Parallels Remote Application Server

Parallels RAS Reference Architecture

19.3

Parallels International GmbH

Vordergasse 59

8200 Schaffhausen

スイス

Tel: + 41 52 672 20 30

www.parallels.com

目次

第 1 章

はじめに

このガイドは、Parallels® Remote Application Server (RAS) を組織に導入および管理するシステム管理者を対象としています。Parallels RAS とその主要コンポーネントの概要から始まり、これらのコンポーネントの動作の基本原則について概説します。このガイドの主なトピックでは、さまざまな Parallels RAS 展開シナリオについて説明し、図やその他の情報を提供します。このガイドは、Parallels RAS で使用される通信ポートに関する情報と SSL 証明書の使用に関する情報で締めくくられています。

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	更新 1	2022 / 08 / 31
19.0	修正 1	2022 / 09 / 16
19.0	修正 2	2022 / 09 / 30
19.0	修正 3	2022 / 10 / 14
19.1	更新 2	2022 / 11 / 15
19.2	更新 3	2023 / 07 / 06
19.3	初回リリース	2023 / 10 / 17

Parallels RAS とは

Parallels RAS は、あらゆるデバイス、あらゆる場所での Windows アプリケーション公開のマーケット リーダーです。主要なハイパーバイザーおよび Microsoft リモート デスクトップ サービスと連携し、PC、Mac、およびモバイル ユーザーにシームレスなエクスペリエンスを提供すると同時に、セキュリティを強化し、IT コストを削減します。さらに、Parallels RAS は Azure Virtual Desktop をサポートしています。シンプルで、ユーザーが好きなように作業できる自由と柔軟性を備えています。

Parallels RAS を使用すると、Windows、Linux、macOS、iOS、Android、Chrome など、事実上すべてのオペレーティング システムを実行している任意のデバイスからリモート デスクトップとアプリケーションにアクセスできます。ブラウザ ベースの Web Client によるアクセスも可能です。

Parallels RAS の豊富な機能の詳細については、Parallels のウェブサイトからダウンロードできる **Parallels RAS 管理者ガイド**をお読みください。

Parallels RAS ソリューションの利点

サーバー ベースのコンピューティング

管理の削減、可用性の向上、TCO の削減。

簡素化された管理

ユーザーの集中管理、サーバー ベースの OS パッチ管理、アプリケーションの更新とバックアップ。

より高いセキュリティ

すべてのデータは、一元化されたセキュリティとバックアップ管理によりサーバー側に保持されます。マウスクリック、キーボードのキーストローク、およびデスクトップやアプリケーションのスクリーンショットのみがクライアント デバイスとの間で送受信されるため、クライアントでのデータ漏洩、ウイルス、トロイの木馬、およびその他の脆弱性が防止されます。

ハードウェアの独立性

最小限のハードウェア要件で、Windows、Linux、macOS、iOS、Android、Chrome、HTML 5 などを含む、クライアント デバイス上の事実上すべてのプラットフォームをサポートします。

マルチ テナント アーキテクチャと機能

Parallels RAS マルチ テナント アーキテクチャと Parallels RAS Tenant Broker を使用すると、Parallels Secure Gateway や高可用性のロード バランサー (HALB) などのアクセス レイヤーをテナントとサイト間で共有できます。テナント ブローカーは、共有 RAS Secure Gateway と HALB をホストするための個別の RAS インストールです。テナント ファームは、従来の 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、公開済みリソース (RD セッション ホスト、VDI、Azure Virtual Desktop、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 やロード バランサーは不要です。

展開の柔軟性

Parallels RAS は、オンプレミス、クラウドまたはマルチクラウド環境のいずれを使用する場合でも、柔軟なクラウド展開モデルのサポートを提供し、企業が総所有コストを削減しながらさまざまなテクノロジーを活用できるようにします。

簡単にアクセス

従業員、顧客、およびパートナーは、どこからでも、どのデバイスでも follow-me apps とデスクトップを使用して、より簡単に在宅勤務やローミングができます。

拡張された Windows PC ライフサイクル

Windows PC を疑似シンクライアントに変換することにより、ハードウェア交換のコスト削減を実現します。Windows のレガシー オペレーティング システムを引き続き使用して、ネイティブの OS 機能へのアクセスを制限しながら仮想アプリケーションを安全に実行します。さらに、管理者は、ユーザーが PC 上でローカルおよびリモートで実行するアプリケーションを選択できます。

プロアクティブ モニタリング

Parallels RAS レポートは、IT 管理者が潜在的な問題が発生する前に取り組むのに役立ち、一元化された Parallels RAS コンソール上で、リソースとサービスに関するレポートと統計を提供します。

エンド ユーザー サポート

Windows クライアント管理により、クライアント デバイスのシャドーイング (ユーザー セッション制御) とヘルプデスクの電源管理が可能になり、エンド ユーザーによる日常的な支援が容易になります。

Parallels RAS コンポーネント

ファームは、一意のデータベースとライセンスを持つ論理エンティティとして維持される Parallels RAS コンポーネントのコレクションです。

サイトは通常、物理的な場所に基づく管理エンティティです。各サイトは、少なくとも RAS Connection Broker、RAS Secure Gateway、および RD セッション ホスト、仮想化サーバー、および Windows PC にインストールされているエージェントで構成されています。特定のファームに複数のサイトが存在する可能性があります。

Parallels RAS コンソールは、Parallels RAS を管理する管理者向けのデスクトップ アプリケーションです。

Parallels RAS 管理ポータルは、最新の Web ベースの構成および管理ポータルです。管理ポータルは、デスクトップまたはラップトップ コンピューター、あるいはモバイル デバイスを使用して構成や日常のアクティビティを実行する管理者向けに設計されています。

RAS Connection Broker は、公開済みアプリケーションとデスクトップへのアクセスを提供し、アプリケーション トラフィックの負荷を分散します。セカンダリ RAS Connection Broker をサイトに追加することで、高可用性を実現できます。

RAS RD セッション ホスト エージェントは RD セッション ホストにインストールされ、サーバー リソース (アプリケーションとデスクトップ) の公開を可能にします。RAS RD セッション ホスト エージェントは、実行中のサーバーから必要な情報を収集し、それを RAS Connection Broker に送信します。RAS Connection Broker は、それを負荷分散やその他の目的に使用します。

RAS Remote PC Agent は、物理 Windows コンピューターまたは Windows 仮想マシンにインストールされます。これにより、コンピューター リソース (アプリケーションとデスクトップ) の公開が可能になります。RAS Remote PC Agent は、実行中のコンピューターから必要な情報を収集し、それを RAS Connection Broker に送信します。RAS Connection Broker は、それを負荷分散やその他の目的に使用します。

RAS Guest Agent は、仮想マシンのゲスト オペレーティング システムにインストールされます。RAS Guest Agent は、VDI ホストと VDI RD セッション ホストからのリソース公開を可能にし、RAS Connection Broker に必要な情報を収集します。

RAS Provider Agent は、Parallels RAS インフラストラクチャから情報を収集し、ネイティブ API を介してプロバイダを制御します。RAS Provider Agent には 2 つの種類があります。1 つは RAS Connection Broker に組み込まれており、デフォルトで使用できます。Parallels RAS ファーム内の複数のプロバイダを制御するために使用できます。もう 1 つは、プロバイダ ホストに手動でインストールできる個別のコンポーネントです。この場合、そのホストでのみ機能します。組み込みの RAS Provider Agent は、[**libvirt を使用した QEMU KVM**] と [**Nutanix Acropolis**] を除く、Parallels RAS でサポートされている任意のプロバイダで使用できます。これらの 2 つのハイパーバイザーでは、専用の RAS Connection Broker をプロバイダ ホスト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、以下の [**専用の RAS Provider Agent**] を参照してください。

専用の RAS Provider Agent は、Parallels RAS インストーラーからインストールできる個別のコンポーネントです。これは、上記の組み込みの RAS Provider Agent と同じ目的を果たします。違いは、専用の RAS Provider Agent のみを使用して、インストールされているプロバイダを制御できることです。

RAS Secure Gateway は、クライアント デバイスで実行されている Parallels Client ソフトウェアと Parallels RAS の間のプロキシとして機能するサービスです。Secure Gateway は SSL を使用して通信を暗号化します。複数の RAS Secure Gateway は、Parallels HALB を使用して高可用性モードで動作できます。

High Availability Load Balancing (HALB) は、RAS Secure Gateway にロードバランシング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、Hyper-V および VMware で使用できます。複数の HALB 仮想サーバーを構成し、それぞれに異なる仮想 (およびフローティング) IP を割り当てて、同じ RAS サイト内の Secure Gateway へのトラフィックを負荷分散することができます。これにより、管理者は、たとえば、内部アクセスと外部アクセスに異なる Secure Gateway を使用する場合や、異なる支店を使用する場合に、分離アクセス用に仮想サーバーを構成できます。複数の HALB デプロイメントを同時に実行でき、1 つはプライマリとして機能し、他はセカンダリとして機能します。サイトの HALB 展開が多いほど、エンド ユーザーがダウンタイムを経験する可能性は低くなります。プライマリおよびセカンダリ HALB 展開は、共通または仮想 IP アドレス (VIP) を共有します。プライマリ HALB の展開が失敗した場合、セカンダリがプライマリにプロモートされ、代わりに使用されます。HALB 仮想アプライアンスはロードバランシングにソース IP を使用するため、クライアント デバイスのソース IP を保持するように、仮想アプライアンスの前にファイアウォールまたはルーターを設定する必要があります。

Parallels Device Manager は、管理者が Windows コンピューターを管理できるようにする Parallels RAS 機能です。Windows 7 以降がサポートされています。

Parallels Desktop の交換は、Parallels Device Manager のサブ機能です (上記を参照) 。これにより、管理者は、オペレーティング システムを交換することなく、標準のデスクトップをシンクライアントに似た限定されたデバイスに変換できます。

RAS Enrollment Server は、SAMLSSO 認証機能の重要なコンポーネントです。これは、Microsoft 認証局 (CA) と通信して、Parallels RAS 環境での SSO 認証のために、ユーザーに代わってデジタル証明書を要求、登録、および管理します。

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、Windows 10 および Windows 11 エンタープライズ マルチセッション ホストの新製品を含む RD セッション ホストおよび VDI へのアクセスを提供します。Parallels RAS 18 は、Parallels RAS の既存の技術機能に加えて、Azure Virtual Desktop ワークロードを統合、構成、保守、サポート、およびアクセスする機能を提供します。

Microsoft FSLogix プロファイル コンテナは、移動プロファイルおよびユーザー プロファイル ディスク (UPD) の後継として推奨されるプロファイル管理ソリューションです。非永続的な環境でユーザー 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 エクスペリエンスを提供するように設定されています。

シナリオの配置図の理解

用語と略語

シナリオの配置図には、次の表で説明する用語と略語が含まれています。

CB	RAS Connection Broker。
SG	RAS Secure Gateway (ユーザー ポータルを含む) 。
Private SG	Private RAS Secure Gateway (ダイレクト クライアント接続に使用) 。
RDSH, RDS host RDSH Agent	RD セッション ホスト (旧ターミナル サーバー) 。 RD セッション ホストにインストールされた RAS RD セッション ホスト エージェント。
Remote PC	RAS Remote PC Agent がインストールされたリモート Windows コンピューター。
VDI	仮想デスクトップ インフラ (仮想マシンを実行しているハイパーバイザーを備えた VDI ホスト) 。各仮想マシンには、RAS Guest Agent がインストールされている必要があります。
HALB	高可用性ロード バランス。RAS Secure Gateway に負荷分散を提供するアプライアンスです。
Converted PC	シンクライアントのような OS に変換された Windows を搭載した PC。
Enrollment Server	RAS 登録サーバー (SAML SSO 認証機能の重要な部分) 。

アイコン

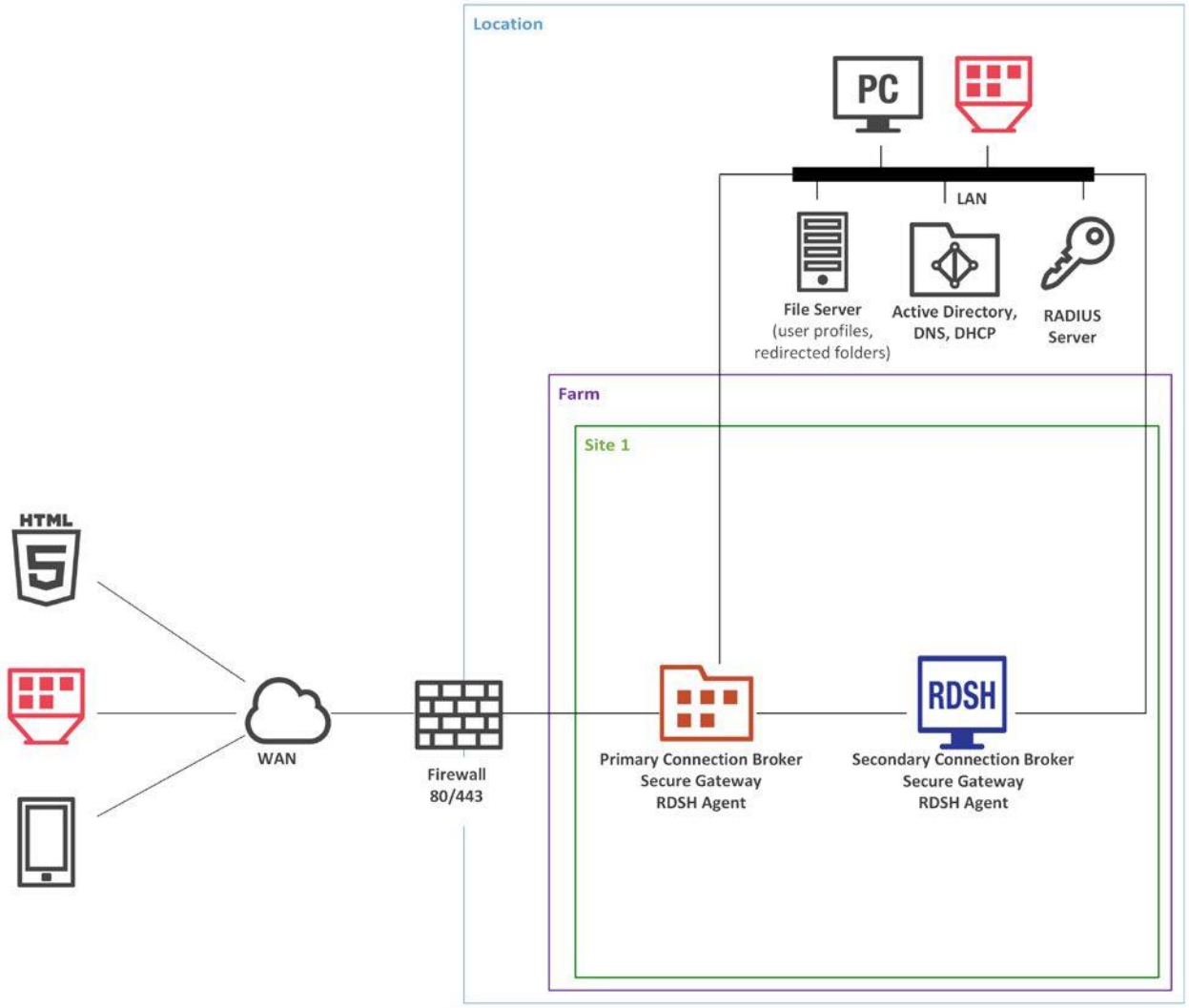
次の表で、シナリオの配置図で使用されるアイコンについて説明します。

Parallels RAS サーバー コンポーネント	
	RAS Connection Broker をホスティングしているサーバー。展開によっては、他の Parallels RAS コンポーネントをホストする場合もあります。
	RAS Secure Gateway (ユーザー ポータル含む) は、セキュア (SSL) なクライアント接続に使用されます。
	プライベート RAS Secure Gateway。ダイレクト クライアント接続に使用されます。
	RAS RD セッション ホストエージェントがインストールされた RD セッション ホスト。
	RAS Remote PC Agent がインストールされたリモート Windows コンピューター。以下で説明する変換済み PC (赤い色の同様のアイコン) と混同しないよう注意してください。
	仮想デスクトップ インフラストラクチャ (仮想マシンを実行するハイパーバイザーを備えた VDI ホスト) 。各仮想マシンには、RAS Guest Agent がインストールされている必要があります。
	高可用性ロード バランス。RAS Secure Gateway に対し、負荷分散を提供するアプライアンスです。
Parallels RAS クライアント デバイス	
	Parallels Client がインストールされたデスクトップ コンピューター (Windows、Linux、Mac) 。

	シンクライアントのような OS に変換された Windows を搭載した PC。上記のリモート PC (オレンジ色の同様のアイコン) と混同しないよう注意してください。
	キオスクモードが有効になっている変換された PC (上記と同じ) 。
	HTML 5 対応の Web ブラウザ。
	モバイル デバイス (iOS、Android) 。
その他のコンポーネント	
	Active Directory、DNS、および DHCP サーバー。
	Microsoft SQL Server データベース。
	RAS Reporting と SQL Server Reporting Services (同じサーバーにインストールされています) 。
	RADIUS サーバー (二段階認証に使用) 。
	ユーザー プロファイルとリダイレクトされたフォルダーを保存するためのファイル サーバー。
	ファイアウォール (ポート 80 と 443 は開いています) 。
	オンプレミス VPN ゲートウェイ。
	RAS 登録サーバー。
	Azure ロード バランサーまたは Azure VPN ゲートウェイ。

図のレイアウト

図のレイアウトを理解するために、次のサンプル図を検討してください。



図の左側には、Parallels RAS に接続できるクライアント デバイスが表示されています。上記の例のクライアントは以下の通りです (上から下に説明します) 。

- HTML 5 対応の Web ブラウザ
- キオスクモードで実行されている変換された Windows PC
- モバイル デバイス (iOS、Android)

[**Location**] の枠は、オフィスなどの物理的な場所を示します。

煉瓦造りの壁で表される [**Firewall**] は、ネットワーク保護を担当します。シナリオの説明に DMZ またはファイアウォールに関する詳細が含まれていない場合、ネットワーク保護の実装方法を決定するのは管理者またはネットワーク セキュリティ担当者の責任であることに注意してください。

[**Farm**] の枠は、1 つ以上のサイトで構成される Parallels RAS ファームを表します。

[**Site 1**] の枠は、個々のサーバーとコンポーネントを備えたサイトを表します。上記の例では、サイトに RAS Connection Broker (CB)、RAS Secure Gateway (SG)、および RAS RD セッション ホスト エージェントがインストールされた 1 台のサーバーがあります。

[**LAN**] の線は、次のコンピューターとサーバーが接続されているローカル エリア ネットワークを表します。

- デスクトップ コンピューター
- キオスクモードで実行されている変換された Windows PC
- ファイル サーバー
- Active Directory、DNS、および DHCP サーバー
- RADIUS サーバー

アイコン間の線は、個々のコンポーネント間の通信チャネルを示します。

[**インストールに関する注意事項**] セクションでは、対応するサーバーに 1 つまたは複数のコンポーネントをインストールする方法について説明します。Parallels RAS サーバー コンポーネントのインストールには、次のインストール方法が使用されます。

- **Parallels RAS インストーラー (標準インストール)**：これは、アプリケーションをインストールするために Windows で実行する標準の MSI インストーラー パッケージです。
- **Windows インストーラー (カスタム インストール)**：これは上記と同じタイプのインストーラーですが、[カスタム] インストール タイプを選択する必要があります。これにより、インストールするコンポーネントを選択できます。
- **プッシュ インストール**：コンポーネントは、MSI インストーラー パッケージをリモートサーバーにプッシュし、そのコンポーネントに無人インストールを実行することにより、RAS コンソールからリモートでインストールされます。
- **仮想アプライアンス**：VMware または XenServer 用に事前構成された仮想アプライアンス。以下の URL から Parallels ウェブサイトにアクセスして、使用しているハイパーバイザー用の仮想アプライアンスをダウンロードできます。https://www.parallels.com/jp/products/ras/download/links/

Parallels RAS の基本的な概念

ユーザーが Parallels Client から Parallels RAS に接続すると、公開済みリソース (アプリケーション、デスクトップ、ドキュメントなど) が表示されます。ユーザーがリソースを選択して起動します。システムはユーザー要求を自動的に負荷分散し、最も負荷の少ないホストからリソースを起動します。その後、ユーザーには RDP プロトコルを介してシームレスにリソースが表示されます。

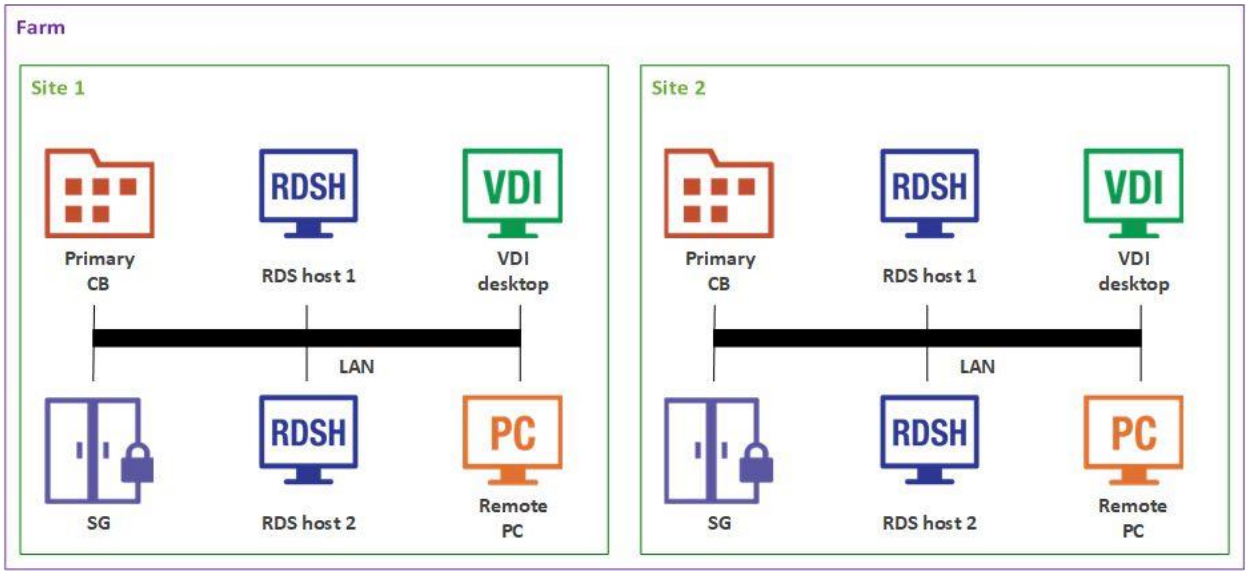
Parallels RAS ビルディングブロックは次の通りです (詳細な説明については、前のセクションを参照してください) 。

- Farm (ファーム)
- Site (サイト)

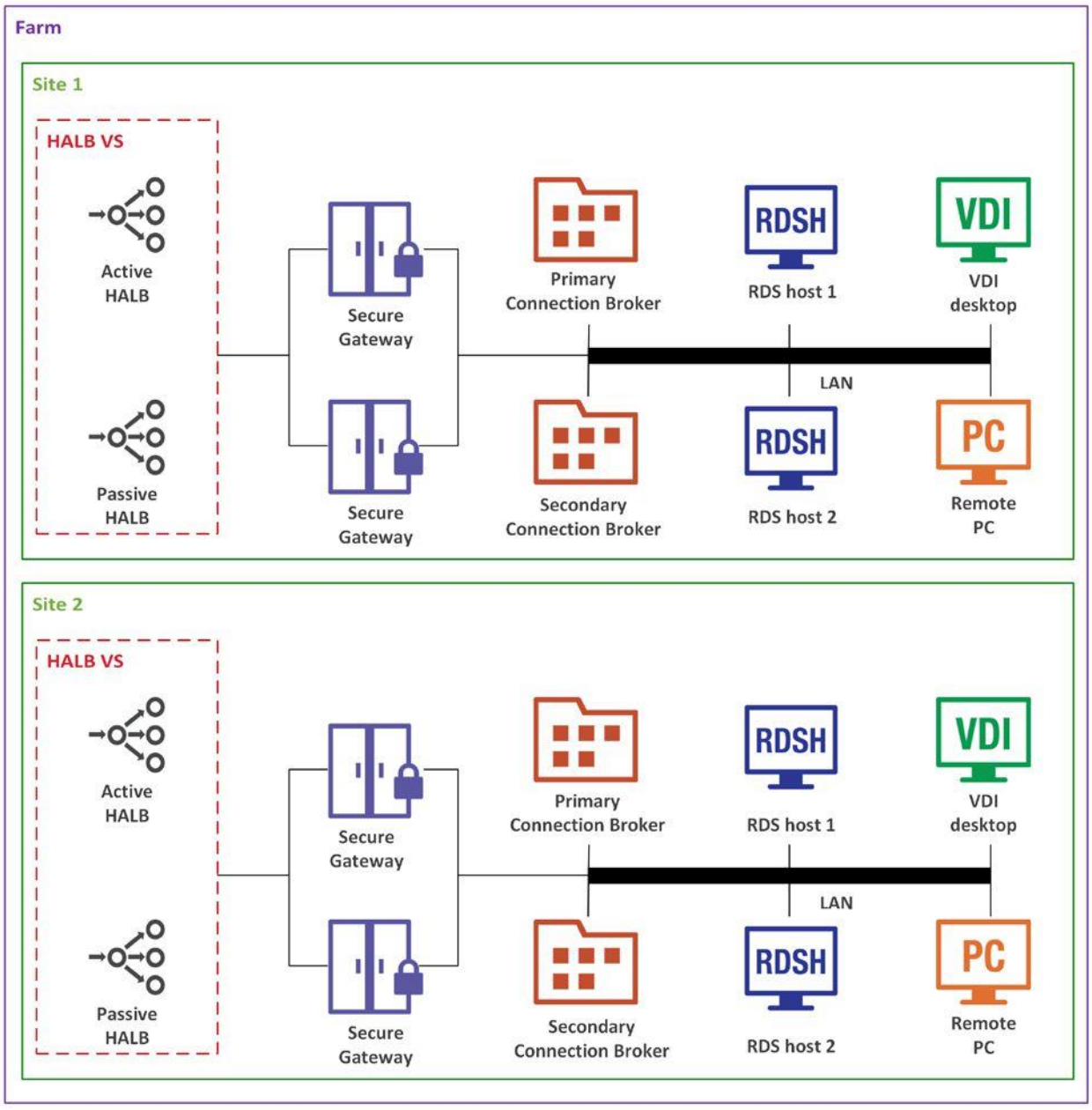
- Agents (エージェント)

ファームに追加された最初のサーバーは新しいサイトを作成し、そのサイトのプライマリ RAS Connection Broker になります。このサーバーは、デバイス接続ライセンスを処理するファームのライセンス サーバーにもなります。ファーム内のすべての Connection Broker (複数存在する場合) は、Parallels RAS 構成データベースの同期コピーを保持します。管理者が Parallels RAS コンソールで Parallels RAS 構成に変更を加えると、その変更は他のすべての Connection Broker に複製されます。

次の図は、2 つのサイト (Site 1 と Site 2) を使用した Parallels RAS のインストールを示しています。各サイトは、プライマリ Connection Broker (Primary CB)、RAS Secure Gateway (SG) 、RD Session Host (RDS host 1) 、2 番目の RD Session Host (RDS host 2) 、VDI サーバー (Virtual Desktop Infrastructure) 、および Windows PC で構成されています。



RAS Connection Brokerと RAS Secure Gatewayを追加することで、システムの冗長性を高めることができます。HALB Virtual Server (VS) は、HALB アプライアンスを仮想的に表現したもの (オプションコンポーネント) であり、アプリケーション トラフィックの負荷分散のために追加できます。



注：1 つのサイトのメンバーであるリソース (RD セッション ホスト、リモート PC、VDI ホスト) を他のサイトと共有することはできません。たとえば、RDS ホスト 1 サーバーはサイト 1 のメンバーです。つまり、サイト 2 にある Secure Gatewayと Connection Brokerを介して接続しているユーザーはアクセスできません。

Parallels Client 接続の流れ

クライアント接続フローは、アプリケーションの列挙とアプリケーションの起動の 2 つの段階で構成されます。以下では、各段階について詳しく説明します。以下で説明する手順は、リモート デスクトップ、ドキュメント、Web アプリケーション、ネットワークフォルダーなど、他のすべての種類の公開済みリソース (アプリケーションだけでなく) にも同様に適用されることに注意してください。

アプリケーションの列挙

1. アプリケーションの列挙は、特定のユーザーが使用できる公開済みリソースのリストを取得するプロセスです。この段階は、次の手順で構成されます。
2. ユーザーがデバイスで Parallels Client を起動し、(構成済みの場合は) RAS 接続をダブルクリックします。
3. Parallels Client は、RAS Secure Gateway または (インストールされている場合は) HALB アプライアンスに接続します。
4. HALB VS が構成されている場合、プライマリ HALB アプライアンスは負荷分散ルールに従って Parallels Client を Secure Gateway に転送します。
5. RAS Secure Gateway は、Connection Broker との接続トンネルを構築して、クライアント認証を開始します。
6. Parallels Client は、ユーザー資格情報を Connection Broker に送信します。
7. ユーザー認証が成功すると、Connection Broker は Secure Gateway SSL トンネルを介してアプリケーション リストを Parallels Client に返します。
8. アプリケーション リストがユーザーのデバイスの Parallels Client ウィンドウに表示されるため、ユーザーは起動するアプリケーションを選択できます。

アプリケーションの起動

この段階は、次の手順で構成されます。

1. ユーザーがアプリケーションを起動します。
2. Parallels Client は、Secure Gateway トンネルを介して Connection Broker に要求を送信します。
3. Connection Broker は、最も負荷の少ない RD セッション ホストを選択し、その IP アドレスを Secure Gateway 経由で Parallels Client に送り返します。
4. クライアント側で選択された接続モード (以下の「クライアント接続モード」を参照) に応じて、Parallels Client はダイレクトまたは RAS Secure Gateway を介して RD セッション ホストに接続し、ユーザー資格情報を渡します。
5. RD セッション ホストは、受信した資格情報を確認し、有効な場合は RDP セッションを開始します。

クライアント接続モード

Parallels Client は、次の接続モードのいずれかを使用して Parallels RAS に接続できます。

- ダイレクト
- ダイレクト SSL
- ゲートウェイ
- ゲートウェイ SSL

ダイレクトモード

ダイレクトモードを使用するには、Parallels Client がホスト上のリソースに直接アクセスできる必要があります。

接続は次のように確立されます。

1 Parallels Client は、ポート 80 を介して RAS Secure Gateway に接続し、接続をネゴシエートしてセッションを確立します。

2 Parallels Client は、ポート 3389 を介してホストとの RDP セッションを開始します。

3 最後に、Parallels Client は Secure Gateway から切断し、サーバーとの新しいセッションを確立します。

RAS Secure Gateway は一時的に短時間しか使用されないため、ダイレクトモードが最も効率的な接続です。

ダイレクト SSL モード

ダイレクト SSL モードはダイレクトモードと同じですが、SSL 暗号化を使用します。ダイレクト SSL モードを使用するには、Parallels Client がホスト上のリソースに直接アクセスできる必要もあります。

接続は次のように確立されます。

1 Parallels Client は、ポート 443 を介して RAS Secure Gateway に接続します。クライアントと Secure Gateway は、接続をネゴシエートしてセッションを確立します。

2 Parallels Client は、ポート 3389 を介してホストとの RDP セッションを開始します。

3 Parallels Client は Secure Gateway から切断し、サーバーとの新しいセッションを確立します。

ゲートウェイモード

Parallels Client がホストに直接アクセスできない場合は、ゲートウェイモードを使用する必要があります。ゲートウェイモードは、利用可能な最も単純な接続モードです。管理者は、通常はポート 80 である単一のポートのみを開く必要があります。

接続は次のように確立されます。

1 Parallels Client は、ポート 80 で RAS Secure Gateway に接続し、接続をネゴシエートしてセッションを確立します。

2 Parallels Client は、同じ接続を使用してホストとのポート 3389 を介して RDP セッションを確立するように Secure Gateway に要求し、トンネルを形成します。

3 Parallels Client とサーバー間のすべての通信は、確立されたトンネルを使用して実行されます。

ゲートウェイ SSL モード

ゲートウェイ SSL モードは、ゲートウェイモードと同じですが、SSL 暗号化を使用します。

接続は次のように確立されます。

1 Parallels Client は、ポート 443 で RAS Secure Gateway に接続します。

2 SSL トンネルが確立されると、クライアントと Secure Gateway は安全なセッションを確立するためにネゴシエートします。

3 Parallels Client は、同じ接続を使用してホストとのポート 3389 を介して RDP セッションを確立するように Secure Gateway に要求し、トンネルを形成します。

4 Parallels Client とサーバー間のすべての通信は、確立されたトンネルを使用して実行されます。

混合モード：ダイレクト SSL とゲートウェイ SSL

Parallels RAS は、複数の接続モードを同時に処理できます。RAS Secure Gateway をより有効に活用するには、可能な限り LAN クライアントにダイレクトモードを使用することをお勧めします。セキュリティを強化するために、WAN クライアントにはゲートウェイ SSL モードを使用することをお勧めします。

第 2 章

展開シナリオ

この章では、一般的な Parallels RAS の展開シナリオについて説明します。

この章の内容

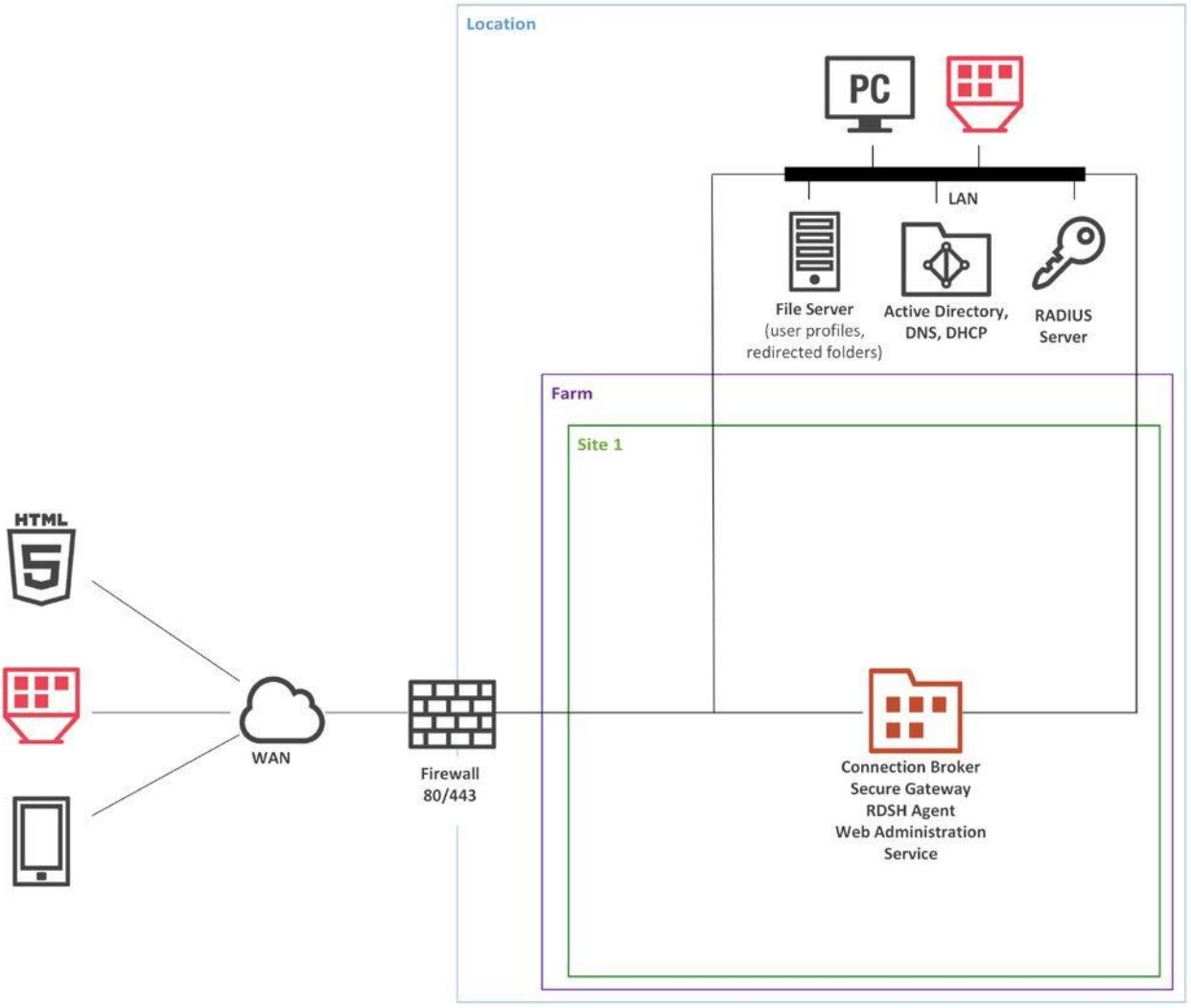
概要

Parallels RAS インストールのサイズに関係なく、可能な限り最大の稼働状態を確保するため、セットアップのコアコンポーネント間の冗長性をお勧めします。小規模な展開では、すべての役割を単一のサーバーにインストールできますが、大規模なセットアップでは役割の分担をお勧めします。

RD セッション ホストや VDI ホストを含む Parallels RAS ファームの物理的な場所は、データベースやファイル サーバーなどのバックエンド リソースの場所に基づいて選択する必要があります。これは、フロントエンドアプリケーションがデータベースに接続するか、ファイル サーバー上のファイルを操作する場合、フロントエンドアプリケーションがインストールされる RD セッション ホストは、高速で、信頼性の高い、低遅延の LAN 接続にてイントラネット上のデータベース (またはファイル サーバー) に構築する必要があります。たとえば、ユーザーが利用できるようにしたいクライアントサーバーアプリケーションがあるとします。これを使うには、クライアント部分を RD セッション ホストにインストールし、ユーザーに公開します。データベースは引き続き専用サーバーで実行されます。高速で信頼性の高いデータベースアクセスを保証するには、RD セッション ホストサーバーとデータベースサーバーがローカルネットワーク上で互いに隣接している必要があります。

Parallels RAS 展開シナリオ

1 つの RD セッション ホストを持つ単一のファーム



このシナリオでは、アプリケーションとデスクトップの公開に単一の RD セッション ホストを使用します。SSL およびユーザー ポータルは、自己署名付きサーバー証明書を使用してデフォルトで有効になっています。サーバー証明書は、クライアント デバイスによって信頼されている必要があります。外部アクセスする場合には、エンタープライズ証明書またはサードパーティの信頼できる認証局を使用できます (詳細については、「SSL 証明書」セクション (p. 69) を参照してください) 。

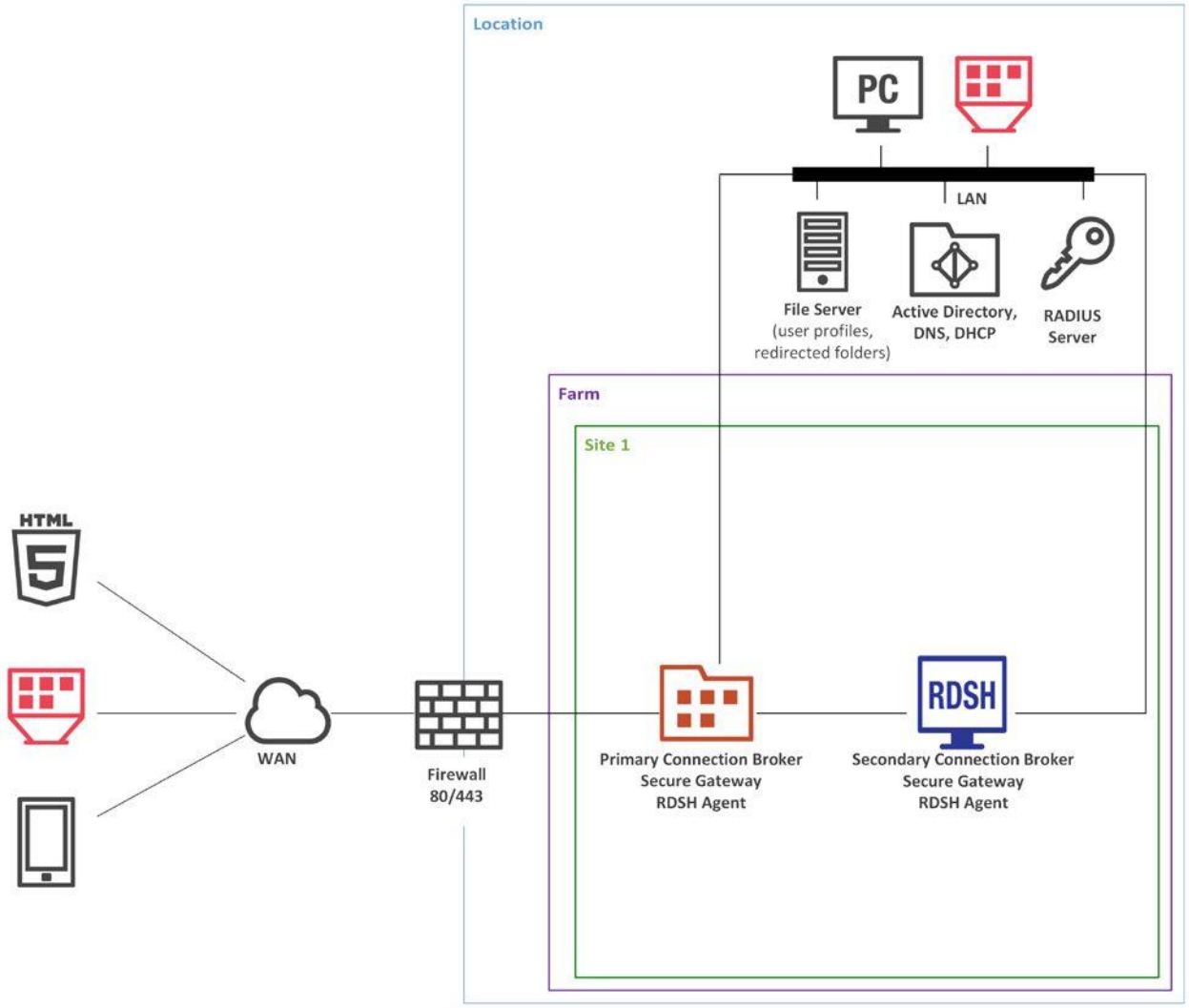
導入時の注意

Parallels RAS のすべてのサーバー コンポーネントは、Parallels RAS インストーラーを使用してインストールされます (標準インストール) 。

単一サーバーの展開は、サービスの高可用性を提供しない為、実稼働環境には推奨しません。このような展開は、テスト環境または開発者環境の範囲で使用として下さい。

2 つの RD セッション ホストを備えた単一のファーム

このシナリオは、2 つの RD セッション ホスト間で公開されたアプリケーションとデスクトップの負荷を分散する必要がある組織によって実装できます。高可用性を実現するには、セカンダリ RAS Connection Broker と RAS Secure Gateway を 2 番目のサーバーにインストールする必要があります。



導入時の注意

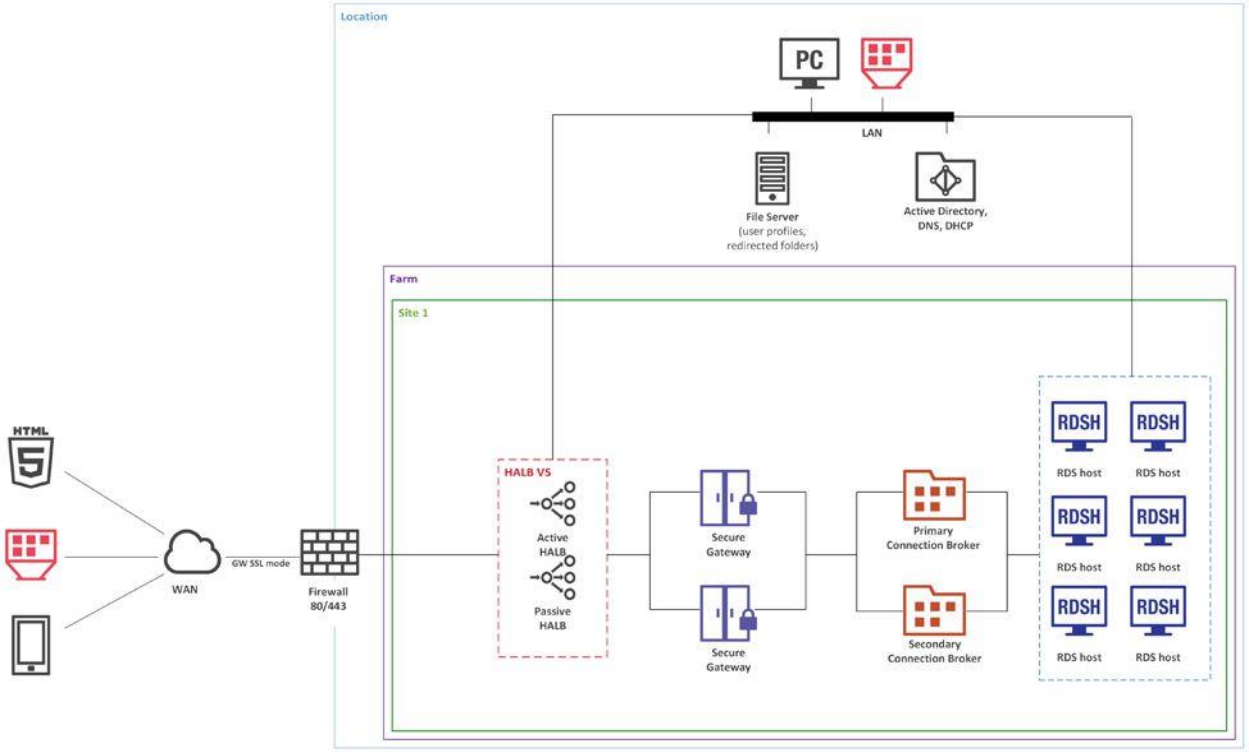
プライマリ RD セッション ホスト (プライマリ RAS Connection Broker がインストールされている場所) のコンポーネントは、Parallels RAS インストーラー (標準インストール) を使用してインストールされます。

セカンダリ RD セッション ホストのコンポーネントは、RAS コンソールからプッシュ インストールされます。

RD セッション ホスト自動スケーリングを備えた単一ファーム

このシナリオは、RD セッション ホストに単一のイメージ管理を使用し、公開されたアプリケーションとデスクトップに動的なリソース割り当てを使用する必要がある組織によって実装できます。

高可用性を実現するには、HALB 仮想サーバー (VS) にセカンダリ HALB アプライアンスが必要であり、追加の RAS Connection Broker と RAS Secure Gateway を展開する必要があります。HALB 仮想サーバー (VS) は、HALB アプライアンスの仮想表現です。



導入時の注意

プライマリ RAS Connection Broker のコンポーネントは、Parallels RAS インストーラーを使用してインストールされます (標準インストール) 。

新しいタイプの RAS テンプレートは、RAS ゲスト エージェントと RD セッション ホスト エージェントの両方が RAS コンソールから VM にプッシュ インストールされるゲスト VM で実行される RD セッション ホストのサポートを追加します。

RD セッション ホスト プールには RAS テンプレートが割り当てられ、アプリケーションとデスクトップの公開に使用されます。

RD セッション ホストの作成、保守、および削除は、RAS テンプレートを介して行われます。

RD セッション ホスト プールは、オンデマンドで RD セッション ホストを割り当て、ワークロードの増加に対し、より多くのリソースを提供しワークロードの減少に対して RD セッション ホストの割り当てを解除します。

HALB 仮想サーバー (VS) は、2 つの HALB アプライアンスで構成されています。

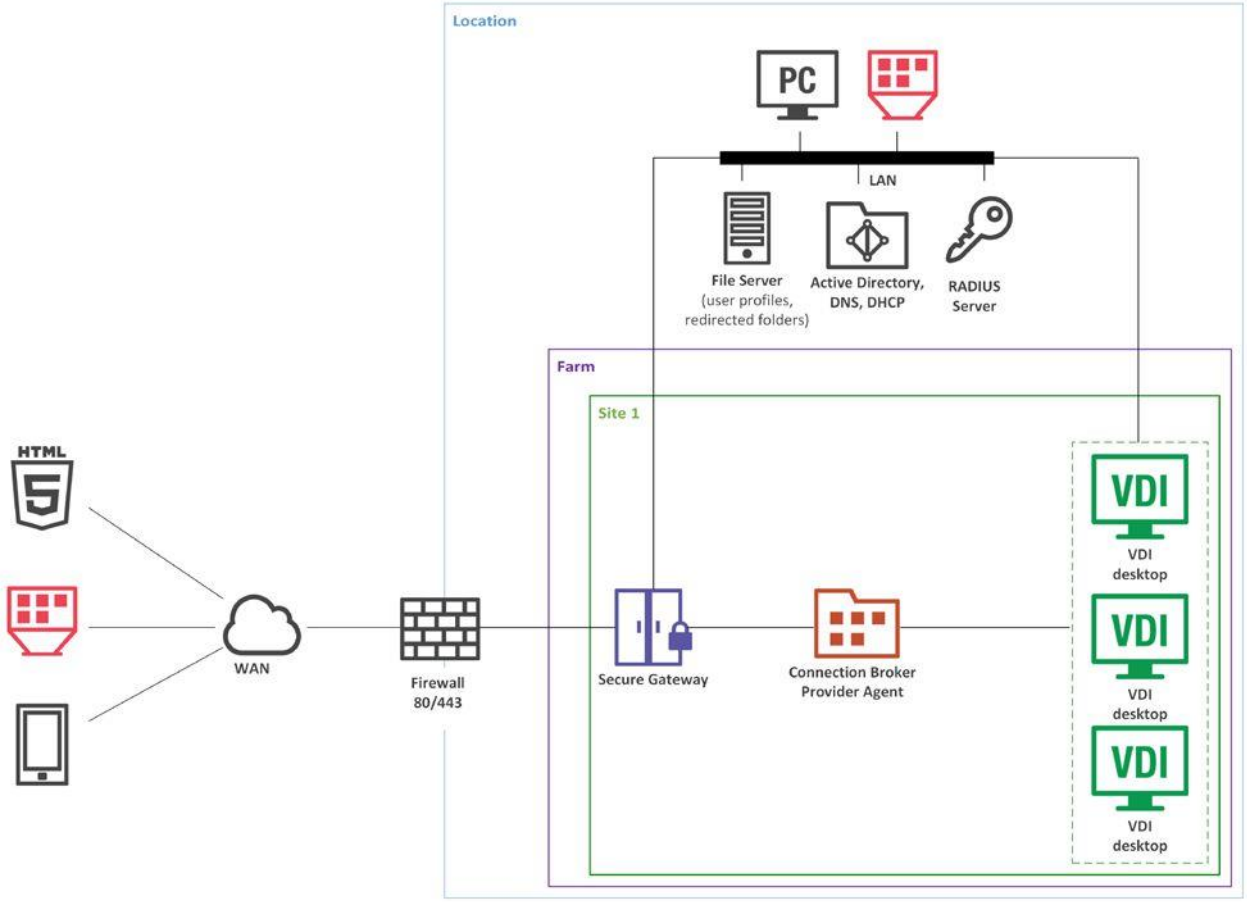
VDI ホストを備えた単一のファーム

VDI ホスト プールは、単一のデータセンターにあるホスト (完全またはリンクされたクローン) からのアプリケーションおよびデスクトップ パブリッシングを対象としています。

VDI ホストには、次の利点があります。

- ハイパーバイザー上に仮想マシン (VM) を作成するために、単一の Windows 7 、8 、または 10 のデスクトップ イメージを使用して、社内のネットワーク全体に共通にサポートされているデスクトップ環境を迅速に展開します。
- Windows VDI デスクトップへの更新と変更の集中展開-必要事項としては、単一のイメージの更新のみとなります。
- 障害が発生した場合、単一のイメージ バックアップを使用して VDI デスクトップを簡単に復元できます。

- データ セキュリティの強化により、組織は動的なセキュリティ権限を備えた追加の保護レイヤーを利用できます。これは Parallels RAS クライアントを使用せずに VDI にアクセスできないようにするセキュリティ機能です。セッションが確立された後、Parallels RAS はユーザーを「リモート デスクトップ ユーザー」グループに動的に追加し、ログオン時のアクセス許可を付与し、ログオフ時のアクセス許可を削除します。VDI 仮想マシン (VM) のホスト名または IP アドレスが記載されている場合でも、Parallels Client から接続を設定しない限り、ユーザーは VDI VM に接続できません。



導入時の注意

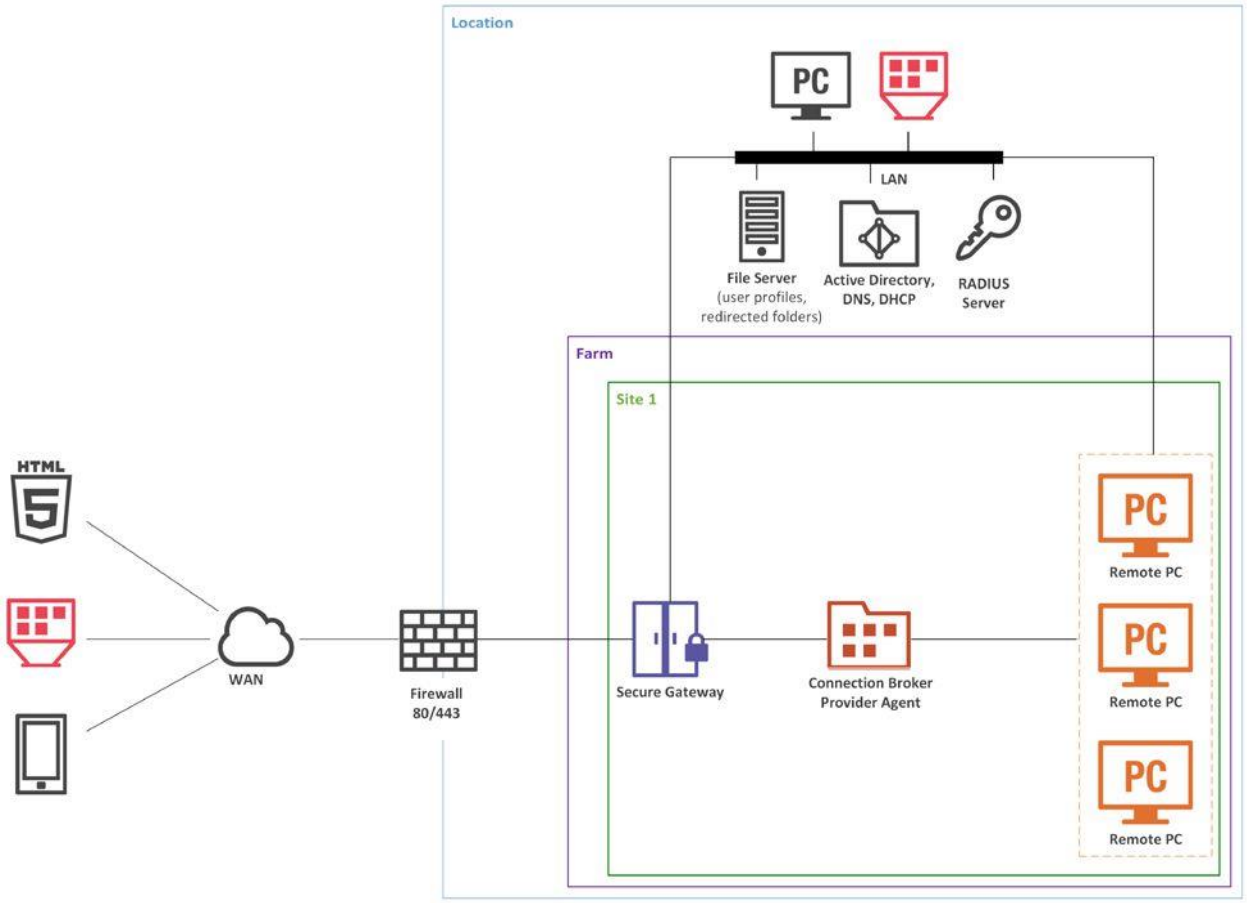
RAS Connection Broker は、Parallels RAS インストーラーを使用してインストールされます (標準インストール) 。

RAS Secure Gateway、RAS Guest Agent は、RAS コンソールからプッシュ インストールされます。

リモート PC ホストを備えた単一のファーム

リモート PC は、リモート アプリケーションとデスクトップ パブリッシングに使用できる Windows を実行する物理デスクトップです。すべての PC が 1 人のユーザーに対して公開され、公開用に指定する必要がある個々のリモート PC に加えて、Parallels RAS にリモート PC ホスト プールを追加しました。

リモート PC ホスト プールは、単一のデータセンターにあるリモート PC からのアプリケーションおよびデスクトップ パブリッシングを対象としています。リモート PC ホスト プールは、シフト制を導入している企業 (24 時間年中無休のサービスを提供する企業など) またはユーザーが遠隔地にいる場合に、最も効果的なハードウェア使用率を提供します。ユーザーには、最初の使用時にリモート PC が割り当てられます。シフトが終了すると、その PC は次のシフトのユーザーが再利用できるようにホスト プールに戻されるか、管理者の設定に応じて、永続性が保持されます (デフォルトでは 3 日) 。



導入時の注意

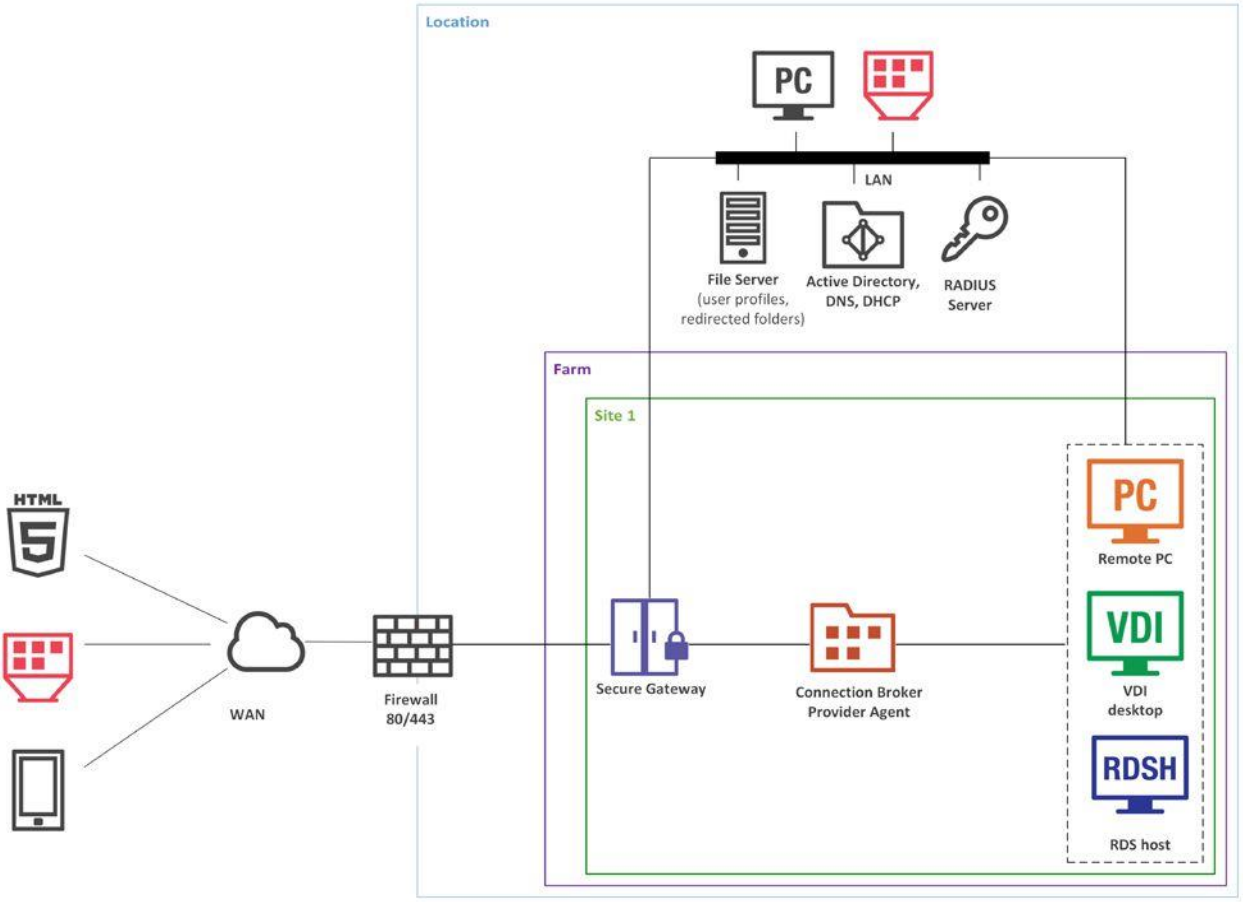
RAS ゲスト エージェントは、リモート PC エージェントの代わりにリモート PC ホスト プールで使用されます。ホスト プールメンバーシップは、PC リスト (手動で個々の PC を追加するか、CSV ファイルからリストをインポートする) または Active Directory OU の場所 (リストは 5 分ごとに RAS Connection Broker によって更新される) のいずれかから構築されます。

RAS Connection Broker は、Parallels RAS インストーラーを使用してインストールされます (標準インストール) 。

RAS Secure Gateway、RAS Guest Agent は、RAS コンソールからプッシュ インストールされます。

混合ホストを備えた単一のファーム

このシナリオを使用すると、オフィスにある仮想マシン、RD セッション ホスト、および Windows デスクトップ コンピューターからアプリケーションとデスクトップを公開できます。



導入時の注意

RAS Secure Gateway とプライマリ RAS Connection Broker は、Parallels RAS インストーラーを使用してインストールされます (標準インストール) 。

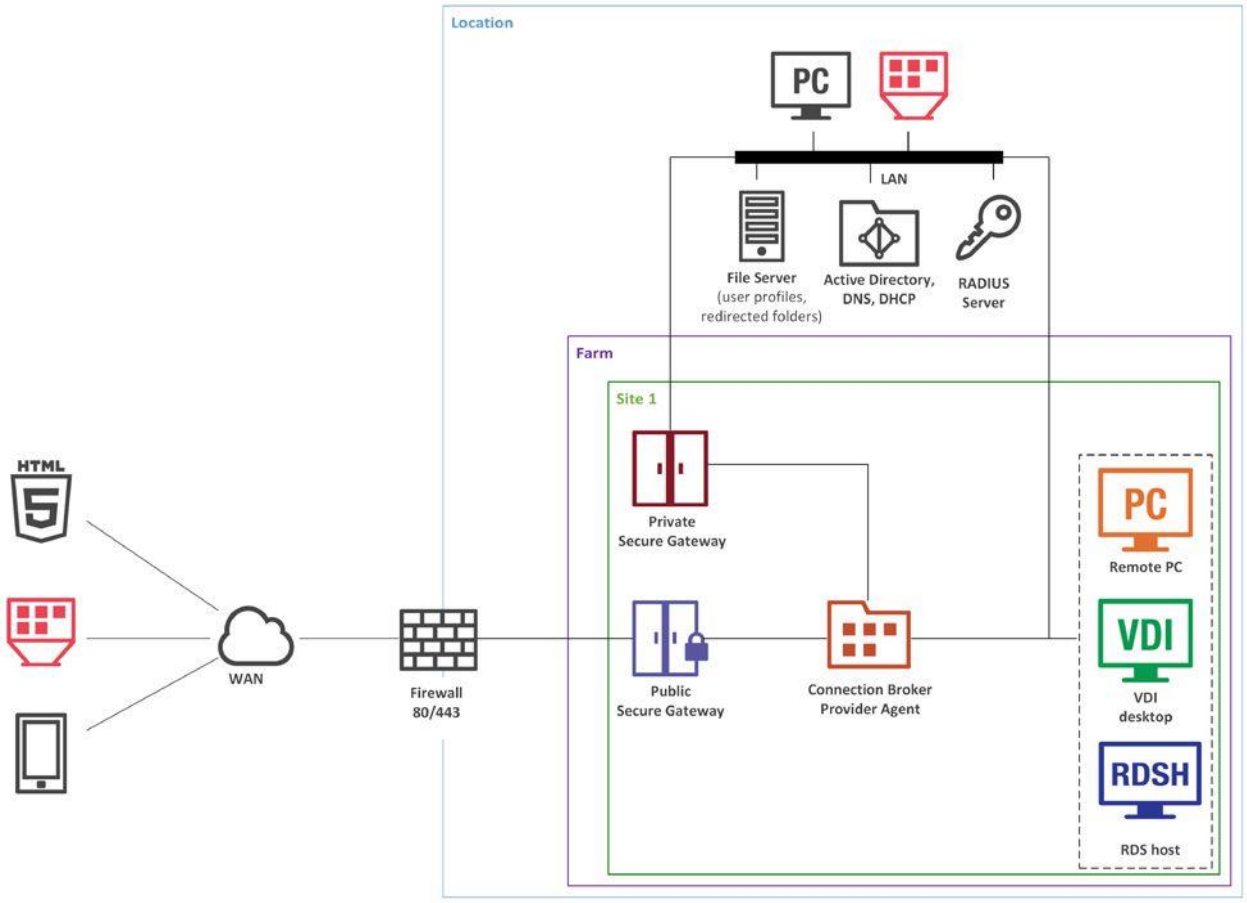
他のすべてのコンポーネントは、RAS コンソールからプッシュ インストールされます。

パブリックおよびプライベート RAS Secure Gateway を備えたシングル ファーム

Secure Gateway でより多くの接続を処理するには、ダイレクト クライアント接続モードのイントラネット ユーザー (プライベート) には、指定された RAS Secure Gateway を使用することをお勧めします。

インターネットにアクセスできるサーバーにより厳しいセキュリティ設定を適用するには、ゲートウェイ SSL クライアント接続モードのインターネット ユーザー (パブリック) には、指定された Secure Gateway を使用することをお勧めします。

適切な RAS 接続設定をすると、Parallels RAS コンソールのクライアント ポリシーを介して一元的に適用することも、Parallels Client にて手動適用することもできます。



導入時の注意

パブリック RAS Secure Gateway とプライマリ RAS Connection Broker は、Parallels RAS インストーラーを使用してインストールされます (標準インストール) 。

他のすべてのコンポーネントは、RAS コンソールからプッシュ インストールされます。

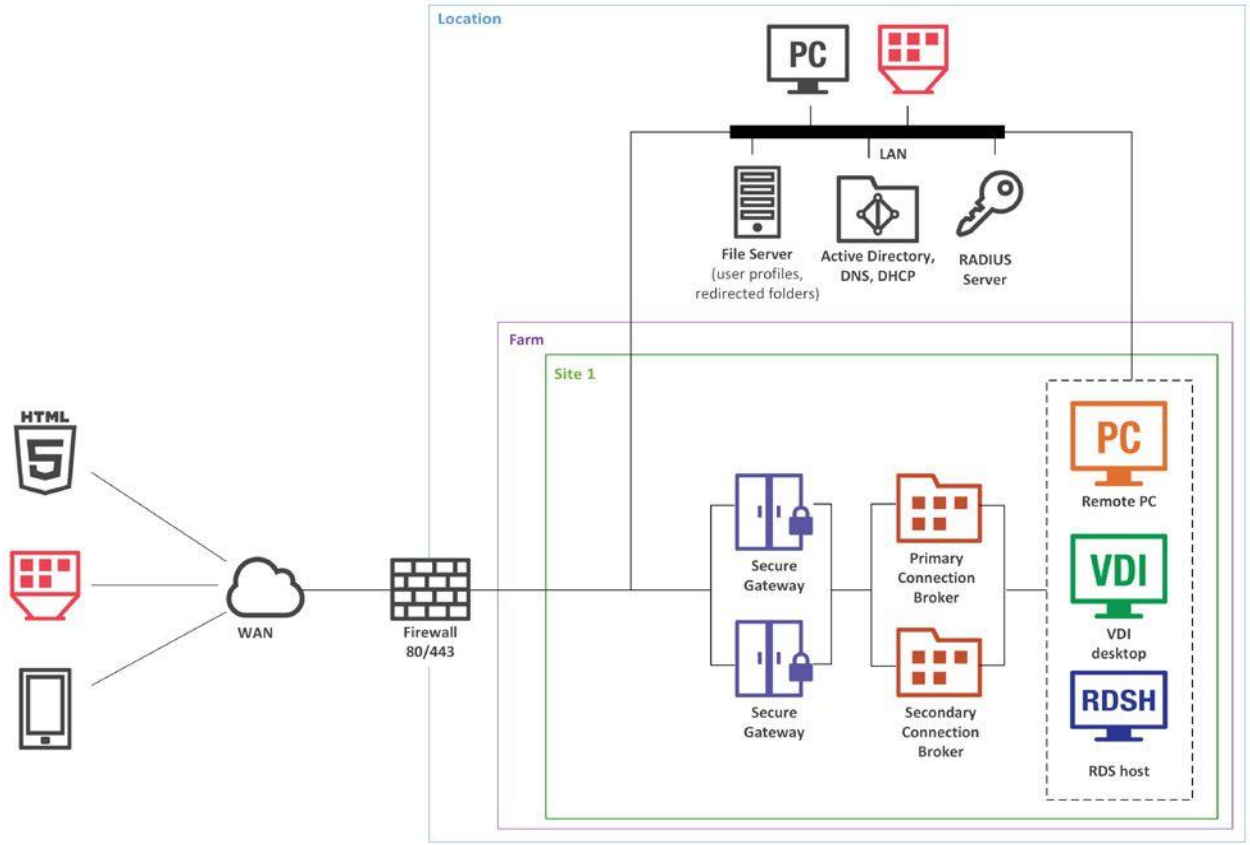
デュアル RAS Secure Gateway を備えたシングル ファーム

このシナリオでは、Parallels Client 側またはラウンドロビン DNS のいずれかで RAS 接続設定を行い、クライアント接続の高可用性を実現します。

RAS 接続設定を使用したクライアント接続の高い可用性を有効にするには、RAS 接続プロパティのプライマリおよびセカンダリ接続設定を使用し、Secure Gateway に接続するよう Parallels Client を構成する必要があります。この場合、プライマリおよびセカンダリ RAS Secure Gateway は、同じ RAS Connection Broker に接続するように構成する必要があります (Client Gateway の詳細設定を使用する) 。プライマリ RAS Secure Gateway が使用できない場合、Parallels Client はセカンダリ RAS Secure Gateway を使用してファームに接続できます。クライアント設定は、一元的 (RAS コンソールのクライアント ポリシーを使用) または手動で適用することができます。

ラウンドロビン DNS を使用したクライアント接続の高可用性を有効にするには、DNS 前方参照ゾーンに同じ名前 (myhost.example.com など) で、プライマリとセカンダリの RAS Secure Gateway の 2 つの異なる IP アドレスを使用して 2 つの新しいホスト レコードを作成する必要があります。

注：2 つの Secure Gateway 間のラウンドロビン DNS 負荷分散は、TCP プロトコルでのみ機能します。UDP 負荷分散が正しく機能しない場合があります。



導入時の注意

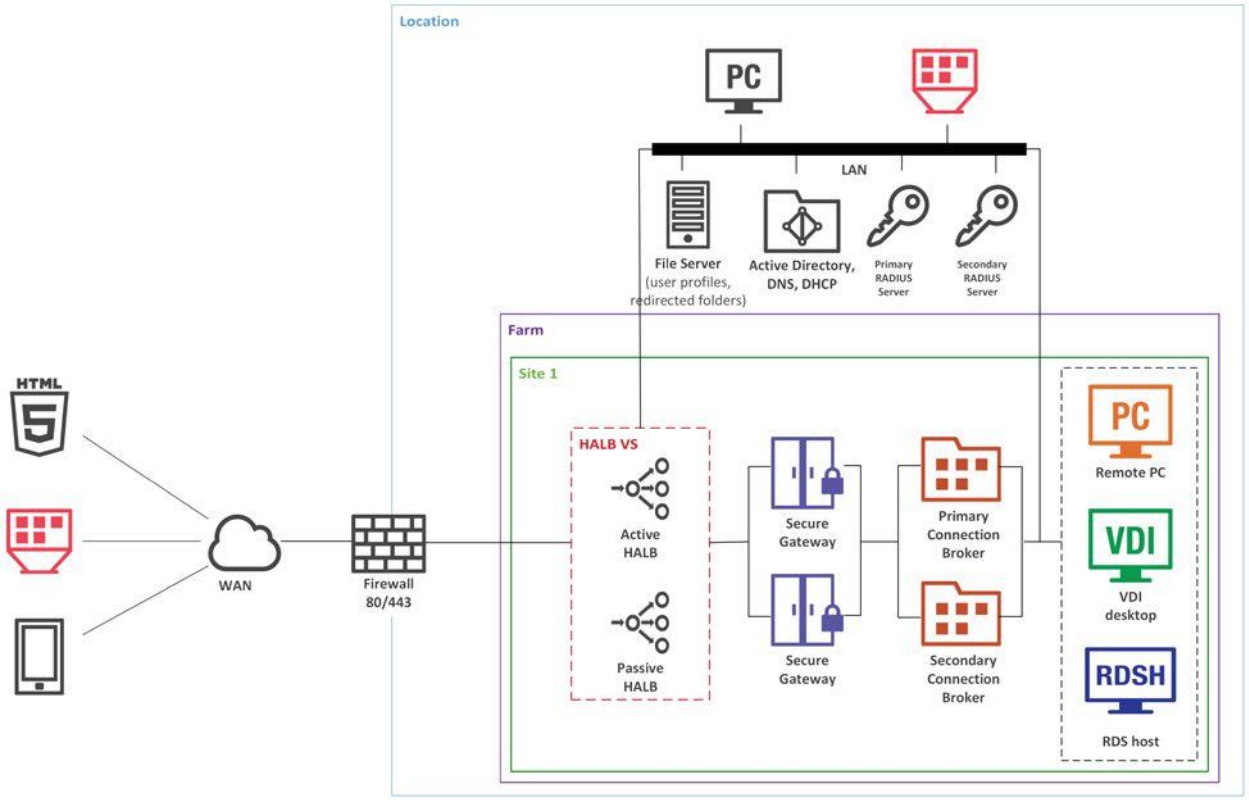
RAS Connection Broker は、Parallels RAS インストーラーを使用してインストールされます (標準インストール) 。

他のすべてのコンポーネントは、RAS コンソールからプッシュ インストールされます。

複数のゲートウェイによる高可用性について

このシナリオは、SSL モードで接続された 300 人を超える同時ユーザーがいる高可用性環境に最適です。各クライアントゲートウェイは、300 ~ 500 の同時ユーザー接続*を最適に処理する必要があります (以下の注を参照) 。これは、それに応じて水平方向にスケーリングできます。

LAN ユーザーと WAN ユーザーの両方が、内部ネットワーク内の HALB 仮想アプライアンスを表す HALBVS の IP アドレスに接続します。



上の図には、高可用性を提供するためにアクティブ/アクティブまたはアクティブ/パッシブとして使用できるオプションのセカンダリ RADIUS サーバーが含まれていることに注意してください。

容量に関する考慮事項 (p. **エラー! ブックマークが定義されていません。**) も参照してください。

すべての RAS Secure Gateway は、同じ RAS Connection Broker に接続するように構成する必要があります (Client Gateway の詳細設定を使用-上記を参照) 。

導入時の注意

RAS Connection Broker は、Parallels RAS インストーラーを使用してインストールされます (標準インストール) 。

HALB は、すぐに使用できる仮想アプライアンスとしてインストールされ、HALB とプロパティで構成されます。

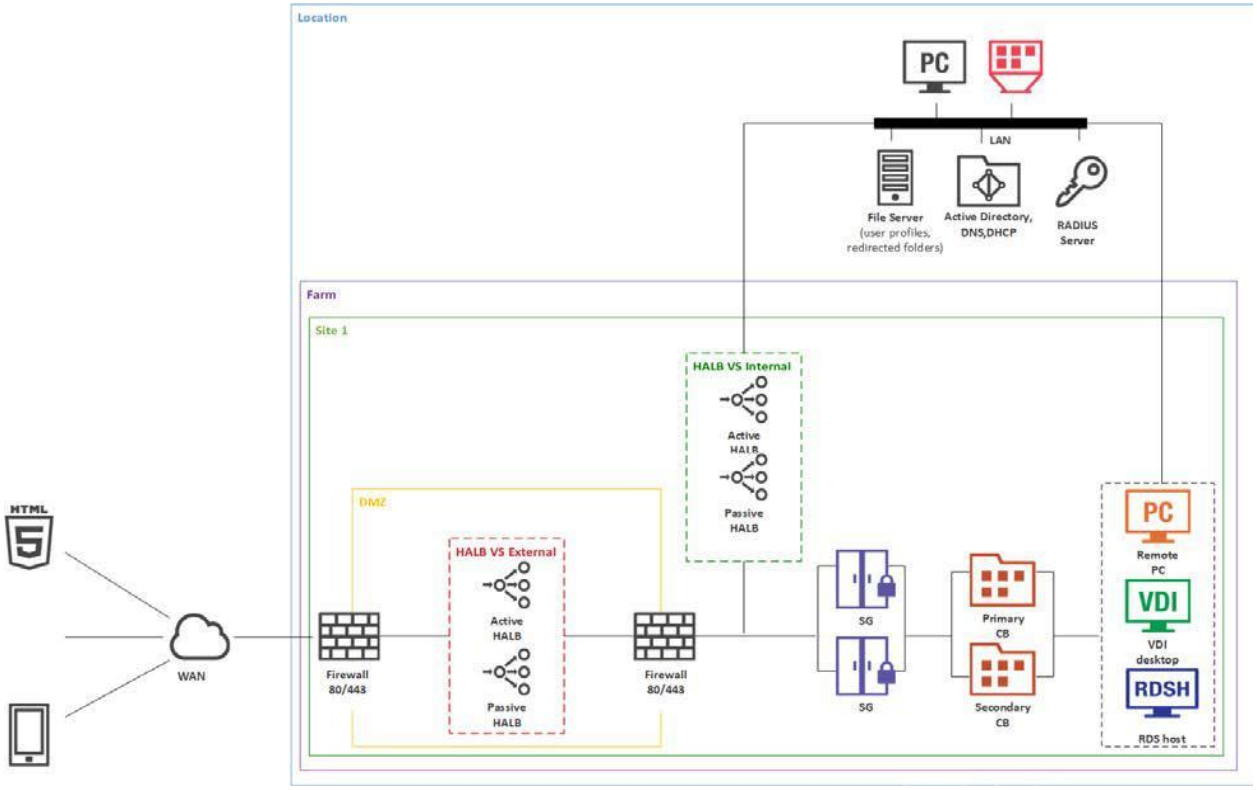
他のすべてのコンポーネントは、RAS コンソールからプッシュ インストールされます。

シングルホップまたはダブルホップ DMZ による高可用性について

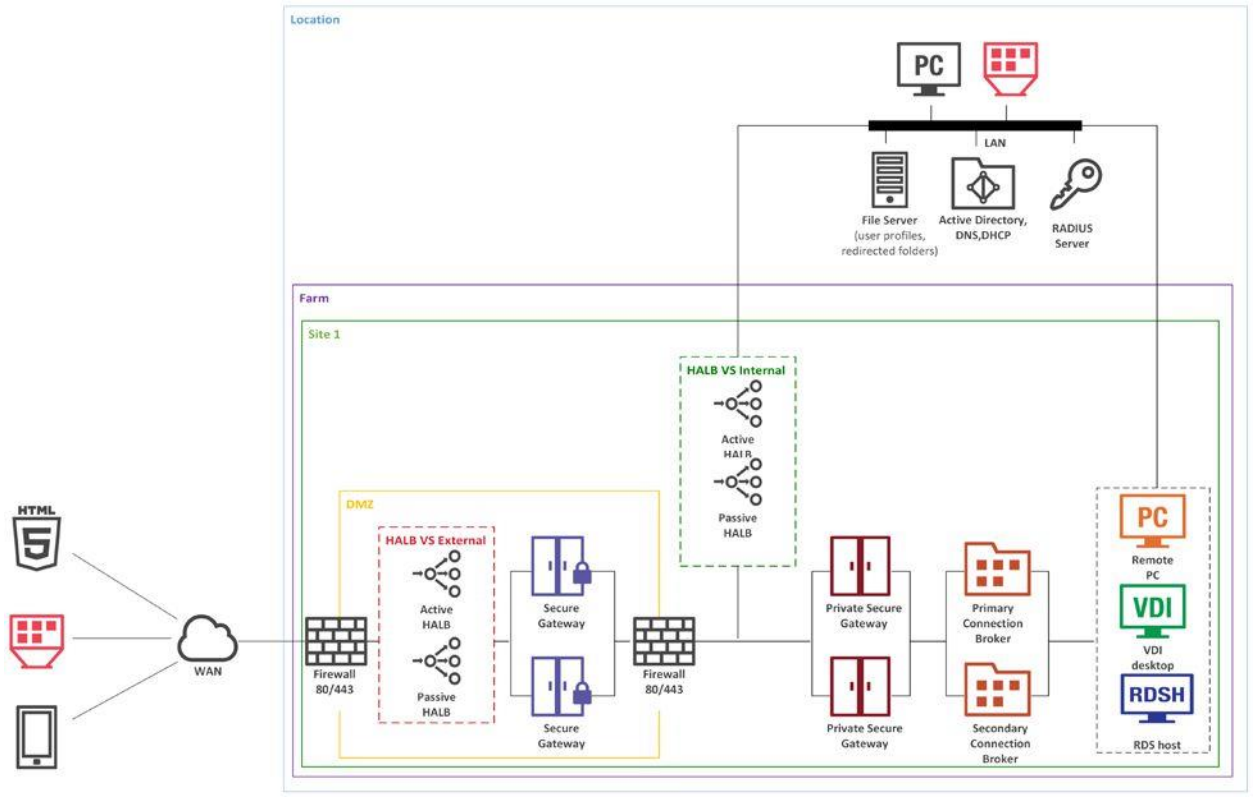
多くの企業は、境界ネットワーク (DMZ) を使用して、公開されたサービスを処理するサーバーを備えたパブリック ネットワークと、内部サービスを処理するサーバーを備えた内部ネットワークを分離しています。DMZ には 2 つのタイプがあります。シングルホップとダブルホップです。後者は 3 つのファイアウォールを使用するため、より高価ですが、より安全です (異なるファイアウォール技術を使用した 3 つのファイアウォールにより、1 つの弱点または 1 つのタイプの攻撃がすべてのファイアウォールを突破するのを防ぐことができます) 。RAS Secure Gateway とイントラネットの間のファイアウォールは、ゲートウェイとシステムが標準ポートを使用して RAS Connection Broker に接続できるようにする必要があります。

シングルホップ DMZ (2 つのファイアウォール)

シングルホップ DMZ シナリオでは、ファイアウォール システムは、RAS Secure Gateway から RAS Connection Broker への接続を適切にルーティングできる必要があります。ファイアウォール システムは、インターネットから、HALB 仮想アプライアンスまたはその他の一般的なプロトコル負荷分散シナリオを表す HALB 仮想サーバー (HALB VS) の仮想 IP アドレスへの接続も担当します。この場合、2 つの HALB 仮想サーバーが内部の Secure Gateway への内部および外部のトラフィック負荷分散に使用されることに注意してください。



内部ネットワークと外部ネットワークの間でトラフィックを区別するために、パブリック Secure Gateway とプライベート Secure Gateway を使用できます (どちらも RAS の観点からは同等です) 。



このタイプの構成では、HALB アプライアンスは内部境界ネットワーク (DMZ) の RAS Secure Gateway の前にインストールされます。WAN ユーザーは外部 HALBS VS の IP アドレスに接続し、LAN ユーザーは内部ネットワークにある Secure Gateway の前に設置された HALB アプライアンスを使用する内部 HALB VS の IP アドレスを使用します。Parallels Client の設定は、一元的に (Parallels RAS コンソールのクライアント ポリシーを介して) 、または Parallels Client が実行されているデバイス上でローカルに構成できます。HALB VS の高可用性を追加するために、2 番目のアプライアンスを外部内部および HALB VS に展開できます。

導入時の注意

RAS Connection Broker は、Parallels RAS インストーラーを使用してインストールされます (標準インストール) 。

HALB は、すぐに使用できる仮想アプライアンスとしてインストールされ、HALB VS プロパティで構成されます。

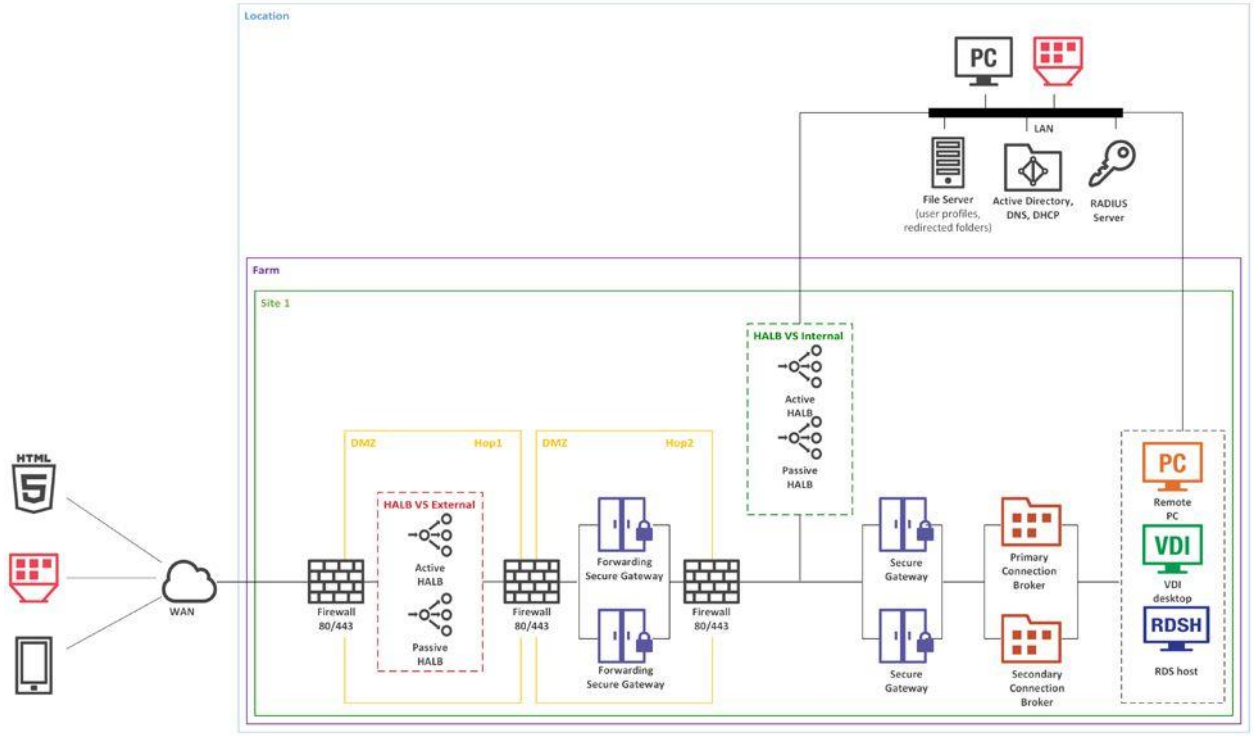
他のすべてのコンポーネントは、RAS コンソールからプッシュ インストールされます。

ダブルホップ DMZ（ 3 つのファイアウォール)

ダブルホップ DMZ シナリオでは、設定が簡単になり、外部の悪意のあるエージェントからの保護が強化されます。ダブルホップ DMZ では、境界ネットワークにインストールされた RAS Secure Gateway を転送して、内部の 2 番目の境界ネットワーク（ 2 番目のホップ) にある RAS Secure Gateway にクライアント接続を渡す必要があります。

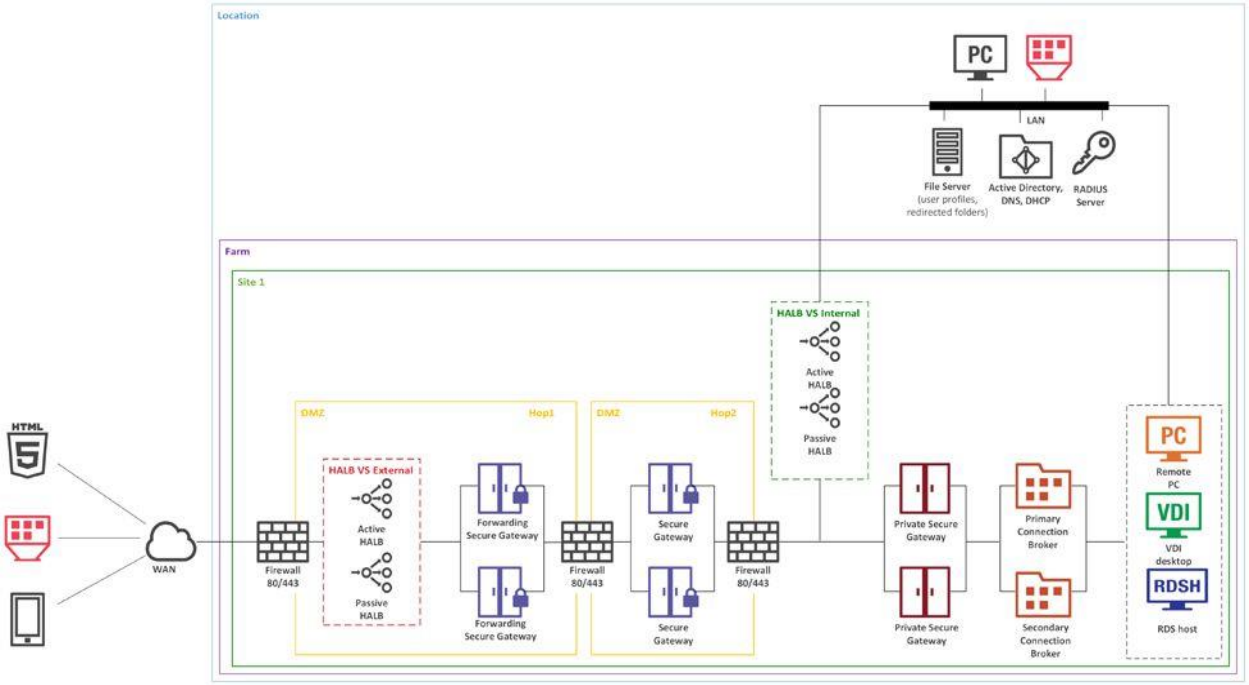
このような構成では、HALB ペア (プライマリとセカンダリ) を備えた HALB VS が、DMZ の転送 RAS Secure Gateway の前にインストールされます。WAN ユーザーは HALB VS の IP アドレスを使用して Parallels RAS に接続し、LAN ユーザーは内部ネットワークにある Secure Gateway の前に設置された HALB アプライアンスを使用する内部 HALB VS の IP アドレスを使用します。Parallels RAS 接続プロパティは、一元的に (RAS コンソールのクライアント ポリシーを使用して) 設定することも、Parallels Client で手動設定することもできます。

転送 RAS Secure Gateway は、[**転送 RAS Secure Gateway**] プロパティの [**詳細**] タブにある [**次の RAS Secure Gateway にリクエストを送信する**] オプションを使用してネットワーク トラフィックを転送します。



Parallels は、ダブルホップ DMZ 展開でのみ転送 RAS Secure Gateway を使用することをお勧めします。

内部ネットワークと外部ネットワークの間でトラフィックを区別するために、パブリック Secure Gateway とプライベート Secure Gateway を使用できます (どちらも RAS の観点からは同等です) 。



導入時の注意

RAS Connection Broker は、Parallels RAS インストーラーを使用してインストールされます (標準インストール) 。

HALB は、すぐに使用できる仮想アプライアンスとしてインストールされ、HALB VS プロパティで構成されます。

他のすべてのコンポーネントは、RAS コンソールからプッシュ インストールされます。

何らかの理由で転送 RAS Secure Gateway をプッシュ インストールできない場合は、ターゲットサーバーで Parallels RAS インストーラーを実行できます。その際、[**カスタム**] インストール タイプを選択してから、[**RAS Secure Gateway**] コンポーネントを選択します。

Microsoft Azure 上の RAS

次の情報を使用して展開を計画してください。

- **Azure リージョン** - Azure リージョンは、レイテンシーが定義された境界内にデプロイされ、専用のリージョンの低レイテンシーネットワークを介して接続されたデータセンターのセットです。Azure は、お客様が必要な場所にアプリケーションをデプロイする柔軟性を提供します。https://azure.microsoft.com/ja-jp/explore/global-infrastructure/geographies/

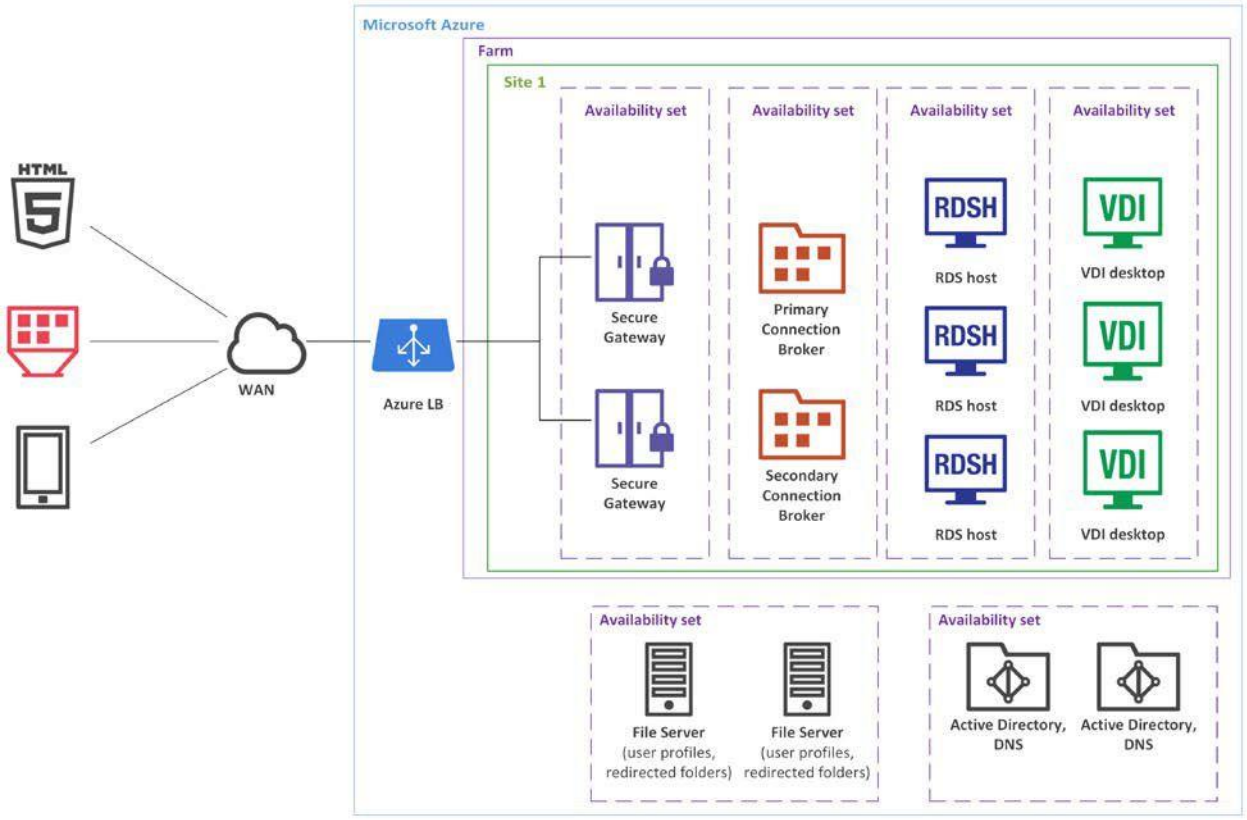
- アベイラビリティー ゾーン - アベイラビリティー ゾーンは、Azure リージョン内の物理的に離れた場所です。各アベイラビリティー ゾーンは、独立した電源、冷却、ネットワークを備えた 1 つ以上のデータセンターで構成されます。アベイラビリティー ゾーンにより、お客様は高可用性と低遅延でミッション クリティカルなアプリケーションを実行できます。復元力を確保するために、有効なすべてのリージョンに少なくとも 3 つの個別のゾーンがあります。https://learn.microsoft.com/ja-jp/azure/reliability/availability-zones-overview
- 可用性セット - 可用性セットは、VM リソースが展開されたときに VM リソースを相互に分離するための論理的なグループ化機能です。Azure は、可用性セット内に配置する VM が、複数の物理サーバー、コンピューティングラック、ストレージユニット、およびネットワーク スイッチで実行されることを確認します。ハードウェアまたはソフトウェアの障害が発生した場合、影響を受けるのは VM のサブセットのみであり、ソリューション全体が引き続き機能します。可用性セットは、信頼性の高いクラウド ソリューションを構築するために不可欠です。https://learn.microsoft.com/ja-jp/azure/virtual-machines/windows/tutorial-availability-sets

Microsoft Azure の設計はこのガイドの範囲外であることに注意してください。

Parallels RAS は、Azure でアプリケーションとデスクトップを配信するための 2 つの最も一般的なシナリオを提供します。これらのシナリオを以下に説明します。

クラウド内の Parallels RAS インフラストラクチャ

Parallels RAS インフラストラクチャ サーバー (RAS Connection Broker、RAS Secure Gateway、RAS Enrollment Server など) は Azure 上にあります。RAS 展開の各コンポーネントは、全体的な可用性を最大化するために、独自の可用性セットに含める必要があります。たとえば、Connection Broker、Secure Gateway、登録サーバーなどには、個別の可用性セットを使用する必要があります。

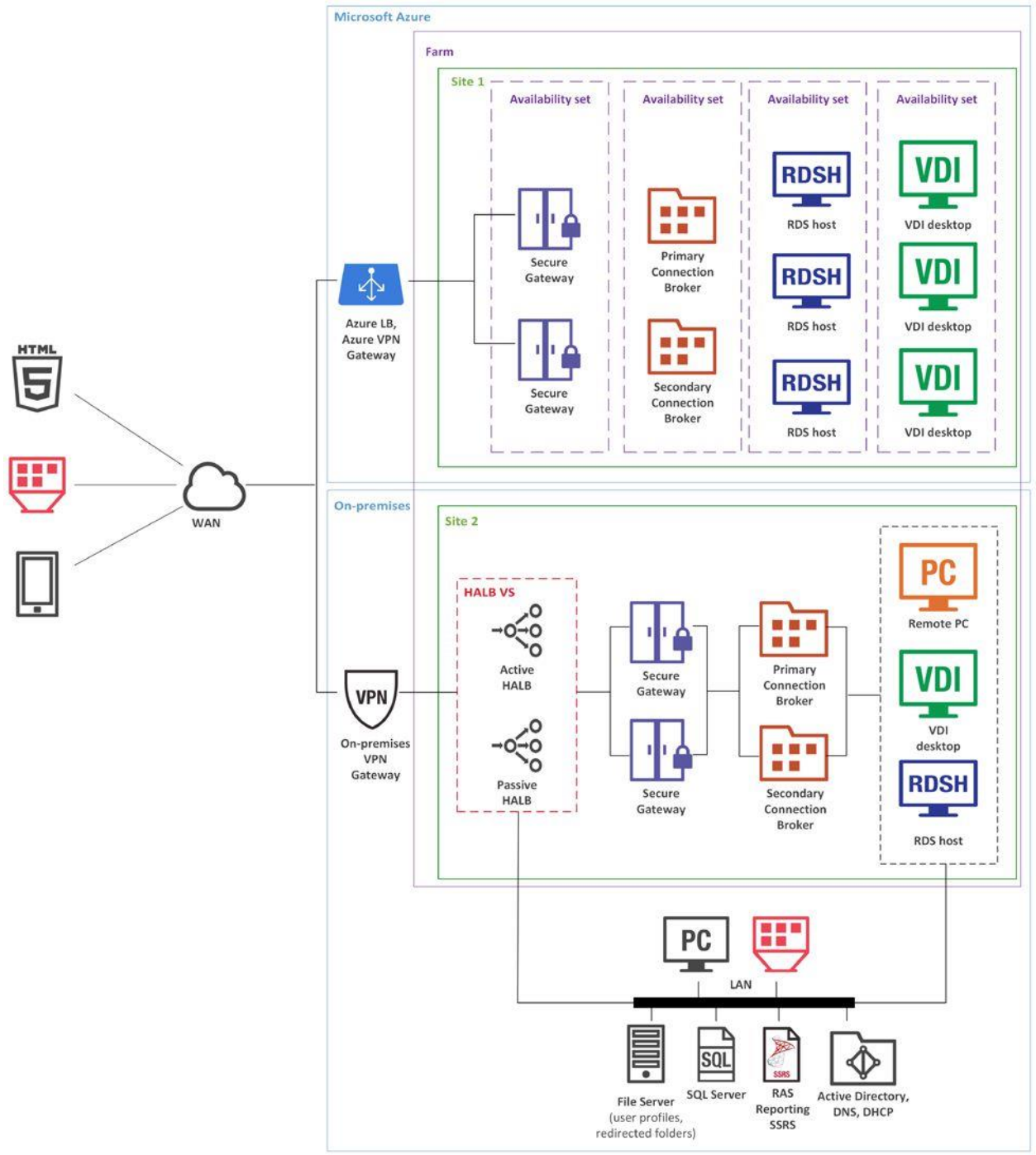


Azure を SAML IdP プロバイダとして使用したり、VDI / RDS リソース ホストのクラウド コンピューティング プラットフォームとして使用して、アプリケーションやデスクトップを提供したりすることもできます。

サイト間 VPN（または ExpressRoute）を使用したバックアップ サイトを備えたオンプレミス

Parallels RAS Connection Broker、RAS Secure Gateway、RAS 登録サーバーなどの RAS インフラストラクチャ サーバーは施設内に配置されていますが、VDI / RDSH リソース ホストは Azure 上の可用性セットにデプロイされています。これは、使用量の急増やビジネスの継続性をサポートする必要がある場合に実用的です。

注：1 つのファームが 2 つのサイトで使用されます。

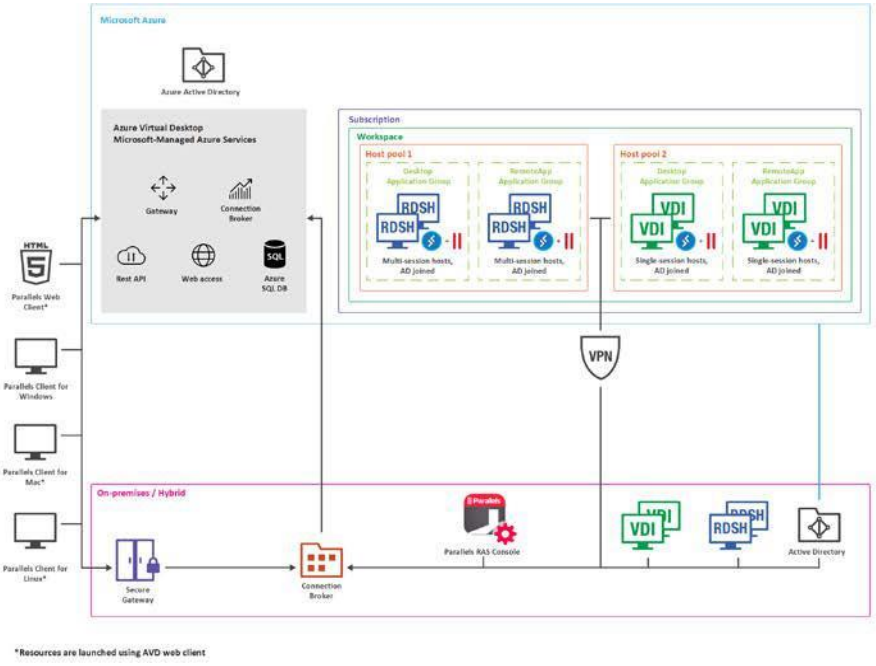


Azure Virtual Desktop の結合

Azure Virtual Desktop は、Microsoft Azure 上で動作するデスクトップおよびアプリの仮想化サービスであり、Windows 10 および 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ます。Parallels RAS 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、およびアクセスする機能を提供します。

次の図は、以下の特性を備えた Parallels RAS と Azure Virtual Desktop のハイブリッド展開を示しています。

- 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、あるいはサービス経由の Microsoft Azure 上でも利用できます。
- ワーク スペース、ホスト プール、デスクトップ、Remote App グループなどの Azure Virtual Desktop オブジェクトは、Parallels RAS コンソール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、管理と構成の為に 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ており、単一のインターフェイスからエンド ユーザーにリソースの可用性を提供します。



前に強調したように、完全な Parallels RAS 環境を Microsoft Azure に常駐させて、Azure Virtual Desktop を使用した完全なクラウド展開を実現することもできます

拡張された価値と機能

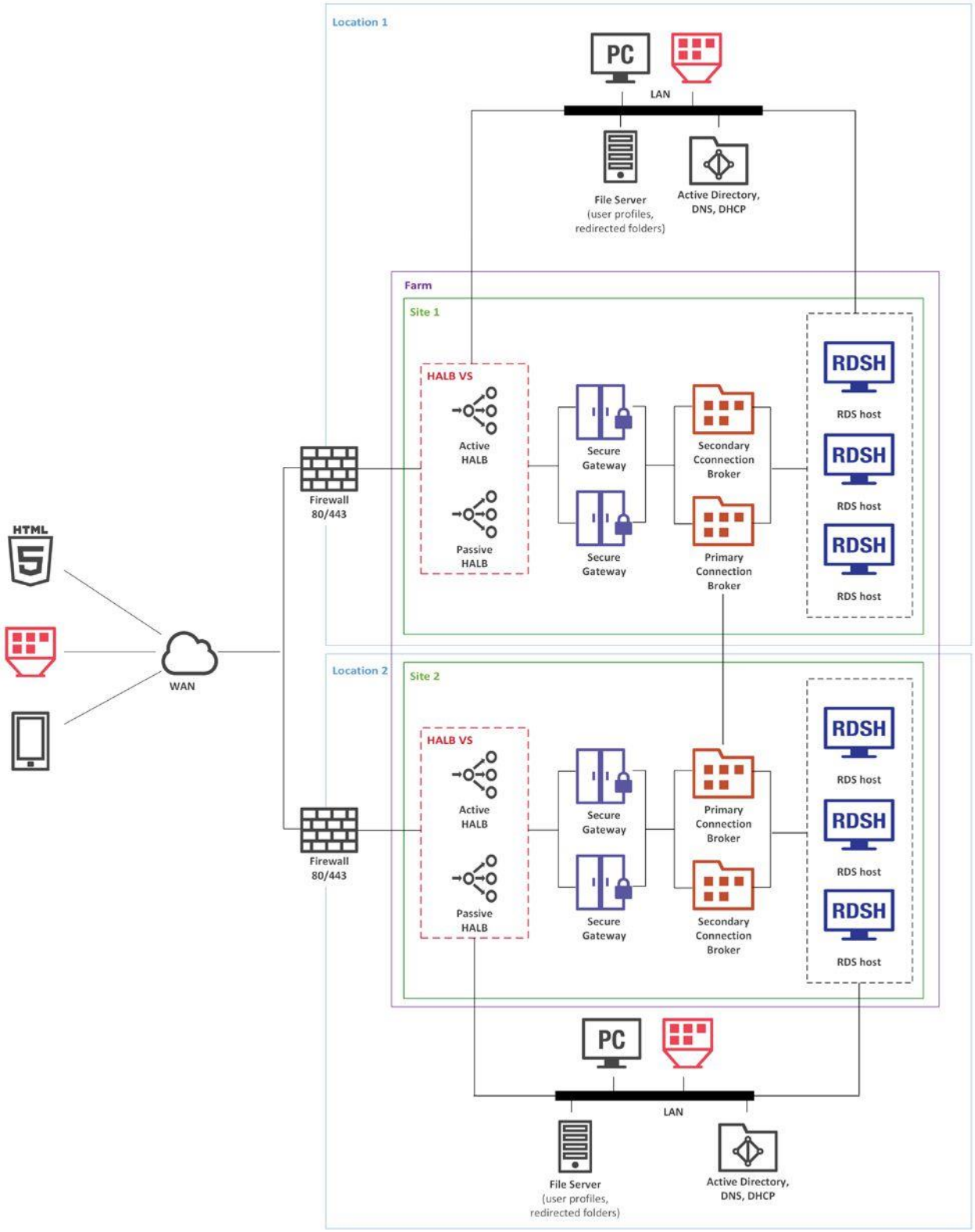
- Azure Virtual Desktop の展開および管理の簡素化と拡張。

- 管理と UX の統合 – 一元的なインターフェイス – Parallels クライアントおよび Parallels RAS コンソール。
- 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 および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、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の利用。
- AI ベースのセッション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化**] オプションを有効にすることで、ファイル 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。
- クライアント管理。
- クライアント向けのセキュリティ ポリシー。
- RAS コンソールからの RAS レポートおよびモニタリングの活用。

混合シナリオ

マルチ サイト シナリオ

このシナリオは、公開済みリソースが 2 つ以上の場所に物理的に分散されている環境に適しています。さまざまな管理者が、複数のサイトを含む Parallels RAS ファームを管理できます。


Location 1
PC
LAN
File Server
(user profiles,
redirected folders)
Active Directory,
DNS, DHCP
Farm
Site 1
HALB VS
Active
HALB
Passive
HALB
Secure
Gateway
Secure
Gateway
Secondary
Cconnection
Broker
Primary
Connection
Broker
RDSH
RDS host
RDSH
RDS host
RDSH
RDS host
Firewall
80/443
HTML
WAN
Location 2
Site 2
HALB VS
Active
HALB
Passive
HALB
Secure
Gateway
Secure
Gateway
Primary
Connection
Broker
Secondary
Connection
Broker
RDSH
RDS host
RDSH
RDS host
RDSH
RDS host
Firewall
80/443
PC
LAN
File Server
(user profiles,
redirected folders)
Active Directory,
DNS, DHCP

各サイトは、少なくとも RAS Connection Broker、RAS Secure Gateway (または複数の Secure Gateway) 、および RD セッション ホストまたは VDI サーバー、あるいは Windows PC にインストールされたエージェントで構成されます。

注： HALB の高可用性を追加するために、2 番目のアプライアンスを各サイトに展開できます。

リソースセットが類似している場合、エンド ユーザーは単一の RAS 接続を介して両方のサイトを使用できます。Parallels Client の RAS 接続プロパティとして次の設定を使用する必要があります。

Site 1 の LAN ユーザー

- プライマリ接続 – ローカル プライマリ Secure Gateway
- セカンダリ接続
  - ローカル セカンダリ Secure Gateway
  - Site 2 の HALB VS の IP アドレス

Site 2 の LAN ユーザー

- プライマリ接続 – ローカル プライマリ Secure Gateway
- セカンダリ接続
  - ローカル セカンダリ Secure Gateway
  - Site 1 の HALB VS の IP アドレス

WAN ユーザー

- プライマリ接続 – Site 1 の HALB VS の IP アドレス
- セカンダリ接続 – Site 2 の HALB VS の IP アドレス

RAS 接続設定は、(Parallels RAS コンソールのクライアント ポリシーを経由して) 一元的または手動で構成できます。

導入時の注意事項

RAS Connection Broker は、Parallels RAS インストーラーを使用してインストールされます (標準インストール) 。

HALB は、すぐに使用できる仮想アプライアンスとしてインストールされ、HALB VS プロパティで構成されます。

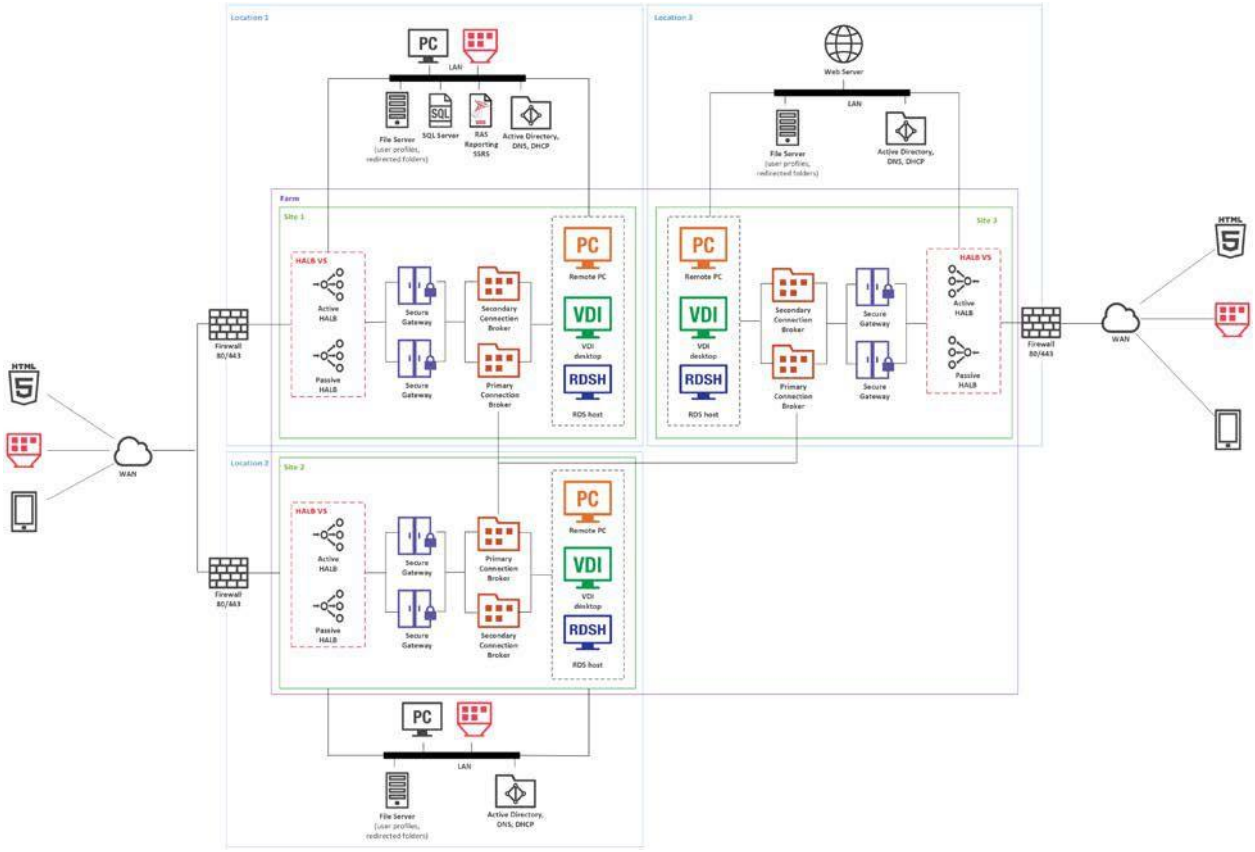
他のすべてのコンポーネントは、RAS コンソールからプッシュ インストールされます。

ビジネスの継続性とディザスタ リカバリ

Parallels RAS ファームの配置は、バックエンド リソースの場所によって異なります。したがって、バックエンド リソースが複製されるリモート ロケーションを追加し (適切なソフトウェアおよびハードウェア ソリューションはこのドキュメントの範囲外です) 、このロケーションにもう 1 つの Parallels RAS サイトを配置することで、運用を継続できます。

ディザスタ リカバリ サイトを設定してから、最も近いサイトをプライマリ接続として使用し、ディザスタ リカバリ サイトをセカンダリ接続として使用するように Parallels Client を設定することで、ユーザーは常にプライマリ サイトに接続でき、障害が発生した場合でもディザスタ リカバリ サイトを使用して作業を続けることができます。

Parallels Client 側の RAS 接続設定で、WAN ユーザーを招待して、すべてのサイトを使用し、最初のサイトの HALB VS IP アドレスをサーバー アドレスとして、2 番目と 3 番目のサイトの HALB VS IP アドレスをセカンダリ サーバーIP として設定できます。RAS 接続設定は、(Parallels RAS コンソールのクライアント ポリシーを経由して) 一元的または手動で構成できます。



導入時の注意事項

プライマリ RAS Connection Broker は、Parallels RAS インストーラーを使用してインストールされます (標準インストール) 。セカンダリ RAS Connection Broker は、RAS コンソールからプッシュ インストールされます。

HALB は、すぐに使用できる仮想アプライアンスとしてインストールされ、HALBVS プロパティで構成されます。

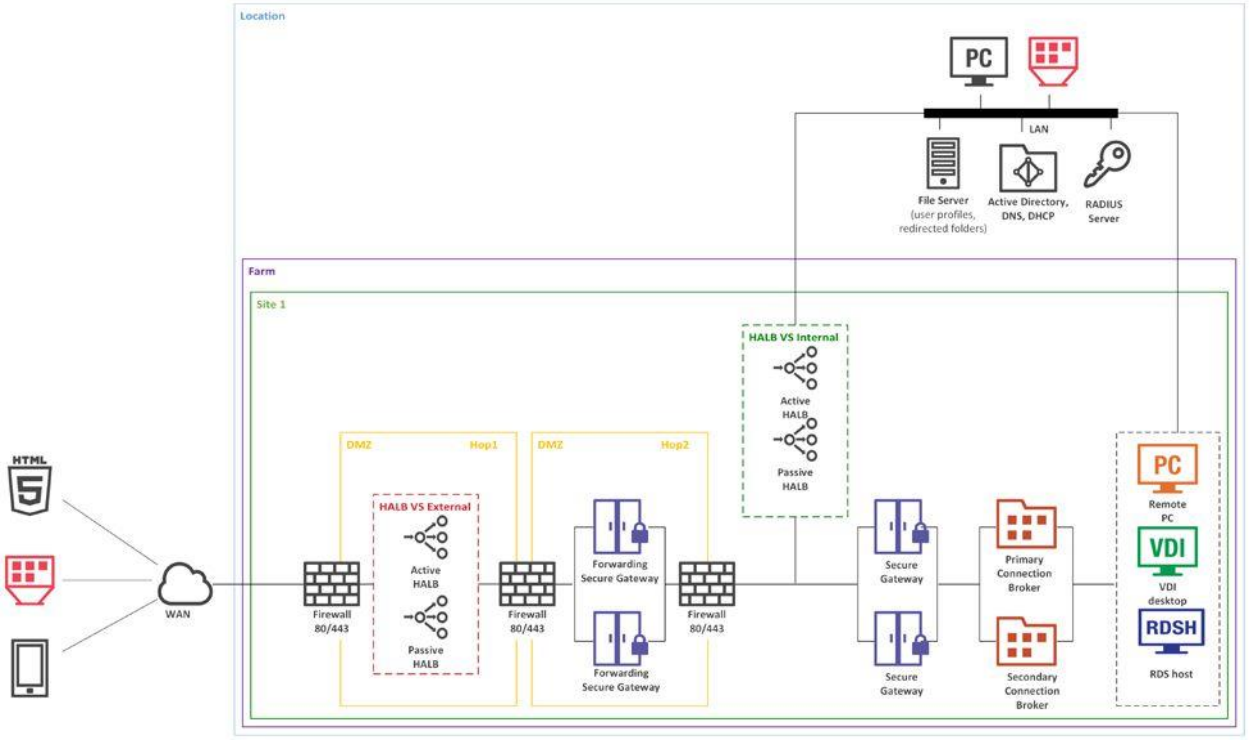
他のすべてのコンポーネントは、RAS コンソールからプッシュ インストールされます。

ダブルホップ DMZ と二段階認証による安全なセットアップ

二段階認証は、二要素認証用のさまざまなタイプのセキュリティ トークンを経由して高レベルの保護を提供します。ユーザーは、リモート アプリケーション リストを取得するために、連続する 2 つの段階を経て認証する必要があります。標準のユーザー名とパスワード、またはスマートカード認証に加えて、二段階認証では、トークンによって生成されたワンタイム パスワードが使用されます。第 2 段階の認証は、DualShield、Safenet、RADIUS、または Google 認証システムによって提供されます。

アプリケーションの列挙を高速化するために、RADIUS サーバーを RAS Connection Broker および Active Directory ドメインコントローラーと一緒にイントラネットに配置することをお勧めします。

アクセス制御リストを指定して、無線アクセスポイントおよびその他のデバイスが RADIUS サーバーと通信するために必要な IP アドレスとプロトコル/ポートのみを許可することをお勧めします。他のデバイスには、RADIUS サーバーへのパスがありません。



このタイプの構成では、RADIUS サーバーを介した第 2 レベルの認証が最初に実行されます。認証手順が成功すると、次の認証は、ユーザー名とパスワード、またはスマートカードのいずれかを使用して Active Directory レベルで実行されます。

導入時の注意

プライマリ RAS Connection Broker は、Parallels RAS インストーラーを使用してインストールされます (標準インストール) 。セカンダリ RAS Connection Broker は、RAS コンソールからプッシュ インストールされます。

HALB はすぐに使用できる仮想アプライアンスとしてインストールされ、HALB VS プロパティで構成されます。

他のすべてのコンポーネントは、RAS コンソールからプッシュ インストールされます。

SAML SSO 認証

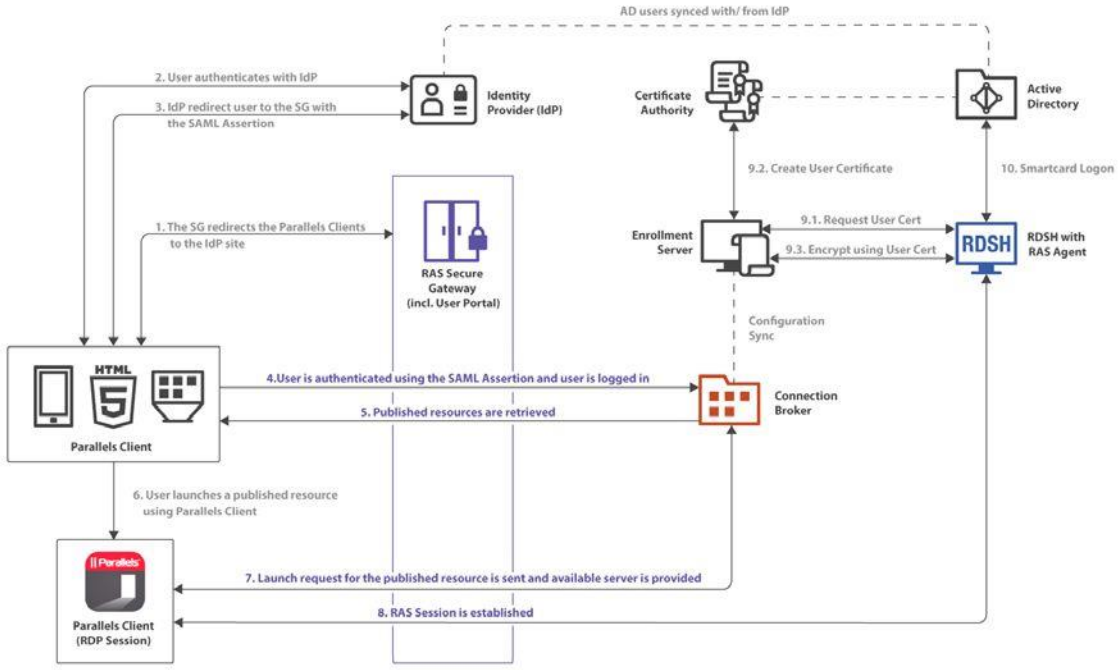
SAML 認証により、サービス プロバイダおよび複数の子会社を持つ企業は、ID 管理の負担を ID プロバイダにオフロードすることでコストを削減できます。サードパーティの ID プロバイダと統合することで、顧客とパートナーはエンド ユーザーに真の SSO エクスペリエンスを提供できます。

前述のシナリオと比較すると、新しいサーバーの役割をファームに追加する必要があります。SAML SSO プロセスの一部として、RAS Enrollment Server コンポーネントを備えた新しいホストは Microsoft Certificate Authority (CA) と通信して、ユーザーに代わってデジタル証明書を要求、登録、および管理し、ユーザーが Active を入力しなくても認証を完了します。

Parallels RAS は、次の配信オプションをサポートしています。

- Web Client
- Web Client ポータルによる Windows 用 SAML 認証
- Web Client ポータルによる Mac および Linux 用 SAML 認証
- Web Client ポータルによる Android および iOS 向け SAML 認証
- Parallels Client for Windows による SAML 認証
- Parallels Client for Mac による SAML 認証

以下の高レベルの論理図は、Parallels RAS 環境内の SAML 認証とログイン プロセスを示しています。



上の図の SAML 認証とログインの手順は次のとおりです。

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 ユーザーは IdP で認証します。

3 IdP は、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、ユーザーはログインします。

5 利用可能な RAS 公開済みリソースのリストが取得されます。

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、使用可能なサーバー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。

- 証明書が要求されます。
- 証明書が作成されます。
- 暗号化は、証明書を使用して実行されます。

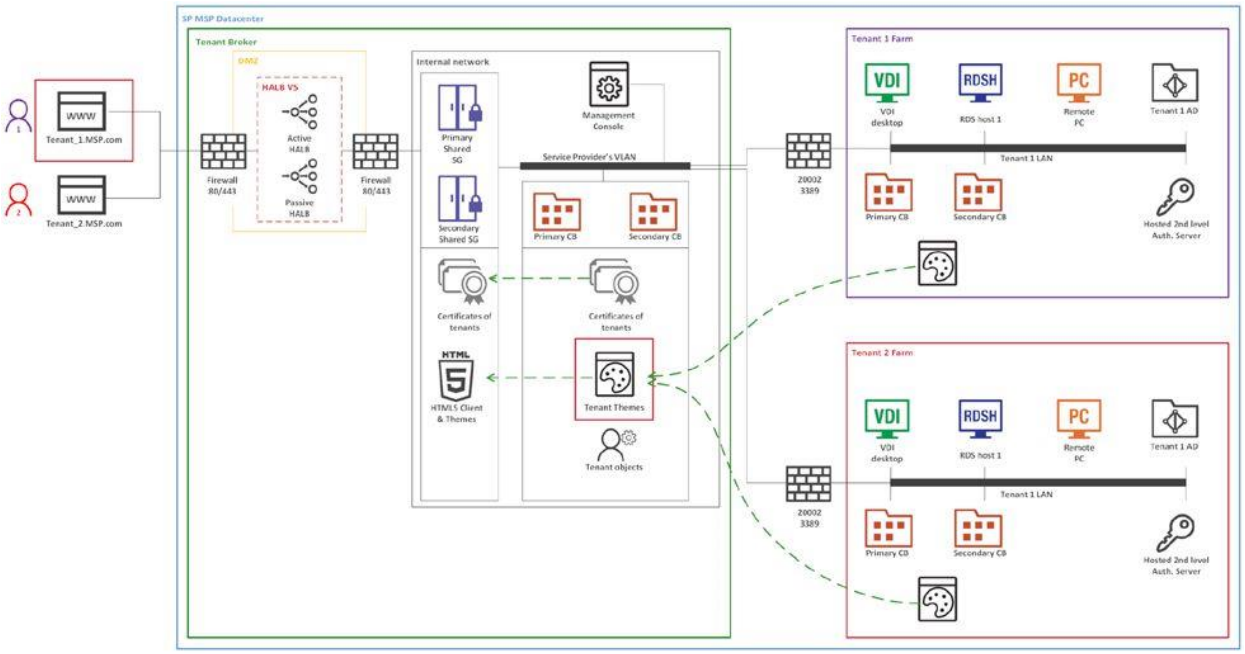
10 スマートカードログオンができます。

マルチ テナント アーキテクチャ

このシナリオは、個別のクライアント (部門、グループ、チームなど) の公開リソースを分離しておく必要がある環境に適しています。Parallels RAS マルチ テナント アーキテクチャにより、組織は、 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しながら、クライアント データを分離してコストを削減することができます。

RAS のマルチ テナント アーキテクチャは、サービス プロバイダや組織に対して以下のようなメリットを提供します。

- RAS Secure Gateway と HALB (High Availability Load Balancer) の台数を削減し、リソースの最大活用と統合によるコスト削減を実現。
- 新しいテナントや顧客の迅速な受け入れ。
- マルチ テナント環境の一元管理を簡素化。
- インフラ共有によるコスト拡張により、あらゆる規模の組織で運用コストを削減し、市場を拡大。



- テナントは、個別の RAS ファームまたはサイトとして展開されます。
- テナント ファームには、独自の RAS Secure Gateway と HALB は必要ありません。ただし、テナントが内部接続のために Secure Gateway や HALB を必要とする場合は導入が可能です。
- すべての外部ユーザーは、テナント ブローカー インフラストラクチャを通じてテナント ファームに接続します。

- テナントのネットワーク構成には、テナント Connection Broker とテナント ブローカーConnection Broker の接続が必要です。さらに、共有 RAS Secure Gateway は、公開リソースをホストするサーバーやテナント Connection Broker と通信する必要があります。これらの通信に必要なのは、以下に示す限られたオープン ポートだけです。
  - テナント Connection Broker > テナント ブローカーConnection Broker：ポート 20003
  - テナント ブローカー ゲートウェイ > テナント ブローカーConnection Broker：ポート 20002
  - テナント ブローカー ゲートウェイ > テナント Connection Broker：ポート 20002
  - テナント ブローカー 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
- テナント ドメインとの通信は、常にローカルのテナント Connection Broker から実行され、テナント ブローカー 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 アドレスを設定する必要があります。しかし、複数の固有ドメイン アドレスは、同じ IP アドレスに解決することができます。

導入時の注意

テナント ブローカー上の RAS Connection Broker は、Parallels RAS インストーラーからテナント ブローカー インストール オプションを使用してインストールします。

テナントの RAS Connection Broker は、Parallels RAS インストーラーから標準インストールを使用してインストールします。

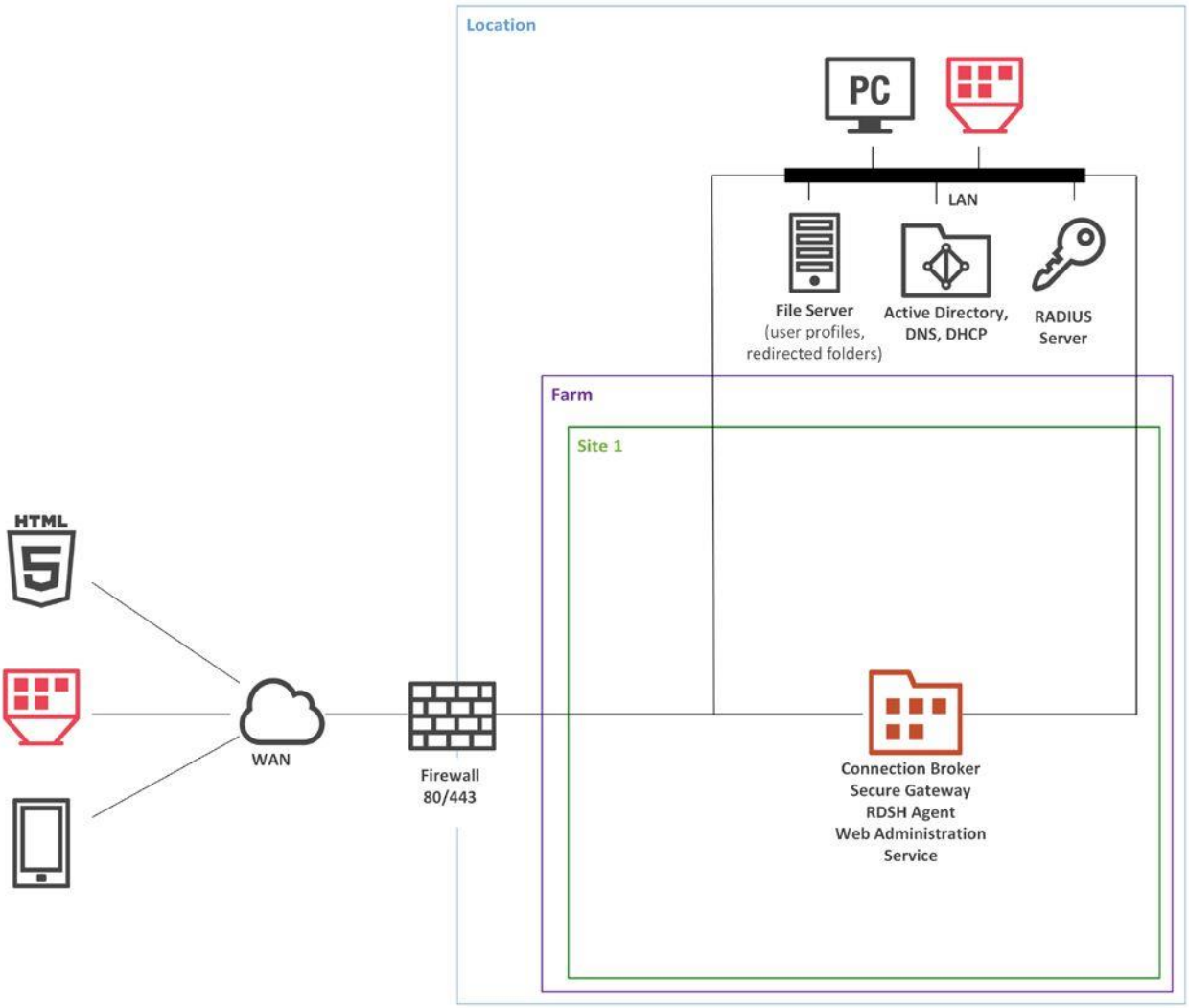
HALB はすぐに使える仮想アプライアンスとしてインストールされ、HALB VS のプロパティで設定されます。

その他のコンポーネントは、RAS コンソールからリモートでインストールされます。

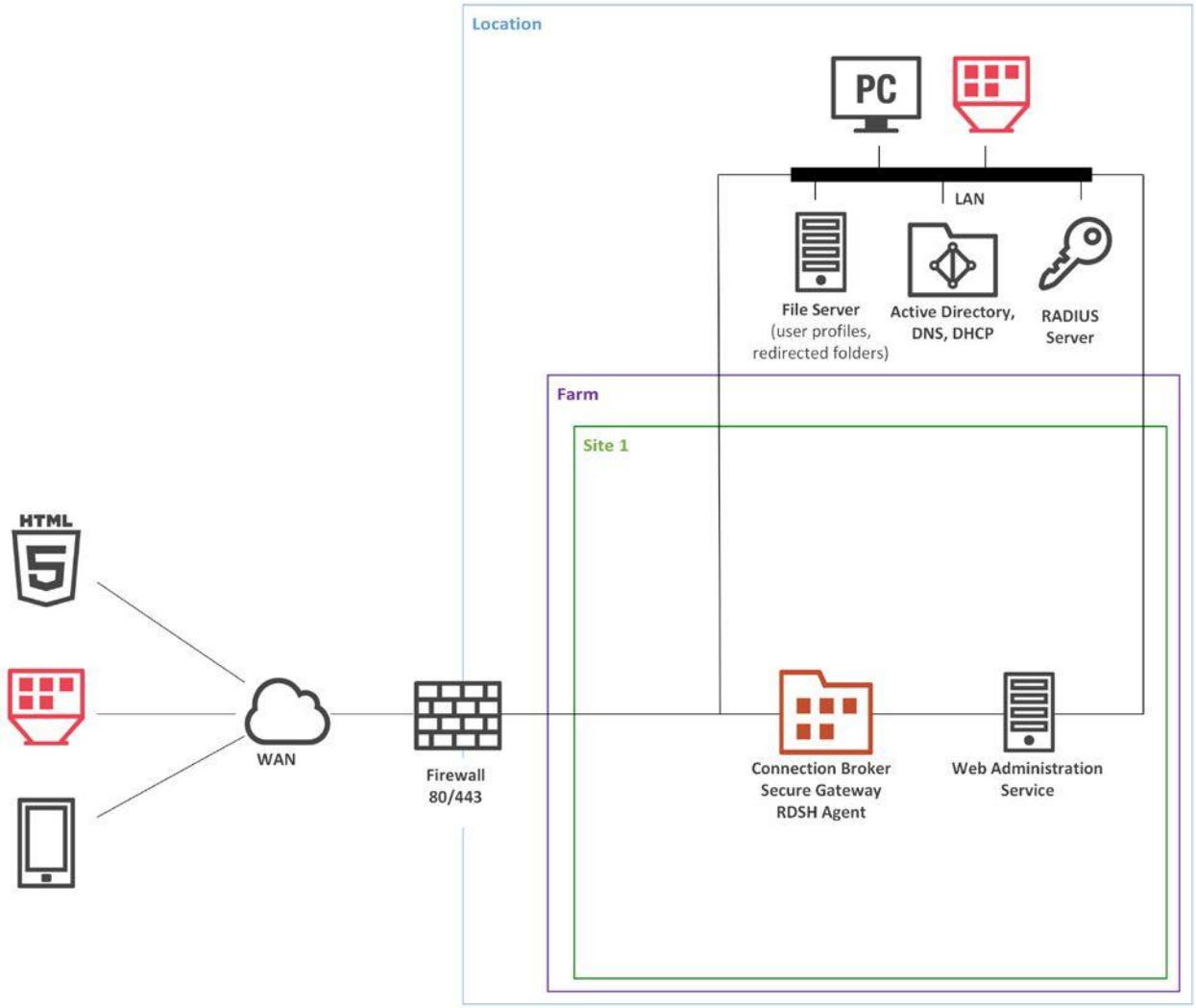
- テナント ブローカー コンポーネントは、テナント ブローカー コンソールからインストールします。
- テナント コンポーネントは、テナント コンソールからインストールします。

マネジメント ポータル

Parallels RAS Management Portal は、デスクトップまたはモバイル デバイスを使用して Parallels RAS 管理者が設定や日々の作業を行うために設計された、最新のウェブベースの設定・管理コンソールです。RAS Farm で RAS Management Portal を使用するには、RAS Web Administration Service 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、Connection Broker を搭載したマシン、または専用マシンにインストールすることができます。



このシナリオでは、RAS Web Administration Service を含むすべてのコンポーネントが、 1 つの RD セッション ホストにインストールされます。この構成は、概念実証や小規模な環境でのみ推奨されます。



導入時の注意

プライマリ RAS Connection Broker 上のコンポーネントは、Parallels RAS インストーラーを使用してインストールされます (標準インストール) 。

複数の管理作業を行う大規模な環境では、Connection Broker の負荷を軽減するために、RAS Web 管理サービスをホストする専用サーバーを使用することを推奨します。

導入時の注意

プライマリ RAS Connection Broker 上のコンポーネントは、Parallels RAS インストーラーを使用してインストールされます (標準インストール) 。

RAS Web Administration Service は、Windows インストーラーを使用してインストールされます (カスタム インストール) 。

クライアント マネージャーとデスクトップの置き換え

クライアント マネージャー機能を使用すると、管理者は Windows 7 以降を実行している 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 デバイスの登録が実行されると、デスクトップの置き換え、キオスクモード、電源オフ、再起動、シャドウなどの機能が利用できるようになります。

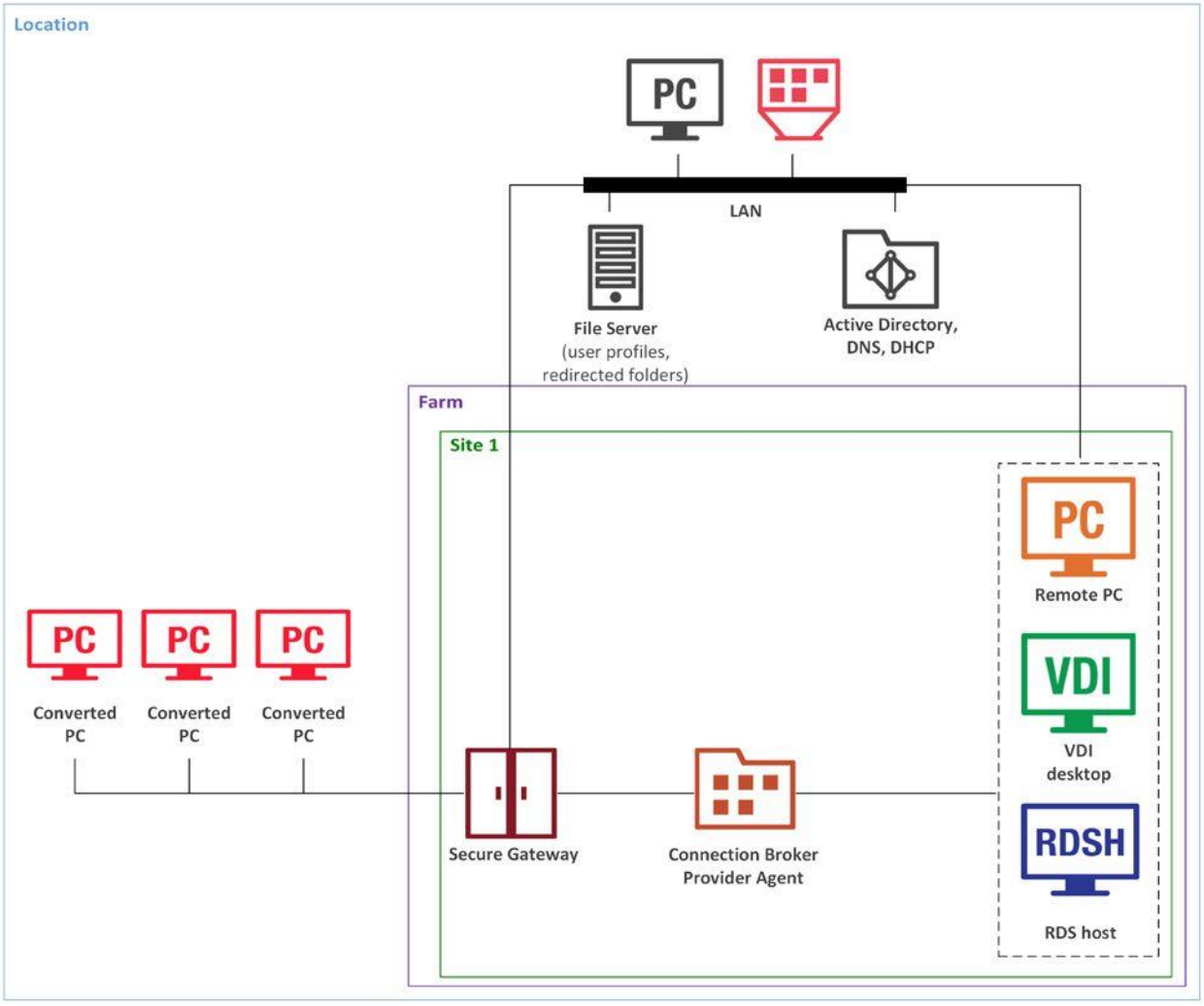
シャドーイング

シャドーイングは、完全な Windows クライアント デバイス デスクトップへのアクセスを提供し、システム上でローカルに実行されているアプリケーション、および Parallels RAS から公開されたリモート アプリケーションを制御できるようにします。シャドーイングには、Parallels RAS コンソールが実行されているマシンとデバイス自体をダイレクト接続する必要があります。

デスクトップの交換

デスクトップの置換オプションは、ユーザーがシステム設定を変更したり、新しいアプリケーションをインストールしたりすることを制限します。Windows デスクトップを Parallels Client に置き換えると、オペレーティング システム自体を置き換えることなく、Windows オペレーティング システムがシンクライアントのような OS に変わります。このように、ユーザーはクライアントからのみアプリケーションを展開できるため、管理者は接続されたデバイスをより高度に制御できます。

さらに、キオスクモードでは、ユーザーがコンピューターをシャットダウンしたり再起動したりすることはできません。



導入時の注意

RAS Connection Broker は、Parallels RAS インストーラーを使用してインストールされます (標準インストール) 。

他のすべてのサーバー側コンポーネントは、RAS コンソールからプッシュ インストールされます。

Parallels Client は、クライアント デスクトップ コンピューターにインストールされ、Parallels Client インストーラーを使用して Windows PC に変換されます。

第 3 章

容量に関する考慮事項

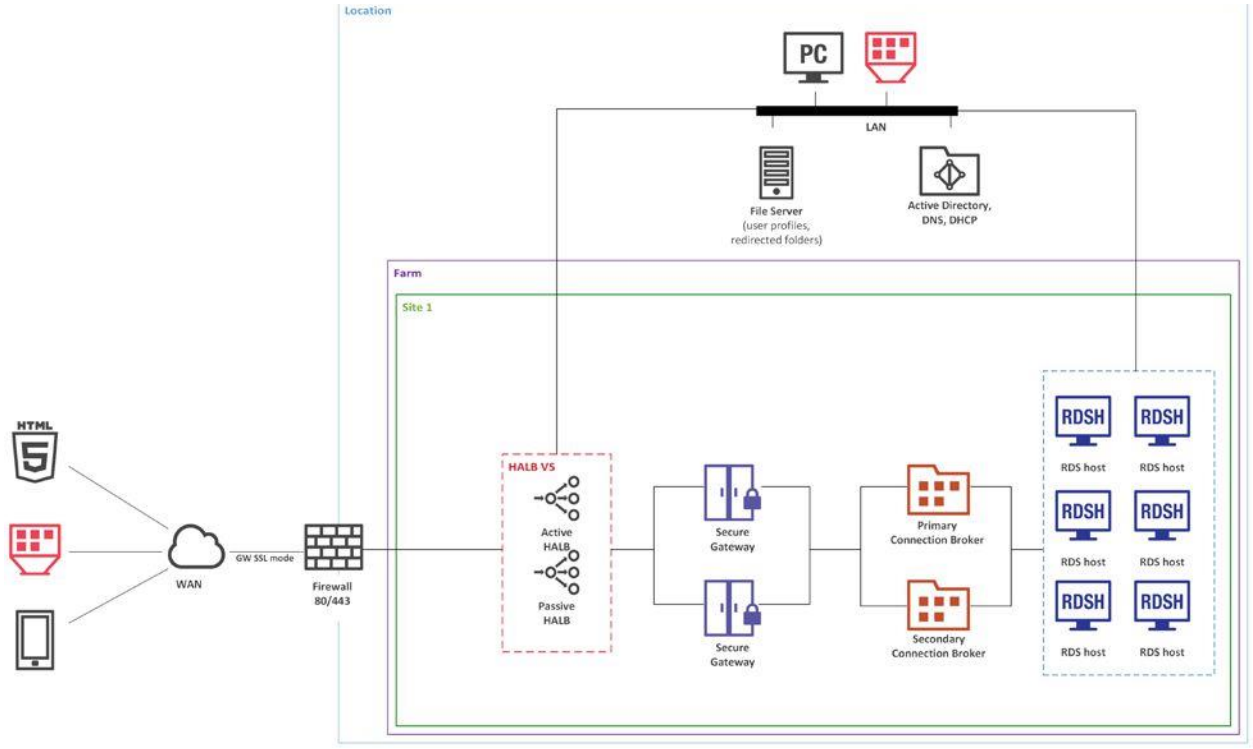
Parallels は、次のハードウェア コンポーネントで構成される合計 2 つの HP DL 360 を使用して、社内で Parallels RAS 負荷試験を実施しました。

コンポーネント	説明
CPU	2 x Xeon E 5 - 2670 v 1 , 2.6 GHz, 20 MB L3 , 115 W TDP
RAM	128 GB, 16 x 8 GB Micron DDR- 4 - 2100 at 1600 MHz
HDD	Westem Digital Blue 1 TB SSD

次の Parallels RAS ラボ環境が使用されました。

- ファームは 1 つのサイトで構成されます
- シングルホップ DMZ
- 各 Secure Gateway は、ゲートウェイ SSL モードで 1200 セッションをホストできます (SL + User Portal での RDP セッションの列挙とプロキシング) 。
- 各 Secure Gateway は、User Portal を有効にし、同じポート 443 を使用して HALB でバランスを取っています。 (URL https://HALB-VIP/userportal/ を使用する場合、SSL セッション パーシスタンスがあるため、着信接続は適切に分散されます) 。

> **注：** SSL およびユーザー ポータルを有効にするには、サーバー証明書のインストールが必要です。



250 ユーザー

Parallels RAS は、次のように Windows 2016 Server 上の VMware Sphere 6.5 に導入されました。

Parallels RAS コンポーネント	総 VM 数	各 VM の vCPU 数	各 VM の RAM 数
RAS Connection Broker	2	2	4 GB
RAS Secure Gateway	2	2	4 GB
High Availability Load Balancing	2	1	2 GB
RD Session Host	6	6	24 GB

- すべてのコンポーネントを二重化して冗長性を確保
- 冗長性のための RDSHN + 1

上記の構成は、内部ツールと Login VSI の両方でテストされています。詳細については、次の URL で入手できる [**Parallels RAS Scalability Testing with Login VSI**] ペーパーを参照してください。

https://download.parallels.com/ras/v19/docs/ja_JP/Parallels-RAS-Scalability-Testing-Login-VSI_JA.pdf

500 ユーザー

Parallels RAS は、次のように Windows 2016 Server 上の VMware vSphere 6.5 に導入されました。

Parallels RAS コンポーネント	総 VM 数	各 VM の vCPU 数	各 VM の RAM 数
RAS Connection Broker	2	2	4 GB
RAS Secure Gateway	2	2	4 GB
High Availability Load Balancing	2	1	2 GB
RD Session Host	12	6	24 GB

- すべてのコンポーネントを二重化して冗長性を確保
- 冗長性のための RDSHN + 2

1000 ユーザー

Parallels RAS コンポーネント	総 VM 数	各 VM の vCPU 数	各 VM の RAM 数
RAS Connection Broker	2	2	4 GB
RAS Secure Gateway	2	2	4 GB
High Availability Load Balancing	2	1	2 GB
RD Session Host	24	6	24 GB

- すべてのコンポーネントを二重化して冗長性を確保
- 冗長性のための RDSHN + 4

第 4 章

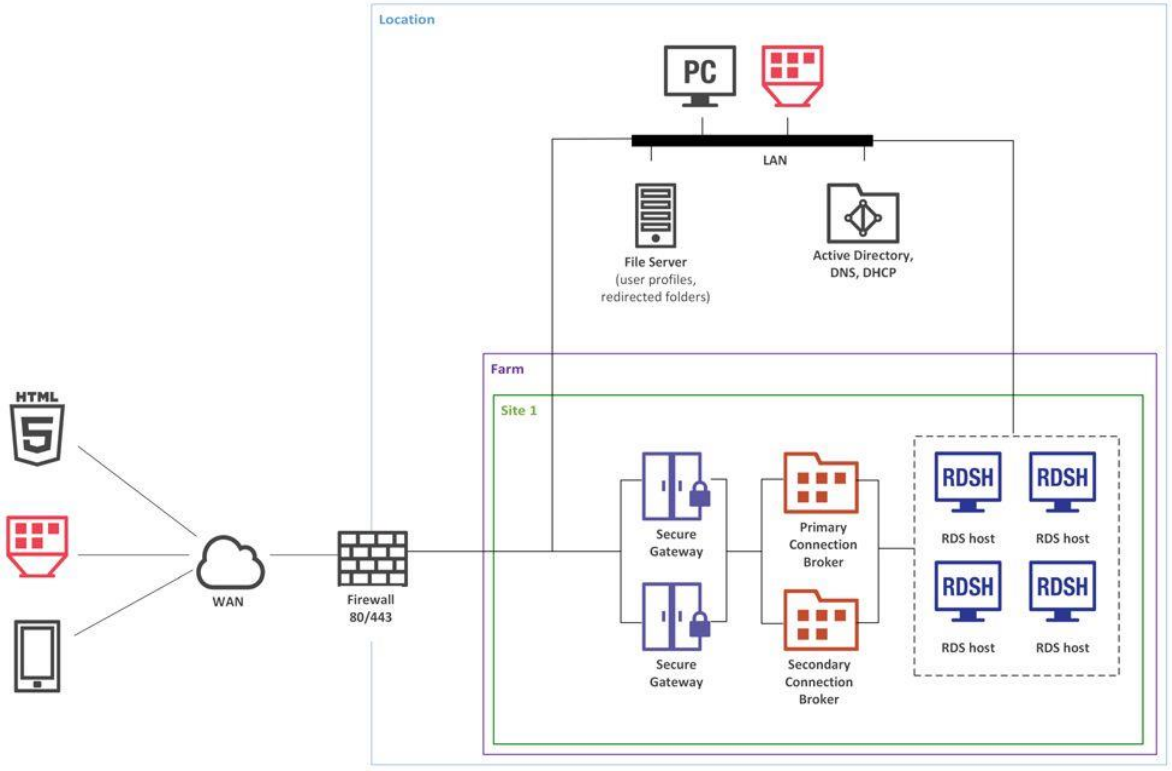
Parallels RAS レポートの展開

この章では、Parallels RAS レポートを展開するための一般的なシナリオについて説明します。

この章の内容

複数の RD セッション ホストを備えた 1 つのサイト

RAS レポートは、Microsoft SQL Server および SQL Server Reporting Services (SSRS) に依存しています。小規模な環境では、SQL Server データベース インスタンス、SSRS、および RAS レポートを、プライマリ RAS Connection Broker が実行されている同じサーバーにインストールできます。



導入時の注意

プライマリ RAS Connection Broker は、Parallels RAS インストーラーを使用してインストールされます (標準インストール) 。

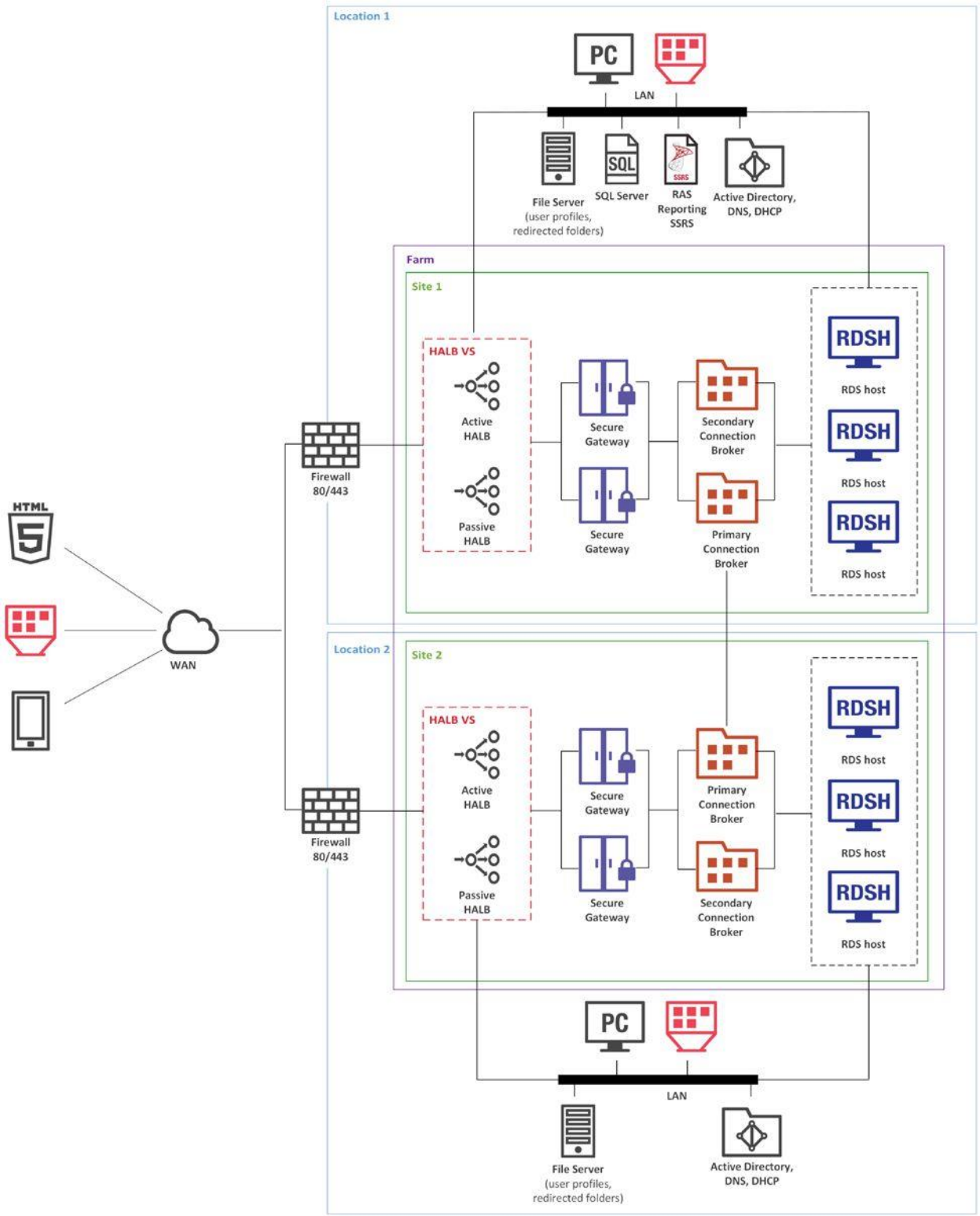
セカンダリ RAS Connection Broker は、RAS コンソールからプッシュ インストールされます。

RAS レポートは、Parallels RAS インストーラーを使用してインストールされます。

他のすべてのコンポーネントは、RAS コンソールからプッシュ インストールされます。

複数の RD セッション ホストとリモート SQL Server を備えた複数のサイト

マルチサーバー環境で実行されている Parallels RAS インストールの場合、RAS Reporting と SSRS 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。SQL Server データベース エンジンも専用サーバーにインストールする必要がありますが、SSRS および RAS レポートと一緒にインストールできます。


Location 1
PC
LAN
File Server
(user profiles,
redirected folders)
SQL Server
RAS
Reporting
SSRS
Active Directory,
DNS, DHCP
Farm
Site 1
HALB VS
Active
HALB
Passive
HALB
Secure
Gateway
Secure
Gateway
Secondary
Connection
Broker
Primary
Connection
Broker
RDSH
RDS host
RDSH
RDS host
RDSH
RDS host
Firewall
80/443
HTML
WAN
Location 2
Site 2
HALB VS
Active
HALB
Passive
HALB
Secure
Gateway
Secure
Gateway
Primary
Connection
Broker
Secondary
Connection
Broker
RDSH
RDS host
RDSH
RDS host
RDSH
RDS host
Firewall
80/443
PC
LAN
File Server
(user profiles,
redirected folders)
Active Directory,
DNS, DHCP

インストールに関する注意事項

プライマリ RAS Connection Broker は、Parallels RAS インストーラーを使用してインストールされます (標準インストール) 。セカンダリ RAS Connection Broker は、RAS コンソールからプッシュ インストールされます。

HALB は、すぐに使用できる仮想アプライアンスとしてインストールされ、HALBVS プロパティで構成されます。

RAS レポートは、Windows インストーラーを使用してインストールされます。

他のすべてのコンポーネントは、RAS コンソールからプッシュ インストールされます。

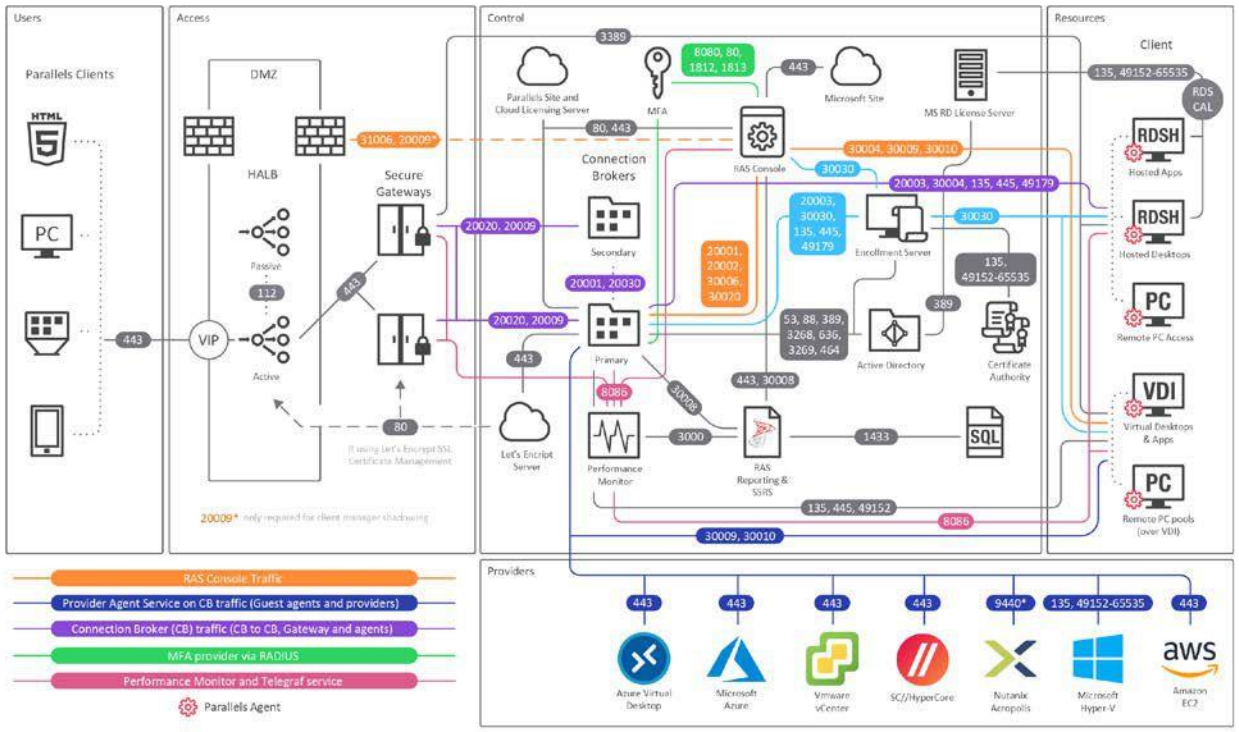
第 5 章

ポート参照と SSL 証明書

この章の内容

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、Web ブラウザで原寸大の図が表示されます。https://download.parallels.com/ras/v18/docs/en_US/Parallels-RAS-18-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	80, 443	管理およびユーザー セッション接続。
		TCP, UDP	20009	ファイア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) 。
	転送モードでの RAS Secure Gateway	TCP, UDP	80, 443	管理およびユーザー セッション接続。
		TCP, UDP	3389	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) 。
		UDP	20000	Secure Gateway はブロードキャストを検索します。
	通常モードでの RAS Secure Gateway	TCP, UDP	80, 443,	管理およびユーザー セッション接続。
		TCP, UDP	3389	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) 。
		TCP, UDP	20009	ファイア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)
		UDP	20000	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, Remote PC)	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	443	Azure Virtual Desktop Gateway 接続。
		UDP	3390	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

Web ブラウザ

ソース	宛先	プロトコル	ポート	説明
Web ブラウザ (HTML 5) と Let's Encrypt サービス	RASWeb 管理サービス (RAS 管理ポータル)	TCP	20443	管理者は RAS 環境の HTML 5 ベースの管理ポータルにアクセスします。
	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、ポート 80 と 443 は受信リクエストに対してオープンである必要があります。
	RAS Secure Gateway	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、ポート 80 と 443 は受信リクエストに対してオープンである必要があります。

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。
	転送モードでの RAS Secure Gateway	TCP, UDP	80, 443	管理およびユーザー セッション接続。
	通常モードでの 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。 ファイア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
転送モードでの RAS Secure Gateway	通常モードでの 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。
通常モードでの 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	20002	RAS Connection Broker サービスのポート - RAS Secure Gateway と RAS コンソールの通信 (通常モードのみ) 。

		TCP, UDP	20009	RAS コンソールが RAS Connection Broker 上で実行されている場合、ファイア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 ポータルの Web サーバーとの通信 (NodeJS) 。

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 エージェント	TCP, UDP	30004	Connection Broker サーバーのリクエスト。
	RAS Provider Agent	TCP, UDP	30006	Provider Agent の通信ポート。
	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) 。
	2 FA 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 エージェント 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 Service	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 コンソール

ソース	宛先	プロトコル	ポート	説明
RAS コンソール	RAS レポート	TCP	30008	RAS コンソールは、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 コンソールからシャドーイング。
	RAS RD セッション ホスト エージェント	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 への RAS ブラウザ プラグイン接続。
	RAS Connection Broker	TCP	20002, 20001	Connection Broker および冗長サービスとの通信。
	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 コンソールでは、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 コンソールは 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) 。

RASWeb 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
RASWeb 管理サービス	RAS RD セッション ホスト エージェント	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	CB 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 エージェント 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 エージェント	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	CB 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 の通信ポート。
	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	TCP	135, 49152 - 65535	ゲ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 エージェント

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 エージェント	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 エージェント (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 Remote 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

SSL 証明書

このセクションでは、Parallels Application Server の展開で SSL 証明書を使用する方法について説明します。このガイドで説明した 1 つ以上の展開シナリオをテストするために RAS 環境をセットアップする場合は、このセクションをお読みください。

注：詳細については、「**Parallels RAS 管理者ガイド**」の [**SSL 証明書管理**] の章を参照してください。

デフォルトでは、自己署名証明書は RAS Secure Gateway にインストールされます。各 RAS Secure Gateway には独自の証明書があり、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。

Parallels Client の構成を簡素化するために、サードパーティの信頼できる認証局またはエンタープライズ認証局 (CA) のいずれか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。

エンタープライズ CA 証明書が使用されている場合、Windows クライアントは Active Directory からエンタープライズのルート証明書または中間 CA 証明書を受け取ります。他のプラットフォームのクライアントデバイスは手動で構成する必要があります。

広く利用されている信頼できる認証局 (Verisign など) によって発行されたサードパーティの証明書が使用されている場合、クライアント デバイスは、プラットフォームの信頼できる認証局の更新を使用して信頼します。

サードパーティの信頼できる認証局の使用

CSR の生成

サードパーティの CA から証明書を取得するには、以下に説明するように、証明書署名要求 (CSR) を生成する必要があります。

RAS コンソールで、**[ファーム] > [サイト] > [証明書]** に移動します。**[タスク] > [証明書要求の作成]** 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てください。

- **名称**：この証明書の名前を入力します。このフィールドは必須です。
- **説明**：オプションの説明。
- **使用法**：証明書を RAS Secure Gateway または HALB、あるいはその両方に使用するかどうかを指定します。この選択は必須です。
- **キーサイズ**：証明書のキーサイズ (ビット単位) 。ここでは、事前定義値から選択できます。デフォルトは 2048 ビットです。これは、現在の業界標準に従って必要な最小の長さです。
- **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。
- **市区町村**：市区町村名。
- **組織**：組織の名前。
- **部門**：部門の名前。
- **メールアドレス**：あなたの E メールアドレス。このフィールドは必須です。
- **コモンネーム**：コモンネーム (CN) 。完全修飾ドメイン名 (FQDN) とも呼ばれます。このフィールドは必須です。

情報を入力したら、[**生成**] 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 コンソールに表示され、[**状態**] 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。

証明書のインポート

証明書を Parallels RAS にインポートする必要があります。その為には、[**証明書**] タブで、**[タスク] > [証明書をインポート]** 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。
- **使用法**：証明書に 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 コンソールのリストに表示され、[**状態**] 列には [**インポート済み**] と表示されます。

証明書情報を表示するには、証明書を右クリックして [**プロパティ**] を選択します。表示されたダイアログでプロパティを確認し、[**証明書情報の表示**] ボタンをクリックして、証明書の信頼に関する情報、詳細、照明のパス、および証明書の状態を表示してください。もしくは、証明書情報を右クリックして [**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の場合、[プロパティ] ダイアログに [中間] タブが追加されます。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、このタブに中間証明書が表示されます。必要に応じて、別の中間証明書をこのタブに貼り付けることもできます。

エンタープライズ認証局の使用

IIS を使用して、エンタープライズ CA から証明書を受信し、証明書を PFX 形式でエクスポートします。Parallels RAS に PFX 証明書をインストールするには、上記の [**証明書のインポート**] サブセクションの説明に従ってインポートします。

注： Parallels Client 側の trusted.pem ファイルには、サードパーティベンダーからの証明書を検証できるようにするための中間証明書が含まれている必要があります。ベンダーの中間証明書が trusted.pem ファイルにない場合は、手動で貼り付けるか、適切な中間証明書を使用して trusted.pem テンプレートファイルを作成してから、古い trusted.pem ファイルを新しく更新されたものに置き換える必要があります。このファイルは、クライアント側の Program Files\Parallels or Program Files(x86)\Parallels にあります。

証明書のゲートウェイへの割り当て

証明書をサイトに追加した後、証明書の作成時に指定した使用法の種類に応じて、RAS Secure Gateway または HALB、あるいはその両方に証明書を割り当てることができます (この章の冒頭で説明しています) 。証明書の [**使用法**] オプションについては、以下にて詳しく説明します。

証明書の使用方法

証明書の [**使用法**] 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 または HALB、あるいはその両方で使用できるようにするかどうかを指定します。このオプションを設定する場合、以下から選択できます。

- **ゲートウェイ**：RAS Secure Gateway で証明書を利用できるようになります
- **HALB**：HALB で証明書を利用できるようになります

上記のオプションのどちらか、または両方を選択できます。両方を選択すると、Secure Gateway と HALB の両方で証明書が利用できるようになります。

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。証明書を選択する際は、特定の証明書に対して [**使用法**] オプションがどのように構成されているかに応じて、次のオプションを使用できます。

- **<一致する使用方法すべて>**：これはデフォルトのオプションであり、常に使用できます。このオプションは、[**使用法**] の選択値がオブジェクトタイプ (Secure Gateway または HALB) に一致する証明書が使用されることを意味します。たとえば、Secure Gateway を構成していて、[**使用法**]が「Gateway」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。証明書の使用法オプションで [**Gateway**] 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 Secure Gateway 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 でも同様に機能します。なお、このオプションが Secure Gateway や HALB で選択されているものの、一致する証明書が 1 つも存在しない場合は、警告メッセージが表示されます。この場合、最初に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 [**使用法**] の設定に応じて、リストに表示される場合と表示されない場合があります。たとえば、HALB の LB SSL ペイロードを構成し、[**使用法**] 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、[**使用法**] が「Secure Gateway」に設定されている証明書はリストに表示されません。

別の例として、1 つの証明書だけですべての Secure Gateway を使用したい場合は、証明書を作成し、[**使用法**] オプションを「ゲートウェイ」に設定する必要があります。次に、各 Secure Gateway にこの証明書を使用するように構成するか、または [**<一致する使用方法すべて>**] の選択値をデフォルト値のままにします。この場合、証明書は Secure Gateway 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。

Secure Gateway

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] > [ゲートウェイ]** に移動します。
2. Secure Gateway を右クリックして、[**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。このオプションでは、使用法が Secure Gateway に設定されているか、あるいは Secure Gateway と HALB の両方に設定されている証明書が使用されます。

Parallels Client の構成

証明書が自己署名されている場合、または証明書がエンタープライズ CA によって発行されている場合、Parallels Client は次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 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を使用して SSL 経由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) 。