフォルトのポートは 30008 です。

5 以下のいずれかのユーザーログインオプションを指定します:

- ユーザーにログイン情報の入力を促す - このオプションを選択すると、Parallels RAS Console のユーザーは、レポートを実行する前に認証情報を入力するよう求められます。
- 次の資格情報を使用 - このオプションが選択された場合、指定されたユーザー名とパスワードが使用されます。デフォルト（ビルトイン）のユーザー名は RASREPORTINGVIEW です。RAS Reporting をインストールしたときに別のユーザーを指定した場合は、ユーザーの認証情報をここで指定します。

6 データベース接続をテストするには、[接続をテスト] ボタンをクリックします。

詳細設定を構成する

これらの設定は任意です。必要に応じて設定してください。

詳細設定にアクセスするには:

1 [管理] > [報告] タブページで、[追跡設定] ボタンをクリックします。[詳細設定] ダイアログが開きます。

2 [セッション情報] セクションで、次のオプションを指定します。

- 追跡を有効化: セッションデータを記録します（サーバーレポート以外のすべてのレポートに影響します）。
- 情報を次の期間保持: どのくらいの期間、情報をデータベースに保存するかを選択します。

3 [サーバーカウンター情報] セクションで、以下を指定します。

- 追跡を有効化: 選択すると、サーバーカウンターのデータを記録します（サーバーレポートのみに影響します）。
- 情報を次の期間保持: どのくらいの期間、情報をデータベースに保存するかを選択します。
- 変更が次の数字よりも多い場合に CPU/メモリカウンターを追跡（%）: この 2 つのオプションを使って、データの記録に必要な CPU とメモリーの最小使用量を設定します。

4 [カスタムレポート] セクションを使用して、Parallels RAS Console のカスタムレポートを有効化できます。[カスタムレポートを有効化] オプションを選択して、カスタムレポートが保存されるフォルダー名を指定します（またはデフォルト名の”カスタムレポート”を使用します）。これは SQL Server Reporting Services 側に配置された仮想フォルダーであることに注意してください。このため従来のようにパスではなく、名前を指定する必要があります。レポートが含まれる他の定義済みフォルダーとともに、[レポート] カテゴリ内の Parallels RAS Console のフォルダーが表示されます。

Parallels RAS レポートの実行

Parallels RAS のレポートを表示するには、RAS Console で [報告] カテゴリーを選択します。レポート情報は以下のように表示されます:

- 中央ペインには、利用できるレポートのリストが表示されます。完全なリストについては、下の「定義済みのレポート」サブセクションを参照してください。青い”フォルダー”アイコン（リストの最上部）では、タイプ別にレポートをグループ化したり、フラットなリストとしてすべてのレポートを表示したりできます。”更新”アイコンでは、レポートリストをデータベースから取得して、レポートリストを更新します（この機能は、レポート機能を有効または無効にするときやカスタムレポート（リストに自動表示されません）を追加するときに便利です）。
- 初めて [報告] カテゴリーを開くときに、右ペインには [情報] タブページのみが表示されます。ここに、Parallels RAS Reporting がアクティブかどうかが表示されます。そうでない場合は、インストールされていて有効になっているかどうかを確認する必要があります。
- [タスク] ドロップダウンリスト（RAS Console の右上）の先頭にある青い”正方形”アイコンを使用すると、レポートインターフェイスがフルスクリーンで表示されます。[タスク] ドロップダウンリストでは、次のアクションを実行できます: [複製]（レポートタブを複製する）、[フルスクリーン]（オン/オフ）、さまざまな [レポートを閉じる] オプション、[委任の許可]（レポートを表示する権限を、これらの権限を持っていない上級管理者やカスタム管理者など、他の RAS 管理者に付与することができます）。

レポートを実行するには、中央ペインをダブルクリックします。右ペインのタブページ内にレポートが開きます。

- ほとんどの事前定義レポートにコントロールが含まれており、これを使用すると、[開始日] / [終了日]、[並べ替え]、[並べ替える]、[チャートタイプ]、[サーバー名] などを操作できます。その他はレポートタイプによります。このコントロールのいずれかの値を変更するときは、[レポートを表示] ボタンをクリックして新しい値/オプションを適用し、レポートを再実行します。
- メインのレポート領域（データがグラフ、テキスト、数字で表示されている下の部分）には、メニューバーとアイコンが含まれます。これらを使用して、倍率の変更、レポートページの一覧表示（複数含まれる場合）、テキストの検索、レポートのファイルへの保存、レポートの印刷、レポートの利用可能な任意の形式（Word、Excel、PowerPoint、PDF）またはデータフィードへのエクスポートを実行することができます。

注: レポートを最初に表示するときに、信頼できるウェブサイトとして https://<サーバーのドメイン / IP> を追加するように要求される場合があります。これは、Parallels RAS マシンの Internet Explorer セキュリティ強化の構成に基づいて表示されます。

定義済みのレポート

Parallels RAS Reporting には、定義済みのレポートが多数あり、次のグループに分けられます。

1. ユーザーレポート: このグループには、エンドユーザーが Parallels RAS をどのように使用しているかについてのレポートが含まれます。
   - すべてのユーザーのセッションアクティビティ - システム内のすべてのユーザーが生成したすべてのセッションが示されます。このレポートには各セッションについての情報が表示され、アクティブ時間、アイドル時間、非接続時間、合計時間などが含まれます。ユーザーは、ユーザー名と IP アドレスで識別されます。Secure Gateway の情報も記載されています。
   - ユーザーのセッションアクティビティ - 1 人のユーザーが生成したすべてのセッションが示されます。このレポートには各セッションについての情報が表示され、アクティブ時間、アイドル時間、非接続時間、合計時間などが含まれます。
   - ユーザーのアプリケーション使用状況 - 使用回数や合計時間を含む、指定したユーザーが使用したアプリケーションが表示されます。
   - ユーザーのデバイス使用状況 - ユーザーが使用しているデバイスの情報が表示されます。このレポートには、デバイスベンダー、デバイスモデル、合計使用時間などの情報が含まれます。
   - ユーザーのオペレーティングシステム使用状況 - 指定したユーザーが使用しているオペレーティングシステムが表示されます。
   - 完全なユーザー情報 - 指定したユーザーについての詳細な情報が表示されます。
2. ユーザーグループレポート: これらのレポートには、ユーザーグループが Parallels RAS をどのように使用しているかに関する情報が表示されます。
   - すべてのグループのセッションアクティビティ - システム内のすべてのグループが生成したすべてのセッションが表示されます。このレポートには、アクティブ時間、アイドル時間、非接続時間が含まれます。
   - グループのセッションアクティビティ - システム内のグループが生成したすべてのセッションが表示されます。このレポートには、グループ内の各ユーザーが生成した各セッションの情報が表示され、開始時間、終了時間、アクティブ時間、アイドル時間、非接続時間、合計時間が含まれます。
   - グループのアプリケーション使用状況 - 使用回数や合計時間を含む、指定したグループが使用したアプリケーションが表示されます。

- グループのデバイス使用状況 - 指定したグループのメンバーとしてユーザーが使用したデバイスの情報が表示されます。このレポートには、デバイスベンダー、モデル、合計使用時間が含まれます。
- グループのクライアントオペレーティングシステム使用状況 - 特定のグループのメンバーが使用したクライアントオペレーティングシステムが表示されます。

3 デバイスレポート: このグループには、Parallels RAS に接続しているデバイスに関するレポートが含まれます。

- 使用したデバイス - システムを使用しているすべてのデバイスが表示されます。このレポートには、デバイスの製造元、モデル、デバイスで開かれたセッション数が含まれます。
- 使用したクライアントオペレーティングシステム - システムを使用しているデバイスと、対応するオペレーティングシステムが表示されます。
- 使用した Parallels Client バージョン - デバイスモデルについての情報、使用した Parallels Client バージョン、セッション情報が表示されます。

4 サーバーアクティビティレポート: このグループには、Parallels RAS サーバーコンポーネントのアクティビティに関するレポートが含まれます。

- RD セッションホストのセッションアクティビティ - 特定の RD セッションホストにおけるユーザーのセッションアクティビティが表示されます。レポートには、開始時間、終了時間、アクティブ時間、アイドル時間、非接続時間が含まれます。
- VDI プロバイダーのセッションアクティビティ - 特定のプロバイダーにおけるユーザーのセッションアクティビティが表示されます。レポートには、開始時間、終了時間、アクティブ時間、アイドル時間、非接続時間が含まれます（スタンドアロンの Hyper-V および VMware ESXi のみ）。
- AVD プロバイダーのセッションアクティビティ - 特定の AVD プロバイダーにおけるユーザーのセッションアクティビティが表示されます。レポートには、開始時間、終了時間、アクティブ時間、アイドル時間、非接続時間が含まれます。
- RD セッションホストのセッションアクティビティ - 特定の RD セッションホストにおけるユーザーのセッションアクティビティが表示されます。レポートには、開始時間、終了時間、アクティブ時間、アイドル時間、非接続時間が含まれます。
- VDI ホストプールのセッションアクティビティ - 特定の VDI ホストプールにおけるユーザーのセッションアクティビティが表示されます。レポートには、開始時間、終了時間、アクティブ時間、アイドル時間、非接続時間が含まれます。

- AVD ホストプールのセッションアクティビティ - 特定の AVD ホストプールにおけるユーザーのセッションアクティビティが表示されます。レポートには、開始時間、終了時間、アクティブ時間、アイドル時間、非接続時間が含まれます。
- ゲートウェイでトンネリングされたセッション - 指定したゲートウェイでトンネリングされたセッションの情報を表示します。

5 サーバー健全性レポート: このグループには、Parallels RAS の各コンポーネントのサーバー CPU および RAM 使用量に関するレポートが含まれます。

- RD セッションホストの正常性 - ファーム内の指定したサーバーの CPU および RAM の使用率が表示されます。
- プロバイダーの正常性（サーバー別） - ファーム内の指定したプロバイダーの CPU および RAM の使用率が表示されます。
- リモート PC の正常性 - ファーム内の指定したリモート PC の CPU および RAM の使用率が表示されます。
- ゲートウェイの正常性 - ファーム内の指定したゲートウェイの CPU および RAM の使用率が表示されます。
- Connection Broker の正常性 - ファーム内の指定した Connection Broker の CPU および RAM の使用率が表示されます。
- 登録サーバーの正常性 - ファーム内の指定した登録サーバーの CPU および RAM の使用率が表示されます。

6 アプリケーションレポート: アプリケーションに関連するレポートです。

- すべてのアプリケーションのアクティビティ - システム内で使用されたアプリケーションに関する情報が提供されます。レポートにはアプリケーション名、使用回数、合計使用時間などの情報が含まれます。レポートを表示するときは、必要に応じて、[すべてのアプリケーション] または [RAS 公開済みのアプリケーション] を選択してください。後者のオプションを選択している場合、レポートには公開されていないアプリケーションや複製は含まれません。
- アプリケーションのアクティビティ - 指定された期間中における個別ユーザーによるアプリケーションの使用状況を示します。各セッションの開始時間、終了時間、合計時間が表示されます。他にも、ホストサーバー名やセッション ID などの情報も表示されます。

7 ログオン期間のレポート: ユーザーのログオン時間に関する詳細情報を示すレポートです。また、接続時間、認証時間、RAS ポリシー検索時間、ホスト準備時間、グループポリシーロード時間、デスクトップロード時間に関する情報も表示されます。

- すべてのユーザーのログオン時間 - 各サーバーにおけるすべてのユーザーの最小、最大、平均ログオン時間を示します。
- ユーザーのログオン時間 - 各サーバーにおける特定のユーザーの最小、最大、平均ログオン時間を示します。
- RD セッションホストのログオン時間 - 指定した RD セッションホストにおける、各ユーザーの最小、最大、平均ログオン時間を示します。
- VDI プロバイダーのログオン時間 - 特定のプロバイダーにおける各ユーザーの最小、最大、平均ログオン時間を示します。
- AVD プロバイダーのログオン時間 - 各ユーザーの特定の AVD プロバイダーでの最小、最大、平均ログオン時間を示します。またレポートには、接続時間、認証時間、RAS ポリシー検索時間、ホスト準備時間、グループポリシーロード時間、デスクトップロード時間に関する情報も示されます。

8 UX エバリュエーターのレポート: UX エバリュエーターに関するレポートで、クライアント側の最初の手順（ユーザーのアクション）から最後の手順（レスポンスの画像表示）までの時間間隔を測定したものです。

- すべてのユーザーの UX エバリュエーター - 各サーバーのすべてのユーザーに対応する UX エバリュエーターを表示します。
- ユーザーの UX エバリュエーター - 各サーバーの特定のユーザーに対応する UX エバリュエーターを表示します。
- RD セッションホストの UX エバリュエーター - 各ユーザーの指定された RD セッションホストに対応する UX エバリュエーターを表示します。
- VDI プロバイダーの UX エバリュエーター - 各ユーザーの特定のプロバイダーに対応する UX エバリュエーターを表示します。
- AVD プロバイダーの UX エバリュエーター - 各ユーザーの特定の AVD プロバイダーに対応する UX エバリュエーターを表示します。

9 転送プロトコルのレポート: セッション中における各転送プロトコルの使用時間を表示します。

- すべてのユーザーの転送プロトコル - すべてのユーザーの転送プロトコル使用に関する情報を表示します。
- ユーザーの転送プロトコル - 特定のユーザーの転送プロトコル使用に関する情報を表示します。

- RD セッションホストの転送プロトコル - 特定の RD セッションホストの転送プロトコル使用に関する情報を表示します。
- VDI プロバイダーの転送プロトコル - 特定の VDI プロバイダーの転送プロトコル使用に関する情報を表示します。
- AVD プロバイダーの転送プロトコル - 特定の AVD プロバイダーの転送プロトコル使用に関する情報を表示します。

10 接続品質レポート: 接続品質に関する情報を示すレポートです。

- すべてのユーザーの接続品質 - すべてのユーザーの接続品質に関する情報を表示します。
- ユーザーの接続品質 - 特定のユーザーの接続品質に関する情報を表示します。
- RD セッションホストの接続品質 - 特定の RD セッションホストの接続品質に関する情報を表示します。
- VDI プロバイダーの接続品質 - 特定の VDI プロバイダーの接続品質に関する情報を表示します。
- AVD プロバイダーの接続品質 - 特定の AVD プロバイダーの接続品質に関する情報を表示します。

11 レイテンシーに関するレポート: レイテンシーに関する情報を示すレポートです。

- すべてのユーザーのレイテンシー - すべてのユーザーのセッションレイテンシーに関する情報を表示します。
- ユーザーのレイテンシー - 特定のユーザーのセッションレイテンシーに関する情報を表示します。
- RD セッションホストのレイテンシー - 特定の RD セッションホストのセッションレイテンシーに関する表示します。
- VDI プロバイダーのレイテンシー - 特定の VDI プロバイダーのセッションレイテンシーに関する情報を表示します。
- AVD プロバイダーのレイテンシー - 特定の AVD プロバイダーのセッションレイテンシーに関する情報を表示します。

12 帯域幅の可用性レポート: 帯域幅の可用性に関する情報を示すレポートです。

- すべてのユーザーの帯域幅可用性 - すべてのユーザーの帯域幅可用性に関する情報を表示します。
- ユーザーの帯域幅可用性 - 特定のユーザーの帯域幅可用性に関する情報を表示します。

- RD セッションホストの帯域幅可用性 - 特定の RD セッションホストの帯域幅可用性に関する情報を表示します。
- VDI プロバイダーの帯域幅可用性 - 特定の VDI プロバイダーの帯域幅可用性に関する情報を表示します。
- AVD プロバイダーの帯域幅可用性 - 特定の AVD プロバイダーの帯域幅可用性に関する情報を表示します。

13 セッション中断レポート: 最も多い切断理由と再接続回数を示すレポートです。

- すべてのユーザーのセッション切断 - 全ユーザーの上位の切断理由と再接続回数を表示します。
- ユーザーのセッション切断 - 指定されたユーザーの上位の切断理由と再接続回数を表示します。
- RD セッションホストのセッション切断 - 指定された RD セッションホストの上位の切断理由と再接続回数を表示します。
- VDI プロバイダーのセッション切断 - 指定された VDI プロバイダーの上位の切断理由と再接続回数を表示します。
- AVD プロバイダーのセッション切断 - 指定された AVD プロバイダーの上位の切断理由と再接続回数を表示します。

GDPR 準拠

Parallels RAS のレポートデータベースには、ユーザーについての情報が保存されています。これにはユーザーの個人情報が含まれる可能性があります。GDPR を遵守するために、Parallels RAS では、データベースからいつでもユーザーデータをクリアできる機能を提供しています。Parallels RAS Reporting Tools は、このタスクを実行するときに使用できるシンプルなアプリケーションです。このツールは、Parallels RAS をインストールすると自動的にインストールされます。

ユーザーデータをクリアするには次の手順を実行します。

1 Parallels RAS をインストールしたコンピューターで、`C:\Program Files (x86)\Parallels\RAS Reporting` に移動します。

2 上述のフォルダーで、RASReportingTools アプリケーションを探して実行します。

3 アプリケーションが起動したら、[ユーザーデータ] フィールドにユーザー名を入力して、[ユーザーを探す] をクリックします。ユーザーが見つかった場合は、ユーザー情報が表示さ

れます。ユーザーが見つからない場合は、RAS レポートデータベースにはそのユーザーについての情報が保存されていないということを意味します。

4 RAS レポートデータベースに保存されているユーザー情報を参照するには、[完全なユーザー情報を表示] ボタンをクリックします。これによって、ウェブブラウザーに [完全なユーザー情報] レポートが開きます（このレポートは、RAS Console の [報告] カテゴリでも利用できます）。レポートを調べて、任意のユーザー情報が GDPR の要件に従っていることを確認します。

5 ユーザーデータをクリアするには、Parallels RAS Reporting Tool アプリに戻り、[ユーザーデータのクリア] ボタンをクリックします。メッセージが表示されたら、データのクリアを確定します。

第　24　章

Performance Monitor

この章の内容

概要

Parallels RAS Performance Monitor はブラウザーベースのダッシュボードで、管理者が Parallels RAS の展開のボトルネックやリソース使用率の分析に使用できるようになっています。このダッシュボードではパフォーマンスメトリクスを視覚的に表示でき、Parallels RAS Console またはウェブブラウザーに表示することができます。

コンポーネント

Parallels RAS Performance Monitor は次のコンポーネントで構成されています。

- InfluxDB データベース - システムパフォーマンスデータのストレージ用データベース。
- Grafana ダッシュボード - パフォーマンスメトリクスを視覚的に表示するブラウザーベースのダッシュボード。
- Telegraf サービス - インストールされているサーバー上でパフォーマンスデータを収集するサービス。同サービスは Parallels RAS ファームにサーバーを追加し、対応する RAS Agent（RAS Secure Gateway Agent、RD セッションホスト Agent、Remote PC Agent など）をインストールすると自動的にインストールされます。

仕組み

Telegraf サービスはデフォルトで停止されており、データを収集しないようになっています。ファームの各サーバーで同サービスを起動するには、パフォーマンスモニタリング機能を構成

し、Parallels RAS Console で有効にする必要があります。有効にすると、Telegraf サービスが定義済みのパフォーマンスカウンターを一定間隔（10 秒）で収集し始めます。その後、ストレージ用の InfluxDB データベースに収集したデータを送信します。パフォーマンスメトリクスを表示するには、ダッシュボード（Grafana）を使って、リアルタイムのパフォーマンスカウンターを視覚的に表示します。

パフォーマンスメトリクスはタイプ（セッション、CPU、メモリ、ディスクなど）ごとにダッシュボードでグループ化されており、メトリクスの各グループを個別に表示することができます。ファームあるいはサイトの 1 つ以上の特定サーバーのパフォーマンスメトリクスを表示するか、またはすべてのサーバーのパフォーマンスメトリクスを表示するかを選択することもできます。さらに、データを表示する特定のサイトを選択することもできます。

RAS Performance Monitor をインストールする

要件

Parallels RAS Performance Monitor は、Parallels RAS の独立したコンポーネントであり、専用のインストーラーを備えています。このツールは、専用サーバーまたは Parallels RAS コンポーネントのいずれかのホストサーバーにインストールすることができます。インストーラーを実行すると、InfluxDB データベースと Grafana ダッシュボードサービスが自動的にインストールされます。詳細については、以下の「インストール」のサブセクションを参照してください。

Parallels RAS Performance Monitor をインストールしたサーバーには、以下のファイアウォールルール（開放ポート）が自動的に追加されます。

- TCP ポート 8086（InfluxDB データベースで使用）。
- TCP ポート 3000（Grafana パフォーマンスダッシュボードで使用）。

インストール

Parallels RAS Performance Monitor をインストールするには:

1. https://www.parallels.com/products/ras/download/links/ より Parallels RAS Performance Monitor のインストーラーをダウンロードします。
2. インストールウィザード（RASPerformanceMonitor.msi ファイル）を実行し、画面の指示に従って作業を進めます。

3 完了したら、ウィザードを閉じます。

Parallels RAS Performance Monitor の使用

Parallels RAS Performance Monitor へのアクセスを構成する

データ収集を有効にし、ダッシュボードを表示するには:

1 RAS Console で [管理] > [報告] に移動します。

2 [RAS Performance Monitor を有効にする] オプション（[RAS Performance Monitor の構成] セクション）を選択します。

3 InfluxDB データベースおよび Grafana ダッシュボードがインストールされているサーバーの FQDN または IP アドレスを入力します。

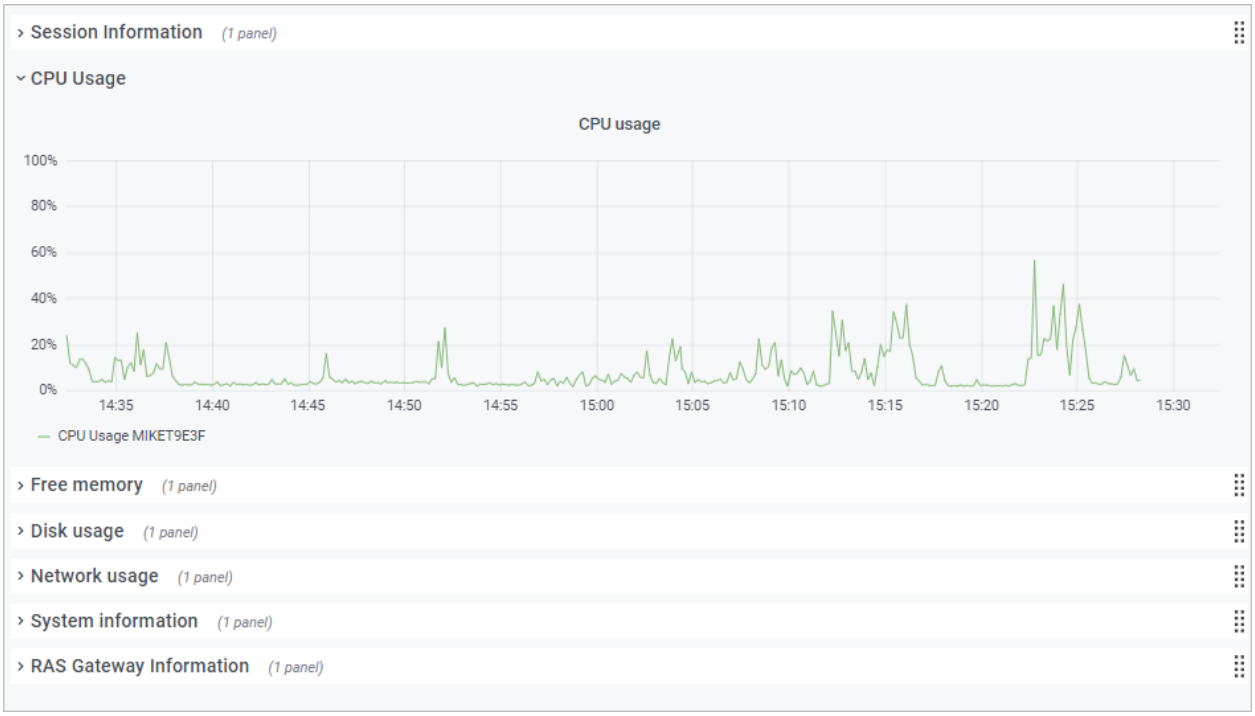
4 [適用] をクリックして変更を確定します。

上記の手順を実行したら、サイトの各サーバーで Telegraf サービスが起動し、データ収集を開始します。

パフォーマンスメトリクスの表示

注: Parallels RAS Performance Monitor ではパフォーマンスデータを表示する前に収集に少々時間がかかります（初回インストールでは約 1 時間）。

パフォーマンスメトリクスを表示するには、RAS Console で [管理者] カテゴリーを選択します。データが右ペインに表示されます。ログオンは自動的に実行されるため、ログオン情報は必要ありません。



[モニタリング] タブ（ダッシュボード下部）のボタンは以下の通りです。

- ホーム: ホームページを表示します。このボタンはダッシュボードで外部リンクをクリックして外部ウェブページに移動する場合に便利です。
- 更新: 現在のページをリロードします。
- ブラウザーで開く：パフォーマンスダッシュボードをウェブブラウザで開きます。

特定のタイプのメトリクスを表示するには、ダッシュボードの主要部にカテゴリーを展開します。カテゴリーには以下のものが含まれます。

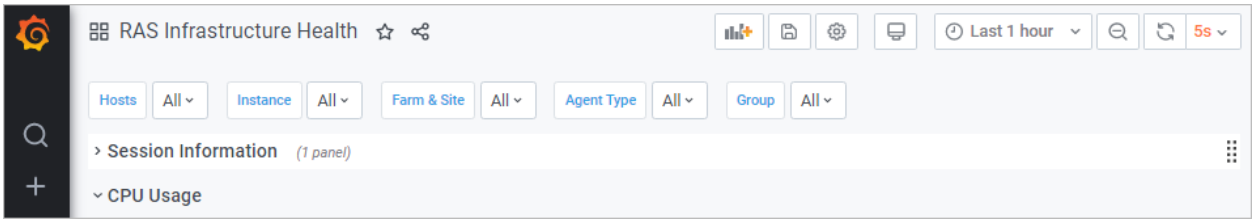
- セッション情報: アクティブなセッションおよび接続していないセッションに関する情報を表示します。
- CPU 使用率: CPU カウンター。
- メモリ容量: 物理メモリのカウンター。
- ディスク使用率: ディスク入出力のカウンター。

- ネットワーク使用率: ネットワークインターフェースの出入力カウンター。
- システム情報: システム情報カウンター。
- RAS ゲートウェイ情報: RAS Gateway カウンター:

パフォーマンスメトリクスはダッシュボードにグラフ表示されます。異なるカウンターは別の色で表示されます。

グラフの特定部分にズームインするには、マウスで長方形のブロックを選択します。また、ダッシュボード上部にある [ズーム] コントロールを使って、時間範囲をズームアウトしたり、推移時間を進めたり戻したりできます。特定の時間範囲を選択するには、上部の”時計”アイコンをクリックして、時間範囲を指定します。

デフォルトでは、ダッシュボードはキオスクモードで開きます。終了するには、”ESC”キーを押します。表示モードを切り替えるには、右上の”モニター”アイコンをクリックします。キオスクモードの場合、「RAS インフラストラクチャ正常性」ページが表示されます。



上部のメニューには次の項目があります。

- ホスト: パフォーマンスメトリクスを表示するサーバーを 1 つまたは複数選択できます。サイトのすべてのサーバーデータを表示するには、[すべて] を選択します。リストにサーバーが何も表示されない場合は、Parallels RAS Performance Monitor が初回の統計データを収集するまで待つ必要があります。これは、初回のインストール時のみ起こります。
- インスタンス: 特定のカウンターのインスタンス（1 つ以上ある場合）を選択できます。ネットワークカウンターの場合、通常ネットワークインターフェース名が使われます。ディスクカウンターの場合、ディスク名になります。その他のカウンターでは通常インスタンスが複数あることはありません。
- ファームとサイト: データを表示するサイトを選択します。[すべて] を選択すると、ファームのすべてのサイトのデータを表示します。別の RAS ファームがある場合、RAS Performance Monitor が構成されていて有効なときは、そのファームからサイトを選択することもできます。
- Agent タイプ: RAS Agent タイプを選択します。

- グループ: RDS グループを選択します。

パフォーマンスメトリクスおよびその意味について詳しくは、次の Microsoft の記事を参照してください。

- https://technet.microsoft.com/en-us/library/cc976785.aspx
- https://technet.microsoft.com/en-us/library/2008.08.pulse.aspx

「RAS Performance Counters」（p. 647）も参照してください。

RAS Performance Monitor のセキュリティの構成

デフォルトでは、どのユーザーでも [Performance Monitor] ページにアクセスして、パフォーマンスメトリクスを表示できます。セキュリティの向上のため、許可されたユーザーのみが表示できるように、RAS Performance Monitor が資格情報を使用するように設定できます。

最初に、以下のように Grafana 構成ファイルから匿名認証を削除します。

1 ファイル C:\Program Files\Parallels\RAS Performance Monitor\conf\defaults.ini を開きます。

2 ファイルで次を探します。

```
################################### Anonymous Auth
######################
[auth.anonymous]
# enable anonymous access
enabled = true
```

3 "enabled = true" を "enabled = false" に変更します。

> **注:** 匿名アクセスを無効にすると、ユーザーは自動的に管理者パスワードを変更するよう促されます。これに引き続き、Grafana の公式ドキュメントに従って、パスワードを変更できます: https://grafana.com/docs/grafana/latest/manage-users/user-admin/change-your-password/。

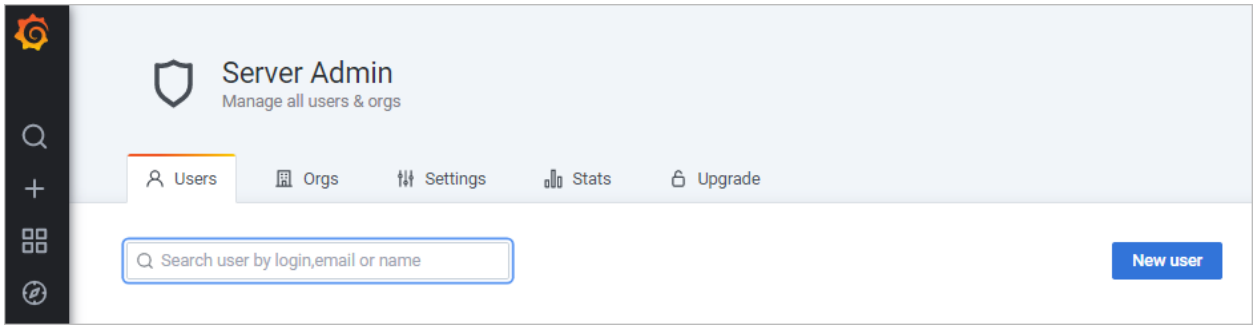
4 Grafana サービスを再起動します。

5 [モニタリング] カテゴリーを選択し、以下の認証情報を使用して Grafana にログインします。

- ユーザー: admin
- パスワード : admin（以前にパスワードを変更した場合は、現在のパスワードを使用してください）。

6 ログイン後、”Esc”キーを押し、”盾”のアイコン > [ユーザー] をクリックします。

7 [新規ユーザー] をクリックして、新しいユーザーを作成します。



8 ここで、ユーザーを組織のリストに追加する必要があります。そのためには、[ユーザー] リストで、[編集] をクリックしてユーザーを編集し、組織を設定して、ユーザーを [ビューアー] にします。

9 [追加] をクリックして、ユーザーを組織のリストに追加します。これで、ユーザーは RAS Performance Monitor 統計データを表示できます。

RAS Performance Monitor をアップデートする

新しいバージョンの Grafana には、OS にインストールされているブラウザーとの互換性がない場合があります。最新の Edge ブラウザーに対応しており、RAS Console に自動的に埋め込まれます。これを使用しない場合は、プラグインの形で提供されている再配布可能なブラウザーを使用することをお勧めします。プラグインは、他の Parallels RAS ディストリビューションと同様に、個別の msi パッケージとして配布されます。

潜在的な問題を回避するために、Parallels RAS は、インストールされている Grafana とブラウザーのバージョンを監視し、必要に応じて RAS 管理者に対して通知を行います。そのような状況で、[モニタリング] カテゴリーを選択すると、通常はダッシュボードが表示されません。代わりに、更新されたブラウザープラグインをインストールする必要があるというメッセージが表示されます。プラグインをインストールするには、以下の手順を実行します。

1. メインメニュー（上部）で、[ツール] をクリックして、[プラグイン] を選択します。
2. [プラグイン] ダイアログで、[ブラウザーエンジン] プラグインに進みます。[状態] 列には、インストールされていないことを示す表示があるはずです。
3. プラグインを選択し、次のボタンのいずれかをクリックします。
   - オンラインでインストールする - インターネットからプラグインをダウンロードしてインストールします。ご利用の環境でインターネットにアクセスできる場合、このボタンをクリックします。
   - オフラインでインストールする - オフライン環境の場合、管理者はプラグインのリストを取得できません。代わりにローカルファイルサーバーからプラグインの Zip ファイルをアップロードします。プラグインテーブルでは、インストールされているプラグインのみが一覧表示されます。
4. プラグインをインストールしたら、[モニタリング] カテゴリーに戻ることができます。今回は、Grafana ダッシュボードが表示されます。

プラグインを更新または削除するには（必要な場合）、上記と同じ手順を使用しますが、”インストール済み”とマークされているプラグインを選択して、[オンラインで更新]（またはオフライン）または [アンインストール] をクリックします。Parallels RAS 18 から将来のバージョンにアップグレードした後も、カスタムダッシュボードが維持されることに注意してください。

第　25　章

一般的な管理タスク

この章では、ファームのステータスのモニタリング、ライセンス管理、バックアップ管理などの、Parallels RAS の一般的な管理タスクについて説明します。

この章の内容

リカバリ - 管理者の追加

このトピックでは、root 管理者を利用できないときやドメインが変更されたときに発生する可能性のある問題を扱います。このようなときは、システムにアクセスできなくなります。この問題を発見した場合は、プライマリ RAS Connection Broker をホストしているサーバーで次のコマンドを実行することで、root 管理者を迅速に追加できます。

`2XRedundancy -c -AddRootAccount` *user* `[`*domain*`]`

緊急のリカバリであるため、開いている Parallels RAS Console には、新しいアカウントについての通知が行われません。[管理] 領域で新しいアカウントを参照するには、ログアウトしてからログインし直す必要があります。

ホスト名解決

サーバーコンポーネント（Connection Broker、ゲートウェイ、RD セッションホスト、プロバイダーなど）を RAS ファームに追加する場合、コンポーネントの FQDN または IP アドレスを指定する必要があります。通常はユーザーが任意で FQDN また IP アドレスのいずれを使用するかを選択できます。ただし、サーバーの IP アドレスは将来変更される可能性があります。この場合、RAS ファームの対応するコンポーネントを再構成する必要が生じます。一方、通常はサーバーの FQDN が変わることはありません。このため IP アドレスではなく FQDN を使用すれば、RAS の構成を変更する必要はなくなります。これによりユーザーは、ファームのすべてのサーバーコンポーネントで、Parallels RAS により IP アドレスから FQDN を解決するためのオプションをいつでも利用することができます。

名前解決を常時使用可能にするためには、次の手順を実行します。

1. RAS Console で、メインメニュー（RAS Console ウィンドウ上部のメニュー）から [ツール] > [オプション] をクリックします。
2. [オプション] ダイアログで、[ホストを追加する場合は、常に完全修飾ドメイン名（FQDN）で解決する] オプションを選択します。
3. [OK] をクリックします。

ファームにコンポーネントを追加して、名前ではなく IP アドレスを入力すると、自動的に FQDN に解決されます。FQDN を確定できない場合、エラーメッセージが表示され、替わりに IP アドレスを使用するかを尋ねられます。

次の事例では、異なるコンポーネントで名前解決がどのように自動的に動作するかを示します。

RAS Connection Broker を追加する

1. [Connection Broker] タブで、[タスク] > [追加] をクリックします。
2. [サーバー] フィールドで、サーバーの IP アドレスを入力します。
3. [次へ] をクリックします。

4 開いたダイアログで、 IP アドレスが FQDN に解決されていることと、[サーバー] フィールドに FQDN が記載されていることを確認します。

RAS Secure Gateway の追加

1 [ゲートウェイ] タブで、[タスク] > [追加] をクリックします。

2 [サーバー] フィールドで、サーバーの IP アドレスを入力します。

3 [解決] をクリックします。これにより、IP アドレスが [IP] フィールドにコピーされます。その後 [次へ] ボタンをクリックして有効にします。

4 [次へ] をクリックします。

5 [RAS Secure Gateway をインストール] ダイアログで、サーバーの IP アドレスが FQDN に置き換わっていることを確認します。

RD セッションホストを追加

1 [RD セッションホスト] タブで、[タスク] > [追加] をクリックします。

2 ウィザードの最初のページで、サーバーの IP アドレスを入力して、プラスマークのアイコンをクリックします。

3 サーバーがリストに追加されており、IP アドレスが自動的に解決された FQDN に置き換わっていることを確認します。

プロバイダーの追加

1 [ファーム] > [サイト] > [プロバイダー] タブで、[タスク] > [追加] をクリックします。

2 追加するプロバイダーを選択します。

3 [アドレス] フィールドにプロバイダーの IP アドレスを入力します。

4 残りのプロパティを入力し、[次へ] をクリックします。

5 プロバイダーのアドレスが FQDN に置き換わっていることを確認します。

コンピューター管理ツール

標準的な Windows コンピューター管理タスクを実行する必要があるときに、RAS Console から離れることなくタスクを実行できます。タスクには、リモートデスクトップ接続、コンピューター管理、サービス管理、イベントビューアー、PowerShell、再起動などが含まれます。こ

れらのタスクを実行するには、[サイト] メニューや各 Parallels RAS インフラストラクチャサーバーおよびセッションホストから利用できる [ツール] メニューを使用します。

コンピューター管理ツールを使用するための要件

一部のツールは、RAS Console で使用する前に適切なターゲットホスト構成が必要になります。次に記載する要件を満たしていることを確認してください。

リモートデスクトップを使用するには、ターゲットホスト上でリモート接続が有効になっている必要があります。Windows 標準のリモートデスクトップ接続アプリケーションを使用して確認し、リモートサーバーに接続できるかどうかを確かめることができます。

PowerShell 関連ツールを使用するには、対象サーバー上で PowerShell のリモート接続が有効になっている必要があります。PowerShell のリモート接続を有効にするには、対象のコンピューターの PowerShell ウィンドウで管理者権限を使用して `Enable-PSRemoting` コマンドレットを実行します。次の点に注意してください。

- このコマンドレットは、PowerShell リモートコマンドを受け取れるようにコンピューターを構成します。
- このコマンドレットは、他のタスク全体に対して WinRM（Windows リモート管理）サービスを開始します。WinRM サービスが実行中かどうかを確認するには、`Test-WSMan` コマンドレットを使用します。
- このコマンドレットを実行すると、すべてのタスクについて、実行するかどうかの確認が行われます。このような確認なしでコマンドを実行するには、`-Force` オプションを使用します。
- “このコンピューターのネットワーク接続の種類の 1 つがパブリックに設定されているため、WinRM ファイアウォール例外は機能しません”という内容のエラーが発生した場合は、`-SkipNetworkProfileCheck` オプションを使用してこのコマンドレットの実行を試みるか、このホストのネットワーク接続タイプをドメインまたはプライベートに変更することができます。

PowerShell を使用してリモートホストを管理するには、RAS Console をインストールしたコンピューターの TrustedHosts リストにそのホストを追加する必要もあります。現在の TrustedHosts リストを表示するには、PowerShell ウィンドウで次のコマンドを実行します。

```
Get-Item WSMan:\localhost\Client\TrustedHosts
```

TrustedHosts リストにホストを追加するには、以下に説明するいずれかのオプションを使用します。最後の例を除き、以下の例ではすべて既存の TrustedHosts リストが上書きされます。

特定のコンピューターを既存のリストに追加するには、最後の例（-Concatenate パラメーターを使用した例）に従ってください。

すべてのコンピューターをリストに追加する。

```
Set-Item WSMan:\localhost\Client\TrustedHosts *
```

すべてのドメインコンピューターを追加する。

```
Set-Item WSMan:\localhost\Client\TrustedHosts *.domain-name.dom
```

特定のコンピューターを追加する（複数可）。

```
Set-Item WSMan:\localhost\Client\TrustedHosts <computer-name>,[<computer-name>]
```

1 台のコンピューターを既存のリストに追加する（既存の TrustedHosts リストを上書きしない唯一の例です）。

```
Set-Item WSMan:\localhost\Client\TrustedHosts -Concatenate <ComputerName>
```

利用可能なツール

以下の表に、[タスク] > [ツール] メニューで利用できるツールとその実行文字列を示します。

ツール:	実行文字列	説明
リモートデスクトップ	mstsc.exe /v:<selectedRDShostName>:<port> /admin	選択した RDS ホストへの標準 RDP 接続を開始します。
コンピューター管理	compmgmt.msc /computer:<selectedRDShostName>	選択したホストに接続して、コンピューター管理をローカルで開始します。
サービス管理	services.msc /computer:<selectedRDShostName>	選択したホストに接続して、サービス管理をローカルで開始します。
イベントビューアー	eventvwr.msc /computer:<selectedRDShostName>	選択したホストに接続して、イベントビューアーをローカルで開始します。
共有フォルダー	smgmt.msc /computer:<selectedRDShostName>	選択したホストに接続して、共有フォルダーをローカルで開始します。

Powershell	Enter-PSSession - ComputerName <selectedRDShostName> [-Credential username]	選択したホストに接続して、ローカルで PowerShell を開始します。
IPconfig	- 選択したホストに対する Powershell リモート接続 - Get-NetIPConfiguration	選択したホストのネットワーク構成を提供します。
Ping	- 選択したホストに対する Powershell リモート接続 - Test-NetConnection -ComputerName www.microsoft.com | Select -ExpandProperty PingReplyDetails | FT Address, Status, RoundTripTime	選択したホストの ICMP 応答をステータスおよび RTT と共に提供します。
Netstat	- 選択したホストに対する Powershell リモート接続 - Get-NetTCPConnection	選択したホストの Transmission Control Protocol のネットワーク接続を表示します。
再起動	shutdown /m \\<selectedRDShostName> /f /r /t 0	選択したホストを再起動します。
シャットダウン	shutdown /m \\<selectedRDShostName> /f /s /t 0	選択したホストをシャットダウンします。

なお、各ツールが利用できるかどうかは、サーバーの種類によって異なります。たとえば HALB の場合、 [ツール] メニューで利用できるのは [Ping] のみです。

サイト情報

サイト情報を表示するには、RAS Console で [情報] カテゴリーを選択します。

[サイト情報] タブに、利用できるサーバー、Connection Broker、Secure Gateway（「Viewing Gateway Summary and Metrics」（p. 107）を参照してください）、ローカルコンピューター上のセッションについての情報が表示されます。実行中のアプリケーションについての情報を表示するには、[アプリケーション情報を表示] オプション（ページ下部）を選択します。

[ローカル情報] タブには、ローカルサーバーで実行されている RAS のコンポーネントのステータスが表示されます。

サイト設定

一般的なサイト設定を表示して構成するには、RAS Console で、[ファーム] > <サイト> > [設定] に移動します。

監査

[監査] タブでは、各種の監査を構成できます。有効にすると、アプリケーション監査によって、サイトで実行中のプロセスがモニタリングされ、監査ファイル内にこの情報が記録されます。この情報を表示するには、[監査を表示する] ボタン（ページ下部）をクリックします。この情報は、[情報]>/ [サイト] ページと RAS レポートにも表示されます。

アプリケーション監査を有効または無効にするには、[監査] ドロップダウンリスト（ページ下部）を使用します。[監査ファイルをクリア] ボタンを押すと、現在の監査がクリアされます。

[次のプロセスのフィルタリング] リストを使用して、監査から除外するプロセスを指定できます。[タスク] ドロップダウンリストを使用して、プロセスを追加または削除します。[タスク] メニューを使用して、CSV ファイルでプロセスのリストをインポートおよびエクスポートすることもできます。[タスク] > [プロパティ] メニュー項目を使用して、プロセス名を編集できます。[デフォルト] メニュー項目では、リストをリセットして標準プロセスのデフォルトのセットを含めます。

グローバルロギング

[グローバルロギング] タブでは、Parallels RAS コンポーネントのログレベルを指定できます。ログは、Parallels RAS サポートエンジニアが、Parallels RAS インストールで起こる可能性のある問題を分析するために使用します。ログレベルを指定するには、リスト内のサーバーを 1 つ以上選択し、[ログの構成] 項目をクリックします。ダイアログが開いたら、次のいずれかを選択します。

- 標準 - 最も重要なイベントのみを記録する標準のログレベルです。後述のいずれかのログレベルを使用するように Parallels RAS サポートから指定された場合以外は、常にこのレベルを使用してください。
- 拡張 - このログレベルでは、標準ロギングよりも多くの情報が含まれます。ただし、収集する必要のある情報が増加するため、システムの速度が低下します。

- 詳細 - 詳細ロギングには拡張ロギングよりも多くの情報が含まれるため、システムの速度が大幅に低下する可能性があります。

パフォーマンスの低下を回避するには、拡張ロギングと詳細ロギングを（分析のために必要な情報を収集する上で十分な）限定的な期間のみ有効にする必要があります。この期間は [後で標準レベルにリセット] オプションを使用して設定できます。デフォルト値は 12 時間です。場合によっては、Parallels サポートエンジニアが、この期間に別の値を設定するようにアドバイスします。この期間が終了すると、ログレベルがリセットされて標準に戻ります。

収集されたログファイルが含まれる ZIP アーカイブを取得するには、[取得] 項目をクリックし、ファイルを保存する場所を指定します。[クリア] 項目は、すべてのログをクリアします。

サーバーの種類（RD セッションホスト、ゲートウェイなど）が表示されているページに移動して、[タスク]（または右クリック） > [トラブルシューティング] > [ロギング] をクリックすることで、個別のサーバーにログレベルを設定することもできます。開いているコンテキストメニューには、上述と同じ [構成]、[取得]、[クリア] の各オプションが表示されます。サーバーのリスト内の [ログレベル] 列は、現在の設定レベルを示しています。

URL リダイレクト

[URL/メールのリダイレクトを許可] オプションが RD セッションホスト、仮想マシンまたは Remote PC に対して有効になっている場合に（対応するサーバープロパティの [Agent 設定] タブ）、[URL リダイレクト] タブでリダイレクトルールを作成して拒否される URL を指定できます。また、特定の URL のリダイレクトを拒否することも可能です。URL は、リダイレクトが許可されている場合はクライアント側で、リダイレクトが拒否されている場合はリモートセッションホストで開きます。

リダイレクションルールについては、以下に注意してください。

- リダイレクションのルールは上から下の順に適用されます。
- URL にマッチした最初のルールだけが適用されます。
- URL の一部がルールに一致すると、リダイレクトされます。たとえば、https://www.parallels.com、www.parallels.com、remoteapplicationserver、および www.parallels.com/remoteapplication はすべて、https://www.parallels.com/remoteapplicationserver にリダイレクトされる有効なルールです。

新しいリダイレクトルールを追加するには、次の操作を実行します。

1. クライアントデバイスで Parallels Client を構成し、URL リダイレクトを許可します。
2. 特定のアプリケーションでは、RD セッションホスト、またはリモート PC で URL リダイレクトを有効にする必要があります（対応するサーバーのプロパティの [Agent 設定] タブを参照）。
3. （RD セッションホストのみ）特定のアプリケーションでは、アプリケーションが公開されているサーバーで [登録されたアプリケーションを置き換え] オプションを有効にする必要があります。これを行うには、[ファーム] > [RD セッションホスト] > RD セッションホストを右クリック > [プロパティ] > [Agent 設定] > 構成を選択します。
4. RAS Console で [ファーム] > [設定] に移動します。
5. [URL リダイレクト] タブを選択します。
6. [タスク] > [追加] をクリックします（または [+] アイコンをクリックします）。
7. [URL] フィールドには、リダイレクトする必要のある URL を指定します。
8. [アクション] ドロップダウンリストで、[リダイレクト] または [リダイレクトしない] を選択します。
9. [OK] をクリックします。
10. [適用] をクリックします。

通知

「システムイベント通知」（p. 594）を参照してください。

クライアントの設定

「クライアント設定の指定」（p. 324）を参照してください。

機能

「FSLogix プロファイルコンテナー」（p. 140）と 「Windows Virtual Desktop の有効化とプロバイダーの追加」（p. 247）を参照してください。

アプリケーションパッケージ

「MSIX アプリケーションパッケージの使用」（p. 576）を参照してください。

MSIX アプリケーションパッケージの使用

Parallels RAS 19 は、MSIX app attach テクノロジーをベースにした新しい最新のアプリケーション配布方法である、アプリケーションパッケージを提供します。MSIX app attach は、Microsoft のアプリケーションレイヤー化ソリューションで、ユーザーセッションに対してアプリケーション（コンテナー化された MSIX パッケージ）を動的に接続できるようにする機能を提供します。アプリケーションを OS から切り離すことで、適切なユーザーに必要なアプリケーションを提供できるようになり、より制御しやすくなります。Parallels RAS でのアプリケーションモデレーションには、appCURE などのサードパーティソリューションも使用できます。

前提条件

- 「RD セッションホスト」（p. 108）、「VM」（p. 164）、「AVD ホスト」（p. 241）。
- MSIX App Attach を利用するには、Windows Server 2022、Windows 11、Windows 10 version 2004 以降を実行しているホストが必要です。
- MSIX イメージの保存先となるネットワーク共有。ストレージの要件と推奨事項については、以下を参照してください: https://docs.microsoft.com/en-us/azure/virtual-desktop/app-attach-file-share。
- すべてのホスト（コンピューターアカウント）に、MSIX イメージが保存されているネットワーク共有に対する読み取り権限が付与されている。

注: Parallels RAS 19 では、Windows Server 2022 を使用している場合のみ、MSIX app attach アプリケーションを Parallels RAS Console から直接展開および管理できます。

アプリケーションパッケージ機能を有効化する

MSIX アプリケーションパッケージで作業を開始するには、アプリケーションパッケージ機能を有効にする必要があります。

アプリケーションパッケージ機能を有効化するには:

1. [ファーム] > [サイト] > [設定] に移動して、[アプリケーションパッケージ] タブを選択します。
2. [アプリケーションパッケージ機能を有効化] オプションを選択します。

次に、Parallels RAS にパッケージを追加する必要があります。

MSIX イメージの作成

MSI、EXE、ClickOnce、App-V などのデスクトップインストーラーから MSIX パッケージを作成するには、MSIX パッケージングツール、https://docs.microsoft.com/en-us/windows/msix/packaging-tool/tool-overview を使用します。

MSIX パッケージのアプリケーションを MSIX イメージに展開するには、MSIXMGR ツール https://docs.microsoft.com/en-us/azure/virtual-desktop/app-attach-msixmgr を使用します。

MSIX アプリケーションパッケージを Parallels RAS に追加する

MSIX アプリケーションパッケージを Parallels RAS に追加するには、以下の手順を実行します。

1. [ファーム] > [サイト] > [アプリケーションパッケージ] に移動します。
2. [タスク] > [追加] をクリックします（または [+] アイコンをクリックします）。[MSIX イメージから追加] ウィザードが開きます。
3. [MSIX イメージパス] フィールドで、イメージのパスを指定するか、[参照] ボタンをクリックしてファイルエクスプローラーで選択します。ファイルは、ネットワーク共有に存在している必要があります。VHD、VHDX、CIM イメージからパッケージを追加できます。すべてのホスト（コンピューターアカウント）に、MSIX イメージが保存されているネットワーク共有に対する読み取り権限が付与されている。
4. [パッケージ] ドロップダウンリストで、追加したいパッケージを選択します。
5. [表示名] フィールドで、Parallels RAS でこのパッケージに使用される名前を指定します。その後、残りの項目は自動的に入力されます。
6. [完了] をクリックします。

次に、ホストを追加する必要があります。追加されたパッケージアプリケーションは、ホストにインストールされた場合と同様、通常のアプリケーションと同じように動作します。

ホストにパッケージを追加する

ホストにパッケージを追加するには、次の手順を実行します。

1. 上記のように、パッケージが Parallels RAS に追加されていることを確認します。

2 [ファーム] > [サイト] > [RD セッションホスト] > [RD セッションホスト] に移動します。

3 パッケージをインストールするホストをダブルクリックします。

4 プロパティダイアログの [アプリケーションパッケージ] タブで、[タスク] > [追加] をクリック（または [+] アイコンをクリック）します。

5 左側の最初の列で、ホストにインストールするパッケージを選択します。

6 バージョン列で、パッケージのバージョンを選択します。アプリケーションのバージョンアップを容易にするために、バージョンタグ（p. 576）の活用を推奨します。選択したパッケージに依存関係がある場合、警告とともに、関連するすべてのパッケージのリストが表示されます。

7 [OK] をクリックします。

選択されたパッケージは、ホストに追加されます。

VDI プールにパッケージを追加する

VDI プールにパッケージを追加するには、次の手順を実行します。

1 上記のように、パッケージが Parallels RAS に追加されていることを確認します。

2 [ファーム] > [サイト] > [VDI] > [プール] に移動します。

3 パッケージをインストールするプールをダブルクリックします。

4 プロパティの [アプリケーションパッケージ] タブで、[既定の設定を継承] オプションをオフにします。

5 上述のサブセクション「ホストにパッケージを追加する」で説明した、手順 4 から続行してください。

選択されたパッケージは、プールですべての VM に追加されます。

AVD プールにパッケージを追加する

AVD プールにパッケージを追加するには、次の手順を実行します。

1 上記のように、パッケージが Parallels RAS に追加されていることを確認します。

2 [ファーム] > [サイト] > [Azure Virtual Desktop] > [ホストプール] に移動します。

3 パッケージをインストールするプールをダブルクリックします。

4 プロパティの [アプリケーションパッケージ] タブで、[既定の設定を継承] オプションをオフにします。

5 プロパティで、上述のサブセクション「ホストにパッケージを追加する」で説明した、手順 4 から続行してください。

選択されたパッケージは、プールですべてのホストに追加されます。

グループのデフォルト値にパッケージを追加する

グループのデフォルト値にパッケージを追加するには、次の手順を実行します。

1 上記のように、パッケージが Parallels RAS に追加されていることを確認します。

2 [ファーム] > [サイト] > [RD セッションホスト] > [グループ] に移動します。

3 パッケージをインストールするグループまたはプールをダブルクリックします。

4 プロパティで、上述のサブセクション「ホストにパッケージを追加する」で説明した、手順 4 から続行してください。

サイトのデフォルト値にパッケージを追加する

サイトのデフォルト値にパッケージを追加するには、次の手順を実行します。

1 上記のように、パッケージが Parallels RAS に追加されていることを確認します。

2 上述のように、グループまたはプールのプロパティを開きます。

3 [アプリケーションパッケージ] タブで、[サイトの既定値] をクリックします。

4 開いたダイアログで、上述のサブセクション「ホストにパッケージを追加する」で説明した、手順 4 から続行してください。

バージョンタグを使用する

バージョンタグを使用することで、パッケージの管理を簡素化できます。たとえば、公開準備の整ったパッケージとテスト段階のパッケージとで、異なるタグを割り当てることができます。Parallels RAS ではデフォルトで、 3 つのタグを使用できます。「本番」、「本番前」、「カスタム」です。タグの名前を変更することはできますが、追加や削除はできません。

タグの名前を変更するには、次の操作を実行します。

1 [ファーム] > [サイト] > [設定] に移動して、[アプリケーションパッケージ] タブを選択します。

2 名前を変更するタグを選択します。

3 [タスク] > [編集] をクリックします。

4 タグの名前を変更し、Enter キーを押します。

タグを使用するには、タグを割り当てる必要があります。

パッケージにタグを割り当てるには、次の操作を実行します。

1 [ファーム] > [サイト] > [アプリケーションパッケージ] に移動します。

2 パッケージをダブルクリックします。

3 [バージョンタグ] セクションで、必要なタグを選択します。また、1 つのパッケージに複数のタグを割り当てることも可能です。

パッケージに割り当てられたすべてのタグを削除するには、次の操作を実行します。

1 [ファーム] > [サイト] > [設定] に移動して、[アプリケーションパッケージ] タブを選択します。

2 パッケージを選択します。

3 [タスク] > [すべてのタグを削除] をクリックします。

証明書の取り扱いについて

Parallels RAS はコード署名証明書を使用して、MSIX アプリケーションパッケージの信頼性とコンテンツの整合性を確保します。

以下のコード署名証明書を使用できます。

- 自己署名証明書
- CA 証明書
- 内部 CA 証明書

GPO を使用してコード署名証明書をプロビジョニングするか、Parallels RAS によってホストに自動的にインストールできます。パッケージのコード署名証明書は、そのパッケージを使用するすべてのホストから信頼される必要があります。

Parallels RAS では、ホストに証明書を自動的に追加できます。このオプションは、自己署名証明書の場合に推奨されます。

証明書の自動プロビジョニングを有効にするには、次の操作を実行します。

1 [ファーム] > [サイト] > [設定] に移動して、[アプリケーションパッケージ] タブを選択します。

2 オプション、[パッケージ証明書の自動プロビジョニング] を選択します。

証明書の有効期限は、[ファーム] > [サイト] > [アプリケーションパッケージ] に表示されます。

MSIX アプリケーションパッケージの管理

追加されたパッケージは、[ファーム] > [サイト] > [アプリケーションパッケージ] タブで管理できます。

[タスク] のドロップダウンリストで、以下の操作を実行できます:

- 追加: 新しいパッケージを追加します。
- バージョンタグを変更: パッケージにタグを割り当てます。
- すべてのタグを削除: パッケージからすべてのタグを削除します。
- 公開済みのリソースを表示: パッケージから公開されているすべてのアプリケーションと、それらが公開されているホストの一覧を開きます。
- 割り当て済みのセッションホストを表示: 選択したパッケージが割り当てられているホストの一覧を表示します。
- 検索: フィルタリングにより、リスト内のパッケージを検索することができます。
- 削除: Parallels RAS からパッケージを削除します。
- 設定監査: パッケージに加えられた変更を表示できる [設定監査] ダイアログが開きます。
- 更新: パッケージリストを更新します。
- プロパティ: パッケージのプロパティを表示します（下記参照）。

パッケージのプロパティ

[アプリケーションパッケージのプロパティ] ウィンドウでは、次の設定が可能です。

[一般] タブ:

- サイトのアプリケーションパッケージを有効化: このオプションは、パッケージを有効にする場合に選択します。

- パッケージ: パッケージの名前です。
- 表示名: Parallels RAS 内で使用されるパッケージの名前です。
- バージョン: パッケージのバージョンです。
- 公開者: 公開者のコモンネームです。
- MSIX イメージパス: MSIX イメージへのパスです。
- バージョンタグ: パッケージに割り当てられたタグです。パッケージに割り当てるタグは、ここから変更できます。
- アプリケーション: パッケージから追加されたアプリケーションの一覧です。
- 依存関係: パッケージのすべての依存関係です。

- [証明書] タブ:
  - キーサイズ: 証明書のサイズです。
  - 有効期限: 証明書の有効期限です。
  - コモンネーム: 証明書に指定されたコモンネームです。
  - 証明書情報の表示: 証明書に関する情報を表示します。

パッケージステータス

ステータスの色	パッケージステータス	説明
緑	待機	パッケージが有効になり、登録できるようになりました。
緑	使用中	パッケージはセッションで使用されています。
オレンジ	無効	セッションの登録解除を待機しています。
赤	ステージングに失敗しました	登録に問題が発生しました。「アプリケーションパッケージ」(p. 135)の説明に従って、登録を再試行できます。
赤	見つかりません	イメージファイルまたはネットワークロケーションが利用できません。管理者はステージングを再試行できます。

赤	証明書の紛失	パッケージ証明書がホスト上で見つかりません。
赤	バージョンが見つからない	ホスト構成で選択されたタグが付けられたアプリケーションパッケージが見つかりません。
適用されません	適用されません	設定が変更されましたが、適用されていません。

テンプレートバージョンの使用

テンプレートのバージョンでは、ホスト上で変更を安全にテストし、必要に応じてロールバックを実行することができます。

サポート対象のプロバイダー

テンプレートのバージョンは以下のプロバイダーに対応しています:

ハイパーバイザープロバイダー:

- Microsoft Hyper-V
- Microsoft Hyper-V Failover Cluster
- VMware ESXi
- VMware VCenter

クラウドプロバイダー:

- Microsoft Azure

仮想化サービス:

- Azure Virtual Desktop

新しいバージョンを作成する

新しいバージョンを作成するには、次の操作を実行します。

1 次のいずれかを実行します。

- RD セッションホストテンプレートの新しいバージョンを作成するには、[ファーム] > [サイト] > [RD セッションホスト] > [テンプレート] に移動します。
- VDI ホストテンプレートの新しいバージョンを作成するには、[ファーム] > [サイト] > [VDI] > [テンプレート] に移動します。
- AVD ホストテンプレートの新しいバージョンを作成するには、[ファーム] > [サイト] > [Azure Virtual Desktop] > [テンプレート] に移動します。

2 テンプレートを選択し、メンテナンスモードに入ってから、変更を加えて終了します。新しいテンプレートバージョンを作成するよう促すダイアログが表示されます。[新しいバージョンを作成] オプションを選択します。

> **注:** 1 つのテンプレートに最大 5 つのバージョンを含めることができます。別のバージョンを作成したい場合は、すでに存在するバージョンを削除する必要があります。

3 [次へ] をクリックします。

4 [新しいテンプレートのバージョン] ページで、名前と説明を指定し、バージョンのタグを選択します。タグが以前に別のバージョンに割り当てられていた場合、そのタグはこのバージョンから削除されます。タグは、複数選択できます。

5 [次へ] をクリックします。

6 （オプション）[ホストプールを選択] ページで、スケジュールで再作成するホストプールを選択し、[構成] ボタンをクリックします。再作成を予約するダイアログが表示されます。必要に応じてスケジュールを構成し、[次へ] をクリックします。

7 [完了] をクリックします。

バージョンタグを使用する

タグの名前を変更するには、次の操作を実行します。

1 [ファーム] > [サイト] > [設定] に移動して、[テンプレートのバージョン] タブを選択します。

2 名前を変更するタグをダブルクリックします。

3 タグの名前を変更し、Enter キーを押します。

バージョンのタグを再割り当てするには次の操作を実行します。

1 次のいずれかを実行します。

- RD セッションホストテンプレートのタグを再割り当てするには、[ファーム] > [サイト] > [RD セッションホスト] > [テンプレート] に移動します。
- VDI ホストテンプレートのタグを再割り当てするには、[ファーム] > [サイト] > [VDI] > [テンプレート] に移動します。
- AVD ホストテンプレートのタグを再割り当てするには、[ファーム] > [サイト] > [VDI] > [Azure Virtual Desktop] > [テンプレート] に移動します。

2 テンプレートを選択し、[タスク] > [バージョン] をクリックします。[バージョン] ダイアログが開きます。

3 バージョンを選択し、[タスク] > [プロパティ] をクリックします。

4 [バージョンタグ] セクションで、必要なタグを選択します。タグが以前に別のバージョンに割り当てられていた場合、そのタグはこのバージョンから削除されます。また、1 つのバージョンに複数のタグを割り当てることも可能です。他のホストプールが同じタグで同じバージョンを使用している場合、そのホストプールでホストを再作成するためのダイアログが表示されます。

バージョンを削除する

バージョンを削除するには、以下の操作を実行します。

1 次のいずれかを実行します。

- RD セッションホストテンプレートのバージョンを削除するには、[ファーム] > [サイト] > [RD セッションホスト] > [テンプレート] に移動します。
- VDI ホストテンプレートのバージョンを削除するには、[ファーム] > [サイト] > [VDI] > [テンプレート] に移動します。

- AVD ホストテンプレートのバージョンを削除するには、[ファーム] > [サイト] > [VDI] > [Azure Virtual Desktop] > [テンプレート] に移動します。

2 テンプレートを選択し、[タスク] > [バージョン] をクリックします。[バージョン] ダイアログが開きます。

3 バージョンを選択し、[タスク] > [削除] をクリックします。

設定監査

設定監査では、最近変更されたバージョンを確認することができます。

設定監査を行うには、次の操作を実行します。

1 次のいずれかを実行します。

- RD セッションホストテンプレートのバージョン設定監査を行うには、[ファーム] > [サイト] > [RD セッションホスト] > [テンプレート] に移動しします。
- VDI テンプレートのバージョン設定監査を行うには、[ファーム] > [サイト] > [VDI] > [テンプレート] に移動しします。
- AVD テンプレートのバージョン設定監査を行うには、[ファーム] > [サイト] > [VDI] > [Azure Virtual Desktop] > [テンプレート] に移動しします。

2 テンプレートを選択し、[タスク] > [バージョン] をクリックします。[バージョン] ダイアログが開きます。

3 バージョンを選択し、[タスク] > [設定監査] をクリックします。

設定監査

Parallels RAS では、コンポーネント、オブジェクト、リソース、ユーザーのいずれかの変更など、Parallels RAS ファームに加えられた変更を監査する機能が利用できます。この情報は、確認し、必要な場合は元に戻せるようにデータベースに保存されます。この情報はプライマリデータベースに保存されますが、Parallels RAS Console が実行されているコンピューターのローカルデータベースに複製されます。

以下のいずれかのオプションを使用して、変更の一覧を表示できます。

- [管理] > [設定監査] に移動します。タブには、ファームのコンポーネント/オブジェクトに対するすべての変更のメインリストが表示されます。変更を元に戻せる場合は、ここで実行できます。

- この機能をサポートする RAS Console の任意のペインで、[タスク] > [設定監査] をクリックします。メインリスト（上で説明）とは異なり、特定のペインで管理される同じタイプのコンポーネントまたはオブジェクトに対する変更のみが表示されます。元に戻せる変更はここで元に戻すこともできます。[設定監査] メニューオプションが特定のペインで使用できない場合、この機能はそのペインが管理するタイプのコンポーネントまたはオブジェクトには利用できない機能であることを意味しています。

次に、ファームの変更を表示する方法と元に戻す方法について詳しく説明します。

メイン設定監査リストの表示

ファームに対するすべての変更のメインリストを表示するには、次の操作を実行します。

1. Parallels RAS Console で、[管理] カテゴリーを選択し、[設定監査] タブをクリックします。
2. 同期プロセスは、ローカルの監査データベースがプライマリデータベースと同期しているかどうかを確認し、必要に応じて更新します（同期の進行中、進行状況のインジケーターが表示される場合があります）。
3. 同期が完了したら、[設定監査] タブにデータが入力されます。リストの各エントリは、RAS 管理者またはシステムサービスにより実行された変更に対応します。

監査データベースの同期を解除する

デフォルトでは Parallels RAS により、すべての Connection Broker で監査データベースが同期されます。データベースの規模が大きくなると、所要時間も長くなります。データベースの同期を解除することもできます。この場合、現在のライセンス Connection Broker 上の監査データベースにのみアクセスできます。ライセンス Connection Broker を変更した場合、同期を有効にしないと以前の監査データベースにアクセスできなくなります。

監査データベースの同期を解除するには次の手順を実行します。

1. [監査の設定] タブで [タスク] ドロップダウンリストをクリックし、[設定] を選択します。
2. [すべての Connection Broker で管理者の監査データを複製する] オプションを解除します。
3. [OK] をクリックします。

変更に関する情報

リストにある各エントリの情報には、以下が含まれます。

- 日付: 変更の日付と時刻。
- セッション: セッション ID。
- ユーザー名: 変更を担当した管理者または RAS サービスの名前。RAS サービスには、システム（冗長サービス）および Connection Broker（コントローラーサービス）が含まれます。
- アクション: 接続、切断、作成、アップデート、サイトの切り替え、その他の実行されたアクション。
- ID: 影響を受けたオブジェクトの ID です。
- サイト: 影響を受けたサイトの数と名前です。[グローバル] は、変更がすべてのサイトに影響したことを意味します。
- タイプ: 変更のタイプ。これは通常、[アクション] 値と合わせて表示すると筋が通ります。
- 名前: この列の値はいくつかのエントリに対して表示され、変更されたオブジェクトの名前などの追加情報が得られます。

共通タスク

一覧にある次のアクションを実行できます。

- リストを更新するには、[リサイクル] アイコン（右上）をクリックします。
- エントリーの詳細を表示するには、対象のエントリーをダブルクリックします（または、エントリーを選択し、[タスク] > [エントリーを見る] をクリックします）。
- 特定のエントリー（または複数のエントリー）を検索するには、虫眼鏡アイコン（右上）をクリックします。リストの最上部に行を追加して、検索条件を入力できます。1 つまたは複数の列に、検索する文字列を入力できます。入力すると検索が実行され、リストがフィルタリングされて、一致するエントリーのみが表示されます。フィルタリングを中止してリスト全体を表示するには、虫眼鏡アイコンを再度クリックします。

変更を元に戻す

メインリストで変更を元に戻すには、次の操作を実行します。

1 [設定監査] タブで目的のエントリーをダブルクリックします。

2 [エントリの監査] ダイアログが開きます。ここでは、[次へ] ボタンと [前へ] ボタンをクリックして、メインリストに表示されている次の項目または前の項目に移動できます。

3 変更を元に戻すには、[元に戻す] ボタンをクリックします。ボタンが無効な場合、変更は元に戻せないことを意味します。

元に戻せない変更には、以下が含まれます。

- システムまたは Connection Broker が実行した変更（[ユーザー名] 列の表示に従います）。
- この機能が存在していなかった以前のバージョンの Parallels RAS で実行された変更。
- 管理者アカウントに関連する変更。

ローカル設定監査リストの表示

特定のタイプの RAS コンポーネントまたはオブジェクトに対する構成の変更も表示および元に戻すことができます。RAS Console の特定のペイン（またはタブ）を表示しているときに、[タスク] > [設定監査] メニューオプションを探します（または右クリックして [設定監査] を選択します）。オプションがある場合は、変更を表示して、必要な場合は元に戻すことができます。下の例を考えてみましょう。

RD セッションホストに加えられた変更を表示したいとします。このためには、次の操作を実行します。

1 RAS Console で、[ファーム] > <サイト> > [RD セッションホスト] に移動します。

2 [タスク] > [設定監査] をクリックします。

3 [設定監査] ダイアログが開き、RD セッションホストに加えられたすべての既知の変更が一覧表示されます。変更には、RD セッションホストの作成、移動、削除、またはアップデートなどが含まれます。変更のタイプは、リストの [アクション] 列に表示されます。

4 変更を元に戻すには、選択して [元に戻す] ボタン（ダイアログの右下）をクリックします。特定のエントリを選択したときにボタンが無効になっている場合は、変更を元に戻せないことを意味します。

ローカル設定監査機能は、Parallels RAS Console のほとんどの主要なコンポーネントおよびオブジェクトで利用できます。これには、RD セッションホスト（グループおよびスケジューラーを含む）、VDI、リモート PC、ゲートウェイ、Connection Broker、テーマ、公開、クイックキーパッド、その他多数が含まれます。上記と同様に、特定のペインを表示するには、[タスク] > [設定監査] メニューオプションを探します（または右クリックして、[設定監査] を選択します）。オプションがある場合は、変更を表示して、必要な場合は元に戻すことができます。

RAS Agent のアップグレード

Parallels RAS コンポーネントをファームに追加するとき、そこに対応する RAS Agent をインストールします。これには、RAS Connection Broker、RD セッションホスト Agent、Provider Agent、Guest Agent、Remote PC Agent が含まれます。Agent のステータスを確認し、必要な場合はアップデートできる機能に加えて、一括 Agent アップデートまたはアップグレードも実行できます。

Agent をアップデートする必要があるかどうかを確認する方法は 2 つあります。Parallels RAS から通知を受け取ること、またステータスを確認してアップデート手順を手動で開始することができます。

Parallels RAS Console を起動すると、Agent のインストールまたはアップデートが必要なことを伝えるメッセージボックスが表示されることがあります。ダイアログで [はい] をクリックすると、アップデート手順を開始できます。Agent をアップデートする必要のあるすべてのサーバーのリストが表示されます。ここで、サーバーを一括アップデート手順に含めるか、除外するかを決定できます。選択したら、画面の指示に従って Agent をアップデートします。

手順を手動で開始するには、このメニューを利用できる RAS Console （多くのビューが合理的な場所にあります）で [タスク] > [すべての Agent をアップグレード] をクリックします。ビューの内側を右クリックして、[すべての Agent をアップグレード] を選択することもできます。画面の指示に従って、Agent のアップデートまたはアップグレードが必要なサーバーを選択します。特定のペインに表示されたすべてのサーバーのすべての Agent が最新の状態である場合、メニューオプションは無効にされることに注意してください。

たとえば、すべてのサイトですべてのプライマリ Connection Broker をアップグレードするには、[ファーム] > [ファーム] を選択し、[タスク] > [すべての Agent をアップグレード] をクリックします（またはペインの内側を右クリックして、[すべての Agent をアップグレード] を選択します）。サイトのすべてのサーバーで一括して Agent をアップグレードするには、[ファーム] > <サイト> を選択し、[タスク] > [すべての Agent をアップグレード] をクリックします。同様に、すべての RAS Secure Gateway で Agent をアップグレードするには、[ファーム] > <サイト> > [Secure Gateway] を選択し、同じ [タスク] > [すべての Agent をアップグレード] メニュー項目を使用します。他のコンポーネントについても、まったく同じように実行します。すべてのサーバーで同じ資格情報を使用する場合は、1 回のみそれらを入力する必要があります。アップデート手順では、最後に入力した資格情報が記憶され、この資格情報がすべてのサーバーで使用されます。資格情報がサーバーで機能しない場合は、再度入力を求められます。

[タスク] > [すべての Agent をアップグレード] メニューをクリックした後に開くダイアログには、アップデートまたはアップグレードが必要な Agent があるホストが表示されることに注意してください。リストの [ステータス] 列は、アップデートまたはアップグレードが必要なことと、ホストがアップグレードのために事前に選択されることを示します。未確認の Agent もリストに含まれますが、事前に選択されません。そこにアップグレードが必要な Agent があると思われる場合は、選択できます。

注: テンプレート（VDI）内で Agent をアップデートするときは、完全な複製のテンプレートとリンクされた複製のテンプレートが別々に更新されます。重要な情報を含む詳細については、「テンプレートのメンテナンス」セクション（p. 208）を参照してください。

ライセンス

[ライセンス] カテゴリでは、Parallels RAS ライセンスを管理できます。[ライセンス] カテゴリーをクリックすると、[ライセンスの詳細] タブに以下の情報が表示されます。ライセンスの種類（前払いのサブスクリプション、SPLA、NFR、トライアル）によって、表示される情報が異なりますのでご注意ください。また、NFR（非売品）ライセンスには、前払いのサブスクリプションと SPLA があり、NFR ライセンスの場合は異なる情報が表示されることがあります。ご注意ください。

[ライセンスの詳細] タブに表示される情報は以下の通りです。

- ライセンスの種類: ご使用の Parallels RAS ライセンスの種類（前払いのサブスクリプション、SPLA、NFR、トライアルなど）。
- ライセンスキー: ファームのアクティベーションに使用されたライセンスキー（末尾の文字のみ表示）。
- サポートの有効期限: サポートプランの有効期限です。
- アップグレード保証: サブスクリプションベースのライセンスを使用している場合、ライセンスは自動アップグレードの対象となるため、サブスクリプションの有効期限とアップグレード保証の有効期限は一致します。
- 有効期限: ライセンスの有効期限（トライアルライセンスの場合は残り日数）です。
- 初回アクティベート: ファームが初めてアクティベートされた日付です。
- ピークユーザー数: ピーク時の同時接続ユーザー数です。前払いのサブスクリプションでは、この値を使用して、同時使用ユーザー数を増やすためにサブスクリプションをアップグレードする必要があるかどうかを判断できます。

- 当日の使用状況: SPLA ライセンスのみです。当日に記録された最大同時使用ユーザー数です。なお、”当日”は UTC の 0 時から始まります。
- 現在の期間の使用状況: SPLA ライセンスのみです。同じライセンスキーでアクティベートされたすべてのファームおける全体の使用状況（SPLA ライセンスでは、同じキーで複数のファームをアクティベートできます）。
- 請求期間開始日: SPLA ライセンスのみです。現在の請求期間の開始日です。
- 請求期間終了日: SPLA ライセンスのみです。現在の請求期間の終了日です。
- 現在のユーザー数: Parallels RAS ファームに現在接続しているユーザーの数です。
- 同時使用ユーザー数の上限です。前払いのサブスクリプションと NFR ライセンスのみです。ご使用のライセンスで許可される同時使用ユーザー数の上限。たとえば、前払いのサブスクリプションを利用していて、さらに同時使用接続数が必要な場合、サブスクリプションをアップグレードする必要があります。
- Parallels アカウントユーザーメール: ファームのアクティベーションに使用された Parallels ビジネスアカウントのメールです。
- Parallels アカウントユーザー名: Parallels ビジネスアカウントのユーザー名です。
- Parallels アカウント企業: Parallels ビジネスアカウントの企業名です。

Parallels アカウントでもこれらの値（およびその他）を確認できることに注意してください。詳細については、Parallels ウェブサイトで利用できる「Parallels RAS ライセンスガイド」および「Parallels RAS SPLA ガイド」をお読みください。

[アクティブユーザーの表示] ボタンを押すと、ダイアログが開き、現在のアクティブユーザーとライセンスの使用数を確認できます。ツールバーのボタンを使用して、リストの更新とクリップボードへの情報のコピーを行います。

[ライセンスを管理] ボタンを使用すると、別の Parallels アカウントに切り替え、異なるライセンスキーを使用して Parallels RAS をアクティベートできます。このボタンをクリックすると、[Parallels My Account へのサインイン] ダイアログが表示されます。このダイアログを使用して、既存のアカウントを使用してサインインするか、[登録] をクリックして、新しいアカウントを作成します。新しいアカウントを作成している場合、そこに Parallels RAS ライセンスキーを登録し、そのキーを使用して Parallels RAS ファームをアクティベートする必要があります（下記参照）。

異なるライセンスキーを使用して Parallels RAS をアクティベートするには、次の操作を実行します。

1. [Parallels My Account へのサインイン] ダイアログで、アカウントの登録に使用した電子メールアドレスとパスワードを入力し、[サインイン] をクリックします。[ライセンス認証] ダイアログが表示されます。
2. [ライセンスキーを使用してアクティベートする] オプションを選択し、提供されたフィールドにキーを入力します。フィールドの横にあるボタンをクリックすると、Parallels My Account に登録されているサブスクリプションと永久ライセンスキーのリストを表示することができます。リストが空の場合は、まだサブスクリプションがなく、まず初めに購入する必要があります。
3. サブスクリプションをオンラインで購入するには、[ライセンスを購入する] リンクをクリックします。
4. ライセンスキーを入力した後、[アクティベート] をクリックします。Parallels RAS が正常にアクティベートされたことを示す確認メッセージが表示されます。

HTTP プロキシ設定の構成

ネットワークで HTTP プロキシサーバーを使用する場合、RAS Console で構成する必要があります。プロキシサーバー設定は Parallels RAS ライセンスアップデート中に Parallels クラウドと通信する他の機能が使用します。

プロキシサーバーを構成するには、次の手順に従います。

1. RAS Console で [管理] > [設定] に移動します。
2. [HTTP プロキシ設定] セクションでは、[プロキシを設定] ボタンをクリックします。
3. ダイアログが開いたら、次のオプションのいずれかを選択します。
   - [プロキシサーバーなし] - プロキシサーバーを使用しない場合。
   - [手動での HTTP プロキシ構成] - 手動で設定を指定する場合はこのオプションを選択します。[設定を検出する] ボタンは、自動的にプロキシ設定を検出しようとします。

     [プロキシ認証が必要] オプションにより、プロキシサーバーの資格情報を指定または省略できます。プロキシサーバーが IP アドレスを使用してクライアントを認証する場合は、資格情報を省略できます。それ以外の場合は、このオプションを選択し、ユーザー名とパスワードを指定します。
4. [OK] をクリックして設定を保存します。

システムイベント通知

[ファーム] > [サイト] > [設定] > [通知] タブで、システムイベント通知を構成できます。通知は、メールを介してシステムイベントについて管理者に知らせるために使用されます。通知を構成すると、その設定はファーム内のすべてのサーバーに適用されます。

通知を構成するには、最初にしきい値（利用可能な場合）や、管理者がメールを介して通知されるかどうかを指定できる、通知ハンドラーを構成する必要があります。イベントが発生したときに自動的に実行される通知スクリプトも構成できます。

通知ハンドラーの構成

通知ハンドラーを構成するには、次の操作を実行します。

1 RAS Console で、[ファーム] > [サイト] > [設定] に移動します。

2 [通知] タブを選択します。

3 [タスク] > [新規] をクリック（またはプラス記号アイコンをクリック）して、ハンドラーを作成するイベントを選択します。イベントとその説明のリストについては、下の「システムイベント」サブセクションを参照してください。

4 イベントハンドラーの設定を指定できるダイアログが開きます。

[一般] タブで、次のオプションを指定します。

- しきい値（数字または割合）。一部のイベント（ライセンス、Agent、およびその他のイベント）には、使用できません。
- 方向（値が指定された値を超えたとき、または下回ったときのどちらでイベントがトリガーするか）。一部のイベント（上記と同じ）には、使用できません。
- 管理者に電子メールで通知するかどうか。
- イベントメッセージを送信する追加の電子メールアドレスです（コンマまたはセミコロンで区切る）。
- イベントがトリガーしたとき、スクリプトを実行するかどうか。ここでは、[通知スクリプトを実行] オプションを選択し、ドロップダウンリストからスクリプトを選択する必要があります。このオプションを使用する前に、「通知スクリプトの構成」（p. 597）の説明に従って、1 つまたは複数のスクリプトを作成する必要があります。

[条件] タブで、以下を指定します。

- タイプ: 通知のトリガーとなるオブジェクトの種類を選択します。
- サイト内の全サーバー: 利用可能なすべてのサーバーを含めるには、このオプションを選択します。
- 使用可能容量: 通知のトリガーとなるオブジェクトを選択します。

[設定] タブで、次を指定します。

- デフォルト設定使用: デフォルト設定を使用する場合は、このオプションを選択します。デフォルトを編集するには、[デフォルトを編集] リンクをクリックします。カスタム設定を使用するには、このオプションをクリアし、下記のようにオプションを指定します。
- 通知ハンドラー猶予期間: イベントの発生から通知がトリガーされるまで待機する時間（分）を指定します。トリガーしても、非常に短時間しか続かないイベントもあります。たとえば、CPU 使用率は、指定されたしきい値を超えて急激に跳ね上がる可能性がありますが、すぐに正常に戻ります。このようなイベントの場合、すぐに通知をトリガーしないのが理にかなっていると思われます。このオプションでは待機時間を指定できます。
- 通知間隔: 前回の通知と次の通知の間の最短間隔（分）を指定します。管理者に複数の通知メールが立て続けに送信されないように（つまり、スパミングを回避）することができます。
- 通知を 1 回送信した後、回復するまで通知の送信を停止: この設定が有効な場合、通知は一度のみ発生し、その後はその通知でモニターされている値が回復するまで停止されます。たとえば、CPU 使用率が 1 日中しきい値を超えている場合、通知ハンドラーを複数回実行するのではなく、RAS は一度のみ実行します。

5 完了したら、[OK] をクリックして、通知ハンドラーを保存します。

送信メールが機能するように、RAS Console でメールボックスを構成してください。このメールボックスは、通常、初めて RAS Console を実行し、RAS 環境を設定するために [開始] カテゴリを使用するときに設定されます。「イベント通知を行うように SMTP サーバー接続を構成する」（p. 601）の説明にあるように、メールボックスを設定することもできます。

イベントハンドラーを有効または無効にするには、最初の列にあるチェックボックスを選択またはクリアするか、イベントを右クリックし、[有効] または [無効] を選択します。ハンドラーを変更するには、テンプレートを右クリックして [プロパティ] を選択します。ハンドラーを削除するには、右クリックして [削除] を選択します。

システムイベント

以下のシステムイベントに対応する通知ハンドラーを作成できます。

- CPU 使用率: CPU 使用率が指定された値を超えたとき、または下回ったときにトリガーします。
- メモリ使用率: メモリ使用率が指定された値を超えたとき、または下回ったときにトリガーします。
- RDSH セッションの数: アクティブなセッション数が指定された値を超えたとき、または下回ったときにトリガーします。
- 切断済み RDSH セッションの数: 切断済みセッションの数が指定された値を超えたとき、または下回ったときにトリガーします。
- RDSH セッション使用率: RDSH セッションの数が最大セッション数に対して指定された割合を超えたとき、または下回ったときにトリガーします。
- RDSH 切断済みセッション使用率: RDSH 切断済みセッション数が最大セッション数に対して指定された割合を超えたとき、または下回ったときに発生します。
- AVD セッション使用率: AVD セッションの数が最大セッション数に対して指定された割合を超えたとき、または下回ったときにトリガーします。
- AVD 切断済みセッション使用率: 切断済み AVD セッションの数が最大セッション数に対して指定された割合を超えたとき、または下回ったときにトリガーします。
- ゲートウェイでトンネリングされたセッション数: ゲートウェイでトンネリングされたセッション数が指定された値を超えたとき、または下回ったときに発生します。
- ゲートウェイでトンネリングされたセッションが失敗しました: ゲートウェイとリソースオブジェクト間の接続が確立できない場合に発生します。
- RAS Agent イベント: エージェントイベントが発生（たとえば、エージェントが切断または再接続）したときにトリガーします。
- ライセンスイベント: ライセンスイベントが発生したときにトリガーします。ここでの注目すべきイベントの 1 つが、ライセンスの使用数が定義済みのしきい値に達することです。具体的には、ライセンスの使用数が利用可能なすべてのライセンスの 90% に達すると、電子メールが送信され、ライセンス数は十分なのか、それとも追加する必要があるのかを決断することになります。他のイベントには、ライセンスのアクティベーション/デアクティベーション、ライセンスの失効、猶予期間の開始/終了、ライセンス情報の変更、ライセンスサーバーとの通信における問題などがあります。

- 認証サーバーイベント: 認証サーバーで接続に関する問題が発生したときにトリガーします。
- 公開済みアイテムイベント: 公開済みアイテムイベントが発生したとき（アプリケーションが同時実行可能インスタンス数の上限に達した場合など）にトリガーします。
- テンプレートイベント: VDI イベント（テンプレートが見つからないなど）が発生するとトリガーします。
- テナントイベント: テナントイベントが発生したときにトリガーを実行します。詳細については、「RAS マルチテナントアーキテクチャ」 > 「通知の構成」（p. 419）を参照してください。

「通知スクリプトの構成」セクション（p. 597）にある [通知タイプ] 表も参照してください。

通知スクリプトの構成

通知スクリプトを構成するには、次の操作を実行します。

1 [通知] タブの [通知スクリプト] セクションで、[タスク] > [新規] をクリック（またはプラス記号アイコンをクリック）します。

2 ダイアログが開いたら、次のオプションを指定します。
   - スクリプト名: スクリプトのフレンドリ名を入力します。
   - コマンド: 実行するコマンド。
   - 引数: コマンドに渡すコマンドライン引数。引数は、定義済みの変数のいずれかにすることが可能で、これを Parallels RAS が自動的に実際の値と置き換えます。下記の「コマンドライン変数」の表を参照してください（ID 列にここで使用できる値が記載されています）。
   - 初回ディレクトリ: プロセスの現在のディレクトリへのフルパス。文字列は、UNC パスも指定できます。
   - ユーザー名]、パスワード: これらは、特定のユーザーアカウントでコマンドを実行する場合に指定できる、オプションのフィールドです。

3 完了したら、[OK] をクリックして、通知スクリプト項目を保存します。

通知スクリプトを変更するには、通知スクリプトを右クリックして [プロパティ] を選択します。

スクリプトを削除するには、右クリックして [削除] を選択します。スクリプトが通知ハンドラーに使用される場合は、警告メッセージが表示されることに注意してください。削除を選択すると、そのスクリプトを使用するすべての通知ハンドラーからスクリプトの関連付けが削除され、影響を受けるすべてのハンドラーが電子メールアラートを送信するように自動的に構成されます。

コマンドライン変数

以下の表は、スクリプトを実行するときに引数として使用できるコマンドライン変数の一覧です（上記の [引数] オプションの説明を参照してください）。

変数	説明
($FARM-NAME)	通知を発した RAS ファームの名前です。
($SITE-NAME)	通知を発した RAS サイトの名前です。
($SERVER-ADDRESS)	通知を発したサーバーの IP アドレスまたは FQDN。RDSH サーバー、RAS Connection Broker、RAS Secure Gateway などをホストしているサーバーの場合があります。
($TRIGGER-ADDRESS)	通知を発した Connection Broker の IP アドレスまたは FQDN。
($THRESHOLD-VALUE)	通知ハンドラーに関連付けられているしきい値。通知タイプでしきい値がサポートされていない場合、引数を空の文字列と置き換える必要があります。
($NOTIFICATION-TIME)	イベントが発生した GMT での時刻と日付。文字列形式では、"R" または "r" 形式指定子を使用します。詳しくは、Microsoft の次の記事を参照してください。 https://docs.microsoft.com/ja-jp/dotnet/standard/base-types/standard-date-and-time-format-strings 注: 時刻は、通知ハンドラーが実行された時刻ではなく、通知が発生した時刻を表す必要があります。猶予期間が有効にされている場合、通知ハンドラーが待機時間ありで実行される場合があります。
($NOTIFICATION-TYPE)	特定の各通知タイプに関連付けられている数値。通知タイプの値は、下記の通知タイプの表にリストされています。

通知タイプ

以下の表はサポートされている通知タイプのリストです（ID 列は（$NOTIFICATION-TYPE）コマンドライン変数に渡される値を表します）。

通知タイプ	ID	説明
CPU 使用率	1	CPU 使用率が特定の値を超過または下回った場合、この

		通知が送信されます。
メモリ使用率	2	メモリ使用率が特定の値を超過または下回った場合、この通知が送信されます。
アクティブなセッション数	3	アクティブなセッション数が特定の値を超過または下回った場合、この通知が送信されます。
接続していないセッション数	4	接続していないセッション数が特定の値を超過または下回った場合、この通知が送信されます。
RAS Agent 再接続	5	Agent が再接続されました。
RAS Agent 切断	6	Agent が切断されました。
VDI テンプレートが見つからない	7	この通知は VDI イベント（テンプレートが見つからないなど）が発生すると送信されます。
公開済みのアプリケーションが制限超過	8	公開済みアイテムイベント（アプリケーションのインスタンス制限を超えたなど）が発生した場合、この通知が送信されます。
マルチ CB 通信エラー	9	マルチ CB 通信エラー:
認証プロバイダーに到達できない	10	この通知は認証サーバーで接続に関する問題が発生すると送信されます。
指定された最大値に占める RDSH セッションの割合	11	RDSH セッション数が最大セッション数に対する特定の割合を超過または下回った場合、この通知が送信されます。
ゲートウェイは X 件のセッションをトンネリングしています	12	ゲートウェイでトンネリングされたセッションの数が特定の値を超えるか下回った場合、この通知が送信されます。
指定された最大値に占める切断された RDSH セッションの割合	13	RDSH 切断済みセッション数が最大セッション数に対する特定の割合を超えるか下回った場合、この通知が送信されます。
Connection Broker の自動昇格	20	Connection Broker の自動昇格
Connection Broker の自動昇格に失敗しました	21	Connection Broker の自動昇格に失敗しました。
Connection Broker の自動昇格フェイルバック	22	Connection Broker の自動昇格フェイルバック。
CA は利用できません	30	この通知は認証局で接続に関する問題が発生すると送信されます。
ライセンスサイトがフェイルオーバーモードに切り替わりました	50	Connection Broker フェイルオーバーモード。
ライセンスサイトはオフラインです	51	ライセンスサイトはオフラインです。
ライセンスサイトが再接続されました	52	ライセンスサイトがオンラインに戻りました。
ライセンス CB の IP が変更されました	53	ライセンスの Connection Broker IP を変更します。
ライセンスの CB ホスト名が変更されました	54	ライセンスの Connection Broker ホスト名を変更します。

セカンダリ CB の IP が変更されました	55	非ライセンスの Connection Broker IP を変更します。
セカンダリ CB のホスト名が変更されました	56	非ライセンスの Connection Broker ホスト名を変更します。
テンプレートのゲスト数が上限に達しました	60	テンプレートのゲスト数が上限値に達しました
テンプレートのサーバーが上限に達しました	61	テンプレートのサーバーが上限値に達しました
テンプレートの複製に失敗しました	62	テンプレートの複製に失敗しました。
ライセンスがアクティベート	100	この通知はライセンスイベント（ファームが正常にアクティベートされたなど）が発生すると送信されます
ライセンスがディアクティベート	101	ライセンスが無効になりました。
ライセンス使用率が最大	102	ライセンス使用量の最大値が x% に到達しました。
まもなく期限が切れるライセンス	103	ライセンスの有効期限が近づいている場合は、残り日数を毎日通知します。
期限切れのライセンス	104	ライセンスが期限切れです。
ライセンスのトライアルが終了	105	トライアル期間が終了
ライセンスの猶予期間開始	106	猶予期間が開始しました。
ライセンスの猶予期間終了	107	猶予期間が終了しました。
ライセンスが無効	108	ライセンスが無効になりました。
ライセンス情報が変更	109	ライセンス情報が変更
ライセンスがサーバーとの通信に失敗	110	ライセンスサーバーとの通信に失敗しました。
ライセンスにファイルがありません	111	ライセンスファイルの読み込みに失敗しました。
ライセンスのバージョンが無効	112	ライセンスファイルのバージョンが無効です。
ライセンスの署名が無効	113	ライセンスの署名が無効です。
ライセンスのライセンスが無効	114	システムエラーです。
ライセンスの MAC アドレスが無効	115	MAC アドレスが無効です（ハードウェアの変更）。
署名されていない猶予期間のライセンス	116	猶予期間の移行が開始しました。
テナントが登録されました	200	この通知は、登録されたテナントに関連するイベントが発生したとき（たとえば、新しいテナントがテナントブローカーに追加された場合やテナントが使用できなくなった場合など）に行われます。
テナントのステータスが変更されました	201	テナントのステータスが変更されました
ブローカーのステータスが変更されました	202	テナントブローカーのステータスが変更されました
テナントの登録が解除されました	203	テナントは、ブローカーから切断されました。

標準ファームのトンネルセッションが失敗しました	220	標準ファームのトンネルセッションが失敗しました。
ブローカーファームのトンネルセッションが失敗しました	221	テナントブローカーのトンネルセッションが失敗しました

イベント通知を行うように SMTP サーバー接続を構成する

[メールボックス] タブの [管理] カテゴリーでは、送信メール用の SMTP サーバーを構成できます。管理者がシステムイベントのアラート（前のセクションを参照）を受信し、ユーザーに招待メールを送信するには、SMTP サーバーが必要です。

SMTP サーバーを構成するには、次の手順に従います。

1 RAS Console で、[管理] カテゴリーを選択し、[メールボックス] タブをクリックします。

2 [メールサーバー] フィールドに、使用するメールサーバーの FDQN または IP アドレスを入力します。

3 [TLS / SSL] ドロップダウンリストで、プロトコルを使用するかどうかを選択します。

4 必要に応じて [SMTP サーバーは認証をリクエストする] オプションを選択して、表示されるフィールドに SMTP サーバーユーザー名およびパスワードを入力します。

5 [送信者情報] セクションで、送信者のメールアドレス（お使いの電子メールなど）を入力します。

6 [テストメールボックス設定] セクションを使用して、SMTP サーバーの構成をテストできます。1 つ以上のメールアドレスをセミコロンで区切って入力します。[テストメール送信] をクリックして、設定をテストします。

RAS セッション変数

リモートユーザーが公開済みのアプリケーションまたはデスクトップを起動すると、ホストサーバーで Parallels RAS によってセッション変数のセットが作成されます。この変数にはクライアントマシンについての情報が含まれます。この内容は必要に応じて調べることができます。変数は常に更新されるため、接続時または切断時に常に最新の値が含まれます。

次の RAS セッション変数を利用できます。

変数名	説明
TUX_REMOTECLIENT_PLATFORM	クライアントマシンで実行中のオペレーティングシステムの名前とバージョン。たとえば、“Windows 8.1 Enterprise Edition (WOW 64)”、“iPhone OS 9.2.1”、“Android 6.0”など。
TUX_REMOTECLIENT_MAC	クライアントマシンの MAC アドレス。
TUX_REMOTECLIENT_IP	クライアントから見たクライアントマシンの IP アドレス。
TUX_REMOTECLIENT_LANG	クライアントマシンの GUI で使用される言語: EN、FR、RU、DE、ES、IT、PT、NL、JP、CS（簡体字中国語）、CT（繁体字中国語）、KR（韓国語）。 macOS、iOS、Android の各デバイスでは、OS で使用されている言語が提示されます。ただしサポートされている言語に限ります。サポートされていない場合は、デフォルトで EN になります。
TUX_REMOTECLIENT_MACHINE	クライアントのコンピューター名。たとえば、“Bob's iPad mini 1st generation”、“BobPC”、“Bob's iMac”など。
TUX_REMOTECLIENT_LOGIN	Parallels RAS へのログインに使用されたユーザー名（ドメインを含む）。たとえば、myuser@somedomain など。
TUX_REMOTECLIENT_VERSION	Parallels Client のバージョン。
TUX_REMOTECLIENT_VENDOR	デバイスベンダー名。たとえば、“Asus”、“Apple”、“Google”など。
TUX_REMOTECLIENT_MODEL	デバイスモデル名。たとえば、“Nexus 5”、“iPad2.6”など。

次の 2 つの方法のうちのいずれかを使用して、RAS セッション変数とその値を表示できます。

- ホストサーバーの Windows レジストリを調べる。
- GetRASVariable.exe ユーティリティ（Parallels RAS が提供している）を実行する。

各方法は以下の通りです。

レジストリを調べる

変数を表示するには、`regedit` を実行し、`HKEY_CURRENT_USER\Software\Parallels\Shell\<Session-ID>` に移動します。ここで、<Session-ID> は RAS Console に表示されているセッションの ID です（たとえば、2、3、4 など）。特定のセッションの変数は、セッション ID ノードの下のリストに表示されます。

接続時または切断時に、実際のクライアント構成を反映するために更新されます。変数はセッションの期間中は存在し、セッションが終了するとレジストリから削除されます。

上述の表に示す変数に加えて、セッション ID の下に（文書化されていない）他の変数が表示されることがあります。これらは Parallels RAS 内部での使用のみを目的としているため、無視してください。

GetRASVariable.exe ユーティリティの使用

GetRASVariable.exe ユーティリティは、Parallels RAS インストールフォルダー（C:\Program Files (x86)\Parallels\ApplicationServer など）にあります。変数の値を取得するには、パラメーターとして変数名を渡してコマンドラインからユーティリティを実行します（上述の表を参照してください）。このユーティリティは値を画面に出力します。

次の例に TUX_REMOTECLIENT_MACHINE 変数の値を示します。

```
GetRASVariable.exe TUX_REMOTECLIENT_MACHINE
```

メンテナンスとバックアップ

Parallels RAS を最新状態に保つ

デフォルトでは、Parallels RAS は、RAS Console が起動されるたびにアップデートがないかどうかを確認します。この動作を変更したい場合、次の操作を実行します。

1. [管理] カテゴリーを選択し、[設定] タブをクリックします。
2. ニーズに合わせて、[Parallels RAS Console の立上げ時にアップデートをチェックする] オプションを選択するか消去します。
3. 必要に応じて、[RAS RD セッションホスト Agent を自動でアップデート] オプションを選択するか消去します。
4. アップデートがないかどうかを手動で確認するには、[すぐにチェック] ボタンをクリックします。

Parallels RAS ファーム構成のバックアップ

Parallels RAS のファーム構成をバックアップするには、次の操作を実行します。

1 [管理] カテゴリーを選択し、[設定] タブをクリックします。

2 [エクスポート設定] ボタンをクリックします。

3 すべてのサイトを同期することを通知するメッセージが表示されます。エクスポートを続行するには [はい] をクリックし、中止するには [いいえ] をクリックします。

4 ファイル名とエクスポート先のフォルダーを指定し、[保存] をクリックします。

注: エクスポート手順では Parallels RAS ファームの構成データをエクスポートするだけです。ダウンロードされた OS など、関連のないオブジェクトはエクスポートファイルに含まれません。

Parallels RAS ファームの構成をバックアップファイルから復元するには、[インポート設定] ボタンをクリックして、バックアップファイル（デフォルトのファイル拡張子は `.dat2` です）を選択します。ファイルから構成をインポートすると、既存のファーム構成はインポートされた構成に完全に置換されます。

Parallels RAS ファームの構成をコマンドラインからエクスポートおよびインポートすることも可能です。詳細な手順については、これから詳しく説明します。

コマンドラインからのファーム設定のエクスポートおよびインポート

Parallels RAS PowerShell を使用すると、Parallels RAS の管理タスクの大部分をコマンドラインから実行できます。

このセクションでは、PowerShell を使用したファーム設定のエクスポートおよびインポートについて説明します。Parallels RAS PowerShell の詳細については、https://www.parallels.com/products/ras/resources/ にアクセスして、「Parallels RAS PowerShell Guide」をダウンロード（またはオンラインで参照）してください。

ファーム設定のエクスポートおよびインポートの使用法の 1 つとして、自動化テストを実行できます。個別の設定を作成し、エクスポートした後、インポートすることで、特定のテストシナリオでその設定を使用できます。この機能を Windows タスクスケジューラーと併用して、ファーム設定の定期的なバックアップを行うこともできます。

Parallels RAS PowerShell のインストール

Parallels RAS のデフォルトインストールを実行すると、RAS PowerShell はデフォルトでインストールされます。RAS PowerShell をまだインストールしていない場合は（または、別のコンピューターにインストールしている場合は）、次の操作を実行します。

1 Parallels RAS インストーラーを実行します。

2 [カスタム] を選択し、[Parallels RAS PowerShell] コンポーネントを選択します。

3 ウィザードを実行し、Parallels RAS PowerShell をインストールします。

Parallels RAS PowerShell の使用

Parallels RAS PowerShell の最新情報はすべて、「Parallels RAS PowerShell Guide」で確認できます。このガイドには、「スタートアップ」の章が含まれ、Parallels RAS PowerShell を手軽に始めるために役に立つだけでなく、完全なリファレンスおよびコードサンプルとしても利用できます。このガイドを参照またはダウンロードするには、https://www.parallels.com/products/ras/resources/ にアクセスしてください。

以下の手順に従って、Parallels RAS ファーム設定をエクスポートおよびインポートします。

Parallels RAS PowerShell モジュールをインポートするには、PowerShell コンソールを開き、次のコマンドを実行します。

```
Import-Module PSAdmin
```

Parallels RAS セッションを作成します（Parallels RAS をインストールしたサーバーの名前または IP アドレスを使用します）。

```
New-RASSession -Server "server.company.dom"
```

ファーム設定をエクスポートするには、次のコマンドを実行します（バックアップファイルのパスおよびファイル名を独自の値で置き換えます）。

```
Invoke-RASExportSettings "C:\Backup\RAS-backup.dat2"
```

ファーム設定をインポートするには、次のコマンドを実行します。

```
Invoke-RASImportSettings "C:\Backup\RAS-backup.dat2"
```

問題の報告とトラブルシューティング

Parallels RAS で問題が発生した場合は、RAS Console ですぐに解決策を検索できます。解決策を見つけられない場合は、Parallels にサポートリクエストを送信できます。このセクションでは、これらの作業をどのようにして行うかを説明します。

解決策を検索

RAS Console で解決策を検索するには、次の操作を実行します。

1. RAS Console のメインメニューで [ヘルプ] をクリックし、[トラブルシューティングおよびサポートのリクエスト] を選択します。
2. [トラブルシューティング] ダイアログが開きます。
3. [カテゴリーを選択] ドロップダウンリストで、発生している問題のカテゴリーを選択します。ダイアログの中央のエリアに、選択したカテゴリーに関連する KB 記事のリストが自動的に読み込まれます。
4. 興味のある記事をクリックして、ウェブブラウザーでお読みください。
5. [ナレッジベースインデックス] リンクまたは [フォーラム] リンクをクリックして、Parallels のナレッジベースまたは Parallels のフォーラムに移動することもできます。

サポートリクエスト

上述のオプションを使用して問題の解決策を見つけられない場合は、Parallels にサポートリクエストを送信できます。そうすると、収集したロギング情報が取得されてメールに添付されるため、Parallels Support で分析することができます。詳細については、「ロギング」（p. 608）を参照してください。

注: サポートリクエストによってサポートチケットが作成されます。このチケットは Parallels サポートに送信されます。サポートリクエストチケットをすでにお持ちの場合は、追加のチケット（または同じチケット）を作成せずに、システムレポートのみを Parallels に送信してください。以下の「レポートの送信」サブセクションを参照してください。有効な RAS サブスクリプションまたはサポート契約がない場合は、チケットは作成されません。サポートを受けるには、サブスクリプション、またはサポート契約を購入する必要があります。

サポートリクエストを送信する前に、RAS Console 内にメールボックスが設定されていることを確認してください。メールボックスを設定していない場合は、次の手順に従って設定してください。

1. RAS Console で [管理] > [メールボックス] に移動します。
2. 送信メールサーバーの情報、メールアドレス、また、必要に応じてセキュリティ/認証情報を入力してください。
3. テストメール用のフィールドにメールアドレスを入力して、[テストメール送信] をクリックすると、テストメールを送信できます。

Parallels にサポートリクエストを送信するには、次の操作を実行します。

1 [トラブルシューティング] ダイアログで、[サポートリクエストを送信] ボタンをクリックします。

2 [サポートに問い合わせ] ダイアログが開きます。

3 あなたのフルネームと企業名を入力してください。

4 件名を入力してください。これは、Parallels サポートに送信されるメールの件名に使用されます。

5 [クエリーの入力] ボックスに、できるだけ詳細に問題を説明してください。

6 ファイルをメールに添付するには、[添付] フィールドを使用してください。ファイルを参照するには、[...] ボタンをクリックします。Parallels サポートが解決策を見つけるのに役立つ、画像やその他のファイルを添付することができます。ログファイルと Parallels RAS の設定は収集され、自動的にメールに添付されるため、ユーザーがこの操作を行う必要はありません。

7 ダイアログの一番下のドロップダウンリストで、メールを送信するか、収集されたデータを自動的に含む zip ファイルとして保存するかのどちらかを選択できます。

8 前の手順で選択したアクションに応じて、[送信] をクリックしてメールを送信するか、[保存] をクリックしてローカルドライブ、またはネットワークフォルダーに zip ファイルを保存します。

レポートの送信

サポートリクエストチケットをすでにお持ちの場合は、（新しい）チケットを作成せずに、システムレポートのみを Parallels に送信してください。

レポートを送信するには、次の操作を実行します。

1 RAS Console のメインメニューで [ヘルプ] をクリックし、[システムレポートを Parallels にアップロード] を選択します。

2 ダイアログが開き、進行状況バーが表示されます。

3 システムレポートデータが収集されて Parallels に送信されると、メッセージボックスが表示され、レポート番号を確認できます。

4 [OK] をクリックして完了します。

ログ

Parallels RAS コンポーネントはモニタリングされており、関連情報を含むログが作成されます。ログは、Parallels RAS サポートエンジニアが、Parallels RAS インストールで起こる可能性のある問題を分析するために使用します。Parallels RAS 管理者は、特定のコンポーネントまたは複数のコンポーネント向けにログレベルを設定することができます。デフォルトでは標準のログレベルが使用されます。このログレベルでは、重要な情報のみが収集されて保存されます。Parallels RAS サポートエンジニアが、問題を分析するために追加情報が必要なときに、拡張ログレベルまたは詳細ログレベルの有効をユーザーに依頼することがあります。

特定のコンポーネントまたはサーバーのログレベルを設定するには、そのタイプのコンポーネント（RD セッションホスト、VDI、ゲートウェイ、Connection Broker など）が表示されている RAS Console のページに移動し、コンポーネントを選択して、[タスク]（または右クリック） > [トラブルシューティング] > [ロギング] > [構成] をクリックします。[ログレベルを設定] ダイアログが開きます。このダイアログで、次の選択肢からログレベルを選択できます。

- 標準 - 最も重要なイベントのみを記録する標準のログレベルです。後述のいずれかのログレベルを使用するように Parallels RAS サポートから指定された場合以外は、常にこのレベルを使用してください。
- 拡張 - このログレベルでは、標準ロギングよりも多くの情報が含まれます。ただし、収集する必要のある情報が増加するため、システムの速度が低下します。
- 詳細 - 詳細ロギングには拡張ロギングよりも多くの情報が含まれるため、システムの速度が大幅に低下する可能性があります。

パフォーマンスの低下を回避するには、拡張ロギングと詳細ロギングを（分析のために必要な情報を収集する上で十分な）限定的な期間のみ有効にする必要があります。この期間は [後で標準レベルにリセット] オプションを使用して設定できます。デフォルト値は 12 時間です。場合によっては、Parallels サポートエンジニアが、この期間に別の値を設定するようにアドバイスします。この期間が終了すると、ログレベルがリセットされて標準に戻ります。

ログファイルが格納されている ZIP アーカイブを取得するには、[タスク]（または右クリック） > [トラブルシューティング] > [ロギング] > [取得] をクリックし、ファイルを保存する場所を指定します。同じコンテキストメニュー内の [クリア] 項目で、すべてのログがクリアされます。

ログレベルは、[ファーム] > <サイト> > [設定] / [グローバルロギング] タブでも設定できます。ここでは、すべてのタイプの RAS コンポーネントを 1 つのリストに表示できます。詳細については、「サイト設定」（p. 573）を参照してください。

ログローテーション

Parallels RAS ログローテーションは次のように動作します。

1. すべてのログファイルの合計サイズが、定義済みのサイズ（デフォルトは 200 MB）に到達すると、ログがアーカイブされます。アーカイブは、ファイル名の末尾に現在のタイムスタンプを追加し、新しい空のログファイルの使用を開始することで、ログ別に実行されます。
2. 古いログに %logname%_%DATE%.zip という名前が付けられるたびに、新しい ZIP ファイルが作成されます（console_10.06.2018.zip、controller_10.06.2018.zip など）。
3. 名前が変更された古いログは、ZIP ファイルに移動されます。Parallels RAS では、デフォルトで 5 個の ZIP ファイルが保管されます。
4. アーカイブ済みのファイル数の上限を超えると、最も古いファイルが削除されます。
5. このログローテーションの仕組みによって、ログファイルサイズの合計が X * Y * Z MB を決して超えないように保証されています。ここで、X は各ログファイルの合計サイズ（デフォルトは 200 MB）、Y は ZIP ファイル数の上限（デフォルトは 5）、Z は RAS コンポーネントの数です。
6. 上述の例の X と Y の値は、該当の RAS コンポーネントをホストするコンピューター上の Windows レジストリに事前に定義されています。すべての RAS コンポーネントのデフォルト値は同じです。値を変更するには、HKEY_LOCAL_MACHINE > SOFTWARE > Wow6432Node > Parallels に移動して、RAS コンポーネントの LogMaxSize と LogMaxBackups の値を設定します。

お勧めの機能

Parallels RAS の新機能について何かアイデアがありましたら、ぜひご意見をお聞かせください。機能を推薦したい場合は、RAS Console でメインメニューの [ヘルプ] をクリックして、[お勧めの機能] を選択します。これにより、[Parallels RAS のお勧めの機能] に移動し、ご意見やアイデアをお知らせいただくことができます。お勧めの機能フォーラムに投稿するには、Parallels アカウントのメールアドレスおよびパスワードを使ってサインインする必要があります。

第　26　章

Parallels RAS 管理ポータル

この章では、Parallels RAS 管理ポータルの概要を説明します。詳細については、Parallels ウェブサイト（https://www.parallels.com/products/ras/resources/）で利用できる「Parallels RAS 管理ポータルガイド」をお読みください。

この章の内容

概要

Parallels® RAS 管理ポータルは、デスクトップ/ラップトップコンピューターまたはモバイルデバイスを使用して構成と日常のアクティビティを実行する Parallels RAS 管理者向けに設計された、最新のウェブベースの構成および管理コンソールです。

Parallels RAS 管理ポータルは、管理者に次の機能を提供します。

- 重要な Parallels RAS コンポーネント（RD セッションホスト、Connection Broker、Secure Gateway など）を一元的に展開、管理、および構成します。
- RD セッションホストからさまざまなリソースを公開します。
- FSLogix プロファイルコンテナーの設定を構成します。
- 印刷とスキャンの設定を構成します。
- SSL 証明書を管理します。
- 接続設定と MFA（Google 認証または Microsoft 認証などの他の時間ベースのワンタイムパスワード（TOTP）アプリ）を構成します。
- ユーザーセッションを監視および管理します。

- 管理者アカウントとセッションを管理します。
- メールボックスを構成します。
- ライセンスを管理します。
- サポートに連絡し、必要なシステムレポートを提供してください。

注: デスクトップベースの Parallels RAS Console で現在利用可能な多くの機能は、本ツールが Parallels RAS のメイン管理ツールとして採用されるようになる前に、今後のリリースで管理ポータルに含められる予定です。

Parallels RAS 管理ポータルに含まれる Azure Virtual Desktop の管理機能は実験的なものであり、今後のバージョンでリリースされる予定です。

前提条件

RAS 管理ポータルは HTML5 をサポートする最新の Web ブラウザー（Internet Explorer 以外）で動作させることができます。

Windows サーバーに次のアップデートがインストールされていることを確認してください（RAS 管理ポータルはアップデートに依存します）。

- Windows Server 2012 R2: KB2999226

新しいバージョンの Windows Server では特定のアップデートは必要ありません。

このウェブサービスは、デフォルトで次のポートでウェブリクエストをリッスンします。

- HTTPS: 20443
- HTTP: 20080

インストール

RAS ファームで RAS 管理ポータルを有効にするには、RAS ウェブ管理サービスコンポーネントをインストールする必要があります。このコンポーネントは、”標準”インストールオプションを使用して Parallels RAS をクリーンインストールすると自動的にインストールされます。また、”カスタム”インストールオプションを使用して、インストールするコンポーネントに”RAS ウェブ管理サービス”を選択して、インストールすることもできます。たとえば、RAS 管理ポータルを専用マシンにインストールしたい場合は、”カスタム”インストールオプ

ションを使用し、インストールするコンポーネントとして”RAS ウェブ管理サービス”を選択します。

RAS ウェブ管理サービスをインストールした後、設定を行う必要があります。つまり、RAS 管理ポータルで管理する RAS ファームを指定したり、いくつかのパラメーターを設定したりする必要があります。詳しい説明については、「RAS ウェブ管理サービスの構成」（p. 612）を参照してください。

RAS 管理ポータルへのログイン

RAS ウェブ管理サービスをインストールしたマシンで RAS 管理ポータルを開くには、[アプリ] > [Parallels] に移動し、[Parallels RAS 管理ポータル] をクリックします。

リモートコンピューターから RAS 管理ポータルにログインするには、ウェブブラウザーに以下の URL を入力します:

```
https://<server-address>:20443
```

<server-address> は、RAS ウェブ管理サービスがインストールされているサーバーの FQDN または IP アドレスです。デフォルトでは、HTTPS 接続にはポート 20443 が使用されます。「RAS ウェブ管理サービスの設定」（p. 612）で説明されているように、必要に応じてポート番号を変更することができます。

[ようこそ] ページで、RAS 管理者のユーザー名とパスワードを入力し、[サインイン] をクリックします。

RAS ウェブ管理サービスの構成

最初に、以下のように RAS ウェブ管理サービスを構成する必要があります。

1. RAS 管理ポータルで、右上の [ユーザー] アイコンをクリックし、[管理ポータルの構成] を選択します。
2. 再度サインインを求められます。なお正常にサインインするためには、RAS ウェブ管理サービスがローカルサーバー上で稼働している必要があります。これは、リモートサーバーのユーザーが RAS ウェブ管理サービスの構成ページアクセスするのを防ぐためです。

3 ローカル管理者またはドメイン管理者のメンバーのユーザー名とパスワードを入力し、 [サインイン] をクリックします。

4 [RAS 管理ポータルの構成] ページが開きます。

5 [RAS ファームアドレス] フィールドに、この RAS 管理ポータルで管理する RAS ファームのアドレスを指定します。これは、ファームにインストールされている RAS Connection Broker のアドレスです。

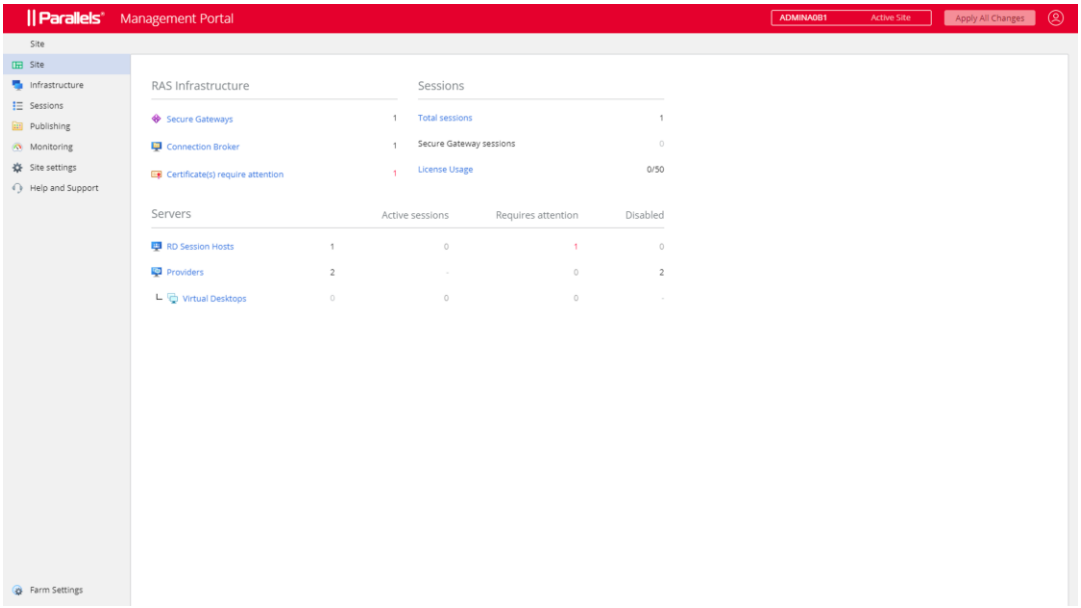
6 [詳細設定] セクションで以下を指定します。

- 証明書：この接続に使用する証明書です。[アップロード] をクリックして、証明書を選択します。
- 証明書のパスワード: 証明書のパスワードです。
- ポート: RAS 管理ポータルが接続を待機するポート番号です。デフォルトのポートは 20443 です。この番号は、RAS Secure Gateway ポートと競合しないように設定されています。可能であれば 443 に変更することもできます。その場合、接続 URL にポート番号を含める必要はありません。また、任意のカスタムポートに変更することも可能です。たとえば、デフォルトの”URL”：”https://*:20443”を”URL”：”http://*:20080”に変更できます。
- 管理セッションのタイムアウト: 管理者セッションが切断されるまでの時間です。
- ポーリング間隔: RAS 管理ポータルで表示されている情報を更新する間隔です。多数の管理者が同時に作業している場合や、多数のホストまたセッションなどが存在する場合は、この値を最大 30 秒まで増やすことができます。

7 完了したら、[保存] をクリックします。

RAS 管理ポータルのユーザーインターフェイス

RAS 管理ポータルのすべてのナビゲーションは、管理カテゴリーをリストアップした左のサイドバーから開始します。デフォルトではサイトカテゴリーが選択されています。



カテゴリー

次の表は、RAS 管理ポータルで管理できる、利用可能なすべてのカテゴリーの一覧です。ルート管理者は、すべてのカテゴリーを閲覧および管理することができます。他の種類（上級、カスタム）の管理者は、特定のカテゴリーを閲覧するのに権限が必要になる場合があります。

カテゴリー	説明
サイト	現在のサイト概要を表示します。
インフラ	RD セッションホスト、VDI、Gateway、Connection Broker などの RAS インフラストラクチャの管理。
セッション	セッション管理。
公開	公開リソースおよび公開済みリソースの管理。
監視	RAS Performance Monitor

サイト設定	接続、認証、FSLogix、ユニバーサルプリント、スキャン。
ヘルプとサポート	ヘルプとサポート。
ファーム設定	左側のサイドバーの下部に表示されるこのカテゴリーでは、管理者、メールボックス、ライセンスなど、ファームのグローバルな設定を管理します。

各カテゴリーについては、このガイドの後半で詳しく説明します。

管理権限

デスクトップの RAS Console で構成された管理者権限によっては、RAS 管理ポータルの一部のカテゴリーや処理が表示されない、または許可されない場合があります。管理者権限の設定方法については、「Parallels RAS 管理者ガイド」を参照してください。このガイドでは、「管理者アカウントの権限」のトピックを探します。このガイドは、Parallels のウェブサイト（https://www.parallels.com/products/ras/resources/）でご覧いただけます。

サブカテゴリー

一部のカテゴリーにはサブカテゴリーがあります（インフラストラクチャおよびサイト設定）。カテゴリーを選択すると、RAS 管理ポータルの右側に、サブカテゴリーを選択できる 1 つまたは複数の追加ペインが表示されることがあります。

ナビゲーションバー

一部のコンポーネントでは、設定や情報が機能ごとにまとめられています（概要、プロパティ、セッションなど）。コンポーネントのプロパティを表示すると、中央にナビゲーションバーが表示され、これらの設定を参照することができます。ナビゲーションバーで項目を選択すると、その設定内容が右側ペインに表示されます。

ブレッドクラム

カテゴリー、サブカテゴリー、個別の項目を選択すると、ページ上部にブレッドクラムが表示され、現在の位置がわかります。1 ステップ以上戻るには、リストのリンクをクリックします。

ページのヘッダー項目

ページのヘッダーには以下の項目があります:

- ファームと現在のサイトの名前。複数のサイトがある場合は、ドロップダウンリストから選択することができます。RAS 管理ポータルがそのサイトに切り替わり、サイトのコンポーネントを管理できるようになります。
- ”ユーザー”アイコンはドロップダウンリストになっており、以下の項目があります。現在のユーザー名（例: Administrator）、詳細（[詳細] ダイアログを開く）、フィードバックを行う（Parallels にフィードバックを行うウェブページに移動する）、管理ポータルの構成（p. 612）、ログアウト（ログアウトする）。
- すべての変更を適用: このボタンで、RAS 管理ポータルで行った変更をファームのコンポーネントに適用します。コンポーネントやオブジェクトを作成したり変更したりしても、その変更がファームのコンポーネントに自動的に適用されることはなく、サイトやファームに影響を与えることもありません。[すべての変更を適用] ボタンをクリックすると、ファームやサイト全体に変更が適用されます。なお、変更のたびにこのボタンをクリックする必要はありません。異なる領域で複数の変更を必要とする作業を行っている場合は、すべての変更を完了してから [すべての変更を適用] ボタンをクリックすると、すべての変更がまとめて適用されます。

編集

いずれかの設定を変更できるビューを開いたとき、そのビューは通常、読み取り専用になります。編集を有効にするには、右上の [編集] ボタンをクリックします。ボタン名が [保存] に変わります。編集が終わったら、[保存] をクリックします。変更内容を破棄する場合は、[キャンセル] をクリックします。

なお、ある管理者が編集可能な状態にしたオブジェクトは、他の管理者が同時に編集することはできませんのでご注意ください。このようなオブジェクトの編集を有効にしようとすると、エラーが発生して、オブジェクトをロックしている管理者の名前が表示されます。

編集ツールバー

一部のビュー（特にリスト）では、右上にツールバーがあり、そこから処理を実行することができます。ツールバーの項目名を見るには、マウスでその項目にカーソルを合わせます。ツールバーの標準的な項目（アイコン）は以下の通りです:

- フィルターを表示: フィルターを指定すると、条件を満たすエントリーのみが表示されます。
- 列を選択: テーブルの列を選択して、表示/非表示を切り替えます。

- 追加: 新しいエントリーを追加します。たとえば、新しいゲートウェイや RD セッションホストを追加できます。
- 更新: 表示を更新します。
- 省略: 省略メニューは、ビューの種類によって項目が異なります。一部の項目には、対応するツールバー項目が表示されます（例: 追加、更新）。

またビューによっては、[実行中のプロセスを表示] や [セッションを表示] など、他の項目も表示されます。

ウィザード

ファームにコンポーネントを追加すると、通常はウィザードが開き、コンポーネントの設定やオプションを指定する一連のページが表示されます。ウィザードには、通常の [次へ] と [戻る] のナビゲーションボタンと、ウィザードを閉じて操作を取り消すことのできる [キャンセル] ボタンがあります。

モーダルダイアログ

メニューやナビゲーションバーの項目をクリックすると、モーダルダイアログが表示されます。通常、これらの項目では、処理の確認や追加情報の入力が必要となります。

オブジェクトのプロパティ表示

RAS 管理ポータルのすべてのオブジェクト（コンポーネント）には、プロパティがあります。これらのプロパティを表示するには、カテゴリーとサブカテゴリーを選択し、リスト内のオブジェクト名をクリックします。これにより、オブジェクトのプロパティが表示され、独自のナビゲーションバーを利用できるようなります。そこからオブジェクトの構成、処理の実行、追加情報の表示が可能になります。

第 27 章

Parallels RAS の API

Parallels RAS には複数の API があり、これにより API が統合されたカスタムアプリケーションを開発できます。これには RAS PowerShell API と RAS REST API が含まれます。

さらに、RAS Web Client API および Parallels Client の URL スキームを使用すると、Parallels Client for Windows/macOS/Linux/iOS/Android および Web Client との統合が可能です。

この章の内容

RAS PowerShell API

RAS PowerShell API は、RAS 管理業務の自動化を望む RAS 管理者を想定しています。この API には、RAS 管理タスクを実行するための多くのコマンドが含まれます。

Parallels RAS の要件

Parallels RAS PowerShell API のバージョンは、通信対象である RAS Connection Broker のバージョンと一致する必要があります。この 2 つのコンポーネントは別々にインストールできるため、これらのバージョンが一致していることを確認する必要があります。

Microsoft Windows コンポーネントの要件

次のコンポーネントが、Parallels RAS PowerShell コマンドレットを実行するコンピューターにインストールされている必要があります。

- Windows PowerShell 3.0 以降
- Microsoft .NET Framework 4.5.2 以降

インストール

Parallels RAS PowerShell をインストールするには、Parallels RAS の標準インストーラーを実行し、[カスタム] インストールを選択して、[Parallels RAS PowerShell] コンポーネントのインストールを選択します。画面の指示に従い、コンポーネントをインストールします。

RAS PowerShell API のバージョン

Parallels RAS 18 では、RAS PowerShell API が次のように変更されています。

- RAS PowerShell モジュール名が PSAdmin から RASAdmin に変更されました。
- ほとんどのコマンドには、RASGW や RASApply などの”RAS”プレフィックスが付記されるようになりました。
- API のバージョン: バージョン 2.0（最新）とバージョン 1.0 は、下位互換性を確保するためにサポートされています。

現在の RAS PowerShell モジュールでは、API バージョン 1.0 が引き続き使用できることに注意してください。古いモジュール名とコマンド名を使用する既存のスクリプトが存在する場合、最小限の変更でそれらを使用できます。これを行うには、RAS PowerShell モジュールをインポートするときに API バージョン 1.0 を読み込む必要があります。API バージョンの詳細については、以下を参照してください。

バージョン 2.0

このバージョンは、デフォルトでシステムによって読み込まれます。また、モジュールをインポートするときに、`-RequiredVersion` パラメーターが指定されていない場合も読み込まれます。「RAS PowerShell API の基本概念」の例を参照してください。

バージョン 1.0

このバージョンでは、古い PSAdmin モジュールとの下位互換性が維持されており、管理者が小さな変更を加えることで既存のスクリプトを使用できるようにします。このバージョンには次のものが含まれます。

- コマンドレットエイリアス
- エイリアスのパラメーター
- 古いプロパティと新しいプロパティの返還

RAS PowerShell API の概念

RAS PowerShell を手軽に始めるには、次の手順を実行します。

1 Windows PowerShell コンソールを開きます。

2 次のいずれかのコマンドを使用して、Parallels RAS PowerShell モジュールをインポートします。

- `Import-Module RASAdmin -`：現在の API（バージョン 2.0）を読み込みます。
- `Import-Module RASAdmin -RequiredVersion 1.0 -`：API（バージョン 1.0）を読み込みます。

3 `New-RASSession` コマンドレット（下の例を参照）を実行して Parallels RAS セッションを作成します。サーバー名（引用符内）は、お使いの Parallels RAS ライセンスサーバーの名前または IP アドレスに置き換えてください。入力を求められたら、RAS 管理者のユーザー名とパスワードを入力します。

```
New-RASSession -Server "server.company.dom"
```

4 次のコマンドレットを実行して、Parallels RAS PowerShell モジュールに含まれるコマンドレットのリストを確認します。

```
Get-Command -Module RASAdmin
```

5 他のコマンドレットを実行します。たとえば、`Get-GW` コマンドレットを実行して RAS Secure Gateway についての情報の取得してみます。下の例は、RAS ライセンスサーバーのサイトで利用できるすべての RAS Secure Gateway についての情報を返します。

```
Get-RASGW
```

6 コマンドレットのヘルプを参照するには、コマンドレット名を渡して `Get-Help` を実行します。

```
Get-Help Get-RASGW
```

7 ファームの構成に行った変更を適用するには、`Invoke-RASApply` コマンドレットを使用します（このコマンドレットでは、RAS Console の [適用] ボタンと同じアクションが実行されます）。

```
Invoke-RASApply
```

8 Parallels RAS ライセンスをアクティベートするには、`Invoke-RASLicenseActivate` コマンドレットを使用します。

```
Invoke-RASLicenseActivate
```

上述のコマンドレットを実行すると、Parallels アカウントのメールアドレスとパスワードの入力を求められます。オプションの `-Key` パラメーターを使用して Parallels RAS のライセンスキーを指定することができます。省略した場合は（上の例を参照）、Parallels RAS はトライアル版としてアクティベートされます。

Parallels RAS PowerShell ガイド

新しい「Parallels RAS PowerShell ガイド」（バージョン 2.0）は、Parallels ウェブサイト（https://www.parallels.com/products/ras/resources）で、確認およびダウンロードしてください。

RAS REST API

このセクションでは、RAS REST API を紹介します。このセクションを読んで、システム要件、インストール、構成、基本的な使用方法について学んでください。

インストール

RAS ファームで RAS REST API を有効にするには、RAS ウェブ管理サービスをインストールする必要があります。RAS Connection Broker サーバーまたはその他のサーバーにインストールできます。別のサーバーにサービスをインストールする場合は、（インストール後に）RAS Connection Broker が正しく指定されるように構成を変更する必要があります。デフォルトの構成では、”localhost”に指定されています。

注: Parallels RAS 管理ポータルをすでに構成して使用している場合は、RAS ウェブ管理サービスがすでにインストールされていると考えられますので、この手順をスキップできます。

RAS ウェブ管理サービスをインストールするには、次の操作を実行します。

1. RAS Connection Broker またはその他のサーバーで、Parallels RAS インストーラーを実行します。
2. [インストールタイプの選択] ページで、[カスタム] を選択します。
3. 次のページで、Parallels RAS ウェブ管理サービスコンポーネントのインストールを選択します。
4. [次へ] をクリックし、画面上の指示に従います。

RAS ウェブ管理サービスの構成

RAS ウェブ管理サービスが別のサーバーにインストールされている場合、サービスの構成を変更し、RAS Connection Broker サーバーのアドレスを指定する必要があります。同じ構成ファイルを使用して、ポート番号と証明書情報を変更することもできます。RAS ウェブ管理サービスの構成の詳細については、ナレッジベースの記事（https://kb.parallels.com/en/124701）を参照してください。

サービス構成を変更する場合は、次の点に注意してください。

- 構成用の JSON ファイルでは、RAS Connection Broker のアドレスが”LicenseServer”パラメーターを使用して指定されます。
- デフォルトでは、HTTPS のポート番号は 20443 に設定されています。この番号は、RAS Secure Gateway ポートと競合しないように設定されています。可能な場合は、443 に変更できます。こうすれば、ポータルを開くときに、URL にポート番号を含める必要はありません。

権限

任意の RAS REST リソースにアクセスするには、リクエストを実行しているユーザーが、特定のリソースにアクセスできる十分な権限を持つ必要があります。これは、基本的に、RAS 管理者が Parallels RAS Console で持っているのと同じ権限です。たとえば、root 管理者は任意の RAS REST リソースにアクセスできます。一方、（一例として）サイト設定を変更する権限を持たない上級管理者は、対応する REST リソースにアクセスできません。同様に、たとえば、RD セッションホストの表示および変更の権限のみを持つカスタム管理者は、特定の REST リソースのみにアクセスでき、それ以外にはアクセスできません。

使用を開始する

アプリケーションは、HTTP または HTTPS リクエストを送信することで、Parallels RAS と通信します。Parallels RAS は、あらゆる HTTP リクエストに対して JSON ファイルを使用して応答します。

Parallels RAS リソースの取得および管理に使用されるすべての HTTP リクエストは、次の基本構造を持ちます。

```
https://<API-host>/api/<URI>
```

上述の URL の各パラメーターは以下の通りです。

- <API-host> は、RAS ウェブ管理サービスがインストールされているサーバーの IP アドレスまたは FQDN です。
- <URI> は、扱う REST リソースのパスです。

ログインおよびリクエストの送信

このセクションでは、手軽に始めるときに役に立つ RAS REST API の使用方法の例を紹介します。例では、次の方法を説明しています。

1. Parallels RAS にログインしてセッショントークンを取得する。
2. 利用できるすべての RD セッションホストについての情報を取得する。
3. 特定の RD セッションホストについての情報を取得する。
4. RD セッションホストプロパティを変更する。

Parallels RAS にログインしてセッショントークンを取得する

任意のリソースにアクセスするには、管理者の資格情報を使用して Parallels RAS にログインし、セッショントークンを取得する必要があります。これを実行するには、次のリクエストを送信します。

```
POST https://<API-host>/api/session/logon
```

リクエストヘッダー: このログオンリクエストには、Content-Type リクエストヘッダーのみを含める必要があります。この後の例で示されるように、後続のリクエストには、さらに auth_token ヘッダーを含める必要があります。

```
Content-Type: application/json; api-version=1.0
```

リクエスト本文: リクエスト本文には、RAS 管理者のユーザー名とパスワードを含める必要があります。

```
{
 "username": "USER",
 "password": "PASSWORD"
}
```

応答: ログオンリクエストの送信後、セッショントークンが含まれる返信を受け取ります。これは、後続のすべてのリクエストで使用します。

```
{
 "authToke            n": "Lj+KddoJkANhzvbDRvB=K=DFCroRjXJHeeWGbGlIRKaz-EXplbmhVWvWTiDVqtOq"
}
```

RD セッションホストについての情報を取得する

セッショントークンを入手したので、さまざまなリソースにアクセスするためのリクエストを送信できるようになりました。この例では、まず、利用できるすべての RD セッションホストについての情報を取得します。この後の例で、特定の RD セッションホストについての情報を取得します。

RD セッションホスト情報を取得するには、次のリクエストを送信します。

```
GET https://<API-host>/api/RDS
```

リクエストヘッダー: 今回は、auth_token リクエストヘッダーも含まれ、ここに、事前に取得したセッショントークンが含まれている必要があります。

Content-Type: application/json; api-version=1.0

auth_token:
Lj+KddoJkANhzvbDRvB=K=DFCroRjXJHeeWGbGlIRKaz-EXplbmhVWvWTiDVqtOq

応答: 応答は次のようになります(ファーム内の複数の RD セッションホストを使用すると、結果セットの各ブロックに個別のサーバーについての情報が含まれます)。

```
[
    {
        "directAddress": "IP_ADDR",
        "rasTemplateId": 0,
        "inheritDefaultAgentSettings": true,
        "inheritDefaultPrinterSettings": true,
        "inheritDefaultUPDSettings": true,
        "inheritDefaultDesktopAccessSettings": true,
        "port": 3389,
```

```
            …
            "restrictDesktopAccess": false,
            "restrictedUsers": [],
            "server": "IP_ADDR",
            "enabled": true,
            "description": "",
            "siteId": 1,
            "id": 2
        }
]
```


特定の RD セッションホストについての情報を取得する

特定のサーバーについての情報を取得するには、上述と同じリクエストを使用しますが、末尾にサーバー ID を追加します。

```
GET https://<API-host>/api/RDS/2/
```

この応答も上述の例と同様になり、特定のサーバーのみの情報が含まれます。

RD セッションホストプロパティを変更する

この例では、事前に取得した RD セッションホストのプロパティを変更します。わかりやすくするため、[説明] フィールドを変更します。

RD セッションホストのプロパティを変更するリクエストの構文は次のようになります。

```
PUT https://<API-host>/api/RDS/2/
```

リクエストの末尾に“2”が付いていますが、これは、変更する RD セッションホストの ID を指定しています。

リクエストヘッダー:

- Content-Type: application/json; api-version=1.0
- auth_token: Lj+KddoJkANhzvbDRvB=K=DFCroRjXJHeeWGbGlIRKaz-EXplbmhVWvWTiDVqtOq

リクエスト本文:

```
{
    "description": "description was updated!"
}
```

応答: PUT リクエストが成功すると、空の応答と、コード“204: No Content”を受け取ります。[説明] フィールドが実際に変更されたかどうかを確認するには、以前に使用したのと同じ GET リクエストを使用します。GET https://<API-host>/api/RDS/2/

ご覧のように、結果に更新された [説明] フィールドが含まれるようになりました。

```
[
    {
        "directAddress": "IP_ADDR",
        "rasTemplateId": 0,
        "inheritDefaultAgentSettings": true,
        …
        "server": "IP_ADDR",
        "enabled": true,
        "description": "description was updated!",
        "siteId": 1,
        "id": 2
    }
]
```

詳細情報

Parallels RAS REST API には「Parallels RAS REST API ガイド」が付属しています。このガイドには、より多くの例と、リソースおよびスキーマの完全なリファレンスが含まれています。ガイドの閲覧やダウンロードを行うには、https://www.parallels.com/products/ras/resources/ にアクセスしてください。

RAS Web Client API および Parallels Client の URL スキーム

RAS Web Client API および Parallels Client の URL スキームを使用すると、Parallels Client と統合することができます。

RAS Web Client API または URL スキームを使用すると、アプリケーションハブやウェブポータルなどの社内ソリューションを実装して、ユーザーを認証したり、リモートアプリケーション、デスクトップやその他の公開リソースを起動したりすることができます。このような実装は、サポート対象プラットフォーム（Windows、macOS、Linux、iOS、Android）向けの Parallels Client および RAS Web Client を含む Parallels Client とカスタムソリューションを統合することで可能になります。

以下でこの API および URL スキームを簡単に説明します。

- RAS Web Client API - Web Client を介してウェブブラウザーから呼び出す、接続、ユーザー認証、リソース起動の手法を提供しています。
- Parallels Client の URL スキーム - ユーザーデバイスにインストールされている Parallels Client でアクションを実行できるようにするカスタム URL スキームです。アクションには、接続の構成、ユーザーの認証、公開リソースの起動などが含まれます。

RAS Web Client API および Parallels Client の URL スキームの詳細については、「Parallels Clients との統合」ガイドに記載されています。このガイドは Parallels ウェブサイトからダウンロードできます: https://www.parallels.com/products/ras/resources/。

第　２８　章

付録

この章の内容

Parallels RAS の Microsoft ライセンスの要件

このセクションは、Parallels RAS 環境での Microsoft ライセンス要件を明確にするためのガイダンスとして使用されます。除外リストとしては使用することは意図されていません。詳細については、Microsoft のライセンスパートナーにお問い合わせください。

Microsoft ライセンスの要件には以下の内容が含まれます。

一般

- 使用されるいずれかの Windows Server およびデスクトップオペレーティングシステム（OS）。
- アクセスされる Windows Server OS は、Microsoft Windows Server クライアントアクセスライセンス（CAL）の対象である必要があります。

RD セッションホスト

Windows Server にリモートでアクセスする場合（管理以外の作業の場合）、リモートデスクトップサービス（RDS）のアクセス用ライセンスが必要です。

- Windows Server でリモートデスクトップサービス機能を利用するユーザーまたはデバイスには、RDS CAL が必要となります。次の種類の RDS CAL を使用できます。
  a. RDS デバイス CAL: 1 台のデバイス（任意のユーザーが使用）が、任意のサーバーでリモートデスクトップサービス機能を使用することを許可します。

b RDS ユーザー CAL: 1 ユーザー（任意のデバイスを使用）が、任意のサーバーでリモートデスクトップサービス機能を使用することを許可します。

c RDS 外部コネクター: 複数の外部ユーザーが、単一のリモートデスクトップサーバーにアクセスすることを許可します。複数のサーバーが存在する場合は、必須の Windows Server 外部コネクターに加えて、複数の外部コネクターが必要となります。

サーバーソフトウェアでは、RDS デバイス CAL と RDS ユーザー CAL を組み合わせて使用することもできます。この場合、RDS ユーザー CAL または RDS デバイス CAL に加えて、通常のユーザーまたはデバイス CAL が必要となります。

- RDS SAL は、コンピューティングリソースで作成された仮想マシンに対し、Microsoft リモートデスクトップサービスのサブスクライバーアクセスライセンス（「RDS SAL」と呼ばれる）を提供するサービスです。これにより、3 人以上のユーザーがコンピューティングリソース内に存在する特定の仮想マシンのリモートデスクトップ（RD セッションホスト）に接続できるようになります（SPLA パートナーの場合）。

さらに詳しく:

- 「クライアントアクセスライセンス（CAL）を使用して RDS 展開をライセンスする」: https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/rds-client-access-license。
- RDS ライセンスデータシート（ https://download.microsoft.com/download/6/B/A/6BA3215A-C8B5-4AD1-AA8E-6C93606A4CFB/Windows_Server_2012_R2_Remote_Desktop_Services_Licensing_Datasheet.pdf）。
- RDS CAL の概要と FAQ（ https://download.microsoft.com/download/3/D/4/3D42BDC2-6725-4B29-B75A-A5B04179958B/Licensing-Windows-Server-2012-R2-RDS-and-Desktop-Apps-for-RDS.pdf）。
- Windows Server RDS による Microsoft デスクトップアプリケーションソフトウェアの使用（ https://download.microsoft.com/download/3/d/4/3d42bdc2-6725-4b29-b75a-a5b04179958b/desktop_application_with_windows_server_remote_desktop_services.pdf）。

ハイパーバイザーと VDI

1 Microsoft Hyper-V をハイパーバイザーとして使用する場合は、Microsoft Windows Server オペレーティングシステム（OS）のライセンスが必要です

さらに詳しく:

- Windows Server 2022 ライセンスデータシート（https://www.microsoft.com/en-us/windows-server/pricing）。
- Windows Server 2019 ライセンスデータシート（https://download.microsoft.com/download/7/C/E/7CED6910-C7B2-4196-8C55-208EE0B427E2/Windows_Server_2019_licensing_datasheet_EN_US.pdf）。
- Windows Server 2016 ライセンスデータシート（https://download.microsoft.com/download/7/2/9/7290EA05-DC56-4BED-9400-138C5701F174/WS2016LicensingDatasheet.pdf）。

2 仮想デスクトップインフラストラクチャ（VDI）を使用する場合は、Windows ソフトウェアアシュアランスまたは Azure Virtual Desktop アクセス（VDA）ライセンスが必要です。Microsoft は、アクセスデバイスごとに Windows ライセンスを付与します。

- 仮想デスクトップのアクセス権は、Windows クライアントソフトウェアアシュアランス（SA）の利点です。SA の対象となる PC を使用するカスタマーは、追加料金なしで VDI デスクトップにアクセスできます。
- シンクライアントなど、Windows クライアント SA の対象とならないデバイスを使用する場合は、Windows VDI デスクトップにアクセスするために、それらのデバイスに Azure Virtual Desktop アクセス（VDA）のライセンスを付与する必要があります。Windows VDA は、業務委託先や従業員が所有する PC などのサードパーティデバイスにも適用できます。

さらに詳しく:

- Windows 11 ライセンスポータル（https://www.microsoft.com/en-us/Licensing/product-licensing/windows）。
- Windows 10 ライセンスポータル（https://www.microsoft.com/ja-jp/licensing/product-licensing/windows10?activetab=windows10-pivot:primaryr3）。
- 仮想マシンで Windows デスクトップオペレーティングシステムを使用するためのライセンス（https://download.microsoft.com/download/9/8/d/98d6a56c-4d79-40f4-8462-da3ecba2dc2c/licensing_windows_desktop_os_for_virtual_machines.pdf）。
- VDI 環境向け Windows デスクトップのライセンス（https://docs.microsoft.com/en-us/answers/storage/temp/12620-microsoft-vdi-and-vda-faq-v3-0.pdf）。

Microsoft Azure

Microsoft 365 や Microsoft Azure などの Microsoft Online ビジネスサービスでは、サインインのために、また ID 保護によってサポートを提供するために、Microsoft Entra ID が必要です。Microsoft Online ビジネスサービスのサブスクリプションを入手すると、すべての無料機能にアクセスできる Microsoft Entra ID が自動的に取得されます。Microsoft Entra ID の実装を強化するために、Microsoft Entra ID プレミアム P1 またはプレミアム P2 ライセンスにアップグレードして、有料機能を追加することもできます。

さらに詳しく:

- Microsoft Entra ID の実装
  https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis
- Azure ハイブリッド特典（https://azure.microsoft.com/ja-jp/pricing/hybrid-benefit/）

Azure Virtual Desktop

- 次のいずれかのユーザーライセンスをお持ちの場合、追加コスト（コンピューティング、ストレージ、およびネットワークのコストを除く）を負担することで、Windows 10 Enterprise マルチセッション、Windows 11 Enterprise マルチセッション、Windows 10 Enterprise、および Windows 11 Enterprise デスクトップ/アプリへのアクセスを利用できるようになります。
  - **a** Microsoft 365 E3/E5
  - **b** Microsoft 365 A3/A5/学生使用特典
  - **c** Microsoft 365 F3
  - **d** Microsoft 365 Business Premium
  - **e** Windows 10 Enterprise E3/E5
  - **f** Windows 10 Education A3/A5
  - **g** Windows 10 VDA（ユーザー単位）
- アクティブなソフトウェアアシュアランス（SA）が付属する、ユーザー単位またはデバイス単位の RDS CAL ライセンスをお持ちの場合、追加費用（コンピューティング、ストレージ、およびネットワークのコストを除く）を負担することで、Windows Server 2012 R2 以降を実行している Windows Server リモートデスクトップサービスを利用したデスクトップへのアクセスを利用できます。

さらに詳しく:

- Azure Virtual Desktop の価格（https://azure.microsoft.com/ja-jp/pricing/details/virtual-desktop/）

FSLogix

次のいずれかのライセンスをお持ちの場合は、FSLogix プロファイルコンテナー、Office 365 コンテナー、アプリケーションマスキング、および Java リダイレクトツールを利用できます。

- Microsoft 365 E3/E5
- Microsoft 365 A3/A5/学生使用特典
- Microsoft 365 F1/F3
- Microsoft 365 Business
- Windows 10 Enterprise E3/E5
- Windows 10 Education A3/A5
- Windows 10 VDA（ユーザー単位）
- リモートデスクトップサービス（RDS）クライアントアクセスライセンス（CAL）
- リモートデスクトップサービス（RDS）サブスクライバーアクセスライセンス（SAL）

FSLogix ソリューションは、ユーザーが適切なライセンスを保持している場合に限り、任意のパブリックまたはプライベートのデータセンターで使用できます。

さらに詳しく:

- FSLogix の概要（https://docs.microsoft.com/en-us/fslogix/overview）。

Microsoft SQL Server

Parallels RAS Reporting を使用する場合は、SQL Server が必要です。SQL Server は、以下に基づいてインストールできます。

- データベースのサイズに 10GB の制限がある無料の SQL Express。
- SQL Server 商用版の Standard または Enterprise（コアベースのライセンスまたはサーバー/CAL ベースのライセンスを使用）。

さらに詳しく:

- SQL Server 2019 ライセンスガイド（https://download.microsoft.com/download/6/6/0/66078040-86d8-4f6e-b0c5-e9919bbcb537/SQL%20Server%202019%20Licensing%20guide.pdf）

App-V

App-V は、単体でライセンスが付与されることはありませんが、他のライセンス契約（Microsoft ボリュームライセンス、Windows ソフトウェアアシュアランス、Microsoft リモートデスクトップサービス（RDS）CAL など）に含まれています。より広範な Microsoft ライセンス契約の一部となります。たとえば、RDS CAL（ユーザー単位またはデバイス単位）では、RD セッションホストで App-V クライアントを使用して、App-V アプリケーションを配信できます。

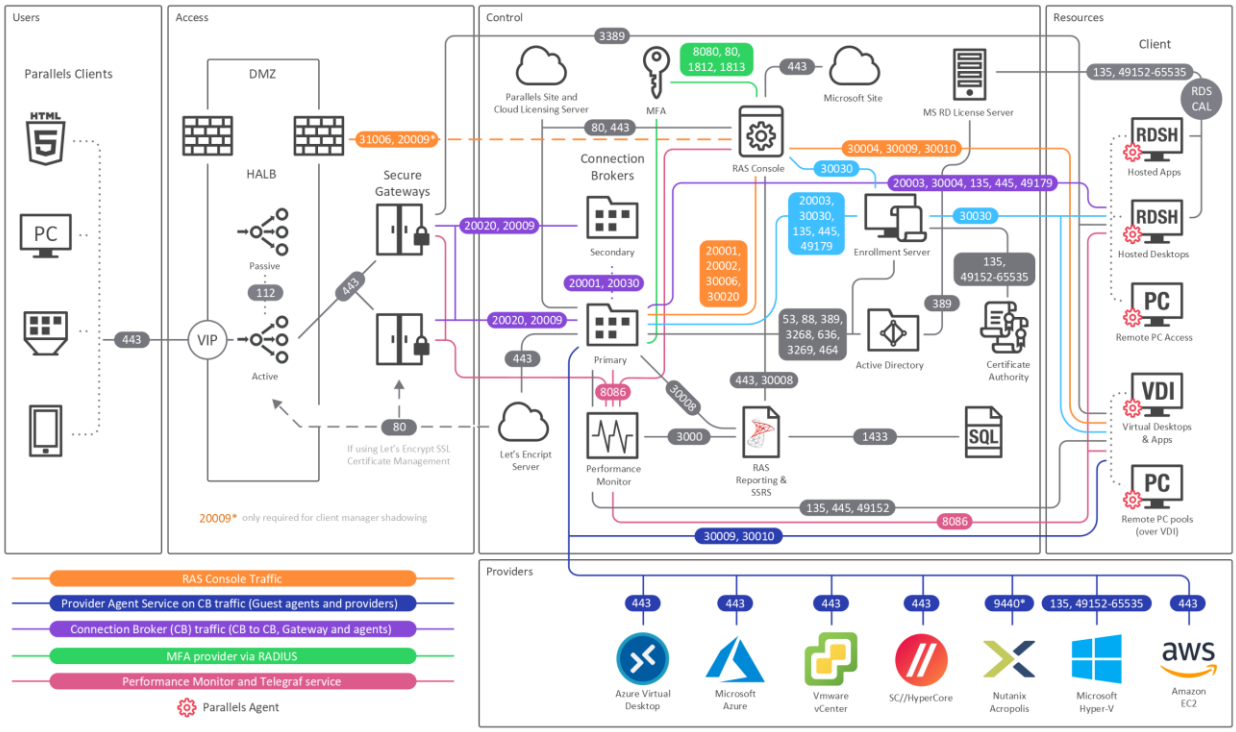
App-V のライセンスを適切に取得するには、Microsoft ボリュームライセンスに精通した Microsoft パートナー（ソリューションプロバイダー）と契約することをお勧めします（Microsoft パートナーのリスト: https://pinpoint.microsoft.com/en-us/search?type=companies&competency=100010）。

他の参照資料

Microsoft ボリュームライセンス製品に使用される用語の詳細なリストについては、https://www.microsoftvolumelicensing.com/Downloader.aspx?documenttype=PT&lang=English を参照してください。

ポート参照

次の図は、Parallels RAS で使用される通信ポートを示しています。



上の図には、RAS 登録サーバーなどの SAML SSO コンポーネントが含まれていますが、テナントブローカーは含まれていません。

ヒント: 本書の PDF 版をご覧の場合、以下のリンクをクリックすると、ウェブブラウザーで原寸大の図が表示されます: https://download.parallels.com/ras/v19/docs/en_US/Parallels-RAS-19-Administrators-Guide/index.htm#47092。

Parallels Client

ソース	宛先	プロトコル	ポート	説明

Parallels Client	HALB	TCP、UDP TCP、UDP	80、443 20009	管理およびユーザーセッション接続 ファイヤウォール経由のデバイスマネージャーのシャドーイング（間接ネットワーク接続）
	転送モードの RAS Secure Gateway	TCP、UDP TCP、UDP UDP	80、443 3389 20000	管理およびユーザーセッション接続 オプション - RDP ロードバランスが有効になっている場合、ユーザーセッションに使用されます（標準 RDP）。 Secure Gateway はブロードキャストを検索します。
	RAS Secure Gateway 通常モード	TCP、UDP TCP、UDP TCP、UDP UDP	80、443、 3389 20009 20000	管理およびユーザーセッション接続 オプション - RDP ロードバランスが有効になっている場合、ユーザーセッションに使用されます（標準 RDP）。 ファイヤウォール経由のデバイスマネージャーのシャドーイング（間接ネットワーク接続） Secure Gateway はブロードキャストを検索します
	セッションホスト（VDI、RDS、RemotePC）	TCP、UDP	3389	ダイレクトモードに限りユーザーセッション接続で使用されます。RDP 接続は常に暗号化。
	Azure Virtual Desktop サービス	TCP UDP	443 3390	Azure Virtual Desktop Gateway 接続 ShortPath モードに限りユーザーセッション接続で使用されます。
	Microsoft サイト	TCP	443	Microsoft リモートデスクトップ（MSRDC）クライアントのダウンロード
	Parallels サイト	TCP	80、443	Parallels Client のアップデートを確認してダウンロード

ウェブブラウザー

ソース	宛先	プロトコル	ポート	説明
Web ブラウザー（HTML5）、Let's	RAS ウェブ管理サービス（RAS 管理ポー	TCP	20443	管理者は RAS 環境の HTML5 ベースの管理ポータルにアクセスします。

Encrypt サービス	タル）			
	HALB	TCP	80、443	エンドユーザーは HALB 経由で Parallels RAS Web Client（通常モードの Secure Gateway）にアクセスします **注:** Let's Encrypt を使用する場合、受信リクエストに対応するためポート 80 と 443 を開けておく必要があります。
	RAS Secure Gateway	TCP	80、443	エンドユーザーは Parallels RAS Web Client（通常モードの Secure Gateway）にアクセスします **注:** Let's Encrypt を使用する場合、受信リクエストに対応するためポート 80 と 443 を開けておく必要があります。

HALB

ソース	宛先	プロトコル	ポート	説明
HALB	HALB	VRRP	112	HALB/HALB 間の通信は、アクティブな HALB に対する VIP の自動割り当てに使用されます。
	転送モードの RAS Secure Gateway	TCP、UDP	80、443	管理およびユーザーセッション接続
	ノーマルモードの RAS Secure Gateway	TCP、UDP TCP、UDP	80、443 20009	管理およびユーザーセッション接続 ファイヤウォール経由のデバイスマネージャーのシャドーイング（間接ネットワーク接続）

RAS Secure Gateway

ソース	宛先	プロトコル	ポート	説明
転送モードの RAS Secure Gateway	ノーマルモードの RAS Secure Gateway	TCP、UDP TCP、UDP	80、443 3389	管理およびユーザーセッション接続 オプション - RDP ロードバランスが有効になっている場合、ユーザーセッションに使用されます。

	RAS Performance Monitor	TCP	8086	Agent（Telegraf サービス）が収集したパフォーマンスデータを InfluxDB に送信。
ノーマルモードの RAS Secure Gateway	リモートデスクトップサービス	TCP、UDP	3389	RDP 接続。
	RAS Connection Broker	TCP TCP、UDP	20002 20009	RAS Connection Broker サービスのポート - RAS Secure Secure Gateway と RAS Console の通信（通常モードのみ）。 RAS Console が RAS Connection Broker 上で実行されている場合、ファイヤウォール経由でのデバイスマネージャーのシャドーイング（間接的なネットワーク接続）
	RAS Performance Monitor	TCP	8086	Agent（Telegraf サービス）が収集したパフォーマンスデータを InfluxDB に送信。
	localhost	TCP	20020	ユーザーポータル Web サーバー（NodeJS）の通信。

RAS Connection Broker

ソース	宛先	プロトコル	ポート	説明
RAS Connection Broker	AD DS コントローラー	TCP TCP TCP、UDP UDP	389、3268 636、3269 88 53	LDAP LDAPS Kerberos DNS
	RAS Connection Broker	TCP	20001 20030	冗長性サービス。 同じサイトで実行されている RAS Connection Broker 間の通信。
	Parallels ライセンスサーバー	TCP	443	RAS Connection Broker（ライセンスサイトのプライマリ Connection Broker）と Parallels ライセンスサーバー（https://ras.parallels.com）の通信。 注: テナントブローカー RAS Connection Broker には必要ありません（「テナントブローカー」のセクションを参照してください）。
	RAS Performance Monitor	TCP	8086	Agent（Telegraf サービス）が収集したパフォーマンスデータを InfluxDB に送

			信。
RAS RD セッションホスト Agent	TCP、UDP	30004	Connection Broker のリクエスト用サーバー。
RAS Provider Agent	TCP、UDP	30006	Provider Agent 通信ポート。
RAS Remote PC Agent	TCP、UDP	30004	Remote PC Agent の通信ポート（Agent の状態、カウンターおよびセッション情報）
2FA サーバー	TCP、UDP	8080、80 1812、1813	Deepnet/Safenet Radius
RAS 登録サーバー	TCP	30030	RAS Connection Broker が RAS 登録サーバーに接続リクエストを送信します
RAS レポート	TCP	30008	マスター RAS Connection Broker は RAS Reporting と通信を行います（SSRS として同じホストにインストール済み）。
RAS リモートインストーラーサービス	TCP	30020	リモート Agent プッシュ
RAS RD セッションホスト Agent RAS Guest Agent RAS Remote PC Agent RAS Connection Broker RAS Secure Gateway RAS 登録サーバー	TCP	135、445、49179	ソフトウェアのリモートインストール、プッシュ/引き継ぎ。
SMTP	TCP	587	Notifdispatcher は、メールボックス設定（+SSL/TLS）で指定されたポートを使用して、メールを送信するサービスです。
Let's Encrypt サービス	TCP	80、443	Let's Encrypt クライアント（プライマリ Connection Broker で利用可能）と Let's Encrypt サーバーとの間の通信。

RAS Console

ソース	宛先	プロトコル	ポート	説明
RAS Console	RAS レポート	TCP	30008	RAS Console は、RAS Reporting と通信を行うプライマリ RAS Connection Broker に接続されます（SSRS として同じホストにインストール済み）。SSRS は TCP 1433（設定で 1433 が確立されていない場合は動的ポート）経由で SQL とのやり取りを行います。
	SSRS	TCP	443	レポートの取得。
	HALB	TCP、UDP	31006	構成に使用されます。
	Parallels Client	TCP	50005	ダイレクトネットワーク接続の場合、RAS Console からシャドーイング。
	RAS RD セッションホスト Agent	UDP、TCP	30004	[Agent をチェック] タスクに使用。 コンポーネント管理に使用。
	RAS Guest Agent	TCP UDP	30009 30010	[Agent をチェック] タスクに使用。 コンポーネント管理に使用。
	RAS Remote PC Agent	UDP、TCP	30004	[Agent をチェック] タスクに使用。 コンポーネント管理に使用。
	RAS Provider Agent	UDP、TCP	30006	[Agent をチェック] タスクに使用。 コンポーネント管理に使用。
	MFA サーバー	TCP、UDP	8080、80、1812、1813	Deepnet / Safenet / Radius
	Microsoft サイト	TCP	80、443	Parallels Client のアップデートを確認してダウンロード
	Parallels サイト	TCP	80	Parallels Client のアップデートを確認してダウンロード
	RAS Performance Monitor	TCP	3000	Grafana に対する RAS ブラウザープラグイン接続。
	RAS Connection Broker	TCP	20002、20001	Connection Broker との通信と冗長化。
	RAS 登録サーバー	TCP、UDP	30030	[Agent をチェック] タスクに使用。 コンポーネント管理とトラブルシューティングに使用されます。

	WYSE ブローカー	UDP	1234（送信のみ） 68（受信のみ）	Wyse ブローカー検出要求ブロードキャストパケット（V_WYSEBCAST）。 Wyse ブローカー検出応答パケット（V_WYSETEST）。
	SMTP	TCP	587	RAS Console では、メールボックス設定（+SSL/TLS）で指定されたポートを使用してテストメールを送信できます

SSRS

ソース	宛先	プロトコル	ポート	説明
SSRS	Microsoft SQL Server	TCP	1433	RAS Console は RAS Reporting に接続されます

RAS レポート

ソース	宛先	プロトコル	ポート	説明
RAS Reporting Service	MS SQL	TCP	1433	RAS アクティビティ情報の保存
	SSRS	TCP	8085、443	レポートの列挙（カスタムレポートを含む）

RAS ウェブ管理サービス（REST/管理ポータル）

ソース	宛先	プロトコル	ポート	説明
RAS ウェブ管理サービス	RAS RD セッションホスト Agent	TCP	30004	ログの取得
	RAS Guest Agent	TCP	30010	ログの取得
	RAS Provider Agent	TCP	30006	ログの取得

	RAS Connection Broker	TCP	20002、20001、30020	GA および冗長サービスとの通信。 公開中に、インストールされているアプリケーションを参照したり、単一のファイル/フォルダーを参照したりするために使用されます。 30020 - リモート Agent プッシュ（RAS 18 より前のバージョン）
	RAS RD セッションホスト Agent RAS Guest Agent RAS Remote PC Agent RAS Connection Broker RAS Secure Gateway RAS 登録サーバー	TCP	135、445	ソフトウェアのリモートインストール、プッシュ/引き継ぎ（RAS 18 より前のバージョン）
	RAS Reporting Service	TCP	3000	管理ポータル iFrame への RAS レポートの統合

RAS PowerShell

ソース	宛先	プロトコル	ポート	説明
RAS PowerShell	RAS RD セッションホスト Agent	TCP	30004	ログの取得
	RAS Guest Agent	TCP	30010	ログの取得
	RAS Remote PC Agent	TCP	30004	ログの取得
	RAS Provider Agent	TCP	30006	ログの取得
	RAS Connection Broker	TCP	20002、20001	GA および冗長サービスとの通信。 公開中に、インストールされているアプリケーションを参照したり、単一のファイル/フォルダーを参照したりするために使用されます。

RAS Provider Agent

ソース	宛先	プロトコル	ポート	説明
RAS Provider Agent	RAS Connection Broker	TCP	20003	Connection Broker 通信ポート。
	RAS Guest Agent	TCP UDP	30010 30009	TCP はコマンドの送信に使用されます。 UDP は、初回のハンドシェイク中に使用されます。
	RAS Performance Monitor	TCP	8086	Agent（Telegraf サービス）が収集したパフォーマンスデータを InfluxDB に送信。Hyper-V のみに適用。
	Hyper-V	TCP	135、49152～65535	ホストの電源がオンになっているかどうかを確認し、エクスポート、インポート、削除、シャットダウン、再起動、またはサスペンドのコマンドを送信するために使用されます。
	Nutanix AHV（AOS）	TCP	9440	ホストの電源がオンになっているかどうかを確認し、複製、削除、シャットダウン、再起動のコマンド（RestAPI 呼び出し、PoSH、リモート ncli）を送信するために使用されます。
	VMWare	TCP	443	ホストの電源がオンになっているかどうかを確認し、複製、削除、シャットダウン、再起動、またはサスペンドのコマンドを送信するために使用されます。
	Microsoft Azure	TCP	443	ゲストの電源がオンになっているかどうかを確認し、複製、シャットダウン、再起動、のコマンドを送信するために使用されます（REST 経由）。
	Azure Virtual Desktop	TCP	443	ホストの電源がオンになっているかどうかを確認し、複製、シャットダウン、再起動、のコマンドを送信するために使用されます（REST 経由）。
	AWS	TCP	443	ホストの電源がオンになっているかどうかを確認し、複製、シャットダウン、再起動、のコマンドを送信するために使用されます（REST 経由）。

	スケーラブル	TCP	443	ホストの電源がオンになっているかどうかを確認し、複製、シャットダウン、再起動、のコマンドを送信するために使用されます（REST 経由）。
	VDI 経由の Remote PC	TCP	135、49152～65535	ホストの電源がオンになっているかどうかを確認し、シャットダウン、再起動、またはサスペンドのコマンドを送信するために使用されます。

RAS 登録サーバー

ソース	宛先	プロトコル	ポート	説明
RAS 登録サーバー	AD DS コントローラー	TCP TCP TCP、UDP UDP	389、3268 636、3269 88 53	LDAP LDAPS Kerberos DNS
	RAS Connection Broker	TCP UDP	20003 20003	同期設定とパフォーマンスカウンター。 接続リクエストを拒否
	認証局（CA）	TCP TCP	135 動的範囲 49152 - 65535	DCOM/RPC ポート

RAS RD セッションホスト Agent

ソース	宛先	プロトコル	ポート	説明
RAS RD セッションホスト Agent	RAS Connection Broker	TCP、UDP	20003	RAS Connection Broker との通信に使用されます。
	localhost	TCP	30005	内部コマンド用（memshell、プリンターリダイレクター）。
	FSlogix	TCP	443	FSlogix インストーラーをダウンロード
	RAS Performance Monitor	TCP	8086	Agent（Telegraf サービス）が収集したパフォーマンスデータを InfluxDB に送信。

	RAS 登録サーバー	TCP	30030	RAS RD セッションホスト Agent（PrlsSCDriver）が接続してログオン資格情報を取得します。

RAS Guest Agent

ソース	宛先	プロトコル	ポート	説明
RAS ゲスト Agent（Azure Virtual Desktop で使用）	Provider Agent	TCP、UDP	30006	Provider Agent との通信 Provider Agent 検索用にサブネットのブロードキャストを送信 通常の UDP ハートビート
	localhost	TCP	30005	内部コマンド用（memshell、プリンターリダイレクター）
	RAS Performance Monitor	TCP	8086	Agent（Telegraf サービス）が収集したパフォーマンスデータを InfluxDB に送信。
	RAS 登録サーバー	TCP	30030	RD ゲスト Agent（PrlsSCDriver）が接続してログオン資格情報を取得します
	FSlogix	TCP	443	FSlogix インストーラーをダウンロード

RAS Remote PC Agent

ソース	宛先	プロトコル	ポート	説明
RAS Remote PC Agent	RAS Connection Broker	TCP、UDP	20003	RAS Connection Broker との通信に使用されます
	localhost	TCP	30005	内部コマンド用（memshell、プリンターリダイレクター）
	RAS Performance Monitor	TCP	8086	Agent（Telegraf サービス）が収集したパフォーマンスデータを InfluxDB に送信。
	RAS 登録サーバー	TCP、UDP	30030	RAS リモート PC（PrlsSCDriver）が接続してログオン資格情報を取得します
	FSlogix	TCP	443	FSlogix インストーラーをダウンロード

テナントブローカー

ソース	宛先	プロトコル	ポート	説明
テナント - RAS Connection Broker	テナントブローカー - RAS Connection Broker	TCP	20003	テナントブローカーを使用して、テナントの RAS Connection Broker と通信を行い、テナントブローカーに参加し、構成とステータスを同期します

Active Directory およびドメインサービスのポート

Active Directory および Active Directory ドメインサービスのポートの要件については、次の記事を参照してください。
https://technet.microsoft.com/en-us/library/dd772723%28v=ws.10%29.aspx。

Azure Virtual Desktop

Azure Virtual Desktop 用に作成した Azure 仮想マシンには、Azure 業務用クラウドの以下の URL にアクセスするための権限が必要です。

住所	送信 TCP ポート	目的	サービスタグ
*.wvd.microsoft.com	443	サービストラフィック	AzureVirtualDesktop
gcs.prod.monitoring.core.windows.net	443	Agent トラフィック	AzureCloud
production.diagnostics.monitoring.core.windows.net	443	Agent トラフィック	AzureCloud
*xt.blob.core.windows.net	443	Agent トラフィック	AzureCloud
*eh.servicebus.windows.net	443	Agent トラフィック	AzureCloud
*xt.table.core.windows.net	443	Agent トラフィック	AzureCloud
*xt.queue.core.windows.net	443	Agent トラフィック	AzureCloud
catalogartifact.azureedge.net	443	Azure マーケットプレイス	AzureCloud
kms.core.windows.net	1688	Windows アクティベーション	インターネット

mrsglobalsteus2prod.blob.core.windows.net	443	エージェントと SXS スタックのアップデート	AzureCloud
wvdportalstorageblob.blob.core.windows.net	443	Azure ポータルのサポート	AzureCloud
169.254.169.254	80	Azure Instance Metadata サービスエンドポイント	N/A
168.63.129.16	80	ホスト正常性モニタリング	N/A
https://download.parallels.com/ras/Configuration_01-20-2022.zip	443	ホストをホストプールに参加させる	AzureVirtualDesktop

次の表は、Azure の仮想マシンがアクセスできるオプション URL の一覧です。

住所	送信 TCP ポート	目的	Azure Gov
*.microsoftonline.com	443	Microsoft Online Service への認証	login.microsoftonline.us
*.events.data.microsoft.com	443	テレメトリーサービス	なし
www.msftconnecttest.com	443	OS がインターネットに接続されているかどうかを検出	なし
*.prod.do.dsp.mp.microsoft.com	443	Windows Update	なし
login.windows.net	443	Microsoft Online Services、Microsoft 365 にサインイン	login.microsoftonline.us
*.sfx.ms	443	OneDrive クライアントソフトウェアのアップデート	oneclient.sfx.ms
*.digicert.com	443	証明書の失効確認	なし
*.azure-dns.com	443	Azure DNS 解決	なし
*.azure-dns.net	443	Azure DNS 解決	なし

最新の情報については、Microsoft のウェブサイト（https://docs.microsoft.com/en-us/azure/virtual-desktop/safe-url-list#required-url-check-tool）も参照してください。

RAS Performance Counter

以下の表は、コンポーネントごとに Parallels RAS で使用できるパフォーマンスカウンターのリストです。

Parallels RAS Gateway（2XProxyGateway.exe）

ID	名前	説明
ras_gw_tot_conn	総接続数	Gateway への総接続数。
ras_gw_tot_threads	総スレッド数	Gateway で実行中の総スレッド数。
ras_gw_rpd_sess	RDP のトンネリングされたセッション	トンネリングされた RDP セッション数。
ras_gw_rpd_sess_s	RDP SSL のトンネリングされたセッション	SSL 上のトンネリングされた RDP セッション数。
ras_gw_html	HTTP 接続	トンネリングされた HTTP ソケット数
ras_gw_html_s	HTTPS 接続	トンネリングされた HTTPS ソケット数
ras_gw_html5	HTML5 接続	トンネリングされた HTTP5 ソケット数
ras_gw_html5_s	HTML5 SSL 接続	SSL 上のトンネリングされた HTTP ソケット数
ras_gw_cm	デバイスマネージャーの接続	Parallels デバイスマネージャー接続数
ras_gw_cm_s	デバイスマネージャーの SSL 接続	SSL 上の Parallels デバイスマネージャー接続数
ras_gw_wyse	Wyse 接続	Wyse 接続数
ras_gw_wyse_s	Wyse SSL 接続	SSL 上の Wyse 接続数
ras_gw_rdpudp	RDP UDP のトンネリングされたセッション	RDP UDP 接続数
ras_gw_rdpudp_s	RDP UDP DTLS のトンネリングされたセッション	DTLS 上の RDP UDP 接続数
ras_gw_cache_sock	キャッシュされたソケット	ゲートウェイと Connection Broker との間でキャッシュされたソケット数
ras_gw_idle_threads	アイドルスレッド	Gateway 上のアイドルスレッド数
ras_gw_client	クライアントの接続	Parallels Client の接続数
ras_gw_client_s	クライアントの SSL 接続	Parallels Client の SSL 経由の接続数

Parallels RAS Connection Broker（2XController.exe）

ID	名前	説明
ras_pa_avg_client_connection_time	クライアントの平均接続時間	クライアント接続時間の平均値。
ras_pa_avg_client_auth_time	ユーザー認証の平均所要時間	ユーザーの認証に要する平均時間。
ras_pa_avg_client_policy_time	ユーザーポリシーの平均取得時間	ユーザーポリシーの取得に要する平均時間。
ras_pa_avg_client_rep_time	クライアントテレメトリーの平均送信時間	クライアントテレメトリーの送信に要する平均時間。CEP で使用されます。
ras_pa_avg_client_applist_time	ユーザーの公開済みアイテム取得平均時間	ユーザーの公開済みアイテムリストの取得に要する平均時間です。
ras_pa_avg_client_appicons_time	アイコン取得平均時間	公開済みアイテムアイコンの取得に要する平均時間です。
ras_pa_avg_client_getidle_time	リクエストの起動平均時間	リクエストの起動に要する平均時間です。

Parallels RAS RDS Agent（2XAgent.exe）

ID	名前	説明
act_sess	[アクティブな RDS セッション]	アクティブな RDS セッションの数。
disc_sess	[切断済み RDS セッション]	切断済み RDS セッションの数。

索引

R