Parallels RAS アドバンス トレーニング

目次

はじめに

本ドキュメントの目的

本ドキュメントは、Parallels Remote Application Server(以降RAS)を初めて学習する方のために、RASの構成から、簡単な環境を実習として作成することにより、RASの理解を深めて頂くことを目的として作成しました。
販売店のエンジニア様や自社でRAS環境を構築することを検討しているエンジニアの方などを対象に、シンプルなシステム構成で構築を完了し、RASのリモート アクセスをお試しいただき体験いただければ幸いです。
本資料でも構成や設定について説明していますが、詳細な内容につきましては、弊社Webサイトにて管理者ガイドを公開しておりますので、そちらをご参照ください。
管理者ガイドを含むマニュアルの公開ページ
https://www.parallels.com/jp/products/ras/resources/

制限事項

本資料は、RAS Ver.20.0をベースに2025年1月時点の情報をベースとして作成しています。そのため、バージョンアップなどにより画面や用語、メニューの記載、手順などが変更となる場合がありますのであらかじめご了承ください。
また、それ以前の製品バージョンの場合でも、基本的な設定手順は同様ですが、画面表記などが異なる部分もありますのでご注意ください。
また、本資料は、RAS製品バージョンにともない、随時更新をする可能性がありますので、ご了承ください。ございます。

免責事項

- 本書の内容は、予告なしに変更されることがあります。
- コーレル株式会社は、本書の技術的もしくは編集上の間違い、欠落について、一切責任をおいません。また、お客様が期待される効果を得るために、本書に従った導入、使用および使用効果につきましては、お客様の責任とさせていただきます。
- 本書に記載されている内容の著作権は、コーレル株式会社に帰属します。本書の内容の一部または全部をコーレル株式会社の許諾なしに複製、改変、および翻訳することは禁止されています。

商標について

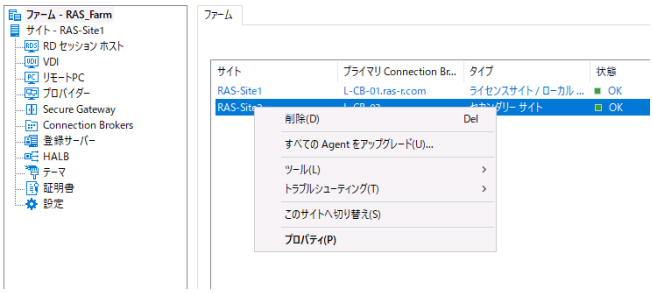
- Parallels Remote Application Server®は、コーレルの登録商標です。
- Microsoft、Windows、Windows Server、Azure、Hyper-Vは、米国Microsoft Corporationの米国およびその他の国における登録商標です。
- Googleは、Google LLCの商標または登録商標です。
- 本書に記載されたその他の製品名および標語は、各社の商標または登録商標です。

サイト、Connection Broker、Secure Gateway

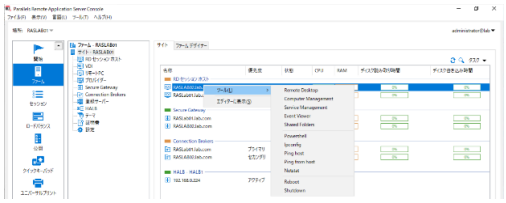
サイト

ベーシックトレーニングでは、ファームにサイトが含まれ、サイトにはさまざまなサイト コンポーネントが含まれる仕組みについて説明しました。1つのファーム内に複数のサイトが存在する可能性がありますが、ライセンス サイトとして指定できるサイトは1つだけです。デフォルトでは、これはRASが新しい環境に初めてインストールされたときに作成された最初のサイトです。他の各サイトはライセンス情報をライセンス サイトに伝達し、ライセンス サイトはParallelsライセンスWebサービスと通信します。ライセンスサイトがオフラインになったり、ライセンス サービスと通信できなくなったりした場合は、別のサイトをライセンスサイトに昇格させてライセンスを処理できます。72時間以内にこの作業が行われない場合、サイトが復元されるか別のサイトが昇格されるまで、ファームは無効な状態になります。また、再アクティブ化する必要があります。RASコンソール内でサイトを昇格するのは簡単です。コンソールで、左ペインのファームをクリックし、次に[ファーム名]をクリックすると、ファーム内のすべてのサイトが一覧表示されます。プロモーションするサイトを右クリックし、[ライセンス サイトとして設定] をクリックします。

注: ライセンス サイトが48 ～ 72時間オフラインになり、月に3回オンラインに戻る場合、3回目以降は Parallels RASライセンス キーを使用して再度アクティブ化する必要があります。



サイトをクリックすると、サイト内のさまざまなホストがすべて表示されます。また、CPU 使用率、RAM 使用率、ディスク I/O、オペレーティングシステム情報など、ホストに関する関連情報も表示されます。右クリック(または画面の右上にある[タスク]ドロップダウンボックスを選択)して[ツール]を選択すると、ホストをリモートで操作できます。管理者は、コンピューター管理を開く、イベントログを表示する、PowerShellスクリプトを実行する、再起動するなど、いくつかのオプションから選択できます。これらのツールは、この画面だけに限定されません。Connection Broker、RDセッションホスト、VDIなど、ホストが表示されている場所ならどこからでもアクセスできます。



Connection Broker

ベーシックトレーニングの復習ですがConnection Brokerには、プライマリConnection Brokerと接続ブローカーとセカンダリConnection Brokerがあります。各サイトにはプライマリが1つだけあります。通信パスは、サイト内の各セカンダリが関連情報をプライマリに通信し、プライマリがその情報をプライマリライセンスサイトに転送し、プライマリライセンスサイト内のプライマリConnection BrokerがParallelsライセンスサービスに通信するというものです。サイト内のすべてのConnection Broker間で中継される情報は他にもありますが、次のスライドで簡単に説明します。

先ほどのスライドで説明したように、ファーム、サイト、そしてConnection Brokerがあります。

Connection Brokerは、新しいサイトが作成されたときに最初にインストールされるコンポーネントです。最初のサイトの最初のサーバーはライセンスサーバーでもあります。これは、Parallelsライセンスサービスと通信する実際のサーバーです。ライセンスサイトがダウンしたり使用できなくなったりした場合とほぼ同じように、このサーバーがダウンしたりオフラインになったりすると、ライセンスサービスとの通信が停止し、次のスライドで説明するその他の機能も停止します。

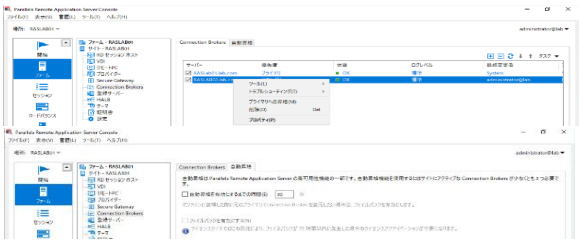
繰り返しになりますが、72時間以内にライセンスサーバーであるConnection Brokerをオンラインに戻すか、同じサイト内の別のConnection BrokerをプライマリConnection Brokerに昇格しなければなりません。各サイトに冗長性を持たせるために、少なくとも2つのConnection Brokerが必要ですが、必須ではあ

りません。セカンダリConnection Brokerをプライマリに昇格する方法は2つあります。

1つ目は、プライマリにしたいセカンダリConnection Brokerを右クリックして手動で昇格する方法です。

2つ目は、組み込みの自動昇格機能を利用する方法です。これには、サイト内に3つのConnection Brokerが必要です。

自動昇格を有効にし、自動昇格が完了するまでの経過時間を設定し、ライセンスサーバーのConnection Brokerがオンラインに戻ったときに元のプライマリに戻るかどうかを設定できます。



ここで、プライマリConnection Brokerとセカンダリ Connection Brokerの違いは何かという疑問が浮かびます。ここに示すチャートは、その違いを示しています。プライマリとセカンダリは、多くの機能にわたってワークロードを共有しますが、いくつかの重要な機能はプライマリが処理します。すでに説明したように、ライセンスサイトへのライセンス情報の通信だけでなく、電子メール通知とアラートの送信、レポート エンジンへの統計の中継など、いくつかの機能があります。

プロセス	プライマリ Connection Broker	セカンダリー Connection Broker
Connection Brokerの監視(カウンター)	○	○
RDセッションホストの監視(カウンター)	○	○
プロバイダーの監視(カウンター)	○	○
RDセッションの監視(カウンター)	○	○
デプロイされた RDS アプリケーションの監視	○	○
VDIセッションの監視(再接続)	○	○
システム設定の管理	○	×
ライセンス情報の送信とハートビート	○	×
CEP情報のプロセスと送信	○	×
レポーティングサーバーへの情報の送信	○	×
RDSスケジューラーの管理	○	×
レポーティングエンジン情報	○	Future Version
シャドーイング	○	Future Version
E-Mail通知の送信	○	×

次にプライマリとセカンダリの共有機能について説明します。Connection Brokerは互いに通信するため、ユーザー接続の観点から、1つの接続ブローカーがダウンしても、他のConnection BrokerがダウンしたBrokerの接続情報をサービスが失われることなく管理できます。これは、サイトに少なくとも2つの接続ブローカーが必要であるもう1つの理由です。

サイト内の接続ブローカーが1つしかない場合、ユーザー エクスペリエンスが低下します。

Secure Gateway

Connection Brokerは公開されたリソースへの確立された接続を処理しますが、クライアントからの接続リクエストは直接接続ブローカーに送られません。接続リクエストがあった場合、Secure Gateway はそれを処理し、そのリクエストを接続ブローカーに転送するコンポーネントです。

複数の接続ブローカーがある場合、Gateway はそれらの間で負荷分散を行います。接続は http(80) または https(443) を介して着信します。

インストールしてすぐに、Secure Gatewayは上記のように動作し、特別な初期設定は必要ありません。これは PoC やシンプルな環境に最適です。

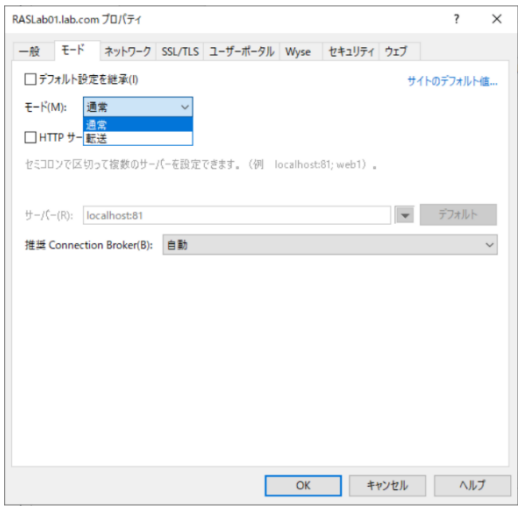
次の数枚のスライドでは、Secure Gateway のその他の機能について説明します。

RAS Secure Gatewayは、以下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、ユーザーの接続要求を受け取り、要求したユーザーがアクセスを許可されているかを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は、多くのリクエストに対応でき、冗長性を高めることができます。
- 転送モード：転送モードのRAS Secure Gatewayは、ユーザーの接続要求を事前に設定されたゲートウェイに転送します。ゲートウェイのフォワーディングモードは、カスケード接続のファイアウォール使用する場合、WAN接続とLAN接続を分離し、問題が発生した場合にLANを中断させずにWANセグメントを切断できるようにするために有効です。

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。

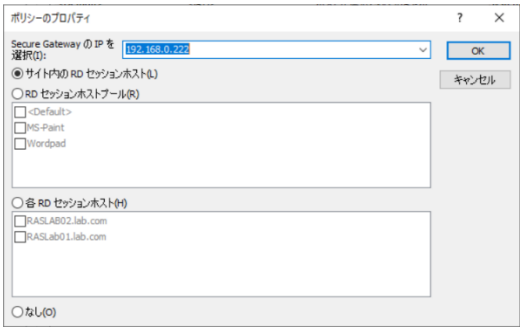
モードは相互に排他的です。



トンネリングポリシーを使用すると、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、右側のペインで[トンネリングポリシー]タブをクリックします。

<既定>ポリシーは事前に構成されたルールであり、常に最後に使用され、構成されていないすべてのSecure Gateway IPアドレスをキャッチし、ファーム内のすべてのサーバー間でセッションを負荷分散します。<既定>ポリシーを右クリックして[プロパティ]をクリックすることで構成できます。



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。これを行うには、トンネリング ポリシーのプロパティで、下部にある[なし]オプションを選択します (これは、Parallels RASインストールのデフォルト設定です)。

こうすることで、ネイティブMSTSCがポート経由でゲートウェイにアクセスすることを制限します(デフォルトのポートは80)。その結果、誰かがIPアドレス:80でMSTSCを使用しようとすると、アクセスが拒否されます。Parallels クライアントからのRDP接続でも同じことが起こります。

RDPアクセスを制限する理由はいくつかあります。

- 1つ目は、ユーザーがParallels RAS接続のみを使用してRASファームに接続し、RDPは使用しないようにする場合です
- 2つ目の理由は、DDoS攻撃を防ぐためです

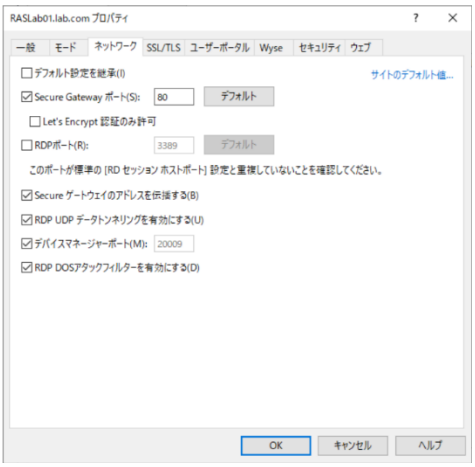
デフォルトでは、RAS Secure GatewayはTCPポート80と443をリッスンして、すべてのParallels RASトラフィックをトンネリングします。ポートを変更するには、RAS Secure Gateway ポート入力フィールドに新しいポートを指定します。

RDPポート3389は、基本的な負荷分散デスクトップセッションを必要とするクライアントに使用され、デフォルトではオフになっています。このポートでの接続は、公開されたリソースをサポートしません。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。独自のポートを設定する場合は、ポート番号が標準の「RDセッションホストポート」設定と競合しないことを確認してください。

注: RDPポートを変更する場合は、新しいポート番号をリモートデスクトップ クライアントの接続文字列に追加する必要があります (例: [IPアドレス]:[port])。

- Secure ゲートウェイのアドレスを伝搬する：このオプションを使用すると、Secure Gatewayアドレスのブロードキャストをオンにして、Parallelsクライアントがプライマリ Secure Gatewayを自動的に見つけられるようにすることができます。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トンネリングを無効にするには、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：このオプションを選択すると、デバイスマネージャーカテゴリからWindowsデバイスを管理できるようになります。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攻撃フィルターを有効にする：このオプションを選択すると、同じIPアドレスからの未完了のセッションの

チェーンが拒否されます。たとえば、Parallelsクライアントが複数の連続セッションを開始し、各セッションでユーザーが資格情報を提供するのを待機している場合、Parallels RASはそ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。



このRDP DOSアタックフィルターの機能と、前のスライドで説明したRDPをブロックするトンネリング機能との違いは、ここでの設定は攻撃を監視しますが、RDPの使用は許可するのに対し、トンネリングはRDPを使用して通過しようとするすべての試みをブロックする点です。

プロバイダー、テンプレート、オートスケーリング

プロバイダー

プロバイダーとテンプレートは互いに結びついています。プロバイダーなしではテンプレートを作成することはできません。プロバイダーは、プロバイダーエージェントがゲストを実行するハイパーバイザーまたはクラウドプラットフォームと通信するために必要な接続情報です。これは理解しておくべき重要な違いです。

プロバイダーは接続情報(ユーザー名、パスワード、接続先のIPなど)を保持しており、プロバイダーエージェントはハイパーバイザーまたはクラウドと通信し、仮想マシンの作成や削除などのコマンドを送信します。

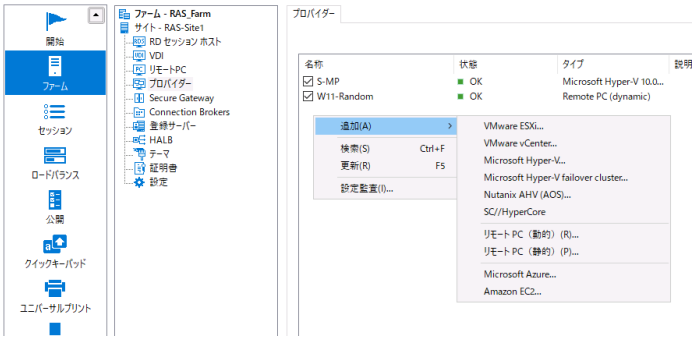
RASは、Microsoft Azureおよび Amazon EC2とともに、ポピュラーなエンタープライズハイパーバイザーをサポートしています。RASでは、同じタイプの接続を使用して複数のプロバイダーを作成できます。

たとえば、vCenterによって管理される 2 つの個別のvSphere環境がある場合、vCenter接続ごとにプロバイダーを作成できます。

同じことがAzureテナントおよびEC2インスタンスにも当てはまります。

RASでファームにインストールできる2種類のRASプロバイダーエージェント:

- 組み込み：このRASプロバイダーエージェントは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。エージェントは複数のプロバイダーを処理でき、高可用性用に構成することもできます。
- 専用：WこのRASプロバイダーエージェントは手動でインストールされます。
  処理できるのは1つのプロバイダーのみです。このエージェントタイプを複数のプロバイダーで使用する場合は、プロバイダーごとに個別のインスタンスをインストールする必要があります。



ハイパーバイザーのプロバイダーの作成手順：

コンソールの左ペインの[ファーム]で[サイト]、[プロバイダー]の順に選択し、プラス記号をクリックして[ハイパーバイザータイプ]を選択します。

- ウィザードは、以前に選択した内容に基づいてタイプが事前に入力された状態で表示されます。
- ウィザードでは、名前と説明をカスタム入力できます。
- 住所はIPアドレスまたはFQDNのいずれかです。
- ユーザー名とパスワードは、ハイパーバイザーの管理者の資格情報である必要があります。
- ウィザードを完了したら、[次へ] をクリックします。
- 次に [適用] をクリックします。
- ウィザードのオプションは、使用しているハイパーバイザーのバージョンによって異なります。
  - バージョン：ハイパーバイザーのバージョンです。使用しているハイパーバイザーのバージョンがリストされていない場合は、[他]を選択します。
  - 住所：プロバイダーホストのIPアドレス。
  - ポート: プロバイダーが着信接続をリッスンするポート番号です。
  - リソースプール: このフィールドはVMware vCenterでのみ有効です。プロバイダーの追加時にvCenterリソースプールを指定した場合、そのプールがここに表示されます。[...]ボタンを使用すると、別のプールを指定できます(または、フィールドが空の場合はプールを選択できます)。ただし、現在のプールのゲストVMがParallels RASで作成または使用されていない場合に限ります。Parallels RASが現在の使用状況を検出すると、警告メッセージが表示され、変更できなくなります。それでも別のリソース プールを選択する場合は、RASコンソール上で手動で完全なクリーンアップを実行し、使用状況がまったく存在しないようにする必要があります。
  - 専用Provider Agent：別のサーバーに専用のRASプロバイダーエージェント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。Agentアドレスフィールドにサーバーの FQDNまたはIPアドレスを入力します。

クラウドプロバイダーの作成手順:

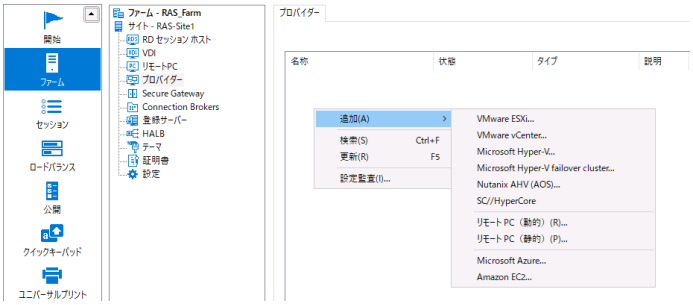
タイプ：クラウドコンピューティングプロバイダーのタイプです（Azureなど）

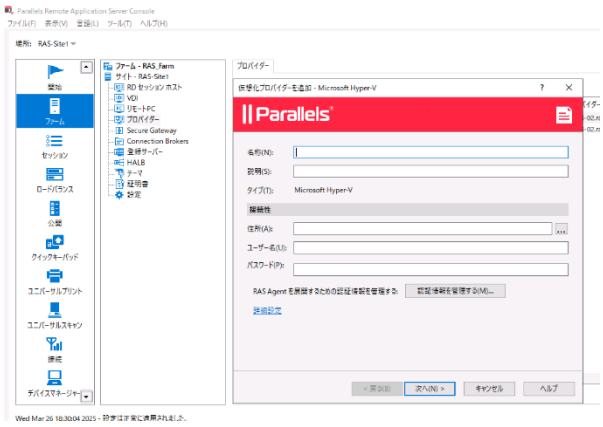
- 名前：プロバイダーの名前を指定します。
- 説明：オプションで説明を記載できます。
- 認証情報を管理する :RASエージェントの展開およびホストの管理に使用する認証情報を設定します
- 専用プロバイダーエージェント：別のサーバーに専用の RAS プロバイダー エージェントがインストールされている場合は、このオプションを選択します。エージェント アドレス フィールドにサーバーの FQDN または IP アドレスを入力します。

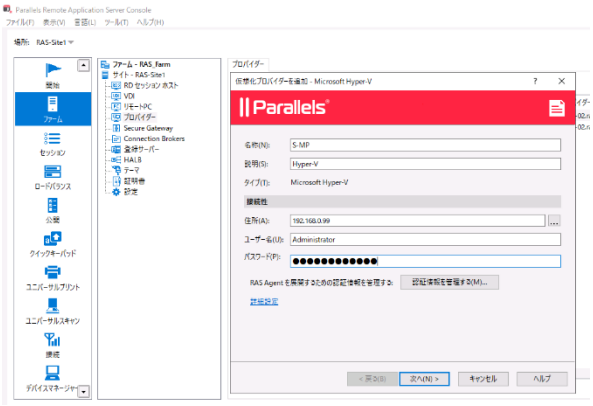
認証情報：ユーザー名とパスワードを設定します

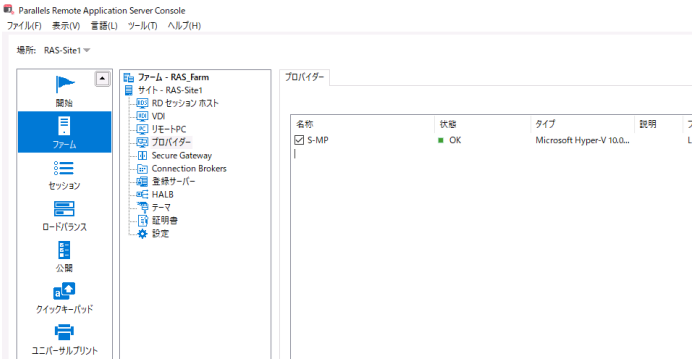
資格情報タブには、ハイパーバイザー ベースのホストかクラウド ベースのホストかに応じて異なるプロパティがあります。

- 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。
- クラウド プロバイダー：クラウドでは、それぞれのクラウドで作成された特別な「ユーザー」と「アプリ登録」が必要です。









テンプレート

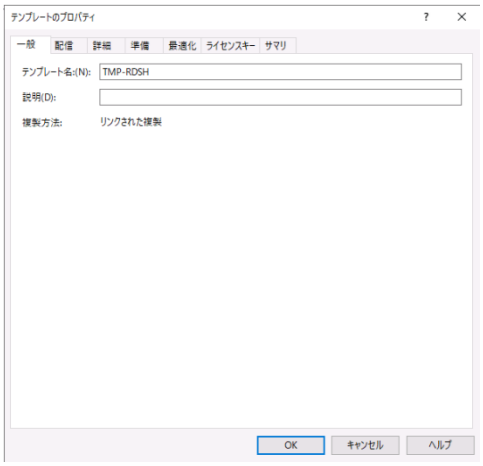
RAS テンプレートは、RAS コンソールで指定された構成設定と仮想マシンの組み合わせです。これらを組み合わせることで、RD セッション ホスト グループと VDI プール内でそれぞれの仮想マシンを展開するために使用されるテンプレートが形成されます。

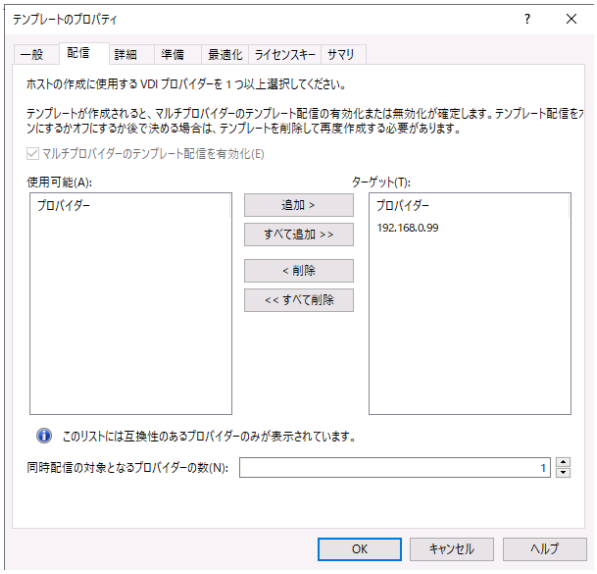
これらの仮想マシンが RAS テンプレートを使用して展開されると、完全に構成され、最適化された状態で (必要に応じて) 表示されます。

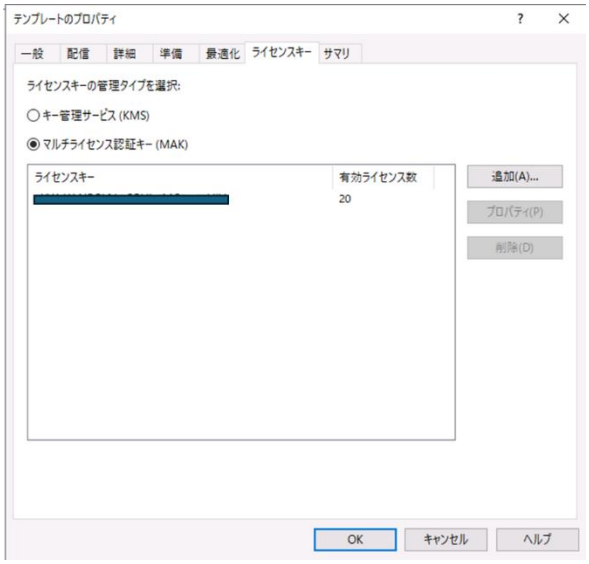
テンプレートと RDSH グループに関する注意

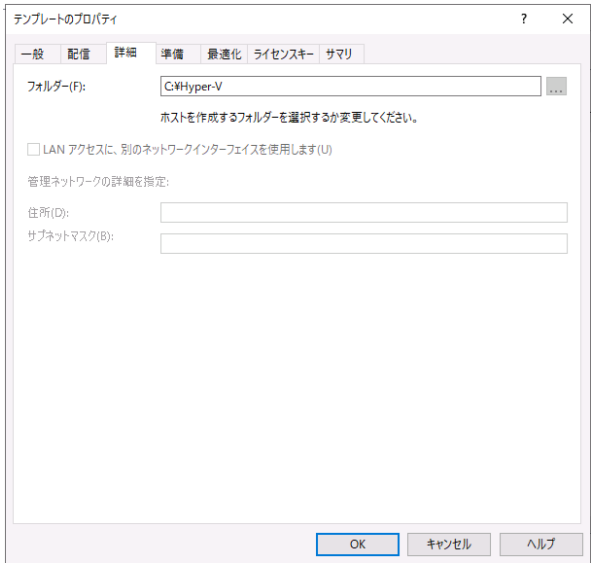
テンプレートは、複数の RDSH グループで使用できます。テンプレートを作成するときに、テンプレートを使用して作成できる仮想マシンの最大数が指定されることを理解しておくことが非常に重要です。この最大数は、テンプレートに適用されます。

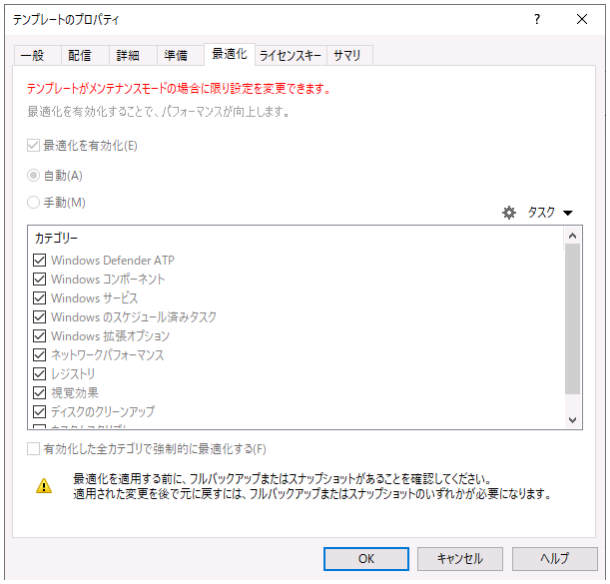
たとえば、同じテンプレートを使用する 3 つの RDSH グループがあり、最大数が 60 のゲスト仮想マシンに設定されている場合、60 の制限には 3 つの RDSH グループすべてが含まれます。プールに容量があっても、テンプレートは 61 番目の仮想マシンを作成しません。

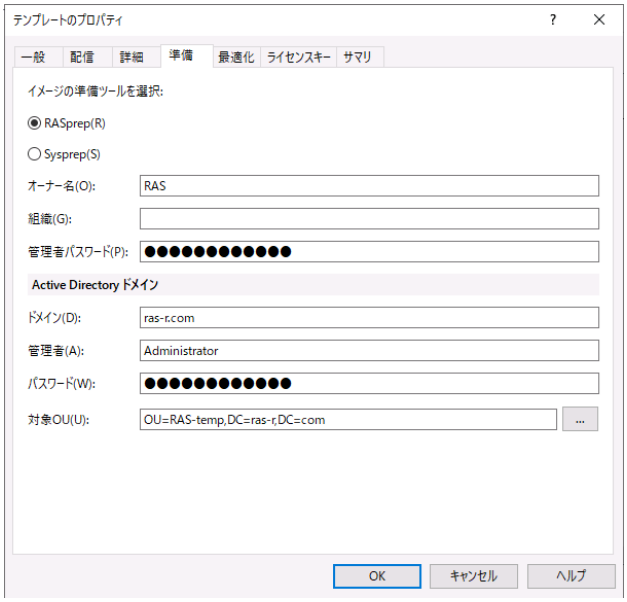


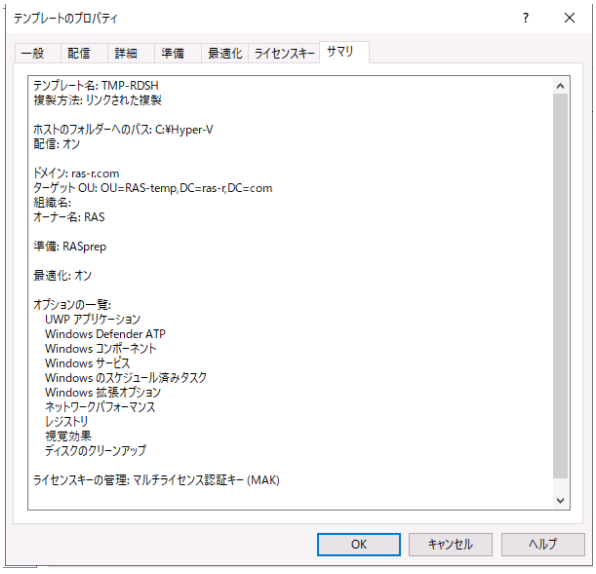












オートスケール

テンプレートを使用すると、RAS 自動スケール機能を使用できます。自動スケールは、RemotePC プロバイダーを除くすべてのプロバイダーで使用できます。

自動スケールは、構成された設定に基づいて、RDSH グループまたはプールの容量を自動的に拡張および縮小します。自動スケールを有効にした後、デフォルト設定を変更できます。常に使用可能なホストの最小数、そのグループまたはプールに作成できるホストの最大数、ホストの追加と削除のトリガーしきい値、ホストの追加が必要な場合に一度に作成するホストの数、およびホストが削除されるまでの待機時間を指定できます。未使用の VM を削除するテンプレート設定が設定されている場合、時間しきい値に達すると削除されます。

RDSH グループや AVD ホスト プールなどのマルチセッションシナリオでは、すべてのユーザーがホストからドレインされるまでホストは削除されないことに注意してください。ホストは接続ブローカーによって使用不可としてマークされ、自動的にドレイン モードになります。

Azure Virtual Desktop

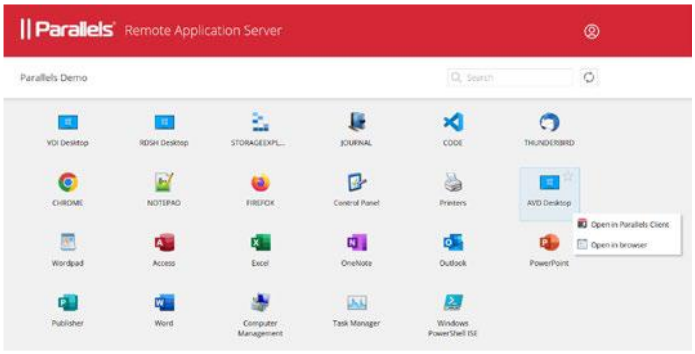
Azure Virtual Desktop は、Microsoft Azure 上で実行されるデスクトップおよびアプリケーションの仮想化サービスで、Windows 10 および Windows 11 Enterprise マルチセッション、必要に応じてサーバー OS を含む、シングルセッションおよびマルチセッションのオペレーティング システム インスタンスへのアクセスを提供します。

Parallels RAS は、Parallels RAS の既存の技術機能に加えて、Azure Virtual Desktop ワークロードの統合、構成、保守、サポート、およびアクセス機能を提供します。

RAS を使用すると、管理者は RAS コンソールから AVD 環境を完全に作成および管理できます。実際、管理者は単一の RAS コンソールからオンプレミス、Azure、AWS EC2、および AVD 環境を管理できます。

エンド ユーザーは、デバイスに Parallels Client をインストールしなくても、Windows 用の RAS クライアントまたは Windows、Mac、または Linux オペレーティング システム上の Web ブラウザーを介して、AVD から公開されたリソースと他のプロバイダーからのリソースをすべて 一か所から表示およびアクセスできます。

- ワークロード ホストは、標準の Parallels RAS 展開を介してオンプレミスで、サービスを介して Microsoft Azure で利用できます。
- 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、管理と構成の目的で Azure Virtual Desktop Agent と RAS Agent の両方が含まれています。
- Parallels Client for Windows と Parallels Web Client を使用すると、Parallels RAS Secure Gateway と Azure Virtual Desktop サービスの両方に接続でき、エンド ユーザーに単一のインターフェイスからリソースの可用性を提供できます。



拡張された価値と機能

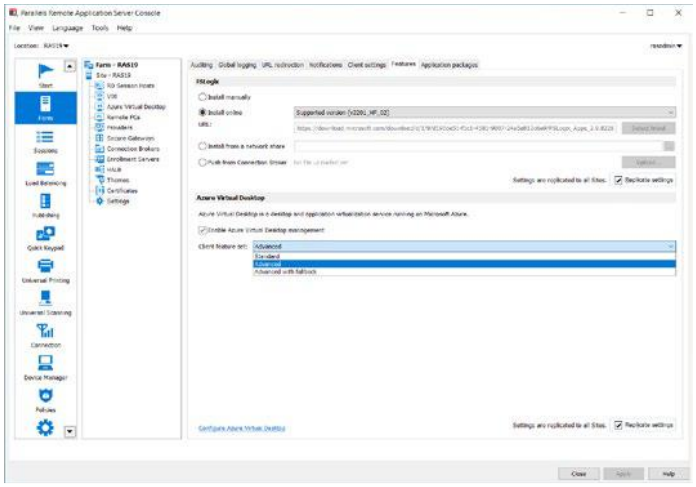
- Azure Virtual Desktop の展開と管理を簡素化および強化します。
- 管理とユーザー エクスペリエンスを統合します – 単一の画面 – Parallels Client と Parallels RAS Console。
- ハイブリッドおよびマルチクラウド展開を使用する柔軟性により、範囲を拡大します。
- Azure Virtual Desktop ワークロードの管理ルーチン、プロビジョニング、および管理を自動化および合理化します。

- Microsoft Azure および/またはオンプレミスでの自動スケール機能が組み込まれています。
- ユーザー、セッション、およびプロセスの管理。
- RAS ユニバーサル プリントおよびスキャンを活用します。
- 超高速ログオンのために AI ベースのセッション事前起動を活用します。
- ドライブ キャッシュ リダイレクトを有効にして、ファイルのリダイレクトを高速化します。
- 自動イメージ最適化と FSLogix プロファイル コンテナーを統合します。
- クライアント管理。
- クライアントのセキュリティ ポリシー。
- RAS コンソールから RAS レポートと監視を活用します。

Azure Virtual Desktop を展開する

RAS AVD プロバイダーを介して RAS を AVD と統合する前に、Azure テナントとサブスクリプション内でいくつかの前提条件を満たす必要があります。RAS 統合専用の前提条件は、こちらにあります。このリンクでは、サブスクリプション、テナント、ネットワークなどの設定方法については説明されていません。 前提条件が準備できたら、残りの展開は RAS コンソールで実行され、次の一連のウィザードを完了することで実行されます。

- 機能の有効化と Azure Virtual Desktop プロバイダーの追加。
- Azure Virtual Desktop ワークスペースの追加。
- 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。
- Azure Virtual Desktop リソースを公開します。



AVD プロバイダー

AVD プロバイダーを作成するときに、公開された AVD リソースの起動時に使用するクライアント機能セットを選択するオプションが提供されます。これらのオプションは次のとおりです。

- 標準: 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に使用されるクライアントである、リモート デスクトップ (MSRDC) クライアントとも呼ばれる Microsoft Windows デスクトップクライアントを使用して公開されたリソースを開いて実行するのと同じです
- 詳細: 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、RAS ユニバーサル プリントおよびスキャン、URL リダイレクト、ドラッグ アンド ドロップなどの高度な Parallels クライアント機能が追加されます
- フォールバック付きの詳細: このオプションは、最初に詳細機能セットを使用して公開されたリソースを開こうとします

  何らかの理由で詳細が機能しない場合は、標準オプションを使用してリソースを開こうとします。選択は、後で AVD プロバイダーを編集することで変更できます。

ホストプール

ホスト プールは、目的に応じてさまざまな方法で構成できます。次の表では、ホスト プールを作成するときに選択できるさ

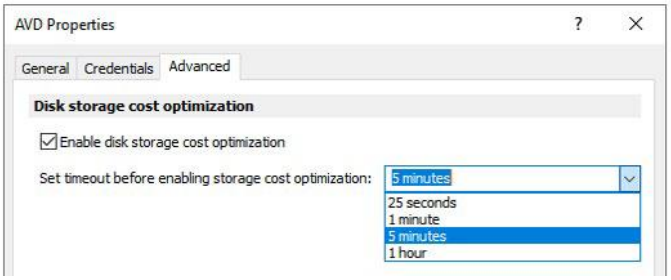
まざまなオプションについて説明します。

オプション	説明
パーソナルvs プールド	• パーソナルホストプールには、それぞれが 1 人のユーザーに割り当てられている単一のセッション ホストが含まれます。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でも保持されます。必要に応じて、ユーザーから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。 • プールされたホスト 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 10/11 マシン) が含まれます。 プール内の各ホストは、複数のユーザー (マルチセッション) に対応できます。
アプリケーションvs 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、同時に公開することはできません。 ホスト プールを作成するときに、デスクトップまたはアプリケーションから公開の種類を選択します。ホスト プールに適した種類 (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。 公開の種類は後で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vs スタンドアローン	ホスト プールを作成するときは、テンプレートまたはスタンドアロンを選択する必要があります。ホスト プールには、既存のホスト (スタンドアロン) を含めることができます。また、既存のゲスト VM に基づくテンプレートを使用することもできますし、Azure Marketplace または共有イメージ ギャラリーのイメージからオンザフライで作成するように選択することもできます。 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、要求があったときに自動的に作成することもできます。 自動ホスト作成 (Parallels RAS では Autoscale と呼ばれます) 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 プールに追加および削除されます。 ホスト (仮想マシン) は、Azure に既に存在し、ドメインに参加している必要があります。

最初の 2 つのオプションは、標準の AVD ホスト プール オプションです。
3 番目のテンプレートとスタンドアロンは、RAS に固有のものです。

Azure マネージドディスクのコスト最適化

クラウドのコスト削減は、Parallels RAS の自動スケーリング、電源管理、および自動イメージ最適化によって実現できますが、RAS は、これらの機能をストレージに拡張することで、さらなるコスト削減策を追加します。
管理者は、VM が停止したときに、RAS がストレージ タイプをよりコスト効率の高いディスク タイプに自動的に変更するように設定できます。VM が再び起動すると、元のディスク タイプが復元されます。この設定は、AVD プロバイダーのプロパティにあります。



FSLogixを使用したプロファイル管理

ユーザー プロファイル管理には、FSLogixs をお勧めします。これは、企業の Microsoft ライセンスの一部である可能性が高い Microsoft テクノロジです。FSLogix は、ローミング プロファイルの必要性を排除するユーザー プロファイル コンテナー テクノロジ (ここでは説明しない他の機能もあります) であり、これにより、ユーザーが接続する非永続的な仮想マシンをより

幅広く使用できるようになります。

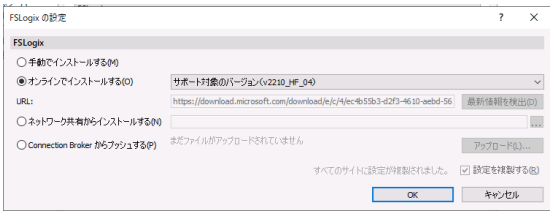
RAS は、FSLogix のインストールと構成をサポートしています。

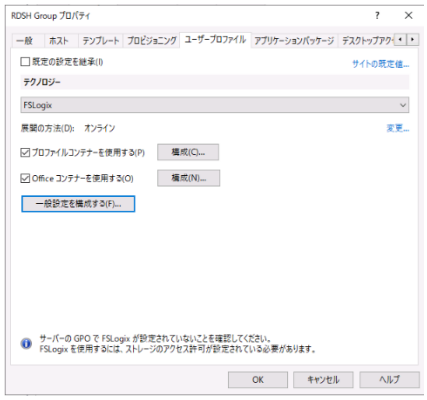
インストールの観点からは、FSLogix エージェントのインストールと更新を手動で管理するか、RAS を使用してエージェントのインストールと更新を支援することができます。インストールを手動で管理しても、RAS で利用できる構成オプションを活用できないわけではありません。

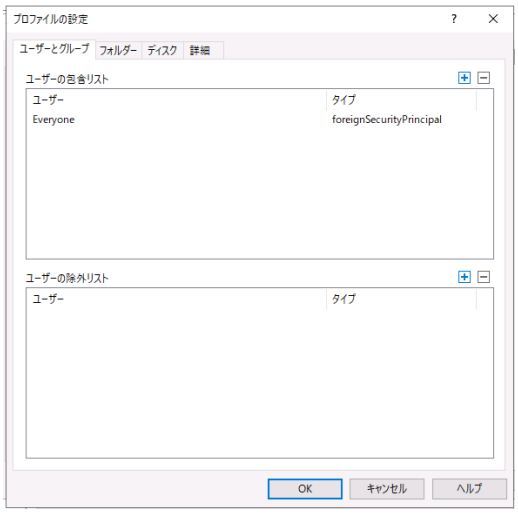
RAS を使用してインストールと更新を管理する場合、上記のように、エージェント パッケージをインストールおよび更新する場所として3つのオプションから選択できます。

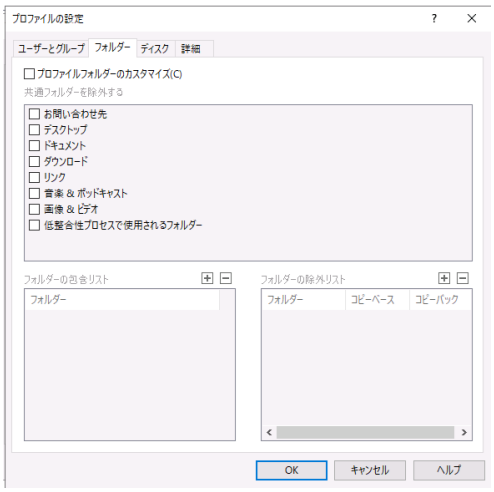
オンライン インストール オプションでは、Microsoft リポジトリを直接使用します。ファイルをダウンロードしてネットワーク共有に配置するか、接続ブローカーからプッシュすることができます。

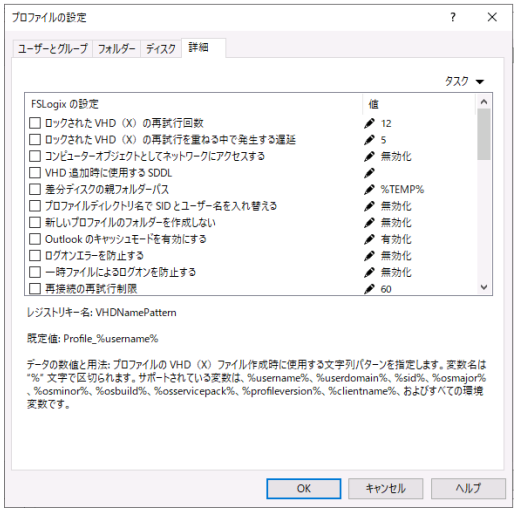
インストール オプションは、サイトレベル、グループまたはプール レベル、または特定のホストで構成できます。サイトレベルですべてのホストにインストールするという包括的なポリシーを設定しつつ、サイト設定の使用から特定のホストまたはグループを個別に除外することも可能です。除外されるホストまたはグループでは、別のリポジトリを使用しているか、エージェントがまったくインストールされていない可能性があります。







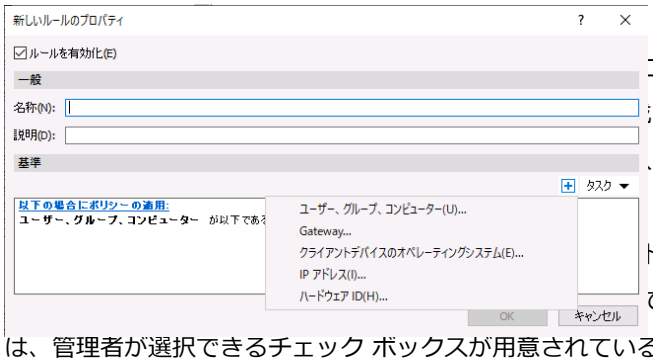




FSLogix の構成も RAS で処理できます。

ほとんどの構成オプションはコンソールで使用でき、さらに追加されています。画像でわかるように、VHD または VHDX、SMB 共有の場所、またはクラウド キャッシュの使用を指定で

きます。また、追加設定ボタンをクリックすると、FSLogix の



は、管理者が選択できるチェック ボックスが用意されているため、このタスクがはるかに簡単になります。また、プロファイル コンテナーに保存するフォルダーを含めるか除外するかを構成することもできます。

ルールとフィルター

ルールとフィルターは、ユーザーや接続に許可または禁止されている操作を決定するために多くの場所で使用されているため、理解しておくべき重要な概念です。適用するポリシー、利用可能なログオン時間、公開されているリソースの可用性、その他を決定します。

新しいルールを作成するときは、名前を付けた後、すべてのフィルター基準が満たされた場合にルールを許可する (デフォルト) か拒否するかを決定する必要があります。デフォルトでは、新しいルールは許可に設定されていますが、基準セクションの [次の場合に許可] をクリックして [次の場合に拒否] に変更することで切り替えることができます。ユーザーまたはグループ、テーマ、クライアント デバイスのエンドポイント、IP アドレス範囲など、ルール内で複数のフィルターを評価できます。ルールを使用する機能ごとに、すべてにアクセスを許可する <default> ルールが自動的に作成されます。このデフォルト ルールを拒否に変更することもできます。

<default> ルールは、他のルール内の基準とフィルターを満たさないすべてのユーザーまたは接続を網羅します。

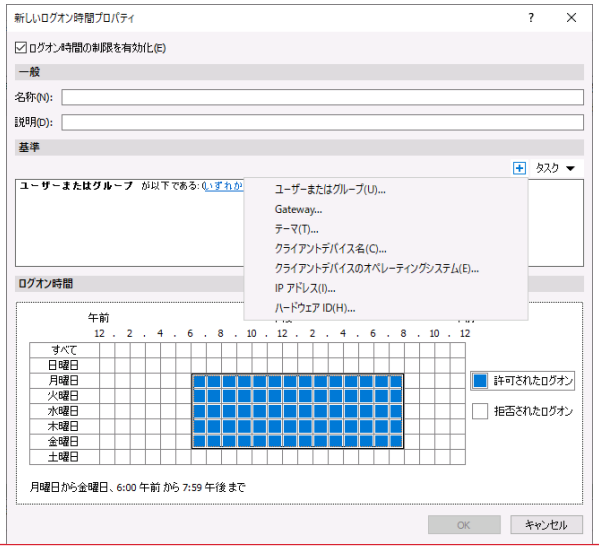
ルールは、リソースに対して上から下にリストされている順序で評価され、一番下が <default> になります。リストを適切に配置し、テストして、希望どおりに適用されることを確認します。管理者が選択できるチェックボックスを提供することで、複数のルールを簡単に設定できます。プロファイル コンテナーに保存するフォルダーや保存しないフォルダーを構成することもできます。ルールの評価はその時点で停止し、他のルールは評価されません。

コネクションとセッション

ルールの用途の 1 つは、ログオン時間の設定と適用です。ルールを使用すると、ユーザー名とグループ、テーマ、IP アドレス範囲などに基づいて、ユーザーのさまざまなログオン時間を設定できます。このルールは管理コンソールの左ペインの[接続]の[ログオン時間]タブで設定します。

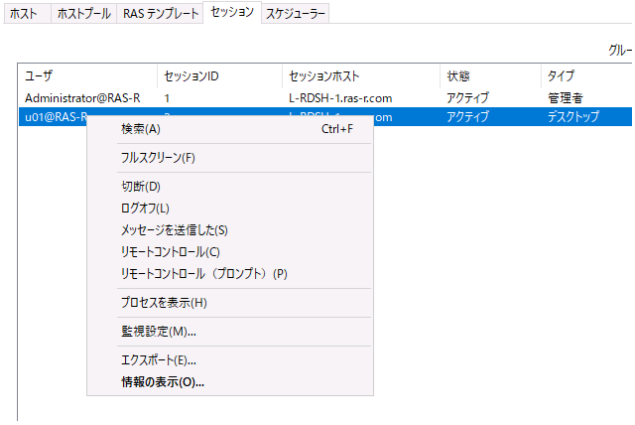
ユーザーがオフィスにいる場合はより長い時間アクセスを許可し、オフィス内から接続していない場合はより短い時間アクセスを許可できます。ログオン時間により、管理者は許可された時間が経過したときにユーザーを強制的にログオフすることもできます。

- Parallels Client が許可されたログオン時間外に接続できないようにする: このオプションを選択すると、Parallels Client はサイトで公開されているリソースに接続できなくなります。
- 時間が経過したらユーザー セッションを切断する: このオプションを選択すると、セッションが切断されることをユーザーに通知します。このオプションを選択すると、以下の設定を指定できます。
  - 切断前にユーザーに通知する: クライアントがファームから切断される前に Parallels RAS がユーザーに通知する時間。
  - ユーザーがセッション時間を延長できるようにする: このオプションを選択すると、ユーザーがセッションを延長できるようになります。



セッション (または複数のセッションを同時に) を管理するには、1 つ以上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アクションから選択します。

- 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：[メッセージの送信] ダイアログが開き、セッション所有者にメッセージを入力して送信できます。
- 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 コントロールします。接続を確立するには、現在の RAS コンソール管理者のドメインまたはローカル Windows アカウントの資格情報 (ユーザーがこのコンピューターにログインするために使用した資格情報) が使用されます。現在のユーザー (特にローカル Windows ユーザーの場合) は、リモート コンピューターへの接続を許可されていない可能性があることに注意してください。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 (以下で説明) を使用します。重要な情報については、以下のユーザー セッションのリモート コントロールのサブセクションも参照してください。
- リモート コントロール (プロンプト)：上記と同じですが、資格情報の入力を求められます。現在のユーザー資格情報を使用してセッションを制御できない場合は、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および管理します



SAML、SSOとセキュリティ

SAML

セキュリティ アサーション マークアップ言語 (SAML) は、ID プロバイダーとサービス プロバイダー間で認証情報を交換するための標準です。SAML 認証は、集中型 ID プロバイダー (IdP) がユーザー認証を実行し、サービス プロバイダー (SP) は認証結果に基づいてアクセス制御の決定のみを行うシングル サインオン メカニズムです。

SAML 認証を使用する主な利点は次のとおりです。

- サービス プロバイダーは独自のユーザー データベースを維持する必要がありません。ユーザー情報は、ID プロバイダー側の集中型データベースに保存されます。ユーザーを追加または削除する必要がある場合は、単一のデータベースでのみ行う必要があります。
- サービス プロバイダーはユーザーを自分で検証する必要がないため、プロバイダー側で安全な認証および承認を実装する必要はありません。
- シングル サインオンとは、ユーザーが一度ログインすれば済むことを意味します。
- それ以降のサインオン (ユーザーが別のアプリケーションを起動した場合) はすべて自動的に行われます。
- ユーザーはサインイン時に資格情報を入力する必要はありません。
- ユーザーはパスワードを覚えて更新する必要がありません
- 弱いパスワードはありません

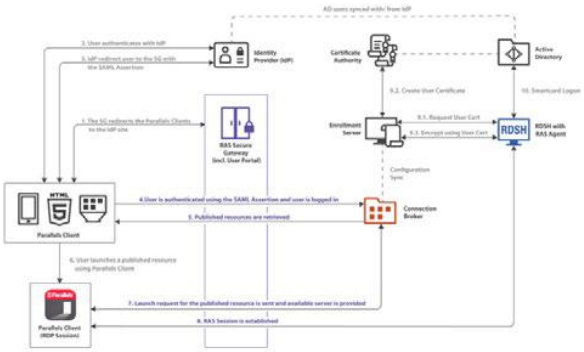
前提条件

Parallels RAS で SAML を構成するには、次のものが必要です:

- 次の 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: 認証されたユーザーに代わって RAS 登録サーバー (ES) を介して証明書を登録するために使用されます。
  - NLA ユーザー: RD セッション ホストや VDI ゲストとの NLA 接続を開始するために使用されます。
- 必要な権限と委任については、Active Directory ユーザー

アカウントの構成を参照してください。Azure Active Directory ドメイン サービス (AADDS) は、SAML SSO での使用がサポートされていないことに注意してください。

- 次のテンプレートを含む Microsoft エンタープライズ証明機関 (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
- Azure、Okta、Ping Identity、Gemalto SafeNet などのサードパーティ ID プロバイダー (IdP)。ユーザー アカウントはここに保存されます。IdP のユーザー アカウントは、Microsoft Active Directory 環境と同期する必要があります。ユーザーを適切に同期する方法については、プロバイダーにご相談ください。
- ドメイン コントローラにはドメイン コントローラ証明書が必要です。
  ドメイン コントローラの証明書はスマート カード認証をサポートする必要があります。証明書は、ドメイン コントローラ認証という Microsoft CA 証明書テンプレートを使用して作成されます。手動で作成されたドメイン コントローラ証明書は機能しない可能性があります。「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た場合は、ドメイン コントローラ証明書を再作成する必要があります。RD セッション ホストと VDI に、信頼されたルート証明機関ストアに CA によって発行されたルート証明書があることを確認してください。
- RD セッション ホストおよび/または VDI ワークロード (64 ビット OS で実行) を含む Parallels RAS ファーム。
- セキュリティ上の理由から、RAS 登録サーバーは専用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 サーバーである必要があります。
- SAML と RAS 登録サーバーの両方の構成は、RAS 環境内のサイト固有の設定です。
  RAS 管理者には、「サイト情報の表示を許可する」および「サイトの変更を許可する」権限が委任されている必要があります。



図の SAML 認証およびログイン手順は次のとおりです:

1. RAS Secure Gateway が Parallels Client ログイン要求を IdP サイトにリダイレクトします。
2. ユーザーが IdP で認証します。
3. IdP が SAML アサーションを使用してユーザーを RAS Secure Gateway にリダイレクトします。
4. ユーザーは SAML アサーションを使用して認証され、ログインします。
5. 使用可能な RAS 公開リソースのリストが取得されます。
6. ユーザーは公開リソースを選択し、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、使用可能なサーバー上でリソースが開始されます。
8. Parallels RAS セッションが確立されます。
9. ユーザー証明書が処理されます:
10. 証明書が要求されます。
11. 証明書が作成されます。
12. 証明書を使用して暗号化が実行されます。
13. スマートカード ログオン。

セキュリティ

接続が許可されるかどうかを判断するには、ユーザーの資格情報やユーザーのアクセス元の認証だけでは不十分な場合があります。場合によっては、接続が許可される RAS クライアントやバージョンを正確に指定する必要があることもあります。
RAS コンソールで、[接続] > [許可されたデバイス] に移動して、このセキュリティ メソッドを有効にし、接続を許可する RAS クライアントを指定できます。古いクライアントにセキュリティ上の脆弱性があり、それらのクライアントが接続できな

いようにしたい場合や、クライアントのオペレーティング システムがサポートされておらず、悪用される可能性がある場合などです。クライアントのアップグレードが完了し、更新されたクライアントのみが接続していることを確認し、見逃されている可能性のあるクライアントを見つけたい場合もあります。

Administrators：ロールベースのアクセスコントロール

最初に行うべきタスクの 1 つは、必要な操作のみを実行できる権限を持つ管理者を追加することです。

コンソールにログインしたら、左ペインの [管理] タブをクリックします。これにより、右ペインに複数のタブが表示されますが、最初は [アカウント] のデフォルト ビューのままにしておきます。

少なくとも、[管理者] グループと、RAS のインストールに使用したアカウントが [ルート管理] 権限で自動的に設定されているはずです。ルート管理権限では、ファーム全体を管理するためのアクセスが許可されるため、この権限は特定の管理アカウントにのみ割り当てる必要があります。

また、これは他の管理者アカウントを作成できる唯一の権限セットです。

もう 1 つの定義済み権限セットは [上級管理者] です。

これらの権限はルートと同様ですが (上記を除く)、特定のサイトまたはカテゴリに範囲を制限できます。

割り当て可能な 3 番目のロールは [カスタム管理] です。

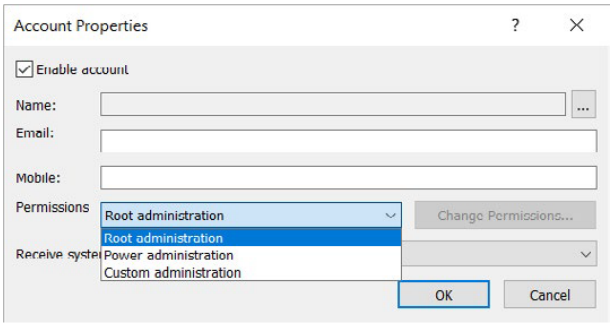
デフォルトでは、これをアカウントまたはグループに割当てても権限はまったく付与されず手動で構成する必要があります。

カスタムを使用すると、コンソールにログインしたときに、さまざまなユーザーまたはグループが表示および管理できる内容を柔軟に制限できます。たとえば、ヘルプデスクに、特定の公開リソースを表示する権限のみを与え、それらのリソースのユーザー セッションを管理する権限を与えることができます。

ユーザーまたはグループを追加して権限を付与するには、「+」をクリックするとダイアログボックスが開きます。名前フィールドは必須で、「…」をクリックすると、権限を割り当てるドメイン ユーザーまたはグループを見つけることができます。電子メール フィールドとモバイルフィールドはオプションで、システム通知の受信はグループではなくユーザー レベルでのみ変更できます。次に、[許可]で権限のレベルをroot管理、上級者管理者、またはカスタム管理者に設定します。ルートでは権限を変更できません。ルート管理者は常にファーム全体にフル アクセス権を持ちます。上級管理者を選択した場合、権限の範囲を広い意味で変更できますが、細かく変更することはできません。たとえば、管理できるサイトを制限し、サイト内の公開リソースの変更を許可しないようにすることができます。カスタム管理者とは異なり、上級管理者とまったく同じ権限を付与しながら、特定の公開リソースを変更する権限を削除することもできます。

カスタム管理者を作成するときは、最初にコンソール内でグループまたはユーザーを作成する必要があります ([OK] をクリック)、その後、そのグループの権限を変更できます。

初めて権限の変更をクリックすると、表示される画面に、すでに割り当てられている権限の概要が表示されます。エントリをクリックすると、ファーム別、グローバル別、サイト別の権限が表示されます。権限の変更をもう一度クリックすると、権限を変更できるようになります。単にアクセス権を付与しないことから、オブジェクトの完全な管理まで、追加できる権限がいくつかあります。依存関係の権限は自動的に付与されます。カスタム管理者に必要のない RAS コンソールの領域は、そのユーザーがコンソールにログインすると非表示になります。



ポリシーとユニバーサルプリントとスキャニング

ポリシー

ポリシーを使用すると、管理者はファームに接続するユーザーの RAS クライアントを管理できます。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、さまざまな RAS クライアント設定をユーザー デバイスにプッシュして、組織のニーズに合わせ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、ディスプレイ、印刷、スキャン、オーディオ、キーボー

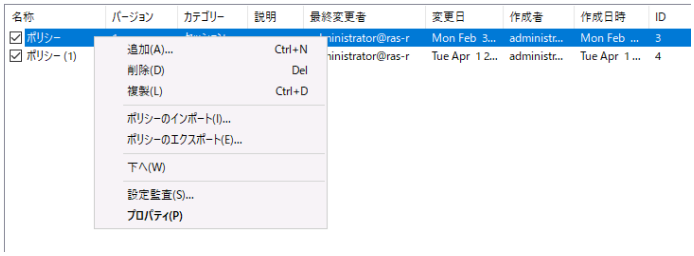
ド、デバイスなどがあります。ポリシーを作成してクライアントデバイスにプッシュすると、デバイスのユーザーはポリシーが適用する設定を変更できなくなります。RAS クライアントでは、これは非表示または無効の接続プロパティとグローバル設定として現れます。適用されるポリシーは、各ポリシーに設定したルールとフィルターによって決まります (前述)。

リマインダー：

- 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 は、ユーザー接続に一致する最初のルールを適用します。
- 他のルールが一致しない場合は、デフォルトのルールが使用されます。

他のルールと一致しない場合は許可、他のルールと一致しない場合は拒否に設定できますが、このルールには条件がありません。

ポリシーは、サポートされているすべてのプラットフォームのすべての RAS クライアントに適用できます。

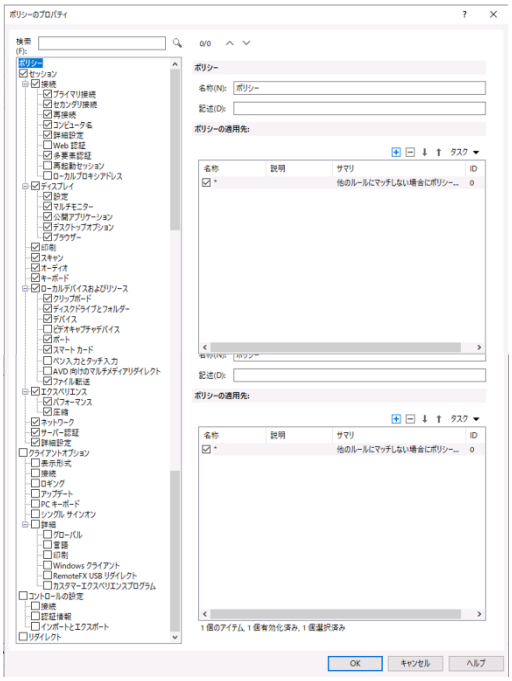


クライアント ポリシーの構造

クライアント ポリシーは、次の 4 つのカテゴリに分かれています。

- セッション - これらの設定は、ユーザー セッションに影響します。たとえば、表示設定、印刷、ネットワークなど。
- クライアント オプション - クライアント設定は、使用中のクライアントとその動作に影響します。たとえば、ログ、自動更新、言語など。
- コントロールの設定 - 管理者は、パスワードを保存するかどうか、ユーザーが接続を追加できるかどうか、設定をインポートおよびエクスポートできるかどうかを制御できます。
- リダイレクト - 管理者は、ユーザー セッションをファーム内の別の Secure Gateway または別のファームにルーティングできます。これを使用して、ユーザー エクスペリエンスを向上させるために、セッションを自分の場所に近いデータセンターにルーティングすることもできます。
    - Secure Gateway に設定されたリダイレクト ポリシーとゲートウェイ基準は、互いに干渉する可能性があります。それに応じて計画およびテストしてください。

ルールとフィルターによって、適用されるポリシー セットが決まります。

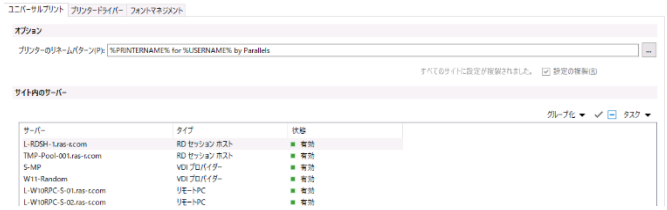


ユニバーサルプリント

多くの組織では、印刷は非常に重要です。

RAS ユニバーサル プリントがデフォルトで有効になっているのはそのためです。

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 エージェント、VDI ゲスト VM エージェント、および RemotePCエージェントとともに自動的にインストールされ、32 ビットおよび 64 ビットのオペレーティング システムをサポートします。



ユニバーサルプリントドライバー

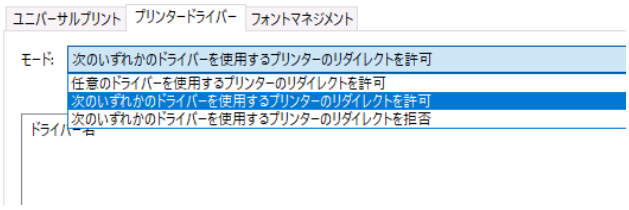
システム管理者は、ユニバーサル プリントのリダイレクト権限を許可または拒否するクライアント側プリンター ドライバーのリストを制御できます。

この機能を使用すると、次のことが可能になります：

- 役に立たないプリンターのリダイレクトによるサーバー リソースの過負荷を回避します。ほとんどのユーザーはすべてのローカル プリンターをリダイレクトすることを選択するため (これが既定の設定です)、実際には使用されないリダイレクトされたデバイスがホスト上に多数作成されます。これは主に、PDFCreator、Microsoft XPS Writer、さまざまな FAX デバイスなどのさまざまなペーパーレスプリンターに関連しています。
- 特定のプリンターによるサーバーの不安定性を回避します。一部のプリンターはホストの不安定性 (スプーラーサービス コンポーネント) を引き起こす可能性があり、その結果、ユーザーは印刷できなくなります。これは、スプーラー サービスがダウンすると、そのホストに接続されているすべてのセッションに影響する RD セッションホストでは特に悪いシナリオです。管理者がそのようなドライバーを「拒否」リストに追加して、印刷サービスの実行を継続できるようにすることが非常に重要です。

以下の点に注意してください:

- 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、プリンター ドライバー名を入力します。
- ドライバー名の比較では大文字と小文字が区別されず、完全一致が必要です (部分的な名前やワイルドカードは不可)。
- このタブで指定した設定は、サイト全体 (個々のサーバーではなく) に影響します。



ユニバーサルプリント設定の管理

サーバーのユニバーサル 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。Ctrl キーと SHIFT キーを押しながらクリックすると、複数のホストを同時に有効または無効にできます。

[タスク] ドロップダウン メニューを使用して [すべて選択] することもできます。

ユニバーサルスキャン

ユニバーサルスキャンは、TWAIN および WIA リダイレクトを使用して、いずれかのテクノロジーハードウェアを使用するホスト上のアプリケーションが、クライアントデバイスに接続され、スキャンできるようにします。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はありません。

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、およびリモートPC エージェントとともに自動的にインストールされます。

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、サーバー機能のデスクトップ エクスペリエンスが必要です。

WIA と TWAIN は別々に管理されます。それぞれに、ユニバーサル スキャン カテゴリの独自のタブがあります。リダイレクトからどちらか一方を無効にするか、両方を有効にするかに関係なく、異なる名前変更パターンを設定できます。

ホストのユニバーサル スキャン サポートを有効または無効にするには、[サイト内のサーバー] リストでホストを右クリックし、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。Ctrl キーと SHIFT キーを押しながらクリックすると、複数のホストを同時に有効または無効にできます。

タスク ドロップダウン メニューを使用して [すべて選択] することもできます。

スキャンの名前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の名前を変更します: %SCANNERNAME% for %USERNAME% by Parallels

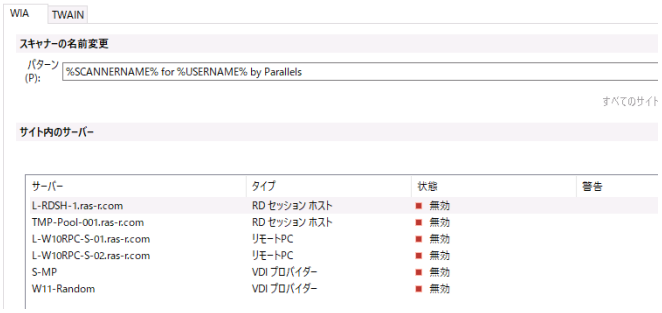
たとえば、SCANNER1 をローカルにインストールしている Lois というユーザーがリモート デスクトップまたは公開アプリケーションに接続すると、そのスキャナーの名前は「SCANNER1 for Lois by Parallels」に変更されます。

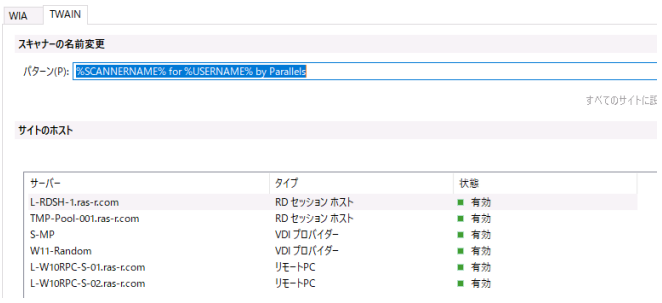
スキャナーの名前変更に使用するパターンを変更するには、[スキャナーの名前変更のパターン入力フィールドで新しいパターンを指定します。定義済みの変数は、入力フィールドの右側にある [...] をクリックしても見つかります。変数を入力するか、メニューで変数をダブルクリックすると、カーソル位置に変数が追加されます。

名前変更に使用できる変数は次のとおりです:

- %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% ― アクティブ セッションの ID。

リスト内のサーバーごとに異なる名前変更パターンを設定できます。





ユーザーポータルとウェブクライアント

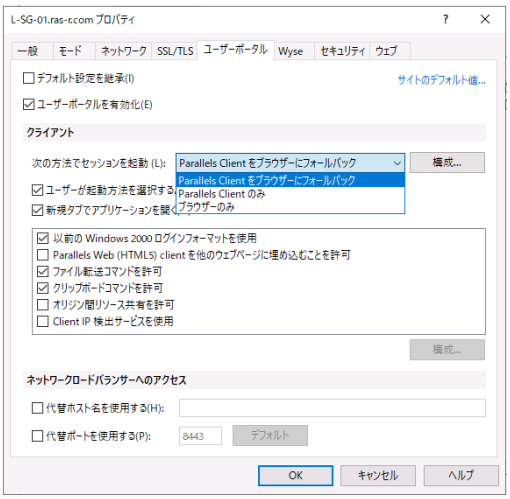
ユーザーポータル

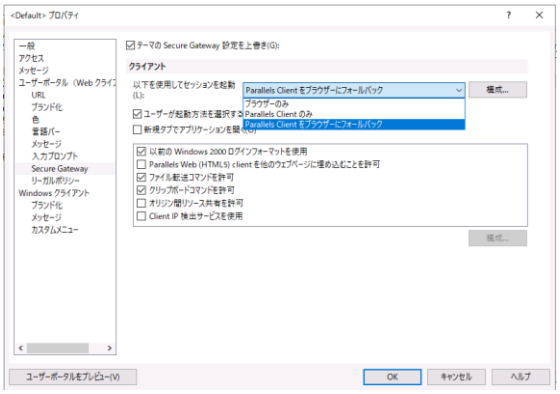
ユーザー ポータルは、RAS Secure Gateway に組み込まれた機能です。ユーザーは手元の自身のデバイスのウェブブラウザーからParallels RAS に接続し、Parallelsウェブクライアントまたはネイティブ クライアントを使用して公開されたリソースを利用することができます。ウェブクライアントはネイティブの RAS クライアントと同様に動作しますが、ユーザーのコンピューターやデバイスに追加のソフトウェアをインストールする必要はありません。ユーザーに必要なのは、HTML5 対応のウェブブラウザーだけです。

ユーザーがユーザーポータルに接続すると、ウェブクライアントを使用してアプリケーションを起動するか、ネイティブにインストールされたクライアントを使用して起動するかを選択できます。このオプションは削除でき、ユーザーはウェブクライアントまたはネイティブ クライアントのいずれかを使用するように強制することも可能です。

これを行うには、次の 3 つの方法があります。

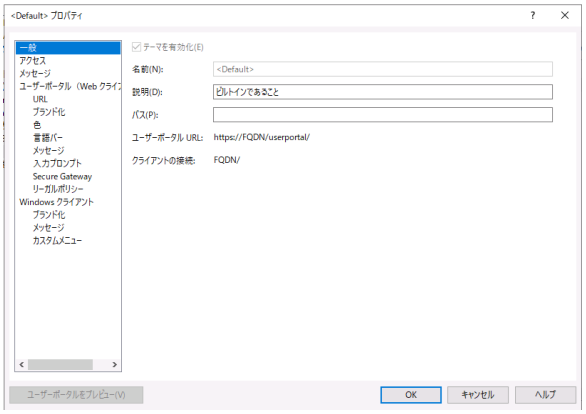
- サイト レベル
- ユーザー ポータルをホストする Secure Gateway
- テーマ





Parallels RAS のテーマは、次の操作を実行できる機能です：

- 特定のユーザー グループにテーマへのアクセスを許可しながら、これらの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 RASクライアント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 ブランディングを実装できます。この機能は、RASウェブクライアントおよびWindows用のParallels RASクライアントでのみ使用できます。



ユーザー ポータル (Web クライアント) カテゴリでは、ユーザーポータルのテーマ設定を構成できます。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。

- URL: 作成された各テーマには、独自の一意の名前が必要です。この名前は、ユーザーがログイン ページにアクセスし、ポータル ページに URL を追加する方法でもあります。
    - たとえば、Theme-S1 というテーマが作成された場合、ユーザーはブラウザーのアドレス バーに次のように入力する必要があります:
      https://<hostname>/Theme-S1 または
      https://<hostname>/userportal/?theme=<Theme-S1>
      どちらも有効です。
- ブランド化: ポータルページを会社のブランディングでカスタマイズできます。
- 色: ヘッダー、フッター、ボタンなどのさまざまな要素の色を選択し変更できます。
- 言語バー: ポータル ページの言語セレクターに表示される言語を選択できます。
- メッセージ: 表示されるログオンごとのカスタム メッセージを作成します。これは、前に指定した既定のメッセージを上書きします。
- 入力プロンプト: テキスト フィールドに入力する必要がある内容をユーザーに示すヒントです。たとえば、user@domain はログイン フィールドで薄い灰色で表示されます。
- Secure Gateway: デフォルトの Secure Gateway ユーザー ポータル設定を上書きする機能。
- リーガルポリシー: 承認する必要がある Cookie の同意とエンド ユーザー ライセンス契約です。

ロードバランス

セッションロードバランシング

RAS でのロードバランスについて議論する場合、通常は高可用性負荷分散 (HALB) アプライアンスを使用して、着信ユーザーセッションまたは Secure Gateway への着信要求の負荷分散を行います。このセクションでは、前者に焦点を当てます。
着信ユーザーセッションのロードバランスは、Connection Brokerによって実行されます。ユーザーが RAS クライアントからアプリケーションまたはデスクトップを開くと、Connection Brokerは、そのセッションがどのホストを使用するように指示されるかを決定します。サイトに複数の

Connection Brokerがある場合、Connection Brokerは、この情報を相互に共有して、正しくロードバランスが行われるようにします。

Connection Brokerがセッションの送信先を決定する方法は 2 つあります。管理者は、リソースベースまたはラウンド ロビンのいずれかを選択できます。

- リソース ベース。サーバーのビジー状態に応じて、セッションをサーバーに分配します。新しい着信セッションは常に、最もビジーでないサーバーにリダイレクトされます。
- ラウンド ロビン。セッションを順番にリダイレクトします。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びサーバー 1 にリダイレクトされます。

ロードバランスオプションは、RAS コンソールのロードバランスカテゴリから構成できます。

サイトで複数のサーバーが使用可能な場合、ロードバランスはデフォルトで有効になります。リソース ベースがデフォルトの方法ですが、[方法] ドロップダウン リストから変更できます。

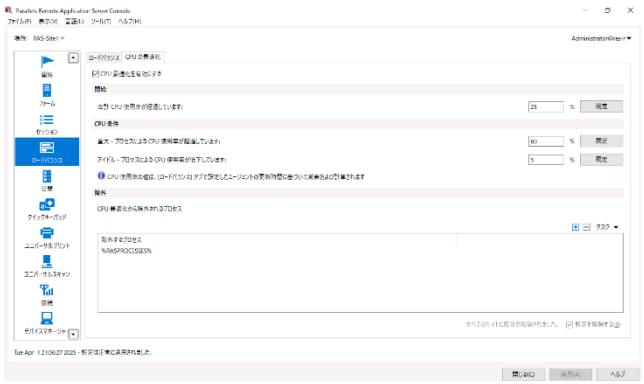
リソースカウンターの設定

リソースベースのロード バランシングでは、次のカウンターを使用して、セッションがルーティングされるホストを決定します。

- ユーザー セッション: セッション数が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: 空き RAM と使用済み RAM の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: 空き CPU 時間と使用済み CPU 時間の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 バランサーはカウンター比率を合計し、最も有利な合計比率を持つサーバーにセッションをリダイレクトします。

CPU 最適化機能を使用すると、要件に応じて CPU ロード バランシングを最適化できます。設定されている場合、CPU ロード バランサーは、CPU 使用率が指定された秒数にわたって指定された値を超えると、プロセスの優先度を下げます。プロセスが特定のパーセンテージを下回って特定の秒数にわたって実行されている場合、ロード バランサーは優先度を元のレベルに戻します。



CPU 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、以下の説明に従って値を指定します。

開始: システム全体の使用状況に基づいて、CPU 最適化をいつアクティブ化するかを指定します。

CPU条件

プロセスごとにしきい値を指定して、どのプロセスの優先度を下げるか (しきい値以上)、およびプロセスを通常どおり優先度付けできるか (しきい値未満) を決定します。

ここでは、[重大]の値と[アイドル]の値を指定できます。CPU ロード バランサーは、これらの値に応じて他の優先度を調整します。

CPU 使用率の値は、[ロード バランス] タブの[構成]で構成されたエージェント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。デフォルトでは、RAS プロセスは除外されます。一部のソフトウェアは最適化を悪意のあるものと解釈するため、ウイルス対策ソフトウェアやセキュリティ ソフトウェアの動作にも注意する必要があります。

重大、アイドルの値が不規則な場合、問題が発生する可能性があります (構成が誤っているためにプロセスがアイドル状態に設定される場合があります)。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。ログを使用してしきい値を確認します。Windows で CPU 使用率パフォーマンス カウンターを確認できます。

- 注: 重大、アイドルのしきい値は、プロセスの最も高いCPU使用率 (絶対 CPU 使用率ではない) に基づいて計算されるため、優先順位を変更してもこの値はログに反映されません。
- 絶対 CPU 使用率は合計 CPU 使用率と同じです。たとえば、2 つのプロセスがそれぞれ 30% 使用している場合、合計 CPU 使用率は 60% になります。 CPU ロードバランサが起動するときの使用率しきい値は 25% (デフォルト) です。
- プロセスの最も高いCPU使用率は、CPU を最も多く使用しているプロセスの CPU 使用率です。たとえば、プロセスが3つあり、そのうち2つが10%、3つ目が40%使用している場合、最高CPU使用率は40%です。

HALB

Parallels RAS の高可用性ロード バランシング (HALB) は、RAS Secure Gateway の負荷を分散する機能です。

ロード バランサーは、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構成された、事前構成された仮想マシンである Parallels HALB アプライアンスに組み込まれています。

Parallels HALB アプライアンスは、次のハイパーバイザーで使用できます：

- Microsoft Hyper-V
- VMware

他のハイパーバイザーも使用できますが、サポートはベスト エフォートで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でネイティブにサポートされている Open Virtualization Platform (OVA) 形式を使用します。

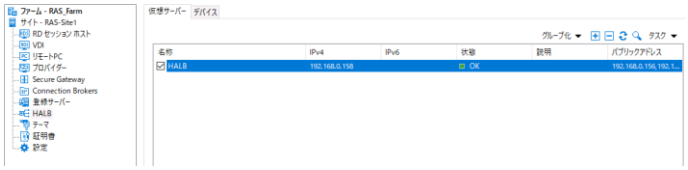
HALB は、Parallels RAS のサイト レベルで展開されます。サイトごとに複数の HALB 構成を持つことができ、これらは仮想サーバーと呼ばれます。各仮想サーバーには独自の IP アドレス (仮想 IP または VIP と呼ばれる) があり、実際の負荷分散を実行する 1 つ以上の HALB アプライアンス (仮想サーバーのコンテキストでは HALB デバイスとも呼ばれます) が割り当てられます。 HALB 仮想サーバーは、HALB デバイスの仮想表現です。HALB デバイスが適切に構成されている場合、HALB デバイスへのトラフィック分散を提供します。

特定の仮想サーバーの IP アドレスはクライアント ソフトウェアの唯一の連絡先であるため、冗長性を確保するために仮想サーバーごとに少なくとも 2 つの HALB デバイスを用意することをお勧めします。

仮想サーバーに割り当てられた複数の HALB デバイスは、1 つがプライマリとして機能し、他のデバイスがセカンダリとして同時に実行できます。仮想サーバーに割り当てられた HALB デバイスの数が多いほど、エンド ユーザーがダウンタイムを経験する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、このアドレスはセカンダリ 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、クライアント接続に同じ IP アドレスを使用してその役割を引き継ぎます。



公開とアプリケーションパッケージ

公開

RAS コンソールからリソースを公開するのはとても簡単です。リソースを追加する場合は、[公開] カテゴリをクリックし、コンソールの下部にある [追加...] ボタンをクリックすると、リソースの公開手順を説明するウィザードが起動します。

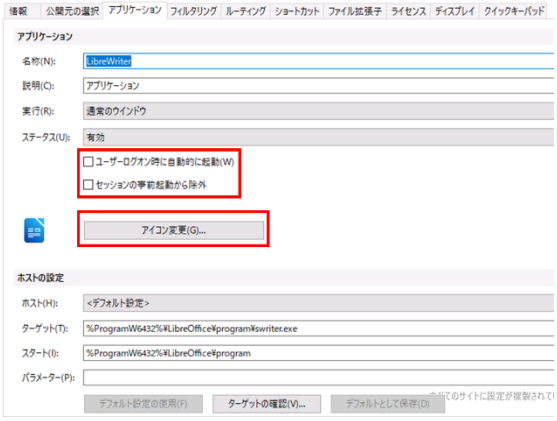
リソースを公開した後、コンソールでそのリソースをクリックすると、リソースに関する現在の情報が表示されますが、公開されたリソースのさまざまな設定を変更することもできます。リソースを公開するサイトを変更したり、公開元のサーバー、説明などを変更できます。

リソースには構成可能なさまざまな設定がありますが、すべてのリソースに共通する定数がいくつかあります。

- 情報: リソースの構成の概要を表示します
- サイト: リソースを公開するサイト
  リソースは複数のサイトから公開できます
- 公開元: リソースを配信しているサーバーまたはホストです
- フィルタリング: リソースにアクセスできるユーザーと対象を決定する強力なフィルターを作成します
- ルーティング: 優先ルーティングを有効にして構成し、セッションに最適な接続を指定します
- ショートカット: アプリケーションショートカットがユーザーデバイスのどこに表示されるかを指定できます

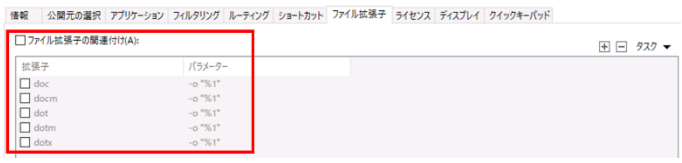
アプリケーション公開の設定

公開されたアプリケーションは、さまざまなタブで使用可能なオプションを使用して構成できます。管理者は、[アプリケーション] タブから、ユーザーのログイン時にアプリケーションを自動的に起動するかどうか、セッションの事前起動機能から除外するかどうか、ユーザーに表示されるアイコンを変更するかどうかを指定できます。



前述のように、ショートカットはユーザーのエンドポイントの複数の場所に配置できます。ショートカットは、デスクトップ、スタート フォルダー、カスタム フォルダー、自動スタート フォルダーに作成できます。

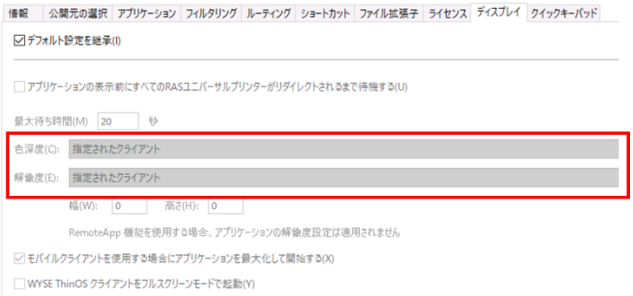
公開アプリケーションでエンドポイントにローカルな特定のファイルタイプを処理する場合は、ファイル拡張子タブを使用して構成します。たとえば、エンドポイントに MS Word がインストールされていないが、ユーザーは MS Word ファイルを開いて編集できる必要があります。[.DOC]、[.DOCX] などのファイル拡張子の関連付けを許可すると、ユーザーは公開されたバージョンの MS Word で MS Word ファイルを開くことができます。ソフトウェアのローカル コピーは必要ありません。



管理者が公開アプリケーションの色深度と解像度を強制する必要がある場合があります。これは、[ディスプレイ] タブで行い

ます。デフォルトでは、アプリケーションはエンドポイント クライアントから渡された設定を使用します。

※注：日本語コンソールではV20では[指定されたクライアント]と表示されていますが、誤訳です



フォルダー

管理者は、[公開リソース] ペインにフォルダーを作成できます。フォルダーは公開リソースを整理するために使用され、フォルダー レベルでフィルタリングとルーティングを構成できます。フォルダーには次の2つの種類があります。

- 管理目的のフォルダー。この種類のフォルダーは、Parallels RAS 管理者 (Parallels RAS Console のユーザー) 向けです。Parallels RAS Console で公開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 デバイスの Parallels Client 画面には表示されません。これらのフォルダーは、管理者が公開リソースをより効率的に管理するために使用されます。
- 通常のフォルダー。これらのフォルダーは、上記の管理フォルダーに似ていますが、ユーザー デバイスのRASクライアント画面に表示されます。通常、これらのフォルダーは、公開リソースをタイプ (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) 別にグループ化するために使用します。

フォルダーはどちらか一方であり、両方のタイプにすることはできません。

フォルダーの種類を変更するには、フォルダーをクリックしてから [フォルダー] タブをクリックし、[管理目的で使用する] の横にあるボックスをオンまたはオフにします。

アプリケーションパッケージ

Parallels RAS 19 は、MSIXアプリアタッチテクノロジーに基づいた、新しい最新のアプリケーション配信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 アプリ アタッチは、アプリケーション (コンテナー化された MSIX パッケージ) をユーザー セッションに動的にアタッチできる Microsoft のアプリケーション階層化ソリューションです。

アプリケーションをオペレーティング システムから分離すると、適切なユーザーに適切なアプリケーションを提供することで、より高度な制御が可能になります。

前提条件

- RD セッション ホストまたはホストとしての VM。
- MSIX アプリ アタッチには、Windows Server 2022、Windows 11、Windows 10 バージョン 2004 以降を実行しているホストが必要です。
- MSIX イメージが保存されるネットワーク共有。

ストレージ要件と推奨事項については、https://docs.microsoft.com/en-us/azure/virtual-desktop/app-attach-file-share で詳しく説明されています。

- すべてのホスト (コンピューター アカウント) には、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

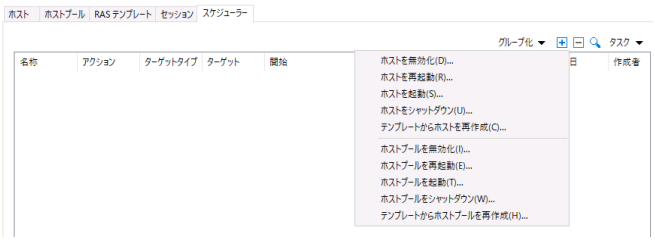
電源管理とテナントブローカー

電源管理

RDSHスケジューラー

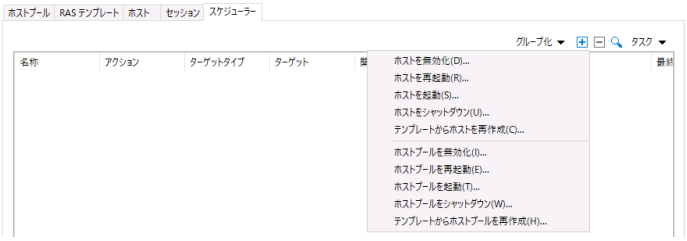
RD セッション ホスト ビューの [スケジューラ] タブでは、スケジュールに従ってテンプレートに基づいてサーバーおよびサーバー グループを再起動したり、一時的に無効にしたりできます。

- サーバーを無効にする
- サーバー グループを無効にする
- サーバーを再起動する
- サーバー グループを再起動する
- サーバーを起動する
- サーバー グループを起動する
- サーバーをシャットダウンする
    - サーバー グループをシャットダウンする



VDI スケジューラ

- スケジューラ タブでは、指定した時間に個々のゲスト VM またはプールを無効化、再起動、起動、シャットダウンできます。個々のゲスト VM のタスクをスケジュールできるのは、テンプレートベースでない場合のみであることに注意してください。
- ゲスト VM およびプール内のゲスト VM を無効化
- ゲスト VM およびプール内のゲスト VM を再起動
- プール内の VM およびゲスト VM を起動
- ゲスト VM およびプール内のゲスト VM をシャットダウン



テナントブローカー

概要

Parallels RAS は、Parallels RAS Tenant Broker を追加することで、真のマルチテナント アーキテクチャを実現できます。これにより、組織は、クライアントデータを分離したままコストを削減しながら、同じ RAS インフラストラクチャのコンポーネントを異なるテナント間で共有できます。

RAS マルチテナント アーキテクチャは、サービス プロバイダーと組織に次の利点を提供します:

- RAS セキュア ゲートウェイと高可用性ロード バランサー (HALB) の数を減らし、リソースの使用と統合を最大化することで**コストを節約**します。
- 新しいテナント/顧客の**オンボーディングを高速化**します。
- マルチテナント環境の**集中管理を簡素化**します。
- 共有インフラストラクチャによるコスト スケーリングを可能にすることで、あらゆる規模の組織の運用コストを削減し、**市場範囲を拡大**します。

ブローカーの動作に関する情報:

- テナントは、個別のファームまたはサイトとして展開されます。個別のファームとして展開されたテナントは完全に独立しており、互いに通信することはありません。
  テナントがサイトとして展開されている場合、すべてのサイトはテナント ブローカーに個別に参加する必要があります。
- 共有リソースには、RAS セキュア ゲートウェイ (ユーザー ポータルを含む) と高可用性ロード バランサー (HALB) が含まれます。
- テナント ファームには、独自の RAS セキュア ゲートウェイと HALB は必要ありません。ただし、内部接続に必要な

場合は、ゲートウェイと HALB を使用した展開が可能です。

たとえば、内部接続と外部接続に異なるポリシーがある場合は、ローカル ユーザーにサービスを提供するためにゲートウェイと HALB をインストールする必要があります。

テナント ブローカーには独自の RAS コンソールが付属しており、共有リソース、テナント オブジェクト、証明書の管理、テナント パフォーマンスの監視、標準的な RAS 管理タスクの実行が可能です。

テナント ブローカーにはライセンスは必要ありません。ライセンスはテナント レベルで管理されます。

テナント ファームは、従来の Parallels RAS ファームと同じように展開されます。唯一の違いは、ファームをインストールするときに、ファームに RAS セキュア ゲートウェイをインストールする必要がないことです。

テナント ファームが稼働したら、その中の 1 つ以上のサイトをテナント ブローカーに参加させることができます。

テナントに参加するには、(1) 招待ハッシュを使用する、または (2) 共有秘密キーを使用するという 2 つの方法があります。この 2 つの違いは次のとおりです。

- 招待ハッシュ。招待ハッシュは、単一のテナントをテナント ブローカーに参加させるために使用できる、自動的に生成される暗号化された文字列です。招待ハッシュは、テナント ブローカー コンソールで作成されるテナント オブジェクトのプロパティです。

  ハッシュをテナント ファーム管理者に電子メールで送信すると、管理者はそれを使用してテナント ブローカーに参加できます。招待ハッシュは、一度使用すると、他のテナントが再度使用することはできません。

- 共有秘密キー。共有秘密キーは招待ハッシュに似ていますが、重要な違いが 1 つあります。共有秘密キーは、無制限の数のテナントに参加するために使用できます。テナント オブジェクトは、テナント ブローカーの秘密キー用に事前に作成されません。代わりに、キーを使用してテナントに参加したときにオブジェクトが作成されます。

  無制限に使用できるため、共有秘密キーにアクセスできるのはテナント ブローカー管理者のみです。

  このシナリオは、複数のテナントがあり、すべて同じテナント ブローカー管理者によって管理されている場合に役立ちます。