Parallels Remote Application Server
管理ポータルガイド

19.3

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

目次

第　1　章

はじめに

この章の内容

Parallels RAS 19 リリース履歴

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

Parallels RAS バージョン	リリース	日付
19.0	初回リリース	2022/07/27
19.0	Update 1	2022/08/31
19.0	ホットフィックス 1	2022/09/16
19.0	ホットフィックス 2	2022/09/30
19.0	ホットフィックス 3	2022/10/14
19.1	Update 2	2022/11/15
19.2	Update 3	2023/07/06
19.3	初回リリース	2023/10/17

概要

Parallels® RAS 管理ポータルは、デスクトップ/ラップトップコンピューターまたはモバイルデバイスを使用して構成と日常のアクティビティを実行する Parallels RAS 管理者向けに設計された、最新のウェブベースの構成および管理コンソールです。

Parallels RAS 管理ポータルは、管理者に次の機能を提供します。

- 重要な Parallels RAS コンポーネント（RD セッションホスト、Connection Broker、Secure Gateway など）を一元的に展開、管理、および構成します。
- RD セッションホストからさまざまなリソースを公開します。
- FSLogix プロファイルコンテナーの設定を構成します。
- 印刷とスキャンの設定を構成します。
- SSL 証明書を管理します。
- 接続設定と MFA（Google 認証または Microsoft 認証などの他の時間ベースのワンタイムパスワード（TOTP）アプリ）を構成します。
- ユーザーセッションを監視および管理します。
- 管理者アカウントとセッションを管理します。
- メールボックスを構成します。
- ライセンスを管理します。
- サポートに連絡し、必要なシステムレポートを提供してください。

注: デスクトップベースの Parallels RAS Console で現在利用可能な多くの機能は、本ツールが Parallels RAS のメイン管理ツールとして採用されるようになる前に、今後のリリースで管理ポータルに含められる予定です。

Parallels RAS 管理ポータルに含まれる Azure Virtual Desktop の管理機能は実験的なものであり、今後のバージョンでリリースされる予定です。

新機能

Parallels RAS 19.3

Parallels RAS 19.3 には、以下の新機能が追加されました。

- FSLogix Office コンテナーのサポートと FSLogix の管理強化（p. 37）。
- Added RADIUS をプロバイダーとして追加する（p. 27）。
- サードパーティの IdP を介したユーザーパスワードの変更機能（p. 24）。

Parallels RAS 19.2

Parallels RAS 19.2 には、以下の新機能が追加されました。

- Parallels Client と RDSH 上のサーバー間の接続にトランスポートプロトコルを選択する機能（p. 47）
- Microsoft Azure を TOTP プロバイダーとして追加（p. 26）。

第　2　章

インストールと構成

この章の内容

前提条件

RAS 管理ポータルは HTML5 をサポートする最新の Web ブラウザー（Internet Explorer 以外）で動作させることができます。

Windows サーバーに次のアップデートがインストールされていることを確認してください（RAS 管理ポータルはアップデートに依存します）。

- Windows Server 2012 R2: KB2999226

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

このウェブサービスは、デフォルトで次のポートでウェブリクエストをリッスンします。

- HTTPS: 20443
- HTTP: 20080

インストール

RAS ファームで RAS 管理ポータルを有効にするには、RAS ウェブ管理サービスコンポーネントをインストールする必要があります。このコンポーネントは、”標準”インストールオプションを使用して Parallels RAS をクリーンインストールすると自動的にインストールされます。また、”カスタム”インストールオプションを使用して、インストールするコンポーネントに”RAS ウェブ管理サービス”を選択して、インストールすることもできます。たとえば、RAS 管理ポータルを専用マシンにインストールしたい場合は、”カスタム”インストールオプションを使用し、インストールするコンポーネントとして”RAS ウェブ管理サービス”を選択します。

RAS ウェブ管理サービスをインストールした後、設定を行う必要があります。つまり、RAS 管理ポータルで管理する RAS ファームを指定したり、いくつかのパラメーターを設定したりする必要があります。詳しい説明については、「RAS ウェブ管理サービスの構成」（p. 13）を参照してください。

第 3 章

RAS 管理ポータルの使用を開始する

この章の内容

RAS 管理ポータルへのログイン

RAS ウェブ管理サービスをインストールしたマシンで RAS 管理ポータルを開くには、[アプリ] > [Parallels] に移動し、[Parallels RAS 管理ポータル] をクリックします。

リモートコンピューターから RAS 管理ポータルにログインするには、ウェブブラウザーに以下の URL を入力します:

```
https://<server-address>:20443
```

<server-address> は、RAS ウェブ管理サービスがインストールされているサーバーの FQDN または IP アドレスです。デフォルトでは、HTTPS 接続にはポート 20443 が使用されます。「RAS ウェブ管理サービスの設定」(p. 13) で説明されているように、必要に応じてポート番号を変更することができます。

[ようこそ] ページで、RAS 管理者のユーザー名とパスワードを入力し、[サインイン] をクリックします。

RAS ウェブ管理サービスの構成

最初に、以下のように RAS ウェブ管理サービスを構成する必要があります。

1 RAS 管理ポータルで、右上の [ユーザー] アイコンをクリックし、[管理ポータルの構成] を選択します。

2 再度サインインを求められます。なお正常にサインインするためには、RAS ウェブ管理サービスがローカルサーバー上で稼働している必要があります。これは、リモートサーバーのユーザーが RAS ウェブ管理サービスの構成ページアクセスするのを防ぐためです。

3 ローカル管理者またはドメイン管理者のメンバーのユーザー名とパスワードを入力し、 [サインイン] をクリックします。

4 [RAS 管理ポータルの構成] ページが開きます。

5 [RAS ファームアドレス] フィールドに、この RAS 管理ポータルで管理する RAS ファームのアドレスを指定します。これは、ファームにインストールされている RAS Connection Broker のアドレスです。

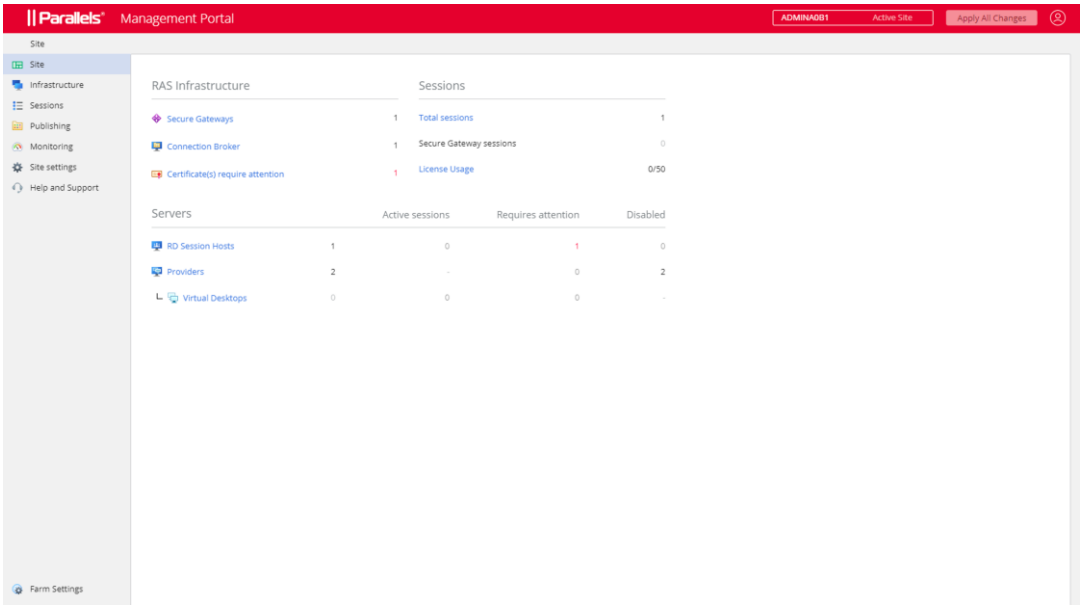
6 [詳細設定] セクションで以下を指定します。

- 証明書：この接続に使用する証明書です。[アップロード] をクリックして、証明書を選択します。
- 証明書のパスワード: 証明書のパスワードです。
- ポート: RAS 管理ポータルが接続を待機するポート番号です。デフォルトのポートは 20443 です。この番号は、RAS Secure Gateway ポートと競合しないように設定されています。可能であれば 443 に変更することもできます。その場合、接続 URL にポート番号を含める必要はありません。また、任意のカスタムポートに変更することも可能です。たとえば、デフォルトの”URL”：”https://*:20443”を”URL”：”http://*:20080”に変更できます。
- 管理セッションのタイムアウト: 管理者セッションが切断されるまでの時間です。
- ポーリング間隔: RAS 管理ポータルで表示されている情報を更新する間隔です。多数の管理者が同時に作業している場合や、多数のホストまたセッションなどが存在する場合は、この値を最大 30 秒まで増やすことができます。

7 完了したら、[保存] をクリックします。

RAS 管理ポータルのユーザーインターフェイス

RAS 管理ポータルのすべてのナビゲーションは、管理カテゴリーをリストアップした左のサイドバーから開始します。デフォルトではサイトカテゴリーが選択されています。



カテゴリー

次の表は、RAS 管理ポータルで管理できる、利用可能なすべてのカテゴリーの一覧です。ルート管理者は、すべてのカテゴリーを閲覧および管理することができます。他の種類（上級、カスタム）の管理者は、特定のカテゴリーを閲覧するのに権限が必要になる場合があります。

カテゴリー	記述
サイト	現在のサイト概要を表示します。
インフラ	RD セッションホスト、VDI、Gateway、Connection Broker などの RAS インフラストラクチャの管理。
セッション	セッション管理。
公開	公開リソースおよび公開済みリソースの管理。
監視	RAS Performance Monitor

サイト設定	接続、認証、FSLogix、ユニバーサルプリント、スキャン。
ヘルプとサポート	ヘルプとサポート。
ファーム設定	左側のサイドバーの下部に表示されるこのカテゴリーでは、管理者、メールボックス、ライセンスなど、ファームのグローバルな設定を管理します。

各カテゴリーについては、このガイドの後半で詳しく説明します。

管理権限

デスクトップの RAS Console で構成された管理者権限によっては、RAS 管理ポータルの一部のカテゴリーや処理が表示されない、または許可されない場合があります。管理者権限の設定方法については、「Parallels RAS 管理者ガイド」を参照してください。このガイドでは、「管理者アカウントの権限」のトピックを探します。このガイドは、Parallels のウェブサイト（https://www.parallels.com/products/ras/resources/）でご覧いただけます。

サブカテゴリー

一部のカテゴリーにはサブカテゴリーがあります（インフラストラクチャおよびサイト設定）。カテゴリーを選択すると、RAS 管理ポータルの右側に、サブカテゴリーを選択できる 1 つまたは複数の追加ペインが表示されることがあります。

ナビゲーションバー

一部のコンポーネントでは、設定や情報が機能ごとにまとめられています（概要、プロパティ、セッションなど）。コンポーネントのプロパティを表示すると、中央にナビゲーションバーが表示され、これらの設定を参照することができます。ナビゲーションバーで項目を選択すると、その設定内容が右側ペインに表示されます。

ブレッドクラム

カテゴリー、サブカテゴリー、個別の項目を選択すると、ページ上部にブレッドクラムが表示され、現在の位置がわかります。1 ステップ以上戻るには、リストのリンクをクリックします。

ページのヘッダー項目

ページのヘッダーには以下の項目があります:

- ファームと現在のサイトの名前。複数のサイトがある場合は、ドロップダウンリストから選択することができます。RAS 管理ポータルがそのサイトに切り替わり、サイトのコンポーネントを管理できるようになります。
- ”ユーザー”アイコンはドロップダウンリストになっており、以下の項目があります。現在のユーザー名（例: Administrator）、詳細（[詳細] ダイアログを開く）、フィードバックを行う（Parallels にフィードバックを行うウェブページに移動する）、管理ポータルの構成（p. 13）、ログアウト（ログアウトする）。
- すべての変更を適用: このボタンで、RAS 管理ポータルで行った変更をファームのコンポーネントに適用します。コンポーネントやオブジェクトを作成したり変更したりしても、その変更がファームのコンポーネントに自動的に適用されることはなく、サイトやファームに影響を与えることもありません。[すべての変更を適用] ボタンをクリックすると、ファームやサイト全体に変更が適用されます。なお、変更のたびにこのボタンをクリックする必要はありません。異なる領域で複数の変更を必要とする作業を行っている場合は、すべての変更を完了してから [すべての変更を適用] ボタンをクリックすると、すべての変更がまとめて適用されます。

編集

いずれかの設定を変更できるビューを開いたとき、そのビューは通常、読み取り専用になります。編集を有効にするには、右上の [編集] ボタンをクリックします。ボタン名が [保存] に変わります。編集が終わったら、[保存] をクリックします。変更内容を破棄する場合は、[キャンセル] をクリックします。

なお、ある管理者が編集可能な状態にしたオブジェクトは、他の管理者が同時に編集することはできませんのでご注意ください。このようなオブジェクトの編集を有効にしようとすると、エラーが発生して、オブジェクトをロックしている管理者の名前が表示されます。

編集ツールバー

一部のビュー（特にリスト）では、右上にツールバーがあり、そこから処理を実行することができます。ツールバーの項目名を見るには、マウスでその項目にカーソルを合わせます。ツールバーの標準的な項目（アイコン）は以下の通りです:

- フィルターを表示: フィルターを指定すると、条件を満たすエントリーのみが表示されます。
- 列を選択: テーブルの列を選択して、表示/非表示を切り替えます。

- 追加: 新しいエントリーを追加します。たとえば、新しいゲートウェイや RD セッションホストを追加できます。
- 更新: 表示を更新します。
- 省略: 省略メニューは、ビューの種類によって項目が異なります。一部の項目には、対応するツールバー項目が表示されます（例: 追加、更新）。

またビューによっては、[実行中のプロセスを表示] や [セッションを表示] など、他の項目も表示されます。

ウィザード

ファームにコンポーネントを追加すると、通常はウィザードが開き、コンポーネントの設定やオプションを指定する一連のページが表示されます。ウィザードには、通常の [次へ] と [戻る] のナビゲーションボタンと、ウィザードを閉じて操作を取り消すことのできる [キャンセル] ボタンがあります。

モーダルダイアログ

メニューやナビゲーションバーの項目をクリックすると、モーダルダイアログが表示されます。通常、これらの項目では、処理の確認や追加情報の入力が必要となります。

オブジェクトのプロパティ表示

RAS 管理ポータルのすべてのオブジェクト（コンポーネント）には、プロパティがあります。これらのプロパティを表示するには、カテゴリーとサブカテゴリーを選択し、リスト内のオブジェクト名をクリックします。これにより、オブジェクトのプロパティが表示され、独自のナビゲーションバーを利用できるようなります。そこからオブジェクトの構成、処理の実行、追加情報の表示が可能になります。

第　4　章

サイトカテゴリー

サイトカテゴリーには、現在のサイトの概要が表示され、ライセンスの問題、更新が必要な RAS Agent などの重要なイベントに関する通知が表示されます。

サイトカテゴリーのメインビューは、以下に説明するセクションで構成されています。

RAS インフラストラクチャ

RAS Connection Broker や RAS Secure Gateway など、RAS のコアコンポーネントが表示されます。特定の種類のコンポーネントが複数ある場合、インストールされているコンポーネントの数が右側に表示されます。

コンポーネントをクリックして、管理ビューに移動できます。[インフラストラクチャ] カテゴリーから管理ビューを開くこともできます（詳細は本ガイドの後半で説明します）。

セッション

このセクションには、セッションとライセンスの使用状況が表示されます。セッションまたはライセンスの管理ビューに移動するには、対応するリンクをクリックします。

ホスト

[ホスト] セクションには、RD セッションホストや VDI（利用可能な場合）など、利用可能なセッションホストに関する情報が表示されます。利用可能なリンクをクリックすると、特定のホストタイプまたはプロバイダーの管理ビューに移動できます。ホスト情報には、ホスト上のアクティブなセッション数、ホストに関する問題の有無、ホストが現在無効になっているかどうかの情報が含まれます。

第　5　章

ファーム設定

ファームのグローバル設定を管理するには、サイドバーの下部にある [ファーム設定] をクリックします。

この章の内容

管理者

アカウント

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

1 [ファーム設定] > [管理者] > [アカウント] を選択します。
2 リスト内の任意の場所を右クリックし、[追加] を選択します。
3 新しいアカウントのプロパティを指定します。

なお、この記事の執筆時点では、管理ポータルに追加できるのはルート管理者のみです。

4 [システム通知] ドロップダウンリストで、[メール] を選択して、すべてのシステム通知を指定のメールアドレスに送信するか、[なし] を選択して、このアカウントでメールによるシステム通知を無効にします。
5 [作成] をクリックしてアカウントを作成します。

アカウントを変更するには、アカウント名をクリックしてから [編集] をクリックします。

アカウントを削除するには、右クリックして [削除] を選択します。

セッション

現在の管理用 RAS セッションを確認するには、[ファーム設定] > [管理者] > [セッション] を選択します。

セッションをログオフするには、セッションを右クリックし、[セッションからログオフ] を選択します。

メールボックス

RAS ファームのメールボックス構成は、Parallels RAS ファームへの参加を促すメールをユーザーに送信したり、イベント通知を他のメールアドレスに送信したりするために使用されます。1 つのファームにはメールボックスを 1 つのみ構成できます。

メールボックスを構成するには、次の操作を実行します。

1 [ファーム設定] > [メールボックス] に移動します。

2 [編集] をクリックして、以下を指定します。

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

3 [保存] をクリックします。

ライセンス

Parallels RAS のライセンス情報を表示するには、[ファーム設定] > [ライセンス] に移動します。次の情報が表示されます。

- ライセンスの種類: 現在使用している Parallels RAS ライセンスの種類（サブスクリプション、トライアルなど）。

- 有効期限: ライセンスの有効期限（またはライセンスの種類によっては残り日数）。
- 同時使用ユーザー数の上限です。現在のライセンスで許可される同時使用ユーザー数の上限。
- ピークユーザー数: サブスクリプションの場合は現在までのピーク時の同時使用ユーザー数、SPLA ライセンスの場合は月間のピークユーザー数と 1 日の使用状況。
- 現在のユーザー数: ファームに現在接続しているユーザーの数。

Parallels アカウントでもこれらの情報（およびその他）を確認できることに注意してください。詳細については、Parallels ウェブサイトで利用できる「Parallels RAS ライセンスガイド」を参照してください。

ライセンスの管理

「ライセンス」ページの上部にあるライセンスの管理リンクをクリックして、[ライセンスの管理] ページを表示します。

Parallels ビジネスアカウントをお持ちの場合、アカウントの認証情報を使用してサインインします。アカウントをお持ちでない場合は、[登録] をクリックして、必要な情報を入力し、[登録] をクリックします。現在の組織にビジネスアカウントが作成されます。Parallels アカウントと Parallels My Account ポータルの詳細については、Parallels ウェブサイトの『Parallels RAS ライセンスガイド』を参照してください。https://www.parallels.com/products/ras/resources/。

サインインすると、[ライセンスの管理] ページで以下の操作を実行できます。

- サブスクリプションに含まれるライセンスキーを使用してファームをアクティベートする。Parallels ビジネスアカウントを使用してサインインすると、ライセンス情報が取得され、画面に表示されます。ファームをアクティベートするには、リストからライセンスキーを選択し、[次へ] をクリックします。
- トライアル版をアクティベートする - [トライアルライセンスをアクティベートする] オプションを選択し、[次へ] をクリックします。
- 現在使用しているライセンスを無効にする - [ライセンスを無効にする] オプションを選択し、[次へ] をクリックします。ライセンスキーはリリースされ、別のファームをアクティブにするために使用できます。同じライセンスキーまたは別のライセンスキーを使用して、いつでもファームを再アクティベートできます。

上記のシナリオのいずれかで [次へ] をクリックすると、処理の進行状況を表示する [進行状況] ページが表示されます。完了すると、ページが更新され、操作の結果が表示されます。

ファームをアクティブにした場合は、ファームの管理を開始できます。ファームを非アクティブにした場合、管理ポータルのライセンス以外のコントロールはすべて無効になります。

第 6 章

サイト設定

サイトは、ファーム階層内における次のレベルのグループです。接続やリモートアプリケーションサービスを提供する、コアコンポーネント、セッションホスト、およびその他のオブジェクトが含まれます。

サイトのグローバル設定を管理するには、サイドバーで [サイト設定] カテゴリーをクリックします。

この章の内容

接続と認証

接続と認証の設定を管理するには、[サイト設定] > [接続] に移動します。

認証タイプの選択

ユーザーがサイトに接続すると、ログインする前に認証が行われます。認証タイプを構成するには、[接続] ペインで [認証] を選択し、次のいずれかを選択します。

- 資格情報: ユーザー資格情報は RAS が実行されている Windows システムによって認証されます。Windows の認証に使用される資格情報も、RDP セッションにログインするために使用されます。
- スマートカード: スマートカード認証。Windows 認証と同様に、スマートカードの資格情報は、RAS と RDP 間で共有されます。そのため、スマートカードの資格情報を入力する必要があるのは 1 回だけです。Windows 認証と異なり、ユーザーに必要な情報はスマートカードの PIN のみです。ユーザー名はスマートカードから自動的に取得されるため、ユーザーはこれを提供する必要がありません。

- ウェブ（SAML）：SAML SSO 認証。

スマートカードの認証情報が無効の場合、RAS Connection Broker は Local Security Authority Subsystem Service （LSASS）を組み込みません。スマートカード認証は、Parallels Client for Windows/Mac/Linux で使用できます。Parallels Client が RDP セッション内で実行されている場合、スマートカードは認証に使用できないことに注意してください。

スマートカードを使用するには、ユーザーのデバイスに有効な証明書をインストールしておく必要があります。そのためには、認証局のルート証明書をデバイスの鍵ストアにインポートしなければなりません。

以下の条件を満たした証明書を使用してください。

- ”キー使用法”フィールドにデジタル署名が入っていなければなりません。
- ”サブジェクト代替名”（SAN）フィールドにユーザーのプリンシパル名（UPN）が入っていなければなりません。
- ”拡張キー使用法”フィールドにスマートカードのログオンとクライアント認証が入っていなければなりません。

認証ドメイン

認証を実行するドメイン（または複数のドメイン）を指定するには、以下のいずれかを選択します。

- 特定: このオプションを選択し、特定のドメイン名を入力します。
- 信頼性のある全ドメイン: Parallels RAS に接続するユーザーについての情報がフォレスト内のさまざまなドメインに保存されている場合、複数のドメインに対して認証するには、[信頼性のある全ドメイン] オプションを選択します。
- [指定されたクライアントドメインを使用]。このオプションを選択すると、Parallels Client の接続プロパティで指定されたドメインを使用します。クライアント側でドメイン名が指定されていない場合、上記の設定に従って認証が行われます。
- クライアントに NetBIOS 資格情報の使用を強制する: このオプションを選択すると、Parallels Client はユーザー名を NetBIOS ユーザー名で置き換えます。

> **注:** スマートカードの資格情報の“Subject Alternative Name”（SAN）フィールドにユーザープリンシパル名（UPN）がない場合（あるいは、“Subject Alternative Name”フィールド自体がない場合）、[クライアントに NetBIOS 資格情報の使用を強制する] オプションを無効にする必要があります。

推奨: ドメイン名の変更や、その他の認証関連の変更を行った後は、セッション ID のキャッシュを削除する必要があります。現時点では、RAS Console で [設定] タブの [セッション ID のキャッシュを削除する] ボタンをクリックすることによってのみ、この作業を実行できます。

スタンドアロンマシンで指定されたユーザーに対してユーザーセッションを認証するには、ドメイン名の代わりに [ワークグループ名] / [マシン名] を入力する必要があります。ワークグループ WORKGROUP のメンバーである SERVER1 と呼ばれるマシン上のローカルユーザーのリストに対してユーザーを認証する場合、ドメインフィールドには次のように入力します。
WORKGROUP/SERVER1

ドメインのパスワードを変更する

ドメインパスワードの変更にカスタム URL を使用するように Parallels Client を構成できます。

ドメインパスワードの変更にカスタム URL を使用するように Parallels Client を構成するには、次の手順を実行します。

1 [”ドメインパスワードを変更”オプションにカスタムリンクを使用する] を選択します。

2 以下のテキストフィールドにリンクを追加します。

許可されたデバイス

[許可されたデバイス] ペインで、ファームに接続するためにクライアントが最新のセキュリティパッチを適用している必要があるかどうかを指定します。通常、このオプションは、脆弱性から環境を保護するために選択する必要があります。セキュリティパッチがインストールされていない古いバージョンの Parallels Client を使用する必要がある場合のみ、このオプションをオフにしてください。詳細については、次のナレッジベースの記事を参照してください: https://kb.parallels.com/en/125112。

多要素認証

多要素認証（MFA）を設定するには、[サイト設定] > [接続] > [多要素認証] に移動します。

多要素認証を使用する場合、ユーザーはアプリケーションリストを取得するために連続する 2 つの段階経由で認証を実行する必要があります。この場合、ネイティブ認証（Active Directory/LDAP）と以下の MFA のうちいずれかが使用されます:

- RADIUS（p. 27）
  - Azure MFA（RADIUS）
  - Duo（RADIUS）
  - FortiAuthenticator（RADIUS）
  - TekRADIUS
  - RADIUS
- TOTP
  - Google Authenticator（p. 29）
  - Microsoft Authenticator
  - TOTP（時間ベースのワンタイムパスワード）
- Deepnet
- SafeNet

なお、本ガイドの執筆時点で RAS 管理ポータルでは、RADIUS または TOTP MFA プロバイダーを追加/構成する操作のみを実行できます。他のプロバイダーを設定するには、デスクトップベースの Parallels RAS Console を使用する必要があります。

RADIUS の使用

RADIUS MFA プロバイダーを追加する

RADIUS MFA プロバイダーを追加するには、以下の操作を実行します。

1. [サイト設定] > [接続] > [多要素認証] に移動します。
2. プラス記号のアイコンをクリックし、追加したいプロバイダーを選択します。
3. 次の要素を指定します。
   - 名前: プロバイダーの名前です。
   - 説明: プロバイダーの説明です。
   - [テーマ] テーブルで、この MFA プロバイダーを使用するテーマを選択します。

4 [次へ] をクリックします。

5 次の要素を指定します。

- 表示名: クライアント側のログオン画面に表示される接続タイプの名前を指定します。ユーザーにとって理解しやすい名前を指定する必要があります。
- プライマリサーバーおよびセカンダリサーバー: この 2 つのフィールドでは、構成に含める RADIUS サーバーを 1 台または 2 台指定できます。2 台のサーバーを指定すると、RADIUS ホストの高可用性を構成することができます（下記参照）。ホスト名または IP アドレスを入力してサーバーを指定するか、[...] ボタンをクリックして Active Directory 経由でサーバーを選択します。

  RADIUS サーバーが 2 台指定されている場合は、[HA モード] ドロップダウンリストから次の高可用性モードのいずれかを選択します。[アクティブ - アクティブ（パラレル）] は、コマンドが両方のサーバーに同時に送信され、最初に応答した方が使用されます。[アクティブ - パッシブ（フェイルオーバー）] は、フェイルオーバー動作を意味し、タイムアウトが 2 倍になり、Parallels RAS は両方のホストからの応答を待ちます。
- HA モード: 上記のプライマリサーバーおよびセカンダリサーバーを参照してください。プライマリサーバーのみを指定した場合、このフィールドは無効になります。
- ポート: RADIUS サーバーのポート番号を入力します。デフォルト値を使用するには、[デフォルト] ボタンをクリックします。
- タイムアウト: パケットタイムアウトを秒単位で指定します。
- 再試行: 接続の確立を試みる場合の再試行回数を指定します。
- 秘密鍵: 秘密鍵を入力します。
- パスワードのエンコード: RADIUS サーバーで指定した設定に従って [PAP]（パスワード認証プロトコル）または [CHAP]（チャレンジハンドシェイク認証プロトコル）から選択します。

6 完了したら、[作成] をクリックします。

RADIUS MFA プロバイダーを構成する

RADIUS MFA プロバイダーを構成するには、以下の操作を実行します。

1 [サイト設定] > [接続] > [多要素認証] に移動します。

2 構成するプロバイダーの名前をダブルクリックします。

3 [編集] ボタンをクリックします。

4 設定可能なカテゴリーは以下の通りです。

- [概要] および [接続] カテゴリー: 上記を参照してください。
- 属性: https://download.parallels.com/ras/v19/docs/en_US/Parallels-RAS-19-Administrators-Guide/46769.htm を参照してください。

> **注:** 一度作成された属性は、RAS 管理ポータルで編集することはできません。属性を編集するには、デスクトップベースの Parallels RAS Console を使用します。

- 自動化: https://download.parallels.com/ras/v19/docs/en_US/Parallels-RAS-19-Administrators-Guide/46770.htm を参照してください。
- 制限: 「MFA ルールの構成」（p. 31）を参照してください。

5 完了したら、[保存] をクリックします。

Google Authenticator の使用

このセクションでは、Google Authenticator を構成する方法を説明します。

Google Authenticator を構成するには、以下の手順を実行します。

1 [サイト設定] > [接続] > [多要素認証] に移動します。

2 構成する Google Authenticator プロバイダーの名前をダブルクリックします。

3 [編集] ボタンをクリックします。

4 次の要素を指定します。

- 名前: プロバイダーの名前です。
- 説明: プロバイダーの説明です。
- [テーマ] テーブルで、この MFA プロバイダーを使用するテーマを選択します。
- 表示名: この場合のデフォルト名は「Google Authenticator」です。その名前は、Parallels Client の登録ダイアログの”Google Authenticator アプリを iOS または Android のデバイスにインストールしてください”という部分に表示されます。名前を変更すると、指定した名前が使用され、”<new-name> アプリを iOS または Android のデバイスにインストールしてください”と表示されます。技術面からすると、どの認証アプリでも使用できますが（つまり、名前を変更することも可能ですが）、この資料の執筆時点では Google Authenticator アプリだけが正式にサポートされています。

- 必要に応じて、デフォルトの TOTP 許容範囲を変更します。
- [登録] セクションでは、必要に応じて Google Authenticator のユーザー登録を制限できます。すべてのユーザーが制限なしで登録できるようにしたり（ [許可] オプション）、指定した日時までに限り登録できるようにしたり（[次の日時まで許可]）、登録を完全に無効にしたり（[許可しない] オプション）できます。有効期限が切れていたり、[許可しない] オプションが選択されていたりして、登録が無効になっている場合にユーザーがログインを試みると、登録が無効化されていることを示すエラーメッセージが表示され、システム管理者に問い合わせるよう促されます。登録を制限したり無効にしたりしても、Google 認証機能や他の TOTP プロバイダーを使用することができますが、それ以上のユーザーの登録を許可しないようなセキュリティが追加されています。これは、危殆化した認証情報を持つユーザーが MFA に登録する可能性を軽減するためのセキュリティ対策です。
- [ユーザー管理] セクションの [ユーザーをリセット] フィールドでは、ユーザーが Google 認証を使用して Parallels RAS に初めてログインしたときに受け取ったトークンをリセットできます。ユーザーをリセットすると、ユーザーは登録手続きを再び実行しなければならなくなります（詳細については、下記の「Parallels Client での Google 認証の使用」を参照）。特定のユーザーを検索することも、すべてのユーザーをリセットすることも、ユーザーのリストを CSV ファイルからインポートすることも可能です。
- 制限: 「MFA ルールの構成」（p. 31）を参照してください。

5 完了したら、[保存] をクリックします。

Parallels Client での Google 認証の使用

重要: Google Authenticator やその他の TOTP プロバイダーを使用するには、ユーザーのデバイスと RAS Connection Broker サーバーの間で時間を同期する必要があります。そうしないと、Google 認証は失敗します。

Google Authenticator は、サポートされているいずれのプラットフォームで実行している Parallels Client でも利用できます（モバイル、デスクトップ、Web Client でサポートされています）。

Google 認証を使用するには、ユーザーが認証アプリを自分の iOS デバイスまたは Android デバイスにインストールしなければなりません。Google Play または App Store にアクセスして、アプリをインストールしてください。認証アプリをインストールしたら、二要素認証を使用して Parallels RAS に接続する準備が整ったことになります。

Parallels RAS に接続するには、以下の手順を実行します。

1. Parallels Client またはユーザーポータルを開き、自分の資格情報を使用してログインします。
2. 多要素認証ダイアログが開き、バーコード（QR コード）と秘密鍵が表示されます。
3. モバイルデバイスで Google 認証アプリを開きます。
   - 初めて使用する場合は、[開始] をタップし、[バーコードをスキャンする] をタップします。
   - Google 認証の別のアカウントを持っている場合は、プラス記号のアイコンをタップし、[バーコードをスキャンする] を選択します。
4. Parallels Client のログインダイアログに表示されているバーコードをスキャンします。

   何かの理由でうまくスキャンできない場合は、アプリに戻り、[秘密鍵を入力する] を選択し、アカウント名と Parallels Client のログインダイアログに表示されている秘密鍵を入力します。
5. アプリで [アカウントを追加する] をタップすると、アカウントが作成され、ワンタイムパスワードが表示されます。
6. Parallels Client に戻り、[次へ] をクリックし、[OTP] フィールドにワンタイムパスワードを入力します。

その後のログインでは、資格情報 ([パスワードの保存] オプションが選択されている場合は不要）と、Google 認証アプリで取得したワンタイムパスワードを入力するだけで十分です（アプリによって新しいパスワードが生成されます）。RAS 管理者がユーザーをリセットすると（このセクションの最初にある [ユーザーをリセット] フィールドの説明を参照）、ユーザーが上記の登録手順を繰り返さなければならなくなります。

多要素認証（多要素認証）ルールの構成

多要素認証（MFA）は、すべてのユーザー接続に対して有効または無効にできますが、特定の接続に対してはより複雑なルールを構成できますこの機能を使用すると、同じユーザーやコンピューターに対して MFA を有効化/無効化し、ユーザーがどの場所のどのデバイスから接続しているかに応じてポリシーを適用することが可能になります。各 MFA プロバイダーには、ユーザー接続に対するマッチングに使用される 1 つまたは複数の条件で構成されるルールがあります。各条件は、マッチング可能な 1 つまたは複数の特定のオブジェクトで構成されています。

次のオブジェクトのマッチングを実行できます。

- ユーザー、ユーザーが所属するグループ、またはユーザーが接続するコンピューター。

- ユーザーが接続する Secure Gateway。
- クライアントデバイスの名前。
- クライアントデバイスのオペレーティングシステム。
- IP アドレス。
- ハードウェア ID。ハードウェア ID の形式は、クライアントのオペレーティングシステムに依存します。

ルールについて、次のことに注意してください。

- 条件は AND 演算子で連結されます。たとえばあるルールに、特定の IP アドレスに一致という条件とクライアントデバイスのオペレーティングシステムに一致という条件が含まれる場合、ユーザーの接続が IP アドレスの条件とクライアントオペレーティングシステムの条件の両方に一致する場合に、ルールが適用されます。
- オブジェクトは OR 演算子で接続されます。たとえば、クライアントデバイスのオペレーティングシステムに一致するという条件のみを作成した場合、いずれかのオペレーティングシステムがクライアント接続に一致すれば、ルールが適用されます。

ルールを構成するには、次の操作を実行します。

1 [サイト設定] > [接続] > [多要素認証] に移動します。

2 構成する Google Authenticator プロバイダーの名前をダブルクリックします。

3 制限リンクをクリックします。

4 [編集] ボタンをクリックします。

5 [デフォルトを継承] オプションをオフにします。

6 ルールの条件を指定します。以下のコントロールを利用できます。

   - Allow: 指定すると、ユーザー接続が条件に一致した場合に、MFA プロバイダーを有効化しなければならなくなります。Allow をクリックして、Deny に変更できます。
   - Disable: ユーザー接続が条件に一致した場合に、MFA プロバイダーを有効にしないというポリシーを指定します。Deny をクリックして、Allow に変更できます。
   - （+）: 新しい条件を追加します。一致条件として、Secure Gateway、クライアントデバイス名、クライアントデバイスのオペレーティングシステム、IP アドレス、ハードウェア ID のいずれかを使用したい場合は、（+）をクリックします。
   - is: ユーザー接続が条件に一致した場合に、MFA プロバイダーを有効化すること（または有効化しないこと。Allow と Deny による）を指定します。is をクリックして、is not に

変更できます。このコントロールは、少なくとも 1 件のオブジェクトが追加されたときに表示されます。

- is not: ユーザー接続が条件に一致しなかった場合に、MFA プロバイダーを有効化すること（または有効化しないこと。Allow と Deny による）を指定します。is not をクリックして、is に変更できます。このコントロールは、少なくとも 1 件のオブジェクトが追加されたときに表示されます。

また、条件の左側のスイッチをクリックすることで、条件を無効化および有効化できます。

7 完了したら、[保存] をクリックします。

FSLogix プロファイルコンテナー

注: 既存の FSLogix プロファイルコンテナー構成があり、その構成を Parallels RAS で管理したい場合は、「Parallels RAS で既存プロファイルの管理を構成する」（p. 35）の追加説明を参照してください。

Microsoft FSLogix プロファイルコンテナーは、ローミングプロファイルおよびユーザープロファイルディスク（UPD）の後継技術として利用されることの多いプロファイル管理ソリューションです。これは、パーシスタントでない環境でユーザーコンテキストを維持し、サインイン時間を最小限に抑え、互換性の問題を排除するネイティブプロファイルのユーザーエクスペリエンスを提供できるように構成されています。

Parallels はバージョン 18 以降、FSLogix プロファイルコンテナーを統合、構成、メンテナンス、およびサポートする機能を提供し、Storage Spaces Direct、Azure Files、Azure NetApp ファイル、SMB および Cloud Cache などでサポートされるプロトコルに基づいて、耐障害性と可用性をサポートします。

サポートされる FSLogix プロファイルコンテナーのリリース

Parallels RAS は、リリース 2105 までの FSLogix プロファイルコンテナーリリースでテストされています。

前提条件

FSLogix プロファイルコンテナーのライセンス資格は、以下のライセンスのいずれかを取得している場合に利用できます。

- Microsoft 365 E3、E5

- Microsoft 365 A3、A5、学生使用特典
- Microsoft 365 F1、F3
- Microsoft 365 Business
- Windows 10 Enterprise E3、E5
- Windows 10 Education A3、A5
- Windows 10 VDA（ユーザー単位）
- リモートデスクトップサービス（RDS）クライアントアクセスライセンス（CAL）
- リモートデスクトップサービス（RDS）サブスクライバーアクセスライセンス（SAL）

その他の前提条件は以下の通りです。

- FSLogix の推奨項目に応じて構成されたプロファイルコンテナーストレージ。
- Parallels RAS が FSLogix 設定を管理するホストでは、FSLogix に関連する GPO ポリシーを無効にしておく必要があります。

Parallels RAS に FSLogix プロファイルコンテナーアプリケーションをインストールする

Parallels RAS 管理ポータルに FSLogix プロファイルコンテナーアプリケーションをインストールするには、次の操作を実行します。

1 [サイト設定] > [FSLogix] に移動します。

2 右ペインで [編集] をクリックし、以下のインストール方法を選択します。

- 手動でインストールする: ホストにインストールされた FSLogix プロファイルコンテナーアプリケーションを手動で使用します（Parallels RAS では FSLogix エージェントはインストールされません）。
- オンラインでインストールする: Microsoft のウェブサイトから FSLogix プロファイルコンテナーをインストールします。ドロップダウンリストで、サポートされている任意のバージョンを選択します。カスタムの URL を指定するには、[カスタム URL] を選択して、所定のフィールドで URL を指定します。最新のサポート対象バージョンを自動的に検出する場合は、[最新情報を検出] をクリックします。最新バージョンが識別され、[オンラインでインストールする] ドロップダウンリストに追加されます。
- ネットワーク共有からインストールする: ローカルで利用可能な FSLogix エージェントをインストールします（Parallels RAS には Microsoft から提供される公式 ZIP アーカイブが必要です）。

- RAS Connection Broker からプッシュする: 最新バージョンの FSLogix エージェントがダウンロードされ、RAS Connection Broker 側に保存されて、ターゲットセッションホストにプッシュされます。

FSLogix プロファイルコンテナーを使用するためのセッションホストの構成

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

セッションホストを構成するには、次の操作を実行します。

1. [インフラストラクチャ] > [RD セッションホスト] に移動します。
2. リストからホストをクリックして、[プロパティ] をクリックします。
3. 中央のペインで [ユーザープロファイル] をクリックします。
4. [編集] をクリックして、編集を有効にします。サイトまたはホストプールのデフォルト値を上書きするには、[デフォルトを継承] を解除して、独自の設定を指定します。サイトまたはホストプールのデフォルトを変更するには、対応するリンクをクリックし、それぞれのビューで編集を行います。
5. ニーズに合わせて設定を指定します。

Parallels RAS で既存プロファイルの管理を構成する

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

ご利用いただく前に

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

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

準備

準備として以下の手順を実行します。

1. 既存のプロファイルをバックアップします。プロファイルデータが喪失または破損することはほとんどありませんが、プロファイル構成を変更する前に有効なバックアップを取得しておくことをお勧めします。
2. FSLogix プロファイルコンテナーの GPO 構成をオフにします。GPO からの FSLogix プロファイル管理と Parallels RAS からの管理を同時に有効にすることはできません。それで、この手順が重要になります。
3. RAS ファーム内のサーバーで FSLogix プロファイルを設定する前に、サーバーでユーザーセッションが実行されていないことを確認してください。業務時間外のメンテナンス期間に移行作業を行うことも考慮できるでしょう。

GPO と FSLogix の構成を複製する

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

RAS 管理ポータルでプロファイルを構成するには:

1. [インフラストラクチャ] > [RD セッションホスト] に移動します。
2. リストからホストをクリックして、[プロパティ] をクリックします。
3. 中央のペインで [ユーザープロファイル] をクリックします。
4. [プロファイルディスクの場所] リストボックスで、FSLogix プロファイルを保存する既存の SMB またはクラウドキャッシュの場所を指定します。さらに、プロファイルディスクのフォーマット、割り当てタイプ、既定サイズを指定します。
5. 中央のペインで、[ユーザーとグループ]、[フォルダー]、[詳細設定] 項目をクリックして、ユーザーの除外やフォルダーの除外など、サーバー上にある FSLogix の他の設定を行います。

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

RAS Console でプロファイルを設定するには:

1 ホスト、サイトのデフォルト値、またはテンプレートの [プロパティ] ダイアログで、[ユーザープロファイル] タブを開きます。

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

3 [詳細設定] ボタンをクリックして、ユーザーの除外やフォルダーの除外など、サーバー上にある FSLogix の他の設定を行います。

推奨事項とテスト

前のセクションの手順を実行する場合、RAS ファームに存在する複数の（またはすべての）サーバーをまとめて構成することは避けてください。1 台のサーバー（例: RD セッションホスト）から着手し、1 人のユーザーを接続した上でテストを行ってください。その後、他のサーバーを設定し、同一ユーザーが複数のサーバーに連続してログインするテストを行います。このテストで、いずれのセッションホストでもプロファイルが読み込まれ、カスタマイズされた機能が利用できることを確認します。特に問題がなければ、他のホスト、ホストプール、またはサイトのデフォルトを構成します。

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

サイトのデフォルト値と FSLogix のホストの構成

FSLogix を設定するには、

1 次のいずれかを実行します。

- サイトのデフォルトを設定するには、[インフラストラクチャ] > [ホストプール] > [RD セッションホスト] > [プロパティ] > [サイトのデフォルト値] > [ユーザープロファイル] に移動します。
- ホストプールを構成するには、[インフラストラクチャ] > [ホストプール] > <ホストプール名> > [プロパティ] > [サイトのデフォルト値] > [ユーザープロファイル] に移動します。
- 個別のホストを構成するには、[インフラストラクチャ] > [RD セッションホスト] > <ホスト名> > [プロパティ] > [ユーザープロファイル] に移動します。

2 プロファイルコンテナーを使用するには、[ユーザープロファイル] > [FSLogix プロファイルコンテナー] に移動します。

- ユーザーとグループ: ユーザーとグループの包含リストと除外リストを指定します。デフォルトでは、すべてのユーザーが FSLogix プロファイルの包含リストに追加されます。一部のユーザープロファイルをローカルのままにする場合は、該当のユーザーを除外リストに追加できます。ユーザーとグループは両方のリストに追加できますが、除外リストが優先されます。
- フォルダー: フォルダーの包含リストと除外リストを指定します。共通フォルダーから選択することも、手動でフォルダーを指定することもできます。フォルダーはユーザープロファイルのパスに配置する必要があります。ご注意ください。
- ディスク: プロファイルディスクの設定を指定します。 場所の種類: プロファイルディスクの場所の種類（SMB の場所、またはクラウドキャッシュ）を選択し、1 つまたは複数の場所を指定します。プロファイルディスクの場所: プロファイルディスクの場所（1 つまたは複数）です。これは、VHD（X）ファイルの場所（FSLogix ドキュメントに記載されている、レジストリ内の VHD の場所の設定）です。プロファイルディスクのフォーマット: 要件に応じて、VHD または VHDX を選択します。VHDX はより新しいフォーマットであり、より多くの機能を備えています。割り当てタイプ: [動的] または [フル] を選択します。この設定は、[デフォルトサイズ] の設定（以下を参照）と一緒に使用して、プロファイルのサイズを管理します。[動的] を選択すると、割り当てられたデフォルトサイズにかかわらず、プロファイルコンテナーは最低限のディスク領域を使用します。ユーザープロファイルにより多くのデータが入力されると、ディスクのデータ量はデフォルトサイズで指定したサイズにまで増加しますが、デフォルトサイズを上回ることはありません。デフォルトサイズ: 新たに作成された VHD（X）のサイズを MB 単位で指定します。
- アドバンスト: このタブでは、FSLogix の詳細なレジストリ設定を変更できます。デフォルトでは、設定は無効になっています。設定を有効にするには、設定名の前にあるチェックボックスをオンにします。各設定の説明は RAS Console に表示されます。FSLogix プロファイルコンテナーの構成について詳しくは、https://docs.microsoft.com/en-us/fslogix/profile-container-configuration-reference を参照してください。

3 プロファイルコンテナーを使用するには、[ユーザープロファイル] > [FSLogix - オフィスコンテナー] に移動します。

- ユーザーとグループ: 上と同様です。
- ディスク: 上と同様です。
- アドバンスト: 上と同様です。

4 クラウドキャッシュを構成するには、[ユーザープロファイル] > [FSLogix - クラウドキャッシュ] に移動します。これらの設定の詳細については、

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

5 ログを構成するには、[ユーザープロファイル] > [FSLogix - ログ] に移動します。これらの設定の詳細については、https://learn.microsoft.com/en-us/fslogix/reference-configuration-settings?tabs=ccd#fslogix-settings-profile-odfc-cloud-cache-logging を参照してください。

ユニバーサルプリント

プリンターリダイレクトでは、ユーザーは印刷ジョブをリモートアプリケーションまたはデスクトップからローカルプリンターにリダイレクトできます。ローカルプリンターは、ユーザーのコンピューターに接続することも IP アドレス経由で接続したローカルネットワークプリンターとして使用することもできます。RAS ユニバーサルプリントでは、クライアント側の特定のローカルプリンターのプリンタードライバーをリモートサーバーにインストールする必要をなくすることで、印刷プロセスを簡素化し、プリンタードライバーのほとんどの問題が解決します。そのため、ユーザーはローカルでどのプリンターをインストールしたかに関係なく印刷でき、RAS 管理者はローカルネットワークに接続されたそれぞれのプリンターにプリンタードライバーをインストールする必要がありません。

ユニバーサルプリントを構成するには、[サイト設定] > [ユニバーサルプリント] に移動します。

プリンターの設定: 名前の変更のパターン

デフォルトでは、Parallels RAS は次のパターンを使用してプリンター名を変更します。`%PRINTERNAME% for %USERNAME% by Parallels`。例えば、Alice という名前のユーザーに Printer1 という名前のローカルプリンターがあるとします。Alice がリモートアプリケーションまたはデスクトップを起動すると、プリンターは `Printer1 for Alice by Parallels` という名前になります。

[プリンター名の変更パターン] フィールドで新しいパターンを指定して、デフォルトのプリンター名変更パターンを変更できます。使用可能な定義済み変数を確認するには、[変数を追加] ボタンをクリックします。変数は次の通りです。

- `%CLIENTNAME%` – クライアントコンピューターの名前。
- `%PRINTERNAME%` - クライアント側のプリンターの名前。

- %SESSIONID% - RAS セッション ID。
- %USERNAME% - RAS に接続しているユーザーの名前。
- <2X Universal Printer> - これはレガシーモードで、RDP セッションでプリンターオブジェクトが 1 つだけ作成されます。

プリンター名変更パターンでは、他の文字列を使用することもできます。たとえば、次の一般的に使用されるパターンを定義できます。

Client/%CLIENTNAME%#/%PRINTERNAME%。

上記のパターン（および前述の例の Alice という名前のユーザー）を使用すると、ローカルプリンターの名前は Client/Alice's Computer#/Printer1 になります

[サイト内のサーバー] リストにある各サーバーに異なるプリンター名変更パターンを指定できます。

注: リダイレクトされたプリンターにアクセスできるのは、管理者とプリンターをリダイレクトしたユーザーのみです。

プリンターの設定: プリンターの保持

クライアント定義のプリンターがリモートセッションにリダイレクトされると、処理に時間がかかり、セッション確立の全体的な動作に影響が及びます。ユーザーエクスペリエンスを改善するために、以前に作成したユーザーのプリンターを使用できます。これを行うには、[プリンターの保持] オプションを [プリンターの保持の最適化を有効にする] に設定します。

ドライバー

システム管理者は、クライアント側のプリンタードライバーのリストを管理できます。プリンタードライバーに対して、ユニバーサルプリントのリダイレクト権限を許可または拒否することができます。

この機能を使用すると、次のことが可能になります。

- 不要なプリンターリダイレクトによるサーバーリソースのオーバーロードを回避します。ユーザーの大半はすべてのローカルプリンターをリダイレクトするため（デフォルトの設定）、多数のリダイレクトされたデバイスを実際には使用していないサーバー上に作成します。これは主に、PDFCreator、Microsoft XPS Writer、または各種の FAX デバイスのようなさまざまなペーパーレスのプリンターが関係します。

- 特定のプリンターが原因でサーバーが不安定になることを回避します。プリンターによってはサーバーが不安定になることがあるため（スプーラーサービスコンポーネント）、その結果、概してすべての接続ユーザーがプリントサービスを使用できなくなる場合があります。プリントサービスの継続して使用するために、管理者がそのようなドライバーの”拒否”リストを作成できることは重要です。

[ドライバー] セクションでプリンタードライバーを指定するには、次の操作を実行します。

1 [モード] ドロップダウンリストで、リダイレクトを許可するプリンターを次のオプションから選択します。
   - 任意のドライバーを使用するプリンターのリダイレクトを許可: （デフォルト）: このオプションは、リダイレクト権限を使用するためにプリンターが使用しているドライバーの種類を制限しません。
   - リストのいずれかのドライバーを使用するプリンターのリダイレクトを許可: このオプションを選択すると、「許可」されたドライバーがリストに追加されます。ドライバーを追加するには、プラス記号のアイコンをクリックし、ドライバー名を入力します。
   - リストのいずれかのドライバーを使用するプリンターのリダイレクトを拒否: これはおそらく、この機能のコンテキストでもっとも便利なオプションです。リストに指定されているドライバーを使用するプリンターのリダイレクト権限を拒否します。その他のすべてのプリンターについてリダイレクトの使用を許可します。
2 リストからプリンタードライバーを削除するには、マイナス記号のアイコンをクリックします。

次の点を確認してください。

- プリンタードライバーをリストに追加するときは、プリンター名ではなく、*ドライバー*名を入力してください。
- ドライバー名は、大文字と小文字を区別し、完全一致する必要があります（名前の一部や、ワイルドカードは使用できません）。
- このタブで指定した設定は、個々のサーバーだけでなくサイト全体に影響します。

フォント

フォントを埋め込む必要があります。ユニバーサルプリントを使用してドキュメントを印刷する場合、ドキュメントがクライアントマシンのローカルスプーラーにコピーされ印刷されます。クライアントマシンにフォントが存在しない場合、印刷が正しく出力されません。

フォントの埋め込みの除外: 特定のフォントタイプを埋め込みから除外するには、リストでそのフォントを選択します。1 つまたは複数のフォントを追加するには、プラス記号のアイコンをクリックします。

自動的にインストールされるフォント: サーバーとクライアントに特定のフォントタイプを自動的にインストールするには、[自動的にインストールされるフォント] セクションのプラス記号のアイコンをクリックします。

注: デフォルトでは、自動インストールリストに追加されているフォントは埋め込みリストから除外されます。そのようなフォントは Windows クライアントにインストールされているため、埋め込む必要はありません。

ユニバーサルスキャン

スキャナーのリダイレクトによって、リモートデスクトップに接続しているユーザーや公開済みのアプリケーションにアクセスしているユーザーは、クライアントマシンに接続されたスキャナーを使用してスキャンを行うことができます。この章では、RAS ユニバーサルスキャンサービスを構成し、使用する方法について説明します。

ユニバーサルスキャンを構成するには、[サイト設定] > [ユニバーサルスキャン] に移動します。

ユニバーサルスキャンでは、WIA および TWAIN リダイレクトが使用されます。これにより、このどちらかのテクノロジーを備えたハードウェアを使用する任意のアプリケーションをクライアントデバイスに接続し、スキャンを行うことができます。ユニバーサルスキャンでは、サーバーに特定のスキャナードライバーをインストールする必要がありません。

注: RD セッションホストで WIA と TWAIN の両方のスキャンを有効にするには、「デスクトップエクスペリエンス」というサーバー機能が必要です。

デフォルトでは、ホストサーバーが RAS ファームに追加され、Agent ソフトウェアがインストールされると、ユニバーサルスキャンドライバーが自動的にインストールされます。

スキャン名の変更パターンの構成

デフォルトでは、Parallels RAS は次のパターンを使用してスキャナー名を変更します。`%SCANNERNAME% for %USERNAME% by RAS`。たとえば、ローカルで SCANNER1 を設置しているユーザーである Lois が、リモートデスクトップまたは公開済みのアプリケーションに

接続した場合、このユーザーのスキャナー名は "SCANNER1 for Lois by RAS" に変更されます。

スキャナー名の変更パターンを変更するには、[スキャナー名の変更パターン] 入力フィールドに新しいパターンを指定します。名前の変更のために使用できる変数は次の通りです。

- %SCANNERNAME% - クライアント側のスキャナー名。
- %USERNAME% - サーバーに接続しているユーザーのユーザー名。
- %SESSIONID% - アクションセッションの ID。

リストのサーバーごとに異なる名前変更パターンを構成できます。

注: リダイレクトされたスキャナーにアクセスできるのは、管理者と、スキャナーをリダイレクトしたユーザーのみです。

スキャンアプリケーションの追加

ユニバーサルスキャン機能を使用する TWAIN アプリケーションは、TWAIN 構成に追加する必要があります。この方法では、TWAIN ドライバーを使用するため、管理者は簡単にセットアップを実行できます。

アプリケーションをスキャンアプリケーションのリストに追加するには、以下の操作を実行します。

1 [TWAIN] カテゴリーを選択します。

2 右側のペインでプラス記号のアイコンをクリックし、実行可能なアプリケーションの名前を入力します。

注: アプリケーションによっては、異なるまたは複数の実行ファイルが使用される場合があります。必要なすべての実行ファイルがスキャンアプリケーションのリストに追加されていることを確認してください。

リストからスキャンアプリケーションを削除するには、リストでアプリケーションを選択し、マイナス記号のアイコンをクリックします。

注: リストからアプリケーションを削除しても、アプリケーションのインストールは影響を受けません。

第 7 章

インフラ

この章の内容

RD セッションホスト

RD セッションホストは、RAS ファーム内に公開リソース（アプリケーション、デスクトップ、ドキュメントなど）をホストするために使用されます。

RD セッションホストを管理するには、[インフラストラクチャ] > [RD セッションホスト] に移動しますメインリストには、既存の RD セッションホストが表示されます。管理機能（追加、削除、プロセスやセッションの表示など）を実行するには、省略記号メニュー、コンテキストメニュー（右クリック）、および場合によっては処理アイコンを使用します。

RD セッションホストを追加

ユーザーに公開済みリソースを提供するには、RD セッションホストに Remote Desktop Service（RDS）役割をインストールする必要があります。

RD セッションホストをファームに追加するには、次の操作を実行します。

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

2 リスト内の任意の場所を右クリックして [追加] を選択します（省略記号メニューから [追加] を選択するか、プラス記号のアイコンをクリックすることもできます）。

3 表示されたリストからホスト（または複数のホスト）を選択するか、[AD を参照] ボタンをクリックし、ホストを参照します。

4 [次へ] をクリックします。

5 次のページで、以下のオプションを指定します。

- ファイアウォールルールを追加: ホスト上で実行されている Windows で Parallels RAS が必要とするファイアウォールルールを追加します。詳細については、「ポート参照」を参照してください。
- RDS 役割をインストール: インストールされていない場合は、RDS 役割をホストにインストールします。このオプションは常に選択する必要があります。
- デスクトップエクスペリエンスを有効にする: ホスト上で実行されている Windows でデスクトップエクスペリエンス機能を有効にします。このオプションは、[RDS 役割をインストール] オプション（上記）が選択されている場合のみ有効です。このオプションは、デスクトップエクスペリエンス機能がデフォルトで有効にされていない、Windows Server 2008 R1/R2 および Windows 2012 R1/R2 に適用されます。
- 必要な場合にサーバーを再起動: 必要な場合にホストを自動的に再起動します。必要に応じて、手動でホストを再起動することもできます。
- ホストプールへホストを追加: ホスト（1 台または複数）をホストプールに追加します。このオプションの下にあるリストボックスで任意のホストプールを選択するか、名前を入力して [作成] をクリックして新しいホストプールを作成します。ホストプールの作成方法については、「RDSH ホストプール」（p.59）を参照してください。

6 [次へ] をクリックします。

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

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

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

ウィザードを使用して Remote Desktop Users グループにユーザーを追加するには、[参照] をクリックして、ユーザーまたはグループを指定します。

8 次のページで、設定を確認し、[作成] をクリックします。

9 ホストに RAS RD セッションホスト Agent がインストールされていない場合、リモートインストールの認証情報を尋ねるダイアログが表示されます。ホストにエージェントソフトウェアをリモートでインストールするために使用するユーザー名とパスワードを入力します。[送信] をクリックし、画面上の指示に従います。

10 インストールが完了したら、[完了] をクリックします。エージェントをインストールできない場合、ホストをファームに追加することはできますが、使用はできませんのでご注意ください。エージェントは後からインストールすることができます。

インストールに成功すると、RD セッションホストリストにホストが表示されます。

追加情報

RD セッションホストサーバーからリソースを公開する方法については、「公開」（p. 104）を参照してください。

RD セッションホストの構成と管理方法については、以下を参照してください。

- RD セッションホストの構成（p. 46）
- RD セッションホストの管理（p. 54）

RD セッションホストの構成

RD セッションホストを構成するには、次の手順を実行します。

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

2 リスト内のホストをクリックすると、ホスト情報を表示するビューが開きます。

3 ナビゲーションバーで、[プロパティ]（下部）をクリックします。以下に説明するように、RD セッションホストを構成します。

サイトまたはホストプールのデフォルト値を使用する

RD セッションホストのプロパティはカテゴリーに分かれており、中央のペインに表示されます。各カテゴリーには、独自のプロパティセットがあります。[概要] と [スキャン] を除くすべ

てのカテゴリーには、共通のリンクがあります。サイトのデフォルト値またはホストプールのデフォルト値では、デフォルトの設定を表示できます。特定のカテゴリーのプロパティにデフォルト設定を継承させる場合は、[デフォルト設定を継承] オプションを選択します。その場合、デフォルト設定は以下のいずれかから継承されます。

- ホストが RD セッションホストのホストプールに割り当てられている場合、ホストプールのデフォルト値。プールについては、「RD セッションホストのグループ化と複製」で説明されています。
- ホストが RD セッションホストのホストプールに割り当てられていない場合、サイトのデフォルト値。ホストプールにはサイトのデフォルトも継承されますが、[ホストプールプロパティ] ダイアログで指定するホストプール向けのカスタム設定によって上書きされます。

ホストプールのデフォルト値またはサイトのデフォルト値リンク（どちらか該当する方）をクリックすると、ホストプールまたはサイトのデフォルトプロパティペインが表示されます。デフォルト設定を変更するには（必要な場合）、[編集] をクリックします。

概要

ナビゲーションバーで、[概要] を選択し、以下を指定します。

- サイト内のホストを有効化: ホストを有効または無効にします。無効化されたホストは、ユーザーに公開済みリソースを提供できません。ホストを無効にすると、メインリストでそのサーバー名がグレーアウトされます。
- ホスト: ホスト名を指定します。
- 説明: ホストの説明を指定します。
- ダイレクトアドレス変更: Parallels Client から RD セッションホストへの直接接続を確立するときに使用するダイレクトアドレスを変更する必要がある場合は、このオプションをオンにします。

Agent 設定

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

デフォルトの設定を使用するには、[デフォルト設定を継承] オプションを選択します。詳細については、「サイトまたはグループのデフォルト値を使用する」（p. 46）を参照してください。特定のホストにカスタム設定を指定する場合は、[デフォルト設定を継承] オプションをオフにして、次の各 Agent プロパティを指定します。

アプリケーションセッションの痕跡

このセクションの設定は、アプリケーションを実行していないセッションにのみ適用されます。

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

他の設定

- ポート: ホストでデフォルト以外のポートが構成されている場合、別のリモートデスクトップ接続ポート番号を指定します。
- セッション最大数: セッションの最大数を指定します。
- Client URL/メールのリダイレクションを許可: ユーザーがリモートアプリケーションで URL または HTML Mailto リンクを開くと、リンクはクライアントコンピューターにリダイレクトされ、リモートホストのアプリケーションではなく、ローカルのデフォルトアプリケーション（ウェブブラウザーまたはメールクライアント）で開かれます。このオプションではリダイレクトを有効化または無効化できます。次のオプションから選択できます。

  a 有効化 - このオプションを選択するとリダイレクトが有効化されます。その後 [Windows シェル URL の名前空間オブジェクトをサポート] オプション（ドロップダウンボックス以下）を選択します。これは、一般的なシナリオで動作するデフォルトのリダイレクト設定です。シェル URL 名前空間オブジェクトをサポートするということは、Parallels RAS がシェル名前空間 API を使用する公開済みアプリケーションでの操作を中断して、リンクを開くことができるということを意味します。これは多くのアプリケーションでの標準的な動作です。シェル URL 名前領域オブジェクトのサポートを無効する機能は、Parallels RAS の旧バージョンとの互換性のために備えられています。Parallels RAS の旧バージョン（RAS バージョン 16.2 以前）で動作させたい場合、このオプションを無効化できます。

  b 有効化（登録済みアプリケーションを置換） - このオプションでは、リンクのリダイレクトの代替メソッドを使用します。これにより、リモートホスト側でデフォルトの Web ブラウザーとメールクライアントを”ダミー”アプリと置換します。これを行うことで、リンクを開く操作を中断し、クライアントコンピューターにリダイレクトできます。

公開済みのアプリケーションで上述のデフォルトオプションが動作しない場合、このオプションを試してみることができます。

c 無効化 - このオプションにより、URL/メールのリダイレクトを無効化します。つまり URL または Mailto リンクは常にリモートホストで開くようになります。

- Windows シェル URL の名前空間オブジェクトをサポート:
- ドラッグ & ドロップ: ドラッグ & ドロップ機能が Parallels Client 内でどのように機能するかを設定できます。[無効]（ドラッグ & ドロップ機能をまったく使用しない）、[サーバーからクライアントのみ]（ローカルアプリケーションへのドラッグ & ドロップのみ許可し、逆方向は許可しない）、[クライアントからサーバーのみ]（リモートアプリケーションへのドラッグ & ドロップのみ許可）、[双方向](デフォルト)から選択できます。Parallels RAS 17.1 以降ではこのオプションが変更されたことに注意してください。それ以前はドラッグ & ドロップを有効化または無効化するチェックボックスであり、[クライアントからサーバーのみ] モードでのみ動作していました。Parallels RAS の以前のバージョンからアップグレードする際、このチェックボックスがオンになっていれば、デフォルトで [クライアントからサーバーのみ] が選択されます。オフになっていた場合は、[無効] オプションが設定されます。必要に応じて、どの新しいオプションに切り替えることも可能です。

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

- 任意の Connection Broker: RD セッションホストが接続する Connection Broker を選択します。これは、サイトコンポーネントが、WAN で通信する複数の物理的な場所に設置されているときに役立ちます。より適切な Connection Broker を指定することによりネットワークトラフィックを減らすことができます。
- 2XRemoteExec がクライアントにコマンドを送信することを許可: ホストで実行されているプロセスにより、クライアント側でのアプリケーションの展開をクライアントに指示することを許可するには、このオプションをオンにします。詳細については、以下の「RemoteExec の使用」サブセクションを参照してください。
- [RemoteApp を使用]（利用できる場合）: このオプションを有効にすると、シェル関連の問題でアプリが正しく表示されない場合に、リモートアプリを使用できます。この機能は、Windows 用 Parallels Client でのみサポートされています。
- [アプリケーションの監視を有効にする]。ホストでのアプリケーションの監視を有効または無効にします。アプリケーションのモニタリングを無効にすると、RAS Connection Broker に情報を転送しているときに、ホストでの CPU 使用率とネットワークの使用率を減らすための WMI モニタリングが停止します。このオプションが有効な場合、収集された情報が対応する RAS レポートに表示されます。このオプションが無効な場合、このホストからの情報はレポートに記載されません。

- RDP 転送プロトコルの管理。Parallels Client とホスト間の接続に使用されるトランスポートプロトコルを選択します。
- ファイル転送コマンドを許可（Web および Chrome クライアント）: リモートセッションでのファイル転送を有効化します。ドロップダウンリストで必要なオプションを選択します。詳細については、以下の「リモートファイル転送を構成する」を参照してください。
- ファイル転送のロケーション: デフォルトのアップロード先として使用するフォルダーの UNC パスです。ここで指定されたパスは、ユーザーがリモートホストからファイルをダウンロードしようとしたときの、デフォルトのソースロケーションとしても使用されます。ドロップダウンリストであらかじめ定義されているロケーションから選択するか、独自のロケーションを指定することができます。Windows の標準的な環境変数である、%USERNAME%、%USERDOMAIN%、%USERPROFILE% を使用することができます。アップロードまたはダウンロードの実行中にロケーションが見つからない場合は、標準（デフォルト）のダウンロードロケーションが使用されます。
- 位置情報の変更を許可しない: [ファイル転送のロケーション] フィールドで指定された UNC パスの変更を禁止します。このオプションを有効にすると、ファイルのアップロードまたはダウンロードを行う際に、ユーザーが別のロケーションを選択できなくなります。このオプションを無効にすると、ユーザーは別のロケーションを指定できるようになります。
- ドライブリダイレクトのキャッシュを有効化: リダイレクトされたドライブ上でのファイルの参照とナビゲーションをより高速にすることで、ユーザーエクスペリエンスを向上させます。

2XRemoteExec の使用

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

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

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

2XRemoteExec の例:

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

```
2XRemoteExec -?
```

このコマンドを実行すると、クライアントでメモ帳が起動します。

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

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

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

リモートファイル転送を構成する

Parallels RAS を使用して、エンドユーザーはリモートでファイルをリモートホストに転送またはリモートホストから転送することができます。

注: この文書の作成時点では、ファイル転送が利用できるのは、Parallels ユーザーポータルおよび Parallels Client for Chrome のみです。なお双方向のファイル転送は、Parallels ユーザーポータルのみでサポートされています。

リモートファイル転送機能を柔軟に設定できるように、Parallels RAS では以下の 3 つのレベルを設定することができます。

- RD セッションホスト、プロバイダー、またはリモート PC
- ユーザーポータル

- クライアントポリシー

各レベルで設定したファイル転送設定の優先順位は、上述の順序になります。たとえば、ファイル転送をユーザーポータルで有効にし、RD セッションホストで無効にしている場合、所定のユーザーポータルから所定の RD セッションホストに接続するすべてのユーザーについて、ファイル転送が無効になります。また、RD セッションホストでファイル転送を有効にし、特定のクライアントポリシー（またはユーザーポータル）で無効にすることもできます。このように、ファイル転送を利用できるクライアントと利用できないクライアントを制御することが可能になります。

リモートファイル転送を構成するには、次の操作を実行します。

1 [ファイル転送コマンドを許可] ドロップダウンリストで、次のオプションのいずれかを選択します。
   - 無効: リモートファイル転送は無効です。
   - Client からサーバー: クライアントからサーバーへのファイル転送のみ。
   - サーバーから Client: サーバーからクライアントへのファイル転送のみ。
   - 双方向: 双方向のファイルを転送が可能。
2 [ファイル転送のロケーション] フィールドには、デフォルトのアップロード先として使用するフォルダーの UNC パスを指定します。ここで指定されたパスは、ユーザーがリモートサーバーからファイルをダウンロードしようとしたときの、デフォルトのソースロケーションとしても使用されます。Windows の標準的な環境変数である、%USERNAME%、%USERDOMAIN%、%USERPROFILE% を使用することができます。アップロードまたはダウンロードの実行中にロケーションが見つからない場合は、標準（デフォルト）のダウンロードロケーションが使用されます。
3 [位置情報の変更を許可しない] オプションにより、[ファイル転送のロケーション] フィールドで指定された UNC パスをユーザーが変更することを禁止します。このオプションを有効にすると、ファイルのアップロードまたはダウンロードを行う際に、ユーザーが別のロケーションを選択できなくなります。このオプションを無効にすると、ユーザーは別のロケーションを指定できるようになります。

重要: なお、[位置情報の変更を許可しない] オプションでは、ユーザーが指定したリモートロケーションへの直接的なアクセスを禁止することはできません。たとえば、ユーザーがファイルをアップロードしようとするときに、デフォルトのロケーションの UNC パス（自分がアクセスできるパス）をメモし、ファイルエクスプローラーで該当のファイルを開き、プロファイルの任意のフォルダーにコピーすることができます。このような操作を防止するために、ここで指定したロケーション以外のロケーションも制御できるようにする追加の方法を導入する必要があります。

ユーザープロファイル

FSLogix テクノロジーに基づいてホストのユーザープロファイルを構成したい場合は、[テクノロジー] ドロップダウンリストで [FSLogix] を選択し、ニーズに合わせて設定を指定します。Parallels RAS で FSLogix プロファイルコンテナーを設定する方法については、「FSLogix プロファイルコンテナー」（p. 33）を参照してください。

デスクトップアクセス

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

デフォルトの設定を使用するには、[デフォルト設定を継承] オプションを選択します。上記の「デフォルト設定を使用する」サブセクションを参照してください。

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

1. [直接デスクトップアクセスを次のユーザーに制限する] オプションを選択します。[デフォルト設定を継承] オプションを選択している場合、[デフォルトを編集] リンクをクリックして、デフォルトの構成を表示し（必要な場合は変更し）ます。残りの手順は、[ホストプロパティ] ダイアログおよび [デフォルトホストのプロパティ] ダイアログの両方に適用されます。
2. プラス記号のアイコンをクリックします。
3. 希望するユーザーを選択します。複数のユーザーを含めるには、セミコロンで区切ります。
4. [OK] をクリックします。

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

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

印刷とスキャン

印刷

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

デフォルトの設定を使用するには、[デフォルト設定を継承] オプションを選択します。上記の「デフォルト設定を使用する」サブセクションを参照してください。

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

[プリンターからセッション番号を削除する] オプションを選択すると、プリンター名から対応する情報を除外できます。

スキャン

スキャンビューでは、ホストで有効にする画像インターフェイスを設定します。WIA、TWAIN、またはその両方を選択します。

RD セッションホストの管理

RD セッションホストの管理タスクを実行するには、次の操作を実行します。

1. [インフラストラクチャ] > [RD セッションホスト] に移動します。
2. ホストをクリックして、ホストのプロパティビューを開きます。
3. ナビゲーションバーを使用して、追加情報の表示やアクションの実行が可能な異なるビューに切り替えます。これらのビューについて、以下に説明します。

概要

[概要] 画面には、以下の情報が表示されます。

- [情報] セクションでは、メインの RD セッションホストリストに表示されるものと同様の RD セッションホスト情報が、単一のビューに分かりやすく表示されます。

- [処理] セクションには、ホスト上で実行できる処理が一覧表示されます（下記を参照）。なおホストを選択し、省略記号メニューからオプションを選択することによって、メインの RD セッションホストリストビューから処理を実行することもできます。

RD セッションホストでは、次の処理を実行できます。

- 全員にメッセージを送信: ホストに接続しているユーザーにメッセージを送信します。
- すべて切断: 現在のすべてのユーザーを切断します。
- すべてのセッションをログオフ: 現在のセッションをすべてログオフします。
- エージェントを更新: 必要に応じて RD セッションホストエージェントを更新します。
- エージェントを無効化: エージェントを一時的に無効にします。

[コントロール] サブメニューには、次の項目があります。

- ログオンを有効化: コンソールからではなく、クライアントセッションからのログオンを有効にします。このオプションは、`change logon /enable` コマンドと同じアクションを実行します。
- ログオンを無効化: コンソールからではなく、クライアントセッションからのそれ以降のログオンを無効にします。現在ログオンしているユーザーには影響しません。このオプションは、`change logon /disable` コマンドと同じアクションを実行します。
- ドレイン: 新しいクライアントセッションからのログオンを無効にします。ただし、既存のセッションへの再接続は許可します。ドレインは、再起動後も管理者がログオンを許可するまで保持されます。

  なお、ホストがドレインモードになっている場合でも、管理者は物理コンソールにログオンすることができます。また、MSTSC の /admin や /console コマンドラインオプションを使って、リモートでログオンすることもできます。これにより管理者は、[ツール] > [リモートデスクトップ] 経由で、RDS ホストをリモートでメンテナンスできます。
- 再起動までドレイン: コンピューターが再起動するまで、新しいクライアントセッションのログオンを無効にします。ただし、既存のセッションへの再接続は許可します。ドレインはホストが再起動されるまで保持されます。`change logon /drainuntilrestart` コマンドと同じアクションを実行します。
- 保留中の再起動をキャンセルする（スケジューラー）: 保留中の再起動をキャンセルします。
- 無効になっている状態をキャンセルする（スケジューラー）: 無効な状態を解除します。
- RDS 役割をインストール: ホストに RDS の役割をインストールできるようにします。

- 再起動: ホストを再起動します。
- シャットダウン: ホストをシャットダウンします。

[ログ] サブメニューには、次の項目があります。

- 構成: ログを構成することができます。ログレベルの説明については、以下を参照してください。
- 取得: ログファイルを含む ZIP アーカイブを指定したロケーションに取得します。
- クリア: 既存のログをすべてクリアします。

利用可能なログレベルは以下の通りです。

- 標準: もっとも重要なイベントのみを記録する標準のログレベルです。後述のいずれかのログレベルを使用するように Parallels RAS サポートから指定された場合以外は、常にこのレベルを使用してください。
- 拡張: このログレベルでは、標準ロギングよりも多くの情報が取得されます。ただし、収集する必要のある情報が増加するため、システムの速度が低下します。
- 詳細: 詳細ロギングでは拡張ロギングよりも多くの情報が取得されるため、システムの速度が大幅に低下する可能性があります。

パフォーマンスの低下を回避するには、拡張ロギングと詳細ロギングを（分析のために必要な情報を収集する上で十分な）限定的な期間のみ有効にする必要があります。この期間は [後で標準レベルにリセット] オプションを使用して設定できます。デフォルト値は 12 時間です。場合によっては、Parallels サポートエンジニアが、この期間に別の値を設定するようにアドバイスします。この期間が終了すると、ログレベルがリセットされて標準に戻ります。

残りの項目は以下の通りです。

- ホストプールに割り当て: ホストをホストプールに割り当てる
- ホストプールから削除: ホストプールからホストを削除します。
- 更新: 画面に表示されているホスト情報をリフレッシュします。
- サイトのデフォルト値: [RDSH サイトのデフォルト値] 画面を開き、サイトのデフォルト値を表示および構成することができます。
- 削除: RAS ファームからホストを削除します。

アクティブなセッション

RD セッションホストのアクティブなセッションを表示および管理するには、ナビゲーションバーで [アクティブなセッション] をクリックします。セッションの詳細情報を表示するには、リストでユーザー名をクリックします。これにより、 セッション情報ビューが表示されます。セッションメトリクスの詳細については、「セッション情報」（p. 96）を参照してください。

セッション（または複数のセッション）に対して処理を実行するには、リストでセッションを選択し、省略記号メニューをクリックします。次の項目のいずれかを選択します。

- セッション情報を表示: セッション情報ビューを開きます。
- メッセージ: セッション所有者にメッセージを送信します。
- 切断: セッションを切断します。
- ログオフ: セッションをログオフします。
- リソースを表示: 実行中のリソースを表示するビューを開きます。
- 実行中のプロセスを表示: 実行中のプロセスを表示するビューを開きます。
- 監視設定: RD セッションホストのセッションメトリクス値のハイライト表示を設定する、監視設定ダイアログを開きます。このダイアログには利用可能なメトリクスが一覧表示され、任意のメトリクスに警告とクリティカルのしきい値を設定することができます。しきい値を設定するには、メトリクス名の前にあるチェックボックスを選択し、必要な値を指定します。RAS ファームの動作中、しきい値に達すると、セッションメトリクス値が以下のようにハイライト表示されます。警告のしきい値: オレンジ、クリティカルのしきい値: 赤。

  指定したしきい値の値をリセットするには、しきい値を選択して、省略記号メニューから [リセット] を選択します（または右クリックして [リセット] を選択します）。また、メトリクスのしきい値の色分けを有効または無効にすることもできます。これを実行するには、メトリクスを選択し、省略記号メニューから [有効] または [無効] を選択します。
- 更新: リストを更新します。
- エクスポート: CSV ファイルに情報をエクスポートします。

実行中のリソース

RD セッションホストで実行中のリソースを表示するには、ナビゲーションバーで [実行中のリソース] 項目をクリックします。リソースの詳細情報を表示するには、リソース名をクリックします。リソースの基本情報（ID、名前、ターゲットなど）と対応するセッション情報を表示す

るビューが表示されます。セッションメトリクスの詳細については、「セッション情報」（p. 96）を参照してください。

リソースに対して処理を実行するには、リストでセッションを選択し、省略記号メニューをクリックします。次のいずれかを選択します。

- メッセージ: セッション所有者にメッセージを送信します。
- 切断: セッションを切断します。
- ログオフ: セッションをログオフします。
- 実行中のプロセスを表示: 実行中のプロセスを表示するビューを開きます。
- ユーザーセッション: セッションの情報を表示するビューを開きます。
- 情報の表示: リソース情報を表示するビューを開きます。
- 監視設定: 「アクティブなセッション」（p. 57）の説明を参照してください。
- 更新: リストを更新します。
- エクスポート: リストを CSV ファイルに保存します。

実行中のプロセス

RD セッションホストで実行中のリソースを表示するには、ナビゲーションバーで [実行中のプロセス] 項目をクリックします。これにより、実行中の全プロセスを表示するビューが表示されます。

1 つまたは複数のプロセスを強制終了するには、リストでそれらのプロセスを選択し、省略記号のメニューから [プロセスの強制終了] を選択します。リストを更新するには、[更新] をクリックします。

トラブルシューティング

トラブルシューティングの情報とタスクについては、ナビゲーションバーで [トラブルシューティング] を選択します。

トラブルシューティングビューに表示されるデータは、RAS Connection Broker を介さずに、RAS 管理ポータルにより、RD セッションホストから直接取得されます。エージェントが、RAS Connection Broker からアクセスできない場合や、現在別の RAS Connection Broker に登

録されている場合でも、RAS RD セッションホスト Agent の問題をトラブルシューティングするのに必要なデータを表示できます。

次のデータが表示されます:

- ホスト: RD セッションホスト名です。
- Agent: Agent のステータスです（例: OK）。
- バージョン: Agent のバージョンです。
- RDS 役割: RD セッションホストで RDS 役割が有効になっているかどうかを示します。
- OS の種類: ホストにインストールされているオペレーティングシステムの種類です。
- ステータス: エージェントの状態を長いバージョンで表示します。エージェントに問題がない場合は、そのように表示されます。問題がある場合、このフィールドで、エージェントに発生している問題が説明されます。この情報を使って、問題のトラブルシューティングを行うことができます。

また、トラブルシューティングビューでは、以下の処理を実行できます。

- ログを取得: ホストログを単一の ZIP アーカイブとして取得します。
- ログを構成: Parallels RAS コンポーネントのログレベルを指定できます。拡張レベルおよび詳細レベルはトラブルシューティングについてのみ使用可能です。これらのレベルを選択する場合、ログレベルが標準に戻るまでの期間も設定できます。
- ログをクリア: 既存のログをすべてクリアします。
- エージェントを再起動: RAS RD セッションホスト Agent を再起動します。
- エージェントをアンインストール: エージェントをアンインストールします。
- 更新: エージェント情報を更新します。

RDSH グループ

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

RD セッションホストのホストプールを使用する主な利点は次の通りです。

- 公開済みのリソースの管理が容易になります。マルチホスト環境での使用を強くお勧めします。
- VDI インフラストラクチャを活用して、テンプレートから作成される RD セッションホストを使用できます。これについてはこのセクションの後半で詳しく説明します。

1 つの RD セッションホストは 1 つのホストプールのメンバーにしかなれないことに注意してください。同じホストを複数のホストプールに追加することはできません。

ホストプールの作成

RDSH ホストプールを作成するには、次の操作を実行します。

1. [インフラストラクチャ] > [RD セッションホスト] > [ホストプール] に移動します。
2. 省略記号のメニューから [新規ホストプール] を選択します（またはプラス記号のアイコンをクリックします）。
3. ホストプール名を入力し、Enter キーを押します。
4. リストで新しいホストプール名をクリックし、ホストプール編集画面を開きます。
5. 中央のペインで [プロパティ] をクリックし、ホストプールの構成を行います。ここでの設定は、個別の RD セッションホストの設定と同様です。「RD セッションホストを構成する」（p. 46）を参照してください。

ホストプールのデフォルト値を使用する

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

- サイトのデフォルト値を構成し、ホストプールにこれらの設定を継承させます。ホストプールに割り当てられている RD セッションホストもサイトのデフォルト値を継承します。新しいホストプールでは、これがデフォルトのシナリオです。
- 対象のホストプールのデフォルト設定を構成します。この方法によって、それぞれが独自にホストプールのデフォルト値（サイトのデフォルト値とは異なる）を持つ、複数のホストプールを設定できます。ホストプールに割り当てられるホストは、ホストプールのデフォルト値を継承します。

Virtual Desktop インフラストラクチャ

Parallels RAS VDI（仮想デスクトップインフラストラクチャ）では、サーバーの仮想化を使用して、公開済みリソースをホストするために必要な物理サーバーの数を減らすことができます。Parallels RAS VDI は、ハイパーバイザーやクラウドベースのプラットフォームなど、数多くの仮想化テクノロジーをサポートしています。

Parallels RAS VDI には、テンプレート機能も搭載されています。これは、事前に構成されたゲスト VM（仮想マシン）からテンプレートを作成し、そこからホストを自動的に複製する機能を備えています。

なおこの記事の執筆時点で、Parallels RAS 管理ポータルの VDI 機能は、既存の仮想デスクトップの表示、ホストの再作成、およびそれらの電源操作の実行に限定されています。その他の VDI タスクの場合は、デスクトップベースの Parallels RAS Console をご利用ください。

Virtual Desktop リスト

ファームに存在する仮想デスクトップのリストを表示するには、[インフラストラクチャ] > [仮想デスクトップ] の順に選択します。

[仮想デスクトップ] テーブルに列を追加または削除するには、歯車のアイコンをクリックして、必要な列を選択またはクリアします。

電源操作を実行するには、仮想デスクトップを選択し、省略記号のメニューから次のいずれかを選択します。

- 開始
- 停止
- 再起動 - 再起動操作（猶予）には 10 分間のタイムアウトがあります。この時間内に操作が完了しない場合は、リセット操作（強制）となります。
- リセット
- 中断
- 更新
- 再作成 - 詳細は以下を参照してください。

ホストを再作成する

テンプレートベースのホストに何かが発生し、使用不能になった場合、削除して新しいホストを作成する必要はありません。代わりに、名前と MAC アドレスはそのままで再作成することができます（VM が DHCP サーバーから同じ IP アドレスを取得することを保証するため）。このようにすれば、サイト設定が破損したホストに依存していた場合でも、他のサイト設定は影響を受けません。ホストを再作成するもう 1 つの理由は、（再作成コマンドを実行せずにメンテナンスを終了するときに）テンプレートに加えられた変更を適用するためです。MAC アドレスの保持は、ESXi、vCenter、Hyper-v、Hyper-v Failover Cluster でのみサポートされていることに注意してください。

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

ホストを再作成する場合:

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

以下も参照してください。

プロバイダー（p. 94）

証明書

Parallels RAS 管理ポータルには、お使いのすべての SSL 証明書を 1 か所で管理できる、証明書管理インターフェイスが含まれています。

証明書はサイトレベルで管理されます。証明書がサイトに追加されると、その証明書は同じサイト上の RAS Secure Gateway や HALB で使用できるようになります。

証明書を管理するには、[インフラストラクチャ] > [証明書] に移動します。証明書リストには、既存の証明書が表示されます。Parallels RAS をインストールすると、<デフォルト> の自己署名証明書が自動的に作成されるので、証明書のリストには少なくともデフォルトの証明書が表

示されます。デフォルトの証明書も、自動的にすべての新しい RAS Secure Gateway や HALB に割り当てられます。

後続のセクションでは、証明書管理タスクについて詳しく説明し、証明書に関するその他の情報や指示を取り上げます。

自己署名証明書の生成

自己署名証明書を生成するには、[インフラストラクチャ] > [証明書] に移動します。省略記号のメニューから [追加] > [自己署名証明書の作成] を選択し、以下のオプションを指定します。

- 名前: 証明書の名前を入力します。このフィールドは入力必須です。
- 説明: オプションの説明。
- 使用方法: 証明書に RAS Secure Gateway と HALB のどちらを使用するか、あるいはその両方を使用するかを指定します。この選択は必須です。
- キーサイズ: 証明書のキーサイズのビット数。ここでは、定義済みの値から選択できます。デフォルト値は、現在の業界標準で必要最小の長さとされる 2048 ビットです。
- 有効期限: 証明書の有効期限。
- 国コード: 国を選択します。
- 都道府県: 都道府県名。
- 市: 市の名前。
- 組織: 組織の名前。
- 部門: 部門名。
- メールアドレス: ご利用のメールアドレスです。このフィールドは入力必須です。
- 氏名: コモンネーム（CN）、または完全修飾ドメイン名（FQDN）とも呼ばれるもの。このフィールドは入力必須です。
- サブジェクト代替名: 1 つまたは複数のサブジェクト代替名（SAN）を追加します。モバイルの Parallels Client はサブジェクト代替名フィールドをサポートしないため、ほとんどのモバイルデバイスで使用される一般的な名前を選択することをお勧めします。

[生成] をクリックして、証明書を作成します。完了すると、作成した証明書は [証明書] リストに表示され、[ステータス] 列には自己署名であることが示されます。

証明書のプロパティを表示および変更するには:

1 [インフラストラクチャ] 以下の証明書ビューで、証明書名をクリックします。

2 右側のペインで、[情報] セクションの証明書プロパティを確認します。

3 [処理] セクションで、証明書を有効または無効にすることができます。また、証明書をファイルにエクスポートすることもできます（p. 67）。証明書を削除するには、[削除] をクリックします。

4 証明書のプロパティの一部を変更する場合は、中央ペインの [プロパティ] をクリックします。

5 必要に応じて、左上の [編集] をクリックし、設定を変更します。証明書の名前と説明を変更したり、証明書の使用方法の設定（Gateway、HALB、またはその両方）を変更したりできます。

証明書署名要求の生成（CSR）

CSR を生成するには、以下の操作を実行します。

1 [インフラストラクチャ] > [証明書] を選択します。

2 省略記号のメニューから [追加] > [証明書リクエストの生成] を選択し、必要な情報を指定します。この情報は、「自己署名証明書を作成する」（p. 63）で説明したものとまったく同じです。

3 情報を入力したら、[作成] をクリックしてください。証明書情報ビューが表示されます。

4 中央ペインの [証明書リクエスト] をクリックすると、リクエストデータが表示されます。証明書リクエスト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。このビューで同時に、パブリックキーをインポートすることもできます。ここでビューを開いたまま、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。

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 証明書リクエストビューが閉じている場合、それを開きます（メインリストでリクエストをクリックし、[証明書リクエスト] をクリックします）。

2 リクエストをコピーして認証局のウェブページに貼り付けるか、電子メールで送信します（この場合は、後でこのビューに戻る必要があります）。

3 証明書認証局から証明書ファイルを取得します。

4 [パブリックキーのインポート] ボタンをクリックし、キーファイルと証明書ファイルを指定して、証明書の登録を完了します。

Let's Encrypt 証明書

Let's Encrypt 証明書を使用する

Let's Encrypt は、グローバルな認証局（CA）です。この組織は非営利団体であり、証明書の発行に費用は一切発生しません。各証明書の有効期限は 90 日間です。RAS Console では、Let's Encrypt の証明書の発行、自動更新、取り消しを行うことができます。

Let's Encrypt 証明書の発行

新しい Let's Encrypt 証明書を発行するには、次の手順を実行します。

1 [インフラストラクチャ] > [証明書] を選択します。

2 省略記号のメニュー（[...] アイコン）をクリックし、[Let's Encrypt 設定]を選択します。

3 [Let's Encrypt EULA を読んで同意しました] オプションを選択します。

4 Lets Encrypt から通知を受領するメールアドレスを、[期限切れのメール] フィールドのリストで指定します。

5 オプションとして、[期限切れの前に自動的に証明書を更新] フィールドで、証明書が自動的に更新される時間を変更できます。

6 [インフラストラクチャ] > [証明書] に戻ります。

7 [...] メニューから [追加] > [Let's Encrypt 証明書を発行] を選択し、以下のオプションを指定します。

- 名前: 証明書の名前です。
- 説明: 証明書の説明です。
- 使用方法: HALB または Secure Gateway を指定できます。
- キーサイズ: キーサイズです。
- 国コード: お住まいの国のコードです。
- 都道府県: お住まいの都道府県です。
- 市: お住まいの市区町村です。
- 組織: 所属している組織の名前です。

- 部門: 所属している組織の部署です。
- メールアドレス: 所属組織のメールアドレスです。
- 氏名: HALB または Secure Gateway の有効なドメイン名です。
- 代替名: HALB または Secure Gateway の有効なドメイン名です。

8 [証明書を発行する] をクリックします。

Lets Encrypt 証明書を手動で更新する

Lets Encrypt 証明書を手動で更新するには、次の手順を実行します。

1 [インフラストラクチャ] > [証明書] を選択します。

2 更新する証明書を選択します。

3 [...] メニューから、[コントロール] > [更新] を選択 します。

Let's Encrypt 証明書を取り消す

Let's Encrypt 証明書を取り消すには、次の手順を実行します。

1 [インフラストラクチャ] > [証明書] を選択します。

2 更新する証明書を選択します。

3 [...] メニューから、[コントロール] > [取り消し] を選択 します。

Parallels RAS が Let's Encrypt に証明書を要求する方法

Parallels RAS を使用して Let's Encrypt 証明書を新規に作成する場合、以下の処理が実行されます。

1 ライセンスロールをホストする Parallels RAS プライマリ Connection Broker が、Let's Encrypt サーバーにアカウントを作成するための最初のリクエストを行います。

2 アカウント作成の確認を受け取ります。Parallels RAS は CSR を作成し、Let's Encrypt サーバーに送信します。

3 チャレンジのリストを受信して、Connection Broker で Let's Encrypt サーバーから送信された HTTP トークンの読み取りが行われます。

4 Secure Gateway または HALB は、Connection Broker からトークンを取得します。

5 準備が整うと、Connection Broker から Let's Encrypt Server に通知が行われます。

6 Let's Encrypt から、Secure Gateway または HALB へのアクセスが行われ、トークンの有無の確認により検証プロセスが開始されます。

7 Secure Gateway または HALB が指定されたドメインに返信できることが確認され、チャレンジが完了します。

8 チャレンジが正常に完了したとの仮定に基づき、Parallels RAS は証明書を要求します。

9 有効な証明書が Let's Encrypt サーバーから Connection Broker にダウンロードされます。

10 Connection Broker から、Secure Gateways または HALB に証明書が配信されます。

証明書をファイルからインポートする

ファイルから証明書をインポートするには、省略記号のメニューから [追加] > [証明書のインポート] を選択し、次のように指定します。

- 名前: 証明書の名前を入力します。
- 説明: オプションの説明。
- 使用方法: 証明書に RAS Secure Gateway と HALB のどちらを使用するか、あるいはその両方を使用するかを指定します。
- 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、[参照] 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。

完了したら [OK] をクリックします。証明書はリストに表示され、[ステータス] 列には [インポート済み] であることが示されます。

証明書をファイルにエクスポートする

証明書をファイルに書き出すには、リストで証明書を選択し、省略記号のメニューから [証明書のエクスポート] を選択します。

その後、[証明書のインポート] を使用して、[プライベートキーファイル] フィールドで証明書ファイルを指定すれば、エクスポートした証明書を別のファームやサイトにインポートできます。

証明書の Gateway や HALB への割り当て

証明書を追加した後、作成時に指定した使用方法のタイプに応じて、証明書を RAS Secure Gateway と HALB のどちらか、あるいはその両方に割り当てることができます。証明書の [使用方法] オプションについては、以下に詳しく説明します。

証明書の使用方法

証明書の [使用方法] は、証明書を RAS Secure Gateway と HALB のいずれか、またはその両方で利用できるようにするかを指定するオプションです。「自己署名証明書を作成する」(p. 63) を参照してください。後で RAS Secure Gateway や HALB の SSL を構成する場合は、SSL 証明書を指定する必要があります。証明書を選択する際は、[使用方法] オプションが特定の証明書にどのように構成されているかに応じて、次のオプションを利用できます。

- 一致する使用方法すべて: これはデフォルトオプションで、いつでも利用できます。このオプションは、[使用方法] の選択内容がオブジェクトのタイプ（ゲートウェイや HALB）に一致する証明書が使用されるというものです。たとえば、ゲートウェイを構成していて、[使用方法] が「ゲートウェイ」に設定されている証明書がある場合、その証明書が使用されます。証明書の使用方法オプションでゲートウェイと HALB が両方とも選択されている場合も、その証明書は該当のゲートウェイで使用できます。これは、LB SSL ペイロードを構成する際の HALB でも同様です。なお、このオプションがゲートウェイや HALB で選択されているものの、一致する証明書が存在しない場合は、警告メッセージが表示されます。この場合、まず証明書を作成する必要があります。
- [証明書] ドロップダウンリストのその他の項目は個別の証明書ごとに扱われ、証明書の [使用方法] の設定に応じて、リストに表示されたり表示されなかったりします。たとえば、HALB の LB SSL ペイロードを構成していて、[使用方法] オプションが「HALB」に設定されている証明書がある場合、その証明書はドロップダウンリストに表示されます。一方、[使用方法] が「ゲートウェイ」に設定されている証明書はリストに含まれません。

また、1 つの証明書だけですべてのゲートウェイを使用したい場合は、証明書を作成し、その [使用方法] オプションを「ゲートウェイ」に設定する必要があります。その後、各ゲートウェイにこの証明書を使用するように構成するか、[一致する使用方法すべて] の選択内容をデフォルト値のままにすれば、証明書はゲートウェイによって自動的に取得されます。これは HALB についても同様です。

ゲートウェイ

証明書を RAS Secure Gateway に割り当てるには、次の操作を実行します。

1 [インフラストラクチャ] > [Gateway] を選択します。

2 リストで Gateway をクリックします。

3 中央ペインで、[プロパティ] をクリックします。

4 SSL/TLS カテゴリーを選択します。

5 [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。

[一致する使用方法すべて] オプションを選択することもできます。そうすると、使用方法が Gateway あるいは Gateway と HALB の両方に設定されている証明書が使用されることになります。

HALB

この記事の執筆時点では、HALB を RAS 管理ポータルで管理することはできません。デスクトップベースの RAS Console ご利用ください。

ゲートウェイ

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

単一テナントの環境では、Parallels RAS が機能するには、少なくとも 1 つの RAS Secure Gateway をインストールする必要があります。RAS サイトに Gateways を追加することで、さらに多数のユーザーやロードバランス接続に対応し、冗長性を実現することができます。

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

1 RAS Secure Gateway は、ユーザーの接続要求を受信します。

2 その後、要求を登録先の RAS Connection Broker に転送します（デフォルトでの推奨 Connection Broker 設定）。

3 RAS Connection Broker は、ロードバランスチェックと Active Directory セキュリティ検索を実行し、セキュリティ権限を取得します。

4 公開済みのリソースをリクエストしたユーザーが十分な権限を持っている場合、RAS Connection Broker はゲートウェイに応答を返します。応答には、ユーザーがどの RD セッションホストに接続できるかについての詳細が含まれます。

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

RAS Secure Gateway の動作モード

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

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

注: 転送モードを構成するには、RAS サイトに複数の RAS Secure Gateway が必要です。

高可用性のためのプラン

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

Secure Gateway を追加

RAS Secure Gateway を追加するには、次の操作を実行します。

1 [インフラストラクチャ] > [Secure Gateway] を選択します。

2 右側ペインで、省略記号のメニューから [追加] を選択します。[Gateway] - [新規追加] ウィザードが開きます。

3 サーバーの FQDN または IP アドレスを入力するか、[AD を参照] ボタンをクリックして、リストからサーバーを選択します。IP アドレスと FQDN を双方向に解決するには、[IP を解決する] または [名前を解決する] をクリックします。

4 [次へ] をクリックします。

5 [モード] ドロップダウンメニュー（通常または転送）からゲートウェイモードを選択します。

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

7 Gateway の説明（オプション）を追加します。

8 RAS ユーザーポータルのサポート（Parallels RAS に接続し、公開済みリソースを起動するために使用できるブラウザーベースのクライアント）を有効にするには、[ユーザーポータルを有効化] オプションを選択します。

9 ゲートウェイをホストしているサーバー上のファイアウォールを自動的に構成するには、[ファイアウォールルールの有効化] を選択します。

10 [次へ] をクリックします。

11 設定を確認し、[作成] をクリックして Gateway をサイトに追加します。

追加情報

RAS Secure Gateway の構成と管理方法については、以下を参照してください。

- Gateway を構成する（p. 71）
- Gateway を管理する（p. 87）

Gateway を構成する

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

1 [インフラストラクチャ] > [Secure Gateway] を選択します。

2 リスト内の Gateway をクリックすると、Gateway 情報を表示するビューが開きます。

3 中央のペインで [プロパティ] をクリックします。

以降のセクションで説明するように、 Gateway のプロパティを設定します。

概要

[サイト内の RAS Secure Gateway を有効化] を選択またはクリアします。

- ホスト: 必要に応じて、別のホストを選択します。

- 説明: オプションの説明を設定または変更します。
- パブリックアドレス: Gateway サーバーのパブリックアドレスを指定します。

クライアント接続用の IP アドレスの設定

次の IP オプションを指定します。

- 次の IP バージョンを使用: 使用する IP バージョンを選択します。RAS Secure Gateway は IPv4 と IPv6 の両方を認識します。デフォルトでは、IPv4 が使用されます。
- IP: 1 つ以上の IP アドレスをセミコロンで区切って指定するか、[解決] をクリックして IP アドレスを自動解決します。それらのアドレスを Gateway サーバーで使用できます。クライアント接続で使用する IP アドレスを指定する場合は、[IP にバインド] セクションを使用します（下記参照）。
- IP にバインド: クライアント接続で Gateway が待機する IP アドレス（複数の場合もあり）を指定するには、このセクションを使用します。特定のアドレスを指定できます。または、利用できるすべてのアドレスを指定して、[IP] フィールドに指定されたすべての IP を使用することもできます。
- 次の…システムバッファを削除: このオプションを使用すると、この Gateway と Parallels Client 間の接続で高遅延が発生した場合（インターネットなど）に、トラフィックが最適化されます。このオプションによりトラフィックが最適化され、Parallels Client 側の操作性が向上します。1 つまたは複数の特定のアドレスを選択できますし、利用できるすべてのアドレスを選択することもできます。また、選択しないこともできます。このオプションは、外部ソケットのパフォーマンスにマッチさせるために内部ソケットを遅延させます。内部ネットワークが速く、外部ネットワークが遅い場合、RDP が速い内部ソケットを検出し、大量のデータを送信します。問題は、データを Gateway からクライアントに十分な速度で送信できず、ユーザーエクスペリエンスが悪化することです。このオプションを有効にすると、データのやり取りが最適化されます。

モード

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

- 通常モード: RAS Secure Gateway は、ユーザー接続リクエストを受け取った後、RAS Connection Broker に対し、要求したユーザーにアクセス権があるかどうかを確認します。このモードで動作するゲートウェイを使用することで、より多くのリクエストをサポートすることができ、冗長性を向上させることができます。

- 転送モード: RAS Secure Gateway は、ユーザー接続リクエストを、事前に構成された Gateway に転送します。ファイアウォールカスケードを使用する場合は、WAN 接続を LAN 接続から切り離すのに転送モードのゲートウェイが役立ちます。また、転送モードのゲートウェイを使用すると、問題発生時に LAN を中断することなく WAN セグメントを切断できます。

注: 転送モードを構成するには、RAS サイトに複数の RAS Secure Gateway が必要です。

サイトのデフォルト設定を使用するには、[デフォルト設定を継承] オプションをクリックします。固有の設定を指定するには、オプションをクリアします。

通常モードの設定

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

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

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

転送モードの設定

転送モードを設定するには、[Gateway モード] ドロップダウンリストで [転送] を選択して、1 つまたは複数の Gateway を指定します。転送モードのゲートウェイは、すべてのユーザー接続リクエストを、事前に構成されたゲートウェイに転送します。ファイアウォールカスケードを使用する場合は、WAN 接続を LAN 接続から切り離すのに転送モードの Gateway が役立ちます。また、転送モードの Gateway を使用すると、問題発生時に LAN を中断することなく WAN セグメントを切断できます。

ネットワーク

[ネットワーク] カテゴリーは、RAS Secure Gateway のネットワークオプションの構成に使用します。

サイトのデフォルト設定を使用するには、[デフォルト設定を継承] オプションをクリックします。独自の設定を指定するには、このオプションをオフにして、次の項目を設定します。

- RAS Secure Gateway ポート: デフォルトでは、RAS Secure Gateway は TCP ポート 80 上で待機し、すべての Parallels RAS トラフィックをトンネリングします。このポートを変更するには、新しいポートを指定します。
- RDP ポート: 負荷分散された基本的なデスクトップセッションを必要とするクライアントでは、RDP ポート 3389 が使用されます。このポート上の接続では、公開済みのリソースはサポートされません。ゲートウェイの RDP ポートを変更するには、[RDP ポート] オプションを選択して、新しいポートを指定します。自分でポートを設定する場合、そのポートが標準の [RD セッションホストポート] 設定と重複していないことを確認してください

  注: RDP ポートを変更した場合、ユーザーはリモートデスクトップクライアント内の接続文字列にポート番号を追加する必要があります（例: IP アドレス:ポート）。
- Secure ゲートウェイのアドレスを伝播する: このオプションを使用して、ゲートウェイアドレスのブロードキャストを有効にすることができます。これにより、Parallels Client でプライマリゲートウェイを自動的に見つけることができます。このオプションは、デフォルトで有効になっています。
- RDP UDP データトンネリングを有効にする: Windows デバイスで UDP トンネリングを有効にするには、このオプションを選択します（デフォルト）。UDP トンネルを無効にするには、このオプションをオフにします。
- デバイスマネージャーポート: このオプションは、Windows デバイスの管理機能を有効にする場合に選択します。このオプションは、デフォルトで有効になっています。
- RDP DOS アタックフィルターを有効にする: このオプションを選択すると、同一 IP アドレスからの一連の未完了セッションが拒否されます。たとえば、Parallels Client が各セッションで複数の連続したセッションを開始し、ユーザーからの資格情報の提供を待っている場合、Parallels RAS はこれ以上の試行を拒否します。このオプションは、デフォルトで有効になっています。

SSL/TLS

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

サイトのデフォルト設定を使用するには、[デフォルト設定を継承] オプションをクリックします。固有の設定を指定するには、オプションをクリアします。

HSTS

[HSTS] セクションを利用すると、HTTP Strict Transport Security（HSTS）を適用できます。これは、安全な HTTPS 接続のみを使用して、ウェブブラウザーにウェブサーバーと通信させるメカニズムです。HSTS が RAS Secure Gateway に適用されると、すべてのウェブリクエストが HTTPS を使用するように強制されます。これは、通常 HTTPS リクエストのみを受け入れることができるユーザーポータルに特に影響します。

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

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

次の要件にも注意してください。

- ウェブサイトに有効な SSL 証明書が存在している必要があります。

- すべてのサブドメイン（サブドメインがある場合）が SSL 証明書でカバーされている必要があります。ワイルドカード証明書を要求することを検討してください。

暗号化

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

SSL 証明書はサイトレベルで作成されます。作成された証明書は、RAS Secure Gateway に割り当てることができます。証明書の作成と管理については、「証明書」（p. 62）を参照してください。

暗号化を構成するには、次の操作を実行します。

1. [ポートで SSL 有効化] オプションを選択し、ポート番号を指定します（デフォルトは 443）。
2. [許可される SSL バージョン] ドロップダウンリストで、SSL バージョンを選択します。
3. [暗号強度] フィールドで、希望する暗号強度を選択します。
4. [暗号] フィールドに暗号を指定します。強い暗号を使用すれば、暗号化の強度が増し、破るのに必要な労力も増大します。
5. [サーバー環境に応じて暗号を使用] オプションは、デフォルトで有効になっています。このオプションを無効にすることで、クライアントの環境設定を使用することができます。
6. [証明書] ドロップダウンリストで任意の証明書を選択します。[一致する使用方法すべて] オプションでは、構成されたすべての証明書がゲートウェイによって使用されます。証明書を作成する場合、”ゲートウェイ”、”HALB”またはその両方を選択できる場所で”使用”プロパティを指定します。このプロパティで [ゲートウェイ] オプションが選択されていれば、ゲートウェイに使用できます。このオプションを選択していても、一致する証明書が存在しない場合には、警告が表示され、先に証明書を作成することになります。

追加情報

「Client およびサーバーの構成」（p. 77）

Client およびサーバーの構成

Parallels Client の接続の暗号化

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

Parallels Client の構成を簡素化するために、サードパーティー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 からルートまたは中間エンタープライズ 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には、手動で設定する必要があります。既知の信頼できる認証局によって発行された第三者証明書が使用される場合、クライアントデバイスは、そのプラットフォームに対し、信頼できる認証局の更新を信頼して使用します。

Parallels Client の構成

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

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

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

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

RDP-UDP 接続の保護

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

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

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

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

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

SSL サーバー構成

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

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

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

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

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

ユーザーポータル

Parallels ユーザーポータルは、RAS Secure Gateway に組み込まれています。これにより、ユーザーはウェブブラウザーから Parallels RAS に接続し、公開済みリソースを開くことができます。

注: ユーザーポータルを使用するには、RAS Secure Gateway で SSL を有効にする必要があります。クライアントを有効にする場合は、[SSL/TLS] カテゴリーまたはネットワークロードバランサーで SSL が有効になっていることを確認してください。[ユーザーポータル] カテゴリーは、Gateway モードが通常に設定されている場合にのみ使用できます。

ユーザーポータルの URL の構成方法と、ウェブブラウザーからクライアントにアクセスする方法については、「ウェブ」セクション（p. 83）を参照してください。

- [ユーザーポータル] タブでサイトのデフォルト設定を使用するには、[デフォルト設定を継承] オプションをクリックします。固有の設定を指定するには、オプションをクリアします。
- RAS ユーザーポータルを有効化/無効化するには、[ユーザーポータルを有効化] オプションを選択/クリアします。

Client

[Client] セクションでは、ユーザーポータルの起動方法やその他の設定を指定できます。

- 以下を使用してセッションを起動: 公開済みリソースを開くために使用する Parallels Client を指定します。ユーザーポータルまたはプラットフォーム固有の Parallels Client を使用できます。ユーザーポータルに比べ、プラットフォーム専用の Parallels Client は機能がさらに豊富で、全体的なユーザーエクスペリエンスにも優れています。次のいずれかを選択します。
  - **a** ブラウザーのみ: ユーザーは Web Client のみを使用してリモートアプリケーションとデスクトップを実行できます。ユーザーにプラットフォーム固有の Parallels Client をインストールさせたくない場合は、このオプションを使用します。
  - **b** Parallels Client のみ: ユーザーは Parallels Client のみを使用してリモートアプリケーションとデスクトップを実行できます。ユーザーが Parallels Web Client を使用して Parallels RAS に接続すると、リモートアプリケーションとデスクトップを起動する前

に、プラットフォーム固有の Parallels Client をインストールするように求められます。ユーザーには、Parallels Client のダウンロードリンクが含まれるメッセージが表示されます。ユーザーが Parallels Client をインストールした後も、Web Client でリモートアプリケーションまたはデスクトップを起動できますが、リソースは Parallels Client で開かれます。

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

- ユーザーが起動方法を選択することを許可: このオプションを選択すると、ブラウザーまたは Parallels Client でリモートアプリケーションを開くかどうかを選択できます。このオプションは、[以下を使用してセッションを起動:] オプション（上記）が [Parallels Client とブラウザーへのフォールバック] に設定されている場合（つまり両方の方法が許可されている場合）にのみ、有効にできます。
- 新規タブでアプリケーションを開く: 選択されている場合、ユーザーは、ウェブブラウザーの新しいタブでリモートアプリケーションを開くことができます。

ネットワークロードバランサーへのアクセス

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

次のオプションを利用できます。

- 代替ホスト名を使用する: このオプションを選択し、代替ホスト名を指定します。代替ホスト名を有効化すると、プラットフォーム別の Parallels Client では RAS ファームまたはサイトへの接続にそのホスト名が使用されます。
- 代替ポートを使用する: このオプションを選択し、代替ポート番号を指定します。ポート番号は、RAS ファームまたはサイトの他のコンポーネントで使用されていないことが必要です。ポート番号をデフォルトに戻すには、[デフォルト] をクリックします。代替ポートを有効化すると、プラットフォーム別の Parallels Client では RAS ファームまたはサイトへの

接続にそのポートが使用されます。Web Client の RDP セッションでは引き続き標準 SSL ポート（443）で接続されることに注意してください。

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

さらに、Parallels Web Client で必要な HTTP/HTTPS トラフィックを処理する AWS アプリケーションロードバランサー（ALB）では、通常自動的に生成される特定の Cookie のみがサポートされています。ロードバランサーは、クライアントからのリクエストを最初に受信すると、リクエストをターゲットにルーティングし、`AWSALB` という Cookie を生成します。これは、選択されたターゲットの情報をエンコードしたものです。ロードバランサーはこの Cookie を暗号化してクライアントへの応答に含めます。スティッキーセッションが有効になっている場合、ロードバランサーは同じターゲットが正しく登録され、正常な状態にあると想定し、クライアントから受信した Cookie を使用してトラフィックをそのターゲットにルーティングします。デフォルトでは、Parallels RAS は `_SessionId` という名前の専用 ASP.NET Cookie を使用します。ただし、上記のスティッキーセッション用 AWS Cookie を指定して Cookie をカスタマイズすることが必要です。これは、[ユーザーポータル] > [ウェブ] サブカテゴリーの、[ウェブ Cookie] フィールドを使用して設定できます。

制限

[制限] セクションは、ユーザーポータルの以下の機能を許可または制限するために使用されます。

- 以前の Windows 2000 ログイン形式を使用: レガシー（Windows 2000 以前）のログインフォーマットを有効化します。
- Parallels ユーザーポータルを他のウェブページに埋め込むことを許可: これを選択すると、Parallels ユーザーポータルのウェブページを他のウェブページに埋め込むことができます。これは、クリックジャックと呼ばれる攻撃による潜在的なセキュリティ上のリスクになる可能性があることに注意してください。
- ファイル転送コマンド: リモートセッションでのファイル転送を有効化します。ドロップダウンリストで必要なオプションを選択します。詳細については、以下の「リモートファイル転送を構成する」を参照してください。
- クリップボードのリダイレクト: クリップボードオプション: リモートセッションで許可するクリップボードオプションを選択します。[Client からサーバーのみ]（クライアントからサーバーへのコピー/ペーストのみ）、[サーバーから Client のみ]（サーバーからクライアントへのコピー/ペーストのみ）、[双方向]（双方向のコピー/ペースト）から選択します。

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

リモートファイル転送を構成する

Parallels RAS を使用して、エンドユーザーはリモートでファイルをリモートサーバーに転送またはリモートサーバーから転送することができます。

注: この文書の作成時点では、ファイル転送が利用できるのは、Parallels Web Client および Parallels Client for Chrome のみです。なお双方向のファイル転送は、Parallels Web Client のみでサポートされています。

リモートファイル転送機能を柔軟に設定できるように、Parallels RAS では以下の 3 つのレベルを設定することができます。

- RD セッションホスト、プロバイダー、またはリモート PC
- ユーザーポータル
- クライアントポリシー

各レベルで設定したファイル転送設定の優先順位は、上述の順序になります。たとえば、ファイル転送をユーザーポータルで有効にし、RD セッションホストで無効にしている場合、ユーザーポータルから所定の RD セッションホストに接続するすべてのユーザーについて、ファイル転送が無効になります。また、RD セッションホストでファイル転送を有効にし、特定のクライアントポリシー（またはユーザーポータル）で無効にすることもできます。このように、ファイル転送を利用できるクライアントと利用できないクライアントを制御することが可能になります。

ユーザーポータルのリモートファイル転送を構成するには、[ファイル転送コマンド] ドロップダウンリストで次のオプションのいずれかを選択します。

- 無効: リモートファイル転送は無効です。
- Client からサーバー: クライアントからサーバーへのファイル転送のみ。
- サーバーから Client: サーバーからクライアントへのファイル転送のみ。
- 双方向: 双方向のファイルを転送が可能。

ウェブ

注: [ウェブ] サブカテゴリーは、ゲートウェイモードが [通常] に設定されている場合にのみ使用できます。

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

リダイレクト URL

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

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

ゲートウェイは、ウェブリクエストを受信すると、[ウェブ] カテゴリーで指定された URL を使用してリダイレクトするよう、ウェブブラウザーに応答します。

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

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

4 置換後の URL がウェブブラウザーに返送され、ブラウザーはその URL を使ってユーザーポータルのログインページを開きます。

デフォルトの URL フォーマット

デフォルトの URL フォーマットは以下のようになっています。

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

- 変数 `%hostname%` は、元のリクエストを受信したサーバーの名前に置き換えられます。この例ではロードバランサーの DNS 名になります。必要であれば、この変数を特定のホスト名や IP アドレス（このゲートウェイや別のゲートウェイなど）に置き換えることもできます。（例: `https://192.168.5.5/userportal`）。この方法では、常時ウェブリクエストが指定のホストに転送され、ユーザーポータルがそこで開かれます。ホストをハードコーディングしてしまうことはあまり実用的ではありませんが、そうすることは可能です。
- `userportal` は定数で、ユーザーポータルログインページへのパスになります。

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

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

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

特定のユーザーポータルテーマを開く

ユーザーポータルのテーマは、ユーザーのグループに合わせてユーザーポータルのデザインや操作性をカスタマイズできる機能です。

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

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

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

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

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

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

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

詳細については、「ユーザーポータルテーマ設定」 > 「URL」 を参照してください。

ユーザーポータルを開く

[ユーザーポータルを開く] ボタンは、指定されたゲートウェイアドレスを使用し、この特定のゲートウェイ上のユーザーポータルを新しいタブで開きます。このボタンを使用して、展開のテストを実行できます。

ウェブ Cookie

ウェブ Cookie フィールドは、セッションの Cookie 名の指定に使用します。RAS HTML5 セッションのパーシスタンスは、通常、ユーザーの IP アドレス（ソースアドレス指定）により設定されます。ソースアドレス指定が使用できない環境では（セキュリティポリシーで許可されない場合など）、セッション Cookie を使用して、クライアントとサーバーの間のパーシスタンスを維持できます。そのためには、パーシスタンスにセッションクッキーを使用できる負荷分散機能を設定する必要があります。デフォルトの Cookie 名は ASP.NET_SessionId です。

Amazon Web Services（AWS）など、サードパーティーのロードバランサーを使用している場合、専用の Cookie 名を指定する必要があります。AWS では、ロードバランサーは、クライアントからのリクエストを最初に受信すると、リクエストをターゲットにルーティングし、AWSALB という Cookie を生成します。これは、選択されたターゲットの情報をエンコードしたものです。ロードバランサーはこの Cookie を暗号化してクライアントへの応答に含めます。スティッキーセッションが有効になっている場合、ロードバランサーは同じターゲットが正しく登録され、正常な状態にあると想定し、クライアントから受信した Cookie を使用してトラフィックをそのターゲットにルーティングします。

Wyse

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

注: [Wyse] カテゴリーは、Gateway モードが [通常] に設定されている場合にのみ使用できます。

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

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

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

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

セキュリティ

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

サイトのデフォルト設定を使用するには、[デフォルト設定を継承] オプションをクリックします。固有の設定を指定するには、オプションをクリアします。

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

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

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

Gateway の管理

RAS Secure Gateway の管理タスクを実行するには、次の操作を実行します。

1 [インフラストラクチャ] > [Secure Gateway] を選択します。

2 ここから、Gateway を選択し、省略記号のメニューを使用して管理タスクを実行できます。また、Gateway をクリックすると、Gateway の詳細を表示するビューが開き、同様のタスクを実行できます。このタスクについて、以下に説明します。

コントロール

Gateway を有効化または無効化できます。

ログ

RAS Secure Gateway は監視され、ログは関連情報を含めた状態で作成されます。ロギングを構成するには、次のいずれかをクリックします。

- 構成: ログを構成することができます。ログレベルの説明については、以下を参照してください。
- 取得: ログファイルを含む ZIP アーカイブを指定したロケーションに取得します。
- クリア: 既存のログをすべてクリアします。

利用可能なログレベルは以下の通りです。

- 標準: もっとも重要なイベントのみを記録する標準のログレベルです。後述のいずれかのログレベルを使用するように Parallels RAS サポートから指定された場合以外は、常にこのレベルを使用してください。
- 拡張: このログレベルでは、標準ロギングよりも多くの情報が取得されます。ただし、収集する必要のある情報が増加するため、システムの速度が低下します。
- 詳細: 詳細ロギングでは拡張ロギングよりも多くの情報が取得されるため、システムの速度が大幅に低下する可能性があります。

パフォーマンスの低下を回避するには、拡張ロギングと詳細ロギングを（分析のために必要な情報を収集する上で十分な）限定的な期間のみ有効にする必要があります。この期間は [後で標準レベルにリセット] オプションを使用して設定できます。デフォルト値は 12 時間です。場合によっては、Parallels サポートエンジニアが、この期間に別の値を設定するようにアドバイスします。この期間が終了すると、ログレベルがリセットされて標準に戻ります。

他の処理

- 更新: 表示されている Gateway 情報を更新します。
- サイトのデフォルト値: サイトのデフォルトビューを開きます。
- 削除: ファームから Gateway を削除します。

Connection Broker

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

RAS Connection Broker の構成

サイトにインストールされた RAS Connection Broker を表示するには、 [インフラストラクチャ] > [Connection Broker] に移動します。

サイトには、少なくともプライマリ Connection Broker がインストールされている必要があり、その [プライオリティ] 列にはプライマリであることが記されています。冗長性を確保するため、セカンダリエージェントを追加することもできます（p. 90）。

Connection Broker の構成を変更するには、リストでそれをクリックし、中央ペインの [プロパティ] をクリックします。[編集] をクリックして、以下のオプションを指定します。

- 有効: Connection Broker を有効または無効にします。
- IP: サーバーの IP アドレスを指定します。

- 代替の IP: 1 つ以上の代替 IP アドレスをセミコロンで区切って指定します。これらのアドレスは、RAS Secure Gateway が、[IP] フィールドに指定されたアドレスを使用して RAS Connection Broker に接続できなかった場合に使用されます。これは、Active Directory に参加していないネットワークから Gateway が接続している場合などに起こる可能性があります。
- スタンバイ: 選択されている場合、セカンダリ Connection Broker をスタンバイモードにします。つまり、別の Connection Broker がオフラインになるまで、どのエージェントもこの Connection Broker に接続しません。このオプションは、すでに存在する 3 つを超えるすべての新しいセカンダリ Connection Broker で自動的に有効になります。システムパフォーマンスが低下する可能性があるため、3 つを超えるアクティブな Connection Broker を使用することは推奨されません。このオプションを使用して、3 つを超える Agent を使用することができますが、必要になるまでスタンバイモードにしておきます。詳細については、「セカンダリ Connection Broker を追加」（p. 90）を参照してください。

変更が完了したら、[保存] をクリックし、[すべての変更の適用] をクリックします。

メイン Connection Brokers ビューの省略記号のメニューには、次の項目が含まれています。

- 追加: RAS Connection Broker をサイトに追加します。セカンダリ Connection Broker の追加方法の詳細については、続くセクションを参照してください。
- エージェントを更新: エージェントをアップデートします。
- エージェントを無効化/有効化: エージェントを有効または無効にします。
- ログ: ロギングの管理を有効にします。
- プライマリへの昇格: セカンダリ Connection Broker をプライマリに昇格します。
- 優先順位を上げる: セカンダリ Connection Broker の優先順位を上げます。（優先順位リストで上に移動します）。
- 優先順位を下げる: セカンダリ Connection Broker の優先順位を下げます（優先順位リストで下に移動します）。
- 更新: Connection Broker リストを更新します。
- 削除: セカンダリ Connection Broker をサイトから削除します。現在のプライマリ Connection Broker を削除するには、まずセカンダリ Connection Broker をプライマリに昇格させる必要があります。

追加情報

- セカンダリ Connection Broker を追加する（p. 90）

- RAS Connection Broker を管理する（p. 93）

セカンダリ Connection Broker を追加する

冗長性を確保するためにセカンダリ Connection Broker がサイトに追加されます。これにより、プライマリ Connection Broker に障害が発生しても、セカンダリ Connection Broker がリクエストを処理できるようになります。Connection Broker は、高可用性を確保するために、アクティブ/アクティブ構成で動作します。Connection Broker に障害が発生しても、負荷に対応可能な予備の Agent が常に待機しています。一般的に、N+1 の冗長構成をサイトごとに使用する必要があります。自動昇格に 3 つを超える Connection Broker を設定することはできません（自動昇格は本セクションで後ほど説明します）。

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

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

プロセス	プライマリ Connection Broker	セカンダリ Connection Broker
PA（カウンター）のモニタリング	はい	はい
RD セッションホスト（カウンター）のモニタリング	はい	はい
プロバイダー（カウンター）のモニタリング	はい	はい
RDS セッション（再接続）のモニタリング	はい	はい
展開済みの RDS アプリケーションのモニタリング	はい	はい
VDI セッション（再接続）のモニタリング	はい	はい
システム設定の管理	はい	いいえ
ライセンス情報とハートビートの送信	はい	いいえ

CEP 情報の処理および送信	はい	いいえ
レポートサーバーへの情報の送信	はい	いいえ
RDS スケジューラーの管理	はい	いいえ
エンジン情報のレポート	はい	今後のバージョン
シャドーイング	はい	今後のバージョン
メール通知の送信	はい	いいえ

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

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

発生する負荷は次のように分散されます。

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

セカンダリ Connection Broker のプランニング

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

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

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

ダリ Connection Broker については、「RAS Connection Broker の構成」で説明されています。

RAS Connection Broker をサイトに追加する

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

1 [インフラストラクチャ] > [Connection Broker] を選択します。

2 省略記号のメニューから [追加] を選択します（またはプラス記号のアイコンをクリックします）。[新規を追加] ウィザードが開きます。

3 [ホスト] ページで、以下を指定します。

- ホスト名: RAS Connection Broker をホストするホストの FDQN です。ホストの IP アドレスを自動的に取得するには、[IP の解決] をクリックします。
- IP アドレス: ホストの IP アドレスホストの FQDN を自動的に取得するには、[名前解決] をクリックします。

4 [Agent 設定] ページで、以下を指定します。

- 代替 IP アドレス: 1 つまたは複数の代替 IP アドレスをセミコロンで区切って指定します。これらのアドレスは、RAS Secure Gateway が、FQDN または前のページで指定されたアドレスを使用して RAS Connection Broker に接続できなかった場合に使用されます。これは、Active Directory に参加していない別のネットワークから Gateway が接続している場合などに起こる可能性があります。
- 説明: 説明を追加します（オプション）。
- ファイアウォールルールを有効にする: ホストでファイアウォールを自動的に設定する場合に選択します。
- 必要な場合にホストを再起動: インストール後にホストの再起動が必要な場合、自動的に再起動します。
- Connection Broker を使って Secure Gateway をイントール: 指定したホストに RAS Secure Gateway もインストールする場合は、このオプションを選択します。このオプションを選択している場合、[HTML5 Gateway を有効化] オプションを選択して、Gateway でユーザーポータルを自動的に有効にすることもできます。

5 [概要] ページで、設定を確認し、[作成] をクリックします。

この時点から、画面上の指示に従って Connection Broker をファームに追加します。

追加情報:

RAS Connection Broker を管理する（p. 93）

RAS Connection Broker を管理する

RAS Connection Broker の管理タスクを実行するには、次の操作を実行します。

1 [インフラストラクチャ] > [Connection Broker] を選択します。

2 リストで Connection Broker を選択し、省略記号をクリックします。

3 メニューで、以下に説明するオプションのいずれかを選択します。

追加

「セカンダリ Connection Broker を追加する」を参照してください。

エージェントの更新、エージェントの無効化/有効化

Connection Broker を更新、無効化、または有効化します。

ログ

ロギングを構成するには、次のいずれかを選択します。

- 構成: ログを構成することができます。ログレベルの説明については、以下を参照してください。
- 取得: ログファイルを含む ZIP アーカイブを指定したロケーションに取得します。
- クリア: 既存のログをすべてクリアします。

利用可能なログレベルは以下の通りです。

- 標準: もっとも重要なイベントのみを記録する標準のログレベルです。後述のいずれかのログレベルを使用するように Parallels RAS サポートから指定された場合以外は、常にこのレベルを使用してください。
- 拡張: このログレベルでは、標準ロギングよりも多くの情報が取得されます。ただし、収集する必要のある情報が増加するため、システムの速度が低下します。

- 詳細: 詳細ロギングでは拡張ロギングよりも多くの情報が取得されるため、システムの速度が大幅に低下する可能性があります。

パフォーマンスの低下を回避するには、拡張ロギングと詳細ロギングを（分析のために必要な情報を収集する上で十分な）限定的な期間のみ有効にする必要があります。この期間は [後で標準レベルにリセット] オプションを使用して設定できます。デフォルト値は 12 時間です。場合によっては、Parallels サポートエンジニアが、この期間に別の値を設定するようにアドバイスします。この期間が終了すると、ログレベルがリセットされて標準に戻ります。

プライマリへの昇格

このオプションは、セカンダリ Connection Broker のみで有効になります。プライマリ Connection Broker に障害があり、復元できない場合、セカンダリ Connection Broker をプライマリに昇格できます。

優先順位を上げる/優先順位を下げる

このオプションは、セカンダリ Connection Broker のみで有効になります。各セカンダリ Connection Broker には優先順位が与えられます。優先順位を変更するには、[優先順位を上げる] または [優先順位を下げる] を選択します。Connection Broker が、メインリスト内で上下に移動します。リスト内で上に配置されている Agent ほど、優先順位が高くなります。

更新

現在のビューを更新します。

削除

ファームから Connection Broker を削除します。

プロバイダー

プロバイダーは、仮想マシンを仮想デスクトップとして使用するために RAS ファームに追加できるハイパーバイザーまたはクラウドベースの仮想化ソリューションです。

なおこの記事の執筆時点では、RAS 管理ポータルで使用可能なプロバイダー機能は、利用可能なプロバイダー、ホスト、およびアクティブなセッションの表示に限定されています。その他

のプロバイダー関連タスクを実行する場合、デスクトップベースの Parallels RAS Console をご利用ください。

プロバイダーのリスト

プロバイダーのリストを表示するには、[インフラストラクチャ] > [プロバイダー] に移動します。

[プロバイダー] テーブルで列を追加または削除するには、歯車のアイコンをクリックして、必要な列を選択またはクリアします。

タスクを実行するには、リストでプロバイダーを選択し、省略記号のメニューから次のいずれかを選択します。

- ホステッド VDI デスクトップを表示: ホストのリスト（p. 61）を開き、フィルターを適用してこのプロバイダーに属するデスクトップのみを表示します。
- アクティブなセッションの表示: セッションリスト（p. 96）を開き、フィルターを適用してこのプロバイダーに属するセッションのみを表示します。

サイトの既定値

[サイトのデフォルト値] カテゴリーでは、さまざまな RAS コンポーネントおよびサービスのデフォルト設定を構成できます。この記事の執筆時点では、以下の項目についてサイトのデフォルト値を構成できます。

- 公開 - 「サイトのデフォルト値（公開）」（p. 114）を参照してください。
- Gateway - 「Gateway を構成する」（p. 71）を参照してください。
- RD セッションホストとホストプール - 「Agent 設定」（p. 47）を参照してください。
- 多要素認証 - 「多要素認証」（p. 26）を参照してください。

RAS ファームにコンポーネントを追加するとき、またはリソースを公開するとき、サイトのデフォルト値が使用されるので、毎回値を手動で入力する必要はありません。必要に応じて、独自の値でデフォルト値を簡単に上書きできます。

サイトのデフォルト値を表示するには、利用可能なカテゴリーのいずれかをクリックします。デフォルトの設定を変更するには、サイトのデフォルト値ビューで [編集] をクリックします。

第 8 章

セッション

この章の内容

概要

[セッション] カテゴリーには、RD セッションホストや VDI など、利用可能なすべてのホストタイプのユーザーセッションが表示されます。ここでは、セッションをホストしているサーバーの種類にかかわらず、現在のすべてのセッションを表示できます。

[セッション] カテゴリーを選択すると、[セッション] ナビゲーションバーに次の 2 つの項目が表示されます。

- ユーザーセッション: 利用可能なすべてのホストのユーザーセッションを一覧表示します。
- 実行中のリソース: すべてのホストで現在実行中の公開済みリソース（アプリやデスクトップ）を一覧表示します。

[セッション] カテゴリーまたは [アクティブセッション] タブを開いたときに、リスト内の列の一部がすぐに表示されない場合があります。これは、これらの値を算出するのに時間がかかるためです。そのような列の例としては、[ログオン時間]、[UX エバリュエーター]、[遅延] などがあります。数秒後にはリストに値が表示されます。

セッション情報

ユーザーセッションを表示するには、[セッション] > [ユーザーセッション] に移動します。このリストには、RD セッションホストや VDI など、利用可能なすべてのタイプのホストに存在するユーザーセッションが含まれています。

テーブルの列を表示または非表示にするには、歯車のアイコンをクリックして、列名を選択またはクリアします。

セッションの詳細を表示するには、セッションを選択し、ユーザー名をクリックします。これにより、セッション情報ビューが開き、セッション情報が表示されます。

以下のグループが表示されます。

- セッションセットアップ: 一般的なセッション情報が表示されます。
- セッションの詳細: 現在のセッションの状態、ログオン時間、受信/送信データサイズ、および一般的なセッション情報が表示されます。
- ユーザーエクスペリエンス: ユーザーエクスペリエンスを評価するために使用できるメトリクスが表示されます。
- ログオンの詳細: ログオンプロセスを評価するために使用できるログオンメトリクスが表示されます。
- 接続の詳細: 接続と認証の詳細を表示します。
- クライアントの詳細: ユーザーデバイスと Parallels Client のタイプとバージョンに関する情報を表示します。

Parallels RAS 18 では、25 を超える新しいセッション詳細メトリクスが導入されています。以下の表は、これらの新しいメトリクスと既存の重要なメトリクスの概要を示しています。

注: 一部の新しいメトリクスを表示するには、最新の Parallels Client が必要です。

セッションセットアップ

メトリクス	記述
セッションホスト*	セッションホスト名
ソース*	セッションカテゴリーのみ。 ホストタイプ: RDSH（VDI 経由の場合も含む）、VDI、リモート PC（VDI 経由のみ）、Azure Virtual Desktop。

* Parallels RAS 18.1 で導入された新機能

セッションの詳細

メトリクス	記述

セッションの状態	アクティブ状態、アイドル状態、切断など
ログオン時間	セッションが確立した日時
セッションの長さ	セッションが確立した時間
アイドル時間	セッションがアイドル状態だった時間
受信データ*	クライアントから受信したデータ量
送信データ*	クライアントに送信したデータ量
解像度	セッションの解像度
色深度	セッションの色深度
帯域幅の使用状況*	クライアントの帯域幅使用状況

* Parallels RAS 18.0 で導入された新機能

ユーザーエクスペリエンス

メトリクス	記述
UX エバリュエーター*	クライアント側の最初の手順（ユーザーのアクション）から最後の手順（レスポンスの画像表示）までの時間間隔を測定したものです。
接続品質*	接続品質を判定（「悪い」～「非常に良い」）
遅延*	ネットワーク遅延
トランスポートプロトコル*	TCP または UDP（RDP 経由）
帯域幅の可用性*	クライアント側の帯域幅の可用性
再接続*	現在のセッションで開始時に接続不良で再接続した回数（正常接続は除く）
最終再接続*	現在のデバイスのセッションで接続不良で再接続した回数（正常接続は除く）
切断の理由*	最終セッションの切断理由

* Parallels RAS 18.0 の新機能

ログオンの詳細

メトリクス	記述
ログオン期間*	ログオンにかかる時間（UI での待機時間を除く）。
ログオン期間の内訳*	接続時間 認証期間 ホストの準備（負荷分散アルゴリズムを含む） ユーザープロファイルの読み込み時間 RAS ポリシーの検索 グループポリシーの処理時間 デスクトップの読み込み時間 その他
ユーザープロファイル*	使用中のユーザープロファイル形式: FSLogix、ユーザープロファイルディスク、その他（エラーコードなどの付加情報も含む）。

* Parallels RAS 18.0 で導入された新機能

接続の詳細

メトリクス	記述
接続モード	クライアントが使用する接続モード（例: GW SSL）。
認証タイプ	クライアントが使用する認証タイプ（例: 資格情報）。
MFA プロバイダー	クライアントが使用する MFA プロバイダー（存在する場合）。
フロー	接続がリソースホストに到達するまでに通過するすべてのホスト（HALB、Gateway、セッションホスト）を一覧表示します。

クライアントの詳細

メトリクス	記述
デバイス名	セッションが確立されたデバイス名
IP アドレス	クライアントのプライベート IP アドレス
クライアント OS*	クライアントで実行されているオペレーティングシステム
クライアント OS バージョン*	クライアントで実行されているオペレーティングシステムのバージョン
クライアントバージョン*	使用中の RAS クライアントのバージョン

* Parallels RAS 18.0 で導入された新機能

セッション情報のエクスポート

セッション情報を CSV ファイルにエクスポートするには、ナビゲーションバーの [エクスポート] をクリックして、場所とファイル名を指定します。

省略記号のメニューで [エクスポート] をクリックして、メインセッションリストからセッション情報をエクスポートすることもできます。リストで選択する項目に応じて、以下のものがエクスポートされることに注意してください。

- シングルセッション - そのセッションに関する情報がエクスポートされます。
- マルチセッション - 選択したすべてのセッションの情報がエクスポートされます。
- 選択なし - 現在のすべてのセッションに関する情報がエクスポートされます。エクスポートされた CSV には、エクスポートされたセッションの詳細と、以下の形式でエクスポートされた詳細が含まれます。

%Administrator% により %date% %time% にエクスポートされた Parallels RAS ファーム %Farm name% およびサイト %Site name% からのセッション詳細（RD セッションホストなどの %Server type%）

ユーザーセッション

1 つのユーザーセッション（または同時に複数のセッション）を管理するには、1 つまたは複数のセッションを選択し、省略記号のメニューを使用して次の処理から選択します。

- セッション情報を表示: セッション情報ビュー（p. 96）に移動します。このオプションは、単一のセッションが選択されている場合にのみ利用できます。
- メッセージ: [メッセージを送信] ダイアログを開きます。ここにメッセージを入力し、セッション所有者に送信できます。
- 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。
- リソースを表示: 実行中のリソースビュー（p. 102）に切り替わります 。
- 実行中のプロセスを表示: 選択したセッションの実行中のプロセスを一覧表示するビューを開きます。このオプションは、単一のセッションが選択されている場合にのみ利用できます。以下の「実行中のプロセス」を参照してください。
- 監視設定: RD セッションホストのセッションメトリクス値のハイライト表示を設定する、監視設定ダイアログを開きます。このダイアログには利用可能なメトリクスが一覧表示され、任意のメトリクスに警告とクリティカルのしきい値を設定することができます。しきい値を設定するには、メトリクス名の前にあるチェックボックスを選択し、必要な値を指定します。RAS ファームの動作中、しきい値に達すると、セッションメトリクス値が以下のようにハイライト表示されます。警告のしきい値: オレンジ、クリティカルのしきい値: 赤。

  指定したしきい値の値をリセットするには、しきい値を選択して、省略記号メニューから [リセット] を選択します（または右クリックして [リセット] を選択します）。また、メトリクスのしきい値の色分けを有効または無効にすることもできます。これを実行するには、メトリクスを選択し、省略記号メニューから [有効] または [無効] を選択します。
- 更新: リストを更新します。
- エクスポート: CSV ファイルにセッション情報をエクスポートします。「セッション情報」（p. 96）を参照してください。

実行中のプロセス

[実行中のプロセスを表示] メニューオプションにより、選択されたセッションのプロセスのみを表示するフィルターを適用した、セッションホストの実行中のプロセスビューが開きます。

省略記号のメニューを使用して、プロセスに対する以下の処理を実行できます。

- プロセスの強制終了: 選択したプロセスを強制終了します。
- 更新: リストを更新します。

実行中のリソース

すべてのホストで現在実行中の公開済みリソースのリストを表示するには、[セッション] > [実行中のリソース] の順に選択します。

注意すべき列をいくつか紹介します。

- 公開済みの名前: 公開済みのリソースの名前（[公開] カテゴリーに表示）。
- ID: 公開済みのリソース ID（[公開] カテゴリーに表示）。
- 説明: 公開済みリソースの説明です。
- プロセス名: 対応するプロセス名です。
- ユーザー: セッション所有者。
- セッション ID: セッション ID。
- セッションホスト: セッションホスト名。
- ソース: セッションソース（RDSH、VDI）です。

リソース上でタスクを実行するには、リストでセッションを選択し、省略記号メニューをクリックします。次のようなタスクを実行できます:

- メッセージ: セッション所有者にメッセージを送信します。
- 切断: セッションを切断します。
- ログオフ: セッションをログオフします。
- 実行中のプロセスを表示: 対応する PID フィルターを適用した上で、セッションホストの実行中のプロセスビューを開きます。

- ユーザーセッション: セッション情報ビュー（p. 96）を開きます。
- 情報の表示: リソースサマリー情報とセッション情報を表示します。セッション情報には、「セッション情報」（p. 96）に記載されているものと同じメトリクスが含まれています。
- 監視設定: 「ユーザーセッション」トピック（p. 101）の [監視設定] メニューオプションの説明を参照してください。
- 更新: リストを更新します。
- エクスポート: リソース情報を CSV ファイルにエクスポートします。

公開済みリソースの詳細情報を表示するには、リソース名をクリックします。公開済みリソースの基本情報（ID、名前、ターゲットなど）と対応するセッション情報を表示するビューが表示されます。セッションメトリクスの詳細については、「セッション情報」（p. 96）を参照してください。リソース名をクリックすると、公開済みリソースが構成されている、[公開] カテゴリーに移動します。ナビゲーションバーの各項目では、前述の対応するメニュー項目と同じ処理を実行できます。

第　9　章

公開

公開は、エンドユーザーが Parallels RAS のリソースを利用できるようにするプロセスです。RAS 管理ポータルから公開できるリソースは以下の通りです。

- アプリケーション
- デスクトップ
- ドキュメント
- ファイルシステム上のフォルダー

公開は、RAS 管理ポータルの [公開] カテゴリーから実行します。

[公開] カテゴリーを選択すると、公開済みリソースが中央ペインに表示されます。リソースを選択すると、そのリソースに関する情報が右側ペインに表示されます。リソースがフォルダーに配置されている場合は、まずフォルダーを展開して、リソースを選択する必要があります。既存の公開済みリソースを修正するには、右側ペインの右上にある [編集] ボタンをクリックします。

公開タスクを実行するには、中央ペインの上部にあるメニューバーを使用します。ここから、新しいリソースの公開、フォルダーの追加（例: 同じ種類のリソースのグループ化）、リソースの複製、リソースの有効化/無効化、リストのソート、その他のタスクを実行できます。

この章の内容

アプリケーションを公開する

アプリケーションを公開するには、次の操作を実行します。

1 RAS 管理ポータルで [公開] カテゴリーを選択します。

2 中央ペインでプラス記号のアイコンをクリックします（または省略記号のメニューから [追加] を選択します）。公開ウィザードが開きます。

3 [公開タイプ] ページで、[アプリケーション] を選択し、[次へ] をクリックします。

4 [サイト] ページで、アプリケーションの公開元となる、1 つまたは複数（利用可能な場合）のサイトを選択します。

5 [次へ] をクリックします。

6 [公開元] ページで、次のオプションから選択します。

- サイト内の全サーバー: このサイトで利用可能なすべてのホストから公開します。
- サーバーホストプール: アプリケーションの公開元となるホストプールを 1 つ以上指定します。
- 個々のサーバー: 1 つまたは複数の個別ホストを指定します。

7 [次へ] をクリックします。

8 [アプリケーションの種類] ページで、以下から選択します。

- インストール済みおよび事前定義されたアプリケーションから選択: このオプションを選択すると、プリインストールされた標準の Windows アプリケーションから選択できます。
- 単一のアプリケーションを手動で追加: このオプションを選択すると、すべてのアプリケーション設定を自分で構成できます。

9 [次へ] をクリックします。

10 前のページで選択したアプリケーションの種類に応じて、次のページが表示されます。

- インストール済みおよび事前定義されたアプリケーションから選択: このページには、プリインストールされているアプリケーションとアプリケーショングループのリストが表示されます。グループ全体または個々のアプリケーションを選択できます。完了したら、[次へ] をクリックし、画面上の指示に従ってウィザードを完了し、アプリケーションを公開します。このセクションの残りの部分はスキップできます。
- 単一のアプリケーションを手動で追加: アプリケーションの設定を指定するページが表示されます。内容をご確認ください。

11 [単一のアプリケーションを手動で追加] を選択した場合、以下のようにアプリケーションを設定するページが表示されます。

[ターゲットアプリケーション] セクションで以下を指定します。

- ターゲット: アプリケーションの実行ファイル名とパスです。
- 起動パス: アプリケーションが現在の作業ディレクトリとして使用するパス（デフォルトでは、実行可能なパス）です。
- パラメーター: アプリケーションの起動パラメーター（存在する場合）です。

[公開済みリソース設定] セクションで以下を指定します。

- 名前: アプリケーションの名前を入力します。
- 説明: 説明を入力します（オプション）。
- ウィンドウモード: 通常、最大化、最少化から選択します。
- ユーザーがログオンすると自動的に起動: ユーザーがログオンしたらすぐにアプリケーションを起動する場合はこのオプションを選択します。このオプションは、デスクトップバージョンの Parallels Client でのみ機能します。
- セッションの事前起動から除外: アプリケーションは、セッションの事前起動から除外されます。
- アイコン: [参照] をクリックしてアプリケーションのアイコンを選択します。アイコン変更: アプリケーションのアイコンを変更します（オプション）。

12 次のページでは、リソースの初期状態を指定します。次のオプションから選択します。

- 有効: エンドユーザーはリソースを起動できます。
- 無効: このリソースは Parallels Client では表示されません。
- メンテナンス中: 該当リソースは Parallels Client で表示されますが、ユーザーはそのリソースを起動できません。リソースがメンテナンス中の場合、ユーザーがそのリソースを起動しようとするとメッセージが表示されます。メッセージをカスタマイズするには、[構成] ボタンをクリックします。詳細については、「サイトのデフォルト値（公開）」（p. 114）を参照してください。

13 [次へ] をクリックし、[完了] をクリックしてアプリケーションを公開します。

デスクトップの公開

デスクトップを公開するには、次の操作を実行します。

1 RAS 管理ポータルで [公開] カテゴリーを選択します。

2 中央ペインでプラス記号のアイコンをクリックします（または省略記号のメニューから [追加] を選択します）。公開ウィザードが開きます。

3 [公開タイプ] ページで、[デスクトップ] を選択し、[次へ] をクリックします。

4 [サイト] ページで、アプリケーションの公開元となる、1 つまたは複数（利用可能な場合）のサイトを選択します。

5 [次へ] をクリックします。

6 [公開元] ページで、次のオプションから選択します。

- サイト内の全サーバー: このサイトで利用可能なすべてのホストから公開します。
- サーバーホストプール: アプリケーションの公開元となるホストプールを 1 つ以上指定します。
- 個々のサーバー: 1 つまたは複数の個別ホストを指定します。

7 [次へ] をクリックします。

8 [デスクトップ] ページで、以下を指定します。

[公開済みリソース設定] セクションで以下を指定します。

- 名前: デスクトップの名前を入力します。
- 説明: 説明を入力します（オプション）。
- 管理セッションに接続: ユーザーを管理セッションに接続するには、このオプションを選択します。
- ユーザーがログインすると自動的に起動: ユーザーのログイン後すぐにデスクトップを開く場合に選択します。
- セッションの事前起動から除外: デスクトップは、セッション事前起動から除外されます。
- アイコン: アプリケーションのアイコンを選択します。

[デスクトップセッション設定] セクションで以下を指定します。

- デスクトップサイズ: サイズを指定します。利用可能なオプションと画面解像度から選択するか、カスタム設定を指定することができます。カスタムの幅および高さを設定するには、[カスタム] を選択し、表示されたフィールドで任意の値を指定します。
- マルチモニター: マルチモニターのサポートを有効にするか、またはクライアントの設定を使用するかを選択します。

9 次のページでは、リソースの初期状態を指定します。次のオプションから選択します。

- 有効: エンドユーザーはリソースを起動できます。
- 無効: このリソースは Parallels Client では表示されません。
- メンテナンス中: 該当リソースは Parallels Client で表示されますが、ユーザーはそのリソースを起動できません。リソースがメンテナンス中の場合、ユーザーがそのリソースを起動しようとするとメッセージが表示されます。メッセージをカスタマイズするには、[構成] ボタンをクリックします。詳細については、「サイトのデフォルト値（公開）」（p. 114）を参照してください。

10 [次へ] をクリックし、[完了] をクリックしてデスクトップを公開します。

ドキュメントの公開

ドキュメントの公開は、アプリケーションの公開と類似していますが、アプリケーションの実行ファイルの代わりに、ドキュメントのファイル名とパスを指定します。詳細については、「アプリケーションの公開」（p. 104）を参照してください。

ファイルシステム上のフォルダーの公開

ファイルシステム上のフォルダーを公開するには、次の操作を実行します。

1 RAS 管理ポータルで [公開] カテゴリーを選択します。

2 中央ペインでプラス記号のアイコンをクリックします（または省略記号のメニューから [追加] を選択します）。公開ウィザードが開きます。

3 [公開タイプ] ページで、[ファイルシステム上のフォルダー] を選択し、[次へ] をクリックします。

4 [サイト] ページで、アプリケーションの公開元となる、1 つまたは複数（利用可能な場合）のサイトを選択します。

5 [次へ] をクリックします。

6 [公開元] ページで、次のオプションから選択します。

- サイト内の全サーバー: このサイトで利用可能なすべてのホストから公開します。
- サーバーホストプール: アプリケーションの公開元となるホストプールを 1 つ以上指定します。
- 個々のサーバー: 1 つまたは複数の個別ホストを指定します。

7 [次へ] をクリックします。

8 [フォルダー] ページで、以下を指定します。

- 名前: フォルダーの名前を入力します。
- 説明: 説明を入力します（オプション）。
- ウィンドウモード: ウィンドウモード（通常、最大化、最少化）を選択します。
- UNC パス: 公開するフォルダーの UNC パスを入力します。
- アイコン: フォルダーのアイコンを選択します

9 次のページでは、リソース（フォルダー）の初期状態を指定します。次のオプションから選択します。

- 有効: エンドユーザーはリソースを開くことができます。
- 無効: このリソースは Parallels Client では表示されません。
- メンテナンス中: 該当リソースは Parallels Client で表示されますが、ユーザーはそのリソースを使用できません。リソースがメンテナンス中の場合、ユーザーがそのリソースを開こうとするとメッセージが表示されます。メッセージをカスタマイズするには、[構成] ボタンをクリックします。詳細については、「サイトのデフォルト値（公開）」（p. 114）を参照してください。

10 [次へ] をクリックし、[完了] をクリックしてフォルダーを公開します。

公開済みリソースの管理

公開済みのリソースを表示するには、RAS 管理ポータルで [公開] カテゴリーを選択します。

[公開] ペインに現在公開されているリソースが一覧表示されます。項目をドラッグして希望の行にドロップすると、リストを並べ替えることができます。

省略記号のメニューを使用して、一般的な管理タスクを実行できます。メニューには次のオプションがあります。

- 追加: 公開ウィザードを開始します。プラス記号のアイコンは、このメニューオプションに対応するツールバー項目です。
- 複製: 選択したリソースの複製を作成します。
- 新しいフォルダー: 公開リストにフォルダーを作成します。これは仮想フォルダーで、アプリケーションリストでリソースをグループ化するためにのみ使用されます。フォルダーは、

Parallels Client のアプリケーションリストに表示されます。フォルダーのアイコンは、このメニューオプションに対応するツールバー項目です。

- 更新: 表示されている情報を更新します。
- ステータスを設定する: リソースを有効化/無効化するか、メンテナンスモードにします。ユーザーは、無効になったリソースを利用できません。メンテナンス中のリソースは、クライアント側のリストに表示されますが、使用することはできません。リソースの状態を”無効”または”メンテナンス中”に変更すると、リスト内のリソース名がグレーになり、現在の状態がカッコで表示されます。
- 上に移動: リスト内で公開済みリソースを上に移動します。この場合、リソース ID などは変更されません。
- 下に移動: リスト内でリソースを下に移動します。
- ソート: リソースをアルファベット順でソートします。この処理項目を有効にするには、[公開済みのリソース] ノード（最上位のノード）または個別のリソースが含まれるフォルダーを選択する必要があります。
- 削除: 公開済みリソースを削除します。公開済みのリソースはファームから削除されますが、実際のアプリケーションは影響を受けません。

追加情報

以降のセクションでは、さまざまなタイプの各公開済みリソースを管理する方法について説明します。

公開済みアプリケーションの管理

ウィザードを使用してアプリケーションを公開する場合、名前、実行ファイルのパスなど、いくつかのアプリケーションパラメーターを指定します。これらのオプションは、アプリケーションの公開後に変更できます。

公開済みアプリケーションを変更するには、[公開] ペインで該当のアプリケーションを選択し、右ペインの [編集] をクリックして編集できるようにします。アプリケーションのプロパティを以下のように変更します。

なお、ここでの設定の大半は、アプリケーションの公開ウィザードでの設定と同じです。個々の設定の詳細については、「アプリケーションを公開する」（p. 104）も参照してください。以下では、ウィザードでは使用できず、ここでのみ設定可能な項目を中心に説明します。

アプリケーション

このビューの設定のほとんどは、公開ウィザードと同じです。新しいオプションセットは、[サーバーごとの設定] です。アプリケーションが複数のサーバーから公開される場合、各サーバーに対して以下のアプリケーションプロパティを個別に設定できます。

- ターゲット
- スタート
- パラメーター

一例として、異なるサーバーで異なるフォルダーにアプリケーションがインストールされているとき、上記のプロパティを変更して、[ターゲット] および [開始] フィールドの値を各サーバーで有効にできます。

フィルタリング

[フィルタリング] カテゴリーのオプションは、公開ウィザードでは使用できず、ここでのみ設定可能です。このカテゴリーは、すべてのタイプの公開済みリソースに共通です。詳細については、「フィルタールールの使用」（p. 116）を参照してください。

ルーティング

「優先ルーティングを構成」（p. 118）を参照してください。

ショートカット

このビューでは、アプリケーションのショートカットを作成するユーザーデバイス上の場所を設定できます。これらの設定はサイトのデフォルト値から継承されますが、特定のアプリケーション用にカスタマイズすることができます。詳細については、「サイトのデフォルト値（公開）」（p. 114）を参照してください。

ファイル拡張子

このカテゴリーでは、アプリケーションのファイル拡張子の関連付けを変更できます。項目を追加/削除/変更するには、[ファイル拡張子] オプションを選択します。リストに新しい拡張子を追加するには、省略記号メニューから [追加] を選択し、必要な拡張子を指定します。既存の関連付けを変更するには、リストで拡張子を選択し、省略記号メニューから [プロパティ] を選択します。

ライセンス

「サイトのデフォルト値（公開）」（p. 114）を参照してください。

ディスプレイ

「サイトのデフォルト値（公開）」（p. 114）を参照してください。

変更した場合は、[保存] ボタンをクリックするか、[キャンセル] をクリックして変更を破棄します。

公開済みデスクトップの管理

公開済みデスクトップを変更するには、公開ビューで該当のデスクトップを選択します。デスクトップ設定を表示および変更するには、中央ペインのナビゲーションバーを使用します。設定を編集するには、[編集] ボタンをクリックします。

概要

このビューには、他のナビゲーションバー項目が簡単な説明付きで表示されます。ここ、またはナビゲーションバーで項目をクリックできます。

公開元

デスクトップの公開元となるホストまたはホストプールを一覧表示します。[公開元] ドロップダウンリストを使用して、個々のホストまたはホストプールを切り替えます。必要に応じて、ホストまたはホストプールを選択またはクリアします。

デスクトップ

このビューには、公開済みデスクトップの設定が表示されます。これらの設定を構成する方法の詳細については、「デスクトップの公開」（p. 106）を参照してください。

フィルタリング

フィルタリングビューの設定は、公開ウィザードでは使用できず、ここでのみ設定可能です。これらの設定は、すべてのタイプの公開済みリソースに共通です。詳細については、「フィルタールールの使用」（p. 116）を参照してください。

ルーティング

「優先ルーティングを構成」（p. 118）を参照してください。

ショートカット

このビューでは、公開済みデスクトップのショートカットを作成するユーザーデバイス上の場所を設定できます。これらの設定はサイトのデフォルト値から継承されますが、特定の公開済みリソース用にカスタマイズすることができます。詳細については、「サイトのデフォルト値（公開）」（p. 114）を参照してください。

変更した場合は、[保存] ボタンをクリックするか、[キャンセル] をクリックして変更を破棄します。

フォルダーの管理

フォルダーを使用して、公開済みのリソースを整理できます。また、フィルターオプションを利用することもできます。

作成できるフォルダーは 2 種類あります。

- 管理目的のフォルダー: このタイプのフォルダーは、Parallels RAS 管理者向けです。これらは RAS 管理ポータルで公開済みのリソースを論理的に整理するために使用されますが、ユーザーデバイス上の Parallels Client Launchpad には表示されません。これらのフォルダーは、管理者が公開済みのリソースをより効率的に管理するのに役立ちます。
- 一般フォルダー: これらのフォルダーは上記の管理目的のフォルダーと似ていますが、ユーザーデバイスの Launchpad に表示されます。通常は、これらのフォルダーを使用して、タイプごとに公開済みのリソースをグループ化します（オフィスアプリケーション、特定のビジネスアプリケーション、ユーティリティなど）。

フォルダーを作成

新しいフォルダーを作成するには、次のいずれかを実行します。

1. [公開] カテゴリーを選択します。
2. [公開] ナビゲーションバーで省略記号メニューをクリックし、[新しいフォルダー] を選択します（またはプラス記号のアイコンが付いたフォルダーをクリックします）。
3. フォルダーの公開元となるサイトを選択します。[次へ] をクリックします。

4 名前と説明（オプション）を入力します。

5 必要に応じて、[管理目的に使用] オプションを選択します（上記の説明を参照）。

6 アイコンを選択するか、デフォルトのアイコンを使用します。

7 [次へ] をクリックします。

8 次のページでは、リソース（フォルダー）の初期状態を指定します。次のオプションから選択します。

- 有効: 該当のフォルダーは、エンドユーザーに対して表示され、エンドユーザーはそのフォルダーに含まれる公開済みリソースを起動できます。
- 無効: このフォルダーは Parallels Client では表示されません。
- メンテナンス中: 該当のフォルダーは Parallels Client で表示されますが、ユーザーはそのフォルダーに含まれるリソースを起動できません。フォルダーにサブフォルダーが含まれている場合、それらは親フォルダーのステータスを継承します。つまり、階層内のどのフォルダーに含まれているリソースも、ユーザー側からはアクセスできないことになります。フォルダーがメンテナンス中の場合、ユーザーが該当のフォルダーからリソースを起動しようとするとメッセージが表示されます。メッセージをカスタマイズするには、[構成] ボタンをクリックします。詳細については、「サイトのデフォルト値（公開）」（p. 114）を参照してください。

9 [完了] をクリックしてフォルダーを作成します。

フォルダーへの公開済みリソースの追加

公開済みリソースをフォルダーに追加するには、リソースを右クリックし、[上に移動] または [下に移動] オプションを使用して、リソースをフォルダーアイコンの下に配置します。

サイトのデフォルト値（公開）

公開済みリソースに対してサイトのデフォルト値を構成するには、次の操作を実行します。

1 [インフラストラクチャ] > [サイトのデフォルト値] を選択します。

2 [公開] をクリックします。

3 デフォルトの設定を表示し、必要に応じて以下のように変更します。

ショートカット

このビューでは、アプリケーションのショートカットを作成するユーザーデバイス上の場所を設定できます。なおショートカットは、すべての種類のオペレーティングシステムで利用できる訳ではありません。

ショートカットを作成するためのオプションは次の通りです。

- デスクトップにショートカットを作成する: このオプションを選択すると、ユーザーのデスクトップにショートカットが作成されます。
- スタートフォルダーにショートカットを作成する: スタートフォルダーにショートカットを作成します。
- 編集フィールドでは、ショートカットを作成するフォルダー名を入力できます。デフォルト値の（ならびに唯一利用可能な）%Groups% 変数では、公開済みのリソースが配置されているホストサーバーに表示される、サブフォルダーが追加されます。たとえば、リソースがホストサーバーの”[Myapps] > [ゲーム]”にある場合、同じフォルダー構造がパスにも追加されます。なお、カスタム変数は一切使用できません。
- 自動スタートフォルダーにショートカットを作成する: アプリケーションのショートカットが [自動スタート] フォルダーに追加され、コンピューターの起動時に自動的に開始されます。

ライセンス

アプリケーションのライセンス使用量をより適切に管理するために、次のオプションを設定します。

- セッションの共有を無効にする: このオプションを有効にすると、特定の公開済みアプリケーションを 1 つのセッションに分離することができます。同じアプリケーションを複数回起動する場合、そのアプリケーションのインスタンスは同じセッションを共有することになります。一方、別のアプリケーションの場合は、独自のセッションで起動します。
- ユーザーごとに単一のインスタンス: このオプションを有効にすると、ユーザーは 1 つのアプリケーションインスタンスのみを起動できます。
- 同時使用ライセンス: このオプションを使用して、アプリケーションが実行できる同時インスタンスの最大数を指定します。たとえば、アプリケーションのライセンスによって、実行できるアプリケーションインスタンスの数が 10 個に限られている場合、[同時使用ライセンス] オプションを 10 に設定します。これにより、この制限に達した場合、他のユーザーが他のインスタンスを実行できなくなります。

- 制限を超えた場合: このドロップダウンメニューから、ライセンスの上限を超えた場合に実行される処理を指定できます。

ディスプレイ

次のオプションを構成します。

- アプリケーションの表示前にすべての RAS ユニバーサルプリンターがリダイレクトされるまで待機する: アプリケーションのロード前にプリンターがリダイレクトされるまで待機する場合は、このオプションを有効にします。ユニバーサルプリンターのリダイレクトの最大待ち時間（秒単位）も指定できます。プリンターのリダイレクトには時間がかかる場合もあります。プリンターのリダイレクト中は、進捗状況バーがユーザーに表示されるので、混乱を避けられます。
- 最大待ち時間（秒）:
- 色濃度: アプリケーションの色濃度を選択します。
- モバイルクライアントを使用する場合にアプリケーションを最大化して開始する: このオプションは、モバイルデバイスで実行する Parallels Client だけに当てはまります。このオプションを選択すると、モバイルデバイスでアプリケーションが最大表示の状態で起動します。ユーザーがリモートアプリケーションを操作しやすくなります。また、RAS 管理者は、このオプションを使用してアプリケーションを簡単に最大化できます。追加の手順は不要です。

メンテナンスメッセージ

メンテナンスメッセージビューでは、公開済みリソースをメンテナンス中に起動しようとしたときにユーザーに表示されるメッセージを指定できます。リソースがメンテナンス中の場合、リソースは Parallels Client で表示されますが、グレーアウトされています（ユーザーポータルでは、リソース名にステータスが表示されています）。ユーザーがリソースを開こうとすると、ここで指定したメッセージが表示されます。変更したメッセージをデフォルトに戻したい場合、任意の言語のメッセージを選択し、[リセット] ボタンをクリックします。

サイトのデフォルト値の変更が完了したら、[保存] をクリックします。

フィルタールールの使用

フィルタリングルールを使用すると、特定の公開済みのリソースにどのユーザーがアクセスできるかを制御できます。各ルールは、ユーザー接続に対するマッチングに使用される 1 つまた

は複数の条件で構成されています。各条件は、マッチング可能な 1 つまたは複数の特定のオブジェクトで構成されています。

次のオブジェクトのマッチングを実行できます。

- ユーザー、ユーザーが所属するグループ、またはユーザーが接続するコンピューター。
- ユーザーが接続する Secure Gateway。
- クライアントデバイスの名前。
- クライアントデバイスのオペレーティングシステム。
- します。
- IP アドレス。
- ハードウェア ID。ハードウェア ID の形式は、クライアントのオペレーティングシステムに依存します。

ルールについて、次のことに注意してください。

- 条件は AND 演算子で連結されます。たとえばあるルールに、特定の IP アドレスに一致という条件とクライアントデバイスのオペレーティングシステムに一致という条件が含まれる場合、ユーザーの接続が IP アドレスの条件とクライアントオペレーティングシステムの条件の両方に一致する場合に、ルールが適用されます。
- オブジェクトは OR 演算子で接続されます。たとえば、クライアントデバイスのオペレーティングシステムに一致するという条件のみを作成した場合、いずれかのオペレーティングシステムがクライアント接続に一致すれば、ルールが適用されます。
- ルールは、上から順にユーザー接続と比較されます。このため、ルールの優先順位は、ルールリスト内の位置によって異なります。Parallels RAS では、ユーザー接続に一致する最初のルールが適用されます。
- いずれのルールにもマッチしない場合には、デフォルトルールが使用されます。このルールは、許可または拒否のいずれかに設定できますが（以下を参照）、条件を利用することはできません。

新しいルールを作成するには、次の操作を実行します。

1 [公開] に移動します。

2 ルールを作成するリソースをクリックします。

3 中央のペインで [フィルタリング] を選択します。

4 [編集] をクリックします。

5 プラス記号をクリックします。

6 ルールの名前と説明（オプション）を指定します。

7 ルールの条件を指定します。以下のコントロールを利用できます。

- Allow: 指定すると、ユーザー接続が条件に一致した場合に、リソースにアクセスできるようになります。Allow をクリックして、Deny に変更できます。
- Deny: 指定すると、ユーザー接続が条件に一致した場合に、リソースへのアクセスを拒否するようになります。Deny if をクリックして、Allow に変更できます。
- （+）: 新しい条件を追加します。一致条件として、Secure Gateway、クライアントデバイス名、クライアントデバイスのオペレーティングシステム、テーマ、IP アドレス、ハードウェア ID のいずれかを使用したい場合は、（+）をクリックします。
- （X）: マッチングから特定のオブジェクトを削除します。たとえば、IP アドレス 198.51.100.1 をマッチングから削除したい場合は、その横にある（X）をクリックします。
- is: ユーザー接続が条件に一致した場合に、リソースがアクセス可能な状態でなければならないことを指定します(アクセス不可を指定することも可能。Allow または Deny による）。is をクリックして、is not に変更できます。このコントロールは、少なくとも 1 件のオブジェクトが追加されたときに表示されます。
- is not: ユーザー接続が条件に一致しなかった場合に、リソースがアクセス不可の状態でなければならないことを指定します（アクセス可能を指定することも可能。Allow または Deny による）。is not をクリックして、is に変更できます。このコントロールは、少なくとも 1 件のオブジェクトが追加されたときに表示されます。

条件の左側のスイッチをクリックすることで、条件を無効化および有効化できます。

8 完了したら、[保存] をクリックします。

優先ルーティングを構成

概要

優先ルーティングは、地理的に異なる展開の Parallels RAS ユーザーが、同じ Parallels RAS ファーム/サイトに接続する場合に便利な機能です。リソースが同じ RAS ファーム/サイト内の別のデータセンターにある場合、共通のアクセスレイヤーの使用（RAS Secure Gateway、HALB、またはサードパーティのロードバランサー）は最適ではありません。この問題を解決するには、特定の公開済みリソースに対して優先的なアクセスレイヤーサーバーを設定します。この場合、ユーザーはデフォルトの Secure Gateway に接続しますが、管理者が設定した近接

ルールを使用してリダイレクトされることになります。一般的に、セッションホストに最も近接した Secure Gateway を使用することで、ユーザーエクスペリエンスの向上、内部ネットワークのトラフィックおよび関連コストの削減、リソースの有効活用が可能になります。

注: 優先ルーティングは、Azure Virtual Desktop の公開済みオブジェクトには適用されません。

優先ルーティングは次のように動作します。

1. Parallels Client は、標準的な認証を使用して Secure Gateway との接続を確立します。
2. RAS Connection Broker を通じて、リソースの優先ルート（設定されている場合）が特定されます。
3. Parallels Client は、リソースを起動するための優先パブリックアドレスを受け取ります。
4. Parallels Client はリダイレクトされたアドレスからリソースを起動しようとします。これが失敗すると元のゲートウェイにフォールバックします。

優先ルーティングを構成

優先ルーティングを構成するには、まず、サイトに対して 1 つまたは複数のカスタムパブリックサーバーアドレスを指定する必要があります。このためには、次の操作を実行します。

1. RAS 管理ポータルで [サイト設定] カテゴリーを選択します。
2. [接続] メニューから、[アドレス] を選択します。
3. プラス記号のアイコンをクリックし、開いたダイアログで、このカスタムアドレスの名前、オプションの説明、パブリックアドレス、ポート、および SSL ポート（ユーザーセッションのルーティングには SSL ポートを使用することを推奨）を指定します。

1 つまたは複数のカスタムサーバーアドレスを構成すると、以下の方法で公開済みリソースにカスタムアドレスを指定できるようになります。

1. [公開] カテゴリーを選択します。
2. 公開済みリソースを選択します。
3. 中央のペインで [ルーティング] を選択します。
4. 編集ペインで [編集] をクリックします。
5. [優先ルーティングを有効にする] オプションを選択します。
6. プラス記号のアイコンをクリックします。

7 リストから、この公開済みリソースの優先ルーティングとして使用するカスタムアドレスを選択します。

第　10　章

監視

この章の内容

概要

[監視] カテゴリーから、Parallels RAS Performance Monitor を利用できます。これは、ブラウザーベースのダッシュボードで、管理者が Parallels RAS の展開のボトルネックやリソース使用率を分析するのに使用できます。このダッシュボードではパフォーマンスメトリクスを視覚的に表示でき、Parallels RAS Console またはウェブブラウザーに表示することができます。

コンポーネント

Parallels RAS Performance Monitor は次のコンポーネントで構成されています。

- InfluxDB データベース - システムパフォーマンスデータのストレージ用データベース。
- Grafana ダッシュボード - パフォーマンスメトリクスを視覚的に表示するブラウザーベースのダッシュボード。
- Telegraf サービス - インストールされているサーバー上でパフォーマンスデータを収集するサービス。同サービスは Parallels RAS ファームにサーバーを追加し、対応する RAS Agent（RAS Secure Gateway Agent、RD セッションホスト Agent、Remote PC Agent など）をインストールすると自動的にインストールされます。

仕組み

Telegraf サービスはデフォルトで停止されており、データを収集しないようになっています。ファームの各サーバーで同サービスを起動するには、パフォーマンスモニタリング機能を構成

し、Parallels RAS Console または Parallels 管理ポータルで有効にする必要があります。有効にすると、Telegraf サービスが定義済みのパフォーマンスカウンターを一定間隔（10 秒）で収集し始めます。その後、ストレージ用の InfluxDB データベースに収集したデータを送信します。Parallels RAS 管理者がパフォーマンスメトリクスを表示するには、Parallels RAS 管理ポータルの [監視] カテゴリーを使用します。これにより、リアルタイムのパフォーマンスカウンターを視覚的に表示できます（Grafana ダッシュボードを使用）。

パフォーマンスメトリクスはタイプ（セッション、CPU、メモリ、ディスクなど）ごとにダッシュボードでグループ化されており、メトリクスの各グループを個別に表示することができます。ファームあるいはサイトの 1 つ以上の特定サーバーのパフォーマンスメトリクスを表示するか、またはすべてのサーバーのパフォーマンスメトリクスを表示するかを選択することもできます。さらに、データを表示する特定のサイトを選択することもできます。

RAS Performance Monitor をインストールする

要件

Parallels RAS Performance Monitor は、Parallels RAS の独立したコンポーネントであり、専用のインストーラーを備えています。このツールは、専用サーバーまたは Parallels RAS コンポーネントのいずれかのホストサーバーにインストールすることができます。インストーラーを実行すると、InfluxDB データベースと Grafana ダッシュボードサービスが自動的にインストールされます。詳細については、以下の「インストール」のサブセクションを参照してください。

Parallels RAS Performance Monitor をインストールしたサーバーには、以下のファイアウォールルール（開放ポート）が自動的に追加されます。

- TCP ポート 8086（InfluxDB データベースで使用）。
- TCP ポート 3000（Grafana パフォーマンスダッシュボードで使用）。

インストール

Parallels RAS Performance Monitor をインストールするには:

1 https://www.parallels.com/products/ras/download/links/ より Parallels RAS Performance Monitor のインストーラーをダウンロードします。

2 インストールウィザード（RASPerformanceMonitor.msi ファイル）を実行し、画面の指示に従って作業を進めます。

3 完了したら、ウィザードを閉じます。

RAS 管理ポータルで監視を有効にする

注: 管理ポータルで RAS Performance Monitor を有効にするには、RAS ファームのルート管理者権限が必要です。

RAS Performance Monitor を有効にするには、次の操作を実行します。

1 管理ポータルで、サイドバーの [監視] カテゴリーを選択します。

2 右ペインで、[ファーム] リンクをクリックします。これにより、[ファーム設定] カテゴリーで、[監視] サブカテゴリーが選択された状態になります。

3 トップパネルで、[編集] ボタンをクリックします。

4 [RAS Performance Monitor を有効にする] オプションを選択します。

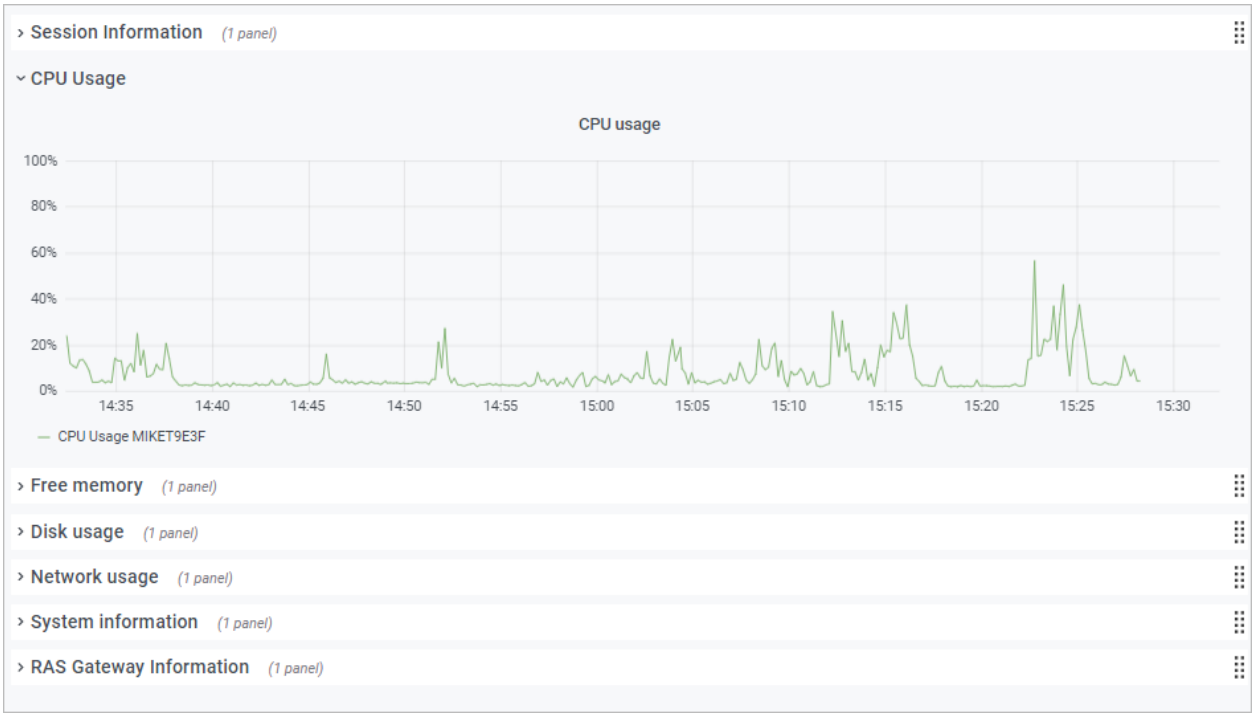
5 RAS Performance Monitor のデータベースをホストしているサーバーへの接続設定を指定する:

- サーバー: InfluxDB データベースおよび Grafana ダッシュボードがインストールされているサーバーの FQDN または IP アドレスを入力します。
- ポート: デフォルトのポートは 8086 です。これは必要に応じて変更できます。

6 [保存] をクリックします。

パフォーマンスメトリクスの表示

パフォーマンスメトリクスを表示するには、サイドバーで [監視] カテゴリーを選択します。パフォーマンスダッシュボードが右ペインに表示されます。



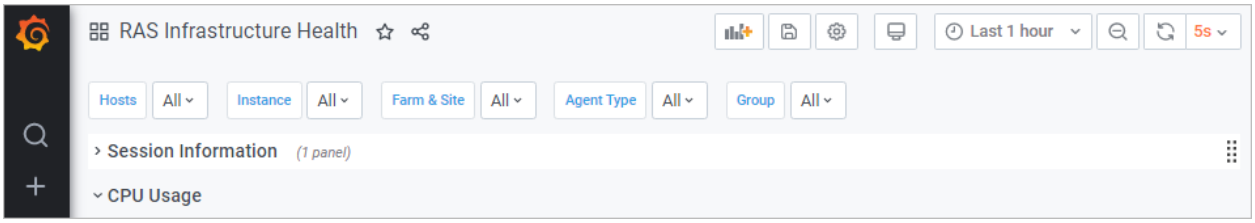
特定のタイプのメトリクスを表示するには、ダッシュボードの主要部にカテゴリーを展開します。カテゴリーには以下のものが含まれます。

- セッション情報: アクティブなセッションおよび接続していないセッションに関する情報を表示します。
- CPU 使用率: CPU カウンター。
- メモリ容量: 物理メモリのカウンター。
- ディスク使用率: ディスク入出力のカウンター。
- ネットワーク使用率: ネットワークインターフェースの出入力カウンター。
- システム情報: システム情報カウンター。
- RAS ゲートウェイ情報: RAS Gateway カウンター:

パフォーマンスメトリクスはダッシュボードにグラフ表示されます。異なるカウンターは別の色で表示されます。

グラフの特定部分にズームインするには、マウスで長方形のブロックを選択します。また、ダッシュボード上部にある [ズーム] コントロールを使って、時間範囲をズームアウトしたり、推移時間を進めたり戻したりできます。特定の時間範囲を選択するには、上部の”時計”アイコンをクリックして、時間範囲を指定します。

デフォルトでは、ダッシュボードはキオスクモードで開きます。終了するには、”ESC”キーを押します。表示モードを切り替えるには、右上の”モニター”アイコンをクリックします。キオスクモードの場合、「RAS インフラストラクチャ正常性」ページが表示されます。



上部のメニューには次の項目があります。

- ホスト: パフォーマンスメトリクスを表示するサーバーを 1 つまたは複数選択できます。サイトのすべてのサーバーデータを表示するには、[すべて] を選択します。リストにサーバーが何も表示されない場合は、Parallels RAS Performance Monitor が初回の統計データを収集するまで待つ必要があります。これは、初回のインストール時のみ起こります。
- インスタンス: 特定のカウンターのインスタンス（1 つ以上ある場合）を選択できます。ネットワークカウンターの場合、通常ネットワークインターフェース名が使われます。ディスクカウンターの場合、ディスク名になります。その他のカウンターでは通常インスタンスが複数あることはありません。
- ファームとサイト: データを表示するサイトを選択します。[すべて] を選択すると、ファームのすべてのサイトのデータを表示します。別の RAS ファームがある場合、RAS Performance Monitor が構成されていて有効なときは、そのファームからサイトを選択することもできます。
- Agent タイプ: RAS Agent タイプを選択します。
- グループ: RDS グループを選択します。

パフォーマンスメトリクスおよびその意味について詳しくは、次の Microsoft の記事を参照してください。

- https://technet.microsoft.com/en-us/library/cc976785.aspx
- https://technet.microsoft.com/en-us/library/2008.08.pulse.aspx

「RAS Performance Counters」（p. 149）も参照してください。

RAS Performance Monitor のセキュリティの構成

デフォルトでは、どのユーザーでも [Performance Monitor] ページにアクセスして、パフォーマンスメトリクスを表示できます。セキュリティの向上のため、許可されたユーザーのみが表示できるように、RAS Performance Monitor が資格情報を使用するように設定できます。

最初に、以下のように Grafana 構成ファイルから匿名認証を削除します。

1 ファイル C:\Program Files\Parallels\RAS Performance Monitor\conf\defaults.ini を開きます。

2 ファイルで次を探します。

```
################################### Anonymous Auth
######################

[auth.anonymous]

# enable anonymous access

enabled = true
```

3 "enabled = true" を "enabled = false" に変更します。

> **注:** 匿名アクセスを無効にすると、ユーザーは自動的に管理者パスワードを変更するよう促されます。これに引き続き、Grafana の公式ドキュメントに従って、パスワードを変更できます: https://grafana.com/docs/grafana/latest/manage-users/user-admin/change-your-password/。

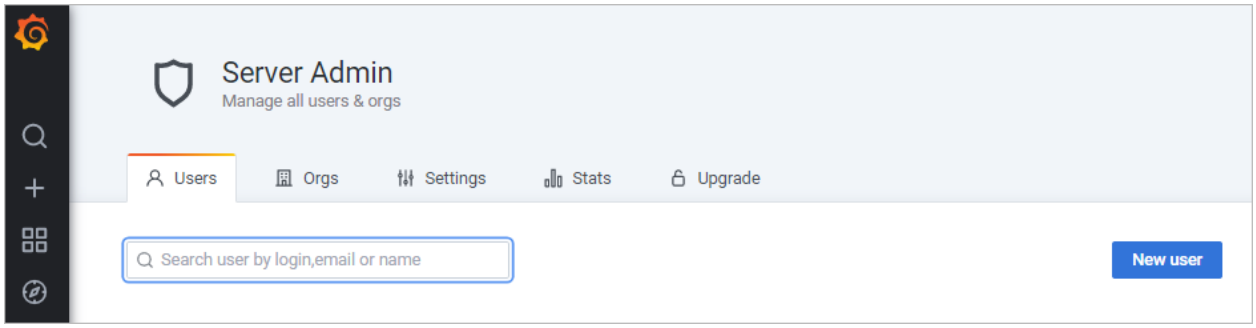
4 Grafana サービスを再起動します。

5 [モニタリング] カテゴリーを選択し、以下の認証情報を使用して Grafana にログインします。

- ユーザー: admin
- パスワード : admin（以前にパスワードを変更した場合は、現在のパスワードを使用してください）。

6 ログイン後、”Esc”キーを押し、”盾”のアイコン > [ユーザー] をクリックします。

7 [新規ユーザー] をクリックして、新しいユーザーを作成します。



8 ここで、ユーザーを組織のリストに追加する必要があります。そのためには、[ユーザー] リストで、[編集] をクリックしてユーザーを編集し、組織を設定して、ユーザーを [ビューアー] にします。

9 [追加] をクリックして、ユーザーを組織のリストに追加します。これで、ユーザーは RAS Performance Monitor 統計データを表示できます。

第 11 章

RAS Agent の更新

Parallels RAS コンポーネントをファームに追加するとき、そこに対応する RAS Agent をインストールします。これには、RAS Connection Broker、RD セッションホスト Agent、Provider Agent、Guest Agent、Remote PC Agent が含まれます。Agent のステータスを確認し、必要な場合はアップデートできる機能に加えて、一括 Agent アップデートまたはアップグレードも実行できます。

Agent をアップデートする必要があるかどうかを確認する方法は 2 つあります。Parallels RAS から通知を受け取ること、またステータスを確認してアップデート手順を手動で開始することができます。

RAS 管理ポータルを開くと、「RAS Agent の更新が必要です」というメッセージが表示される場合があります。メッセージボックスに表示されている [更新] リンクをクリックすると、更新処理が始まります。

手動で処理を開始するには、[サイト] カテゴリーを選択してすべてのエージェントを更新リンクをクリックします。画面の指示に従って、エージェントの更新またはアップグレードが必要なサーバーを選択します。なおすべてのサーバー上で全エージェントが最新である場合、すべてのエージェントを更新リンクは表示されません。

第　12　章

ヘルプとサポート

[ヘルプとサポート] カテゴリーには、質問への回答、問題の解決、ソフトウェアとマニュアルのダウンロード、Parallels サポートへの問い合わせに役立つリソースへのリンクが含まれています。

なお一部のリンクをクリックすると、サインインが必要な Parallels My Account ページに遷移します。Parallels RAS サブスクリプションをご利用のユーザーは、すでにアカウントをお持ちになっています。Parallels アカウントをお持ちでない場合は、作成する必要があります。

Parallels サポートに問い合わせるには、[サポート] セクションのリンクを使用します。

- システムレポートを Parallels に送信: 必要なデータを収集し、Parallels にシステムレポートを送信します。これは正式なサポート依頼ではないことにご注意ください。
- システムレポートをダウンロード: データを収集し、指定された場所に保存します。これは、Parallels サポート担当者がレポートの送信を要求する場合に役立ちます。
- サポートリクエストを作成: Parallels に正式なサポート依頼を送信します。詳細な環境情報を提供するシステムレポートを含めることができます。このリンクをクリックして、画面の指示に従ってリクエストを作成および送信してください。

第　13　章

付録

この章の内容

Parallels RAS の Microsoft ライセンスの要件

このセクションは、Parallels RAS 環境での Microsoft ライセンス要件を明確にするためのガイダンスとして使用されます。除外リストとしては使用することは意図されていません。詳細については、Microsoft のライセンスパートナーにお問い合わせください。

Microsoft ライセンスの要件には以下の内容が含まれます。

概要

- 使用されるいずれかの Windows Server およびデスクトップオペレーティングシステム（OS）。
- アクセスされる Windows Server OS は、Microsoft Windows Server クライアントアクセスライセンス（CAL）の対象である必要があります。

RD セッションホスト

Windows Server にリモートでアクセスする場合（管理以外の作業の場合）、リモートデスクトップサービス（RDS）のアクセス用ライセンスが必要です。

- Windows Server でリモートデスクトップサービス機能を利用するユーザーまたはデバイスには、RDS CAL が必要となります。次の種類の RDS CAL を使用できます。
  - **a** RDS デバイス CAL: 1 台のデバイス（任意のユーザーが使用）が、任意のサーバーでリモートデスクトップサービス機能を使用することを許可します。

b RDS ユーザー CAL: 1 ユーザー（任意のデバイスを使用）が、任意のサーバーでリモートデスクトップサービス機能を使用することを許可します。

c RDS 外部コネクター: 複数の外部ユーザーが、単一のリモートデスクトップサーバーにアクセスすることを許可します。複数のサーバーが存在する場合は、必須の Windows Server 外部コネクターに加えて、複数の外部コネクターが必要となります。

サーバーソフトウェアでは、RDS デバイス CAL と RDS ユーザー CAL を組み合わせて使用することもできます。この場合、RDS ユーザー CAL または RDS デバイス CAL に加えて、通常のユーザーまたはデバイス CAL が必要となります。

- RDS SAL は、コンピューティングリソースで作成された仮想マシンに対し、Microsoft リモートデスクトップサービスのサブスクライバーアクセスライセンス（「RDS SAL」と呼ばれる）を提供するサービスです。これにより、3 人以上のユーザーがコンピューティングリソース内に存在する特定の仮想マシンのリモートデスクトップ（RD セッションホスト）に接続できるようになります（SPLA パートナーの場合）。

さらに詳しく:

- 「クライアントアクセスライセンス（CAL）を使用して RDS 展開をライセンスする」: https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/rds-client-access-license。
- RDS ライセンスデータシート（ https://download.microsoft.com/download/6/B/A/6BA3215A-C8B5-4AD1-AA8E-6C93606A4CFB/Windows_Server_2012_R2_Remote_Desktop_Services_Licensing_Datasheet.pdf）。
- RDS CAL の概要と FAQ（ https://download.microsoft.com/download/3/D/4/3D42BDC2-6725-4B29-B75A-A5B04179958B/Licensing-Windows-Server-2012-R2-RDS-and-Desktop-Apps-for-RDS.pdf）。
- Windows Server RDS による Microsoft デスクトップアプリケーションソフトウェアの使用（ https://download.microsoft.com/download/3/d/4/3d42bdc2-6725-4b29-b75a-a5b04179958b/desktop_application_with_windows_server_remote_desktop_services.pdf）。

ハイパーバイザーと VDI

1 Microsoft Hyper-V をハイパーバイザーとして使用する場合は、Microsoft Windows Server オペレーティングシステム（OS）のライセンスが必要です

さらに詳しく:

- Windows Server 2022 ライセンスデータシート（https://www.microsoft.com/en-us/windows-server/pricing）。
- Windows Server 2019 ライセンスデータシート（https://download.microsoft.com/download/7/C/E/7CED6910-C7B2-4196-8C55-208EE0B427E2/Windows_Server_2019_licensing_datasheet_EN_US.pdf）。
- Windows Server 2016 ライセンスデータシート（https://download.microsoft.com/download/7/2/9/7290EA05-DC56-4BED-9400-138C5701F174/WS2016LicensingDatasheet.pdf）。

2 仮想デスクトップインフラストラクチャ（VDI）を使用する場合は、Windows ソフトウェアアシュアランスまたは Azure Virtual Desktop アクセス（VDA）ライセンスが必要です。Microsoft は、アクセスデバイスごとに Windows ライセンスを付与します。

- 仮想デスクトップのアクセス権は、Windows クライアントソフトウェアアシュアランス（SA）の利点です。SA の対象となる PC を使用するカスタマーは、追加料金なしで VDI デスクトップにアクセスできます。
- シンクライアントなど、Windows クライアント SA の対象とならないデバイスを使用する場合は、Windows VDI デスクトップにアクセスするために、それらのデバイスに Azure Virtual Desktop アクセス（VDA）のライセンスを付与する必要があります。Windows VDA は、業務委託先や従業員が所有する PC などのサードパーティデバイスにも適用できます。

さらに詳しく:

- Windows 11 ライセンスポータル（https://www.microsoft.com/en-us/Licensing/product-licensing/windows）。
- Windows 10 ライセンスポータル（https://www.microsoft.com/ja-jp/licensing/product-licensing/windows10?activetab=windows10-pivot:primaryr3）。
- 仮想マシンで Windows デスクトップオペレーティングシステムを使用するためのライセンス（https://download.microsoft.com/download/9/8/d/98d6a56c-4d79-40f4-8462-da3ecba2dc2c/licensing_windows_desktop_os_for_virtual_machines.pdf）。
- VDI 環境向け Windows デスクトップのライセンス（https://docs.microsoft.com/en-us/answers/storage/temp/12620-microsoft-vdi-and-vda-faq-v3-0.pdf）。

Microsoft Azure

Microsoft 365 や Microsoft Azure などの Microsoft Online ビジネスサービスでは、サインインのために、また ID 保護によってサポートを提供するために、Microsoft Entra ID が必要です。Microsoft Online ビジネスサービスのサブスクリプションを入手すると、すべての無料機能にアクセスできる Microsoft Entra ID が自動的に取得されます。Microsoft Entra ID の実装を強化するために、Microsoft Entra ID プレミアム P1 またはプレミアム P2 ライセンスにアップグレードして、有料機能を追加することもできます。

さらに詳しく:

- Microsoft Entra ID の実装
  https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis
- Azure ハイブリッド特典（https://azure.microsoft.com/ja-jp/pricing/hybrid-benefit/）

Azure Virtual Desktop

- 次のいずれかのユーザーライセンスをお持ちの場合、追加コスト（コンピューティング、ストレージ、およびネットワークのコストを除く）を負担することで、Windows 10 Enterprise マルチセッション、Windows 11 Enterprise マルチセッション、Windows 10 Enterprise、および Windows 11 Enterprise デスクトップ/アプリへのアクセスを利用できるようになります。
  - **a** Microsoft 365 E3/E5
  - **b** Microsoft 365 A3/A5/学生使用特典
  - **c** Microsoft 365 F3
  - **d** Microsoft 365 Business Premium
  - **e** Windows 10 Enterprise E3/E5
  - **f** Windows 10 Education A3/A5
  - **g** Windows 10 VDA（ユーザー単位）
- アクティブなソフトウェアアシュアランス（SA）が付属する、ユーザー単位またはデバイス単位の RDS CAL ライセンスをお持ちの場合、追加費用（コンピューティング、ストレージ、およびネットワークのコストを除く）を負担することで、Windows Server 2012 R2 以降を実行している Windows Server リモートデスクトップサービスを利用したデスクトップへのアクセスを利用できます。

さらに詳しく:

- Azure Virtual Desktop の価格（https://azure.microsoft.com/ja-jp/pricing/details/virtual-desktop/）

FSLogix

次のいずれかのライセンスをお持ちの場合は、FSLogix プロファイルコンテナー、Office 365 コンテナー、アプリケーションマスキング、および Java リダイレクトツールを利用できます。

- Microsoft 365 E3/E5
- Microsoft 365 A3/A5/学生使用特典
- Microsoft 365 F1/F3
- Microsoft 365 Business
- Windows 10 Enterprise E3/E5
- Windows 10 Education A3/A5
- Windows 10 VDA（ユーザー単位）
- リモートデスクトップサービス（RDS）クライアントアクセスライセンス（CAL）
- リモートデスクトップサービス（RDS）サブスクライバーアクセスライセンス（SAL）

FSLogix ソリューションは、ユーザーが適切なライセンスを保持している場合に限り、任意のパブリックまたはプライベートのデータセンターで使用できます。

さらに詳しく:

- FSLogix の概要（https://docs.microsoft.com/en-us/fslogix/overview）。

Microsoft SQL Server

Parallels RAS Reporting を使用する場合は、SQL Server が必要です。SQL Server は、以下に基づいてインストールできます。

- データベースのサイズに 10GB の制限がある無料の SQL Express。
- SQL Server 商用版の Standard または Enterprise（コアベースのライセンスまたはサーバー/CAL ベースのライセンスを使用）。

さらに詳しく:

- SQL Server 2019 ライセンスガイド（https://download.microsoft.com/download/6/6/0/66078040-86d8-4f6e-b0c5-e9919bbcb537/SQL%20Server%202019%20Licensing%20guide.pdf）

App-V

App-V は、単体でライセンスが付与されることはありませんが、他のライセンス契約（Microsoft ボリュームライセンス、Windows ソフトウェアアシュアランス、Microsoft リモートデスクトップサービス（RDS）CAL など）に含まれています。より広範な Microsoft ライセンス契約の一部となります。たとえば、RDS CAL（ユーザー単位またはデバイス単位）では、RD セッションホストで App-V クライアントを使用して、App-V アプリケーションを配信できます。

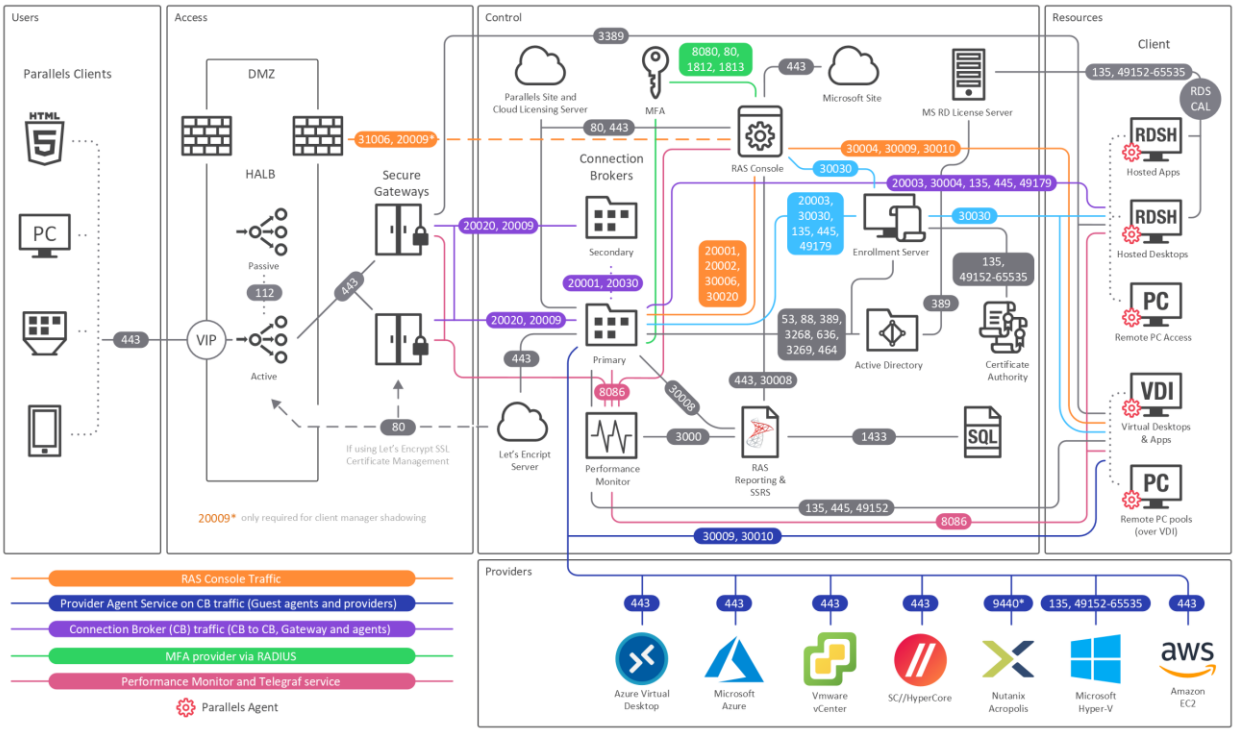
App-V のライセンスを適切に取得するには、Microsoft ボリュームライセンスに精通した Microsoft パートナー（ソリューションプロバイダー）と契約することをお勧めします（Microsoft パートナーのリスト: https://pinpoint.microsoft.com/en-us/search?type=companies&competency=100010）。

他の参照資料

Microsoft ボリュームライセンス製品に使用される用語の詳細なリストについては、https://www.microsoftvolumelicensing.com/Downloader.aspx?documenttype=PT&lang=English を参照してください。

ポート参照

次の図は、Parallels RAS で使用される通信ポートを示しています。



上の図には、RAS 登録サーバーなどの SAML SSO コンポーネントが含まれていますが、テナントブローカーは含まれていません。

ヒント: 本書の PDF 版をご覧の場合、以下のリンクをクリックすると、ウェブブラウザーで原寸大の図が表示されます: https://download.parallels.com/ras/v19/docs/en_US/Parallels-RAS-19-Administrators-Guide/index.htm#47092。

Parallels Client

ソース	宛先	プロトコル	ポート	記述

Parallels Client	HALB	TCP、UDP TCP、UDP	80、443 20009	管理およびユーザーセッション接続 ファイヤウォール経由のデバイスマネージャーのシャドーイング（間接ネットワーク接続）
	転送モードの RAS Secure Gateway	TCP、UDP TCP、UDP UDP	80、443 3389 20000	管理およびユーザーセッション接続 オプション - RDP ロードバランスが有効になっている場合、ユーザーセッションに使用されます（標準 RDP）。 Secure Gateway はブロードキャストを検索します。
	RAS Secure Gateway 通常モード	TCP、UDP TCP、UDP TCP、UDP UDP	80、443、 3389 20009 20000	管理およびユーザーセッション接続 オプション - RDP ロードバランスが有効になっている場合、ユーザーセッションに使用されます（標準 RDP）。 ファイヤウォール経由のデバイスマネージャーのシャドーイング（間接ネットワーク接続） Secure Gateway はブロードキャストを検索します
	セッションホスト（VDI、RDS、RemotePC）	TCP、UDP	3389	ダイレクトモードに限りユーザーセッション接続で使用されます。RDP 接続は常に暗号化。
	Azure Virtual Desktop サービス	TCP UDP	443 3390	Azure Virtual Desktop Gateway 接続 ShortPath モードに限りユーザーセッション接続で使用されます。
	Microsoft サイト	TCP	443	Microsoft リモートデスクトップ（MSRDC）クライアントのダウンロード
	Parallels サイト	TCP	80、443	Parallels Client のアップデートを確認してダウンロード

ウェブブラウザー

ソース	宛先	プロトコル	ポート	記述
Web ブラウザー（HTML5）、Let's	RAS ウェブ管理サービス（RAS 管理ポー	TCP	20443	管理者は RAS 環境の HTML5 ベースの管理ポータルにアクセスします。

Encrypt サービス	タル）			
	HALB	TCP	80、443	エンドユーザーは HALB 経由で Parallels RAS Web Client（通常モードの Secure Gateway）にアクセスします **注：** Let's Encrypt を使用する場合、受信リクエストに対応するためポート 80 と 443 を開けておく必要があります。
	RAS Secure Gateway	TCP	80、443	エンドユーザーは Parallels RAS Web Client（通常モードの Secure Gateway）にアクセスします **注：** Let's Encrypt を使用する場合、受信リクエストに対応するためポート 80 と 443 を開けておく必要があります。

HALB

ソース	宛先	プロトコル	ポート	記述
HALB	HALB	VRRP	112	HALB/HALB 間の通信は、アクティブな HALB に対する VIP の自動割り当てに使用されます。
	転送モードの RAS Secure Gateway	TCP、UDP	80、443	管理およびユーザーセッション接続
	ノーマルモードの RAS Secure Gateway	TCP、UDP TCP、UDP	80、443 20009	管理およびユーザーセッション接続 ファイヤウォール経由のデバイスマネージャーのシャドーイング（間接ネットワーク接続）

RAS Secure Gateway

ソース	宛先	プロトコル	ポート	記述
転送モードの RAS Secure Gateway	ノーマルモードの RAS Secure Gateway	TCP、UDP TCP、UDP	80、443 3389	管理およびユーザーセッション接続 オプション - RDP ロードバランスが有効になっている場合、ユーザーセッションに使用されます。

	RAS Performance Monitor	TCP	8086	Agent（Telegraf サービス）が収集したパフォーマンスデータを InfluxDB に送信。
ノーマルモードの RAS Secure Gateway	リモートデスクトップサービス	TCP、UDP	3389	RDP 接続。
	RAS Connection Broker	TCP TCP、UDP	20002 20009	RAS Connection Broker サービスのポート - RAS Secure Secure Gateway と RAS Console の通信（通常モードのみ）。 RAS Console が RAS Connection Broker 上で実行されている場合、ファイヤウォール経由でのデバイスマネージャーのシャドーイング（間接的なネットワーク接続）
	RAS Performance Monitor	TCP	8086	Agent（Telegraf サービス）が収集したパフォーマンスデータを InfluxDB に送信。
	localhost	TCP	20020	ユーザーポータル Web サーバー（NodeJS）の通信。

RAS Connection Broker

ソース	宛先	プロトコル	ポート	記述
RAS Connection Broker	AD DS コントローラー	TCP TCP TCP、UDP UDP	389、3268 636、3269 88 53	LDAP LDAPS Kerberos DNS
	RAS Connection Broker	TCP	20001 20030	冗長性サービス。 同じサイトで実行されている RAS Connection Broker 間の通信。
	Parallels ライセンスサーバー	TCP	443	RAS Connection Broker（ライセンスサイトのプライマリ Connection Broker）と Parallels ライセンスサーバー（https://ras.parallels.com）の通信。 注: テナントブローカー RAS Connection Broker には必要ありません（「テナントブローカー」のセクションを参照してください）。
	RAS Performance Monitor	TCP	8086	Agent（Telegraf サービス）が収集したパフォーマンスデータを InfluxDB に送

			信。
RAS RD セッションホスト Agent	TCP、UDP	30004	Connection Broker のリクエスト用サーバー。
RAS Provider Agent	TCP、UDP	30006	Provider Agent 通信ポート。
RAS Remote PC Agent	TCP、UDP	30004	Remote PC Agent の通信ポート（Agent の状態、カウンターおよびセッション情報）
2FA サーバー	TCP、UDP	8080、80 1812、1813	Deepnet/Safenet Radius
RAS 登録サーバー	TCP	30030	RAS Connection Broker が RAS 登録サーバーに接続リクエストを送信します
RAS レポート	TCP	30008	マスター RAS Connection Broker は RAS Reporting と通信を行います（SSRS として同じホストにインストール済み）。
RAS リモートインストーラーサービス	TCP	30020	リモート Agent プッシュ
RAS RD セッションホスト Agent RAS Guest Agent RAS Remote PC Agent RAS Connection Broker RAS Secure Gateway RAS 登録サーバー	TCP	135、445、49179	ソフトウェアのリモートインストール、プッシュ/引き継ぎ。
SMTP	TCP	587	Notifdispatcher は、メールボックス設定（+SSL/TLS）で指定されたポートを使用して、メールを送信するサービスです。
Let's Encrypt サービス	TCP	80、443	Let's Encrypt クライアント（プライマリ Connection Broker で利用可能）と Let's Encrypt サーバーとの間の通信。

RAS Console

ソース	宛先	プロトコル	ポート	記述
RAS Console	RAS レポート	TCP	30008	RAS Console は、RAS Reporting と通信を行うプライマリ RAS Connection Broker に接続されます（SSRS として同じホストにインストール済み）。SSRS は TCP 1433（設定で 1433 が確立されていない場合は動的ポート）経由で SQL とのやり取りを行います。
	SSRS	TCP	443	レポートの取得。
	HALB	TCP、UDP	31006	構成に使用されます。
	Parallels Client	TCP	50005	ダイレクトネットワーク接続の場合、RAS Console からシャドーイング。
	RAS RD セッションホスト Agent	UDP、TCP	30004	[Agent をチェック] タスクに使用。 コンポーネント管理に使用。
	RAS Guest Agent	TCP UDP	30009 30010	[Agent をチェック] タスクに使用。 コンポーネント管理に使用。
	RAS Remote PC Agent	UDP、TCP	30004	[Agent をチェック] タスクに使用。 コンポーネント管理に使用。
	RAS Provider Agent	UDP、TCP	30006	[Agent をチェック] タスクに使用。 コンポーネント管理に使用。
	MFA サーバー	TCP、UDP	8080、80、1812、1813	Deepnet / Safenet / Radius
	Microsoft サイト	TCP	80、443	Parallels Client のアップデートを確認してダウンロード
	Parallels サイト	TCP	80	Parallels Client のアップデートを確認してダウンロード
	RAS Performance Monitor	TCP	3000	Grafana に対する RAS ブラウザープラグイン接続。
	RAS Connection Broker	TCP	20002、20001	Connection Broker との通信と冗長化。
	RAS 登録サーバー	TCP、UDP	30030	[Agent をチェック] タスクに使用。 コンポーネント管理とトラブルシューティングに使用されます。

	WYSE ブローカー	UDP	1234（送信のみ） 68（受信のみ）	Wyse ブローカー検出要求ブロードキャストパケット（V_WYSEBCAST）。 Wyse ブローカー検出応答パケット（V_WYSETEST）。
	SMTP	TCP	587	RAS Console では、メールボックス設定（+SSL/TLS）で指定されたポートを使用してテストメールを送信できます

SSRS

ソース	宛先	プロトコル	ポート	記述
SSRS	Microsoft SQL Server	TCP	1433	RAS Console は RAS Reporting に接続されます

RAS レポート

ソース	宛先	プロトコル	ポート	記述
RAS Reporting Service	MS SQL	TCP	1433	RAS アクティビティ情報の保存
	SSRS	TCP	8085、443	レポートの列挙（カスタムレポートを含む）

RAS ウェブ管理サービス（REST/管理ポータル）

ソース	宛先	プロトコル	ポート	記述
RAS ウェブ管理サービス	RAS RD セッションホスト Agent	TCP	30004	ログの取得
	RAS Guest Agent	TCP	30010	ログの取得
	RAS Provider Agent	TCP	30006	ログの取得

	RAS Connection Broker	TCP	20002、20001、30020	GA および冗長サービスとの通信。 公開中に、インストールされているアプリケーションを参照したり、単一のファイル/フォルダーを参照したりするために使用されます。 30020 - リモート Agent プッシュ（RAS 18 より前のバージョン）
	RAS RD セッションホスト Agent RAS Guest Agent RAS Remote PC Agent RAS Connection Broker RAS Secure Gateway RAS 登録サーバー	TCP	135、445	ソフトウェアのリモートインストール、プッシュ/引き継ぎ（RAS 18 より前のバージョン）
	RAS Reporting Service	TCP	3000	管理ポータル iFrame への RAS レポートの統合

RAS PowerShell

ソース	宛先	プロトコル	ポート	記述
RAS PowerShell	RAS RD セッションホスト Agent	TCP	30004	ログの取得
	RAS Guest Agent	TCP	30010	ログの取得
	RAS Remote PC Agent	TCP	30004	ログの取得
	RAS Provider Agent	TCP	30006	ログの取得
	RAS Connection Broker	TCP	20002、20001	GA および冗長サービスとの通信。 公開中に、インストールされているアプリケーションを参照したり、単一のファイル/フォルダーを参照したりするために使用されます。

RAS Provider Agent

ソース	宛先	プロトコル	ポート	記述
RAS Provider Agent	RAS Connection Broker	TCP	20003	Connection Broker 通信ポート。
	RAS Guest Agent	TCP UDP	30010 30009	TCP はコマンドの送信に使用されます。 UDP は、初回のハンドシェイク中に使用されます。
	RAS Performance Monitor	TCP	8086	Agent（Telegraf サービス）が収集したパフォーマンスデータを InfluxDB に送信。Hyper-V のみに適用。
	Hyper-V	TCP	135、49152～65535	ホストの電源がオンになっているかどうかを確認し、エクスポート、インポート、削除、シャットダウン、再起動、またはサスペンドのコマンドを送信するために使用されます。
	Nutanix AHV（AOS）	TCP	9440	ホストの電源がオンになっているかどうかを確認し、複製、削除、シャットダウン、再起動のコマンド（RestAPI 呼び出し、PoSH、リモート ncli）を送信するために使用されます。
	VMWare	TCP	443	ホストの電源がオンになっているかどうかを確認し、複製、削除、シャットダウン、再起動、またはサスペンドのコマンドを送信するために使用されます。
	Microsoft Azure	TCP	443	ゲストの電源がオンになっているかどうかを確認し、複製、シャットダウン、再起動、のコマンドを送信するために使用されます（REST 経由）。
	Azure Virtual Desktop	TCP	443	ホストの電源がオンになっているかどうかを確認し、複製、シャットダウン、再起動、のコマンドを送信するために使用されます（REST 経由）。
	AWS	TCP	443	ホストの電源がオンになっているかどうかを確認し、複製、シャットダウン、再起動、のコマンドを送信するために使用されます（REST 経由）。

	スケーラブル	TCP	443	ホストの電源がオンになっているかどうかを確認し、複製、シャットダウン、再起動、のコマンドを送信するために使用されます（REST 経由）。
	VDI 経由の Remote PC	TCP	135、49152～65535	ホストの電源がオンになっているかどうかを確認し、シャットダウン、再起動、またはサスペンドのコマンドを送信するために使用されます。

RAS 登録サーバー

ソース	宛先	プロトコル	ポート	記述
RAS 登録サーバー	AD DS コントローラー	TCP TCP TCP、UDP UDP	389、3268 636、3269 88 53	LDAP LDAPS Kerberos DNS
	RAS Connection Broker	TCP UDP	20003 20003	同期設定とパフォーマンスカウンター。 接続リクエストを拒否
	認証局（CA）	TCP TCP	135 動的範囲 49152 - 65535	DCOM/RPC ポート

RAS RD セッションホスト Agent

ソース	宛先	プロトコル	ポート	記述
RAS RD セッションホスト Agent	RAS Connection Broker	TCP、UDP	20003	RAS Connection Broker との通信に使用されます。
	localhost	TCP	30005	内部コマンド用（memshell、プリンターリダイレクター）。
	FSlogix	TCP	443	FSlogix インストーラーをダウンロード
	RAS Performance Monitor	TCP	8086	Agent（Telegraf サービス）が収集したパフォーマンスデータを InfluxDB に送信。

	RAS 登録サーバー	TCP	30030	RAS RD セッションホスト Agent（PrlsSCDriver）が接続してログオン資格情報を取得します。

RAS Guest Agent

ソース	宛先	プロトコル	ポート	記述
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	記述
RAS Remote PC Agent	RAS Connection Broker	TCP、UDP	20003	RAS Connection Broker との通信に使用されます
	localhost	TCP	30005	内部コマンド用（memshell、プリンターリダイレクター）
	RAS Performance Monitor	TCP	8086	Agent（Telegraf サービス）が収集したパフォーマンスデータを InfluxDB に送信。
	RAS 登録サーバー	TCP、UDP	30030	RAS リモート PC（PrlsSCDriver）が接続してログオン資格情報を取得します
	FSlogix	TCP	443	FSlogix インストーラーをダウンロード

テナントブローカー

ソース	宛先	プロトコル	ポート	記述
テナント - RAS Connection Broker	テナントブローカー - RAS Connection Broker	TCP	20003	テナントブローカーを使用して、テナントの RAS Connection Broker と通信を行い、テナントブローカーに参加し、構成とステータスを同期します

Active Directory およびドメインサービスのポート

Active Directory および Active Directory ドメインサービスのポートの要件については、次の記事を参照してください。
https://technet.microsoft.com/en-us/library/dd772723%28v=ws.10%29.aspx。

Azure Virtual Desktop

Azure Virtual Desktop 用に作成した Azure 仮想マシンには、Azure 業務用クラウドの以下の URL にアクセスするための権限が必要です。

住所	送信 TCP ポート	目的	サービスタグ
*.wvd.microsoft.com	443	サービストラフィック	AzureVirtualDesktop
gcs.prod.monitoring.core.windows.net	443	Agent トラフィック	AzureCloud
production.diagnostics.monitoring.core.windows.net	443	Agent トラフィック	AzureCloud
*xt.blob.core.windows.net	443	Agent トラフィック	AzureCloud
*eh.servicebus.windows.net	443	Agent トラフィック	AzureCloud
*xt.table.core.windows.net	443	Agent トラフィック	AzureCloud
*xt.queue.core.windows.net	443	Agent トラフィック	AzureCloud
catalogartifact.azureedge.net	443	Azure マーケットプレイス	AzureCloud
kms.core.windows.net	1688	Windows アクティベーション	インターネット

mrsglobalsteus2prod.blob.core.windows.net	443	エージェントと SXS スタックのアップデート	AzureCloud
wvdportalstorageblob.blob.core.windows.net	443	Azure ポータルのサポート	AzureCloud
169.254.169.254	80	Azure Instance Metadata サービスエンドポイント	N/A
168.63.129.16	80	ホスト正常性モニタリング	N/A
https://download.parallels.com/ras/Configuration_01-20-2022.zip	443	ホストをホストプールに参加させる	AzureVirtualDesktop

次の表は、Azure の仮想マシンがアクセスできるオプション URL の一覧です。

住所	送信 TCP ポート	目的	Azure Gov
*.microsoftonline.com	443	Microsoft Online Service への認証	login.microsoftonline.us
*.events.data.microsoft.com	443	テレメトリーサービス	なし
www.msftconnecttest.com	443	OS がインターネットに接続されているかどうかを検出	なし
*.prod.do.dsp.mp.microsoft.com	443	Windows Update	なし
login.windows.net	443	Microsoft Online Services、Microsoft 365 にサインイン	login.microsoftonline.us
*.sfx.ms	443	OneDrive クライアントソフトウェアのアップデート	oneclient.sfx.ms
*.digicert.com	443	証明書の失効確認	なし
*.azure-dns.com	443	Azure DNS 解決	なし
*.azure-dns.net	443	Azure DNS 解決	なし

最新の情報については、Microsoft のウェブサイト（https://docs.microsoft.com/en-us/azure/virtual-desktop/safe-url-list#required-url-check-tool）も参照してください。

RAS Performance Counter

以下の表は、コンポーネントごとに Parallels RAS で使用できるパフォーマンスカウンターのリストです。

Parallels RAS Gateway（2XProxyGateway.exe）

ID	名称	記述
ras_gw_tot_conn	総接続数	Gateway への総接続数。
ras_gw_tot_threads	総スレッド数	Gateway で実行中の総スレッド数。
ras_gw_rpd_sess	RDP のトンネリングされたセッション	トンネリングされた RDP セッション数。
ras_gw_rpd_sess_s	RDP SSL のトンネリングされたセッション	SSL 上のトンネリングされた RDP セッション数。
ras_gw_html	HTTP 接続	トンネリングされた HTTP ソケット数
ras_gw_html_s	HTTPS 接続	トンネリングされた HTTPS ソケット数
ras_gw_html5	HTML5 接続	トンネリングされた HTTP5 ソケット数
ras_gw_html5_s	HTML5 SSL 接続	SSL 上のトンネリングされた HTTP ソケット数
ras_gw_cm	デバイスマネージャーの接続	Parallels デバイスマネージャー接続数
ras_gw_cm_s	デバイスマネージャーの SSL 接続	SSL 上の Parallels デバイスマネージャー接続数
ras_gw_wyse	Wyse 接続	Wyse 接続数
ras_gw_wyse_s	Wyse SSL 接続	SSL 上の Wyse 接続数
ras_gw_rdpudp	RDP UDP のトンネリングされたセッション	RDP UDP 接続数
ras_gw_rdpudp_s	RDP UDP DTLS のトンネリングされたセッション	DTLS 上の RDP UDP 接続数
ras_gw_cache_sock	キャッシュされたソケット	ゲートウェイと Connection Broker との間でキャッシュされたソケット数
ras_gw_idle_threads	アイドルスレッド	Gateway 上のアイドルスレッド数
ras_gw_client	クライアントの接続	Parallels Client の接続数
ras_gw_client_s	クライアントの SSL 接続	Parallels Client の SSL 経由の接続数

Parallels RAS Connection Broker（2XController.exe）

ID	名称	記述
ras_pa_avg_client_connection_time	クライアントの平均接続時間	クライアント接続時間の平均値。
ras_pa_avg_client_auth_time	ユーザー認証の平均所要時間	ユーザーの認証に要する平均時間。
ras_pa_avg_client_policy_time	ユーザーポリシーの平均取得時間	ユーザーポリシーの取得に要する平均時間。
ras_pa_avg_client_rep_time	クライアントテレメトリーの平均送信時間	クライアントテレメトリーの送信に要する平均時間。CEP で使用されます。
ras_pa_avg_client_applist_time	ユーザーの公開済みアイテム取得平均時間	ユーザーの公開済みアイテムリストの取得に要する平均時間です。
ras_pa_avg_client_appicons_time	アイコン取得平均時間	公開済みアイテムアイコンの取得に要する平均時間です。
ras_pa_avg_client_getidle_time	リクエストの起動平均時間	リクエストの起動に要する平均時間です。

Parallels RAS RDS Agent（2XAgent.exe）

ID	名称	記述
act_sess	[アクティブな RDS セッション]	アクティブな RDS セッションの数。
disc_sess	[切断済み RDS セッション]	切断済み RDS セッションの数。

索引