Parallels Remote Application Server

Azure IaaS 上での Parallels RAS 負荷分散構成ガイド

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

本書では、Parallels Remote Application Server (RAS) を Microsoft Azure の環境上に構築し、負荷分散と安全なリモート アクセスを構成するための手順を紹介します。

紹介する構成は、小規模検証を想定した最小構成です。運用環境の場合は、追加で冗長化構成やディスク容量、セキュリティ設定等を検討してください。また、シナリオの説明に設定値に関する具体的な記述がない場合、設定値は担当者の判断に委ねられます。

すべての構成手順に Azure Portal を使用しますが、当然ながら Bicep テンプレート、PowerShell、または REST API などの自動化ツールを使用して同じ構成を実現することも可能です。

想定読者

本書は、Azure IaaS 上での RAS の構成、および管理を担当するシステム管理者を対象としています。読者は Azure Portal、Azure リソースの展開、および RAS に関する基本的な知識を有していることを前提としています。

注意事項

- 本ガイドで紹介した仮想ネットワークおよび仮想サーバー等の導入に関しては自己責任での利用をお願いいたします。
- 本ガイドで示す環境構築および運用手順の実行に関しては、所属する組織等のセキュリティ ポリシーに必ず従ってください。
- 本ガイドに記載されている画面例、URL 等はガイド記載時のものとなるため、画面仕様が実際の画面とは異なることがありますのでご注意ください。
- 本ガイドに記載されている内容は、改善のため予告なしに変更される場合があります。あらかじめご了承下さい。
- 評価の際は、是非、インストール メディアのバージョンを含め、本ガイドの最新バージョンをご使用されることを推奨いたします。

適用範囲

本ガイドは、以下バージョンを対象としています。

- RAS Ver. 20

表記規則

本ガイド内の表記は、以下の規則に沿って行われています。

- UI 上に表示されるメニュー名/タブ名/プロパティ項目名/値/ボタン名は、[　] で囲んで表記しています。
- 可変の値は <　> で囲んで表記しています。

第 2 章

概要

本書では、Azure の負荷分散サービスである、「Azure Load Balancer」「Azure Application Gateway」と、セキュリティ強化のための「Azure Firewall」を使用して、RAS ユーザー ポータルへの HTTPS トラフィックおよび RAS Secure Gateway への TCP/UDP トラフィックの負荷分散を有効にします。

以下の Azure サービスを利用し、セキュアかつスケーラブルな構成を実現します。

- Azure Firewall : 外部・内部通信のセキュリティ制御
- Azure Application Gateway : RAS ユーザーポータルへの HTTPS トラフィックの負荷分散
- Azure Load Balancer : RAS Secure Gateway への TCP/UDP トラフィックの負荷分散

本書で説明する構成を使用することで、以下のシナリオで RAS トラフィックの負荷分散が可能となります。

- **ブラウザ アクセス** : ユーザーは Web ブラウザから Parallels ユーザー ポータルにログインし、組み込みの Web クライアント (HTML5) を使用して Parallels の仮想アプリや仮想デスクトップを起動します。
- **インストール済み Parallels Client アクセス** : ユーザーは、エンドポイント デバイスにインストールされたプラットフォーム専用の Parallels Client を使用してログインし、Parallels Client アプリ、デスクトップ ショートカット、またはスタート メニューを通じて、Parallels の仮想アプリと仮想デスクトップを直接起動します。
- **ブラウザとインストール済み Parallels Client の混合アクセス** : ユーザーは Web ブラウザから Parallels ユーザー ポータルにログインし、エンドポイント デバイスにインストールされたプラットフォーム専用の Parallels Client を使用して、Parallels の仮想アプリと仮想デスクトップを起動します。

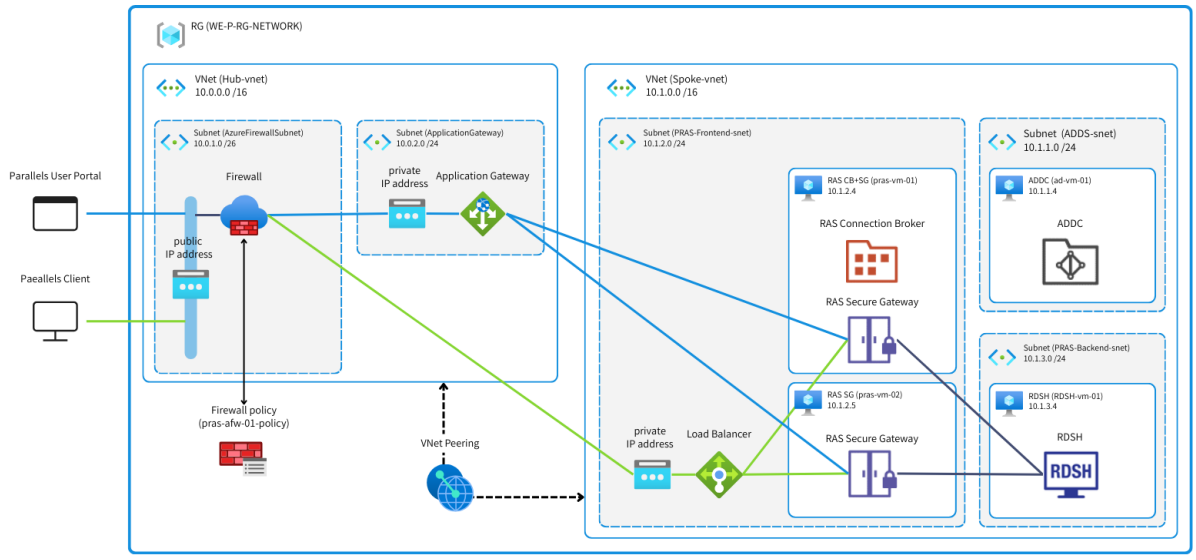
この章の内容

ネットワーク構成

本書では、Microsoft 推奨のハブ&スポーク構成を採用します。この構成では、「ハブ (中心) 」となる仮想ネットワーク (Hub VNet) に、共通サービスを配置し、スポーク間の中継点とします。接続する「スポーク (枝) 」仮想ネットワーク (Spoke VNet) には、ワークロードを用途ごとに分離して配置します。

- Hub VNet : Azure Firewall、Application Gateway を配置
- Spoke VNet : AD、公開リソース (RDSH) 、RAS サーバー群を配置

外部ユーザーへ安全に公開する必要があるが、コストや運用負荷を抑えるため WAF や VPN Gateway を利用せず、Azure Firewall のみを公開点とするシンプルな構成です。



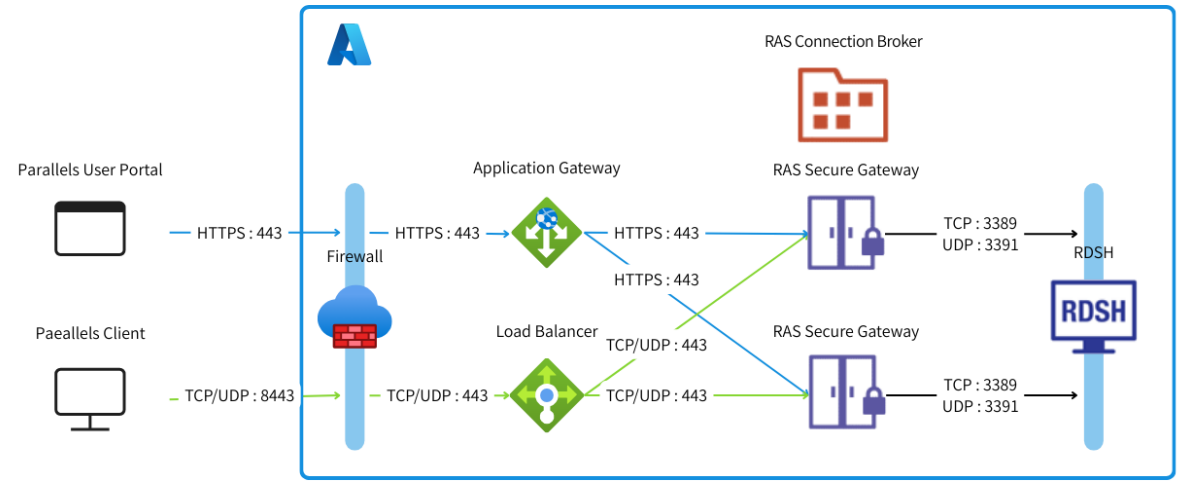
通信フロー

初めに、クライアントからの受信トラフィックは Azure Firewall のパブリック IP アドレスに到達します。

次に、Azure Firewall policy の DNAT 規則により、TCP ポート 443 のトラフィックは Azure Application Gateway に転送されます。TCP/UDP ポート 8443 のトラフィックは Azure Load Balancer に転送されます。

Azure Application Gateway では、受け取った TCP ポート 443 トラフィックを復号化して、ルーティング規則を適用後に再暗号化し、バックエンド プールの各インスタンスへ分散し、RAS ユーザーポータルへのアクセスを提供します。これらの End-to-End TLS 処理には、証明書が必要です。

Azure Load Balancer では、受け取った TCP/UDP ポート 443 トラフィックを、負荷分散規則に従ってバックエンド プールの各インスタンスへ分散し、RAS Secure Gateway へのアクセスを提供します。



前提条件

本書のシナリオを展開するためには、いくつかの要件と権限を整える必要があります。

- Azure サブスクリプションに対する [管理者] または [共同作成者] の権限を持つ Azure アカウント
- 有効な Parallels RAS のライセンス
- RDP または SSH 接続が可能なクライアント PC
- RAS サーバーへの接続に使用する適当なドメイン

第 3 章

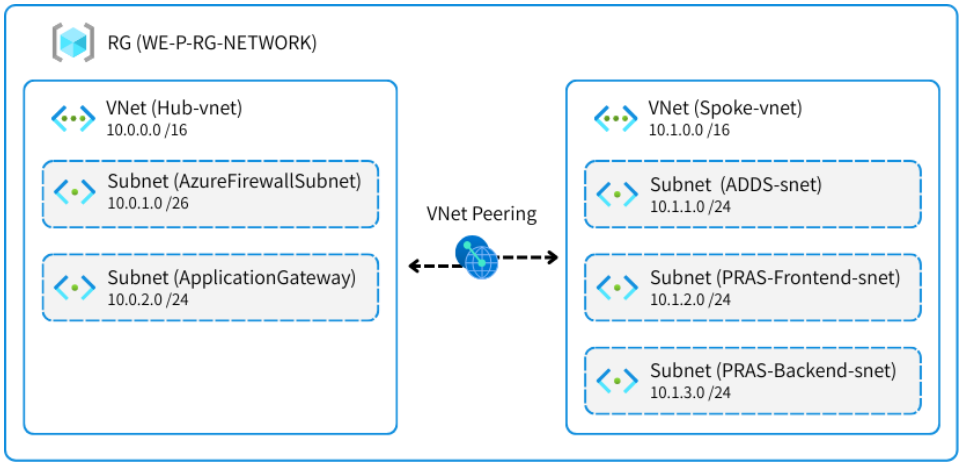
基盤構築

Azure 上でリソースをデプロイするために必要なネットワーク基盤を作成します。

この章の内容

ネットワークの構築

本書の環境をデプロイするために必要なリソースを含めるリソース グループを作成します。その後、仮想ネットワーク (VNet) 、サブネットを作成します。



- リソース グループ : Azure に関連するリソースを保持するコンテナー
- 仮想ネットワーク (Vnet) : Azure 内に作成される仮想的なネットワーク
- VNet ピアリング : 異なる VNet 同士を相互接続する機能
- サブネット : VNet を小さな単位に分けたもので、用途ごとにリソースを整理可能

リソース グループの作成

所要時間: 5 分

リソース グループ (RG) を新規作成します。

詳細なリソース グループの仕様に関しては、以下の Microsoft ガイドをご参照ください。
https://learn.microsoft.com/ja-jp/azure/azure-resource-manager/management/manage-resource-groups-portal#what-is-a-resource-group

この節では、以下のリソースを作成します。

項目	設定値 (例)
リソース グループ	QA-rg-01

リソース グループの作成方法は、以下の通りです。

1 Azure portal (https://portal.azure.com) にアクセスし、[リソース グループ] に遷移します。

2 [+作成] をクリックします。

3 [基本] タブで、以下の情報を設定します。設定後、[レビューと作成] をクリックします。

項目	設定値	例
サブスクリプション *	<Azure サブスクリプションを選択>	Azure サブスクリプション
リソース グループ名 *	<新しいリソース グループの名前を入力>	QA-rg-01
リージョン *	<物理的な距離の近いリージョンを選択>	Japan East

4 [レビューと作成] タブで、内容を確認後、[作成] をクリックします。

5 リソース グループの作成が完了すると、リソース グループの一覧が表示されます。[最新の情報に更新] をクリックし、一覧に作成されたリソース グループが表示されることを確認してください。

6 これでリソース グループの作成は完了です。

仮想ネットワークの作成

所要時間: 5 分

仮想ネットワーク (VNet) を新規作成します。

> 詳細な仮想ネットワークの仕様に関しては、以下の Microsoft ガイドをご参照ください。
> https://learn.microsoft.com/ja-jp/azure/virtual-network/

この節では、以下のリソースを作成します。

項目	設定値 (例)
Hub 用 VNet	Hub-vnet (10.0.0.0 /16)
Spoke 用 VNet	Spoke-vNet (10.1.0.0 /16)

Hub 用 VNet

VNet の作成方法は、以下の通りです。

1 Azure portal にて、[仮想ネットワーク] に遷移します。

2 [+作成] を選択します。

3 [基本] タブで、以下の情報を設定します。[レビューと作成] をクリックします。

項目	設定値	例
プロジェクトの詳細		
サブスクリプション *	<Azure サブスクリプションを選択>	Azure サブスクリプション
リソース グループ *	<作成したリソース グループを選択>	QA-rg-01
インスタンスの詳細		
仮想ネットワーク名 *	<新しい VNet の名前を入力>	Hub-vnet
リージョン *	<リソース グループと同一のリージョンを選択>	Japan East

4 [セキュリティ] [IP アドレス] [タグ] タブの値は、既定値のまま変更なしです。

5 [レビューと作成] タブで、内容を確認後、[作成] をクリックします。

6 デプロイ画面に遷移します。デプロイまで待ちます。(30 秒程度)

7 「デプロイが完了しました」と表示されれば、VNet の作成は完了です。

Spoke 用 VNet

「Hub 用 VNet」の手順を繰り返し、Spoke 用 VNet を構築します。設定内容で「Hub 用 VNet」と異なる点は、「仮想ネットワーク名」と「IPv4 アドレス空間」です。

1 VNet 作成画面に遷移し、[基本] タブで、以下の情報を設定します。設定後、[次へ] をクリックします。

項目	設定値	例
インスタンスの詳細		
仮想ネットワーク名 *	<新しい VNet の名前を入力>	Spoke-vnet

2 [セキュリティ] タブの値は、既定値のまま変更なしです。[次へ] をクリックします。

3 [IP アドレス] タブの値は、構成したいネットワーク設計に合わせて値を変更してください。設定後、[レビューと作成] をクリックします。

項目	設定値	例
IPv4 アドレス空間	< VNet で利用するアドレス範囲を入力>	10.1.0.0 /16

4 [レビューと作成] タブで、内容を確認後、[作成] をクリックします。

5 「デプロイが完了しました」と表示されれば、VNet の作成は完了です。

6 [仮想ネットワーク] の一覧にて、[更新] を選択し、一覧に新しく作成された VNet が表示されることを確認してください。

VNet ピアリングの設定

所要時間: 5 分

標準の状態では、異なる VNet に属するリソース間の通信はできません。VNet 同士を接続する方法として、VNet ピアリングを設定することで、プライベート IP アドレスを用いた VNet 間の直接通信が可能になります。

> 詳細な VNet ピアリングの仕様に関しては、以下の Microsoft ガイドをご参照ください。
> https://learn.microsoft.com/ja-jp/azure/virtual-network/virtual-network-peering-overview

この節では、以下を構成します。

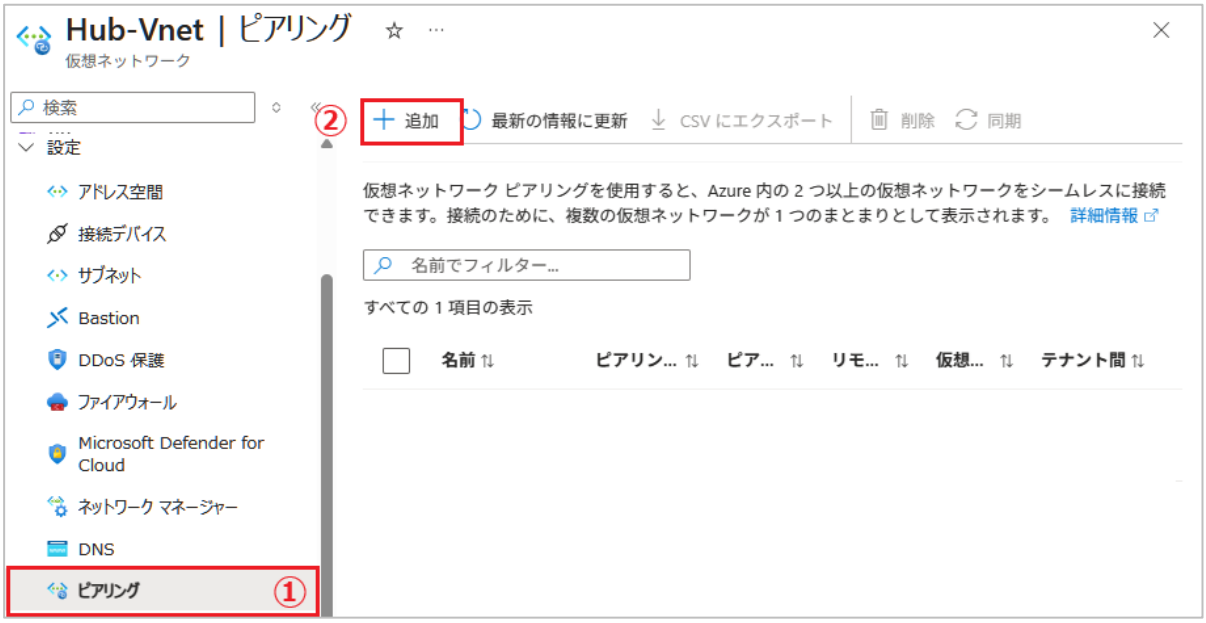
項目	設定値 (例)
ローカル VNet からのピアリング	spoke-hub-peer
リモート VNet からのピアリング	hub-spoke-peer

VNet ピアリングの作成方法は、以下の通りです。

1 Azure portal にて、[仮想ネットワーク] に遷移します。

2 ピアリングを追加する VNet をクリックします。(例では、[Hub-vnet] を選択)

3 左側のナビゲーションから [設定] > [ピアリング] の順にクリックします。[+追加] を選択します。



4 以下の情報を設定します。設定後、[追加] をクリックします。

項目	設定値	例
リモート仮想ネットワークの概要		
ピアリング リンクの名前 *	<ローカル VNet からのピアリングの名前を入力>	spoke-hub-peer
仮想ネットワークのデプロイ モデル	Resource Manager	Resource Manager
サブスクリプション *	<Azure サブスクリプションを選択>	Azure サブスクリプション
仮想ネットワーク *	<VNet を選択>	Spoke-vnet
リモート仮想ネットワーク ピアリングの設定		

'Spoke-vnet' に 'Hub-Vnet' へのアクセスを許可する	☑ 有効	☑ 有効
ローカル仮想ネットワークの概要		
ピアリング リンクの名前 *	<リモート VNet からのピアリングの名前を入力>	hub-spoke-peer
ローカル仮想ネットワーク ピアリングの設定		
'Hub-Vnet' に 'Spoke-vnet' へのアクセスを許可する	☑ 有効	☑ 有効

5 VNet 間でピアリング接続が許可されていることを確認します。

各 VNet の [ピアリング] 画面にて、新しく作成されたピアリングの状態が [接続済み] であることを確認してください。

6 これで VNet ピアリングの作成は完了です。

サブネットの作成

所要時間: 15 分

サブネットを新規作成します。

> 詳細なサブネットの仕様に関しては、以下の Microsoft ガイドをご参照ください。
> https://learn.microsoft.com/ja-jp/azure/virtual-network/virtual-network-manage-subnet?tabs=azure-portal

この節では、以下のリソースを作成します。

項目	設定値 (例)

Azure Firewall 用サブネット	AzureFirewallSubnet (10.0.1.0 /26)
Azure Application Gateway 用サブネット	AppGatewaySubnet (10.0.2.0 /24)
アプリケーション用サブネット 1	ADDS-snet (10.1.1.0 /24)
アプリケーション用サブネット 2	PRAS-Frontend-snet (10.1.2.0 /24)
アプリケーション用サブネット 3	PRAS-Backend-snet (10.1.3.0 /24)

Azure Firewall 用サブネットの作成

Azure Firewall が稼働するため専用に設計されたサブネット「AzureFirewallSubnet」を作成します。

注 : Azure Firewal は、必ず専用サブネットに配置する必要があります。

サブネットの作成方法は、以下の通りです。

1 Azure portal にて、[仮想ネットワーク] に遷移します。

2 Azure Firewall を展開する VNet をクリックします。(例では、[Hub-vnet] を選択)

3 左側のナビゲーションから [設定] > [サブネット] の順にクリックし、[+サブネット] を選択します。

4　以下の情報を設定します。設定後、[追加] をクリックします。

項目	設定値	例
サブネットの目的	Azure Firewall	Azure Firewall
名前 *	AzureFirewallSubnet	<自動>
IPv4		
IPv4 アドレスの範囲	<任意>	10.0.1.0 /16
開始アドレス *	<任意>	10.0.1.0
サイズ	/26	<自動> *1

*1：このサブネットのサイズは最低でも**/26（64 個の IP アドレス）が必要です。

5　これで Azure Firewall 専用のサブネットの作成は完了です。

Azure Application Gateway 用サブネットの作成

Azure Application Gateway 専用のサブネットを作成します。

> 注：Azure Application Gateway が所属するサブネットは、Azure Application Gateway のみ所属させなくてはなりません。

1　[仮想ネットワーク] にて、Azure Application Gateway を展開する VNet をクリックします。(例では、[Hub-vnet] を選択)

2 左側のナビゲーションから [設定] > [サブネット] の順にクリックし、[+サブネット] を選択します。

3 以下の情報を設定します。設定後、[追加] をクリックします。

項目	設定値	例
サブネットの目的	Defalt	Defalt
名前 *	<新しいサブネットの名前を入力>	ApplicationGateway
IPv4		
IPv4 アドレスの範囲	<任意>	10.0.2.0 /24
開始アドレス *	<任意>	10.0.2.0
サイズ	/24	/24 *2

*2 : Microsoft では、Application Gateway 用サブネットの最小サイズとして /24 が推奨されています。

4 [サブネット] の一覧にて、[最新の情報に更新] を選択し、一覧に新しく作成されたサブネットが表示されることを確認してください。

5 これで Azure Application Gateway 専用のサブネットの作成は完了です。

RAS システム用サブネット

RAS コンポーネントおよび公開用リソース、Active Directory 用の VM を配置するためのサブネットを作成します。

「Azure Application Gateway 用サブネットの作成」の手順を繰り返し、アプリケーション用サブネットを構築します。設定内容で「Azure Application Gateway 用サブネットの作成」と異なる点は、「名前」「IPv4 アドレスの範囲」「開始アドレス」です。

1 [仮想ネットワーク] にて、RAS 関連の VM を展開する VNet をクリックします。(例では、[Spoke-vnet] を選択)

2 左側のナビゲーションから [設定] > [サブネット] の順にクリックし、[+サブネット] を選択します。

3 以下の情報を設定します。設定後、[追加] をクリックします。

	サブネット 3 の値	サブネット 4 の値	サブネット 5 の値
サブネットの目的	Defalt	Defalt	Defalt
名前 *	ADDS-snet	PRAS-Frontend-snet	PRAS-Backend-snet
IPv4			
IPv4 アドレスの範囲	10.1.0.0/16	10.1.0.0/16	10.1.0.0/16
開始アドレス *	10.1.1.0	10.1.2.0	10.1.3.0
サイズ	/24	/24	/24

4 [サブネット] の一覧にて、[最新の情報に更新] を選択し、一覧に新しく作成されたサブネットが表示されることを確認してください。

5 これでサブネットの作成は完了です。

仮想マシンの構築

所要時間: 60 分

仮想マシン (VM) を新規作成します。

> 詳細な仮想マシンの仕様に関しては、以下の Microsoft ガイドをご参照ください。
>
> https://learn.microsoft.com/ja-jp/azure/virtual-machines/

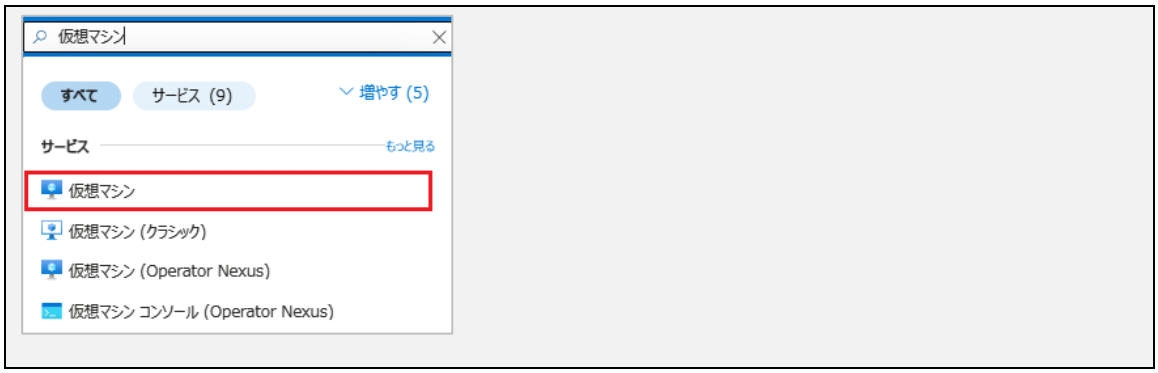
この節では、以下のリソースを作成します。

項目	設定値 (例)
ADDC 用サーバー	ad-vm-01 (10.1.1..4)
RAS CB+SG 用サーバー	pras-vm-01 (10.1.2.4)
RAS SG 用サーバー	pras-vm-02 (10.1.2.5)
RDSH 用サーバー	RDSH-vm-01 (10.1.3.4)

VM の作成方法は、以下の通りです。

1 Azure portal にて、[仮想マシン] に遷移します。

> 注 ： 似たような名前のリソースがありますので、別のリソースを選択しないように注意して下さい。



2 [+作成] > [仮想マシン] の順にクリックします。

3 [仮想マシンの作成] 画面が表示されます。[基本] タブで、以下の情報を設定します。

項目	設定値	例
プロジェクトの詳細		
サブスクリプション *	<Azure サブスクリプションを選択>	Azure サブスクリプション
リソース グループ *	<作成したリソース グループを選択>	QA-rg-01
インスタンスの詳細		
仮想マシン名 *	<新しい VM の名前を入力> *1	**ad-vm-01**
リージョン *	<VNet と同一のリージョンを選択>	Japan East
可用性オプション	<任意> *2	インフラストラクチャ冗長は必要ありません

*1 : 仮想マシン名は、15 文字以上を入力可能ですが、作成された Windows のコンピューター名には、先頭から 15 文字までしか採用されません。

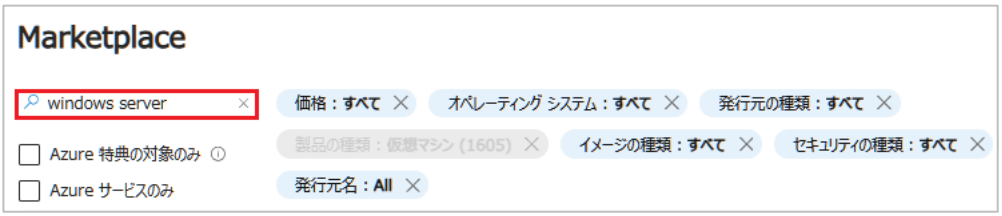
*2 : 本番運用の場合は、冗長構成を組むことが推奨されます。

4 [イメージ] を指定します。

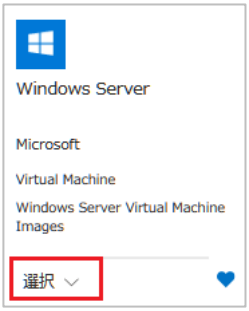
項目	設定値	例
イメージ *	<Windows server OS を選択>	[smalldesk] Windows server 2025

4.1 [すべてのイメージを表示] を選択し、Marketplace の画面に遷移します。

4.2 検索窓に「Windows Server」と入力し検索します。



4.3 表示されるイメージの中から「Windows Server」を見つけて、[選択] をクリックします。



4.4 Windows Server イメージの一覧から、Windows server OS を選択します。

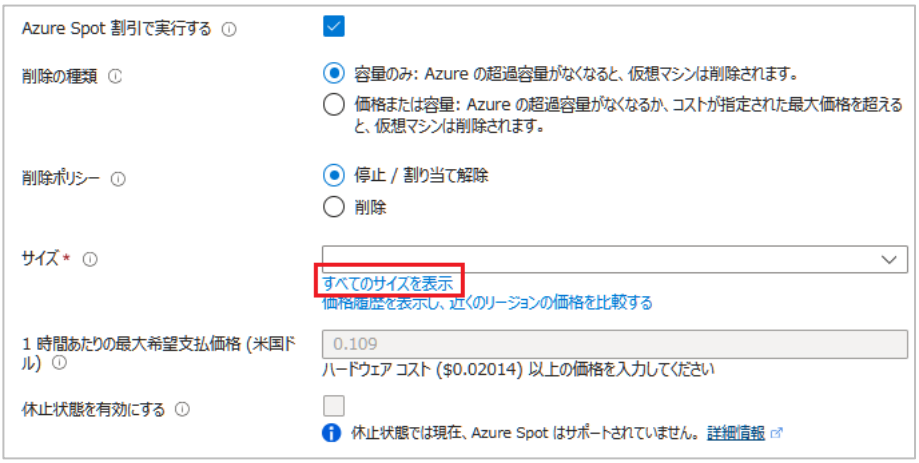
> 注 ： 例では、smalldisk プランを選択しています。これは、OS ディスクサイズが標準の 127 GB よりも小さな 30GB のイメージです。OS ディスクのストレージ料金を節約するのに効果があります。ディスクサイズは、VM デプロイ後にも拡張可能です。

5 [サイズ] を指定します。

項目	設定値	例
Azure Spot 割引で実行する	<任意> *3	☑ 有効
サイズ *	<任意>	Standard_D2

*3 : Azure Spot VM は、Azure 内の余剰リソースを使用することで、割引き価格で VM を利用することが出来る仕組みです。余剰がなくなると VM が強制的に停止されます。

5.1 [すべてのサイズを表示] を選択し、VM サイズの選択画面に遷移します。



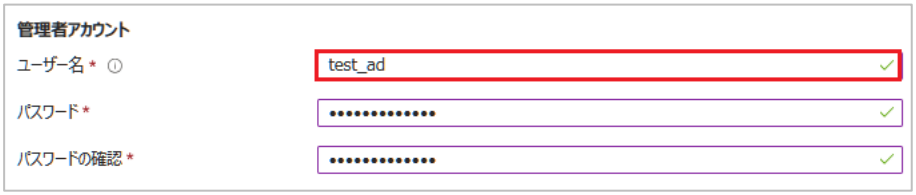
5.2 サイズの一覧から、要件に合うサイズを選択します。

> 注 : AD 用 VM の推奨サイズは、vCPU 2 コア以上、メモリ 4 GB 以上、ディスク 32 GB 以上 (OS 用) ＋ データディスク 10 GB 以上です。
> RAS 用 VM の推奨サイズは、vCPU 2 コア以上、メモリ 8 GB 以上、ディスク 32 GB 以上(OS 用) ＋ データディスク 16 GB 以上です。

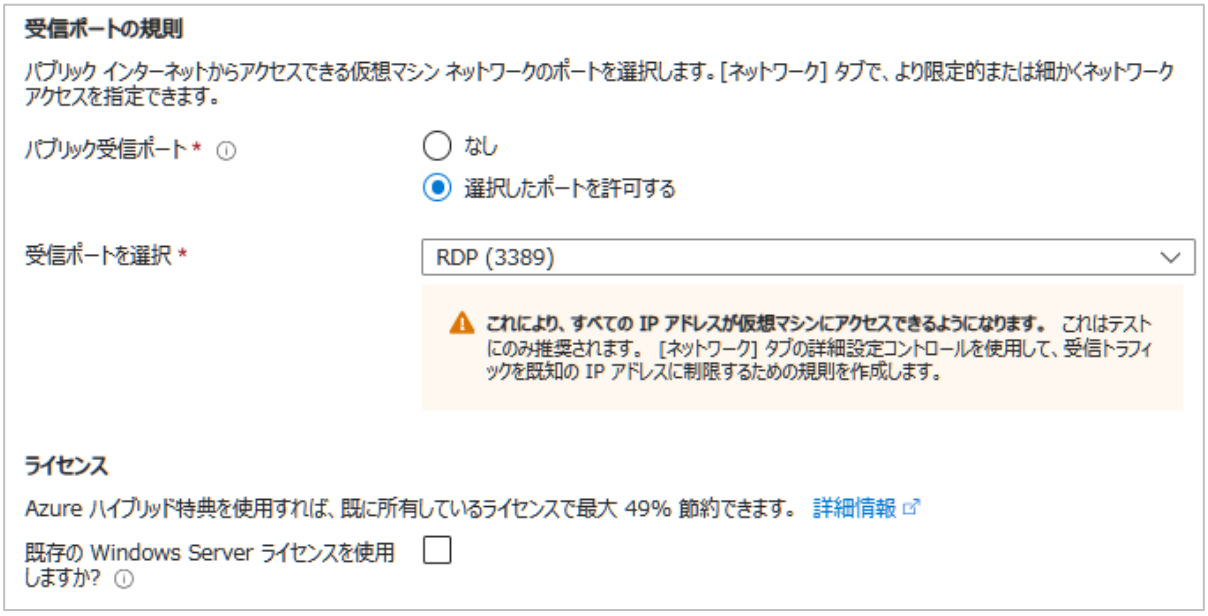
6 [管理者アカウント] を設定します。

項目	設定値	例
ユーザー名 *	<新しいユーザー名を入力>	test_ad
パスワード *	<新しいパスワードを入力> *4	

*4 : パスワードは 12 文字以上で、定義された複雑さの要件を満たす必要があります。

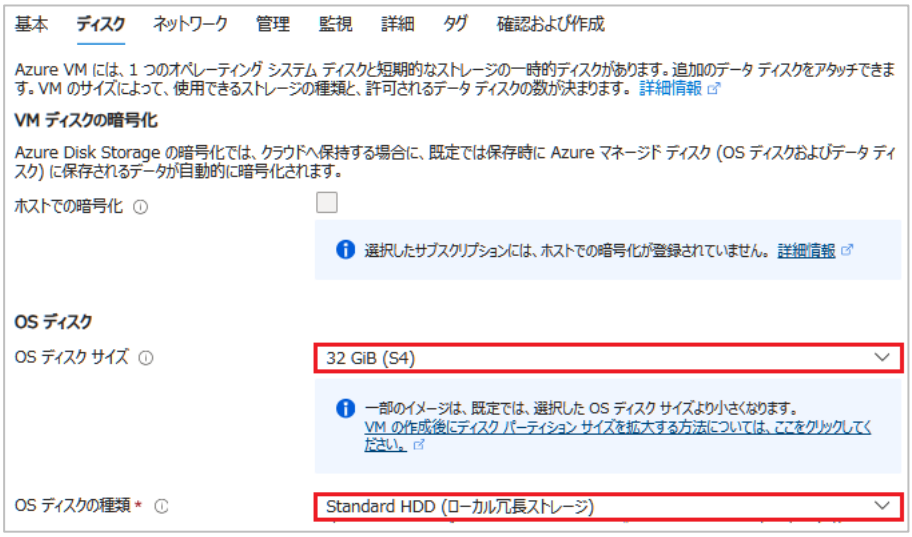


7 [受信ポートの規則] は、既定値から変更する必要はありません。設定後、[次: ディスク >] をクリックします。



8 [ディスク] タブで、以下の情報を設定します。設定後、[次: ネットワーク >] をクリックします。

項目	設定値	例
OS ディスク		
OS ディスク サイズ	<任意>	32 GiB (S4)
OS ディスクの種類 *	<任意>	Standard HDD



9 [ネットワーク] タブで、以下の情報を設定します。設定後、[確認および作成] をクリックします。

項目	設定値	例
ネットワーク インターフェイス		
仮想ネットワーク *	<作成した Spoke 用 VNet を選択>	Spoke-vnet
サブネット *	<作成したサブネットを選択>	**ADDS-snet**
VM が削除されたときに NIC を削除する	<任意>	☑ 有効

10 [確認および作成] タブで、内容を確認後、[作成] をクリックします。

11 デプロイ画面に遷移します。デプロイまで待ちます。(2 分程度)

12 「デプロイが完了しました。」と表示されましたら、[リソースに移動] をクリックし、作成された VM の情報を確認してください。

13 これで 1 台分の VM の作成は完了です。

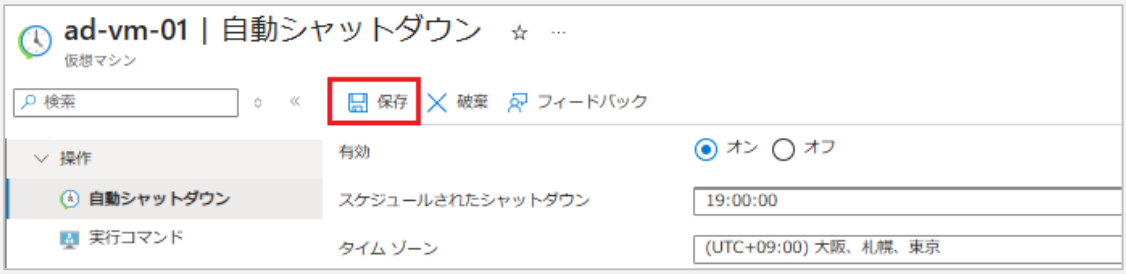
14 手順を繰り返し、VM を 3 台追加で構築します。設定内容で異なる点は、「仮想マシン名」と「サブネット」です。

	RAS CB+SG 用 VM の値	RAS SG 用 VM の値	RDSH 用 VM の値
仮想マシン名	pras-vm-01	pras-vm-02	rdsh-vm-01
サブネット	PRAS-Frontend-snet	PRAS-Frontend-snet	PRAS-Backend-snet

15 [仮想マシン] の一覧にて、[最新の情報に更新] を選択し、一覧に新しく作成された VM が表示されることを確認してください。

16 これで VM の作成は完了です。

補足：[自動シャットダウン] をオンにすることで、停止忘れによる余計な課金が発生するのを防ぐことができます。各 VNet 画面の左側のナビゲーションの [設定] > [自動シャットダウン] にて設定いただけます。



第 4 章

VM 構成

VM 上にそれぞれの機能ごとの設定を行います。

> 補足 ：Windows Server の日本語化を行う場合は、「付録」の「Windows の日本語化」をご確認ください。

この章の内容

Active Directory 構築

所要時間: 60 分

Azure VM 上に Active Directory (AD) を新規作成します。

> 注 ： 本番環境では、複数の ADDC を Azure の冗長化構成 (可用性ゾーンや可用性セット) で配置してください。2 台以上の構成で ADDC のシャットダウンが必要な場合、Azure Portal 上で VM の [停止(割り当て解除)] を実行することは非推奨です。

ディスクの追加

ADDS のデータ保存用のディスクを追加します。

ADDS のデータを配置するディスクは、ディスク キャッシュを無効化しておく事が推奨されます。Azure では、C ドライブのディスク キャッシュを無効化できないため、別途ディスク キャッシュを無効にしたデータ ディスクを追加する必要があります。

ディスクの追加方法は、以下の通りです。

1 [仮想マシン] の一覧にて、作成した AD 用 VM をクリックします。

2 左側のナビゲーションから [設定] > [ディスク] の順にクリックします。

3 [+新しいディスクを作成し接続する] をクリックし、以下の情報を設定します。設定後、[適用] をクリックします。

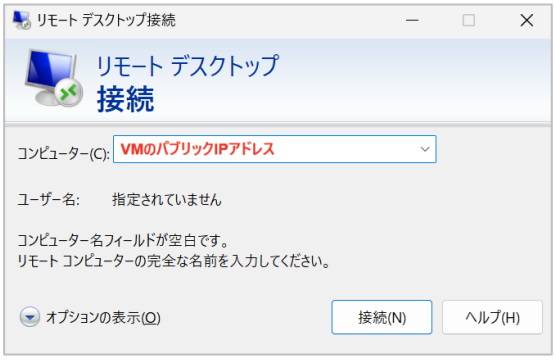
項目	設定値	例
ディスク名	<新しいディスク名を入力>	ad-vm-01-datadisk_0
ストレージの種類	<任意>	Standard HDD
サイズ (GiB)	<任意>	32
暗号化	<任意>	プラットフォーム マネージド キー
ホスト キャッシュ	なし	なし

4 [最新の情報に更新] を選択し、一覧に新しく作成されたディスクが表示されることを確認してください。

5 続いて、追加したディスクを有効化します。ここからは、Windows OS 側で操作します。

6 AD 用 VM へリモート デスクトップ (RDP) 接続します。

コンピューター	<VM のパブリック IP アドレス>

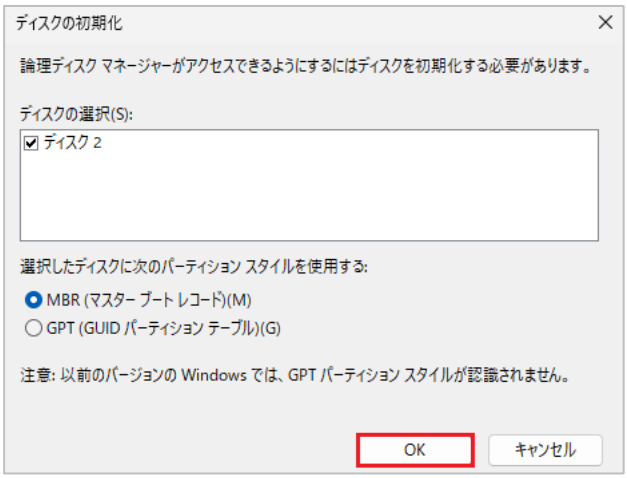


※ [VM のパブリック IP アドレス] は、VM の概要画面から確認できます。

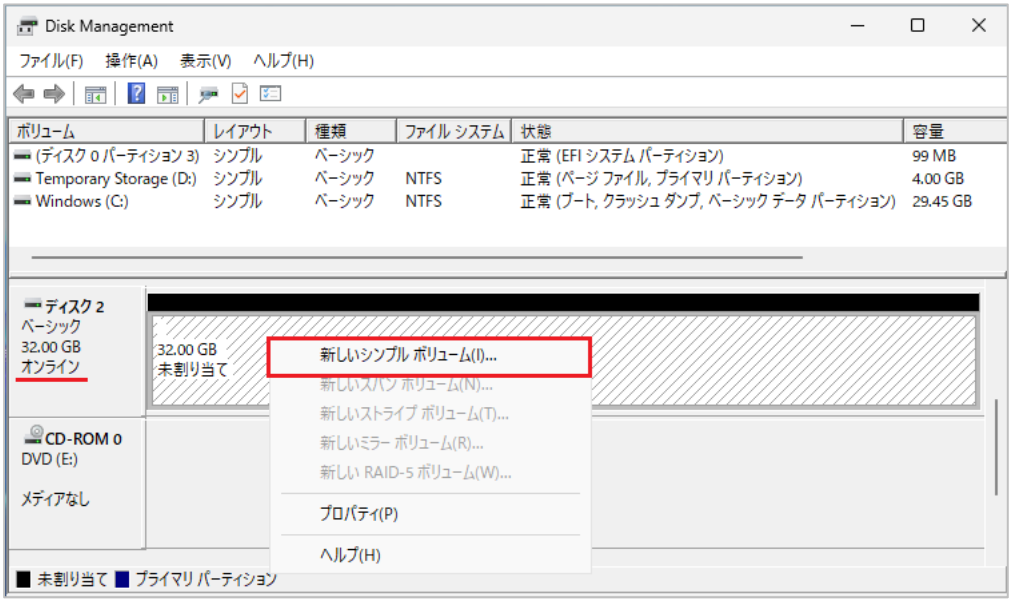
7 [資格情報] には、VM 作成時に設定した「管理者アカウント」情報を入力します。

8 サインイン後、[スタート] アイコンを右クリックして、[ディスクの管理] をクリックします。

9 「ディスクの初期化」ダイアログが表示されるので、[OK] をクリックします。

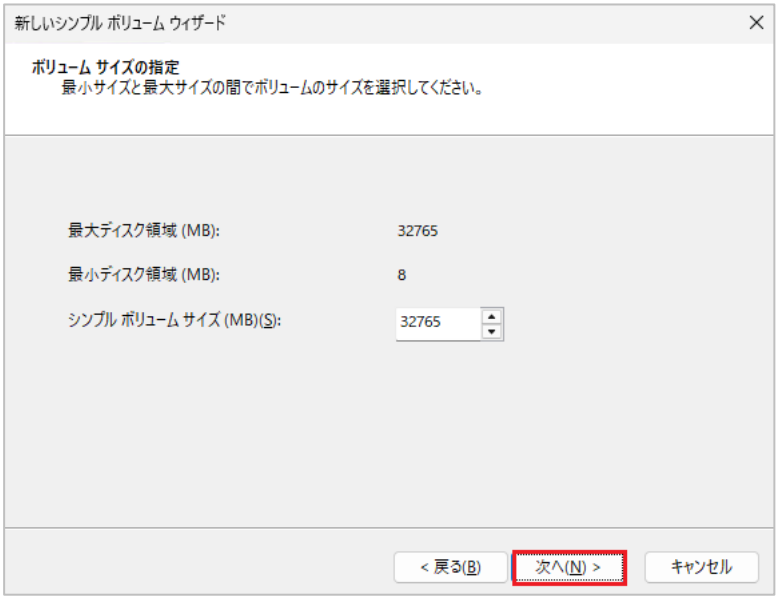


10 ディスクのステータスが「オンライン」であることを確認します。未割当のディスクを右クリックし、[新しいシンプル ボリューム] を選択します。

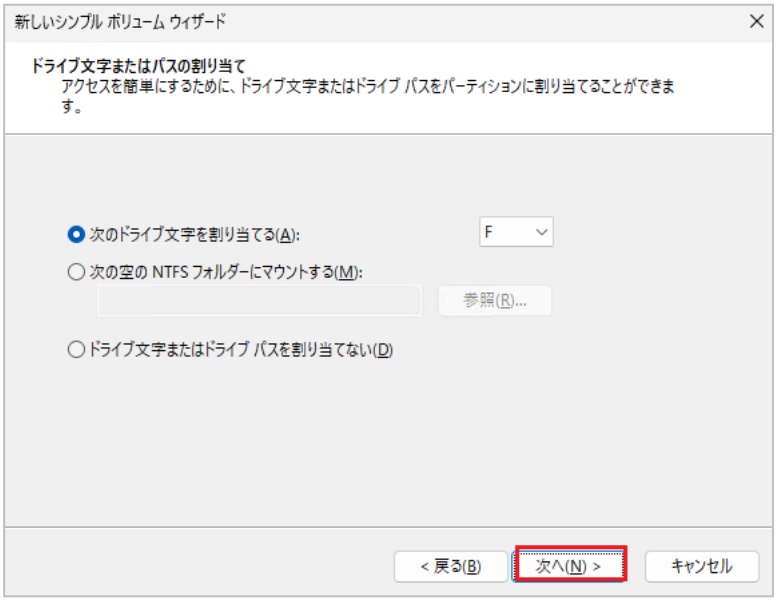


11 「新しいシンプル ボリューム」ウィザードが表示されます。[次へ] をクリックします。

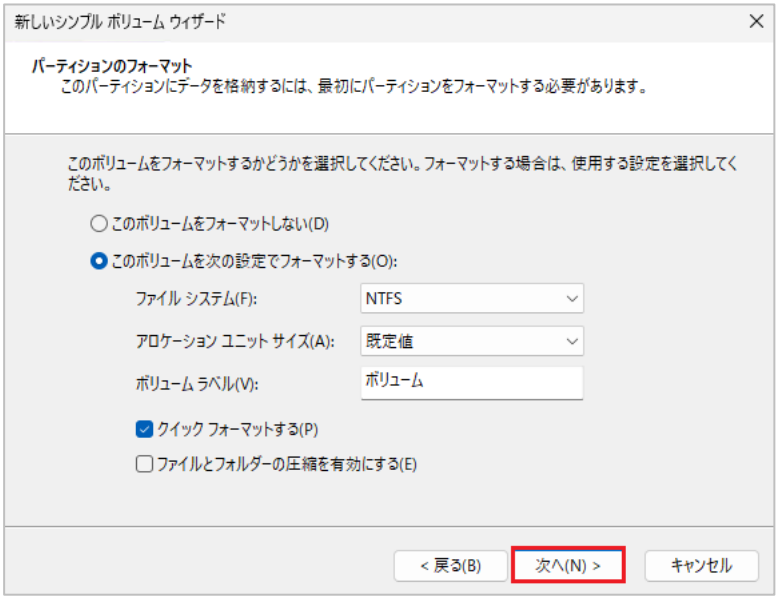
12 既定値 (最大ディスク領域) のまま、[次へ] をクリックします。



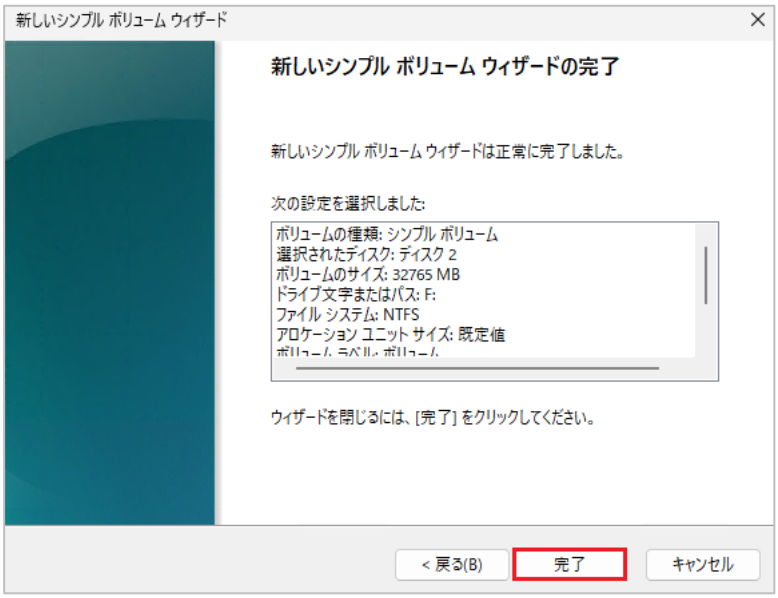
13 既定値 (空いているドライブ文字) のまま、[次へ] をクリックします。



14 既定値のまま、[次へ] をクリックします。



15 内容を確認後、[完了] をクリックします。



16 ボリュームの状態が「正常」と表示されることを確認します。

17 これでディスクの追加は完了です。

IP アドレスの固定

プライベート IP アドレスを静的に設定します。

ADDC を構成する際には、サーバーの IP アドレスが固定されていることが推奨されます。

注 : VM の OS 内のネットワーク インターフェイスの IP アドレスを手動で設定することは非推奨です。IP アドレスを設定する際は、OS 側の設定は「自動」のまま、Azure 側の NIC を設定してください。

IP アドレスを固定する手順は、以下の通りです。

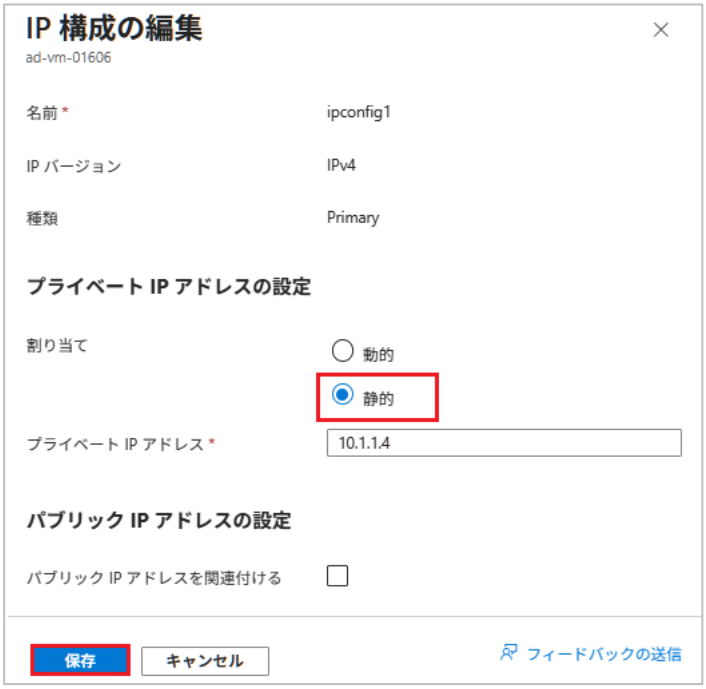
1 [仮想マシン] の一覧にて、ADDC の VM をクリックします。

2 左側のナビゲーションから [ネットワーク] > [ネットワーク設定] の順にクリックします。

3 [<ネットワーク インタフェース名>] をクリックします。

4 左側のナビゲーションから [設定] > [IP 構成] の順に選択して、表示された IP 構成名をクリックします。

5 [割り当て] を「静的」に変更後、[保存] をクリックします。



6 これで IP アドレスの固定は完了です。

ADDS の導入

AD サーバー上に、Active Directory ドメインサービス (ADDS) を導入します。

補足 : Azure 固有の設定はありません。オンプレミスと同様に設定してください。

ADDS の導入手順は、以下の通りです。

1 作成した AD 用 VM へ RDP 接続し、サーバー マネージャーを起動します。
2 [管理] > [役割と機能の追加] の順にクリックします。
3 [役割と機能の追加ウィザード] が起動します。[次へ] をクリックします。
4 [役割ベースまたは機能ベースのインストール] を選択し、[次へ] をクリックします。
5 [サーバー プールからサーバーを選択] が有効かつ、[サーバー プール] に ADDS を導入するサーバーが選択されていることを確認し、[次へ] をクリックします。
6 [役割] のリストから [Active Directory ドメイン サービス] を選択します。
7 確認ウィンドウが表示されます。[管理ツールを含める] を選択し、[機能の追加] をクリックします。
8 「サーバーの役割」画面に戻り、[次へ] をクリックします。
9 内容を確認し、[次へ] をクリックします。
10 […自動的に再起動する] を選択し、[インストール] をクリックします。
11 インストール完了後、[閉じる] をクリックし、ウィザードを閉じます。
12 サーバー マネージャーの右上に表示されている [旗アイコン] > [このサーバーをドメインコントローラーに昇格する] の順にクリックします。

13 「Active Directory ドメインサービス構成ウィザード」が表示されます。[新しいフォレストを追加する] を選択し、[ルート ドメイン名] を入力します。設定後、[次へ] をクリックします。

14 パスワードに任意の値を設定し、その他項目は既定値のまま、[次へ] をクリックします。

15 「DNS オプション」は、既定値のまま [次へ] をクリックします。

16 ルート ドメイン名に指定したサブ ドメイン名が NetBIOS ドメイン名として自動生成されます。[次へ] をクリックします。

17 ADDS データの配置先パスに、「ディスクの追加」で作成したデータ用ディスクを指定して、[次へ] をクリックします。

18 内容を確認し、[次へ] をクリックします。

19 [インストール] をクリックします。インストールが進むと、サーバーが自動的に再起動されます。

注 : IP アドレスが静的ではないと警告が表示されますが、無視してください。

20 再起動後、サーバー マネージャーを起動して [ドメイン] に設定したルートドメイン名が表示されていることを確認してください。

21 これで ADDS の導入は完了です。

カスタム DNS サーバーの設定

ADDS の名前解決をするための DNS を指定する必要があります。AD やドメイン参加対象の VM を配置する VNet にカスタムの DNS アドレスを指定します。

DNS サーバーの設定手順は、以下の通りです。

1 [仮想ネットワーク] に遷移し、AD 用 VM が所属する VNet をクリックします。(例では、「Spoke-vnet」)

2 左側のナビゲーションから [設定] > [DNS] の順にクリックし、DNS サーバー項目の [変更] をクリックします。

3 以下の情報を設定します。設定後、[保存] をクリックします。

項目	設定値	例
DNS サーバー	カスタム	カスタム
IP アドレス	<AD サーバーのプライベート IP アドレス>	10.1.1.4

4 DNS サーバーの設定変更を反映するために、VNet 下の VM を再起動します。

5 DNS サーバー設定が反映されていることを確認します。

VNet 下の VM 上にて、Powershell のプロンプトで「ipconfig /renew」コマンドを実行してください。コマンドを実行すると、新しい DNS サーバーの値がクライアントに反映されます。

6 「nslookup <ルート ドメイン名>」コマンドを実行し、AD サーバーの IP アドレスが応答されることを確認します。

7 これで DNS サーバーの設定は完了です。

Parallels RAS 構築

所要時間: 60 分

Azure VM 上に RAS 環境を新規作成します。

この節では、RAS 環境作成の一環として以下を構成します。

- RAS インフラストラクチャ サーバーと公開リソース用 RDSH サーバーはドメイン環境で運用します。
- RAS インフラストラクチャ サーバーは、サブネット「PRAS-Frontend-snet」内で管理します。
- RAS Connection Broker と RAS プライマリ Secure Gateway は、VM「pras-vm-01 (10.1.2.4) 」内にデプロイします。
- RAS セカンダリ Secure Gateway は、VM [pras-vm-02 (10.1.2.5)] 内にデプロイします。
- 公開リソース用サーバーは、サブネット「PRAS-Backend-snet」内で管理します。
- RDSH は、VM [RDSH-vm-01 (10.1.3.4)] 内にデプロイします。
- RAS Agent と RAS サーバーの通信を有効にするため、TCP 135, 445 ポートを開放します。
- RAS サーバーに CA 証明書を登録します。

注 : RAS のインストール後に、サーバーのホスト名を変更した場合、RAS の再構成が必要になります。

ドメイン参加

RAS のインストール前に、Windows サーバーをドメインに参加させ、正しいホスト名を設定する必要があります。

補足 : Azure 固有の設定はありません。オンプレミスと同様に設定してください。

以下の VM を、ドメインに参加させてください。

項目	設定値 (例)
RAS CB + プライマリ SG 用 VM	pras-vm-01
RAS セカンダリ SG 用 VM	pras-vm-02
RDSH 用 VM	RDSH-vm-01

ドメインへの参加方法は、以下の通りです。

1 ドメインに参加させる対象の VM へ RDP 接続します。

2 [スタート] > [設定] の順にクリックします。

3 Windows の設定で、[アカウント] をクリックします。

4 [職場または学校にアクセスする] を選択して、[+接続] をクリックします。

5 [このデバイスをローカルの Active Directory ドメインに参加させる] をクリックします。

6 [ドメイン名] にルート ドメイン名を入力して、[次へ] をクリックします。

7 AD サーバーの管理者アカウント情報を入力し、[OK] をクリックします。

8 [次へ] をクリックします。

9 [今すぐ再起動する] をクリックします。

10 これでドメイン参加は完了です。

ポートの開放

RAS Agent と RAS サーバーの通信を有効にするために、標準の SMB ポート (135, 445) を開放します。

以下の VM にて、Windows ファイアウォールの受信規則に TCP 135, 445 ポートの許可を追加してください。

項目	設定値 (例)
RAS セカンダリ SG 用 VM	pras-vm-02
RDSH 用 VM	RDSH-vm-01

RAS のファーム作成

以下の VM に RAS インフラストラクチャ サーバー (RAS CB、RAS SG 等) を配置します。

項目	設定値 (例)
RAS CB + プライマリ SG 用 VM	pras-vm-01
RAS セカンダリ SG 用 VM	pras-vm-02

RAS インストール

RAS を新規にインストールします。

> 詳細な RAS インストール手順に関しては、以下の Parallels RAS ガイドをご参照ください。
> https://docs.parallels.com/parallels-ras-administrators-guide-20/nihongo/parallels-ras-noinsutru/parallels-ras-woinsutru

1. VM「pras-vm-01」に RDP 接続します。
2. RAS の MSI インストーラーを使用して、RAS サーバー コンポーネントをインストールします。
3. OS 再起動後、RAS Console を起動し、RAS ファームをアクティベートします。

RAS Secure Gateway の追加

専用サーバーに RAS セカンダリ Secure Gateway をインストールします。

> 詳細な RAS Secure Gateway の追加手順に関しては、以下の Parallels RAS ガイドをご参照ください。
> https://docs.parallels.com/parallels-ras-administrators-guide-20/nihongo/ras-secure-gateway/ras-secure-gateway-no

1. RAS Console の [ファーム] > <サイト> > [Secure Gateway] に遷移します。
2. VM「pras-vm-02」に対して、RAS Secure Gateway Agent をプッシュインストールします。

RDSH の追加

専用サーバーにリモート デスクトップ サービス (RDS) 役割をインストールします。

> 詳細な RDSH の追加手順に関しては、以下の Parallels RAS ガイドをご参照ください。
> https://docs.parallels.com/parallels-ras-administrators-guide-20/nihongo/rd-sesshonhosuto/rd-sesshonhosutowo

1. RAS Console の [ファーム] > <サイト> > [RDSH] に遷移します。
2. VM「RDSH-vm-01」に対して、RAS RDSH Agent と RDS 役割をプッシュインストールします。

証明書の登録

本書では、CA 証明書を使用するため、RAS に CA 証明書のインストールをおこないます。自己署名証明書を使用される場合は、本手順をスキップしてください。

> 詳細な証明書の管理手順に関しては、以下の Parallels RAS ガイドをご参照ください。
> https://docs.parallels.com/parallels-ras-administrators-guide-20/nihongo/ssl-no

証明書のインポート手順は、以下の通りです。

1. RAS Console の [ファーム] > <サイト> > [証明書] に遷移します。
2. [タスク] > [証明書のインポート] の順にクリックします。
3. 以下の情報を設定します。設定後、[OK をクリックします。

項目	設定値	例
名称	<証明書の名前>	demo.pras.com
説明	<任意>	

プライベート キーファイル	<秘密鍵を含む証明書ファイルを指定>	demo.pras.pfx
証明書ファイル	<証明書ファイルを指定>	<自動入力>

4. インポートした証明書が、証明書の一覧に表示され、[ステータス] が [インポート済み] であることを確認します。これで、証明書のインポートは完了です。

NLB アクセス設定

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します。

> 詳細な NLB の管理手順に関しては、以下の Parallels RAS ガイドをご参照ください。
> https://docs.parallels.com/parallels-ras-administrators-guide-20/nihongo/ras-secure-gateway/ras-secure-gateway-no-1/yzptaruwosuru/nettowkurdobaranshenoakusesu

代替ホスト名とポート番号の設定手順は、以下の通りです。

1. RAS Console の [ファーム] > <サイト> > [Secure Gateway] に遷移します。
2. 各 Secure Gateway を右クリックし、 [タスク] > [プロパティ] の順にクリックします。
3. [ユーザー ポータル] タブにて、以下の情報を設定します。設定後、[OK] をクリックします。

項目	設定値	例
代替ホスト名を使用する	<証明書の FQDN>	demo.pras.com
代替ポートを使用する	8443	8443

4. これで、代替ホスト名とポート番号の設定は完了です。

Web Cookie の設定

負荷分散に使用する Azure Application Gateway では、ラウンドロビンで負荷分散が行われるので、ユーザー セッションを維持するために Cookie ベースのセッション アフィニティを設定します。

Web Cookie の設定手順は、以下の通りです。

1. RAS Console の [ファーム] > <サイト> > [Secure Gateway] に遷移します。
2. 各 Secure Gateway を右クリックし、 [タスク] > [プロパティ] の順にクリックします。
3. [web] タブにて、以下の情報を設定します。設定後、[OK] をクリックします。

項目	設定値	例
Web Cookie	<任意> *1	ApplicationGatewayAffinity
安全な Web Cookie を使用する	✅ 有効	✅ 有効

*1 : Azure Application Gateway 側で設定した Cookie 名と一致する必要があります。

4. これで、Web Cookie の設定は完了です。

第 5 章

負荷分散構成

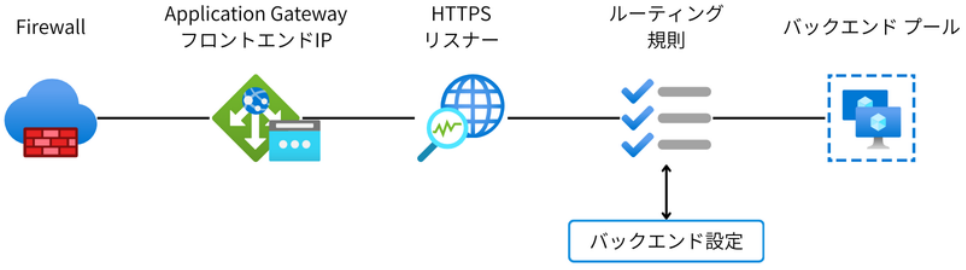
Azure では、4 つの負荷分散サービスが提供されています。本書では、Azure Load Balancer (LB) と Azure Application Gateway (AG) の 2 つのサービスを使用して、Azure VM 上に作成した複数の RAS SG への負荷分散を行います。

それぞれ、Azure Load Balancer はハードウェア、Azure Application Gateway はソフトウェアの負荷分散をサポートします。

- Azure Load Balancer (LB)
  - OSI 参照モデルのレイヤー4 (トランスポート層) のトラフィック (TCP, UDP) を負荷分散する
  - 複数の VM または VM スケールセットといったサーバーに入るトラフィックを分散
- Azure Application Gateway (AG)
  - レイヤー7 (アプリケーション層) のトラフィック (HTTP, HTTPS) を負荷分散する
  - ソフトウェアやアプリケーションごとにトラフィックを分散

Azure Load Balancer では、「フロントエンド」に到着した受信ネットワーク トラフィック (負荷) を、「負荷分散規則」と「正常性プローブ」に従って「バックエンド プール」のインスタンスに分配します。また、フェイルオーバー機能により、サーバーに障害が起きた場合でも、自動的にリクエストを別のサーバーに転送することで可用性を向上します。

Azure Application Gateway では、「フロントエンド」に到着したトラフィック (負荷) を、「リスナー」に関連付けられている「ルーティング規則 (ルール) 」に従って評価し、「バックエンド プール」のインスタンスに分配します。バックエンド プール内に複数の正常なバックエンド サーバーがある場合、ラウンドロビンで負荷分散が実行されます。セキュリティとして、End to End の SSL/TLS 暗号化がサポートされています。



Azure Application Gateway の End to End TLS では、SSL 経由の受信トラフィックを復号化し、ルーティング規則に従って処理後、再暗号化してバックエンドに送信します。

本書では、プライベート (内部) の Azure Load Balancer と Azure Application Gateway を使用して、VNet 内のリソースに対して負荷分散を行います。End to End TLS では、CA 証明書を使用します。

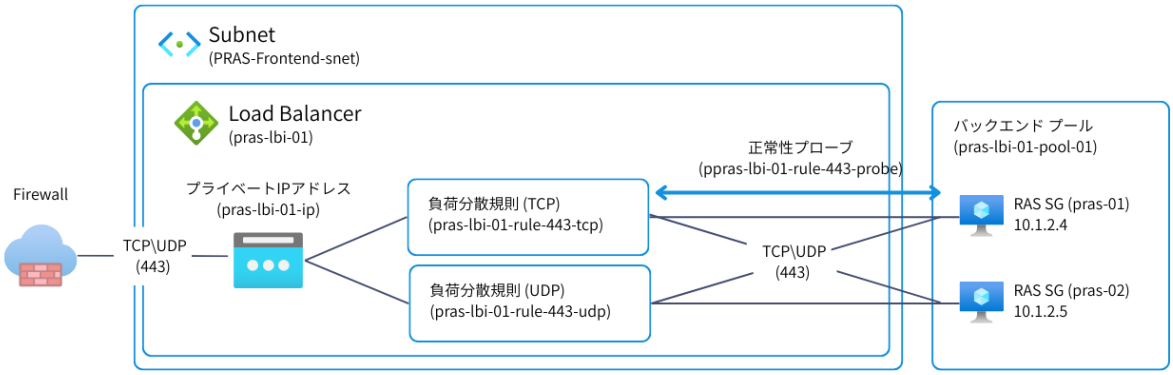
この章の内容

Azure Load Balancer の構築

所要時間: 30 分

プライベートの Azure Load Balancer を新規作成します。

この節では、Azure Load Balancer 作成の一環として以下を構成します。



項目	設定値 (例)
Azure Load Balancer	pras-lbi-01
フロントエンド IP アドレス	pras-lbi-01-ip
バックエンド プール	pras-lbi-01-pool-01
インバウンドの負荷分散規則 (TCP)	pras-lbi-01-rule-443-tcp
インバウンドの負荷分散規則 (UDP)	pras-lbi-01-rule-443-udp
正常性プローブ	pras-lbi-01-rule-443-probe

- Azure Load Balancer は、[Spoke-vnet] のサブネット内にデプロイします。

- フロントエンド IP では、Azure Firewall からリクエストを受け付けるためのプライベート IP アドレスを設定します。
- バックエンド プールでは、負荷分散先となる各 VM (RAS SG) を指定します。
- 負荷分散規則では、受け取ったトラフィックをバックエンド プールの各インスタンスへ分散する規則を 2 つ作成します。
- 正常性プローブでは、バックエンドプールで登録済みの各インスタンスが HTTPS の応答ができる状態にあるか、定期的に監視するように設定します。応答がないインスタンスは負荷分散の対象から除外されます。

詳細な Azure Load Balancer の仕様に関しては、以下の Microsoft ガイドをご参照ください。 https://learn.microsoft.com/ja-jp/azure/load-balancer/

Azure Load Balancer の作成方法は、以下の通りです。

1 Azure portal にアクセスし、[ロード バランサー] に遷移します。

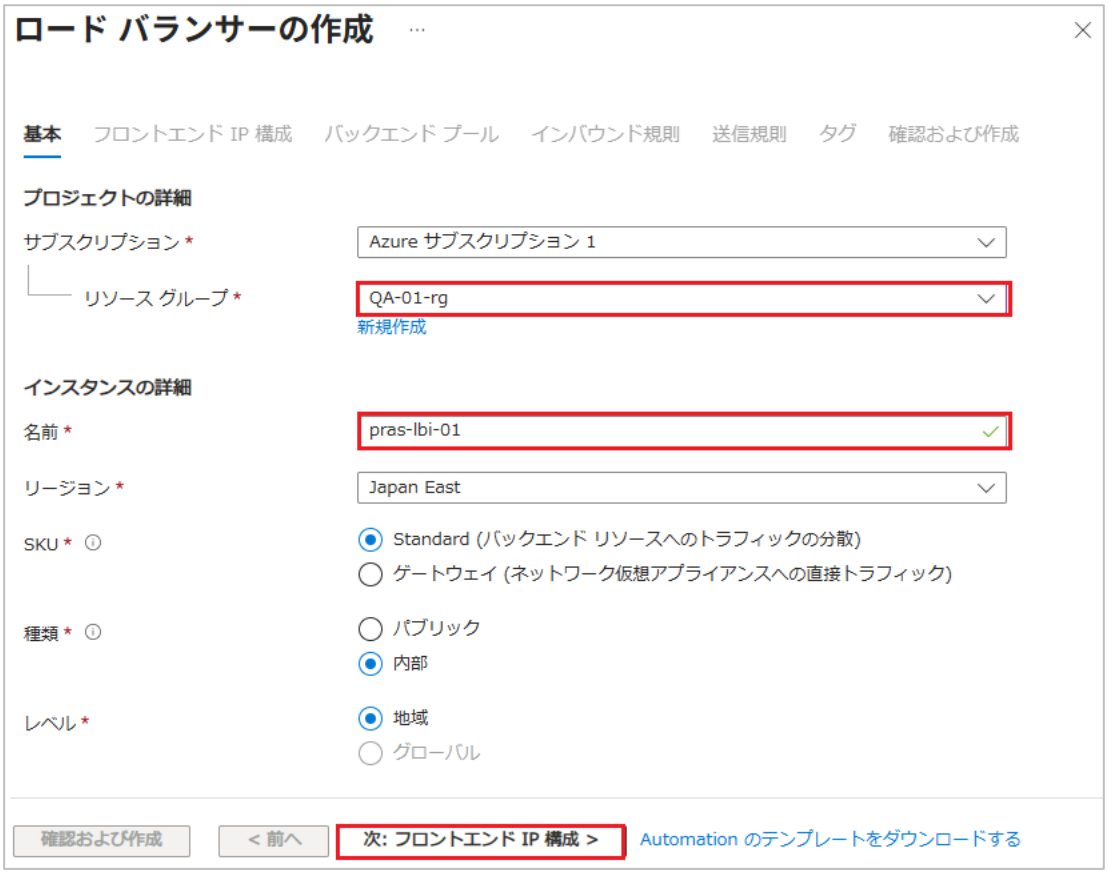
2 [+作成する] をクリックし、在庫管理単位 (SKU) を選選択します。

項目	設定値	例
SKU	Standard Load Balancer	Standard Load Balancer

3 [基本] タブで以下の情報を設定します。設定後、[次: フロントエンド IP 構成 >] をクリックします。

項目	設定値	例
プロジェクトの詳細		
サブスクリプション *	<Azure サブスクリプションを選択>	Azure サブスクリプション
リソース グループ *	<作成したリソース グループを選択>	QA-rg-01
インスタンスの詳細		
名前 *	<Load Balancer の名前を指定>	pras-lbi-01

リージョン *	< RAS SG が配置されている VM と同一のリージョンを選択>	Japan East
SKU *	<任意>	Standard
種類 *	内部	内部 (プライベート)
レベル *	地域	地域



4 フロントエンド IP アドレスを新規追加します。

[フロントエンド IP 構成] タブで、[+フロントエンド IP 構成の追加] をクリックし、以下の情報を設定します。設定後、[保存] をクリックします。

項目	設定値	例
名前 *	<フロントエンド IP の名前を指定>	pras-lbi-01-ip
IP バージョン	IPv4	IPv4
仮想ネットワーク *	< RAS コンポーネントが配置されている VNet を選択>	Spoke-vnet
サブネット *	<RAS コンポーネントが配置されているサブネット>	PRAS-Frontend-snet
割り当て	静的	静的
IP アドレス *	<使用したい IP アドレス>	10.1.2.200
可用性ゾーン *	<任意> *1	なし

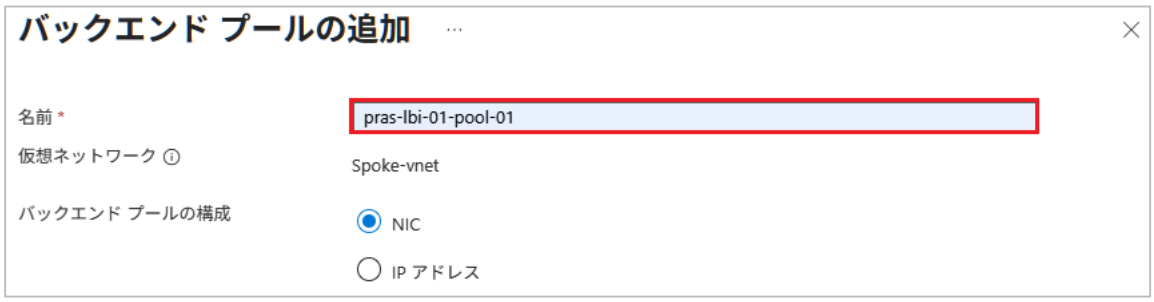
*1：本番環境では、冗長化構成を設定してください。

5 [次: バックエンド プール >] をクリックします。

6 バックエンド プールを新規追加します。

[バックエンド プール] タブで [+バックエンド プールの追加] をクリックし、以下の情報を設定します。

項目	設定値	例
名前 *	<バックエンド IP の名前を指定>	pras-lbi-01-pool-01
バックエンド プールの構成	NIC	NIC



7 [IP 構成] にて [+追加] をクリックします。

8 対象のリソースを選択し、[追加] をクリックします。設定後、[保存] をクリックします。

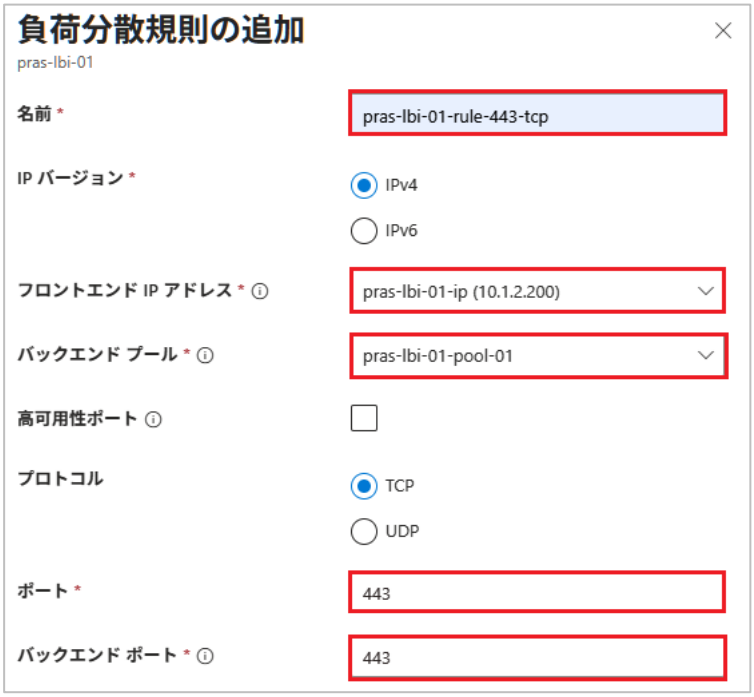
項目	設定値	例
対象のリソース	<すべての RAS SG サーバー>	10.1.2.4, 10.1.2.5

9 [次: インバウンド規則 >] をクリックします。

10 負荷分散規則を 2 つ新規追加します。初めに、TCP トラフィックを許可する規則を追加します。

[インバウンド規則] タブで、[+負荷分散規則の追加] をクリックし、以下の情報を設定します。

項目	設定値	例
名前 *	<負荷分散規則の名前を指定>	pras-lbi-01-rule-443-tcp
IP バージョン *	IPv4	IPv4
フロントエンド IP アドレス *	<作成したフロントエンド IP アドレスを選択>	pras-lbi-01-ip
バックエンド プール *	<作成したバックエンド プールを選択>	pras-lbi-01-pool-01
プロトコル	TCP	TCP
ポート *	443	443
バックエンドポート *	443	443



11 正常性プローブを新規追加します。

[正常性プローブ] セクションで、[新規作成] をクリックします。以下の情報を設定し、[保存] をクリックします。

項目	設定値	例
名前 *	<正常性プローブの名前を指定>	pras-lbi-01-rule-443-probe
プロトコル *	TCP	TCP
ポート *	443	443
サイクル間隔 (秒) *	<最小値は 5 秒>	5

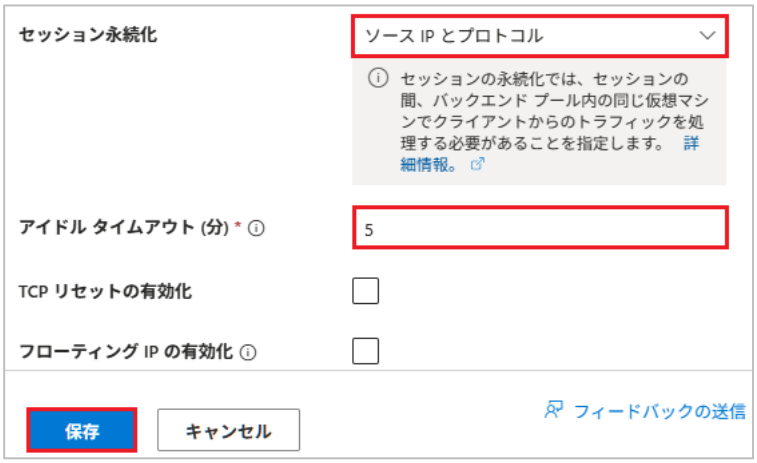
12 続けて、以下の情報を設定します。設定後、[保存] をクリックします。

項目	設定値	例
セッション永続化	ソース IP とプロトコル *2	ソース IP とプロトコル
アイドル タイムアウト (分) *	4 *3	5
TCP リセットの有効化	☐ 無効	☐ 無効
フローティング IP の有効化	☐ 無効 *4	☐ 無効

*2 : [ソース IP とプロトコル] が選択されている場合、同じ IP アドレスかつプロトコルのクライアントからの連続した要求が、同じ VM によって処理されます。

*3 : 推奨は 5~15 分

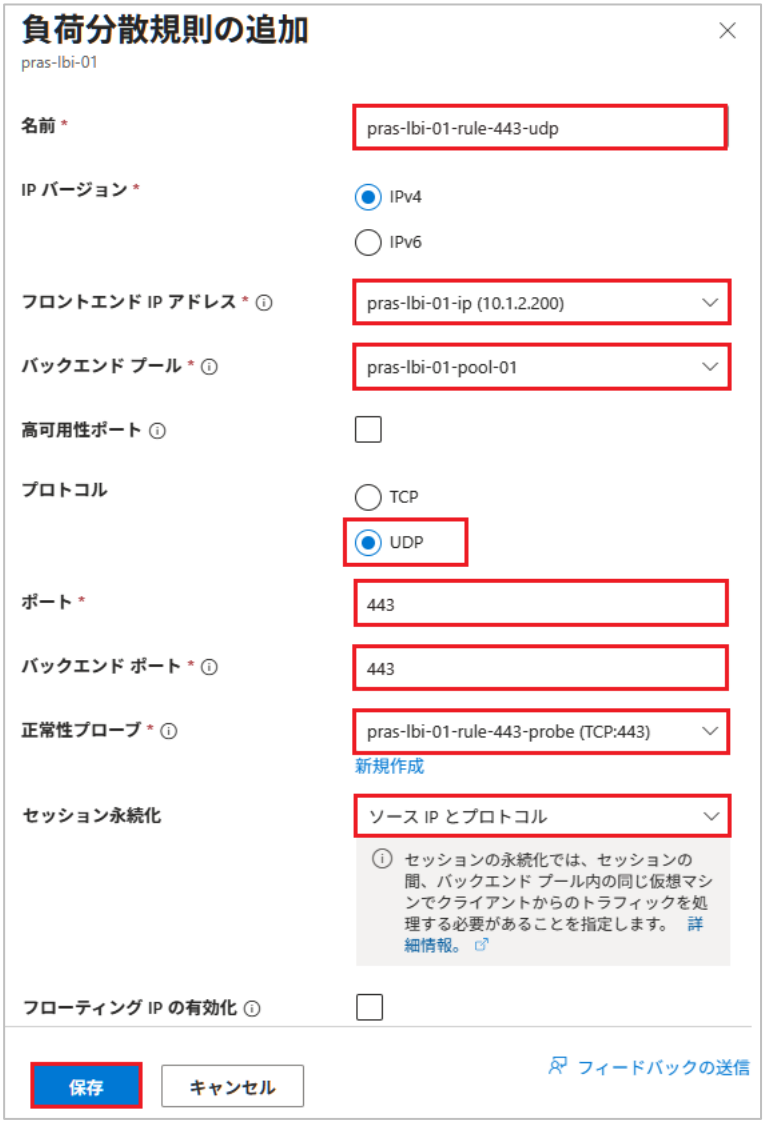
*4 : [無効] が選択されている場合、Azure Load Balancer はノードのプライマリ IP にパケットを送信します。



13 UDP トラフィックを許可する規則を追加します。

[負荷分散規則の追加] をクリックし、以下を設定します。設定後、[保存] をクリックします。

項目	設定値	例
名前 *	<負荷分散規則の名前を指定>	pras-lbi-01-rule-443-udp
IP バージョン *	IPv4	IPv4
フロントエンド IP アドレス *	<作成したフロントエンド IP アドレスを選択>	pras-lbi-01-ip
バックエンド プール *	<作成したバックエンド プールを選択>	pras-lbi-01-pool-01
プロトコル	UDP	UDP
ポート *	443	443
バックエンドポート *	443	443
正常性プローブ *	<作成した正常性プローブを選択>	pras-lbi-01-rule-443-probe
セッション永続化	ソース IP とプロトコル	ソース IP とプロトコル
フローティング IP の有効化	□ 無効	□ 無効



14 [送信規則] と [タグ] は、変更なしです。[確認及び作成] をクリックします。

15 [確認及び作成] タブで、内容を確認後、[作成] をクリックします。

16 「デプロイが完了しました」と表示されれば、プライベートの Azure Load Balancer の作成は完了です。

17 動作確認をします。作成した Azure Load Balancer の左側のナビゲーションから [監視] > [分析情報] の順にクリックします。[分析情報] にて、エラーが表示されていないことを確認します。

Azure Application Gateway の構築

所要時間: 40 分

プライベートの Azure Application Gateway を新規作成します。

この節では、Azure Application Gateway 作成の一環として以下を構成します。

項目	設定値 (例)
Azure Application Gateway	pras-agw-01
フロントエンド IP アドレス (パブリック)	pras-agw-01-pip
フロントエンド IP アドレス (プライベート)	10.0.2.200
リスナー	pras-agw-01-rule-01-listener-01
ルーティング規則 (ルール)	pras-agw-01-rule-01
バックエンド設定 (HTTP 設定)	pras-agw-01-backend-settings-01
バックエンド プール	pras-agw-01-pool-01

- Azure Application Gateway は、[Hab-vnet] の Azure Application Gateway 用サブネット内にデプロイします。
- フロントエンド IP アドレスでは、パブリック IP とプライベート IP の両方を設定します。ただし、パブリック IP は本書の構成では使用しません。(Azure Application Gateway v2 では、プライベートのみの構成はできないため)
- ルーティング規則 (ルール) では、以下の 2 つの構成要素によって、フロントエンドから届くトラフィックをバックエンドに振り分けるための規則を作成します。
  - リスナーでは、Azure Firewall からリクエストを受け付けるためのフロントエンド IP の指定とフロントエンドのポート、プロトコルを設定します。HTTPS を使用するので、証明書の登録も行います。
  - バックエンド設定では、バックエンドに接続するポートとプロトコルを設定します。HTTPS を使用するので、再暗号化用の証明書の登録も行います。ラウンドロビンで負荷分散が行われるので、ユーザー セッションを維持するために Cookie ベースのセッション アフィニティを有効化します。
- バックエンドプールでは、負荷分散先となる各 VM (RAS SG) を指定します。

> 詳細な Azure Application Gateway の仕様に関しては、以下の Microsoft ガイドをご参照ください。
> https://learn.microsoft.com/ja-jp/azure/application-gateway/overview

プライベートの Azure Application Gateway の作成方法は、以下の通りです。

1 Azure portal にアクセスし、[Application Gateways] に遷移します。

2 [+Create] をクリックし、[Application Gateway] を選択します。

3 [基本] タブで以下の情報を設定します。設定後、[次: フロントエンド >] をクリックします。

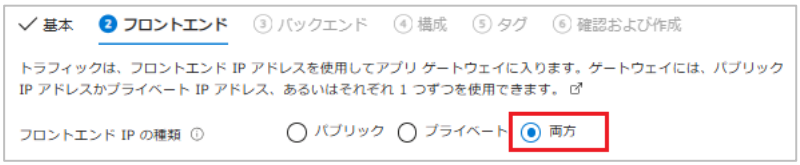
項目	設定値	例
プロジェクトの詳細		
サブスクリプション *	<Azure サブスクリプションを選択>	Azure サブスクリプション
リソース グループ *	<作成したリソース グループを選択>	QA-rg-01
インスタンスの詳細		
ゲートウェイ名 *	<Application Gateway の名前を指定>	pras-agw-01
リージョン *	<VNet と同一のリージョンを選択>	Japan East
レベル *	Standard V2	Standard V2
自動スケール	<任意>	はい
最小インスタンス数 *	<要件に合ったインスタンス数を指定> *1	0
最大インスタンス数	<任意>	10
IP アドレスの種類	<任意>	IIPv4
HTTP2	無効	無効
仮想ネットワークの構成		
仮想ネットワーク *	<作成した仮想ネットワークを選択>	Hub-vnet
サブネット	<作成した Application Gateway 用サブネットを選択>	ApplicationGateway

*1：運用環境では、インスタンス数 2 以上が推奨となります。

4 [フロントエンド] タブで以下の情報を設定します。

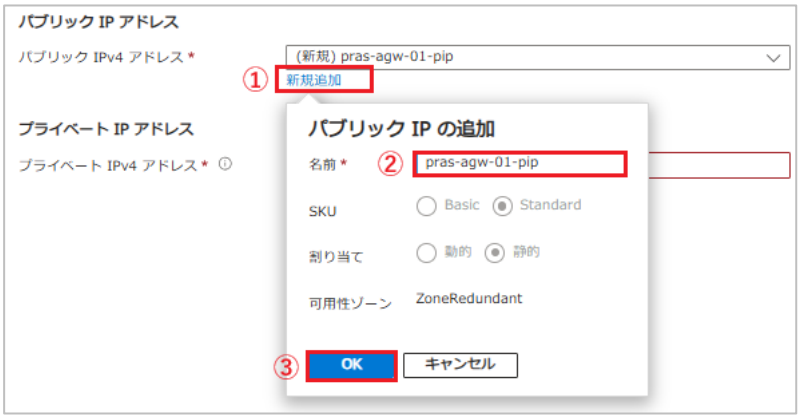
項目	設定値	例
フロントエンド IP の種類	両方 *2	両方

*2 : レベル Standard_v2 の Application Gateway は、フロントエンドとしてプライベート IP アドレスのみを使用できません。そのため、「両方」を設定しますが、パブリック IP は使用しません。



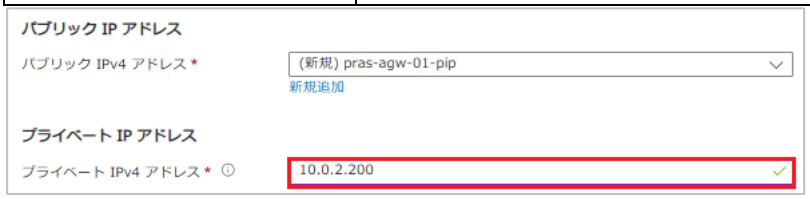
5 [パブリック IP アドレス] の [新規追加] を選択し、名前を設定します。

項目	設定値	例
パブリック IP アドレス名 *	<パブリック IP の名前を入力>	pras-agw-01-pip



6 [プライベート IP アドレス] を指定します。設定後、[次: バックエンド >] をクリックします。

項目	設定値	例
プライベート IP アドレス *	<プライベート IP アドレスを指定>	10.0.2.200



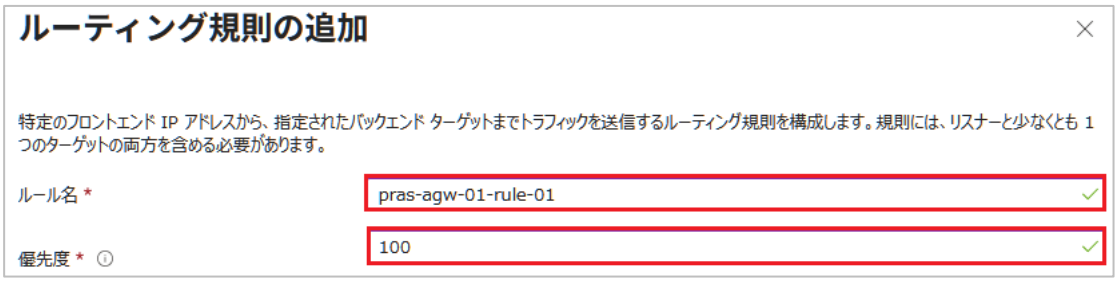
7 [バックエンド] タブで、[バックエンド プールを追加] をクリックし、以下の情報を設定します。設定後、[追加] をクリックします。

項目	設定値	例
名前 *	<バックエンド プールの名前を指定>	pras-agw-01-pool-01
ターゲットを持たないバックエンド プールを追加します	いいえ	いいえ
バックエンド ターゲット	<すべての RAS SG サーバー>	10.1.2.4, 10.1.2.5

8 [次: 構成 >] をクリックします。

9 [構成] タブで、[+ルーティング規則を追加] をクリックし、以下の情報を設定します。

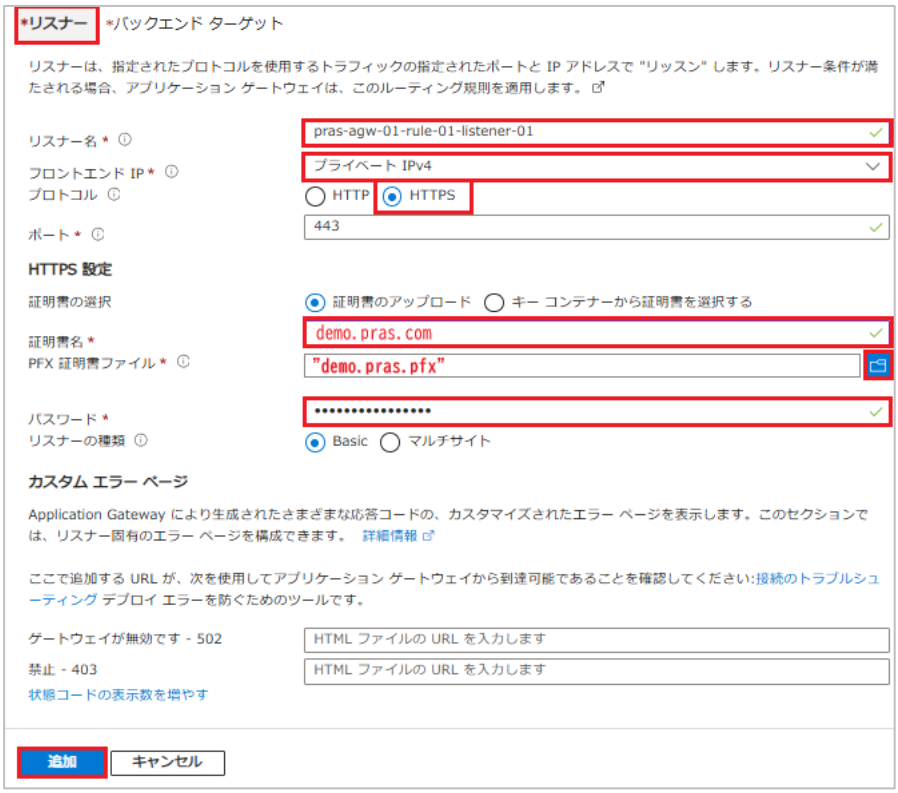
項目	設定値	例
ルール名 *	<ルーティング規則の名前を指定>	pras-agw-01-rule-01
優先度 *	<ルールが処理される順序を指定>	100



10 [リスナー] タブをクリックし、以下の情報を設定します。設定後、[追加] をクリックします。

項目	設定値	例
リスナー名 *	<リスナーの名前を指定>	pras-agw-01-rule-01-listener-01
フロントエンド IP *	プライベート	プライベート
プロトコル	HTTPS	HTTPS
ポート *	443	443
HTTPS 設定		

証明書の選択 *	証明書のアップロード	証明書のアップロード
証明書名 *	<証明書の名前を指定>	demo. pras.com
PFX 証明書ファイル *	<復号化用の秘密鍵が含まれた証明書>	.pfx
パスワード *	<証明書のパスワードを入力>	
リスナーの種類	Basic	Basic
カスタム エラー ページ	<任意>	なし



11 [バックエンド ターゲット] タブをクリックし、以下の情報を設定します。

項目	設定値	例
ターゲット種類	バックエンド プール	バックエンド プール
バックエンド ターゲット *	<作成したバックエンド プールを選択>	pras-agw-01-pool-01

12 [バックエンド設定] 項目の [新規追加] をクリックし、以下の情報を設定します。設定後、[追加] をクリックします。

項目	設定値	例

バックエンド設定名 *	<バックエンド設定の名前を指定>	pras-agw-01-backend-settings-01
バックエンド プロトコル	HTTPS	HTTPS
バックエンド ポート *	443	443
バックエンド HTTPS 検証設定		
バックエンド証明書の検証の種類	*3	検証の完了
追加のバックエンド設定		
Cookie ベースのアフィニティ	有効化	有効化
アフィニティ Cookie 名	<アフィニティ Cookie の名前を指定> *4	ApplicationGatewayAffinity
接続のドレイン	任意	無効化
要求のタイムアウト (秒) *	40 *5	40

*3：証明書によって設定が変わります。Microsoft のガイドをご確認ください。
(https://learn.microsoft.com/ja-jp/azure/application-gateway/ssl-overview?WT.mc_id=Portal-Microsoft_Azure_HybridNetworking#end-to-end-tls-with-the-v2-sku)

*4：任意の名前で構いませんが、RAS 構成の [Web Cookie] に指定した Cookie 名と一致する必要があります。

*5：デフォルト値の 20 は RAS ユーザー ポータルのキープアライブ 30 秒より短いため、アイドル状態のセッションが切断される可能性があります。

13 [次: タグ >] をクリックします。

14 [タグ] タブの値は、既定値のまま変更なしです。[次: 確認および作成 >] をクリックします。

15 [確認および作成] タブで、[作成] をクリックします。

16 「デプロイが完了しました」と表示されれば、Azure Application Gateway の作成は完了です。

17 動作確認をします。作成した Azure Application Gateway の左側のナビゲーションから [監視] > [分析情報] の順にクリックします。[分析情報] にて、エラーが表示されていないことしていることを確認します。

第 6 章

セキュリティ構成

VNet に対するセキュリティを強化するために Azure Firewall を使用します。

Azure Firewall は、Azure 環境で動作するクラウドベースのファイアウォールです。Azure リソースに対するネットワーク トラフィックの制御や監視をおこないます。

Azure Firewall では、既定ですべてのトラフィックが拒否されます。トラフィックを許可するには、「従来の規則」か「Firewall Policy」を使用して、規則を設定する必要があります。規則の種類は、宛先ネットワーク アドレス変換 (DNAT) 、ネットワーク、アプリケーションの 3 種です。

本書では、Azure Firewall をインターネットの出入り口に設置し、Azure Application Gateway や Azure Load Balancer に到達する前にトラフィックを検査およびフィルター処理するように設計します。アクセス管理には Firewall policy を使用し、DNAT 規則によってインバウンド通信を処理します。

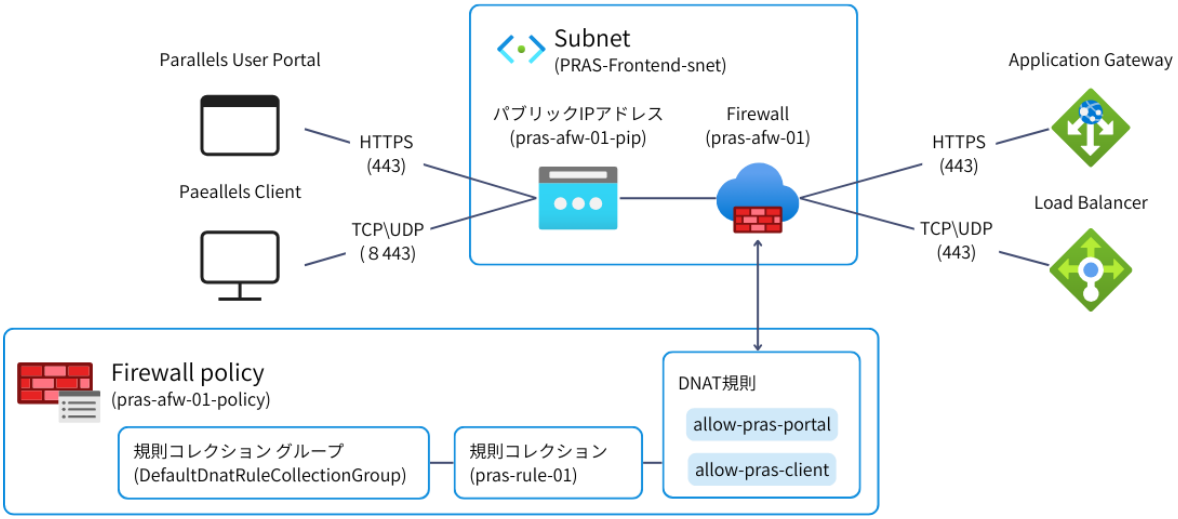
この章の内容

Azure Firewall の構築

所要時間: 30 分

Azure Firewall を新規作成します。

この節では、Azure Firewall 作成の一環として以下を構成します。



項目	設定値 (例)
Azure Firewall	pras-afw-01
パブリック IP アドレス	pras-afw-01-pip
Firewall policy	pras-afw-01-policy
規則コレクション	pras-rule-01
DNAT 規則 1	allow-pras-client
DNAT 規則 2	allow-pras-portal
DNAT 規則 3	allow-pras-rdp

- Azure Firewall は、[Hab-vnet] の Azure Firewall 専用サブネット内にデプロイします。
- Firewall policy では、インバウンド通信を制限するため DNAT 規則を設定します。
- DNAT 規則では、受信トラフィックを許可する規則を 3 つ作成します。
- 規則 1 は、TCP/UDP ポート 8443 での受信トラフィックを許可し、Azure Load Balancer (プライベート IP:443) に転送します。
- 規則 2 は、TCP ポート 443 での受信トラフィックを許可し、Azure Application Gateway (プライベート IP:443) に転送します。
- 規則 3 は、管理用に特定の RDP 接続を許可し、RAS サーバー (プライベート IP:3389) に転送します。

詳細な Azure Firewall の仕様に関しては、以下の Microsoft ガイドをご参照ください。

https://learn.microsoft.com/ja-jp/azure/firewall/

Azure Firewall の作成

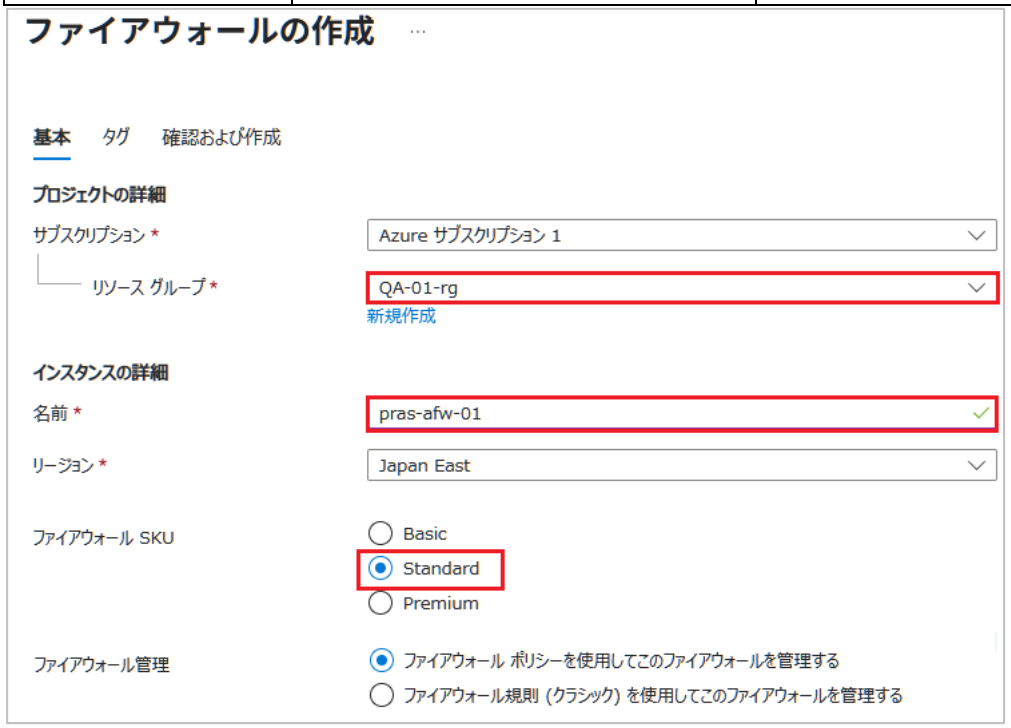
Azure Firewall の作成方法は、以下の通りです。

1 Azure portal にて、[Firewalls] に遷移します。

2 [+作成] を選択します。

3 [基本] タブで、以下の情報を設定します。

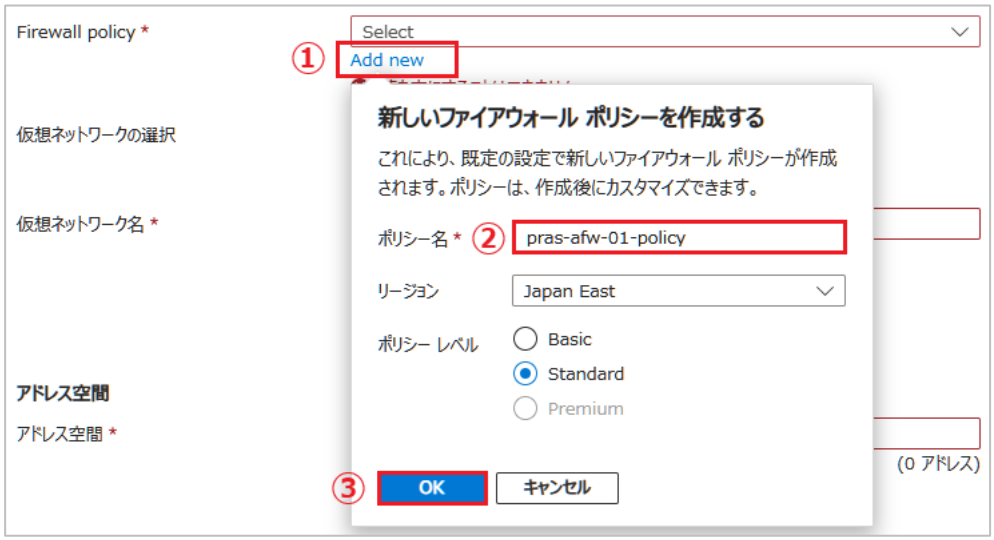
項目	設定値	例
プロジェクトの詳細		
サブスクリプション *	<Azure サブスクリプションを選択>	Azure サブスクリプション
リソース グループ *	<作成したリソース グループを選択>	QA-rg-01
インスタンスの詳細		
名前 *	<新しい Firewall の名前を入力>	pras-afw-01
リージョン *	<VNet と同一のリージョンを選択>	Japan East
ファイアウォール SKU	Standard	Standard
ファイアウォール管理	ファイアウォール ポリシーを使用してこのファイアウォールを管理する	ファイアウォール ポリシーを使用してこのファイアウォールを管理する



4 [Firewall policy] 項目の [Add new] をクリックし、以下を設定します。設定後、[OK] をクリックします。

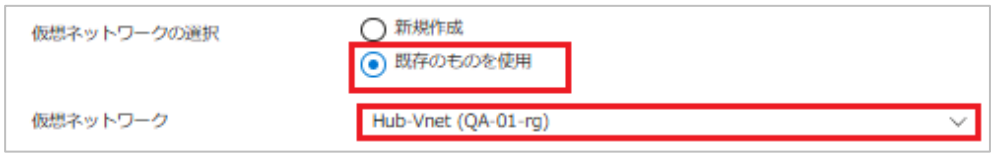
項目	設定値	例
名前 *	<新しい Firewall policy の名前を入力>	pras-afw-01-policy

リージョン	<VNet と同一のリージョンを選択>	Japan East
ポリシー レベル	Standard	Standard



5 [仮想ネットワーク] で、以下の情報を設定します。

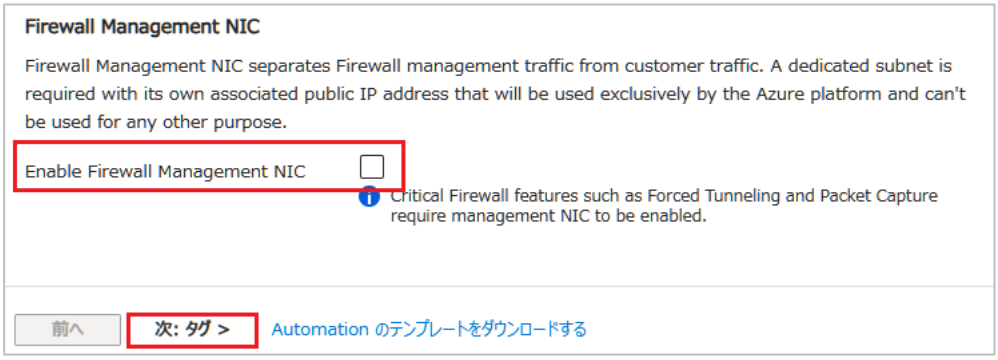
項目	設定値	例
仮想ネットワークの選択	既存のものを使用	既存のものを使用
仮想ネットワーク	<作成した仮想ネットワークを選択>	Hub-vnet



6 [パブリック IP アドレス] 項目の [新規追加] をクリックし、以下を設定します。設定後、[OK] をクリックします。

項目	設定値	例
名前 *	<新しいパブリック IP の名前を入力>	pras-afw-01-pip

7 [Firewall Management NIC] 項目は、[□ 無効] にします。設定後、[次: タグ >] をクリックします。



8 [タグ] タブの値は、既定値のまま変更なしです。[次: 確認および作成 >] をクリックします。

9 [確認および作成] タブで、[作成] をクリックします。

10 「デプロイが完了しました」と表示されれば、Azure Firewall の作成は完了です。

Firewall Policy の設定

DNAT 規則を新規追加します。

Firewall Policy の作成方法は、以下の通りです。

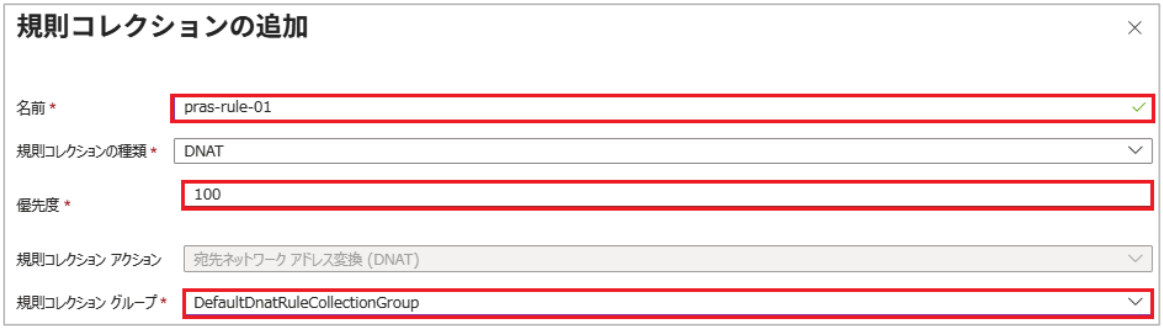
1 Azure portal にて、[Firewall Policy] に遷移します。

2 作成した Firewall Policy をクリックします。

3 左側のナビゲーションから [Rules] > [DNAT 規則] の順にクリックします。DNAT 規則に移動し、[＋規則コレクションの追加] をクリックします。

4 規則コレクションを新規追加します。

項目	設定値	例
名前 *	<規則コレクションの名前を指定>	pras-rule-01
規則コレクションの種類 *	DNAT	DNAT
優先度 *	<任意>	100
規則コレクション グループ *	DefaultDnatRuleCollectionGroup	DefaultDnatRuleCollectionGroup



5 規則を 2 つ新規作成します。初めに、443 ポートを許可する規則を追加します。

項目	設定値	例
名前 *	<規則の名前を指定>	allow-pras-portal
ソースの種類	<任意>	IP アドレス
ソース	<トラフィック送信元の IP>	*
プロトコル *	TCP	TCP
宛先ポート*	443	443
宛先タイプ *	IP アドレス	IP アドレス
宛先 *	<Firewall のパブリック IP アドレス>	
変換タイプ	IP アドレス	IP アドレス
変換アドレス *	< Azure Load Balancer のプライベート IP アドレス>	10.0.2.200
変換ポート*	443	443

6 続けて、8443 ポートを許可する規則を追加します。

項目	設定値	例
名前 *	<規則の名前を指定>	allow-pras-client
ソースの種類	<任意>	IP アドレス
ソース	<トラフィック送信元の IP>	*
プロトコル *	TCP, UDP	TCP, UDP
宛先ポート*	8443	8443
宛先タイプ *	IP アドレス	IP アドレス

宛先 *	<Firewall のパブリック IP アドレス>	
変換タイプ	IP アドレス	IP アドレス
変換アドレス *	<Azure Load Balancer のプライベート IP アドレス>	10.1.2.200
変換ポート*	443	443

7 管理者が RAS Console にアクセスするために、RDP 接続を許可する規則を追加します。設定後、[追加] をクリックして設定を保存します。

項目	設定値	例
名前 *	<規則の名前を指定>	allow-pras-rdp
ソースの種類	<任意>	IP アドレス
ソース	<トラフィック送信元の IP>	<クライアント PC 環境のグローバル IP アドレス>
プロトコル *	TCP	TCP
宛先ポート*	3389	3389
宛先タイプ *	IP アドレス	IP アドレス
宛先 *	<Firewall のパブリック IP アドレス>	
変換タイプ	IP アドレス	IP アドレス
変換アドレス *	<RAS サーバーのプライベート IP アドレス>	10.1.2.4
変換ポート*	3389	3389

8 これで、DNAT 規則の作成は完了です。

DNS レコード登録

Azure Firewall 経由で RAS サーバーに接続する際、接続に使用する URL と Azure Firewall のパブリック IP アドレスを関連付ける必要が有ります。

ドメインのパブリック DNS に、Azure Firewall のパブリック IP アドレスの接続ドメイン名を対応させる A レコードを追加します。

本書の例では、以下の DNS エントリを作成します。

A レコード	demo. pras.com	< Azure Firewall のパブリック IP アドレス>

1. Azure Firewall のパブリック IP アドレスを確認します。

2. ご利用のドメインの DNS にアクセスし、A レコードを追加します。

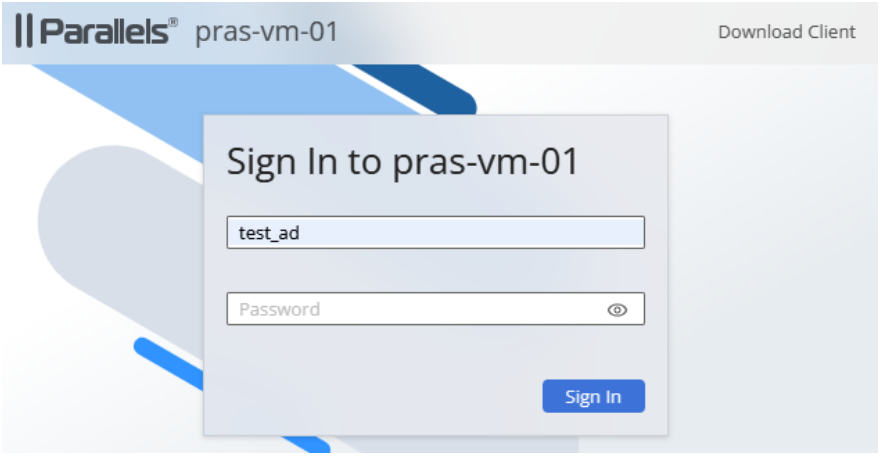
第 7 章

動作検証

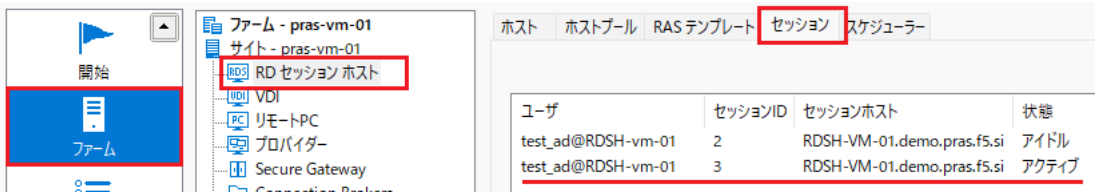
RAS ユーザー ポータル

RAS ユーザー ポータルにて、Parallels Client およびブラウザを使用したアクセスをそれぞれ確認します。

1. クライアント PC の Web ブラウザにて、Azure Firewall に設定した FQDN を入力し、RAS ユーザー ポータルにアクセスします。(例では、https://demo.pras.com にアクセスしています。)
2. ユーザー アカウントの資格情報を入力して、ログインします。



3. 公開リソースをクリックし、新しいセッションを開始します。(例では、公開デスクトップを選択)
4. セッションが正常に開始されたら、セッションの状態を RAS Console 側で確認します。
5. RDP 接続で RAS サーバーにアクセスし、RAS Console を起動します。
6. [ファーム] > <サイト> > [RDSH] の順にクリックします。[セッション] タブにて、アクティブなセッションがあることを確認します。



7. セッションを右クリックし、[プロパティ] を選択します。
8. [RAS Secure Gateway の名前] と [プロトコル] を確認します。

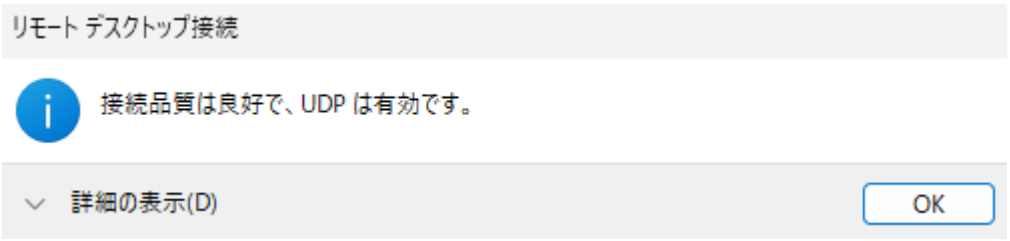
Parallels Client

インストール済み Parallels Client を使用したアクセスを確認します。

1. クライアント PC に Parallels Client をインストールし、起動します。(例では、Windows 版)
2. 接続先を設定します。
3. [ナビゲーション] > [新規接続] を順にクリックします。
4. Azure Firewall 経由で接続するための情報を設定します。設定後、[OK] をクリックします。

項目	設定値	例
プライマリ接続	<Azure Firewall のパブリック IP アドレス>	
	Gateway SSL Mode	Gateway SSL Mode
ポート	8443	8443

5. [接続] をダブルクリックします。
6. 公開リソースをダブルクリックし、新しいセッションを開始します。(例では、公開デスクトップを選択)
7. セッションが正常に開始されたら、上部バーの [接続アイコン] をクリックして、UDP プロトコルも使用されていることを確認します。



8. RDP 接続で RAS サーバーにアクセスし、RAS Console を起動します。
9. [ファーム] > <サイト> > [RDSH] の順にクリックします。[セッション] タブにて、アクティブなセッションがあることを確認します。
10. セッションを右クリックし、[プロパティ] を選択します。
11. [RAS Secure Gateway の名前] と [プロトコル] を確認します。


セッション情報
セッションセットアップ
ユーザ test_ad@RDSH-vm-01
セッションID 3
セッションホスト RDSH-VM-01.demo.pras.f5.si
ホストプール <Default>
タイプ 管理者
テーマ <Default>
接続の詳細
接続モード ゲートウェイSSLモード
認証タイプ 認証情報
MFA プロバイダー
フロー
1. 他 10.0.1.6
2. Secure Gateway pras-vm-02 (10.1.2.5)
ログオンの詳細
ログオン期間 5.43 秒
接続時間 2.43 秒
認証期間 18 ミリ秒
RAS ポリシーの検索 0 ミリ秒
ホストの準備 17 ミリ秒
グループポリシーの読み込み時間 140 ミリ秒
ユーザープロファイルの読み込み時間 87 ミリ秒
デスクトップの読み込み時間 528 ミリ秒
その他 2.21 秒
ユーザープロファイル その他
ユーザーエクスペリエンス
UX エバリュエーター
接続品質
遅延
トランスポートプロトコル UDP
帯域幅の可用性 なし
再接続 0
再接続(CIR) 0
切断の理由
セッションの詳細
状態 アクティブ
ログオン時間 Thu Sep 25 21:49:36 2025
セッションの長さ 7 秒
受信データ 98.65 KB
送信データ 211.16 KB
解像度 1280x800
色深度 32-bit
帯域幅の使用状況 19.40 kbps
クライアントの詳細
デバイス名 ACE0024N
IP アドレス 192.168.1.145
クライアント OS Windows 11 Professional 10.0.26100 (x64)
クライアント OS バージョン 24H2 (10.0.26100.4652)
クライアント バージョン 20.2 (Build 26020)
ポリシー
エクスポート(E)
OK

付録

Azure アカウントの登録

Azure を使用するには、Azure アカウントが必要です。

個人で初めて利用する場合は、Microsoft アカウントの登録を行ってください。

※ 新規登録には、有効なメール アドレス、電話番号、クレジットカード情報、住所の登録が必要です。

Microsoft または GitHub のアカウントをお持ちの場合は、これらのアカウントで Azure をご利用いただけます。

> 詳細なアカウント作成手順に関しては、以下の Microsoft ガイドをご参照ください。
>
> https://learn.microsoft.com/ja-jp/dotnet/azure/create-azure-account

アカウントの登録手順は以下の通りです。

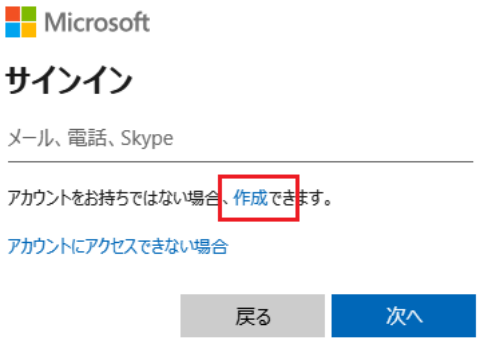
1. 下記の Azure アカウント作成サイトにアクセスし、[Azure を無料でお試しください] をクリックします。

   https://azure.microsoft.com/ja-jp/pricing/purchase-options/azure-account

2. 新規作成の場合、[作成] をクリックします。

   ※ Microsoft または GitHub のアカウントをお持ちの場合は、サインインを行ってください。



3. 画面の指示に従って基本情報を入力し、Microsoft の契約内容を確認して [同意] を選択します。
4. 登録が完了したら、[ポータルに移動] をクリックし、Azure Portal に遷移します。

> 参考 : Azure Portal は、Azure を管理するためのプラットフォームです。

5. これで、Azure への登録とサインインは完了です。

Windows の日本語化

所要時間 : 60 分

VM の日本語化は、該当 VM 上で実施します。ただし、日本語化の作業中は、DNS サーバーを「8.8.8.8」に変更してください。設定完了後、DNS サーバーを元の値に戻してください。

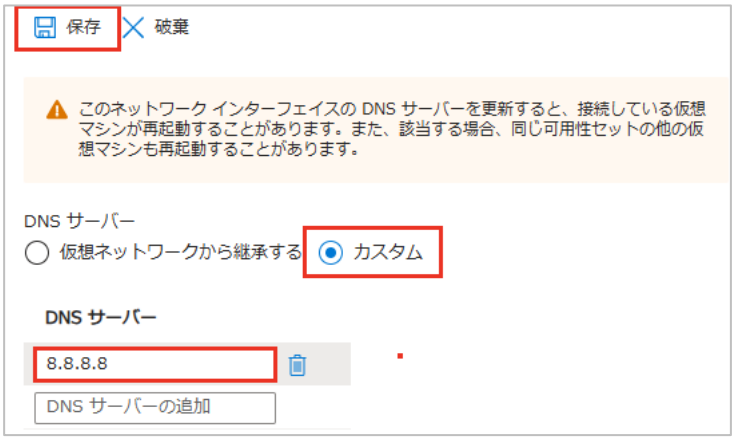
1 Azure portal にて、[仮想マシン] に遷移します。

2 日本語化対象の VM をクリックし、左側のナビゲーションから [ネットワーク] > [ネットワーク設定] の順にクリックします。

3 [ネットワーク インターフェイス] をクリックします。

4 左側のナビゲーションから [設定] > [DNS サーバー] の順にクリックします。

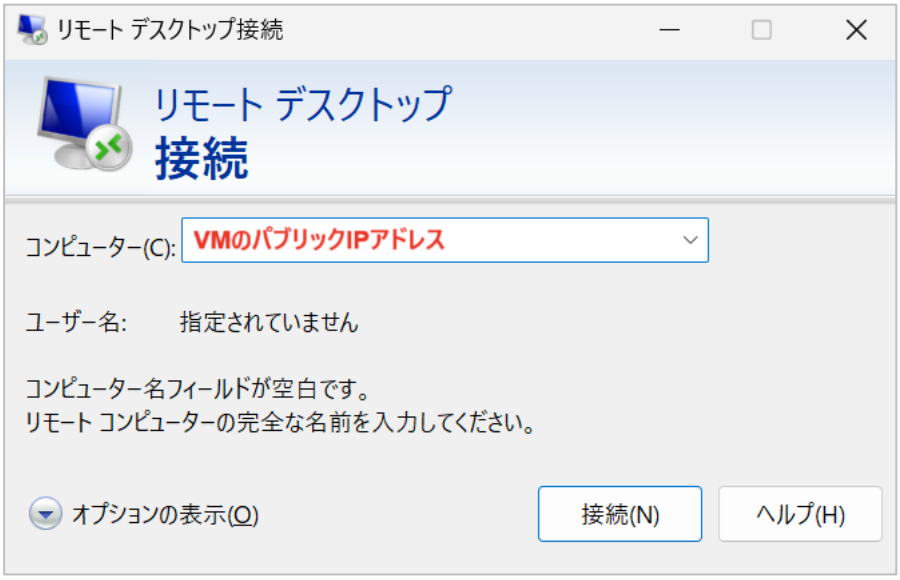
5 [カスタム] 選択し、DNS サーバーに「8.8.8.8」と入力し、[保存] をクリックします。



6 これで Azure portal 側での DNS サーバー設定は完了です。続けて、VM 上での日本語設定をします。

7 作成した VM へ RDP 接続します。

コンピューター	<VM のパブリック IP アドレス>



8 [資格情報] には、VM 作成時に設定した「管理者アカウント」情報を入力します。

9 サインイン後、Powershell にて「ipconfig /all」コマンドを実行し、DNS サーバーに「8.8.8.8」であることを確認します。

10 [スタート] > [設定] の順にクリックします。

11 [Time&Language] > [Language] > [Add a language] の順にクリックします。

12 追加する言語 [Japan] を選択し、[Next] をクリックします。

13 ダウンロード完了後、サインアウトおよび再サインインします。

14 これで日本語化は完了です。次の作業へ進む前に、DNS サーバーを元の値に戻してください。