CLUSTERPRO® X 4.1

Microsoft Azure 向け
HA クラスタ 構築ガイド (Windows 版)

2020.05.13
第2版

改版履歴

版数	改版日付	内 容
1	2019/04/10	新規作成
2	2020/05/13	サポートする OS バージョンに関する説明を追加 2.1 Azure DNS を使用した HA クラスタの場合 2.2 ロードバランサーを使用した HA クラスタの場合

© Copyright NEC Corporation 2019. All rights reserved.

免責事項

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

商標情報

CLUSTERPRO® は、日本電気株式会社の登録商標です。
Microsoft、Windows、Azure、Azure DNS は、米国 Microsoft Corporation の米国およびその他の国における登録商標です。
本書に記載されたその他の製品名および標語は、各社の商標または登録商標です。

目次

はじめに ..... **v**

対象読者と目的 v
適用範囲 v
本書の表記規則 vii
最新情報の入手先 viii

第 1 章 概要 9

1.1 機能概要 9
1.2 基本構成 10
1.3 ネットワークパーティション解決 16
1.4 オンプレミスとMicrosoft Azureの違い 18

第 2 章 動作環境 22

2.1 Azure DNSを使用したHAクラスタの場合 22
2.2 ロードバランサーを使用したHAクラスタの場合 22

第 3 章 構築手順(Azure DNSを使用したHAクラスタの場合) 24

3.1 構築例について 24
3.2 Microsoft Azureの設定 27
3.3 CLUSTERPROの設定 51
3.4 動作確認 68

第 4 章 構築手順(パブリックロードバランサーを使用したHAクラスタの場合) 69

4.1 構築例について 69
4.2 Microsoft Azureの設定 72
4.3 CLUSTERPROの設定 107
4.4 動作確認 126

第 5 章 構築手順(内部ロードバランサーを使用したHAクラスタの場合) 127

5.1 構築例について 127
5.2 Microsoft Azureの設定 130
5.3 CLUSTERPROの設定 160
5.4 動作確認 169

第 6 章 エラーメッセージ一覧 170

第 7 章 注意・制限事項 171

7.1 Azure DNSを使用したHAクラスタの場合 171
7.1.1 Microsoft Azureの注意事項 171
7.1.2 CLUSTERPROの注意事項 171
7.2 ロードバランサーを使用したHAクラスタの場合 172
7.2.1 Microsoft Azureの注意事項 172
7.2.2 CLUSTERPROの注意事項 172

はじめに

対象読者と目的

本書は、クラスタシステムに関して、システムを構築する管理者、およびユーザサポートを行うシステムエンジニア、保守員を対象にしています。
ここでご紹介するソフトウェアや設定例は、あくまで参考情報としてご提供するものであり、各ソフトウェアの動作保証を行うものではありません。

適用範囲

本書では、以下の製品を対象としています。
- CLUSTERPRO X 4.1 for Windows (内部バージョン: 12.10)
- Windows Server 2016 Datacenter
- Microsoft Azure ポータル: 2019/01/16 時点の環境
- Azure CLI 2.0

バージョンが異なる場合、一部の表示や設定内容など異なる可能性がありますので、注意してください。
また、表示や設定内容など今後変更となる可能性があるため、最新の情報については各製品や各サービスの Web サイトやマニュアルを参照してください。

本書の構成

第 1 章	「概要」: 機能の概要について説明します。
第 2 章	「動作環境」: 本機能の動作確認済み環境を説明します。
第 3 章	「構築手順」: Azure DNS を使用した HA クラスタの構築手順について説明します。
第 4 章	「構築手順」: インターネットに接続するパブリックロードバランサーを使用した HA クラスタの構築手順について説明します。
第 5 章	「構築手順」: 内部ロードバランサーを使用した HA クラスタの構築手順について説明します。
第 6 章	「エラーメッセージ一覧」: エラーメッセージと対処について説明します。
第 7 章	「注意・制限事項」: 構築時、運用時の注意事項について説明します。

CLUSTERPRO マニュアル体系

CLUSTERPRO のマニュアルは、以下の 6 つに分類されます。各ガイドのタイトルと役割を以下に示します。

『CLUSTERPRO X スタートアップガイド』(Getting Started Guide)
すべてのユーザを対象読者とし、製品概要、動作環境、アップデート情報、既知の問題などについて記載します。

『CLUSTERPRO X インストール&設定ガイド』(Install and Configuration Guide)
CLUSTERPRO を使用したクラスタシステムの導入を行うシステムエンジニアと、クラスタシステム導入後の保守・運用を行うシステム管理者を対象読者とし、CLUSTERPRO を使用したクラスタシステム導入から運用開始前までに必須の事項について説明します。実際にクラスタシステムを導入する際の順番に則して、CLUSTERPRO を使用したクラスタシステムの設計方法、CLUSTERPRO のインストールと設定手順、設定後の確認、運用開始前の評価方法について説明します。

『CLUSTERPRO X リファレンスガイド』(Reference Guide)
管理者、および CLUSTERPRO を使用したクラスタシステムの導入を行うシステムエンジニアを対象とし、CLUSTERPRO の運用手順、各モジュールの機能説明およびトラブルシューティング情報等を記載します。『インストール&設定ガイド』を補完する役割を持ちます。

『CLUSTERPRO X メンテナンスガイド』(Maintenance Guide)
管理者、および CLUSTERPRO を使用したクラスタシステム導入後の保守・運用を行うシステム管理者を対象読者とし、CLUSTERPRO のメンテナンス関連情報を記載します。

『CLUSTERPRO X ハードウェア連携ガイド』(Hardware Feature Guide)
管理者、および CLUSTERPRO を使用したクラスタシステムの導入を行うシステムエンジニアを対象読者とし、特定ハードウェアと連携する機能について記載します。『インストール&設定ガイド』を補完する役割を持ちます。

『CLUSTERPRO X 互換機能ガイド』(Legacy Feature Guide)
管理者、および CLUSTERPRO を使用したクラスタシステムの導入を行うシステムエンジニアを対象読者とし、CLUSTERPRO X 4.0 WebManager、Builder および CLUSTERPRO Ver 8.0 互換コマンドに関する情報について記載します。

本書の表記規則

本書では、注意すべき事項、重要な事項および関連情報を以下のように表記します。

注: は、重要ではあるがデータ損失やシステムおよび機器の損傷には関連しない情報を表します。

重要: は、データ損失やシステムおよび機器の損傷を回避するために必要な情報を表します。

関連情報: は、参照先の情報の場所を表します。

また、本書では以下の表記法を使用します。

表記	使用方法	例
[ ] 角かっこ	コマンド名の前後 画面に表示される語 (ダイアログボックス、メニューなど) の前後	[スタート] をクリックします。 [プロパティ] ダイアログボックス
コマンドライン中の [ ] 角かっこ	かっこ内の値の指定が省略可能であることを示します。	`clpstat -s[-h host_name]`
>	Windows ユーザが、コマンドプロンプトでコマンドを実行することを示すプロンプト	`> clpstat`
モノスペースフォント (courier)	パス名、コマンドライン、システムからの出力 (メッセージ、プロンプトなど)、ディレクトリ、ファイル名、関数、パラメータ	`C:¥Program Files`
モノスペースフォント**太字** (courier)	ユーザが実際にコマンドラインから入力する値を示します。	以下を入力します。 **`> clpcl -s -a`**
モノスペースフォント斜体 (courier)	ユーザが有効な値に置き換えて入力する項目	**`> ping`** *<IP アドレス>*

最新情報の入手先

最新の製品情報については、以下の Web サイトを参照ください。

https://jpn.nec.com/clusterpro/

第 1 章　概要

1.1 機能概要

本書では、Microsoft Azure のクラウド サービス上に、Azure Resource Manager を使用した CLUSTERPRO X(以下、CLUSTERPRO と記す)による HA クラスタを構築する方法を説明します。

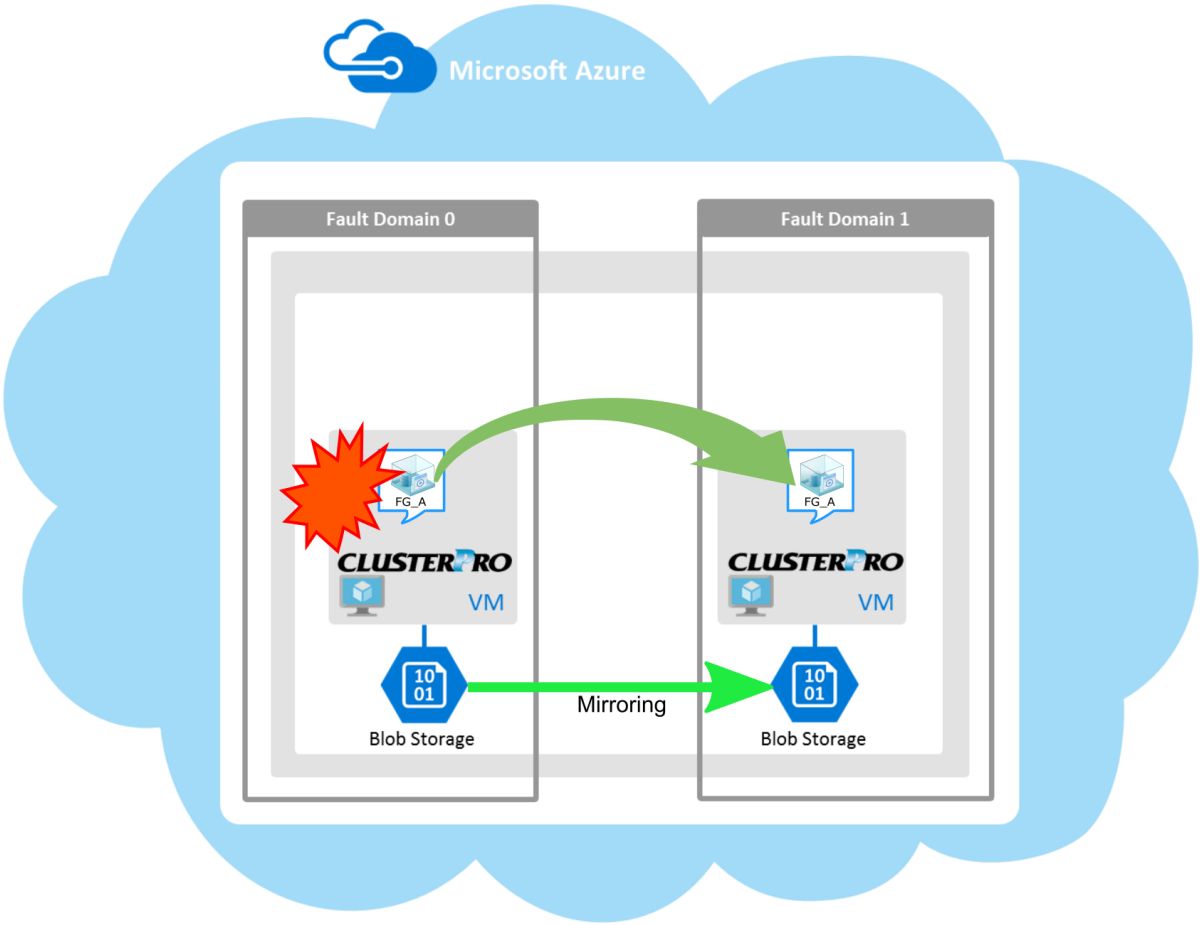


図 1-1 クラウドサービス上のHAクラスタ(Azure DNSを使用した場合)

Microsoft Azure において、Microsoft Azure リージョンや可用性セットを使用し仮想マシン(図 1-1の VM)を HA クラスタ化することで、業務の可用性を高めることができます。

- Microsoft Azure リージョン
  Microsoft Azure リージョンと呼ばれる物理的および論理的な単位に分割されます。
  (たとえば東日本、西日本など) 1つのリージョン内にすべてのノードを構築することも可能ですが、ネットワーク障害や自然災害などによりすべてのノードがダウンし業務を継続できなくなるおそれがあります。
  そこで、ノードを複数のリージョンに分散させて配置することにより、可用性を高めることができます。
- 可用性セット
  Microsoft Azure では、可用性セットと呼ばれる論理的なグループに各ノードを配置できます。可用性セット内に各ノードが配置されることで、Microsoft Azure プラットフォームの計画済みメンテナンスや物理ハードウェアの障害などの計画外メンテナンスによる影響を最小限に抑えることが可能です。本書では、可用性セットを用いた構成の説明をします。
  可用性セットの詳細は、以下の Web サイトを参照してください。
  Azure での Windows 仮想マシンの可用性の管理:
  https://docs.microsoft.com/ja-jp/azure/virtual-machines/windows/manage-availability

1.2 基本構成

本書では、リソースマネージャデプロイモデルにおける Azure DNS を使用した HA クラスタ、リソースマネージャデプロイモデルにおけるロードバランサーを使用した HA クラスタの2種類の HA クラスタを想定しています(いずれも片方向スタンバイクラスタの構成)。それぞれの HA クラスタについて、選択する CLUSTERPRO のリソースは以下のとおりです。

用途	選択する CLUSTERPRO のリソース
DNS 名でクライアントからアクセスしたい場合 (Azure DNS の追加が必要)	Azure DNS リソース
仮想 IP アドレス(グローバル IP アドレス)でクライアントからアクセスしたい場合 (パブリックロードバランサーの追加が必要)	Azure プローブポートリソース
仮想 IP アドレス(プライベート IP アドレス)でクライアントからアクセスしたい場合 (内部ロードバランサーの追加が必要)	Azure プローブポートリソース
仮想 IP アドレス(プライベート IP アドレス)でクライアントからアクセス、かつクラスタ化したアプリケーションが Always On 構成の場合 (内部ロードバランサーの追加および Direct Server Return(以下、DSR と略)の設定が必要)	Azure プローブポートリソース

DSR 構成を作成する場合は以下を参照してください。
https://jpn.nec.com/clusterpro/blog/20181031.html

Azure DNS を使用した HA クラスタ

本構成では、同一の DNS 名でクラスタへアクセスできるよう、2台の仮想マシンが同じリソース グループに属しています。DNS 名でアクセス可能とするために CLUSTERPRO の Azure DNS リソースは、Azure DNS を使用しています。Azure DNS の詳細は以下の Web サイトを参照してください。
Azure DNS: https://docs.microsoft.com/ja-jp/azure/dns/dns-overview

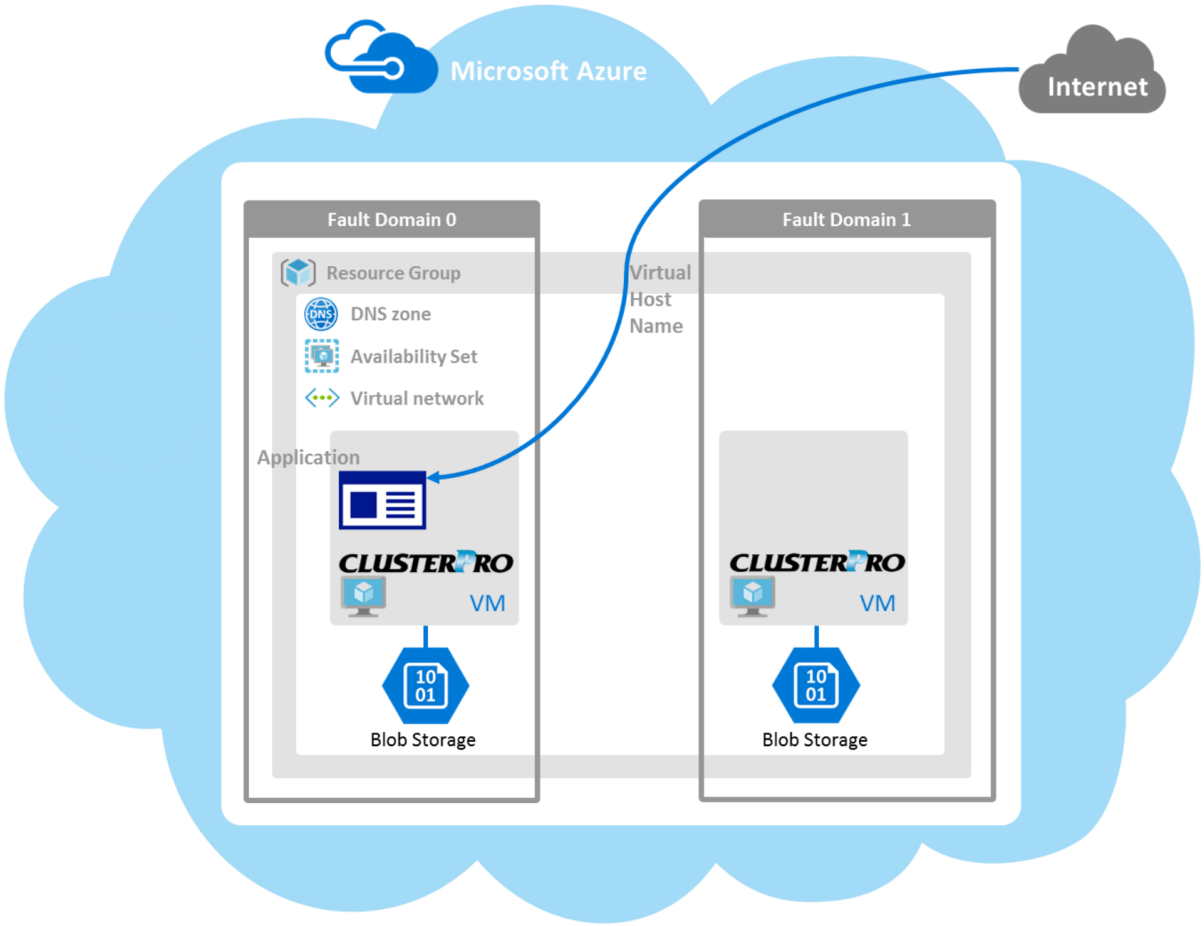


図 1-2 Azure DNSを使用したHAクラスタ

また、Microsoft Azure プラットフォームの計画済みメンテナンスや物理ハードウェアの障害などの計画外メンテナンスによる影響を最小限に抑えるために、2台の仮想マシンで同じ可用性セットを使用しています。図 1-2のクラスタには、Azure DNS ゾーンにおける DNS 名を指定してアクセスします。CLUSTERPRO は、DNS 名から設定した IP アドレスが得られるように Azure DNS ゾーンのレコードセットや DNS A レコードの制御を行います。フェイルオーバまたはグループの移動が発生しても、クライアントは仮想マシンの切り替えを意識する必要がありません。

Azure DNS を使用した HA クラスタ構成において必要なリソース、監視リソースは以下のとおりです。

リソース/監視リソース種別	説明	設定
Azure DNS リソース	DNS 名から設定した IP アドレスを得られるように Azure DNS のレコードセット(A レコード)の制御を行います。	必須
Azure DNS 監視リソース	Azure DNS のレコードセットに対する名前解決結果が正常であることを監視します。	必須
IP 監視リソース	Microsoft Azure の Service Management API へ疎通可能かどうかを監視し、外部ネットワークとの通信の健全性を監視します。	パブリックロードバランサーを使用する場合、かつ仮想マシンで構成されたクラスタ間の通信を監視し、内部ネットワークとの通信の健全性監視が必要な場合に必須
カスタム監視リソース	仮想マシンで構成されたクラスタ間の通信を監視し、内部ネットワークとの通信の健全性を監視します。	パブリックロードバランサーを使用する場合、かつ Microsoft Azure の Service Management API へ疎通可能かどうかを監視し、外部ネットワークとの通信の健全性監視が必要な場合に必須
マルチターゲット監視リソース	上記のIP監視リソースとカスタム監視リソースの両方の状態を監視します。両方の監視リソースの状態が異常となった際に、ネットワークパーティション解決(以下、NP 解決と記す)用の処理を記載したスクリプトを実行します。	パブリックロードバランサーを使用する場合、かつ内部ネットワークと外部ネットワークとの通信の健全性監視が必要な場合に必須
その他のリソース、監視リソース	ミラーディスクなど、HA クラスタで運用するアプリケーションの構成に従います。	任意

ロードバランサーを使用した HA クラスタ

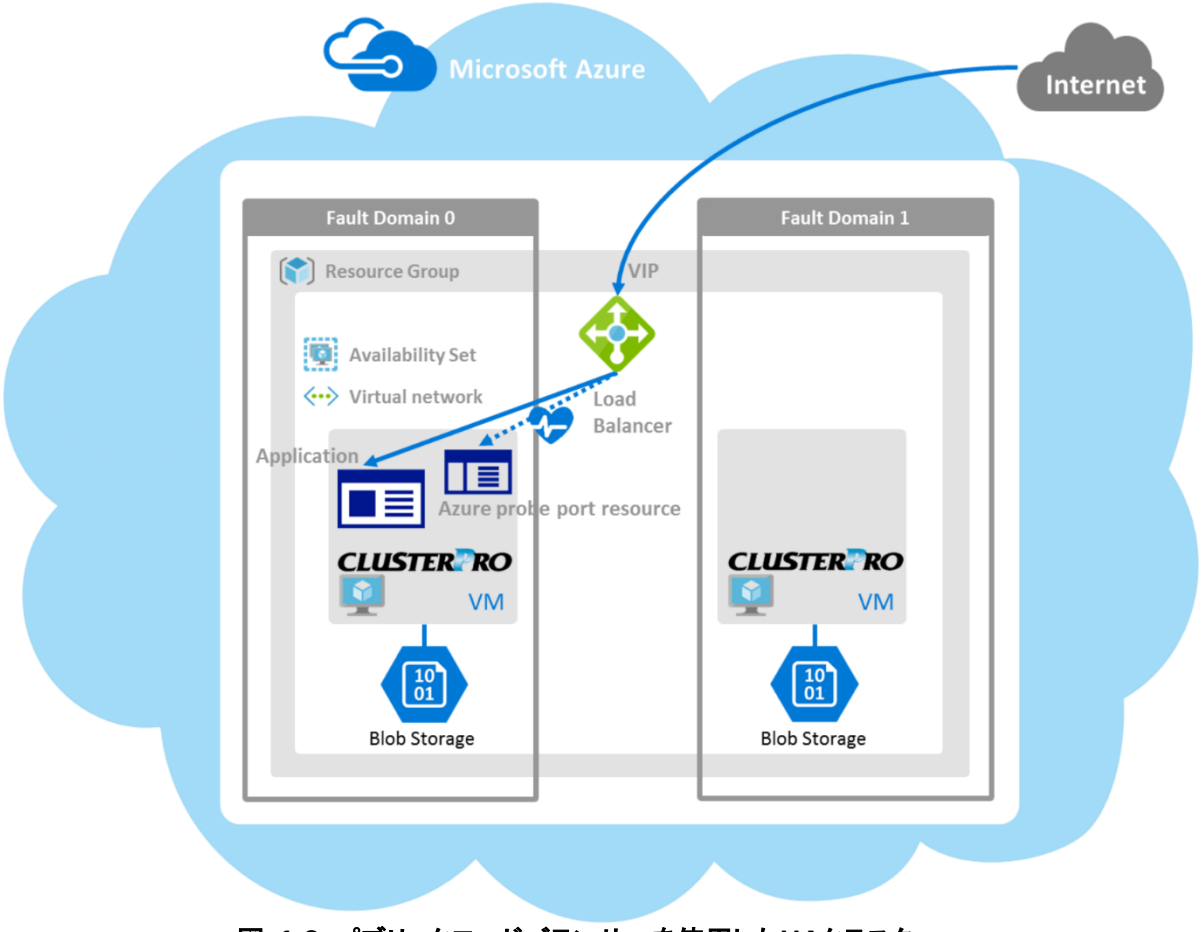


図 1-3 パブリックロードバランサーを使用したHAクラスタ

クライアントアプリケーションは、Microsoft Azure 環境の可用性セット上の仮想マシンに対して、フロントエンドの IP アドレスを使用してクラスタノードに接続することができます。VIP アドレスを使用することにより、フェイルオーバまたはグループの移動が発生しても、クライアントは仮想マシンの切り替えを意識する必要がありません。

図1-3の Microsoft Azure 環境上に構築したクラスタには、Microsoft Azure のロードバランサー(図 1-3の Load Balancer)のグローバルな IP アドレスを指定してアクセスします。
クラスタの現用系と待機系は、Microsoft Azure のロードバランサーにおけるプローブを利用して切り替えます。利用には CLUSTERPRO Azure プローブポートリソースが提供するプローブ ポートを利用します。
Azure プローブポートリソースの活性時に Microsoft Azure のロードバランサーからの死活監視(プローブポートへのアクセス)を待ち受けるためのプローブポート制御プロセスを起動します。
Azure プローブポートリソースの非活性時には死活監視(プローブ ポートへのアクセス)を待ち受けるためのプローブポート制御プロセスを停止します。

Azure プローブポートリソースでは Microsoft Azure の内部ロードバランサー(Internal Load Balancing。以下、ILB と記す)にも対応しています。内部ロードバランサーの場合、VIP は Microsoft Azure のプライベート IP アドレスとなります。

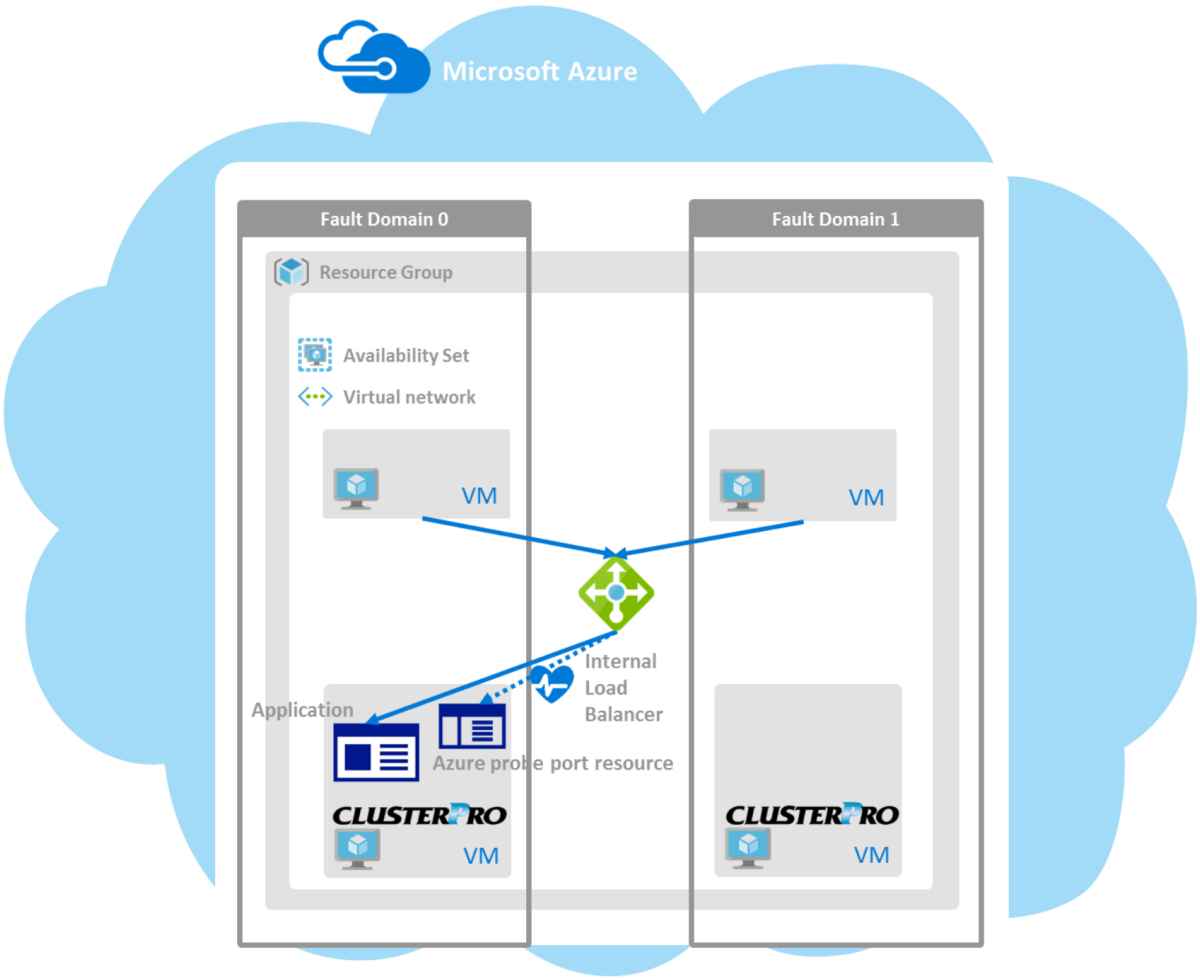


図 1-4 内部ロードバランサーを使用したHAクラスタ

ロードバランサーを使用した HA クラスタの構成例としては以下の2種類があります。用途に応じて使用するロードバランサーを決定してください。

用途	使用するロードバランサー	構築手順
業務を Microsoft Azure のネットワークの外部に公開する場合	パブリックロードバランサー	本書「第 4 章 構築手順(パブリックロードバランサーを使用した HA クラスタの場合)」参照。
業務を Microsoft Azure のネットワークの内部に公開する場合	内部ロードバランサー(ILB)	本書「第 5 章 構築手順(内部ロードバランサーを使用したHAクラスタの場合)」参照。

ロードバランサーを使用したHAクラスタ構成において必要なリソース、監視リソースは以下のとおりです。

リソース/監視リソース種別	説明	設定
Azure プローブポートリソース	業務が稼働するノードの特定のポートでロードバランサーからの死活監視を待ち受ける仕組みを提供します。	必須
Azure プローブポート監視リソース	Azure プローブポートリソースが起動しているノードに対して、Azure プローブポートリソース活性時に起動するプローブポート制御プロセスの死活監視を行います。	必須
Azure ロードバランス監視リソース	Azure プローブポートリソースが起動していないノードに対して、プローブポートと同じポート番号が開放されていないかを監視します。	必須
IP 監視リソース	Microsoft Azure の Service Management API へ疎通可能かどうかを監視し、外部ネットワークとの通信の健全性を監視します。	パブリックロードバランサーを使用する場合、かつ仮想マシンで構成されたクラスタ間の通信を監視し、内部ネットワークとの通信の健全性監視が必要な場合に必須
カスタム監視リソース	仮想マシンで構成されたクラスタ間の通信を監視し、内部ネットワークとの通信の健全性を監視します。	パブリックロードバランサーを使用する場合、かつ Microsoft Azure の Service Management API へ疎通可能かどうかを監視し、外部ネットワークとの通信の健全性監視が必要な場合に必須
マルチターゲット監視リソース	上記のIP監視リソースとカスタム監視リソースの両方の状態を監視します。両方の監視リソースの状態が異常となった際に、ネットワークパーティション解決用の処理を記載したスクリプトを実行します。	パブリックロードバランサーを使用する場合、かつ内部ネットワークと外部ネットワークとの通信の健全性監視が必要な場合に必須
PING ネットワークパーティション解決リソース	内部ロードバランサー(ILB)を使用する場合、Ping などの応答を返却可能な常時稼働している装置(以下、応答確認先と記す)への通信可否を確認することで、サブネット間通信の健全性を監視します。	内部ロードバランサー(ILB)を使用する場合、かつサブネット間通信の健全性監視が必要な場合に必須
その他のリソース、監視リソース	ミラーディスクなど、HA クラスタで運用するアプリケーションの構成に従います。	任意

1.3 ネットワークパーティション解決

HA クラスタを構成している仮想マシンは、お互いにハートビートによって死活監視を行っています。各仮想マシンが異なるサブネットに分散している構成においては、ハートビートが途絶えた時に、サービスの二重起動など望ましくない状態が発生します。サービスの二重起動を回避するために、他の仮想マシンがダウンしたか、自身がネットワークから孤立した状態(ネットワークパーティション状態。以下、NP 状態と記す)かのどちらであるかを区別する必要があります。

ネットワークパーティション解決(以下、NP 解決と記す)は、Ping などの応答を返却可能な常時稼働している装置(応答確認先)に対して Ping や LISTEN ポート確認を行い、応答がない場合は NP 状態が発生したと判断し、設定された処理(警告、回復処理、サーバダウン処理など)を行います。

応答確認先は、Microsoft Azure においては通常以下を使用します。
(※)内部ロードバランサー(ILB)のプライベート IP アドレスは Ping に応答しないため、利用できません。

業務の公開範囲	応答確認先	手段	各手段のために使用する CLUSTERPROのリソース/監視リソース/コマンド
Microsoft Azure 仮想ネットワークの外部	Microsoft Azure サービス管理 API (management.core.windows.net)	LISTEN ポート確認	・カスタム監視リソース ・clpazure_port_checker コマンド
	各クラスタサーバ	Ping	・IP 監視リソース
Microsoft Azure 仮想ネットワークの内部	Microsoft Azure 仮想ネットワークの内部に存在する、クラスタサーバ以外のサーバ(※)	Ping	・PING ネットワークパーティション解決リソース
	Microsoft Azure 仮想ネットワークの内部に存在する Web サーバ	HTTP	・HTTP ネットワークパーティション解決リソース

NP 解決の詳細については、以下のマニュアルを参照してください。

- 『リファレンスガイド』-「第 5 章 ネットワークパーティション解決リソースの詳細」

NP解決先の設定について

クラスタシステムにアクセスするクライアントの配置やオンプレミス環境との接続条件(専用線接続など)によって、NP 解決先や NP 解決の方法は、その都度検討する必要があります。

ネットワークパーティション状態の判定をするには

指定した TCP ポートの LISTEN 状態を確認可能な clpazure_port_checker コマンドを提供しています。カスタム監視リソースやマルチターゲット監視リソースの[この製品で作成したスクリプト] にて使用してください。
clpazure_port_checker コマンドの詳細については、以下を参照してください。

TCP ポートの LISTEN 状態を確認する (clpazure_port_checker コマンド)

clpazure_port_checker　指定したサーバのTCPポートについて、 LISTEN の有無を確認します。

コマンドライン

clpazure_port_checker -h *hostname* -p *port*

説明

本コマンドは、引数で指定されたサーバの TCP ポートについて、LISTEN の有無を確認します。

5 秒(固定)経過しても応答がない場合は異常と判定します(タイムアウト)。

異常の場合は、標準エラー出力にエラーメッセージを出力します。

本コマンドをカスタム監視リソースより実行することで、ネットワークパーティション状態の判定を行うことが可能です。

本コマンドを用いたネットワークパーティション解決の設定例については、「3.3 CLUSTERPRO の設定」、「5.3 CLUSTERPRO の設定」を参照してください。

オプション

-h *hostname*	判定するサーバを *hostname* で指定します(FQDN 名もしくは IP アドレス)。省略できません。
-p *port*	判定するポート番号を*port*で指定します(ポート番号もしくはサービス名)。省略できません。

戻り値

0	正常
1	異常(通信エラー)
2	異常(タイムアウト)
3	異常(引数不正、内部エラー)

1.4 オンプレミスと Microsoft Azure の違い

オンプレミスと Microsoft Azure における CLUSTERPRO の機能差分は以下のとおりです。表内の〇は機能が使用できることを意味し、×は機能が使用できないことを意味します。

機能	オンプレミス	Microsoft Azure
共有ディスク型クラスタの構築可否	〇	×
ミラーディスク型クラスタの構築可否	〇	〇
ハイブリッドディスク型クラスタの構築可否	〇	×
フローティング IP リソースの使用可否	〇	×
仮想 IP リソースの使用可否	〇	×
Azure プローブポートリソースの使用可否	×	〇
Azure DNS リソースの使用可否	×	〇

オンプレミスと Microsoft Azure における、ミラーディスクを使用した2ノードクラスタの構築手順の流れは以下を参照してください。
オンプレミス環境と Microsoft Azure 環境でクラスタを構築する作業手順の違いは、事前準備として Microsoft Azure の設定が必要であることを除き、違いはありません。

Azure DNS を使用した HA クラスタ

Microsoft Azure 上では、下記表における項番1～7は Microsoft Azure ポータル (https://portal.azure.com/)にログインし、作業を行ってください。
Microsoft Azure 上では、下記表における項番8～17は、作成した各仮想マシンにログインし、作業を行ってください。

項番	手順	オンプレミス	Microsoft Azure
CLUSTERPRO インストール前			
1	リソース グループの作成	不要	本書「3.2 Microsoft Azure の設定」を参照。
2	仮想ネットワークの作成	不要	本書「3.2 Microsoft Azure の設定」を参照。
3	仮想マシンの作成	不要	本書「3.2 Microsoft Azure の設定」を参照。
4	プライベート IP アドレスの設定	不要	本書「3.2 Microsoft Azure の設定」を参照。
5	Blob の追加	不要	本書「3.2 Microsoft Azure の設定」を参照。
6	DNS ゾーンの作成	不要	本書「3.2 Microsoft Azure の設定」を参照。
7	DNS サーバの設定	OS や DNS サーバのマニュアルを参照。	不要
8	ミラーディスクリソース用のパーティションを設定	以下を参照。 ・『インストール&設定ガイド』-「第 1 章 システム構成を決定する」-「ハードウェア構成後の設定」 ・『リファレンスガイド』-「ミラーディスクリソースを理解する」	本書「3.2 Microsoft Azure の設定」を参照。
9	OS 起動時間の調整	『インストール&設定ガイド』-「第 1 章 システム構成を決定する」-「ハードウェア構成後の設定」参照	オンプレミスと同様
10	ネットワーク設定の確認		
11	ファイアウォールの設定を確認		

12	サーバの時刻を同期		
13	パワーセービング機能をオフ		
14	Azure CLI のインストール	不要	本書「3.2 Microsoft Azure の設定」を参照。
15	サービス プリンシパルの登録	不要	本書「3.2 Microsoft Azure の設定」を参照。
16	CLUSTERPRO のインストール	『インストール&設定ガイド』-「第 3 章 CLUSTERPRO をインストールする」参照	オンプレミスと同様
CLUSTERPRO インストール後			
17	CLUSTERPRO のライセンスを登録	『インストール&設定ガイド』-「第 4 章 ライセンスを登録する」参照	オンプレミスと同様
18	クラスタの作成-ハートビート方式の設定	『インストール&設定ガイド』-「5 章 クラスタ構成情報を作成する」-「クラスタ構成情報の作成手順」参照。	COM ハートビート、BMC ハートビート、ディスクハートビートは使用できません。
19	クラスタの作成-NP 解決処理の設定	ネットワークパーティション解決リソースを使用。 以下を参照。 ・『インストール&設定ガイド』-「第 5 章 クラスタ構成情報を作成する」-「クラスタ構成情報の作成手順」 ・『リファレンスガイド』-「第 5 章 ネットワークパーティション解決リソースの詳細」	本書「3.3 CLUSTERPRO の設定」を参照。
20	クラスタの作成-フェイルオーバグループの作成、監視リソースの作成	『インストール&設定ガイド』-「第 5 章 クラスタ構成情報を作成する」-「クラスタ構成情報の作成手順」参照	オンプレミスに加え、以下を参照。 ・『リファレンスガイド』-「Azure DNS リソースを理解する」 ・『リファレンスガイド』-「Azure DNS 監視リソースを理解する」 ・本書「3.3 CLUSTERPRO の設定」

ロードバランサーを使用した HA クラスタ

Microsoft Azure 上では、下記表における項番1～5、7～8は Microsoft Azure ポータル (https://portal.azure.com/)にログインし、作業を行ってください。
Microsoft Azure 上では、下記表における項番6、9～15は、作成した各仮想マシンにログインし、作業を行ってください。

項番	手順	オンプレミス	Microsoft Azure
CLUSTERPRO インストール前			
1	リソース グループの作成	不要	使用するロードバランサーにより以下のいずれかを参照。 ・本書「4.2 Microsoft Azure の設定」 ・本書「5.2 Microsoft Azure の設定」
2	仮想ネットワークの作成	不要	使用するロードバランサーにより以下のいずれかを参照。 ・本書「4.2 Microsoft Azure の設定」 ・本書「5.2 Microsoft Azure の設定」
3	仮想マシンの作成	不要	使用するロードバランサーにより以下のいずれかを参照。 ・本書「4.2 Microsoft Azure の設定」 ・本書「5.2 Microsoft Azure の設定」
4	プライベート IP アドレスの設定	不要	使用するロードバランサーにより以下のいずれかを参照。 ・本書「4.2 Microsoft Azure の設定」 ・本書「5.2 Microsoft Azure の設定」
5	Blob の追加	不要	使用するロードバランサーにより以下のいずれかを参照。 ・本書「4.2 Microsoft Azure の設定」 ・本書「5.2 Microsoft Azure の設定」
6	ミラーディスクリソース用のパーティションを設定	以下を参照。 ・『インストール&設定ガイド』-「第 1 章 システム構成を決定する」-「ハードウェア構成後の設定」 ・『リファレンスガイド』-「ミラーディスクリソースを理解する」	使用するロードバランサーにより以下のいずれかを参照。 ・本書「4.2 Microsoft Azure の設定」 ・本書「5.2 Microsoft Azure の設定」
7	ロードバランサーの作成・設定	不要	使用するロードバランサーにより以下のいずれかを参照。 ・本書「4.2 Microsoft Azure の設定」 ・本書「5.2 Microsoft Azure の設定」
8	受信セキュリティ規則の設定	不要	・本書「4.2 Microsoft Azure の設定」

9	OS 起動時間の調整	『インストール&設定ガイド』-「第 1 章 システム構成を決定する」-「ハードウェア構成後の設定」参照	オンプレミスと同様
10	ネットワーク設定の確認		
11	ファイアウォールの設定を確認		
12	サーバの時刻を同期		
13	パワーセービング機能をオフ		
14	CLUSTERPRO のインストール	『インストール&設定ガイド』-「第 3 章 CLUSTERPRO をインストールする」参照	オンプレミスと同様
CLUSTERPRO インストール後			
15	CLUSTERPRO のライセンスを登録	『インストール&設定ガイド』-「第 4 章 ライセンスを登録する」参照	オンプレミスと同様
16	クラスタの作成-ハートビート方式の設定	『インストール&設定ガイド』-「5 章 クラスタ構成情報を作成する」-「クラスタ構成情報の作成手順」参照。	COM ハートビート、BMC ハートビート、ディスクハートビートは使用できません。
17	クラスタの作成-NP 解決処理の設定	ネットワークパーティション解決リソースを使用。 以下を参照。 ・『インストール&設定ガイド』-「第 5 章 クラスタ構成情報を作成する」-「クラスタ構成情報の作成手順」 ・『リファレンスガイド』-「第 5 章 ネットワークパーティション解決リソースの詳細」	使用するロードバランサーにより以下のいずれかを参照。 ・本書「4.3 CLUSTERPRO の設定」 ・本書「5.3 CLUSTERPRO の設定」
18	クラスタの作成-フェイルオーバグループの作成、監視リソースの作成	『インストール&設定ガイド』-「第 5 章 クラスタ構成情報を作成する」-「クラスタ構成情報の作成手順」参照	オンプレミスに加え、以下を参照。 ・『リファレンスガイド』-「Azure プローブポートリソースを理解する」 ・『リファレンスガイド』-「Azure プローブポート監視リソースを理解する」 ・『リファレンスガイド』-「Azure ロードバランス監視リソースを理解する」 使用するロードバランサーにより以下のいずれかを参照。 ・本書「4.3 CLUSTERPRO の設定」 ・本書「5.3 CLUSTERPRO の設定」

第 2 章　動作環境

2.1 Azure DNS を使用した HA クラスタの場合

以下のマニュアルを参照してください。以下のマニュアルに記載している OS バージョンをサポートします。

- 『スタートアップガイド』-「第 3 章 CLUSTERPRO の動作環境」-「Azure DNS リソース、Azure DNS 監視リソースの動作環境」

本書は以下の構成で動作確認済みです。
本書は以下の構成を前提に記載していますが、CLUSTERPRO X 4.1 において Azure がサポートしている OS バージョンであれば同様の手順で利用することが可能です。OS バージョンにより手順が異なる場合は、読み替えてください。また、Microsoft Azure ポータル、Azure CLI の差分により手順が異なる場合も、同様に読み替えてください。

x86_64

OS	Windows Server 2016 DataCenter
CLUSTERPRO	CLUSTERPRO X 4.1 for Windows(内部バージョン 12.10)
Microsoft Azure デプロイモデル	リソースマネージャー
場所	東日本
ミラーディスクサイズ	ディスクサイズ：20GB (クラスタパーティション：1GB、データパーティション：19GB)
Azure CLI	2.0
Python	2.7

Azure DNS リソースが利用するため、Azure CLI および Python のインストールが必要です。
Python は、Azure CLI 2.0をインストールすると同時にインストールされます。Azure CLI の詳細については、以下の Web サイトを参照してください。
Azure CLI の概要:
https://docs.microsoft.com/ja-jp/cli/azure/get-started-with-azure-cli

Azure DNS リソースが利用するため、Azure DNS のサービスが必要です。Azure DNS の詳細については、以下の Web サイトを参照してください。
Azure DNS: https://docs.microsoft.com/ja-jp/azure/dns/dns-overview

2.2 ロードバランサーを使用した HA クラスタの場合

以下のマニュアルを参照してください。以下のマニュアルに記載している OS バージョンをサポートします。

- 『スタートアップガイド』-「第 3 章 CLUSTERPRO の動作環境」-「Azure プローブポートリソース、Azure プローブポート監視リソース、Azure ロードバランス監視リソースの動作環境」

本書は以下の構成を前提に記載していますが、CLUSTERPRO X 4.1 において Azure がサポートしている OS バージョンであれば同様の手順で利用することが可能です。OS バージョンにより手順が異なる場合は、読み替えてください。また、Microsoft Azure ポータルの差分により手順が異なる場合も、同様に読み替えてください。

x86_64

OS	Windows Server 2016 DataCenter
CLUSTERPRO	CLUSTERPRO X 4.1 for Windows(内部バージョン 12.10)
Microsoft Azure デプロイモデル	リソースマネージャー
場所	東日本
ミラーディスクサイズ	ディスクサイズ:20GB (クラスタパーティション:1GB、データパーティション:19GB)

第 3 章　構築手順(Azure DNS を使用した HA クラスタの場合)

3.1 構築例について

本書では、Microsoft Azure において、CLUSTERPRO を使用した2ノードでの片方向スタンバイクラスタの構築手順を紹介します。本手順は、node-1 を現用系サーバとしたミラーディスク型の構成を対象としています。
以下の表は既定値が存在しないパラメータ、および既定値から変更したパラメータについて記載しています。

- Microsoft Azureの設定(node-1、node-2で共通の設定)

設定項目	設定値
リソース グループの設定	
名前	TestGroup1
リソース グループの場所	東日本
仮想ネットワークの設定	
名前	Vnet1
アドレス空間	10.5.0.0/24
サブネット名	Vnet1-1
サブネットアドレス範囲	10.5.0.0/24
リソース グループ名	TestGroup1
場所	東日本
DNSゾーンの設定	
名前	cluster1.zone
リソースグループ	TestGroup1
リソースグループの場所	東日本
レコードセット	test-record1

- Microsoft Azureの設定(node-1、node-2でそれぞれ設定)

設定項目	設定値	
	node-1	node-2
仮想マシンの設定		
ディスクの種類	Standard HDD	
ユーザー名	testlogin	
パスワード	PassWord_123	
リソース グループ名	TestGroup1	
場所	東日本	
ネットワーク セキュリティ グループの設定		
名前	NetSecGroup-1	
可用性セットの設定		
名前	AvailabilitySet-1	
更新ドメイン	5	
障害ドメイン	2	
診断ストレージアカウントの設定		
名前	自動生成(testgroup1diag679)	
レプリケーション	ローカル冗長ストレージ(LRS)	
IP構成の設定		
IPアドレス	10.5.0.120	10.5.0.121
Blobの設定		
名前	node-1Blob1	node-2Blob1

ソースの種類	なし(空のディスク)
アカウントの種類	Standard HDD
サイズ	20

- CLUSTERPROの設定(クラスタプロパティ)

設定項目	設定値	
	node-1	node-2
クラスタ名	Cluster1	
サーバ名	node-1	node-2
タイムアウトタブ - ハートビートタイムアウト	210	

- CLUSTERPROの設定(フェイルオーバグループ)

リソース名	設定項目	設定値
ミラーディスクリソース	リソース名	md
	詳細タブ - データパーティションのドライブ名	G:
	詳細タブ - クラスタパーティションのドライブ名	F:
Azure DNSリソース	リソース名	azuredns1
	レコードセット名	test-record1
	ゾーン名	cluster1.zone
	IPアドレス	(node-1の場合)10.5.0.120 (node-2の場合)10.5.0.121
	リソースグループ名	TestGroup1
	ユーザURI	http://azure-test
	テナントID	xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
	サービスプリンシパルのファイルパス	C:¥Users¥testlogin¥examplecert.pem
	Azure CLI ファイルパス	C:¥Program Files (x86)¥Microsoft SDKs¥Azure¥CLI2¥wbin¥az.cmd

- CLUSTERPROの設定(監視リソース)

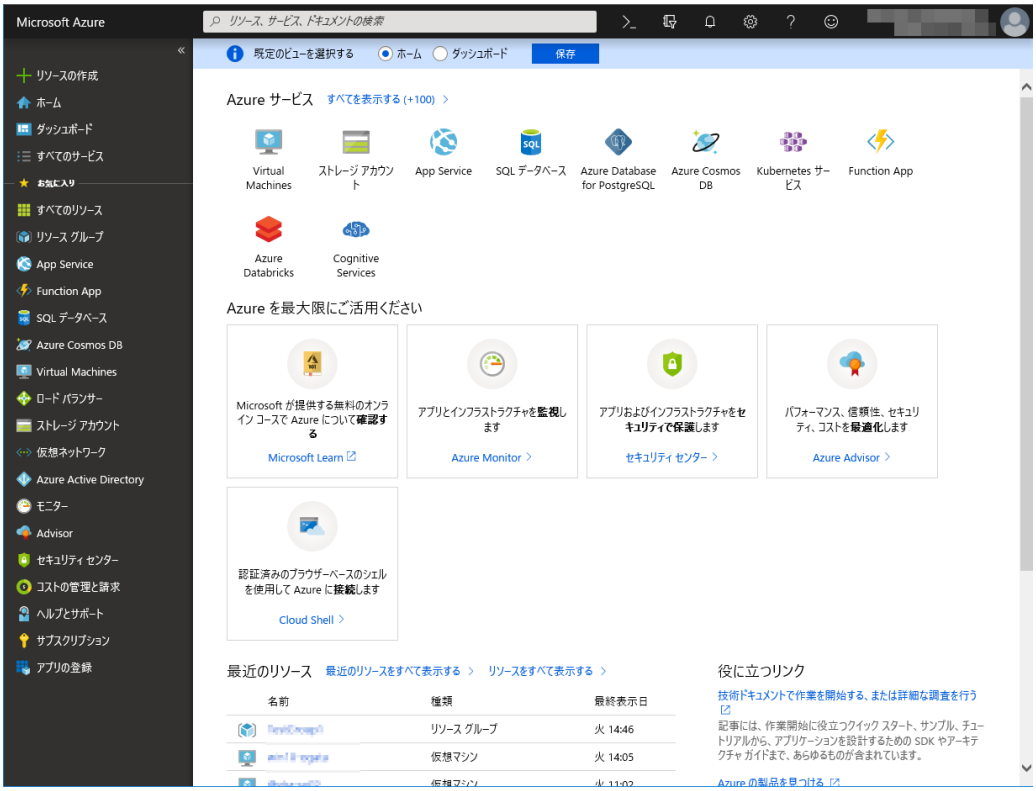
監視リソース名	設定項目	設定値
ミラーディスク監視リソース	－	－
Azure DNS 監視リソース	モニタリソース名	azurednsw1
カスタム監視リソース	監視リソース名	genw1
	この製品で作成したスクリプト	オン
	監視タイプ	同期
	正常な戻り値	0
	回復動作	最終動作のみ実行
	回復対象	LocalServer
IP監視リソース	監視リソース名	ipw1
	監視を行うサーバ	node-1
	IPアドレス	10.5.0.121
	回復動作	最終動作のみ実行
	回復対象	LocalServer
IP監視リソース	監視リソース名	ipw2
	監視を行うサーバ	node-2
	IPアドレス	10.5.0.120
	回復動作	最終動作のみ実行
	回復対象	LocalServer
マルチターゲット監視リソース	監視リソース名	mtw1
	監視リソース一覧	genw1 ipw1 ipw2
	回復動作	クラスタサービス停止とOSシャットダウン
	回復対象	LocalServer

3.2 Microsoft Azure の設定

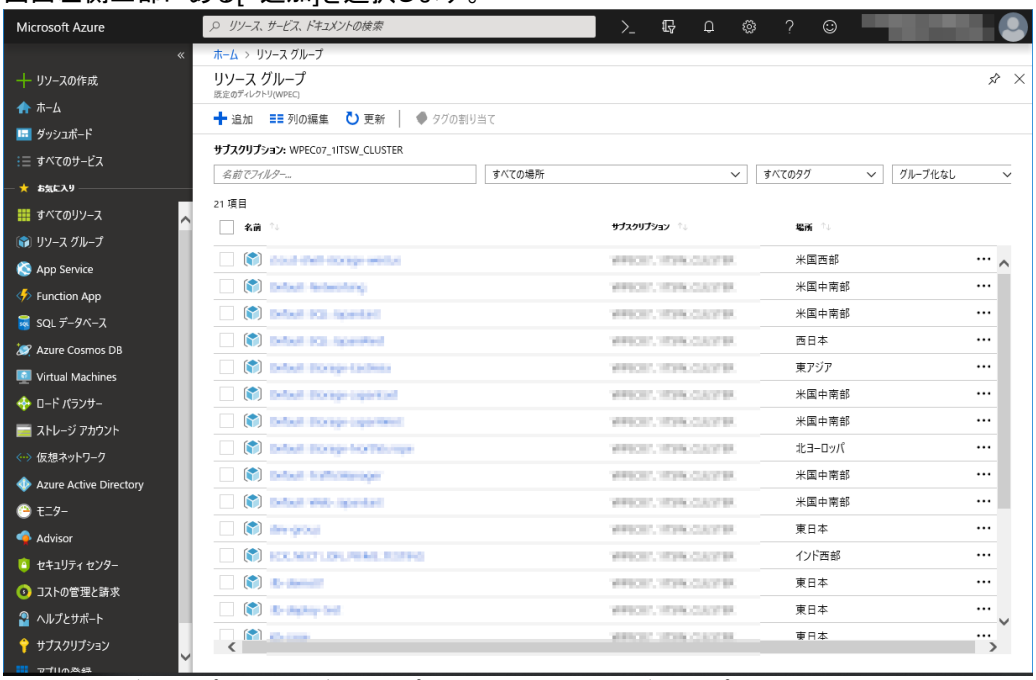
1) リソースグループの作成

Microsoft Azure ポータル(https://portal.azure.com/)にログインし、以下の手順でリソース グループを作成します。

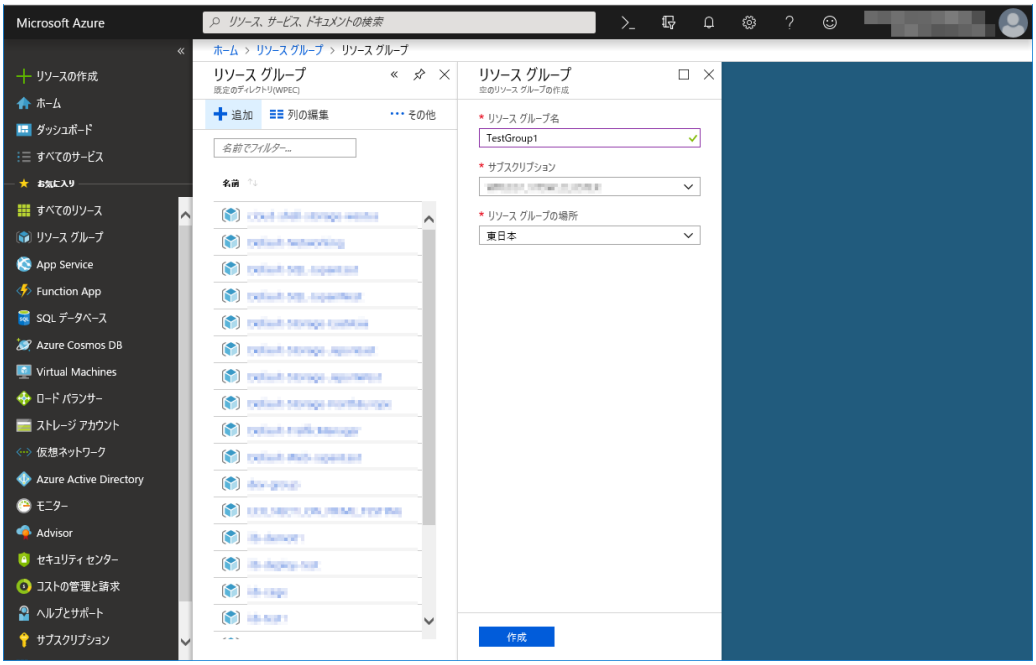
1. 画面左側のメニューにある[リソース グループ]もしくはリソース グループアイコンを選択します。既存のリソース グループがあれば、一覧に表示されます。



2. 画面左側上部にある[+追加]を選択します。



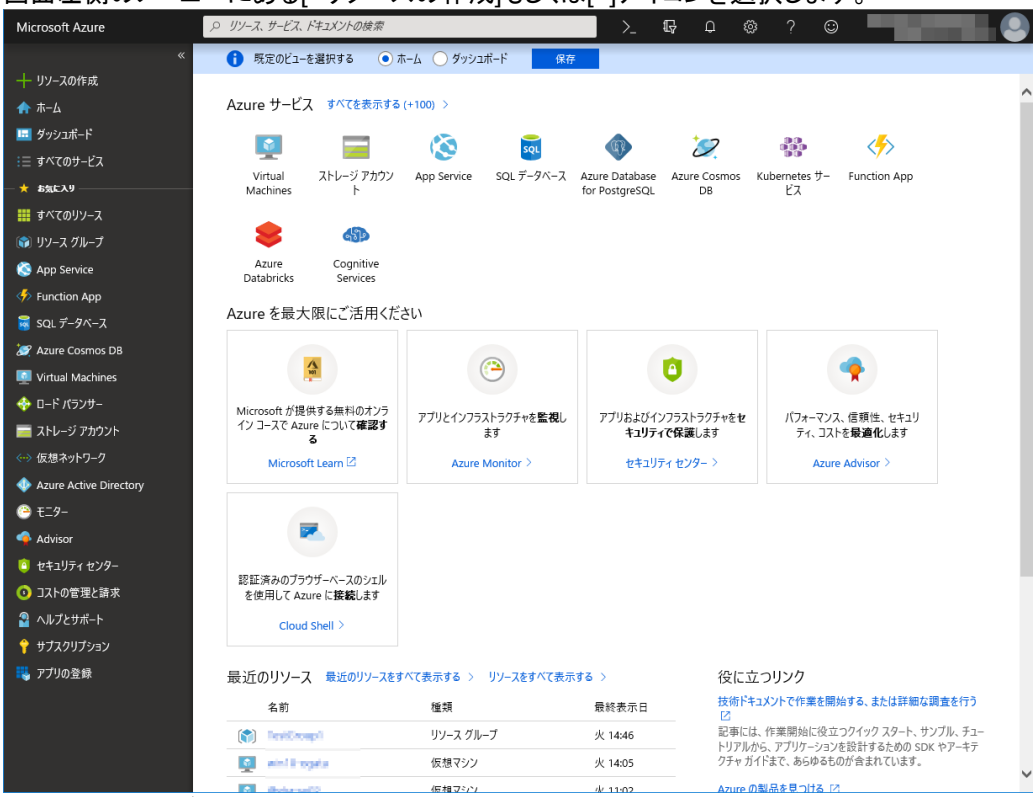
3. [リソース グループ名]、[サブスクリプション]、[リソース グループの場所]を設定し、[作成]を選択します。



2) 仮想ネットワークの作成

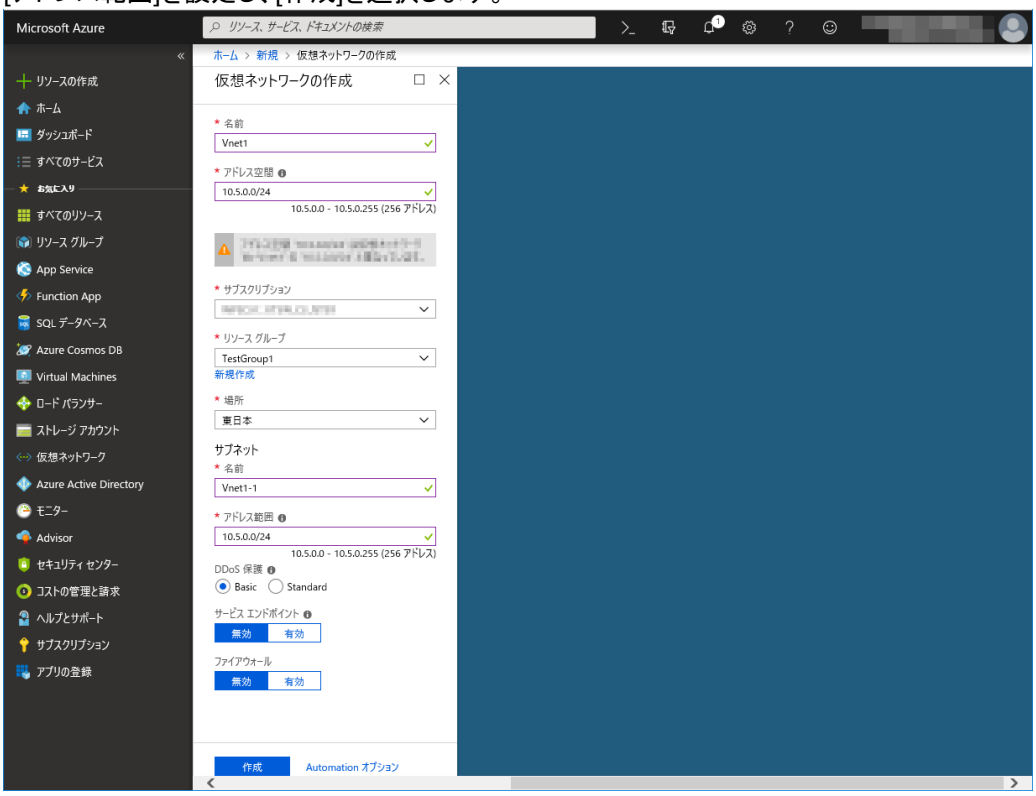
Microsoft Azure ポータル(https://portal.azure.com/)にログインし、以下の手順で仮想ネットワークを作成します。

1. 画面左側のメニューにある[+リソースの作成]もしくは[+]アイコンを選択します。



2. [ネットワーキング]>[仮想ネットワーク]を選択します。

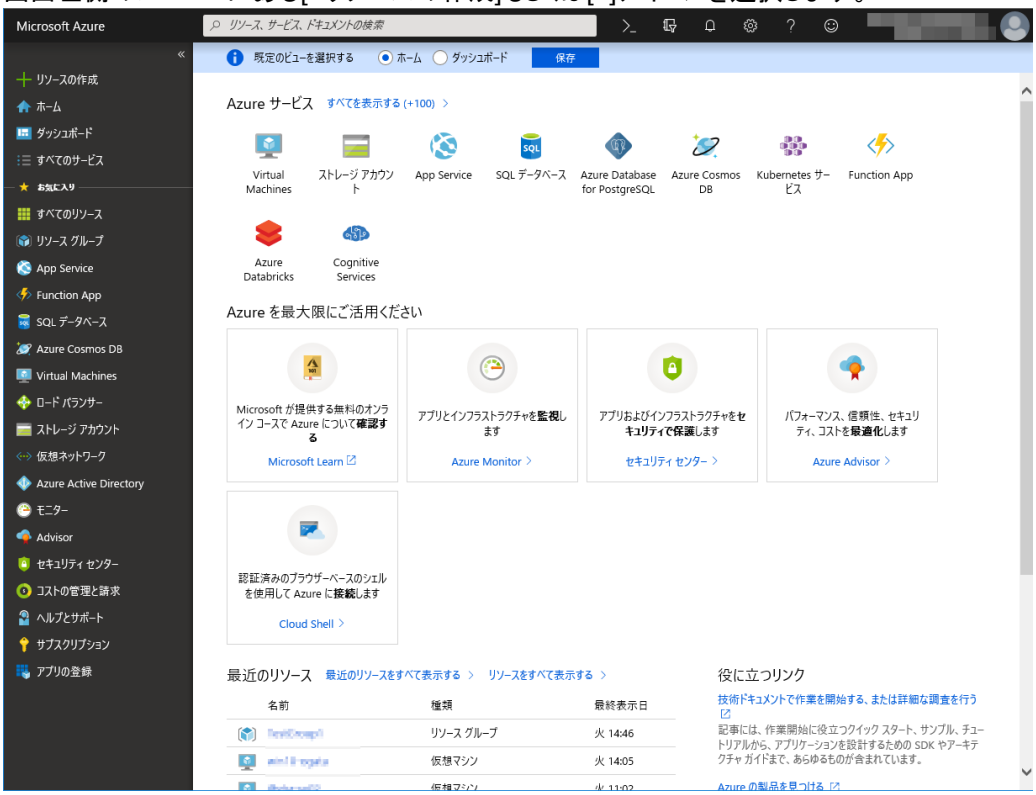
3. [名前]、[アドレス空間]、[サブスクリプション]、[リソース グループ名]、[場所]、サブネットの[名前]、[アドレス範囲]を設定し、[作成]を選択します。



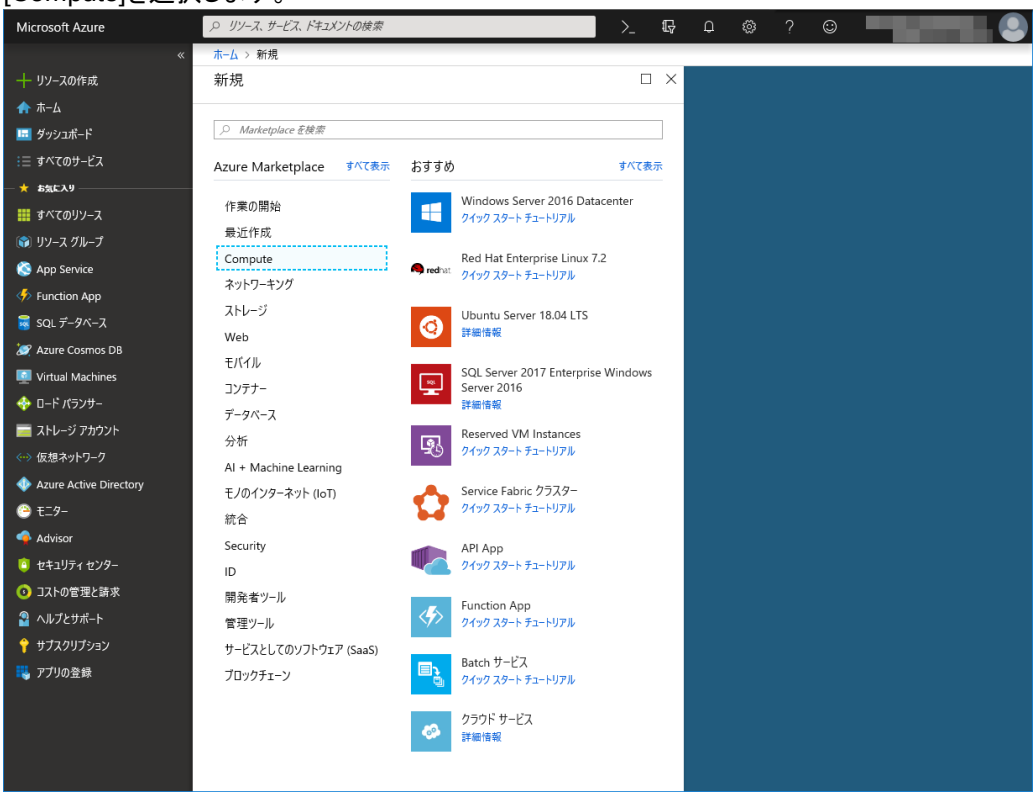
3) 仮想マシンの作成

Microsoft Azure ポータル(https://portal.azure.com/)にログインし、以下の手順で仮想マシンおよびディスクを追加します。
クラスタを構成する仮想マシンを必要な数だけ作成します。node-1、node-2 の順に作成します。

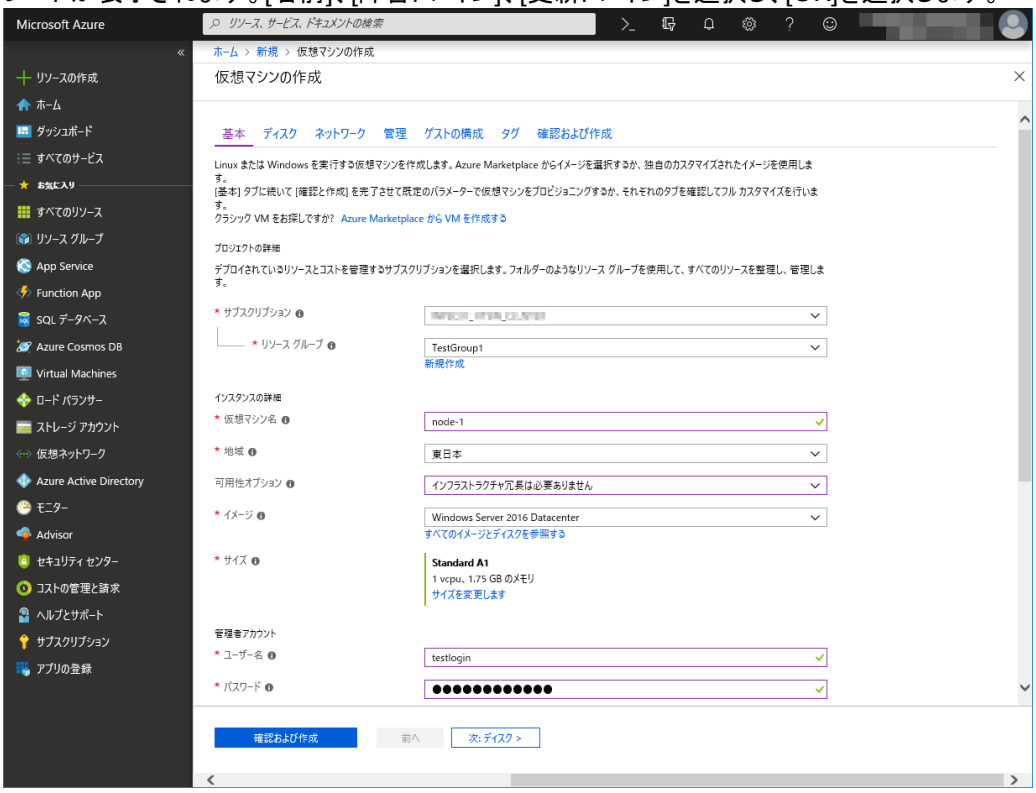
1. 画面左側のメニューにある[+リソースの作成]もしくは[+]アイコンを選択します。

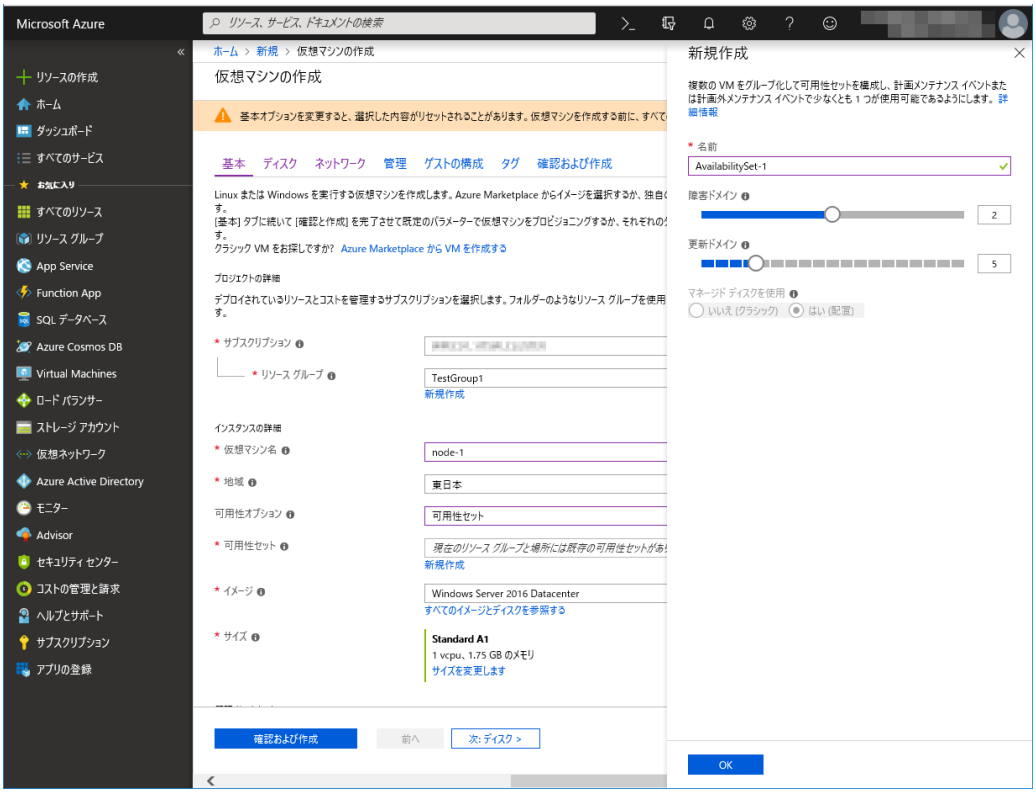


2. [Compute]を選択します。

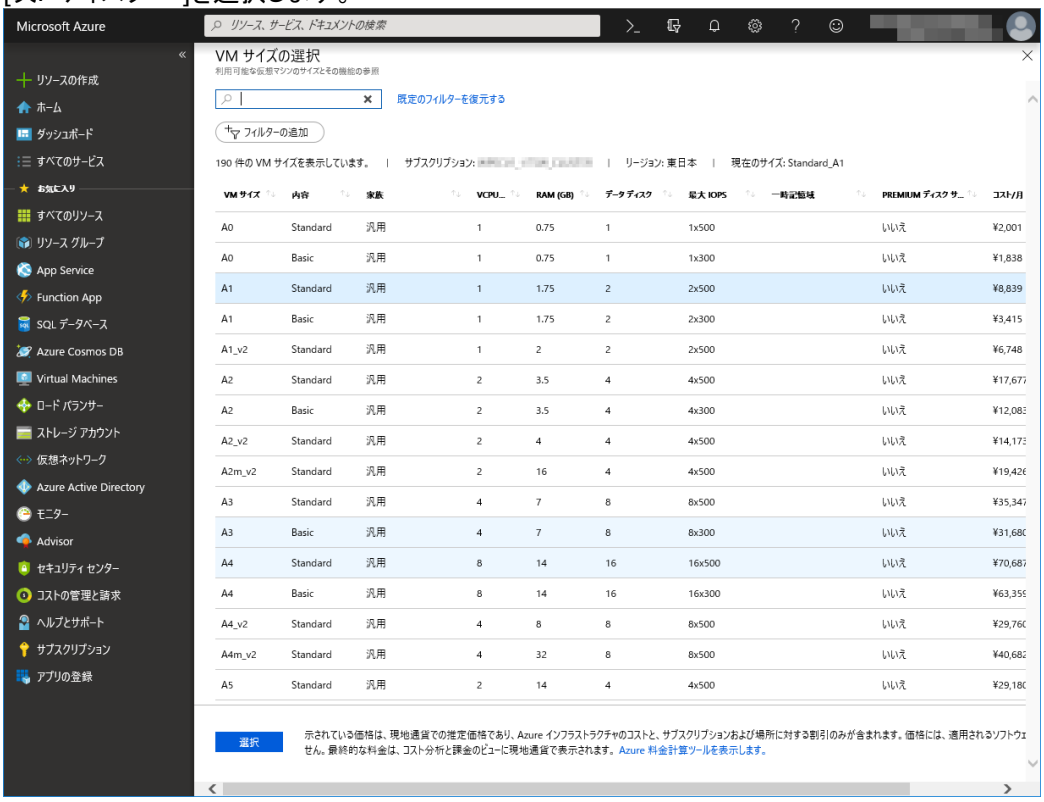


3. [Windows Server 2016 Datacenter]を選択します。
4. [基本]タブが表示されますので、[サブスクリプション]、[リソース グループ]、[仮想マシン名]、[地域]、[イメージ]、[サイズ]、[ユーザー名]、[パスワード]、[パスワードの確認]を設定します。
[可用性オプション]で可用性セットを選択し、[可用性セット]で新規作成を選択すると、[新規作成]ブレードが表示されます。[名前]、[障害ドメイン]、[更新ドメイン]を選択し、[OK]を選択します。

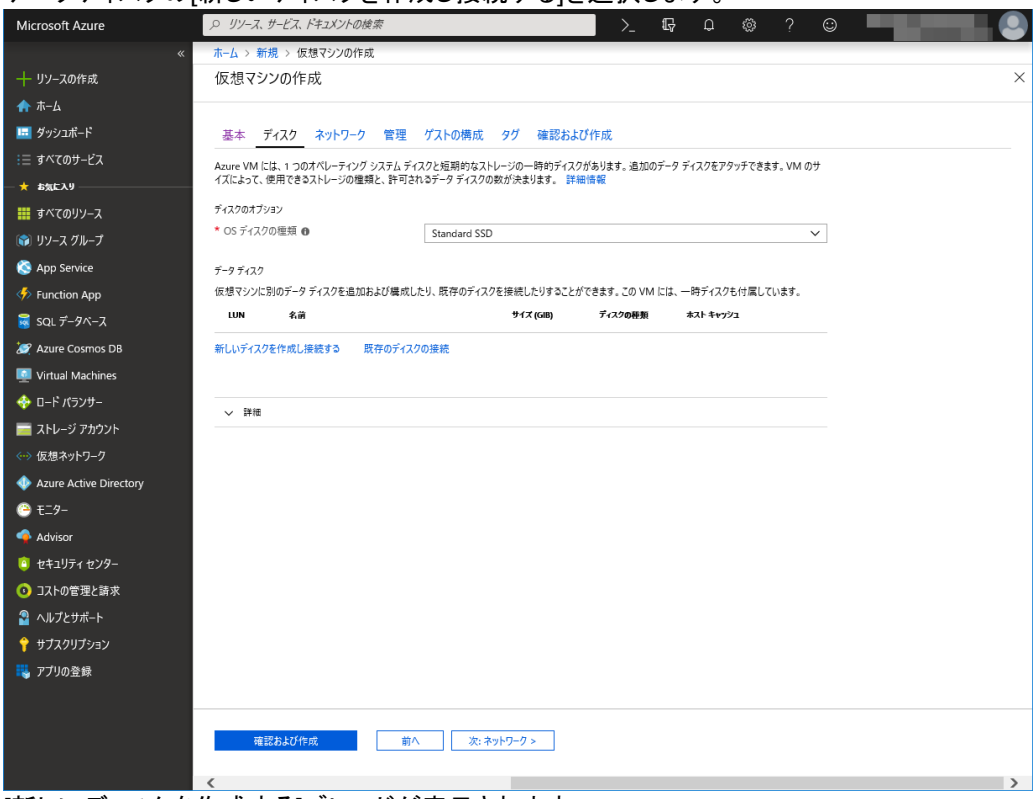




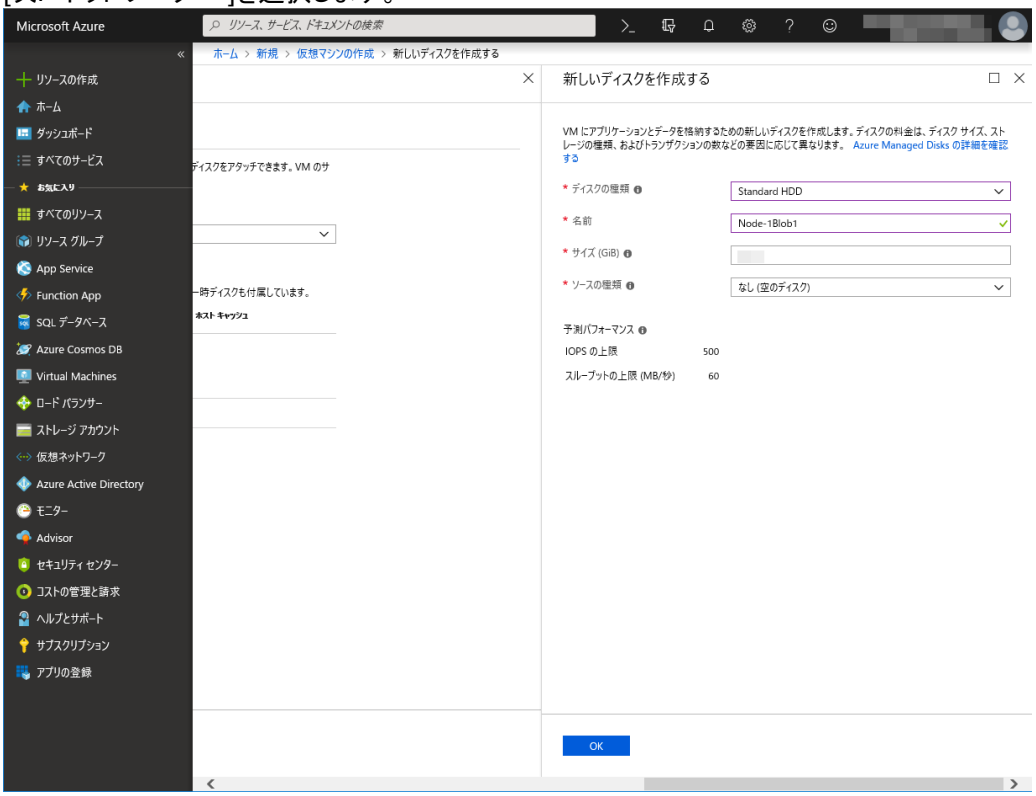
[サイズを変更します]を選択すると、[VM サイズの選択]ブレードが表示されます。
仮想マシンの目的に合ったサイズを一覧から選択し、[選択]を選択します。本書では[A1 Standard]を選択します。
[仮想マシン名]は、node-1 の場合は node-1、node-2 の場合は node-2 です。
[次: ディスク >]を選択します。



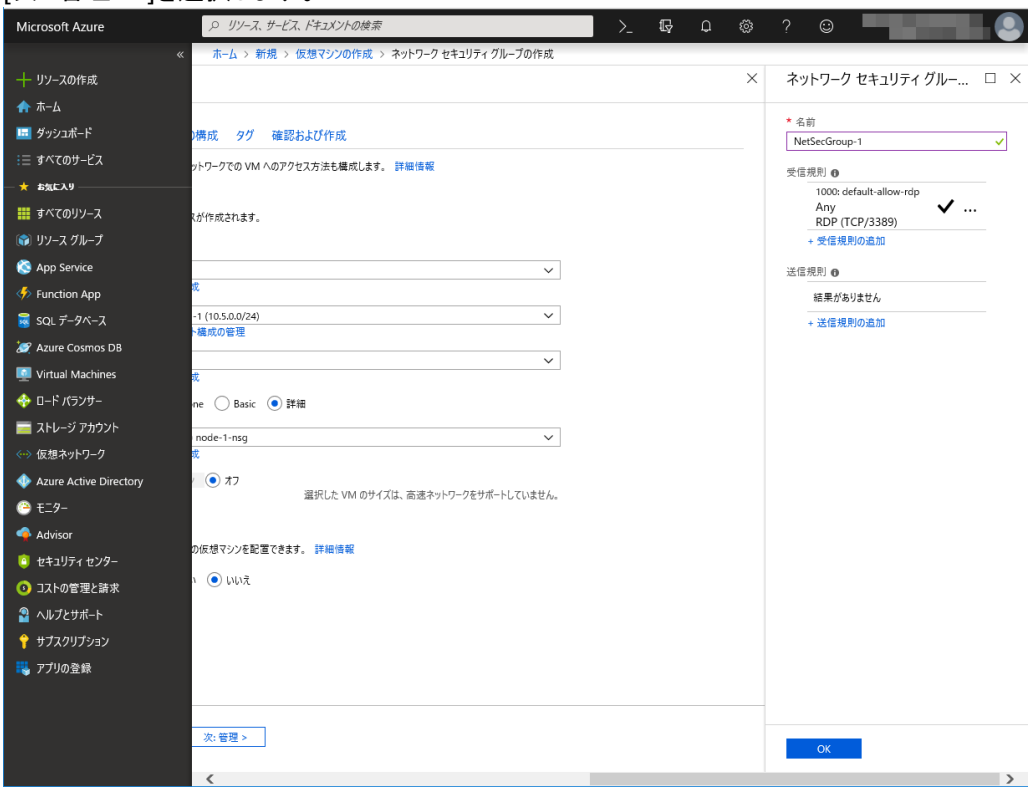
5. [ディスク]タブが表示されますので、以下の手順でミラーディスク(クラスタパーティション、データパーティション)に使用する Blob を追加します。
データディスクの[新しいディスクを作成し接続する]を選択します。



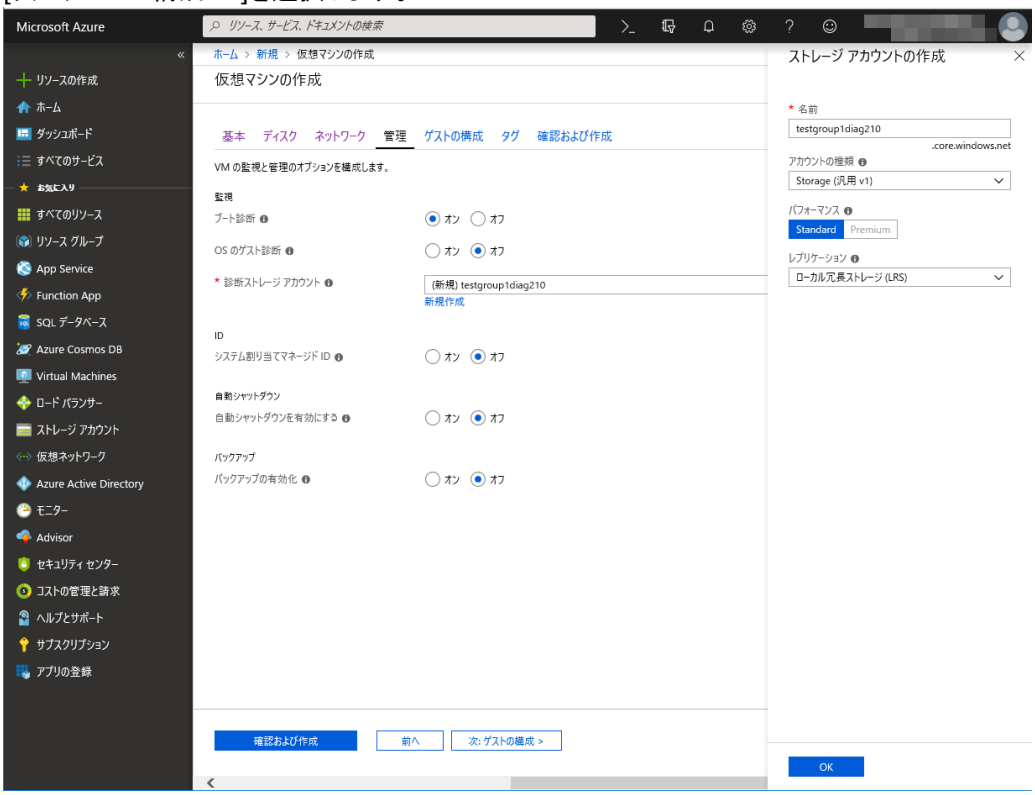
6. [新しいディスクを作成する]ブレードが表示されます。
[ディスクの種類]、[名前]、[サイズ(GiB)]、[ソースの種類]を選択し、[OK]を選択します。
[次: ネットワーク >]を選択します。



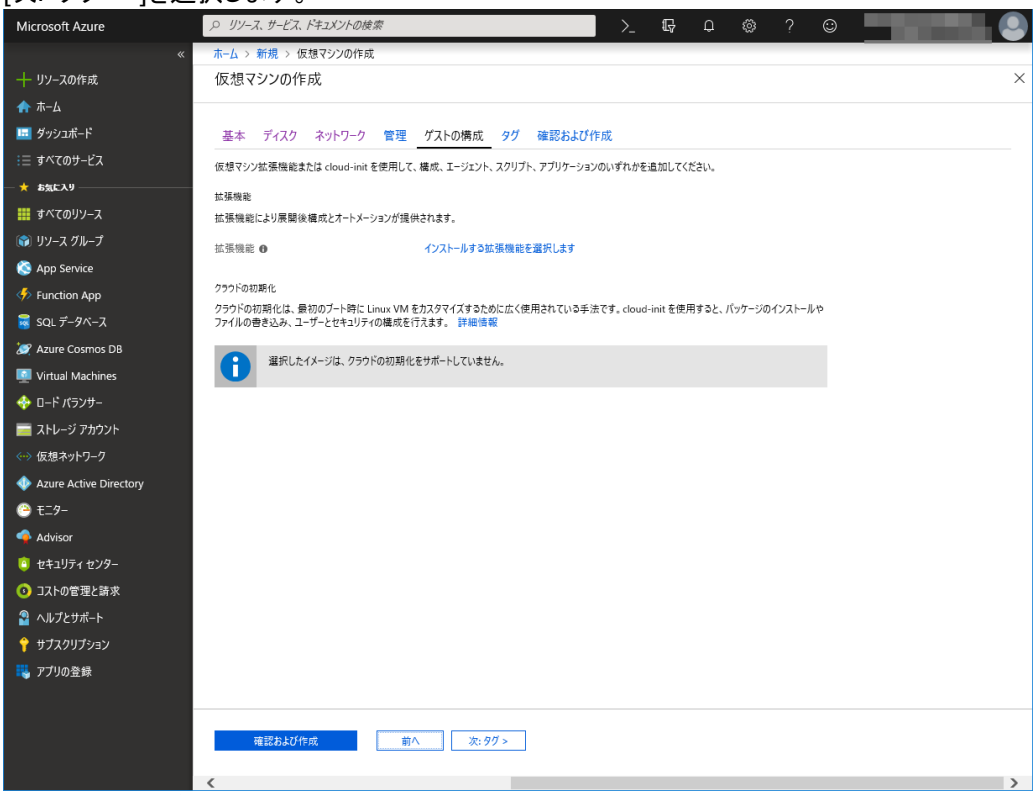
7. [ネットワーク]タブが表示されます。
[仮想ネットワーク]、[サブネット]、[ネットワーク セキュリティ グループ]、[ネットワーク セキュリティ グループの構成]を選択します。
[ネットワーク セキュリティ グループの構成]の新規作成を選択すると、[ネットワーク セキュリティ グループの作成]ブレードが表示されますので、[名前]を選択し、[OK]を選択します。
[次: 管理 >]を選択します。



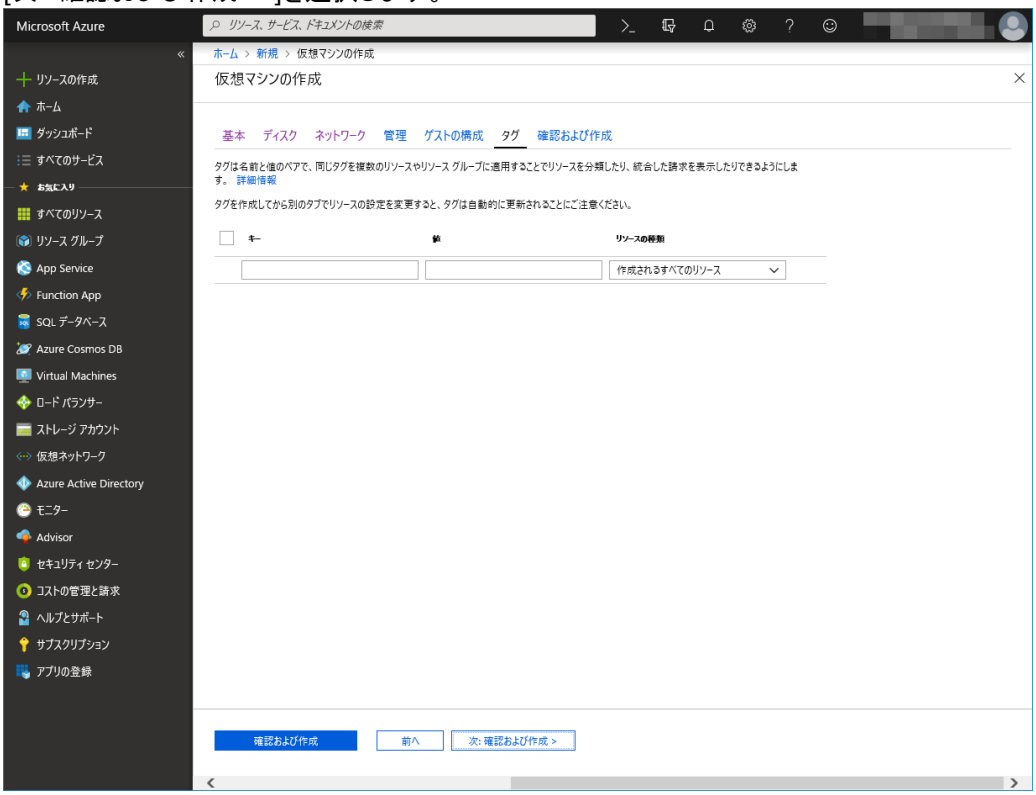
8. [管理]タブが表示されます。
[診断ストレージアカウント]で[新規作成]を選択すると、[ストレージアカウントの作成]ブレードが表示されます。
[名前]、[アカウントの種類]、[レプリケーション]を選択し、[OK]を選択します。
[診断ストレージアカウント]は、自動生成される既定値が入力されています。
[次: ゲストの構成 >]を選択します。



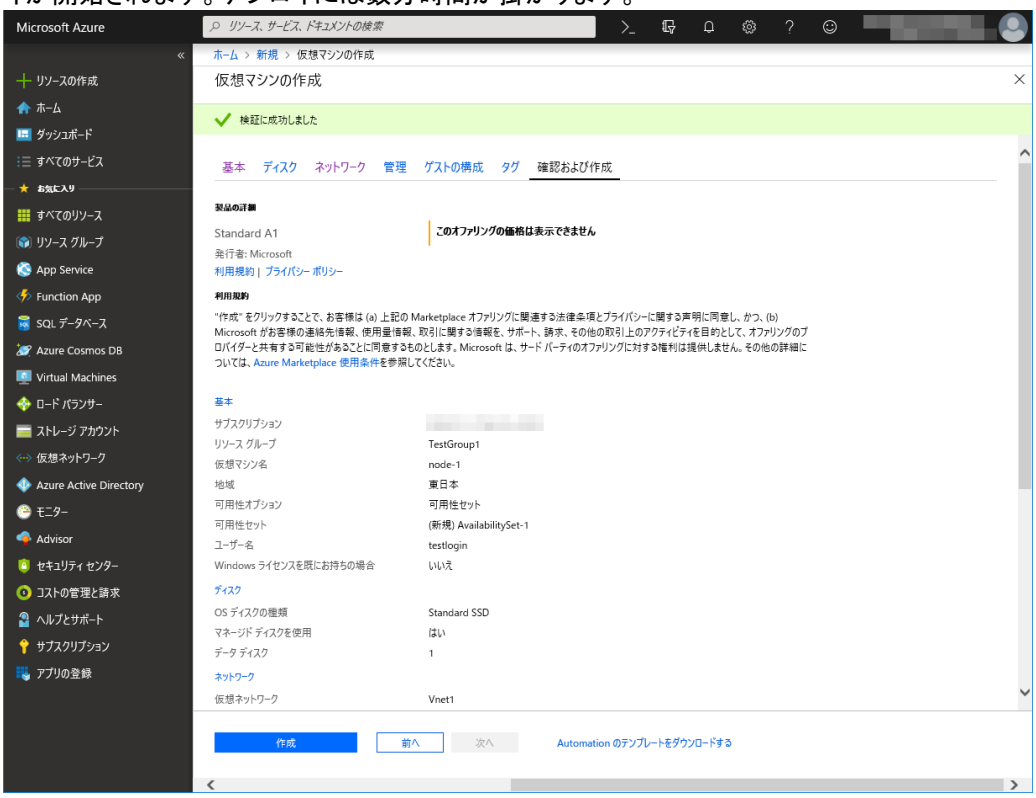
9. [次: タグ >]を選択します。



10. [次: 確認および作成 >]を選択します。



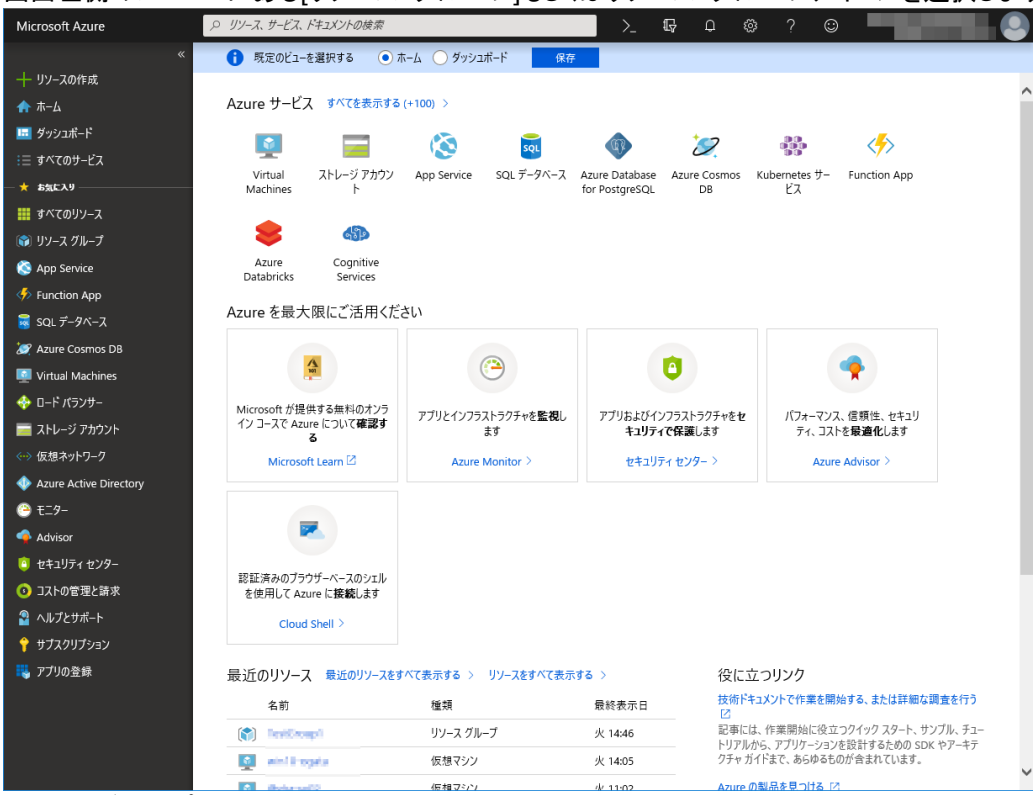
11. [確認および作成]タブが表示されます。内容を確認し、問題がなければ[作成]を選択します。デプロイが開始されます。デプロイには数分時間が掛かります。



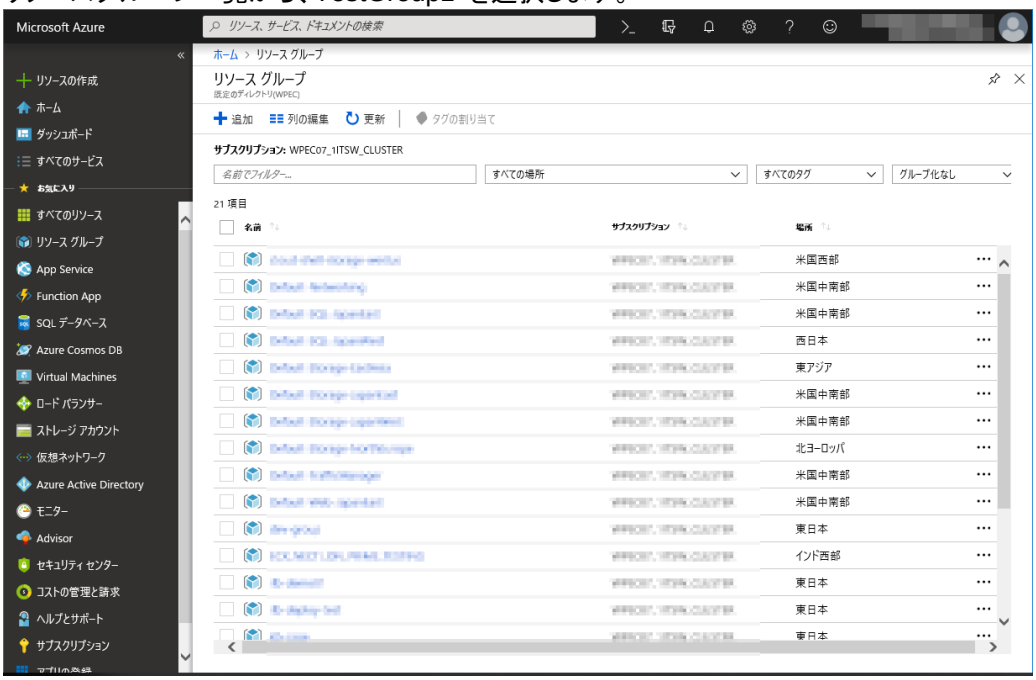
4) プライベート IP アドレスの設定

Microsoft Azure ポータル(https://portal.azure.com/)にログインし、以下の手順でプライベート IP アドレスの設定を変更します。IP アドレスは初期設定では動的割り当てとなっているため、静的割り当てに変更します。node-1、node-2 の順に実行します。

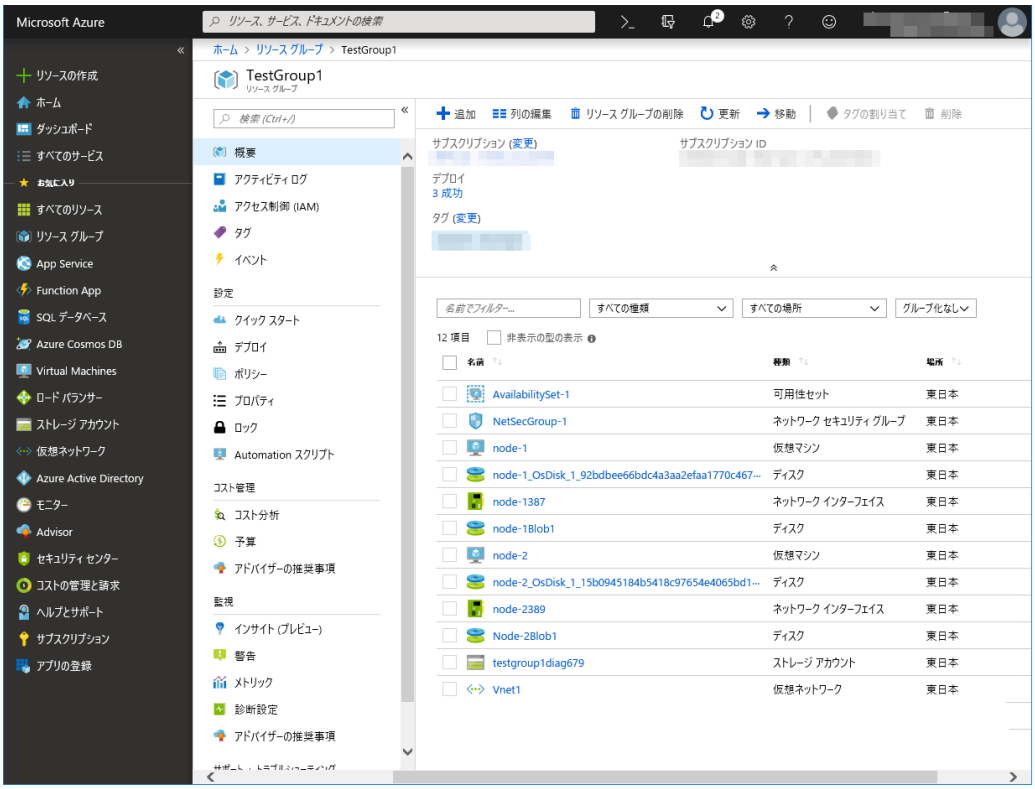
1. 画面左側のメニューにある[リソース グループ]もしくはリソース グループアイコンを選択します。



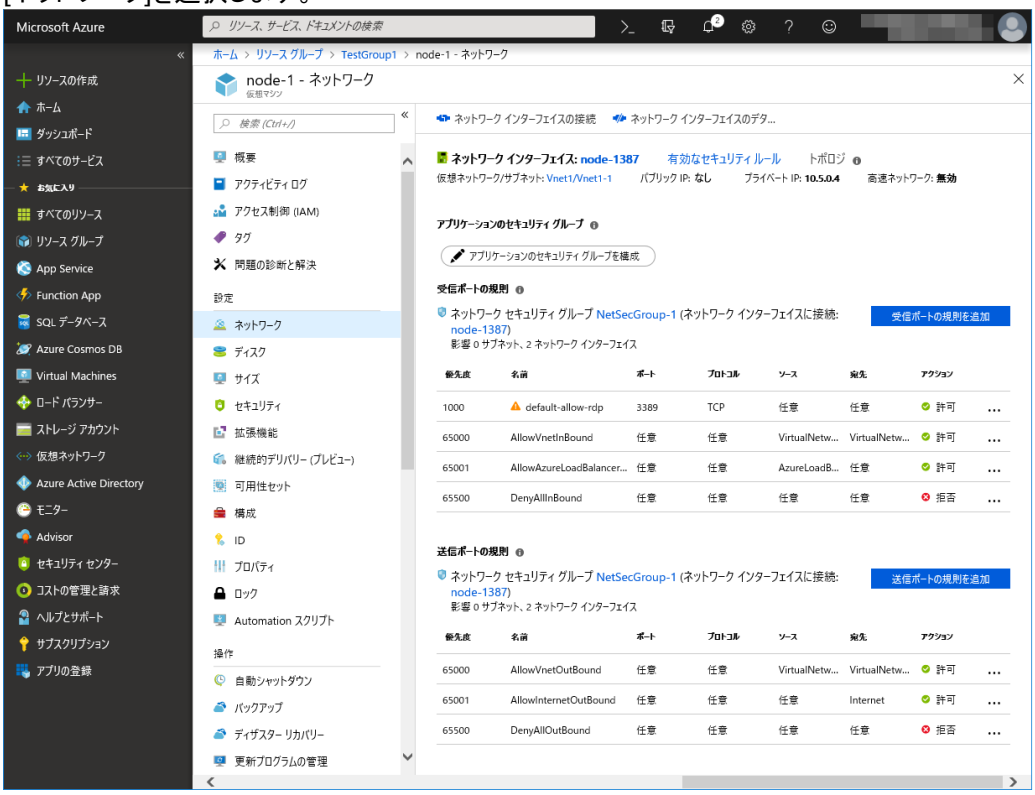
2. リソースグループ一覧から、TestGroup1 を選択します。



3. TestGroup1 の概要が表示されます。項目一覧から仮想マシン node-1 もしくは node-2 を選択します。

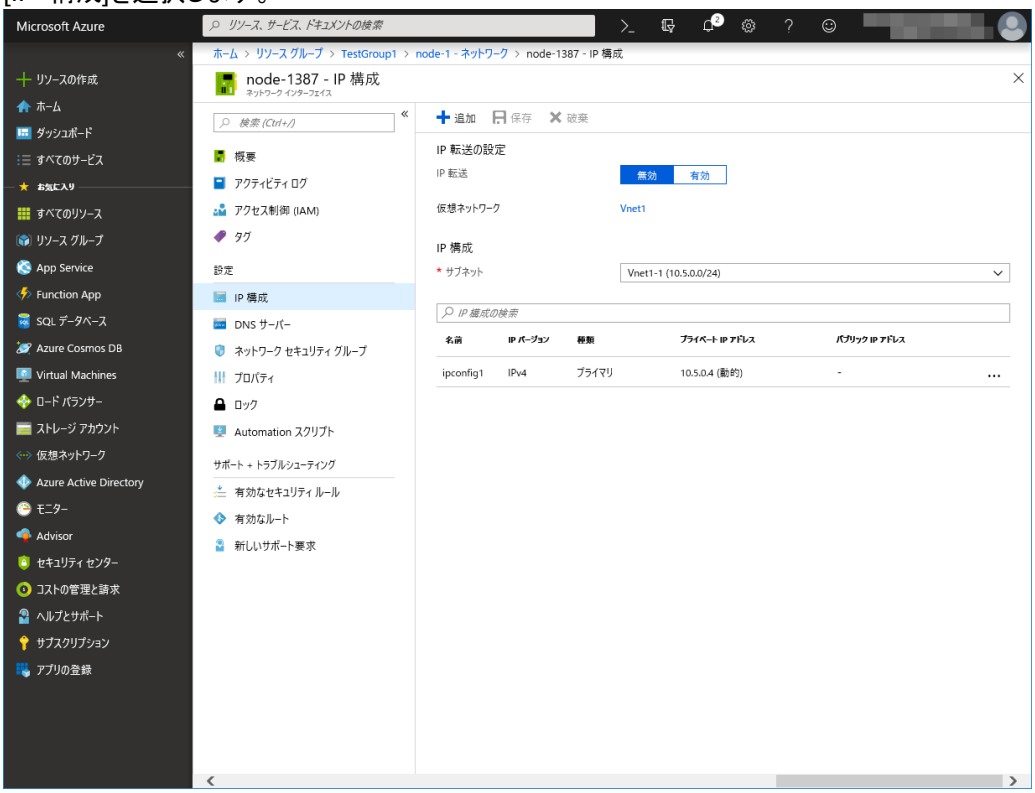


4. [ネットワーク]を選択します。

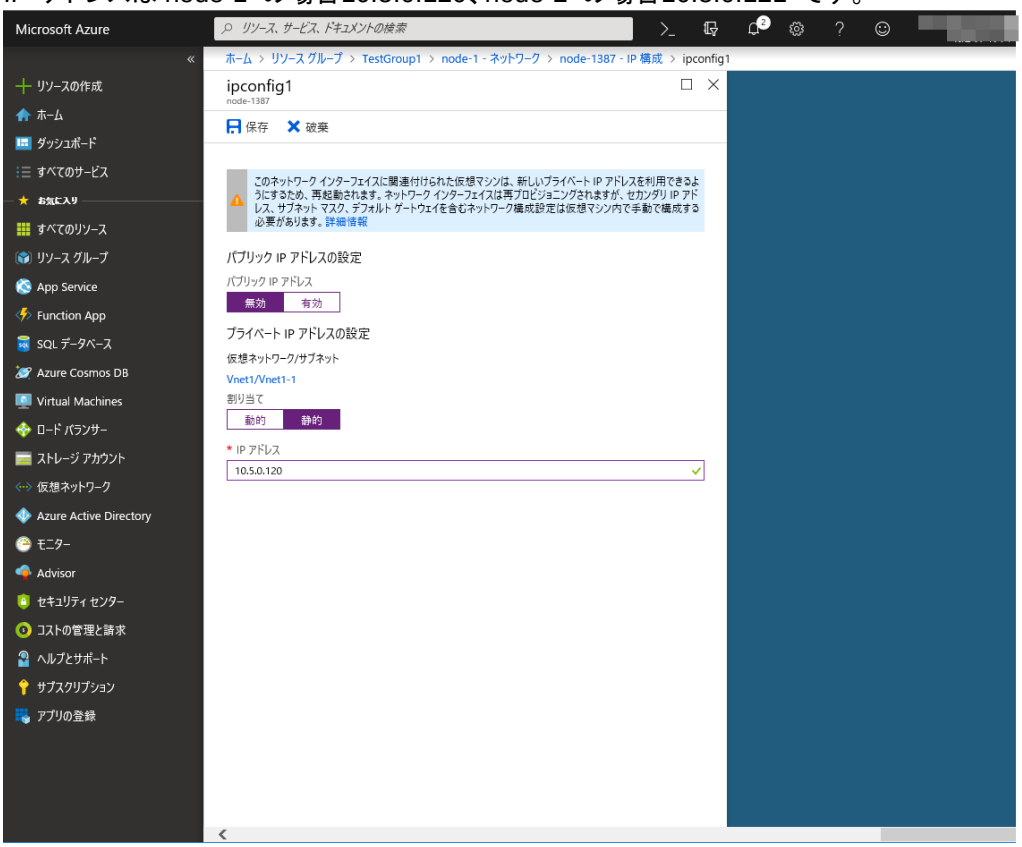


5. 一覧に1 つ表示されているネットワーク インターフェイスを選択します。ネットワーク インターフェイス名は自動生成されます。

6. [IP 構成]を選択します。



7. 一覧に1 つ表示されている ipconfig1 を選択します。
8. [プライベート IP アドレスの設定]の下に表示されている[割り当て]を、[静的]に変更します。その下にある[IP アドレス]に、静的に割り当てる IP アドレスを入力し、画面上部にある[保存]を選択します。IP アドレスは node-1 の場合10.5.0.120、node-2 の場合10.5.0.121 です。

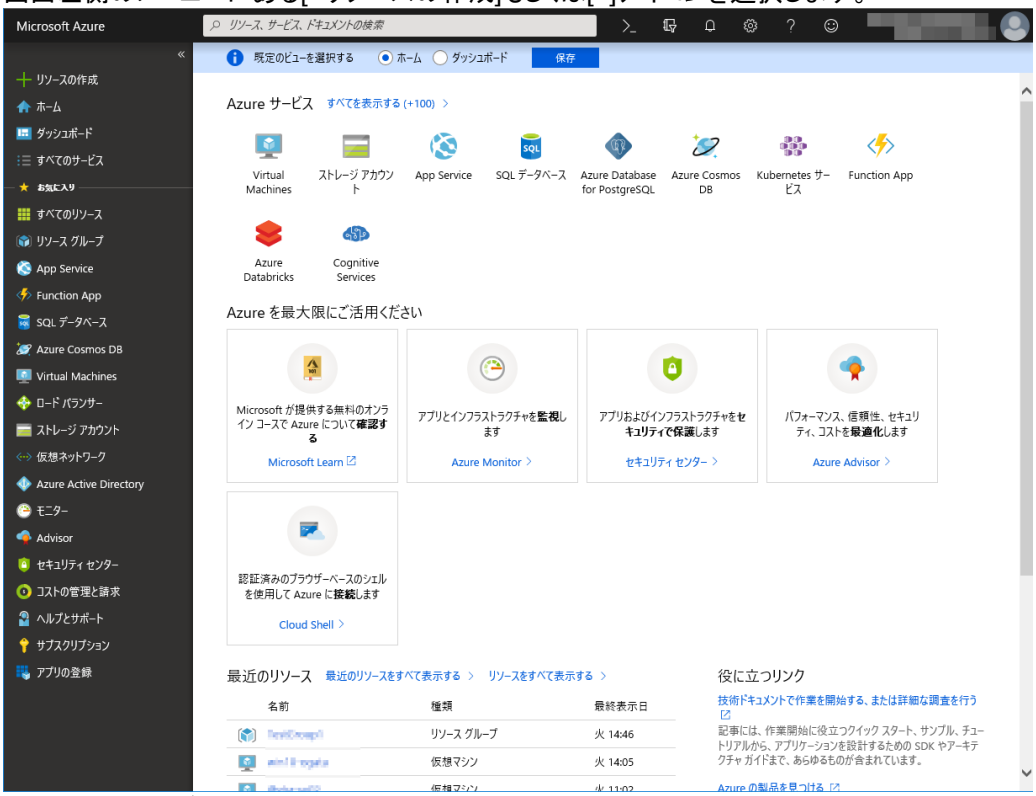


9. 新しいプライベート IP アドレスを利用できるようにするために、仮想マシンが自動的に再起動されます。

5) DNS ゾーンの作成

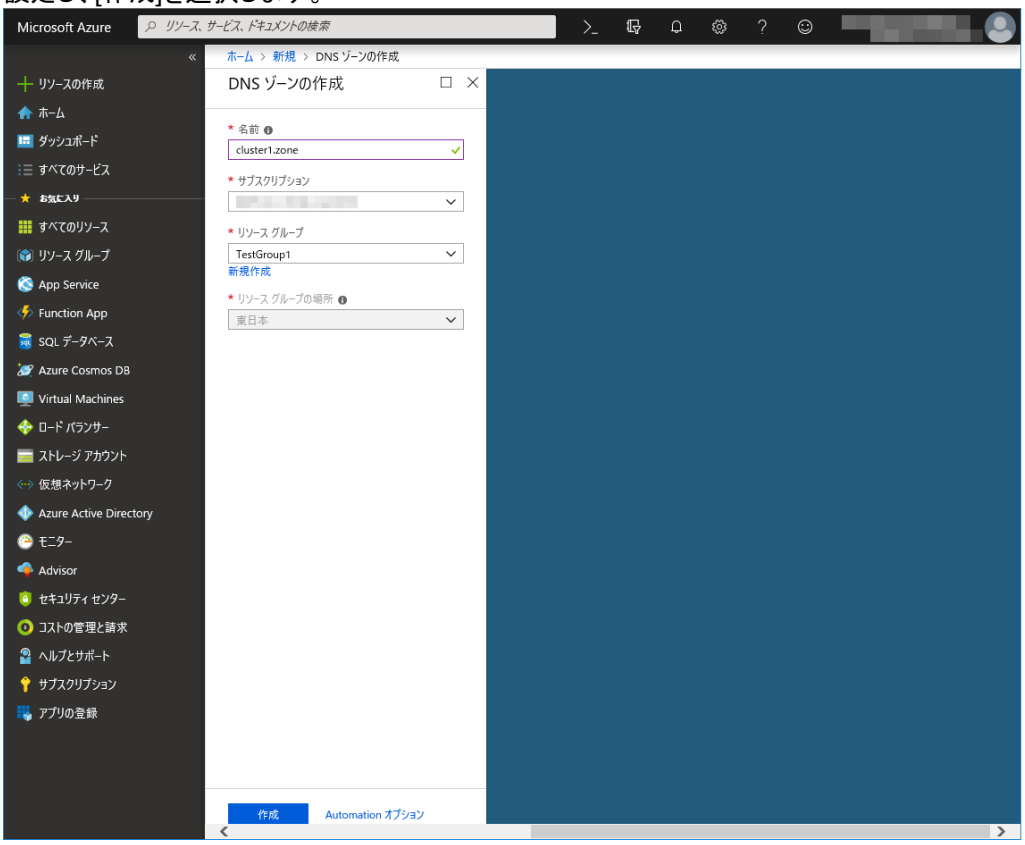
Microsoft Azure ポータル(https://portal.azure.com/)にログインし、以下の手順で DNS ゾーンの設定を行います。

1. 画面左側のメニューにある[+リソースの作成]もしくは[+]アイコンを選択します。



2. [ネットワーキング]>[DNS ゾーン]を選択します。

3. [DNS ゾーンの作成]ブレードが表示されます。[名前]、[サブスクリプション]、[リソース グループ]を設定し、[作成]を選択します。

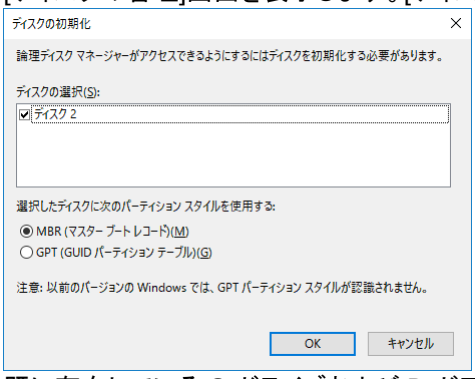


6) 仮想マシンの設定

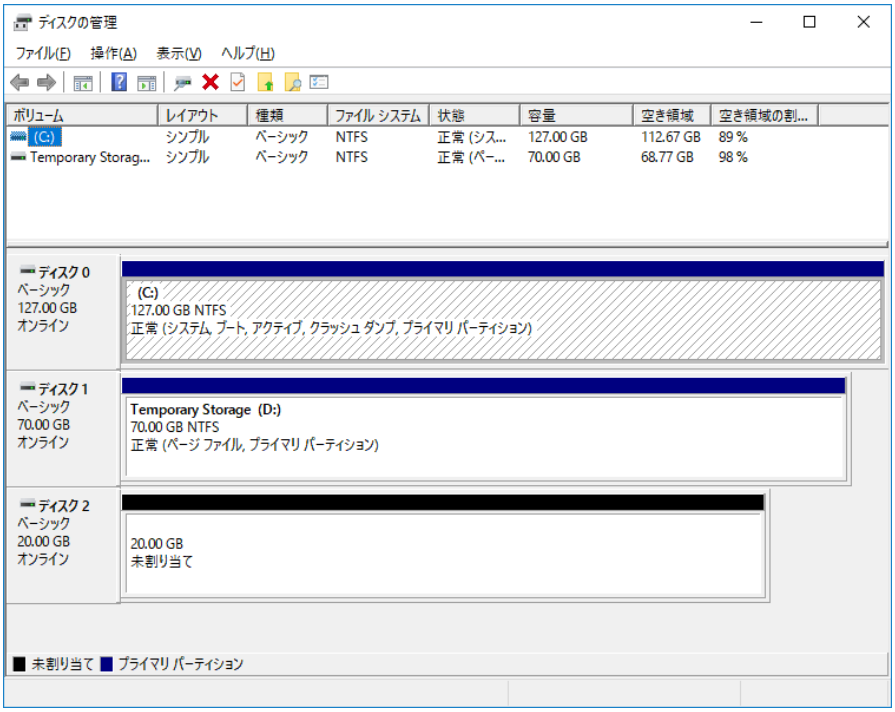
作成した node-1、node-2 へログインし、以下の手順で設定します。
必要な場合、OS を日本語化します。node-1、node-2 の順に実行してください。

次にミラーディスクリソース用のパーティションを設定します。追加した Blob にファイルシステムを作成します。
ミラーディスクリソース用のパーティションについては、『インストール&設定ガイド』-「第1章 システム構成を決定する」-「ハードウェア構成後の設定」-「2. ミラー用パーティションを設定する (ミラーディスク使用時は必須)」を参照してください。

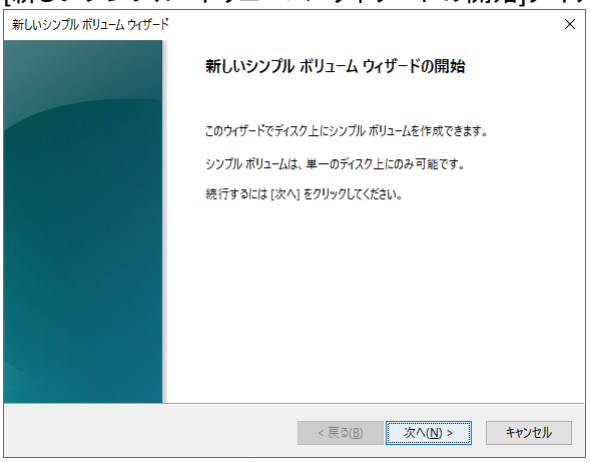
1. [ディスクの管理]画面を表示します。[ディスクの初期化]ダイアログが表示されます。



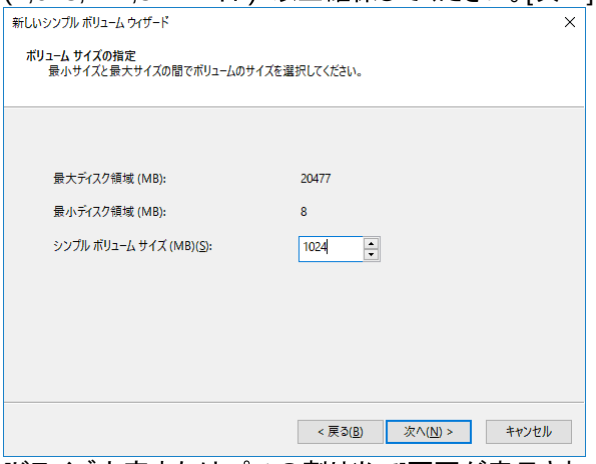
2. 既に存在している C ドライブおよび D ドライブの下に追加ディスクがディスク2 として未割り当て状態で表示されていることを確認します。



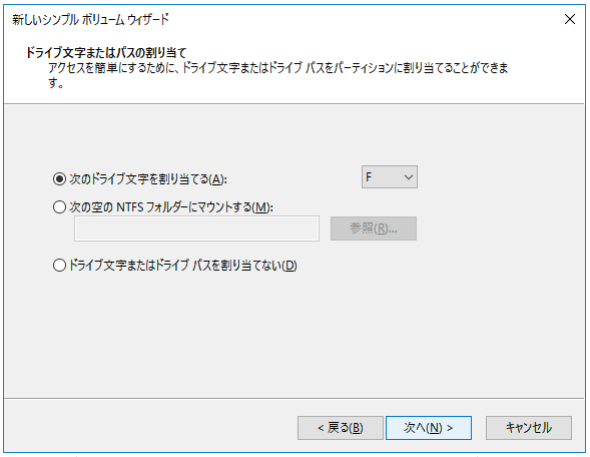
3. クラスタパーティションを作成します。[ディスク2]上で右クリックし、[新しいシンプル ボリューム]を選択します。
4. [新しいシンプル ボリューム ウィザードの開始]ダイアログが表示されます。[次へ]を選択します。



5. [ボリューム サイズの指定]画面が表示されます。クラスタパーティションは 1024MB (1,073,741,824バイト) 以上確保してください。[次へ]を選択します。

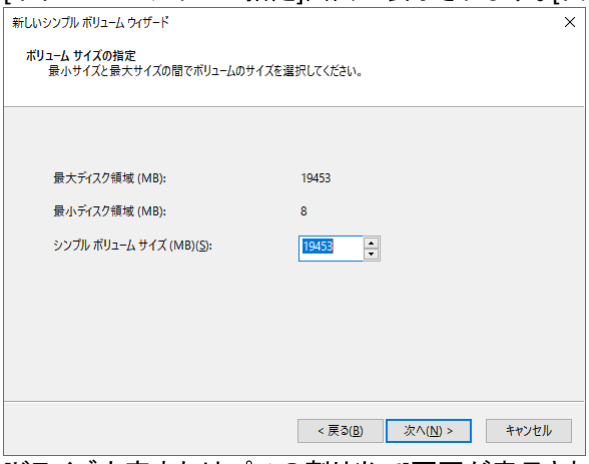


6. [ドライブ文字またはパスの割り当て]画面が表示されます。[次のドライブ文字を割り当てる]にF ドライブを選択します。フォーマットは行わず RAW パーティションのまま使用します。

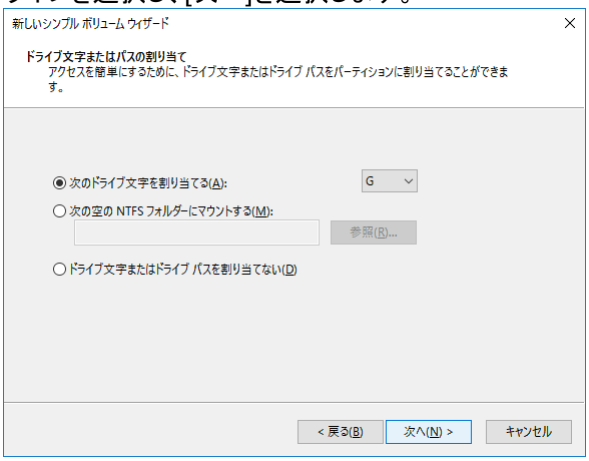


7. 次にデータパーティションを作成します。[ディスク2]上で右クリックし、[新しいシンプル ボリューム]を選択します。
8. [新しいシンプル ボリューム ウィザードの開始]ダイアログが表示されます。[次へ]を選択します。

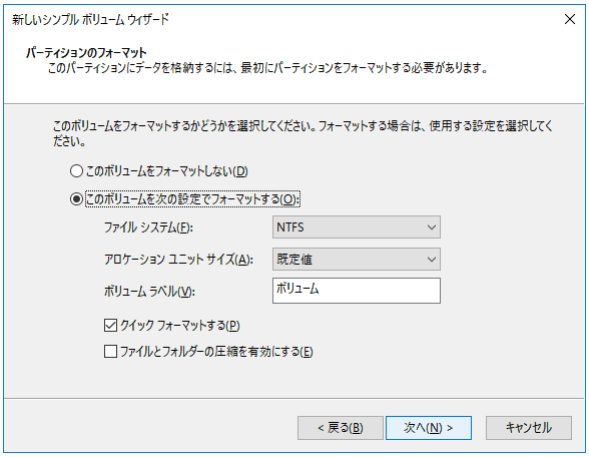
9. [ボリューム サイズの指定]画面が表示されます。[次へ]を選択します。



10. [ドライブ文字またはパスの割り当て]画面が表示されます。[次のドライブ文字を割り当てる]に G ドライブを選択し、[次へ]を選択します。

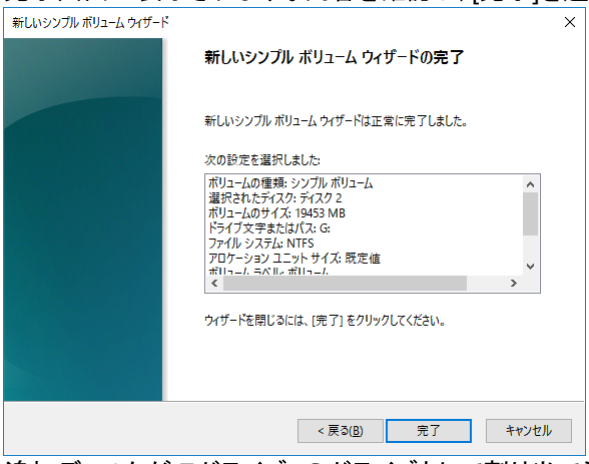


11. [パーティションのフォーマット]画面が表示されます。[ファイル システム]が NTFS であることを確認します。

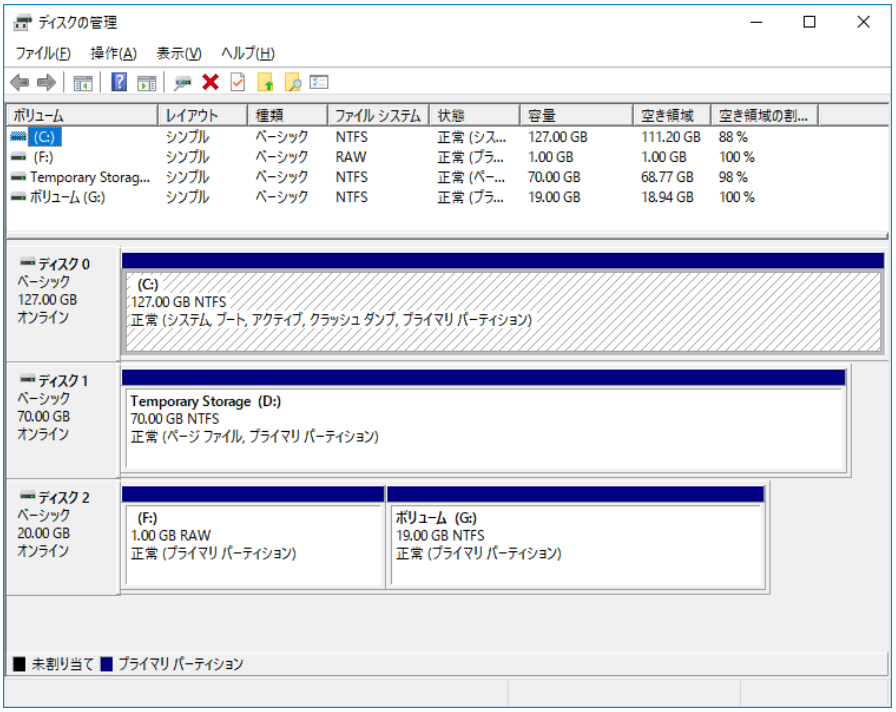


12. [次へ]を選択します。

13. 完了画面が表示されます。内容を確認し、[完了]を選択します。



14. 追加ディスクが Ｆドライブ、Ｇドライブとして割り当てられていることを確認します。



7) OS 起動時間の調整、ネットワーク設定の確認、ファイアウォールの設定を確認、サーバの時刻を同期、パワーセービング機能をオフ

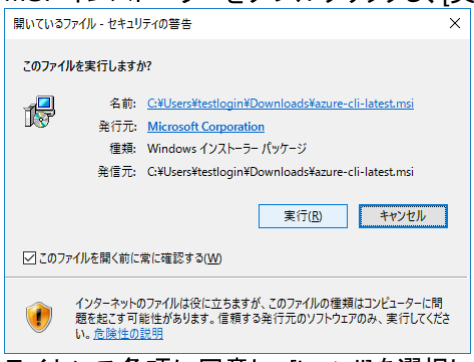
各手順は『インストール&設定ガイド』-「第 1 章 システム構成を決定する」-「ハードウェア構成後の設定」を参照してください。

8) Azure CLI のインストール

次に Azure CLI をインストールします。
Azure CLI をインストーラーからインストールする手順を説明します。
詳細な手順や他の手段については、以下の Web サイトを参照してください。
Azure CLI のインストール:
https://docs.microsoft.com/ja-jp/cli/azure/install-azure-cli?view=azure-cli-latest

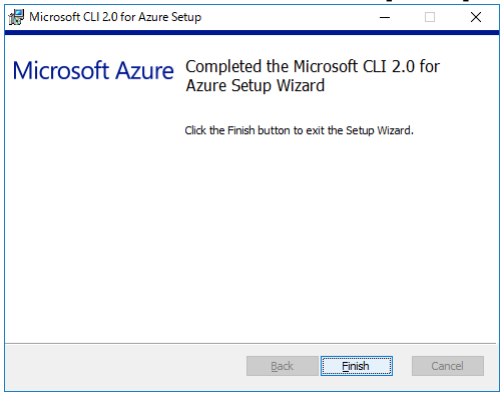
作成した node-1、node-2 へログインし、以下の手順でインストールします。

1. 上記 Web サイトから MSI インストーラーをダウンロードします。
2. MSI インストーラーをダブルクリックし、[実行]を選択します。



3. ライセンス条項に同意し、[Install]を選択します。

4. Install 完了画面が表示されたら、[Finish]を選択します。



9) サービス プリンシパルの作成

次に Azure CLI を使用して、サービス プリンシパルを作成します。
Azure DNS リソースは Microsoft Azure にログインし、DNS ゾーンへの登録や監視を実行します。
Microsoft Azure へのログイン時、サービス プリンシパルによる Azure ログインを利用します。本書ではセキュリティ観点から証明書ベースの認証を記載しています。証明書には有効期限があることに注意してください。詳細は az ad sp create-for-rbac の --years オプションを参照してください。
https://docs.microsoft.com/en-us/cli/azure/ad/sp?view=azure-cli-latest#az-ad-sp-create-for-rbac

サービスプリンシパルや詳細な手順については、以下の Web サイトを参照してください。
Azure CLI を使用してサインインする:
https://docs.microsoft.com/ja-jp/cli/azure/authenticate-azure-cli?view=azure-cli-latest
Azure CLI で Azure サービス プリンシパルを作成する:
https://docs.microsoft.com/ja-jp/cli/azure/create-an-azure-service-principal-azure-cli?view=azure-cli-latest

1. 組織のアカウントでログインします。
   `az login -u <`*アカウント名*`> -p <`*パスワード*`>`
2. サービス プリンシパルを作成し、登録します。Azure 環境設定ファイルに設定するため、表示される name および tenant はメモしてください。
   以下の例では、C:¥Users¥testlogin¥examplecert.pem にサービス プリンシパルが作成されます。
   ```
   az ad sp create-for-rbac --create-cert
   {
     "appId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
     "displayName": "azure-test",
     "fileWithCertAndPrivateKey": "C:¥¥Users¥¥testlogin¥¥examplecert.
     pem",
     "name": "http://azure-test",
     "password": null,
     "tenant": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
   }
   ```
3. ログアウトします。
   `az logout --username <`*アカウント名*`>`
4. 作成されたサービス プリンシパルを利用して、Microsoft Azure へログインできるか確認します。
   `az login --service-principal -u <`*上記の name の値*`> --tenant <`*上記の tenant の値*`> -p <`*上記の fileWithCertAndPrivateKey の値*`>`
   サインインに成功すると、次の出力が表示されます。
   ```
   [
     {
       "cloudName": "AzureCloud",
       "id": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
       "isDefault": true,
       "name": "xxxxxxxxxx",
       "state": "Enabled",
       "tenantId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
       "user": {
         "name": "http://azure-test",
         "type": "servicePrincipal"
       }
     }
   ]
   ```
5. ログアウトします。
   `az logout --username <`*上記の name の値*`>`

作成されたサービスプリンシパルのロールを既定の Contributor(共同作成者)から別のロールに変更する場合、Actions プロパティとして以下のすべての操作へのアクセス権を持つロールを選択してください。この条件を満たさないロールに変更した場合、後程設定する Azure DNS 監視リソースによる監視がエラーにより失敗します。

Azure CLI 2.0の場合
Microsoft.Network/dnsZones/A/write
Microsoft.Network/dnsZones/A/delete
Microsoft.Network/dnsZones/NS/read

10) CLUSTERPRO のインストール

インストール手順は『インストール&設定ガイド』を参照してください。
インストール完了後、OS の再起動を行ってください。

11) CLUSTERPRO のライセンスを登録

ライセンス登録手順は『インストール&設定ガイド』を参照してください。

3.3 CLUSTERPRO の設定

Cluster WebUI のセットアップ、および接続方法は『インストール&設定ガイド』-「第5章 クラスタ構成情報を作成する」を参照してください。

以下のリソース/監視リソースを追加する手順を記述します。

- ミラーディスクリソース
- Azure DNS リソース
- Azure DNS 監視リソース
- カスタム監視リソース(NP 解決用)
- IP 監視リソース(NP 解決用)
- マルチターゲット監視リソース(NP 解決用)

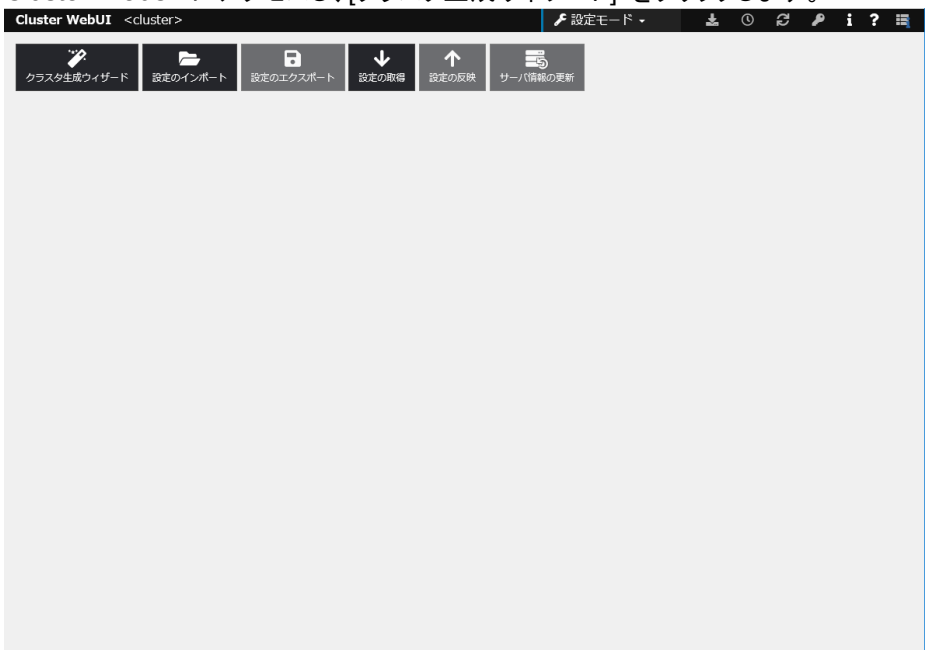
上記以外の設定は、『インストール&設定ガイド』、『リファレンスガイド』を参照してください。

1) クラスタの作成

最初に、クラスタ生成ウィザードを開始し、クラスタを構築します。

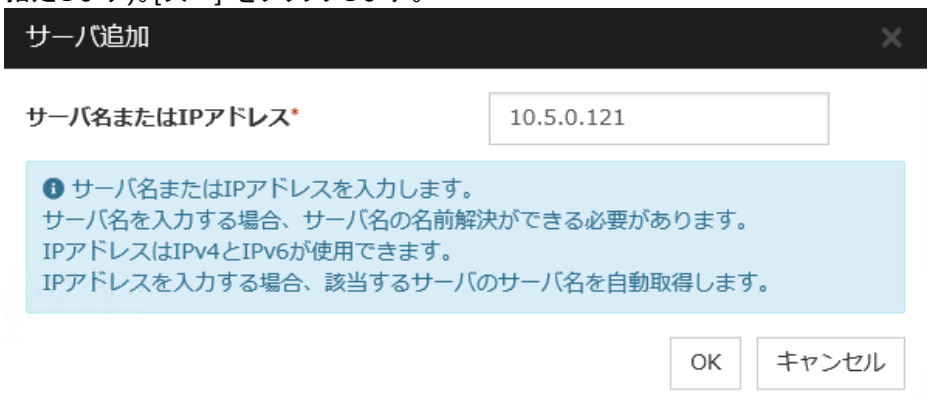
◇ クラスタの構築

1. Cluster WebUI にアクセスし、[クラスタ生成ウィザード] をクリックします。



2. [クラスタ生成ウィザード]画面の[クラスタ]画面が表示されます。
[クラスタ名] に任意のクラスタ名を入力します。
[言語] を適切に選択します。[次へ] をクリックします。

3. [基本設定]画面が表示されます。
Cluster WebUI に接続したインスタンスがマスタサーバとして登録済みの状態で表示されます。
[追加] をクリックし、残りのインスタンスを追加します(インスタンスの Private IP アドレスを指定します)。[次へ] をクリックします。



4. [インタコネクト] 画面が表示されます。
   インタコネクトのために使用する IP アドレス(各インスタンスの Private IP アドレス)を指定します。また、後で作成するミラーディスクリソースの通信経路として [MDC] に mdc1 を選択します。[次へ] をクリックします。

5. [NP 解決] 画面が表示されます。
   ただし、NP 解決は本画面では設定せず、 別途 IP 監視リソース、カスタム監視リソース、マルチターゲット監視リソースを追加することによって同等のことを実現します。NP 解決の設定は、後述の「3) **監視リソースの追加**」で行います。
   クラスタシステムにアクセスするクライアントの配置やオンプレミス環境との接続条件（専用線接続など）によって、NP 解決先や NP 解決の方法は、その都度 検討する必要があります。NP 解決にネットワークパーティション解決リソースを利用することも可能です。
   [次へ] をクリックします。

2) グループリソースの追加

◇ グループの定義
フェイルオーバグループを作成します。

1. [グループ一覧] 画面が表示されます。
[追加]をクリックします。

2. [グループの定義] 画面が表示されます。
[名前] にフェイルオーバグループ名(failover1)を設定します。[次へ] をクリックします。

3. [起動可能サーバ] 画面が表示されます。
何も指定せず [次へ] をクリックします。
4. [グループ属性] 画面が表示されます。
何も指定せず [次へ] をクリックします。
5. [グループリソース一覧] 画面が表示されます。
以降の手順で、この画面でグループリソースを追加していきます。

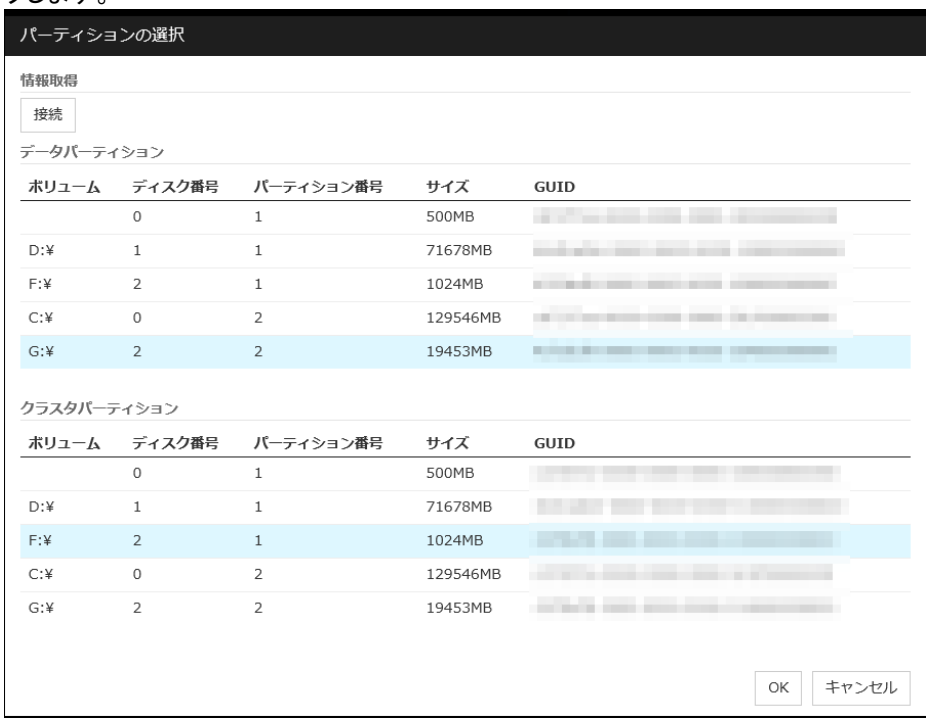
◇ ミラーディスクリソース
ミラーディスクリソースを作成します。
詳細は『リファレンスガイド』-「ミラーディスクリソースを理解する」を参照してください。

1. [グループリソース一覧] で [追加] をクリックします。

2. [グループのリソース定義 | failover1] 画面が開きます。
   [タイプ] ボックスでグループリソースのタイプ(ミラーディスクリソース) を選択し、[名前] ボックスにグループ名 (md) を入力します。[次へ] をクリックします。

3. [依存関係] 画面が表示されます。
   何も指定せず [次へ] をクリックします。
4. [復旧動作] 画面が表示されます。[次へ] をクリックします。
5. [詳細] 画面が表示されます。
   [起動可能サーバ]で[名前]列中のサーバ名を選択し[追加]をクリックします。

6. [パーティションの選択]ダイアログボックスが表示されます。[接続]をクリックし、「6) **仮想マシンの設定**」で作成したデータパーティションと、クラスタパーティションを選択し、[OK]をクリックします。



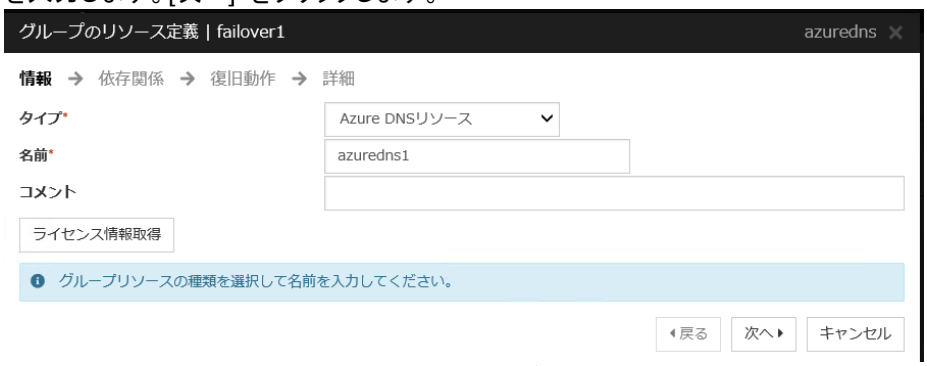
7. node-1について5と6を設定、次に node-2について5と6を設定し、[完了]をクリックします。

◇ Azure DNS リソース
Azure DNS に対してレコードを登録、解除する仕組みを提供します。

Azure DNS リソースの詳細は『リファレンスガイド』-「Azure DNS リソースを理解する」を参照してください。

1. [グループリソース一覧] で [追加] をクリックします。

2. [グループのリソース定義 | failover1] 画面が開きます。[タイプ] ボックスでグループリソースのタイプ (Azure DNS リソース) を選択して、[名前] ボックスにグループ名 (azuredns1) を入力します。[次へ] をクリックします。



3. [依存関係] 画面が表示されます。何も指定せず [次へ] をクリックします。
4. [復旧動作] 画面が表示されます。[次へ] をクリックします。
5. [レコードセット名]、[ゾーン名]、[IP アドレス]、[リソースグループ名]、[ユーザ URI]、[テナント ID]、[サービスプリンシパルのファイルパス]、[Azure CLI ファイルパス]に値を入力します。[IP アドレス]は各サーバの IP アドレスを使用する場合、各サーバのタブで IP アドレスを入力します。サーバ別の設定を行う場合は[共通]タブでは、任意のサーバの IP アドレスを記載し、他のサーバは個別設定を行うようにしてください。

6. [完了] をクリックします。

3) 監視リソースの追加

◇ Azure DNS 監視リソース
Azure DNS に登録したレコードセットの確認および名前解決確認の監視機構を提供します。

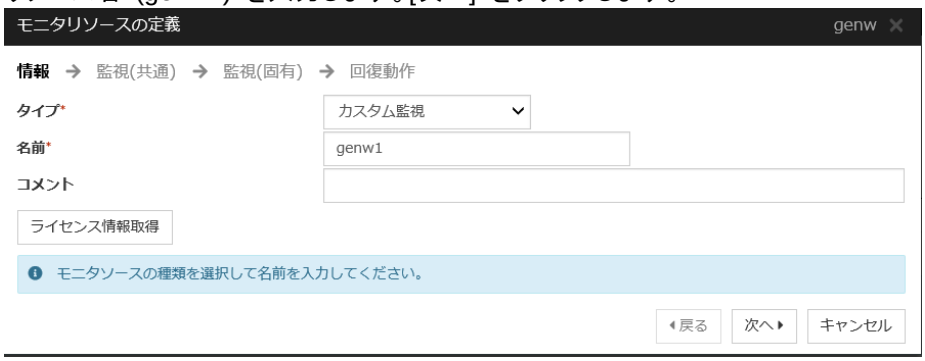
Azure DNS 監視リソースの詳細は『リファレンスガイド』-「Azure DNS 監視リソースを理解する」を参照してください。

Azure DNS リソースを1つ追加すると、Azure DNS 監視リソースが1つ自動的に作成されます。

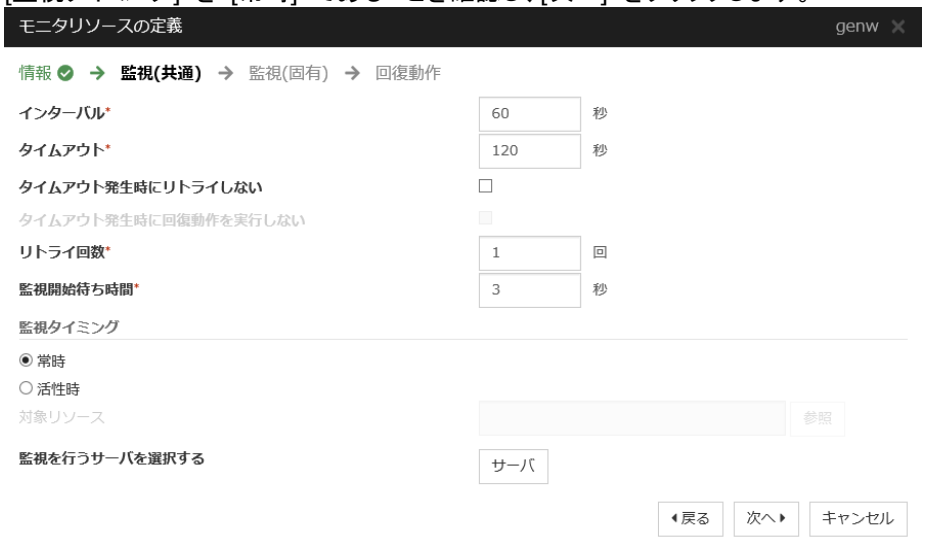
◇ カスタム監視リソース
Microsoft Azure の Service Management API へ疎通可能かどうかを監視し、外部ネットワークとの通信の健全性を監視するためのスクリプトを設定します。

カスタム監視リソースの詳細は『リファレンスガイド』-「カスタム監視リソースを理解する」を参照してください。

1. [モニタリソース一覧] で [追加] をクリックします。
2. [タイプ] ボックスでモニタリソースのタイプ (カスタム監視) を選択し、[名前] ボックスに監視リソース名 (genw1) を入力します。[次へ] をクリックします。



3. [監視(共通)] 画面が表示されます。
[監視タイミング] を [常時] であることを確認し、[次へ] をクリックします。



4. [監視(固有)] 画面が表示されます。
[この製品で作成したスクリプト] をチェックします。
作成するスクリプトのサンプルは以下のとおりです。

<CLUSTERPRO インストールパス>¥bin¥clpazure_port_checker –h management.core.windows.net -p 443
EXIT %ERRORLEVEL%

[監視タイプ] を [同期] にチェックします。[次へ] をクリックします。

5. [回復動作] 画面が表示されます。
[回復動作] に [最終動作のみ実行]、[回復対象] に [LocalServer]、[最終動作] に [何もしない]を設定します。

6. [完了] をクリックして設定を終了します。

◇ IP 監視リソース
仮想マシンで構成されたクラスタ間の通信を監視し、内部ネットワークとの通信の健全性を監視する IP 監視リソースを作成します。

IP 監視リソースの詳細は『リファレンスガイド』-「IP 監視リソースを理解する」を参照してください。

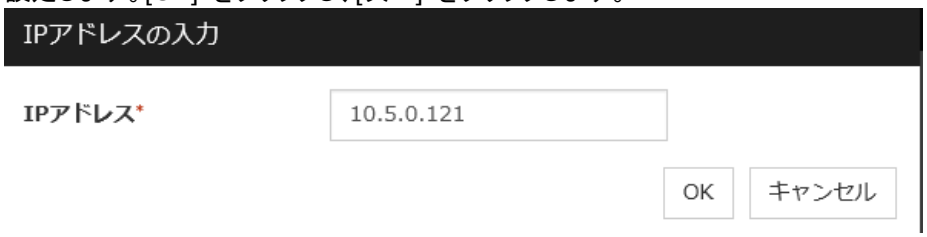
1. [モニタリソース一覧] で [追加] をクリックします。
2. [タイプ] ボックスでモニタリソースのタイプ (IP 監視) を選択し、[名前] ボックスに監視リソース名 (ipw1) を入力します。[次へ] をクリックします。

3. [監視(共通)] 画面が表示されます。
[監視タイミング] が [常時] であることを確認します。

[監視を行うサーバを選択する] で起動可能なサーバをひとつ選択し追加します。[OK] をクリックし、[次へ] をクリックします。

4. [監視(固有)] 画面が表示されます。

[IP アドレス一覧] で [追加] を選択し、3 で選択したサーバとは別のサーバの IP アドレスを設定します。[OK] をクリックし、[次へ] をクリックします。



5. [回復動作] 画面が表示されます。
   [回復動作] に [最終動作のみ実行]、[回復対象] に [LocalServer]、[最終動作] に [何もしない] を設定します。

6. [完了] をクリックして設定を終了します。
7. 次にもう一方のサーバでも、同様の監視リソースを作成します。[モニタリソース一覧] で [追加] をクリックします。
8. [タイプ] ボックスでモニタリソースのタイプ (IP 監視) を選択し、[名前] ボックスに監視リソース名 (ipw2) を入力します。[次へ] をクリックします。
9. [監視(共通)] 画面が表示されます。
   [監視タイミング] が [常時] であることを確認します。
   [監視を行うサーバを選択する] で起動可能なサーバをひとつ選択し追加します。[OK] をクリックし、[次へ] をクリックします。
10. [監視(固有)] 画面が表示されます。
    [IP アドレス一覧] で [追加] を選択し、9 で選択したサーバとは別のサーバの IP アドレスを設定します。[OK] をクリックし、[次へ] をクリックします。

11.[回復動作] 画面が表示されます。
[回復動作] に [最終動作のみ実行]、[回復対象] に [LocalServer]、[最終動作] に [何もしない] を設定します。

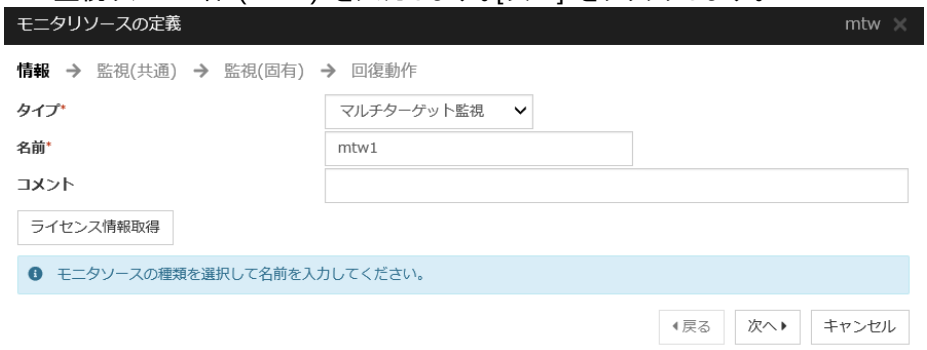
12.[完了] をクリックして設定を終了します。

◇ マルチターゲット監視リソース

Microsoft Azure の Service Management API への通信を監視するカスタム監視リソースと、仮想マシンで構成されたクラスタ間の IP 監視リソースの両方の状態を確認するマルチターゲット監視リソースを作成します。両方の監視リソースの状態が異常となった際に、NP 解決用の処理を記載したスクリプトを実行します。

マルチターゲット監視リソースの詳細は『リファレンスガイド』-「マルチターゲット監視リソースを理解する」を参照してください。

1. [モニタリソース一覧] で [追加] をクリックします。
2. [タイプ] ボックスでモニタリソースのタイプ (マルチターゲット監視) を選択し、[名前] ボックスに監視リソース名 (mtw1) を入力します。[次へ] をクリックします。



3. [監視(共通)] 画面が表示されます。
[監視タイミング] が [常時] であることを確認し、[次へ] をクリックします。

4. [監視(固有)] 画面が表示されます。
   利用可能なモニタリソース一覧から [追加] を選択し、Service Management API への疎通確認用カスタム監視リソース、両サーバに設定したそれぞれの IP 監視リソースの3つの監視リソースを追加します(genw1、ipw1、ipw2)。[次へ] をクリックします。

5. [回復動作] 画面が表示されます。
   [回復動作] に [最終動作のみ実行]、[回復対象] に [LocalServer]、[最終動作] に [クラスタサービス停止と OS シャットダウン] を設定します。

6. [完了] をクリックして設定を終了します。

4) クラスタプロパティの設定

クラスタプロパティの詳細は『リファレンスガイド』-「クラスタプロパティ」を参照してください。

◇ クラスタプロパティ

Microsoft Azure と CLUSTERPRO の連携用に、クラスタプロパティ内の設定を以下のように設定します。

1. Cluster WebUI から設定モードへ移動し、クラスタ名のプロパティアイコンをクリックします。

2. [タイムアウト] タブを選択します。ハートビートの[タイムアウト]に以下の「A + B + C」の結果を設定します。

   A :NP 解決用のマルチターゲット監視リソースで監視している監視リソースの[インターバル] × ([リトライ回数] + 1)

   ※3つある監視リソースのうち上記計算式の結果が大きい方を選択してください。

   B :マルチターゲット監視リソースの [インターバル] × ([リトライ回数] + 1)

   C :30秒(マルチターゲット監視リソースでの異常検出前にハートビートがタイムアウトしないようにするための猶予時間。適宜変更可能)

   注:ハートビートのタイムアウト値が、NP 解決用のモニタで異常を検出する時間より短い場合、NP 解決処理が動作する前にハートビートのタイムアウトを検出します。この場合、待機サーバでサービスが起動され、クラスタ内でサービスの二重起動が発生する可能性があります。

3. [OK] をクリックします。

5) 設定の反映とクラスタの起動

1. Cluster WebUI の設定モード から、[設定の反映] をクリックします。
   [設定を反映しますか。] というポップアップメッセージが表示されますので、[OK] をクリックします。
   アップロードに成功すると、[反映に成功しました。] のメッセージが表示されますので、[OK] をクリックします。
   アップロードに失敗した場合は、表示されるメッセージに従って操作を行ってください。
2. Cluster WebUI の ツールバーのドロップダウンメニューで [操作モード] を選択して、操作モードに切り替えます。
3. Cluster WebUI の[ステータス] タブから [クラスタ開始] をクリックし、確認画面で [開始] をクリックします。

詳細は『インストール&設定ガイド』-「クラスタを生成するには」を参照してください。

3.4 動作確認

構築した環境が正常に動作するかを、監視異常を発生させフェイルオーバグループがフェイルオーバすることにより確認します。
既にクラスタが正常に起動している状態からの確認手順は以下のとおりです。

1. フェイルオーバグループ(failover1)が、現用系ノードの node-1で起動します。Cluster WebUI [ステータス]タブにおいて failover1が node-1で[起動済]になっていることを確認します。
2. Microsoft Azure ポータルにログインし、DNS ゾーンブレードより cluster1.zone を選択後、[概要]を選択します。画面右上に表示されている DNS サーバー(画面例では、ネームサーバー 1、ネームサーバー 2、ネームサーバー 3、ネームサーバー 4)を確認します。
3. 上記で確認した DNS サーバーに対し、nslookup コマンドで該当レコードセットが存在することを確認します。
   nslookup test-record1.cluster1.zone <*上記で確認した DNS サーバー*>
4. Microsoft Azure ポータルにおいて、DNS ゾーンから A レコードを手動で削除します。これにより、azurednsw1は監視異常を検出します。DNS ゾーンブレードより cluster1.zone を選択し、[概要]を選択します。
5. 削除するレコードを選択し、[削除]を選択します。削除確認にて[はい]を選択します。
6. azurednsw1の[インターバル]後にフェイルオーバグループ(failover1)が異常になり、ノード node-2へフェイルオーバします。Cluster WebUI [ステータス]タブにおいて failover1が node-2で[起動済]になっていることを確認します。
7. 上記で確認した DNS サーバーに対し、nslookup コマンドで該当レコードセットが存在することを確認します。
   nslookup test-record1.cluster1.zone <*上記で確認した DNS サーバー*>

以上で、DNS サーバーから A レコードを削除した場合におけるフェイルオーバの動作確認は完了です。
その他の障害発生時の動作確認については適宜実施してください。

第 4 章　構築手順(パブリックロードバランサーを使用した HA クラスタの場合)

4.1 構築例について

本書では、Microsoft Azure において、CLUSTERPRO を使用した2ノードでの片方向スタンバイクラスタの構築手順を紹介します。本手順は、node-1 を現用系サーバとしたミラーディスク型の構成を対象としています。
以下の表は既定値が存在しないパラメータ、および既定値から変更したパラメータについて記載しています。

- Microsoft Azureの設定(node-1、node-2で共通の設定)

設定項目	設定値
リソース グループの設定	
名前	TestGroup1
リソース グループの場所	東日本
仮想ネットワークの設定	
名前	Vnet1
アドレス空間	10.5.0.0/24
サブネット名	Vnet1-1
サブネットアドレス範囲	10.5.0.0/24
リソース グループ名	TestGroup1
場所	東日本
ロードバランサーの設定	
名前	TestLoadBalancer
種類	パブリック
パブリックIPアドレス - 名前	TestLoadBalancerPublicIP
パブリックIPアドレス - 割り当て	静的
Resource group	TestGroup1
場所	東日本
バックエンドプール - 名前	TestBackendPool
関連付け先	可用性セット
ターゲット仮想マシン	node-1 node-2
ネットワークIP 構成	10.5.0.120 10.5.0.121
正常性プローブ - 名前	TestHealthProbe
正常性プローブ - ポート	26001
負荷分散規則 - 名前	TestLoadBalancingRule
負荷分散規則 - ポート	80(業務を提供しているポート番号)
負荷分散規則 - バックエンドポート	8080(業務を提供しているポート番号)
受信セキュリティ規則の設定	
名前	TestHTTP
プロトコル	TCP
宛先ポート範囲	8080(業務を提供しているポート番号)

- Microsoft Azureの設定(node-1、node-2でそれぞれ設定)

設定項目	設定値	
	node-1	node-2

仮想マシンの設定		
ディスクの種類	Standard HDD	
ユーザー名	testlogin	
パスワード	PassWord_123	
リソース グループ名	TestGroup1	
場所	東日本	
ネットワーク セキュリティ グループの設定		
名前	NetSecGroup-1	
可用性セットの設定		
名前	AvailabilitySet-1	
更新ドメイン	5	
障害ドメイン	2	
診断ストレージアカウントの設定		
名前	自動生成(testgroup1diag679)	
パフォーマンス	Standard	
レプリケーション	ローカル冗長ストレージ(LRS)	
IP構成の設定		
IPアドレス	10.5.0.120	10.5.0.121
Blobの設定		
名前	node-1Blob1	node-2Blob1
ソースの種類	なし(空のディスク)	
アカウントの種類	Standard HDD	
サイズ	20	

- CLUSTERPROの設定(クラスタプロパティ)

設定項目	設定値	
	node-1	node-2
クラスタ名	Cluster1	
サーバ名	node-1	node-2
タイムアウトタブ - ハートビートタイムアウト	210	

- CLUSTERPROの設定(フェイルオーバグループ)

リソース名	設定項目	設定値
ミラーディスクリソース	リソース名	md
	詳細タブ - データパーティションのドライブ文字	G:
	詳細タブ - クラスタパーティションのドライブ文字	F:
Azure プローブポートリソース	リソース名	azurepp1
	プローブポート	26001(正常性プローブ - ポートで指定した値)

- CLUSTERPROの設定(監視リソース)

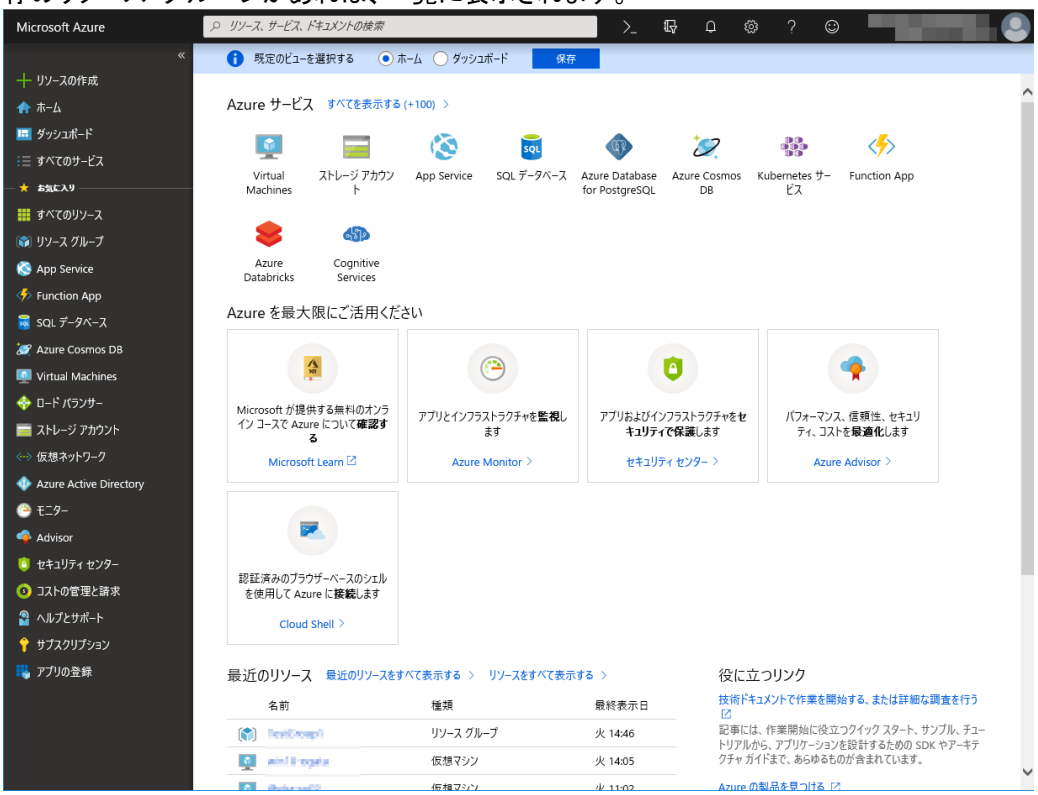
監視リソース名	設定項目	設定値
ミラーディスク監視リソース	－	－
Azure プローブポート監視リソース	監視リソース名	azureppw1
	回復対象	azurepp1
Azure ロードバランス監視リソース	監視リソース名	aurelbw1
	回復対象	azurepp1
カスタム監視リソース	監視リソース名	genw1
	この製品で作成したスクリプト	オン
	監視タイプ	同期
	正常な戻り値	0
	回復動作	最終動作のみ実行
	回復対象	LocalServer
IP監視リソース	監視リソース名	ipw1
	監視を行うサーバ	node-1
	IPアドレス	10.5.0.121
	回復動作	最終動作のみ実行
	回復対象	LocalServer
IP監視リソース	監視リソース名	ipw2
	監視を行うサーバ	node-2
	IPアドレス	10.5.0.120
	回復動作	最終動作のみ実行
	回復対象	LocalServer
マルチターゲット監視リソース	監視リソース名	mtw1
	監視リソース一覧	genw1 ipw1 ipw2
	回復動作	最終動作のみ実行
	回復対象	LocalServer
	最終動作前にスクリプトを実行する	オン
	タイムアウト	30

4.2 Microsoft Azure の設定

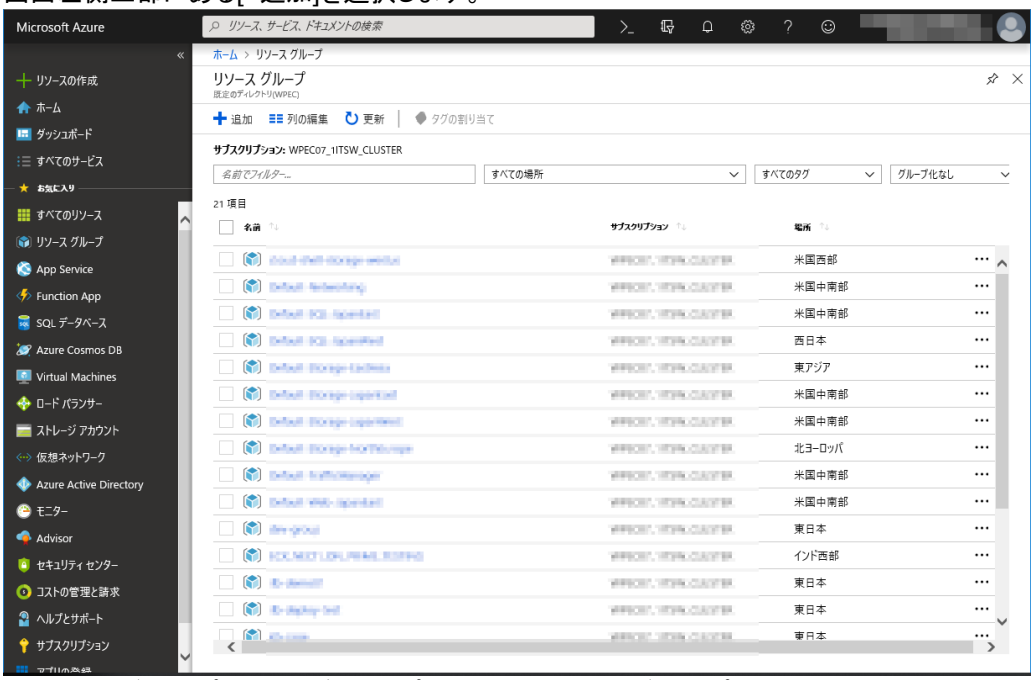
1) リソースグループの作成

Microsoft Azure ポータル(https://portal.azure.com/)にログインし、以下の手順でリソース グループを作成します。

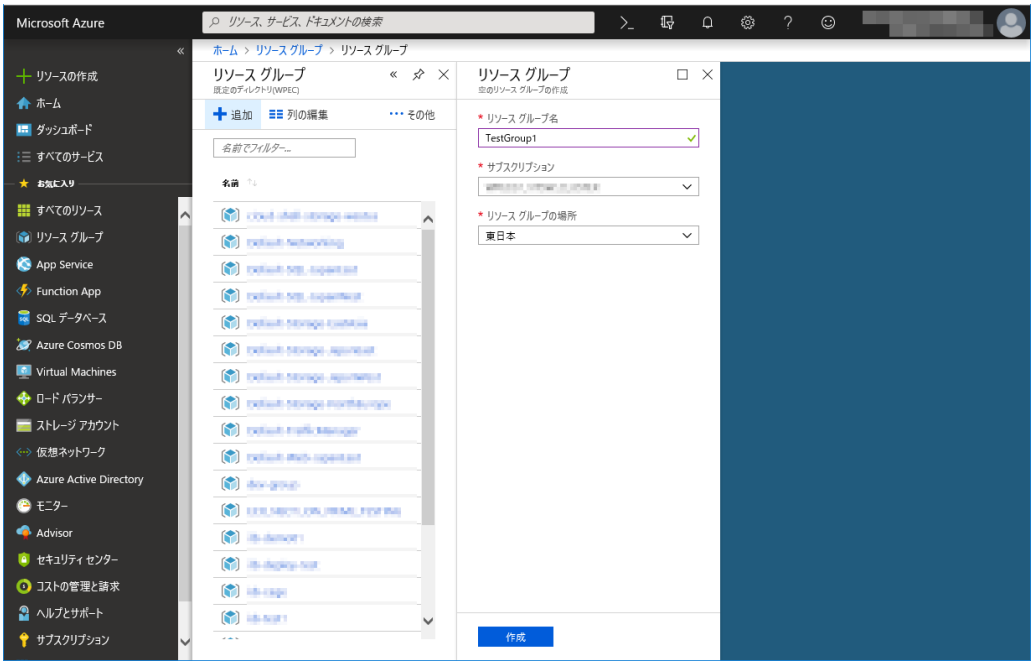
1. 画面左側のメニューにある[リソース グループ]もしくはリソース グループアイコンを選択します。既存のリソース グループがあれば、一覧に表示されます。



2. 画面左側上部にある[+追加]を選択します。



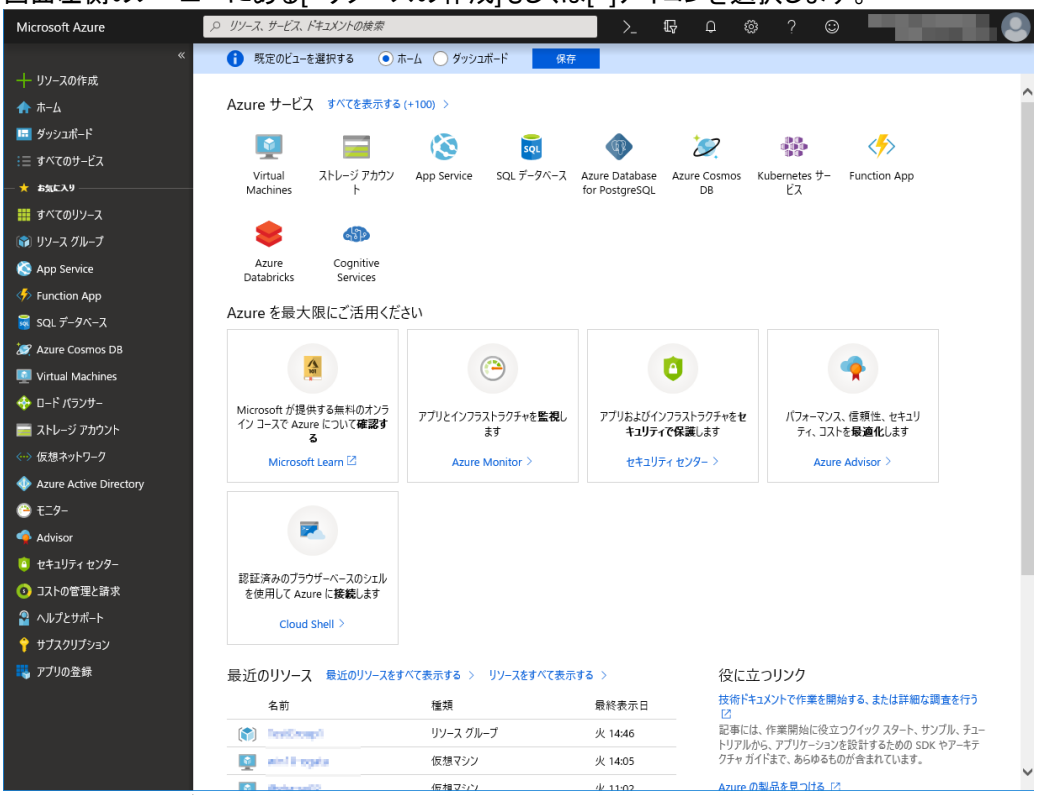
3. [リソース グループ名]、[サブスクリプション]、[リソース グループの場所]を設定し、[作成]を選択します。



2) 仮想ネットワークの作成

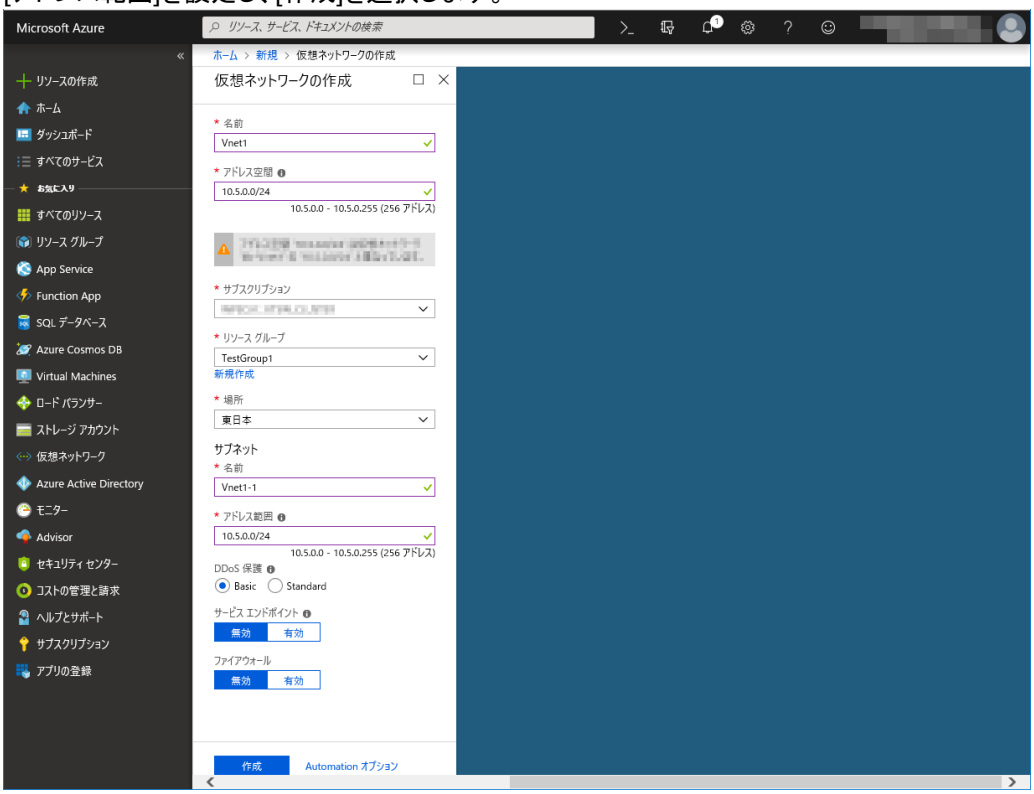
Microsoft Azure ポータル(https://portal.azure.com/)にログインし、以下の手順で仮想ネットワークを作成します。

1. 画面左側のメニューにある[+リソースの作成]もしくは[+]アイコンを選択します。



2. [ネットワーキング]>[仮想ネットワーク]を選択します。

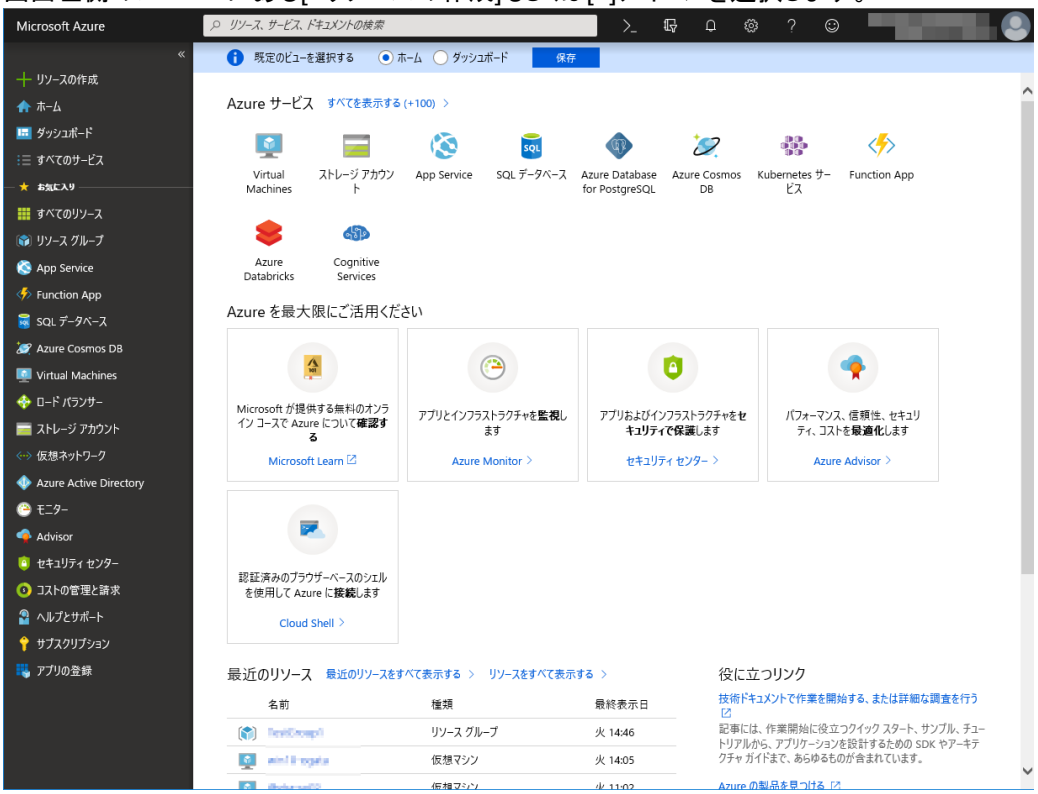
3. [名前]、[アドレス空間]、[サブスクリプション]、[リソース グループ名]、[場所]、サブネットの[名前]、[アドレス範囲]を設定し、[作成]を選択します。



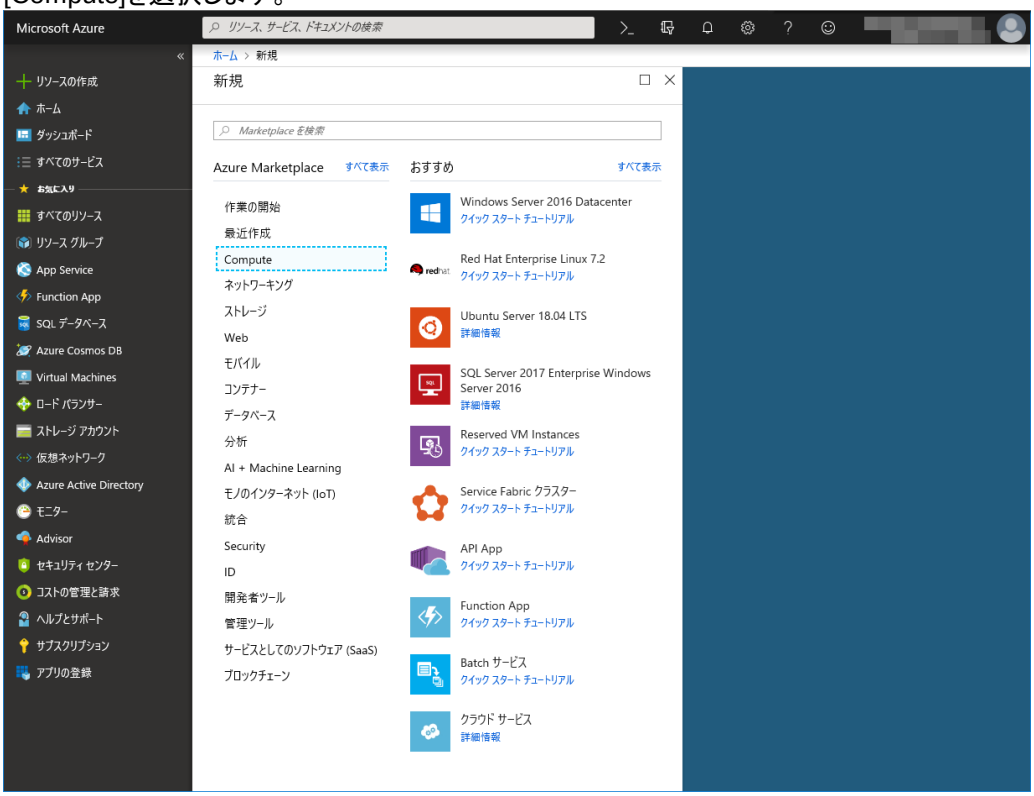
3) 仮想マシンの作成

Microsoft Azure ポータル(https://portal.azure.com/)にログインし、以下の手順で仮想マシンおよびディスクを追加します。
クラスタを構成する仮想マシンを必要な数だけ作成します。node-1、node-2 の順に作成します。

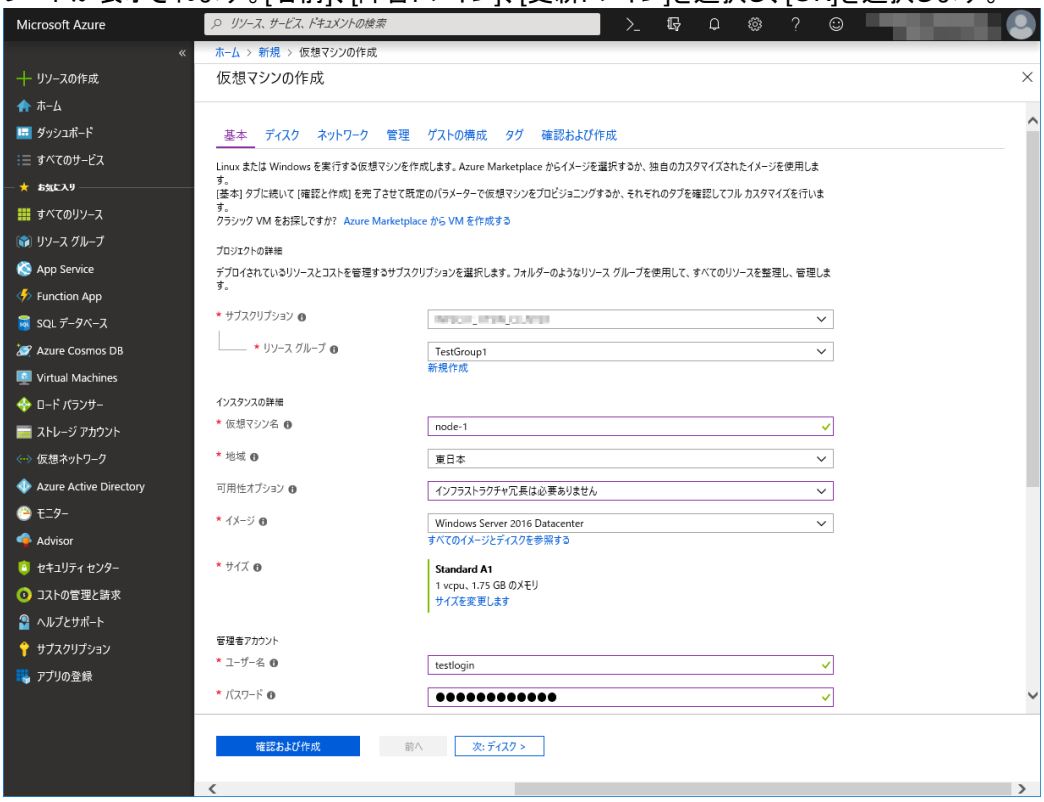
1. 画面左側のメニューにある[+リソースの作成]もしくは[+]アイコンを選択します。



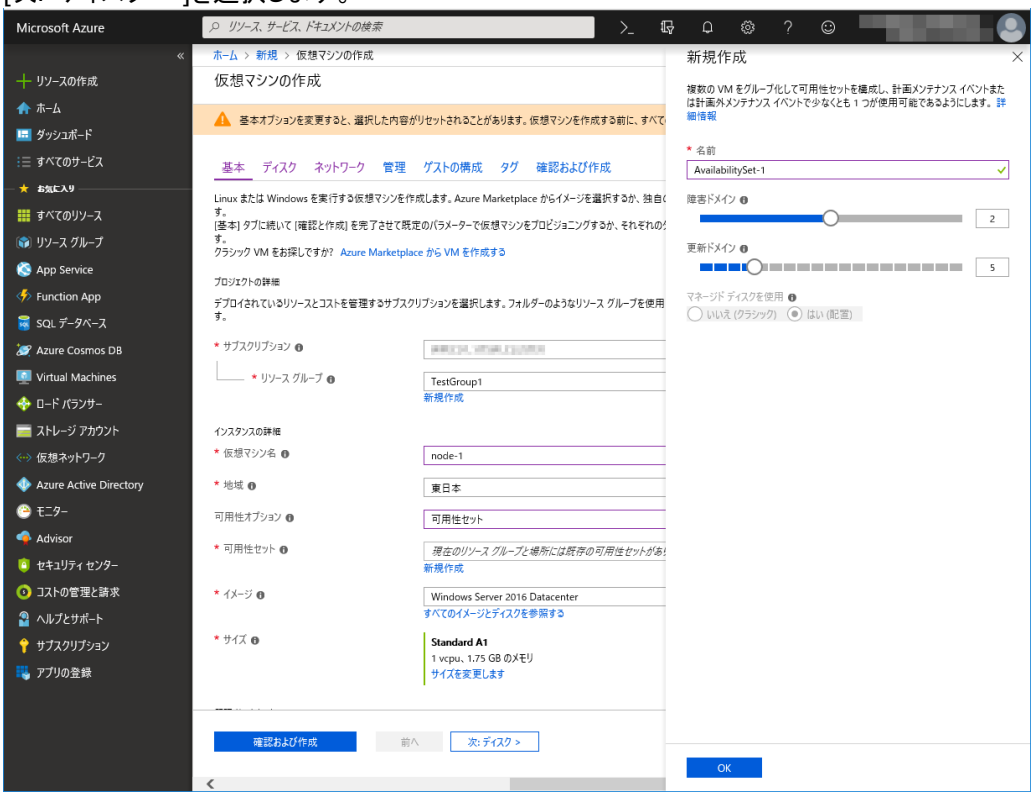
2. [Compute]を選択します。

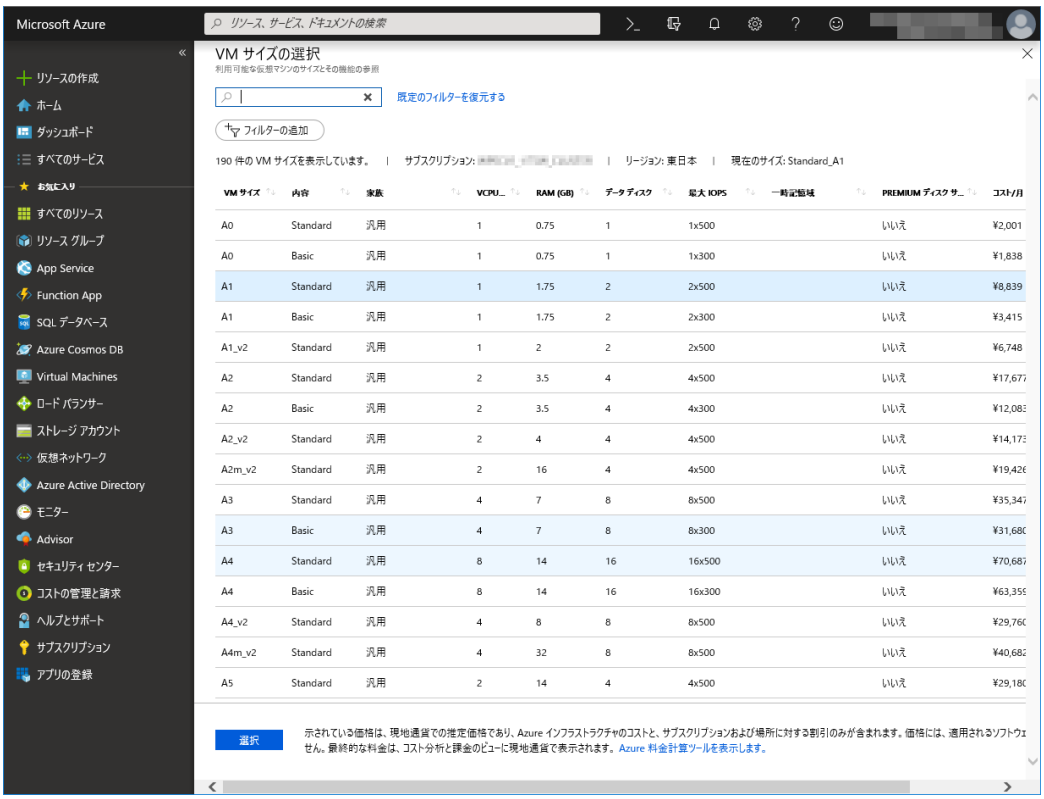


3. [Windows Server 2016 Datacenter]を選択します。
4. [基本]タブが表示されますので、[サブスクリプション]、[リソース グループ]、[仮想マシン名]、[地域]、[イメージ]、[サイズ]、[ユーザー名]、[パスワード]、[パスワードの確認]を設定します。
[可用性オプション]で可用性セットを選択し、[可用性セット]で新規作成を選択すると、[新規作成]ブレードが表示されます。[名前]、[障害ドメイン]、[更新ドメイン]を選択し、[OK]を選択します。

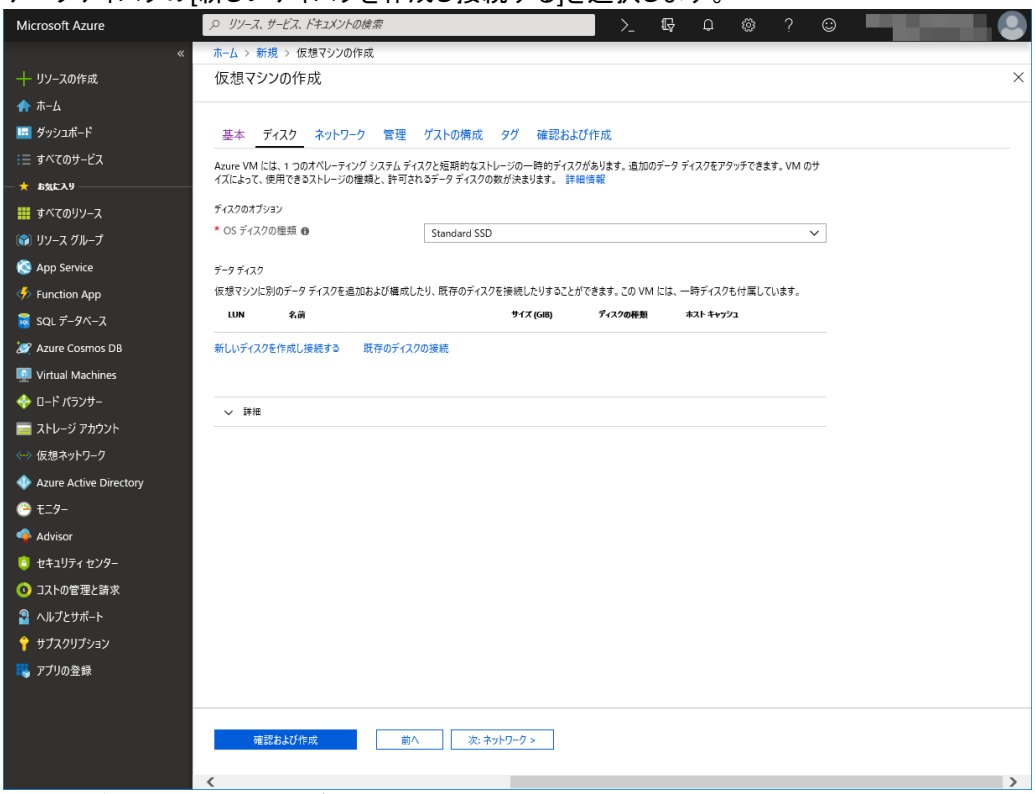


[サイズを変更します]を選択すると、[VM サイズの選択]ブレードが表示されます。
仮想マシンの目的に合ったサイズを一覧から選択し、[選択]を選択します。本書では[A1 Standard]を選択します。
[仮想マシン名]は、node-1 の場合は node-1、node-2 の場合は node-2 です。
[次: ディスク >]を選択します。

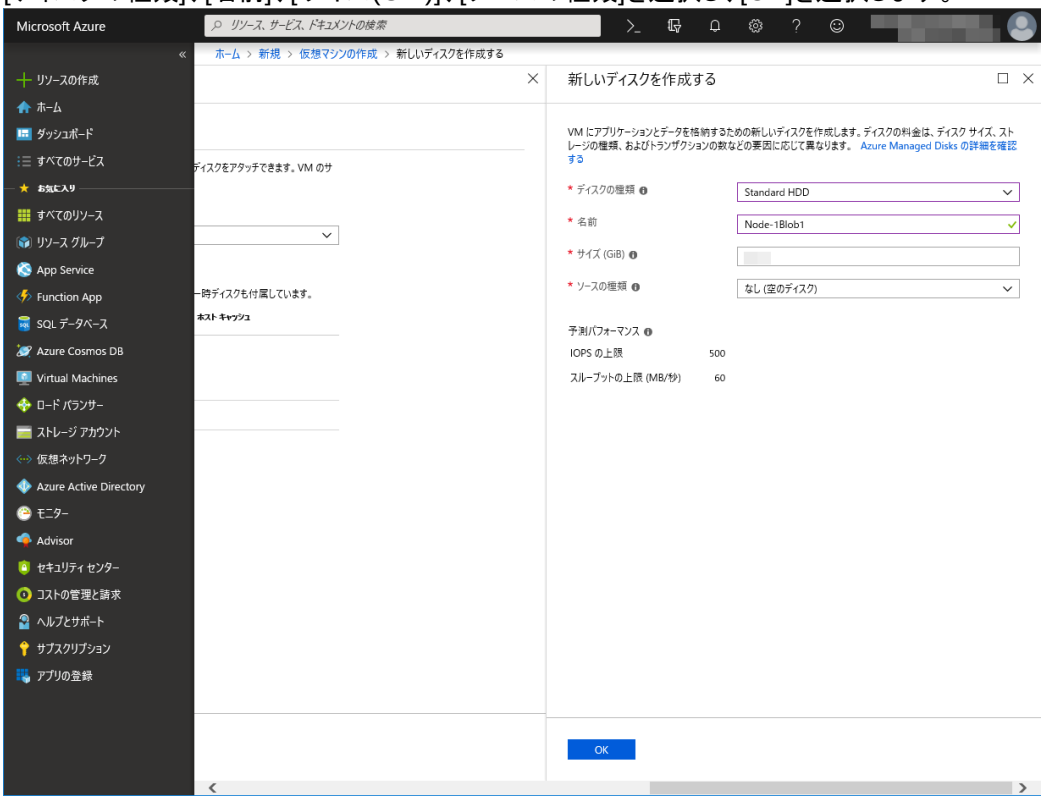




5. [ディスク]タブが表示されますので、以下の手順でミラーディスク(クラスタパーティション、データパーティション)に使用する Blob を追加します。
データディスクの[新しいディスクを作成し接続する]を選択します。

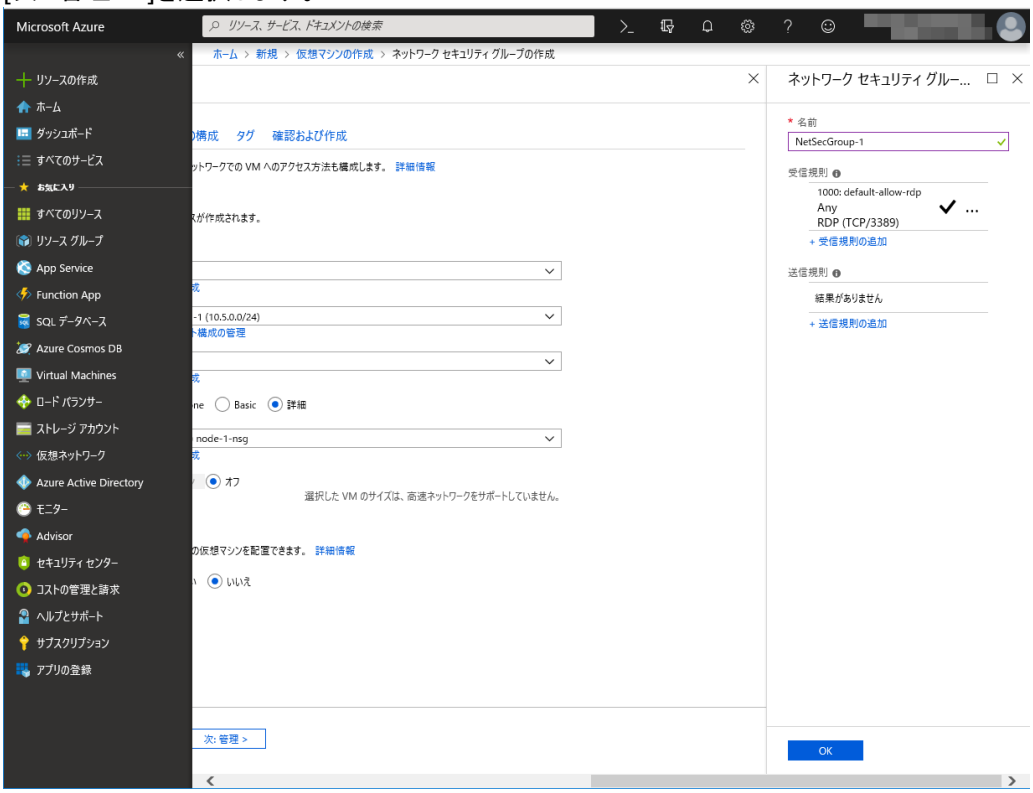


6. [新しいディスクを作成する]ブレードが表示されます。
[ディスクの種類]、[名前]、[サイズ(GiB)]、[ソースの種類]を選択し、[OK]を選択します。

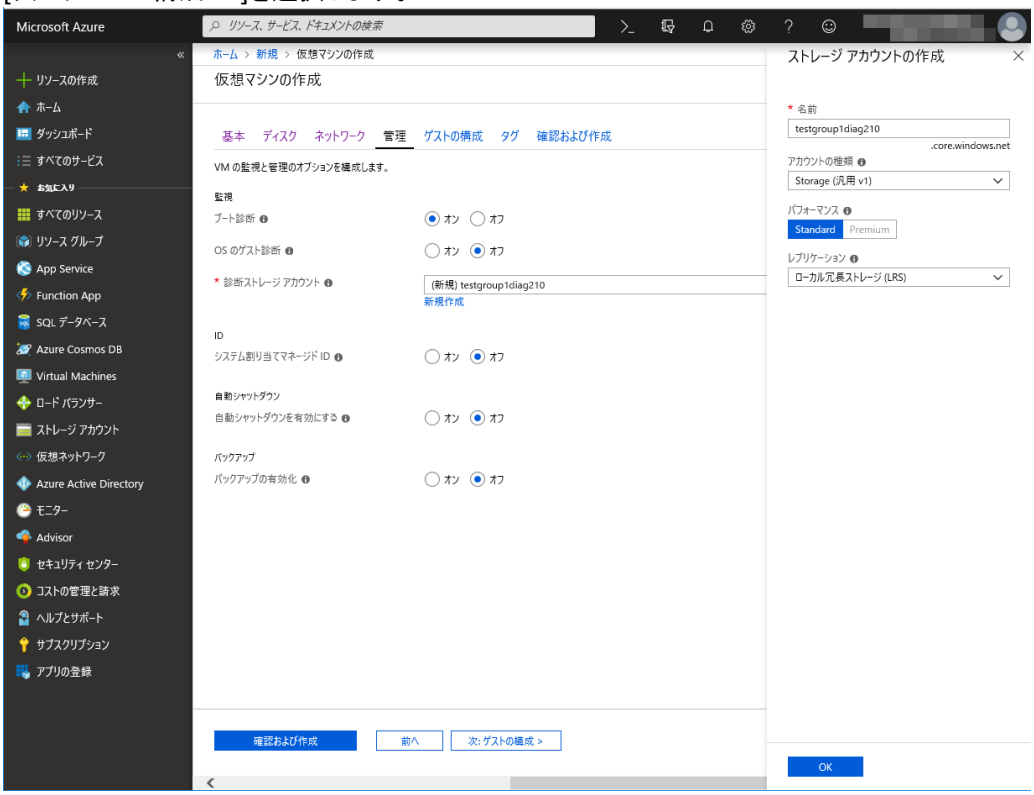


7. [次: ネットワーク >]を選択します。

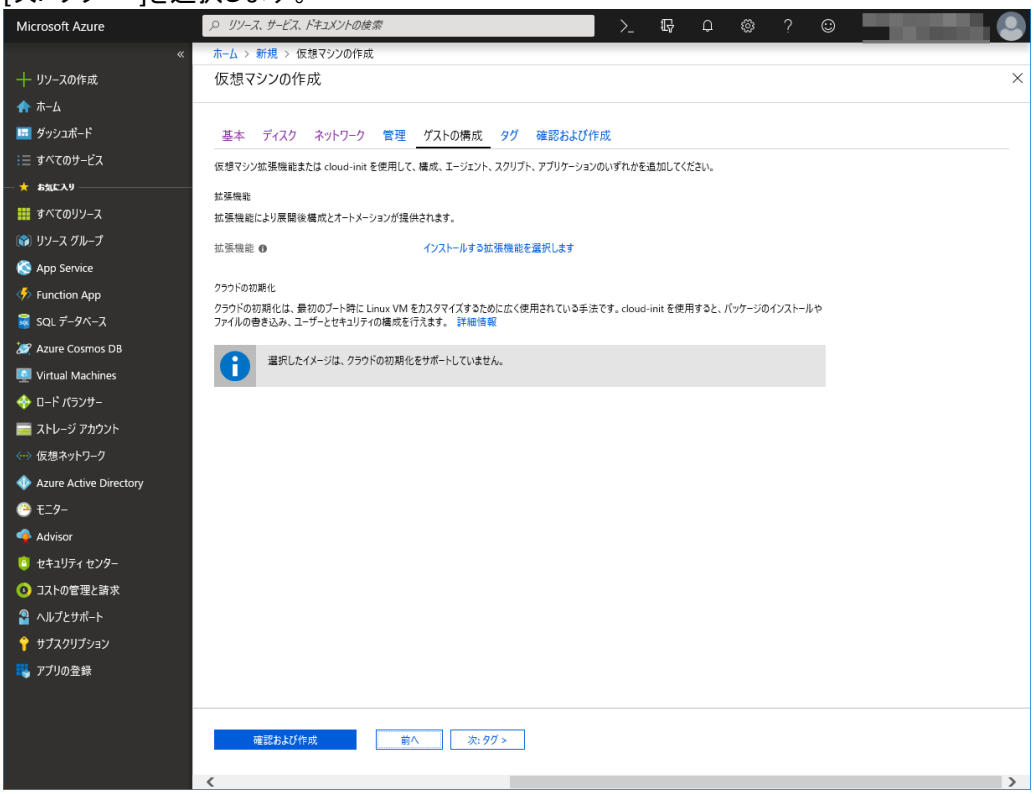
8. [ネットワーク]タブが表示されます。
[仮想ネットワーク]、[サブネット]、[ネットワーク セキュリティ グループ]、[ネットワーク セキュリティ グループの構成]を選択します。
[ネットワーク セキュリティ グループの構成]の新規作成を選択すると、[ネットワーク セキュリティ グループの作成]ブレードが表示されますので、[名前]を選択し、[OK]を選択します。
[次: 管理 >]を選択します。



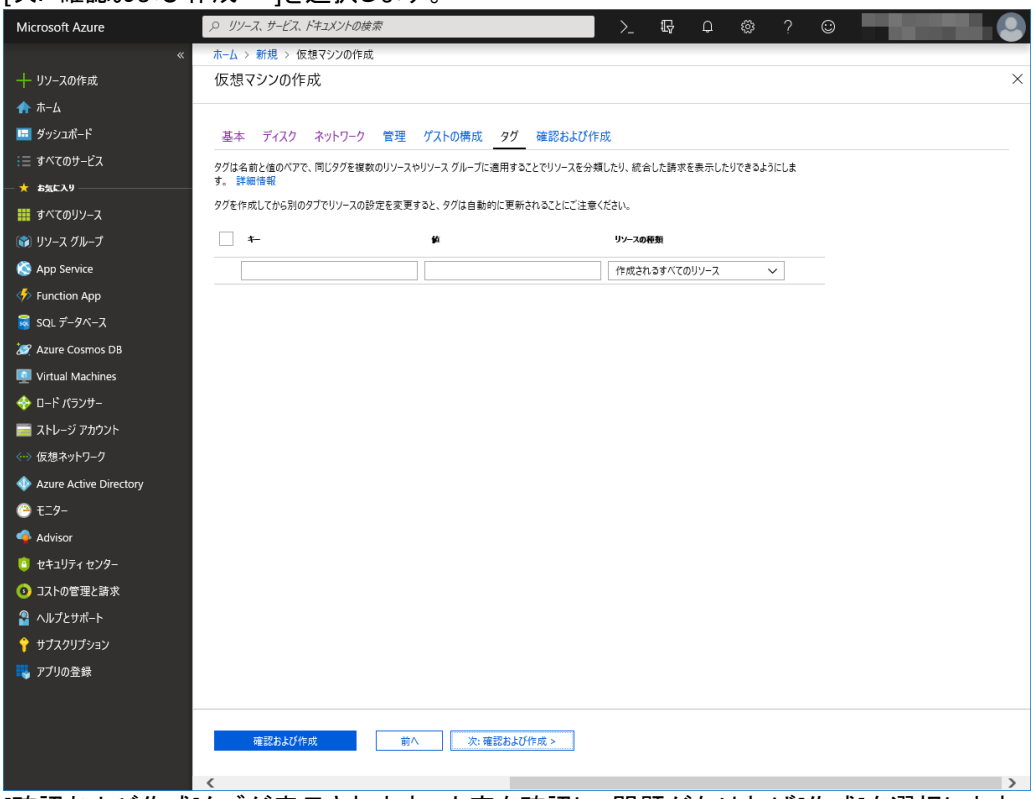
9. [管理]タブが表示されます。
[診断ストレージアカウント]で[新規作成]を選択すると、[ストレージアカウントの作成]ブレードが表示されます。
[名前]、[アカウントの種類]、[レプリケーション]を選択し、[OK]を選択します。
[診断ストレージアカウント]は、自動生成される既定値が入力されています。
[次: ゲストの構成 >]を選択します。



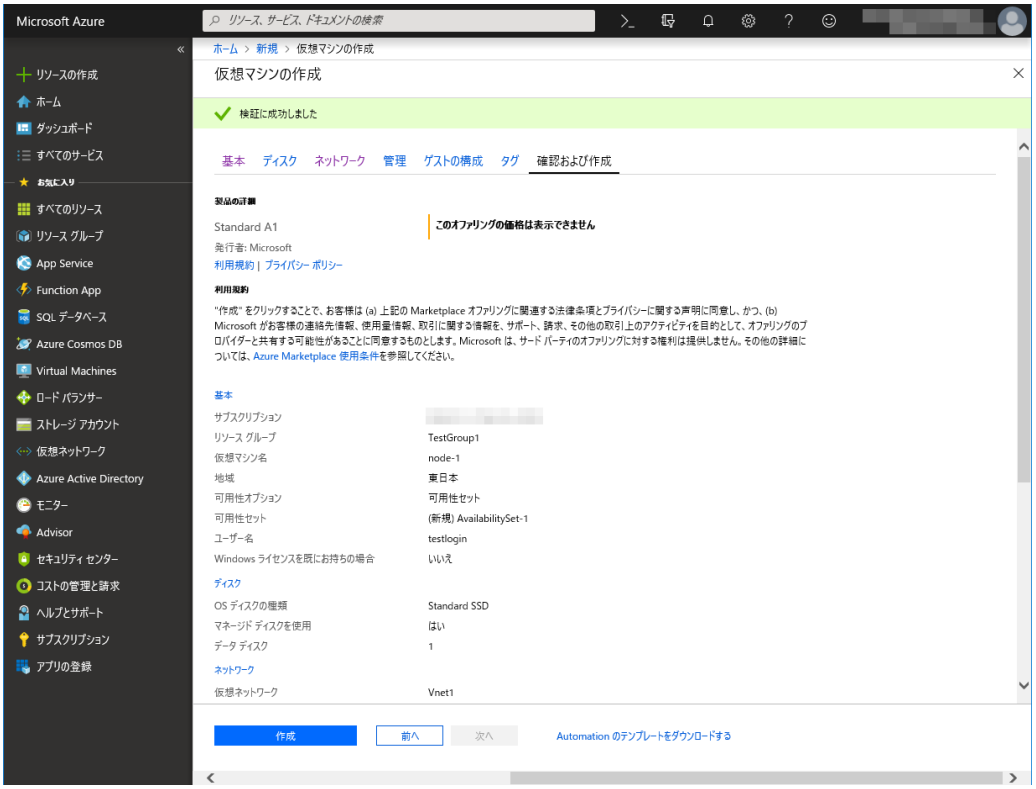
10. [次: タグ >]を選択します。



11. [次: 確認および作成 >]を選択します。



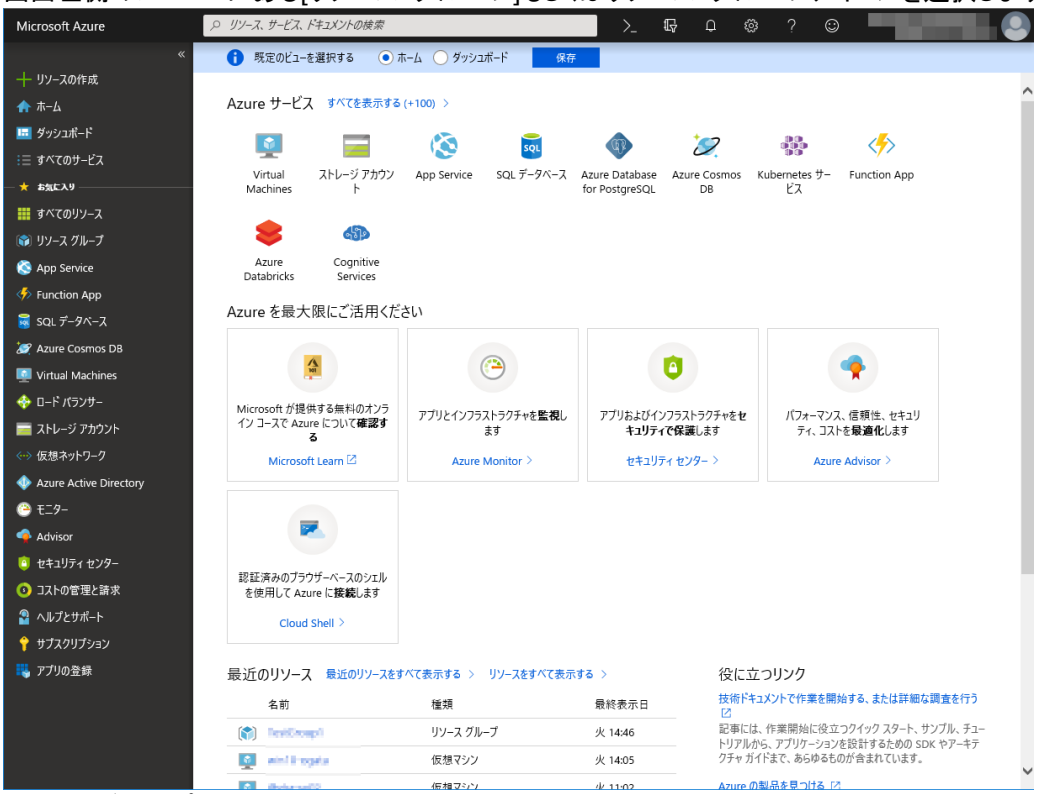
12. [確認および作成]タブが表示されます。内容を確認し、問題がなければ[作成]を選択します。デプロイが開始されます。デプロイには数分時間が掛かります。



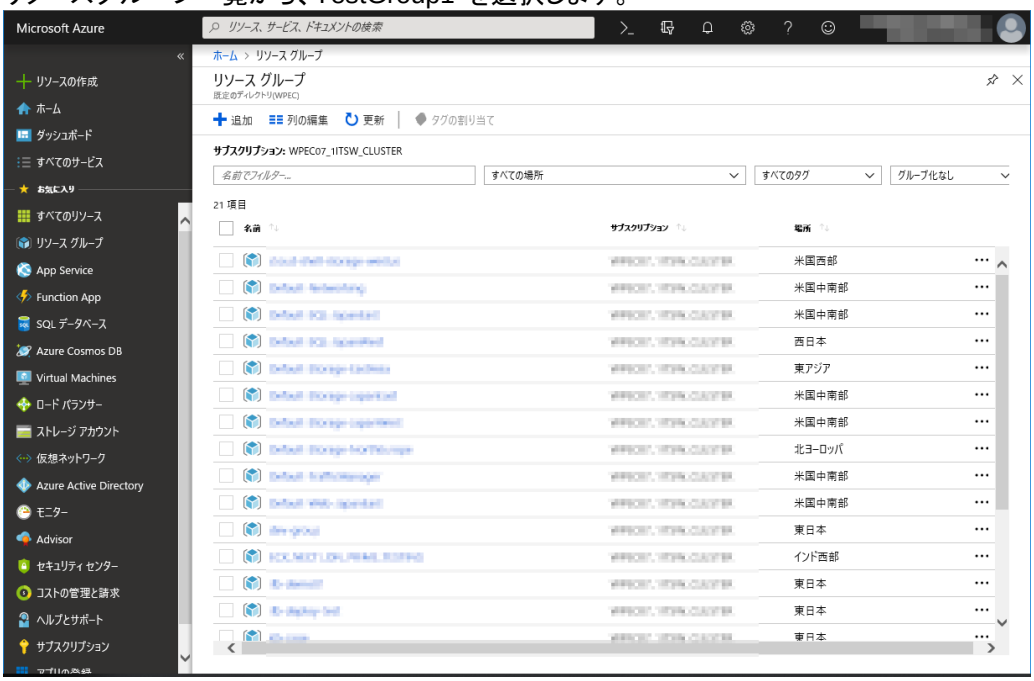
4) プライベート IP アドレスの設定

Microsoft Azure ポータル(https://portal.azure.com/)にログインし、以下の手順でプライベート IP アドレスの設定を変更します。IP アドレスは初期設定では動的割り当てとなっているため、静的割り当てに変更します。node-1、node-2 の順に実行します。

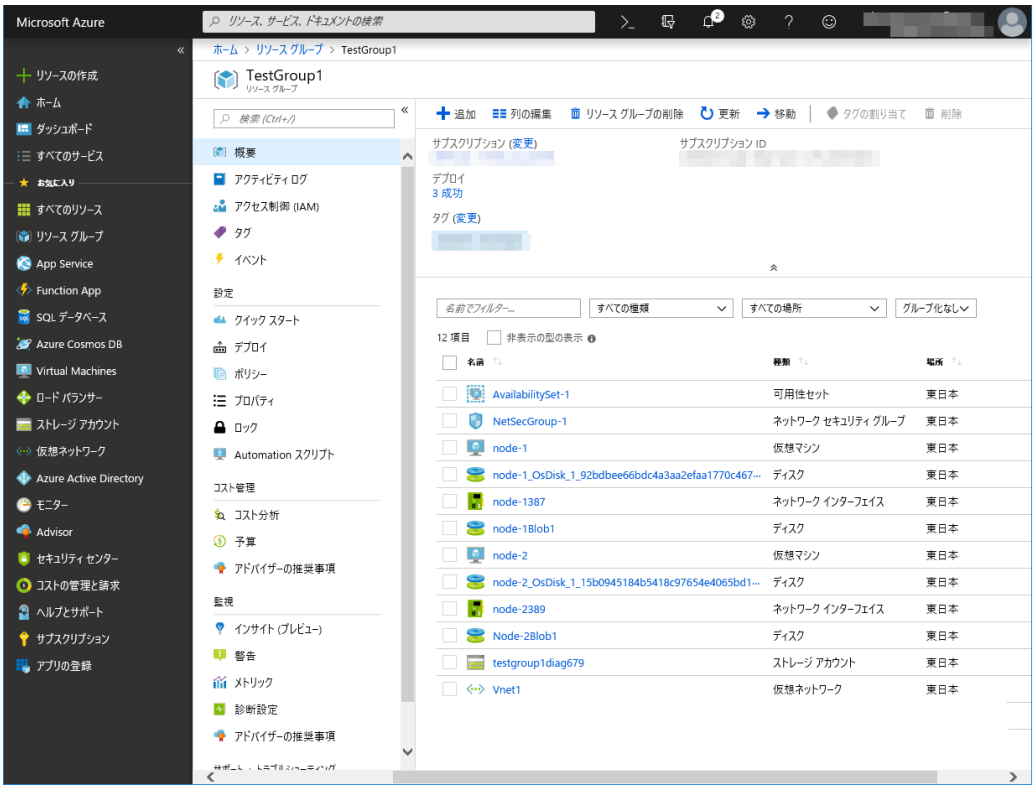
1. 画面左側のメニューにある[リソース グループ]もしくはリソース グループアイコンを選択します。



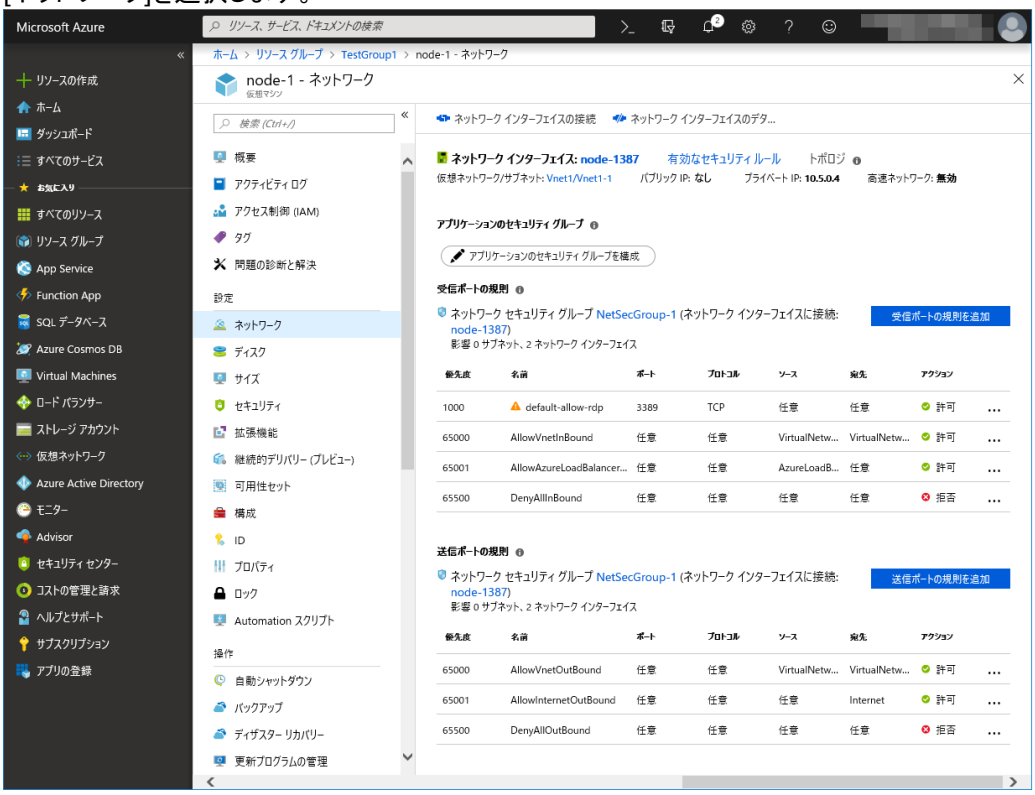
2. リソースグループ一覧から、TestGroup1 を選択します。



3. TestGroup1 の概要が表示されます。項目一覧から仮想マシン node-1 もしくは node-2 を選択します。

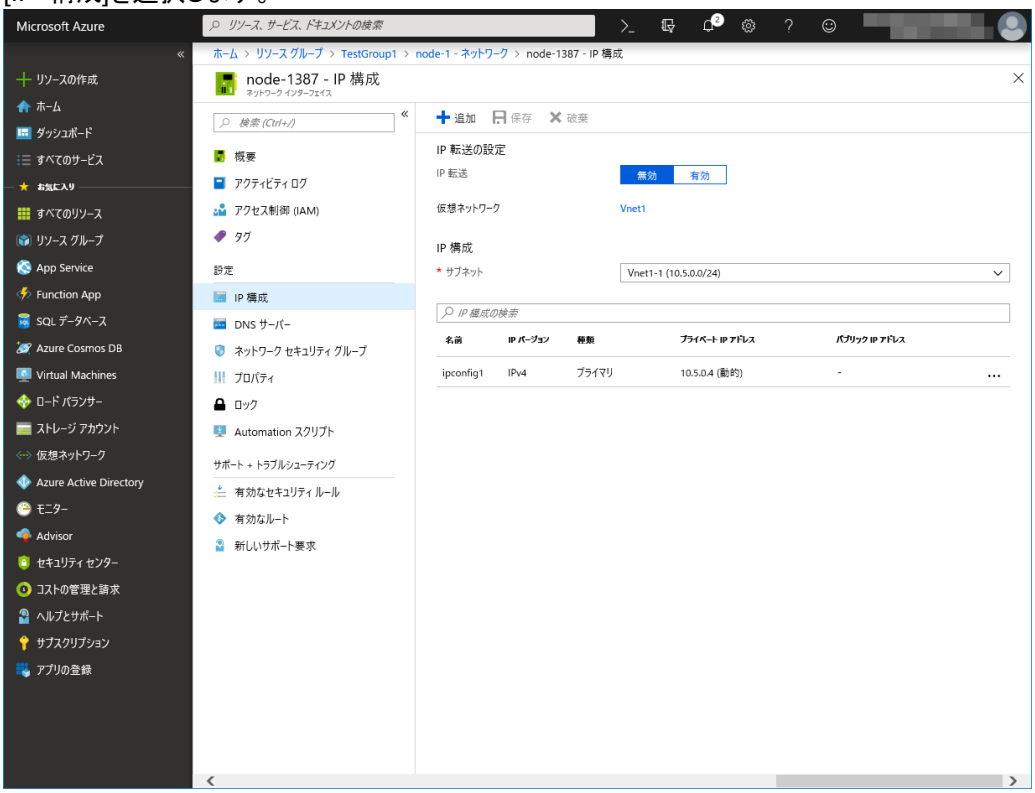


4. [ネットワーク]を選択します。

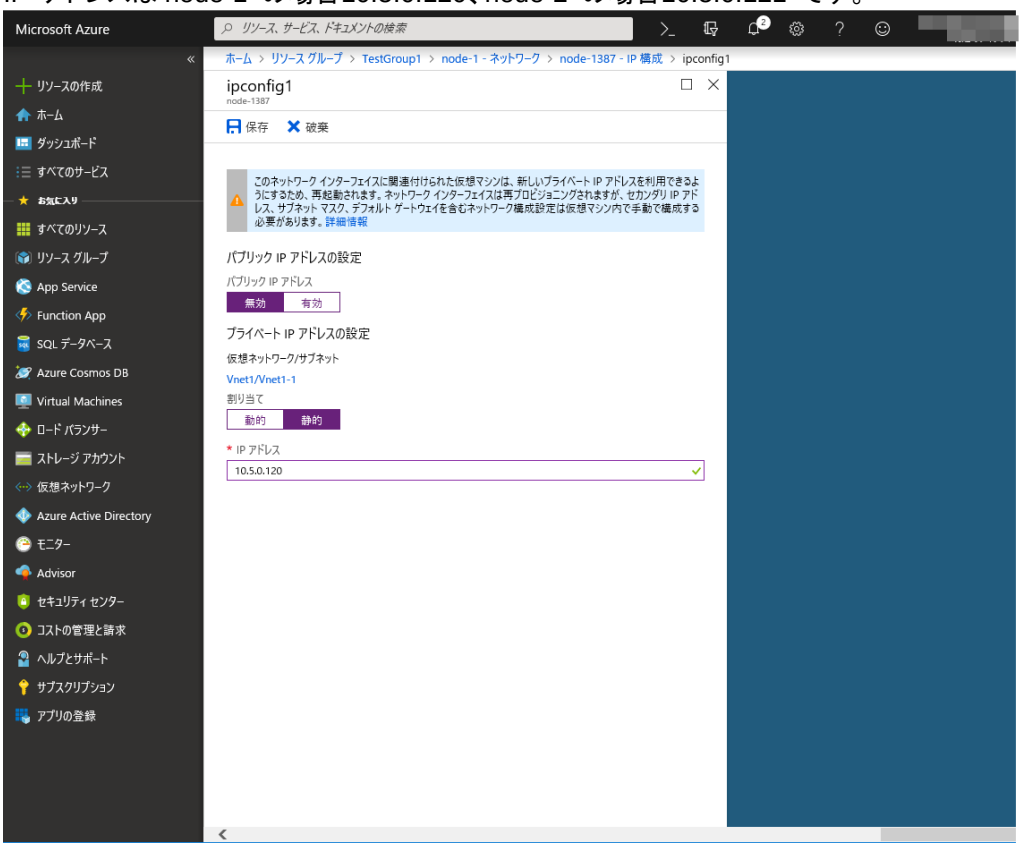


5. 一覧に1 つ表示されているネットワーク インターフェイスを選択します。ネットワーク インターフェイス名は自動生成されます。

6. [IP 構成]を選択します。



7. 一覧に1 つ表示されている ipconfig1 を選択します。
8. [プライベート IP アドレスの設定]の下に表示されている[割り当て]を、[静的]に変更します。その下にある[IP アドレス]に、静的に割り当てる IP アドレスを入力し、画面上部にある[保存]を選択します。IP アドレスは node-1 の場合10.5.0.120、node-2 の場合10.5.0.121 です。



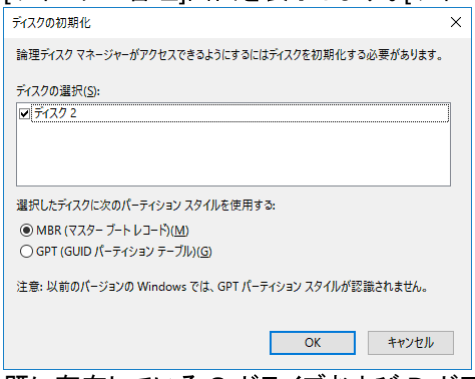
9. 新しいプライベートIP アドレスを利用できるようにするために、仮想マシンが自動的に再起動されます。

5) 仮想マシンの設定

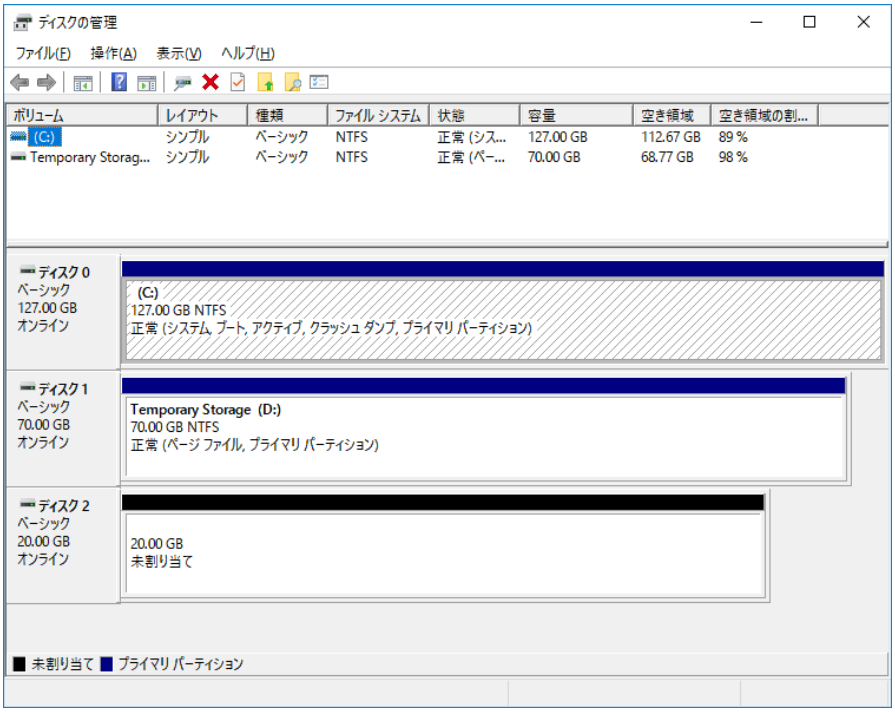
作成した node-1、node-2 へログインし、以下の手順で設定します。
必要な場合、OS を日本語化します。node-1、node-2 の順に実行してください。

次にミラーディスクリソース用のパーティションを設定します。追加した Blob にファイルシステムを作成します。
ミラーディスクリソース用のパーティションについては、『インストール&設定ガイド』-「第1章 システム構成を決定する」-「ハードウェア構成後の設定」-「2. ミラー用パーティションを設定する (ミラーディスク使用時は必須)」を参照してください。

1. [ディスクの管理]画面を表示します。[ディスクの初期化]ダイアログが表示されます。

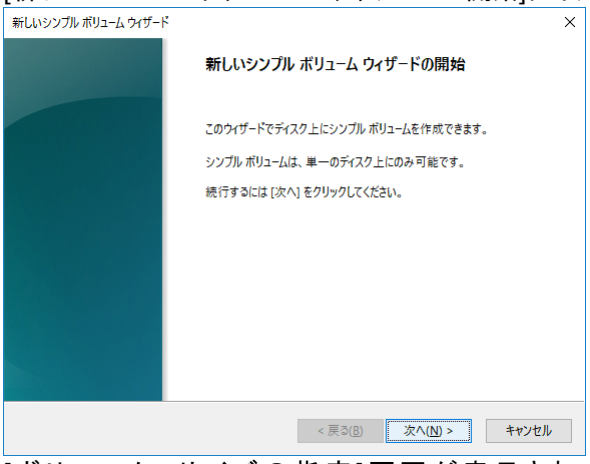


2. 既に存在している C ドライブおよび D ドライブの下に追加ディスクがディスク2 として未割り当て状態で表示されていることを確認します。

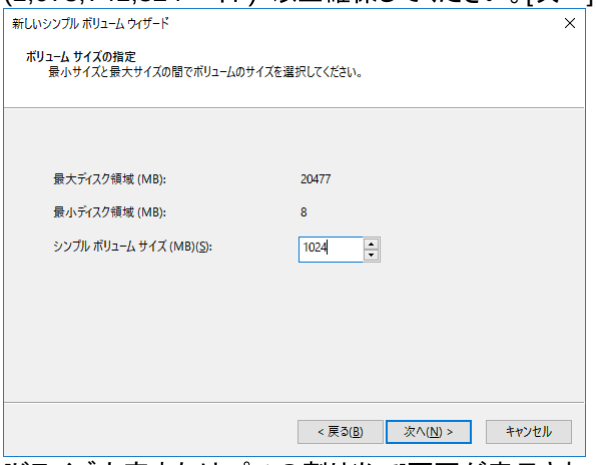


3. クラスタパーティションを作成します。[ディスク 2]上で右クリックし、[新しいシンプル ボリューム]を選択します。

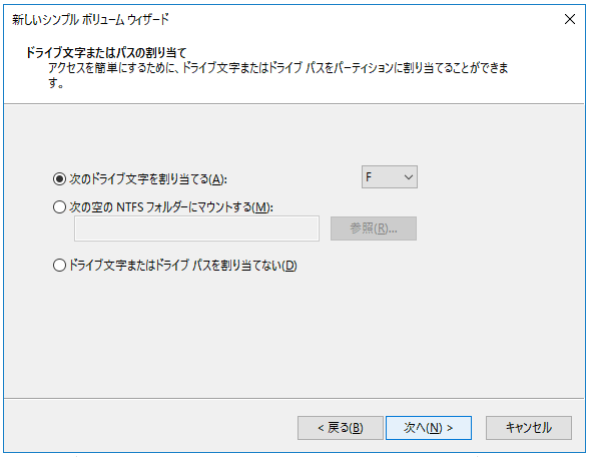
4. [新しいシンプル ボリューム ウィザードの開始]ダイアログが表示されます。[次へ]を選択します。



5. [ボリューム サイズの指定]画面が表示されます。クラスタパーティションは 1024MB (1,073,741,824バイト) 以上確保してください。[次へ]を選択します。

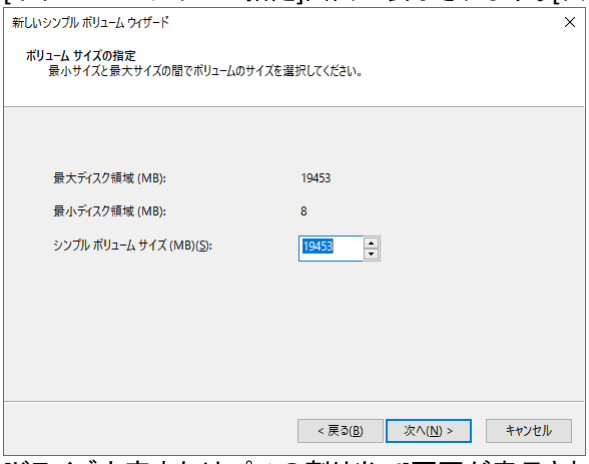


6. [ドライブ文字またはパスの割り当て]画面が表示されます。[次のドライブ文字を割り当てる]にF ドライブを選択します。フォーマットは行わず RAW パーティションのまま使用します。

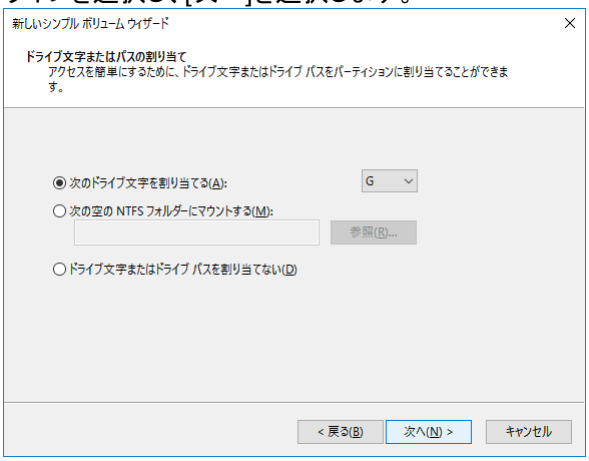


7. 次にデータパーティションを作成します。[ディスク2]上で右クリックし、[新しいシンプル ボリューム]を選択します。
8. [新しいシンプル ボリューム ウィザードの開始]ダイアログが表示されます。[次へ]を選択します。

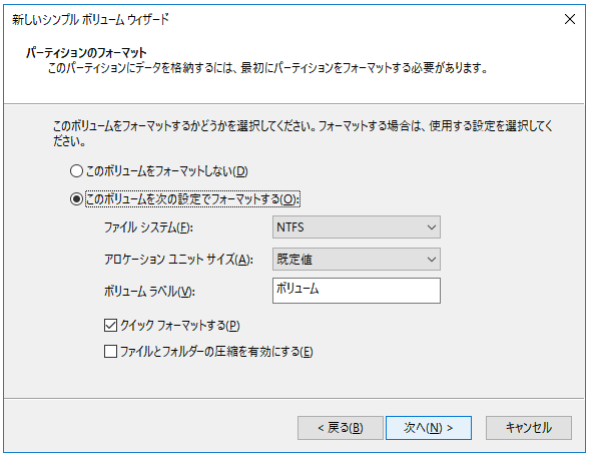
9. [ボリューム サイズの指定]画面が表示されます。[次へ]を選択します。



10. [ドライブ文字またはパスの割り当て]画面が表示されます。[次のドライブ文字を割り当てる]に G ドライブを選択し、[次へ]を選択します。

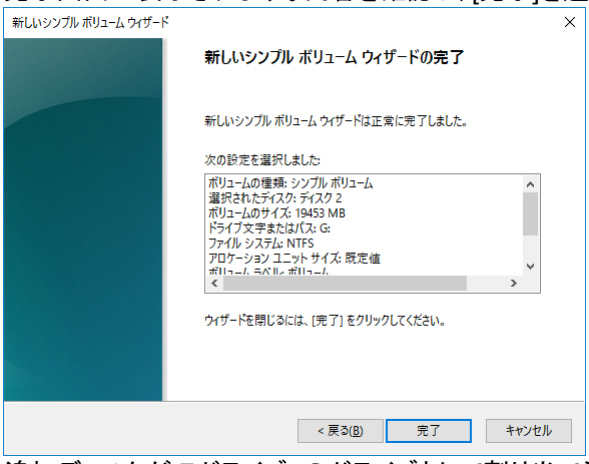


11. [パーティションのフォーマット]画面が表示されます。[ファイル システム]が NTFS であることを確認します。

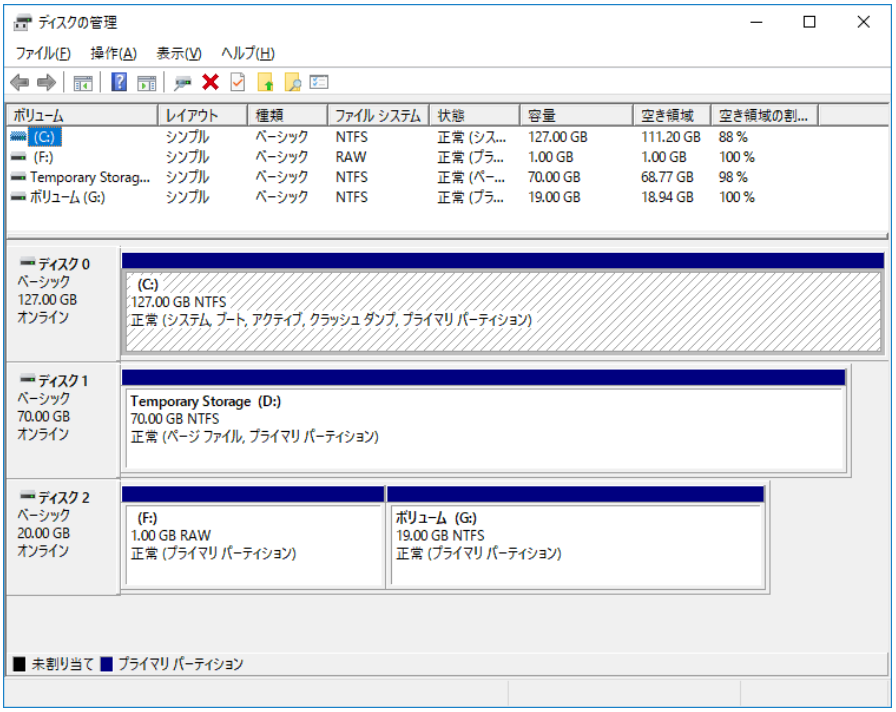


12. [次へ]を選択します。

13. 完了画面が表示されます。内容を確認し、[完了]を選択します。



14. 追加ディスクが Ｆドライブ、Ｇドライブとして割り当てられていることを確認します。

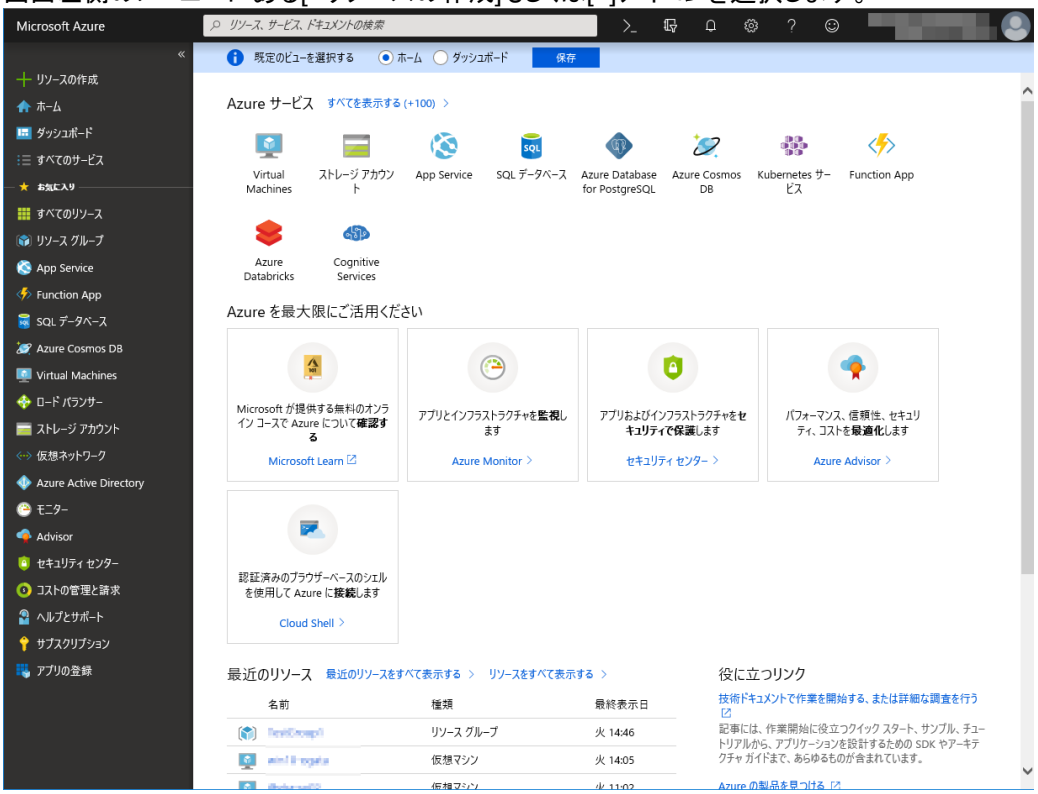


6) ロードバランサーの作成

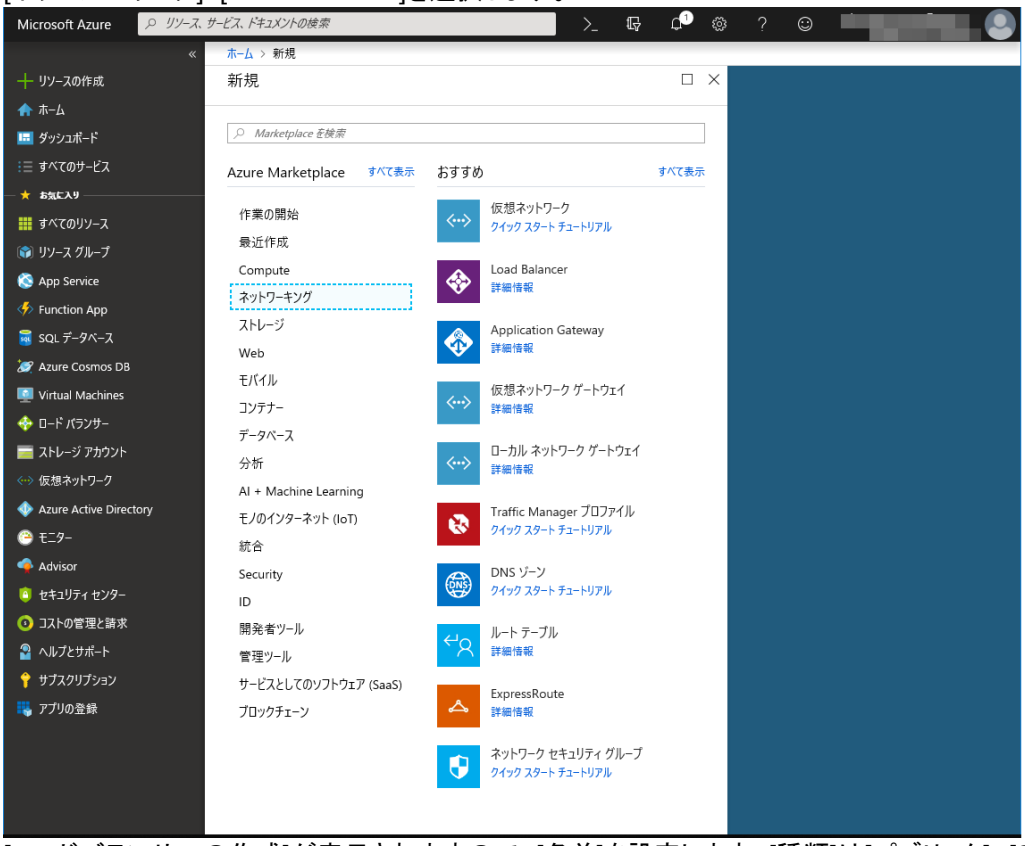
Microsoft Azure ポータル(https://portal.azure.com/)にログインし、以下の手順でロードバランサーを追加します。
詳細は以下の Web サイトを参照してください。

- Load Balancer :
  https://docs.microsoft.com/ja-jp/azure/load-balancer/

1. 画面左側のメニューにある[+リソースの作成]もしくは[+]アイコンを選択します。

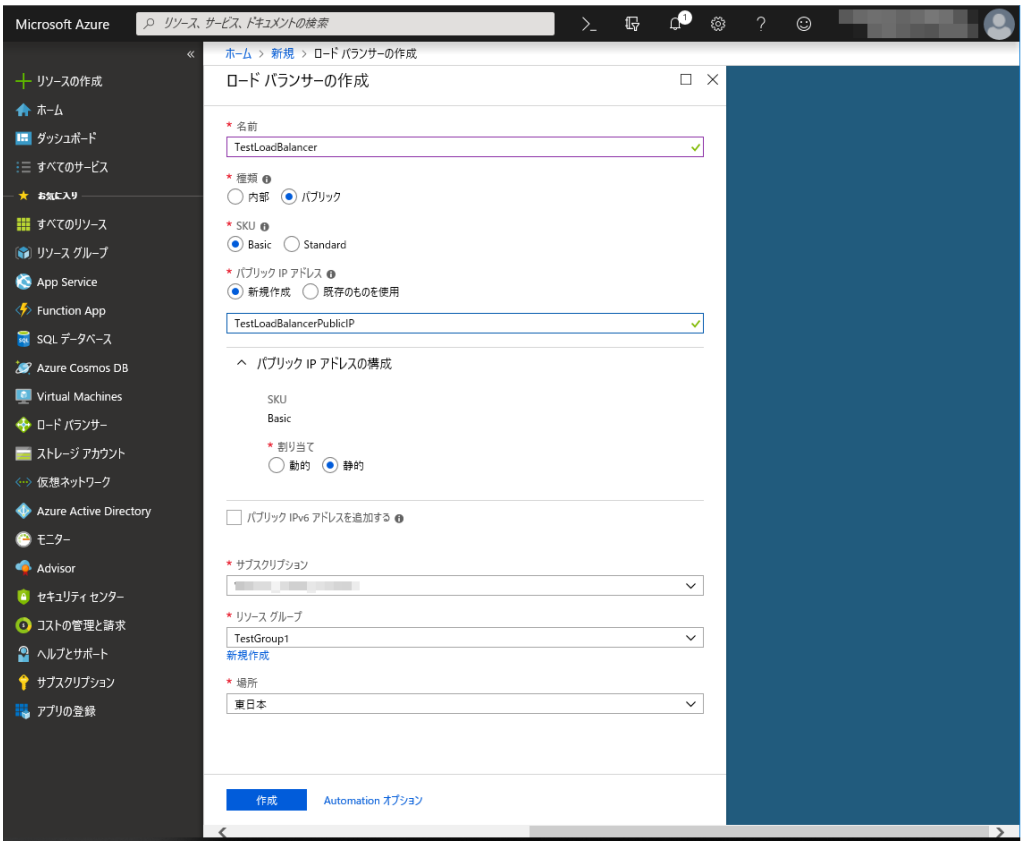


2. [ネットワーキング]>[Load Balancer]を選択します。



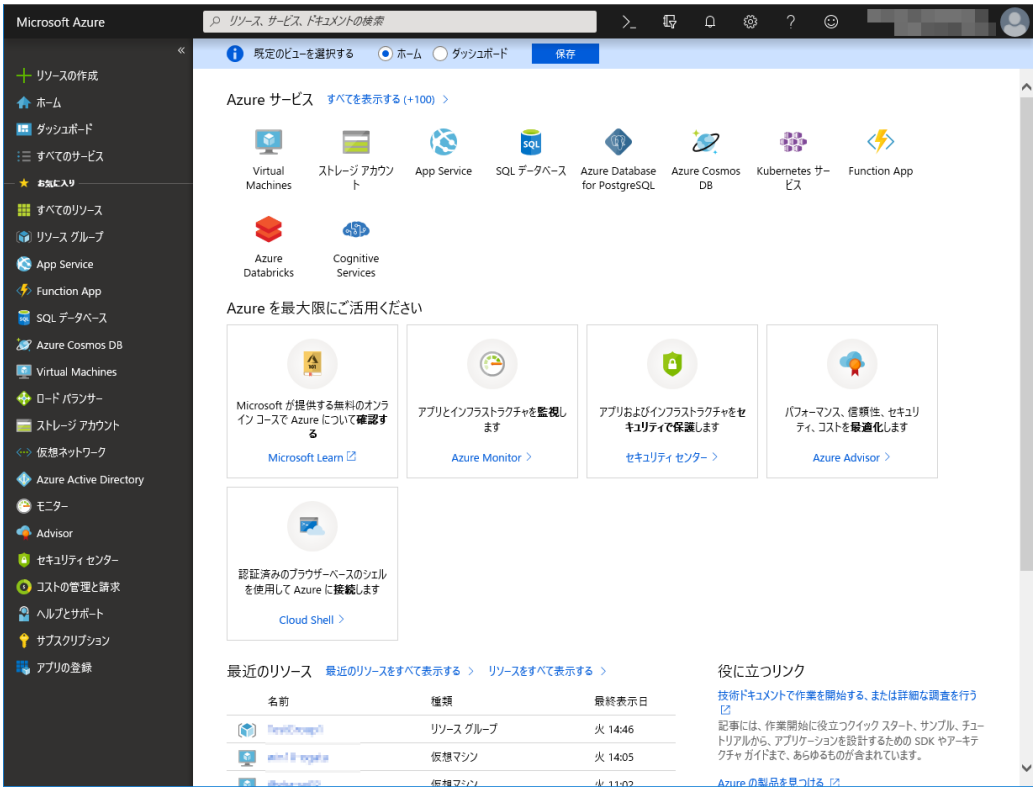
3. [ロードバランサーの作成]が表示されますので、[名前]を設定します。[種類]は[パブリック]、[SKU]は[Basic]を選択します。
4. [パブリック IP アドレス]で[新規作成]、[名前]、[割り当て]を設定します。

5. [サブスクリプション]、[リソースグループ]、[場所]を設定し、[作成]を選択します。ロードバランサーのデプロイが開始されます。デプロイには数分掛かります。

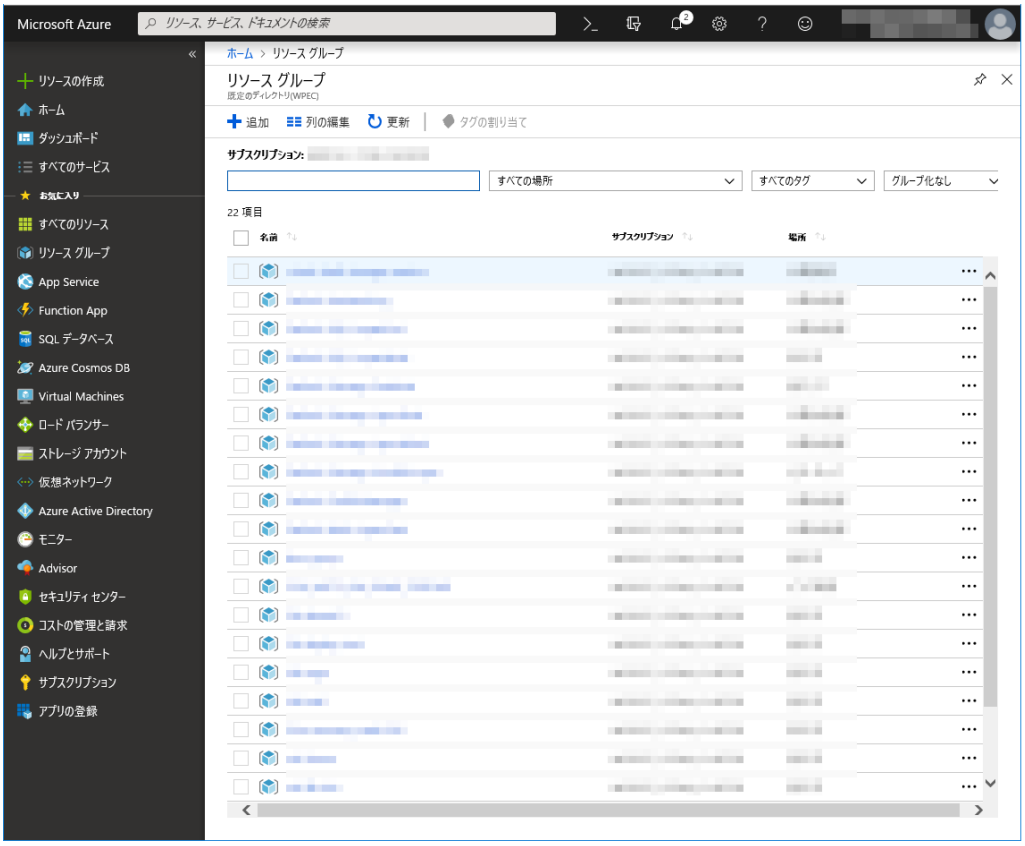


7) ロードバランサーの設定(バックエンドプールの設定)

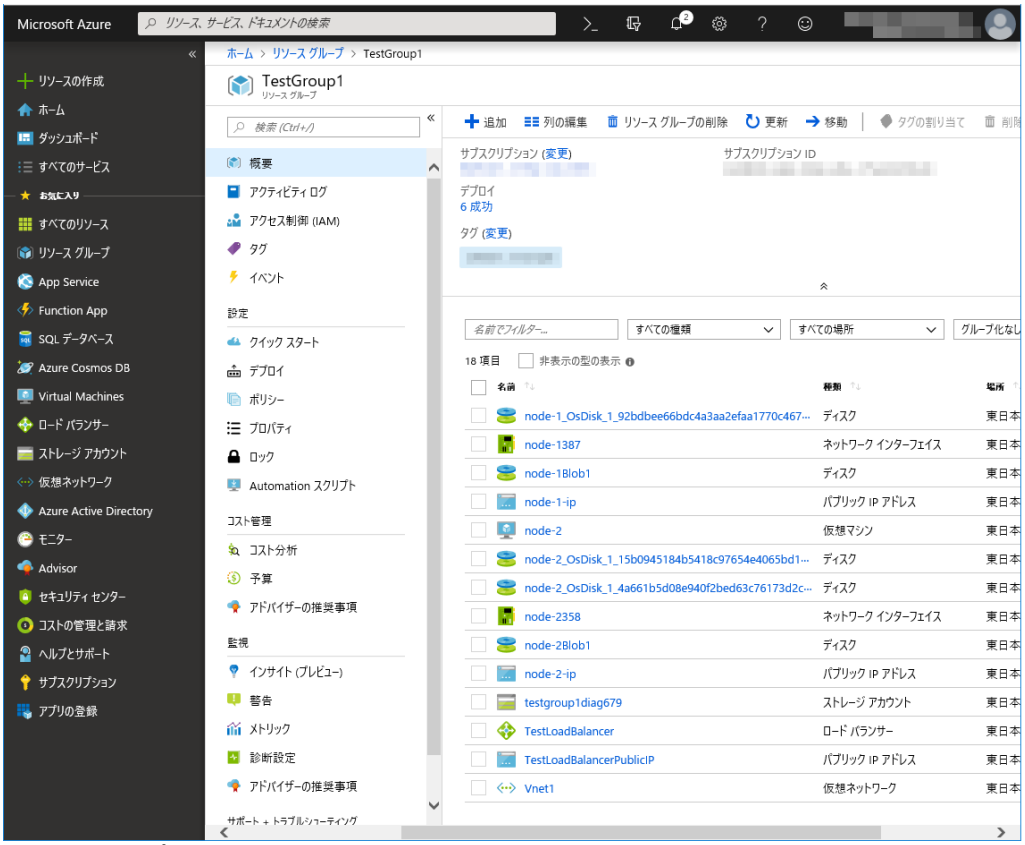
1. 次に可用性セットに登録されている仮想マシンをロードバランサーに紐付けます。ロードバランサーのデプロイが完了したら、画面左側のメニューにある[リソース グループ]もしくはリソース グループアイコンを選択します。



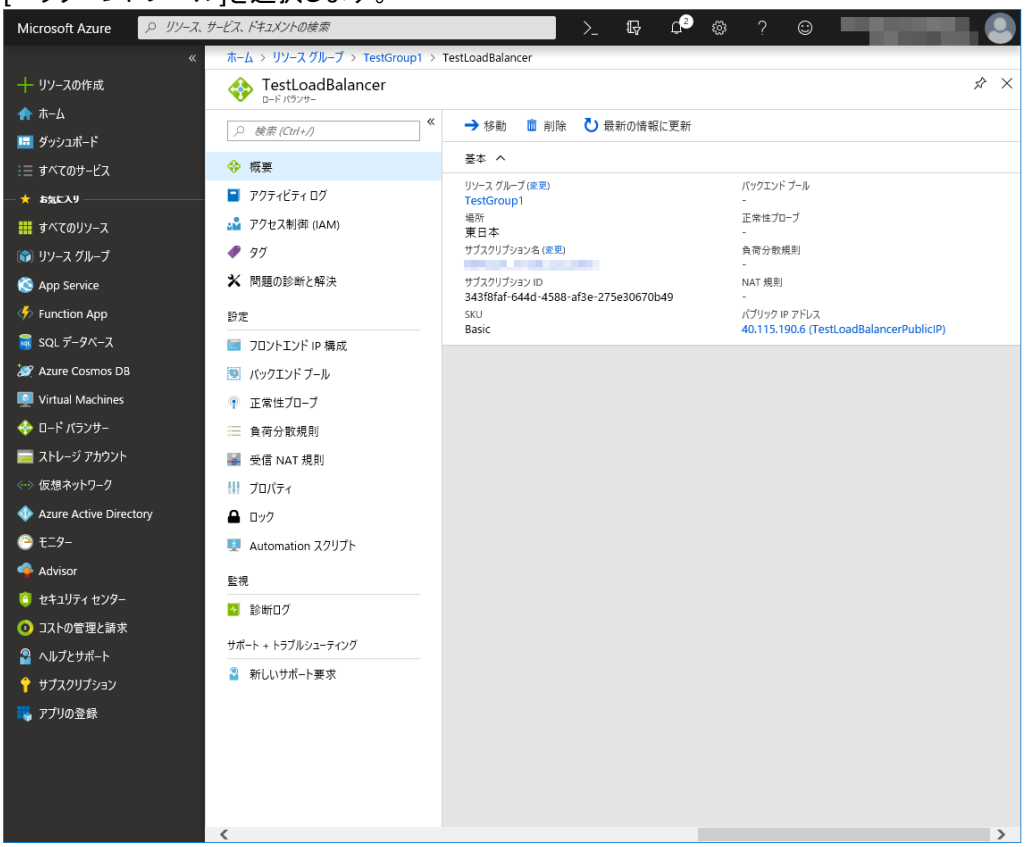
2. リソース グループ一覧から作成したロードバランサーが所属するリソース グループを選択します。



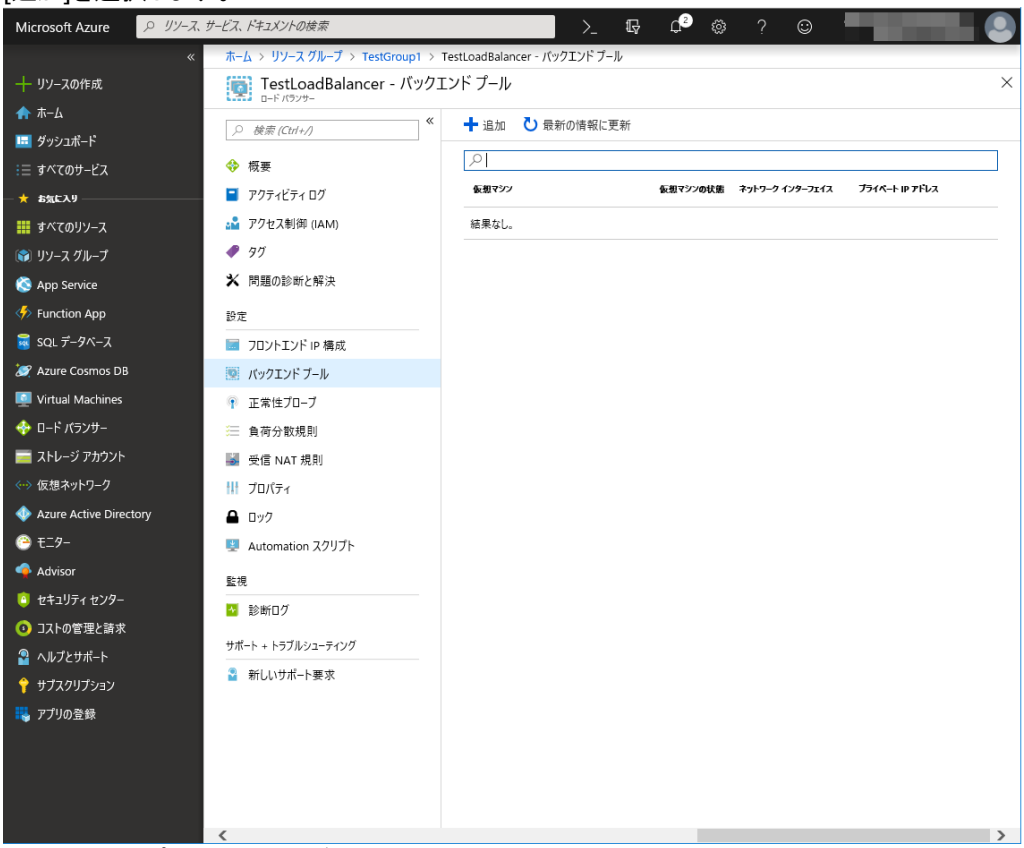
3. リソース グループの概要が表示されます。項目一覧から作成したロードバランサーを選択します。



4. [バックエンドプール]を選択します。

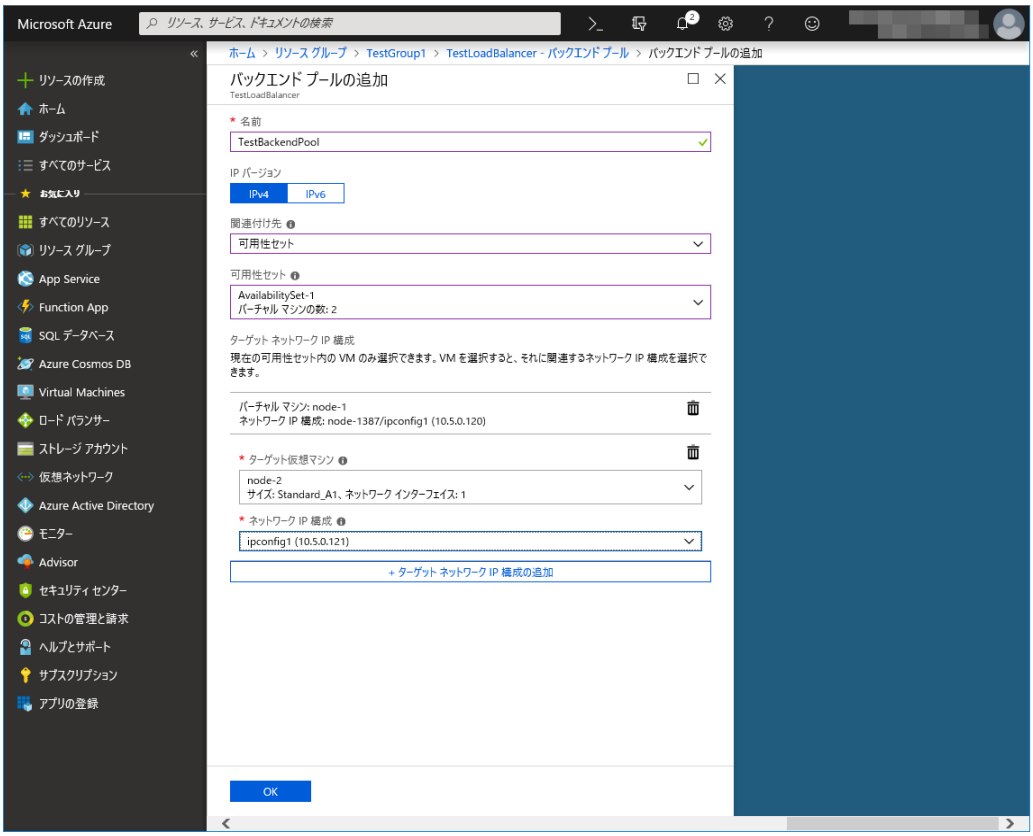


5. [追加]を選択します。



6. [バックエンドプールの追加]ブレードが表示されますので、[名前]を設定します。
7. [関連付け先]は、[可用性セット]を設定します。
8. [可用性セット]を設定します。
9. [+ ターゲットネットワーク IP 構成の追加]を選択します。
10. [ターゲット仮想マシン]、[ネットワーク IP 構成]に対象の仮想マシンを設定します。

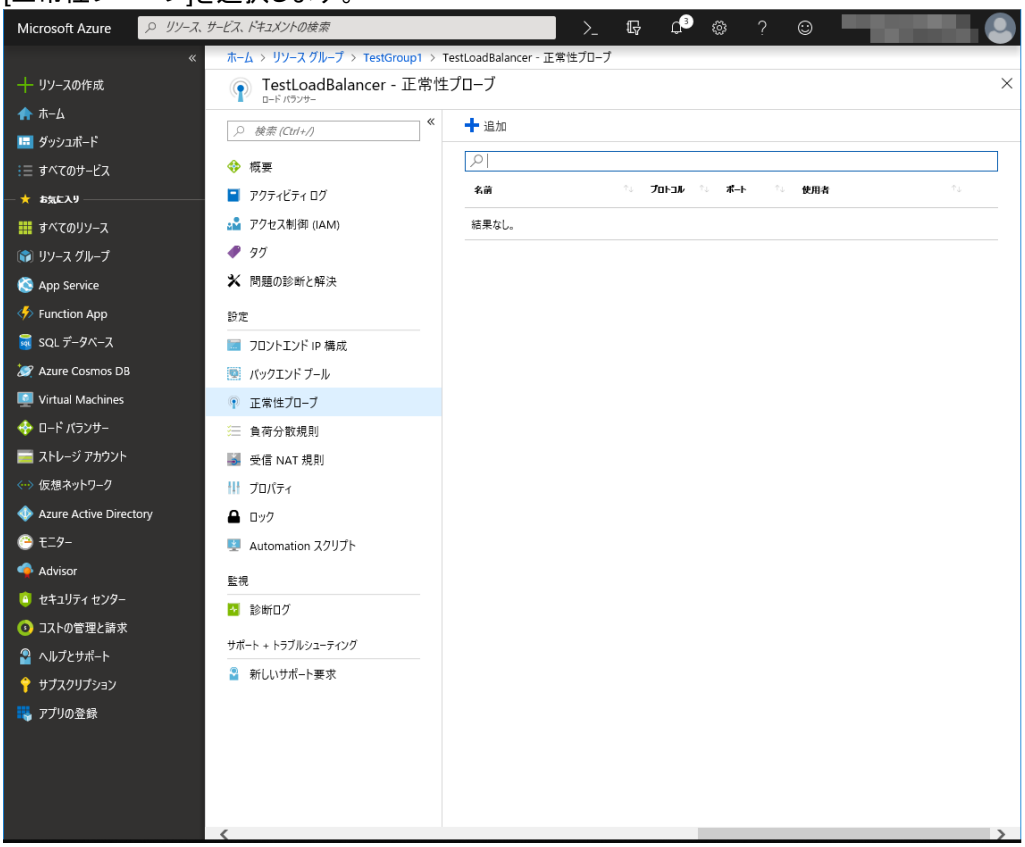
11. 9-10を対象の仮想マシン数分繰り返します。



12. [OK]を選択します。

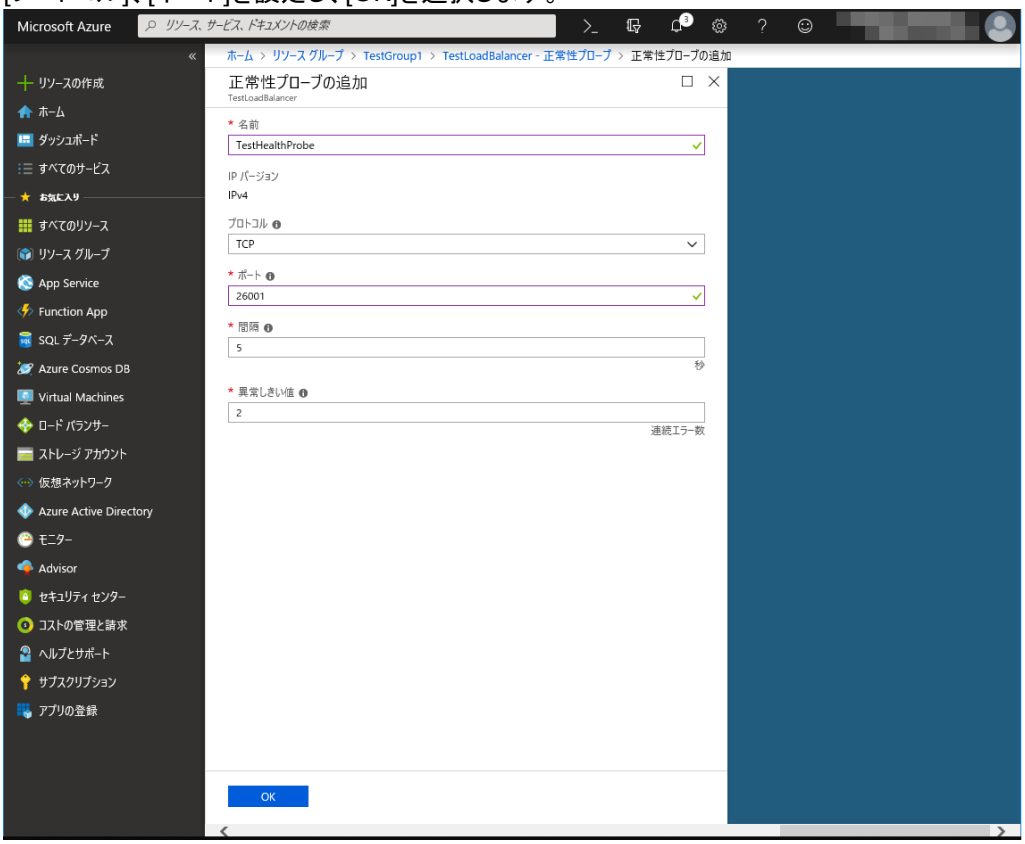
8) ロードバランサーの設定(正常性プローブの設定)

1. [正常性プローブ]を選択します。



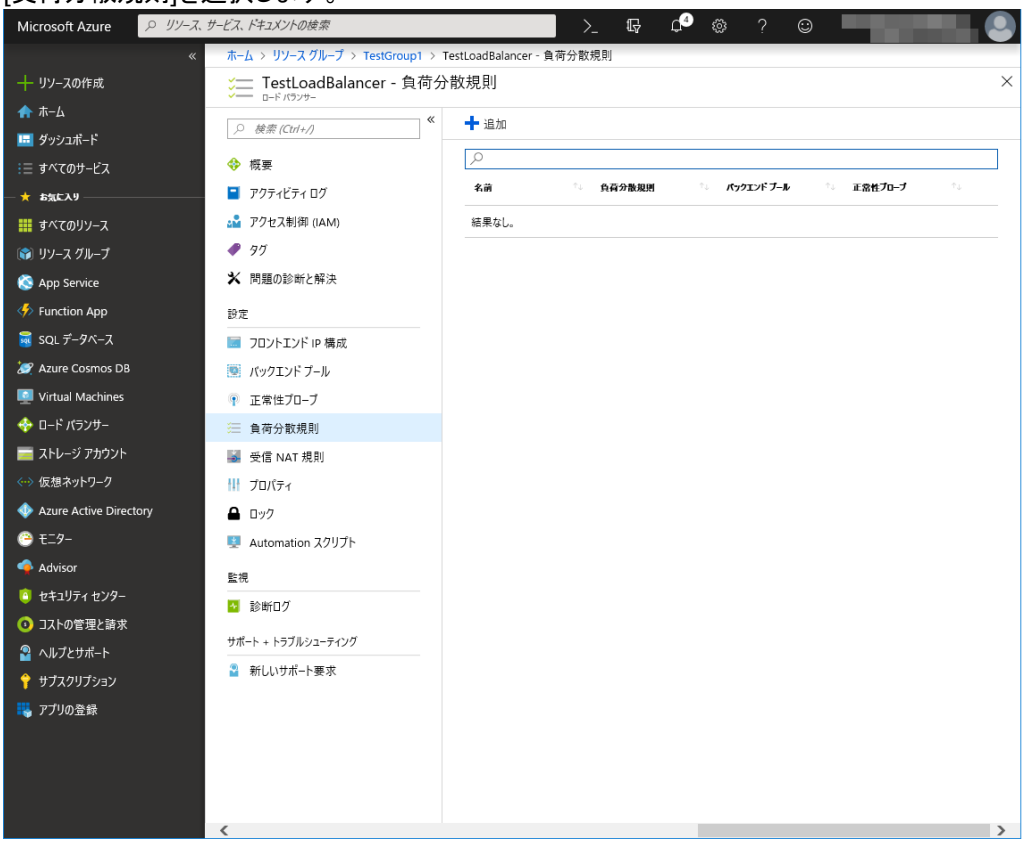
2. [追加]を選択します。
3. [正常性プローブの追加]ブレードが表示されますので、[名前]を設定します。

4. [プロトコル]、[ポート]を設定し、[OK]を選択します。



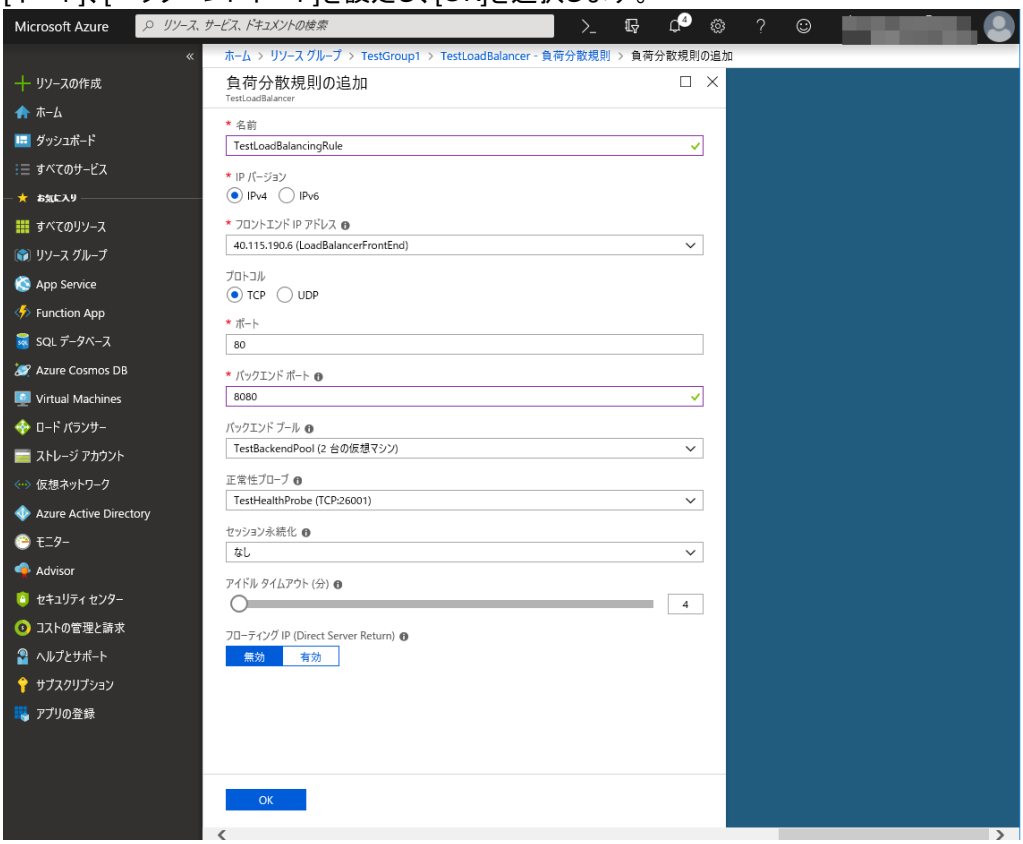
9) ロードバランサーの設定(負荷分散規則の設定)

1. [負荷分散規則]を選択します。



2. [追加]を選択します。
3. [負荷分散規則の追加]が表示されますので、[名前]を設定します。

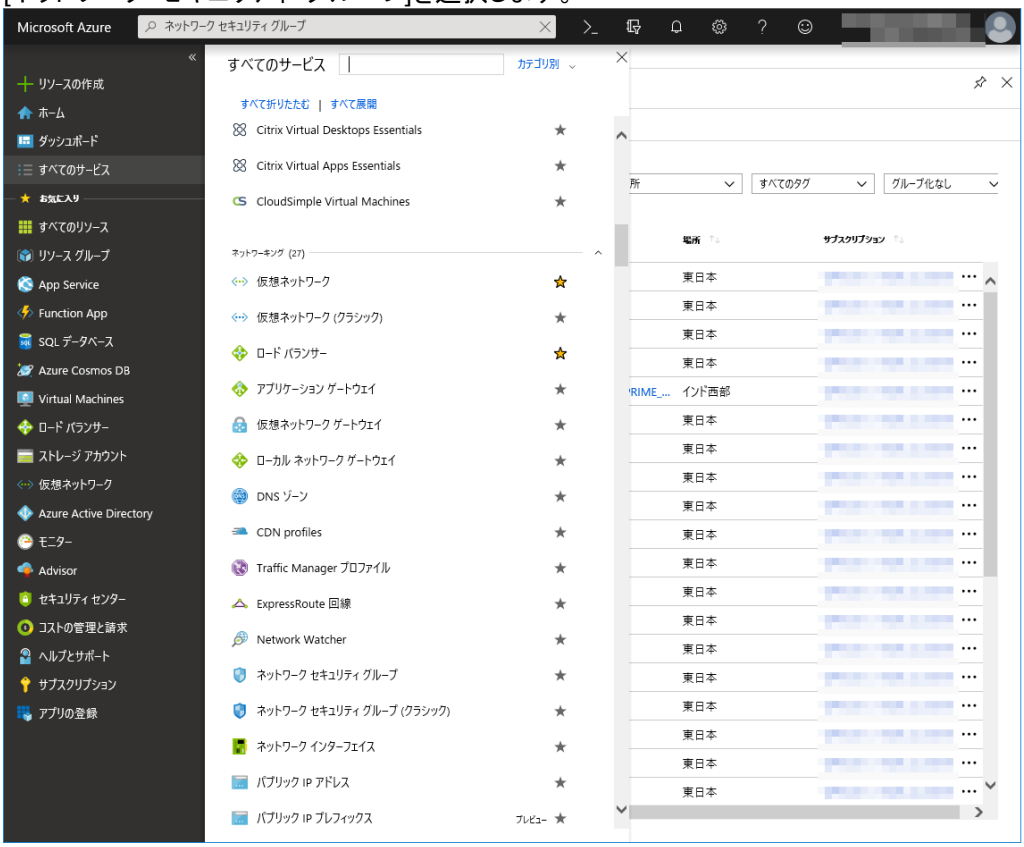
4. [ポート]、[バックエンドポート]を設定し、[OK]を選択します。



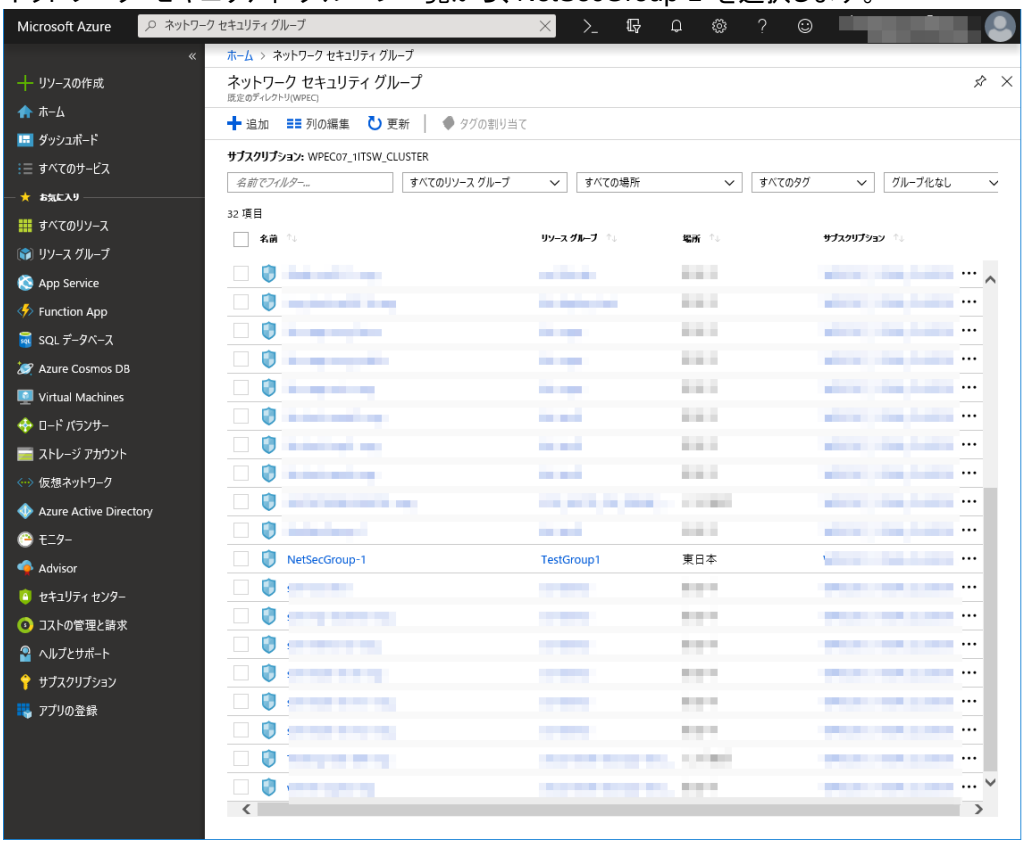
10)　受信セキュリティ規則の設定

Microsoft Azure ポータル(https://portal.azure.com/)にログインし、以下の手順で受信セキュリティ規則の設定を行います。

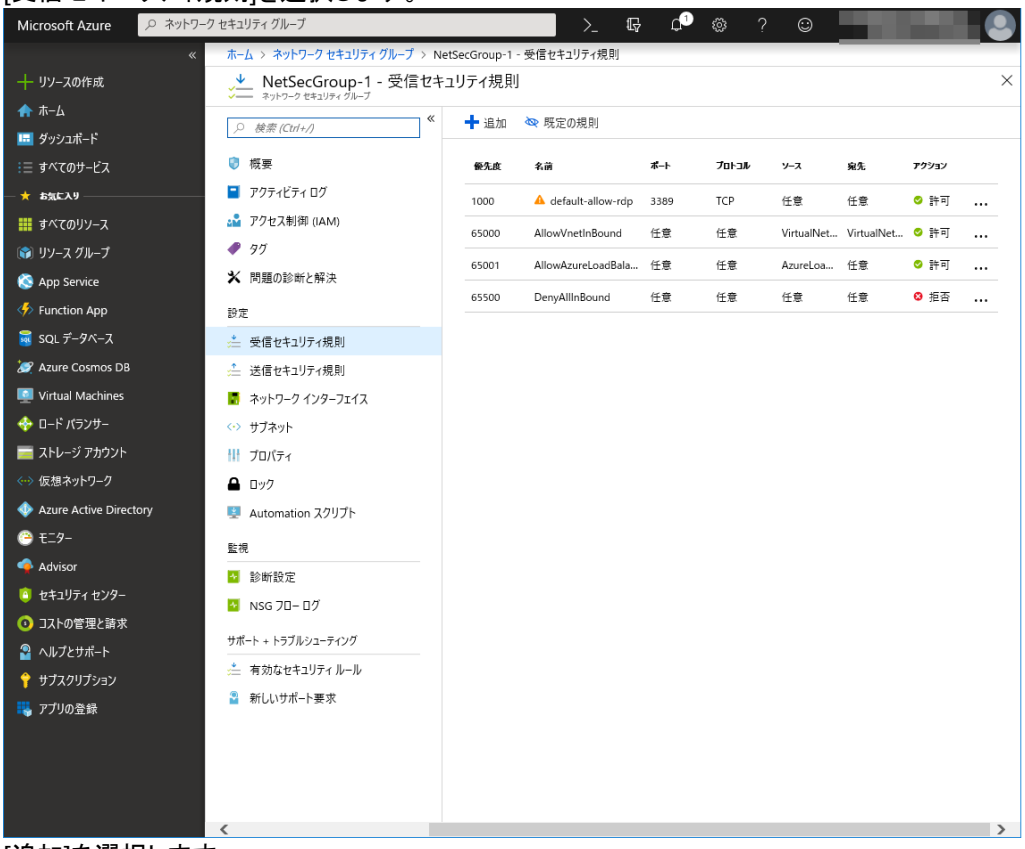
1. 画面左側のメニューにある[すべてのサービス]を選択します。
2. [ネットワーク セキュリティ グループ]を選択します。



3. ネットワーク セキュリティ グループ一覧から、NetSecGroup-1 を選択します。

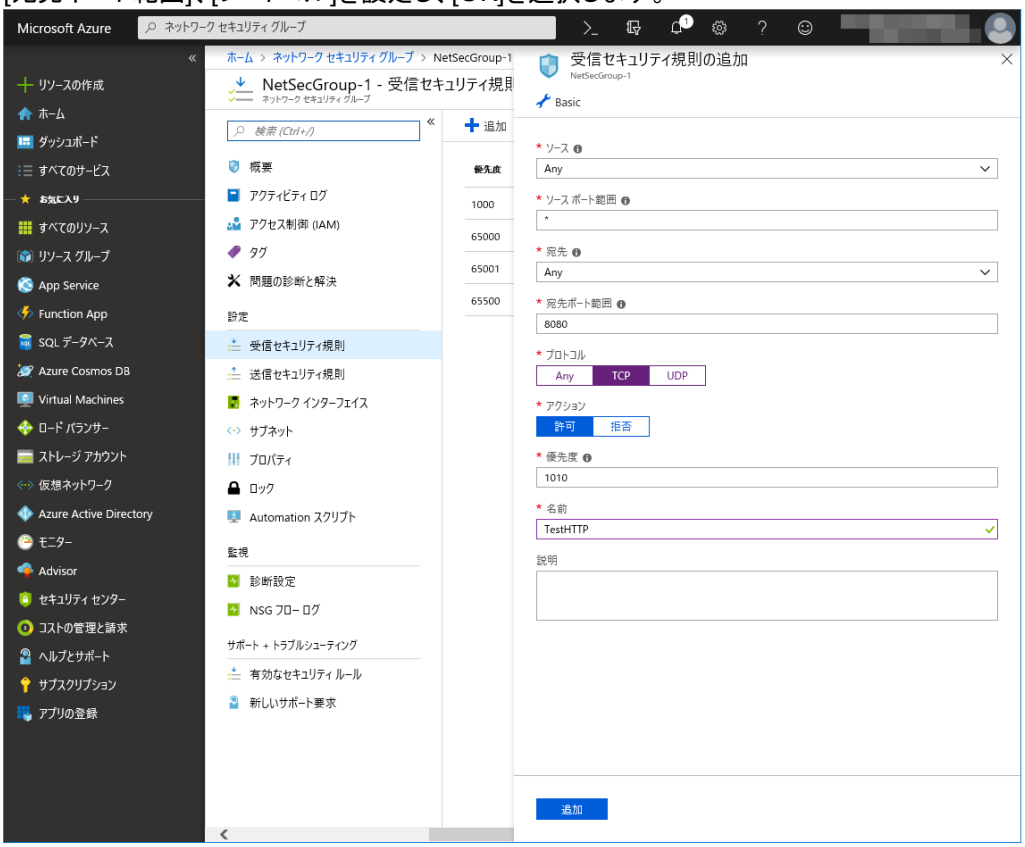


4. NetSecGroup-1 の概要が表示されます。
5. [受信セキュリティ規則]を選択します。



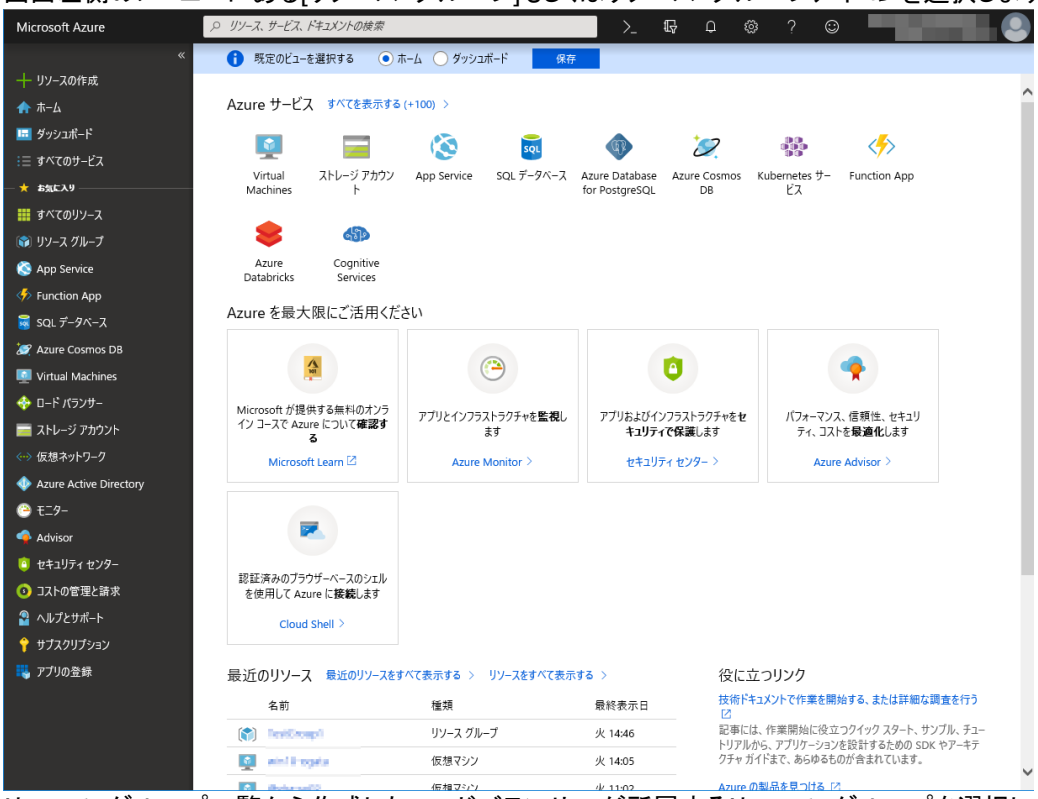
6. [追加]を選択します。

7. [受信セキュリティ規則の追加]が表示されますので、[名前]を設定します。
8. [宛先ポート範囲]、[プロトコル]を設定し、[OK]を選択します。

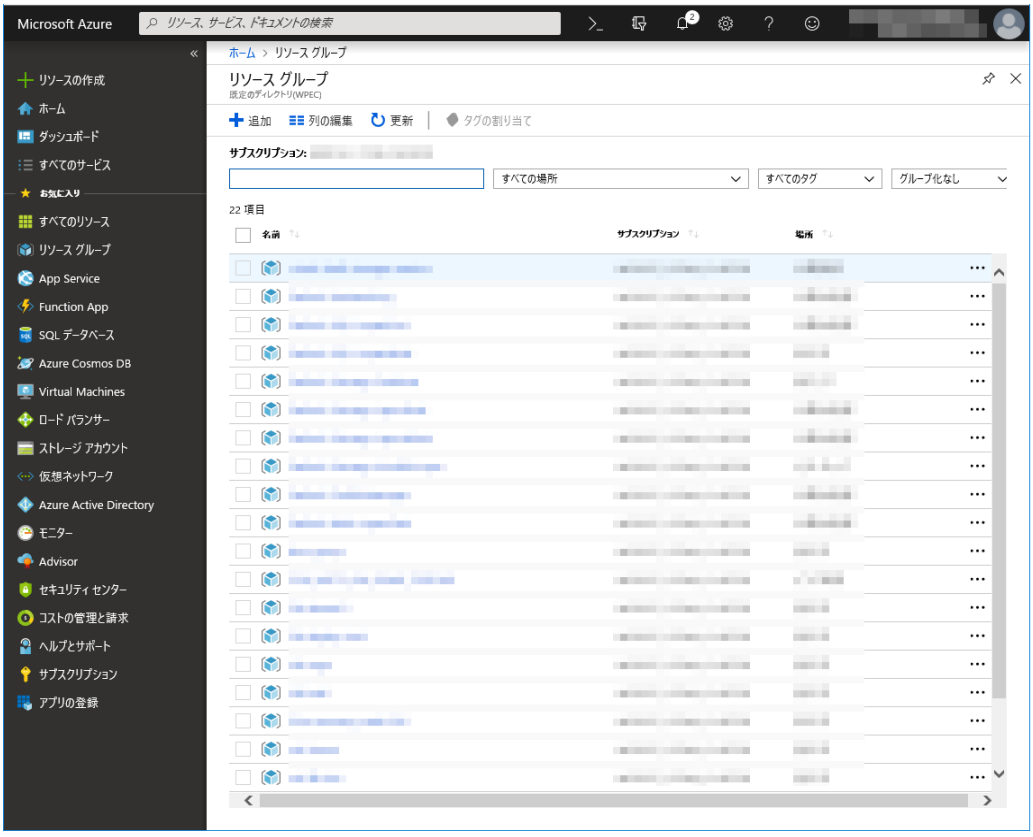


次に「3)**監視リソースの追加**」で設定するマルチターゲット監視リソースの回復動作前スクリプト中に指定する<*ロードバランサーのフロントエンド IP(パブリック IP アドレス)*>を確認します。確認結果はメモしておいてください。

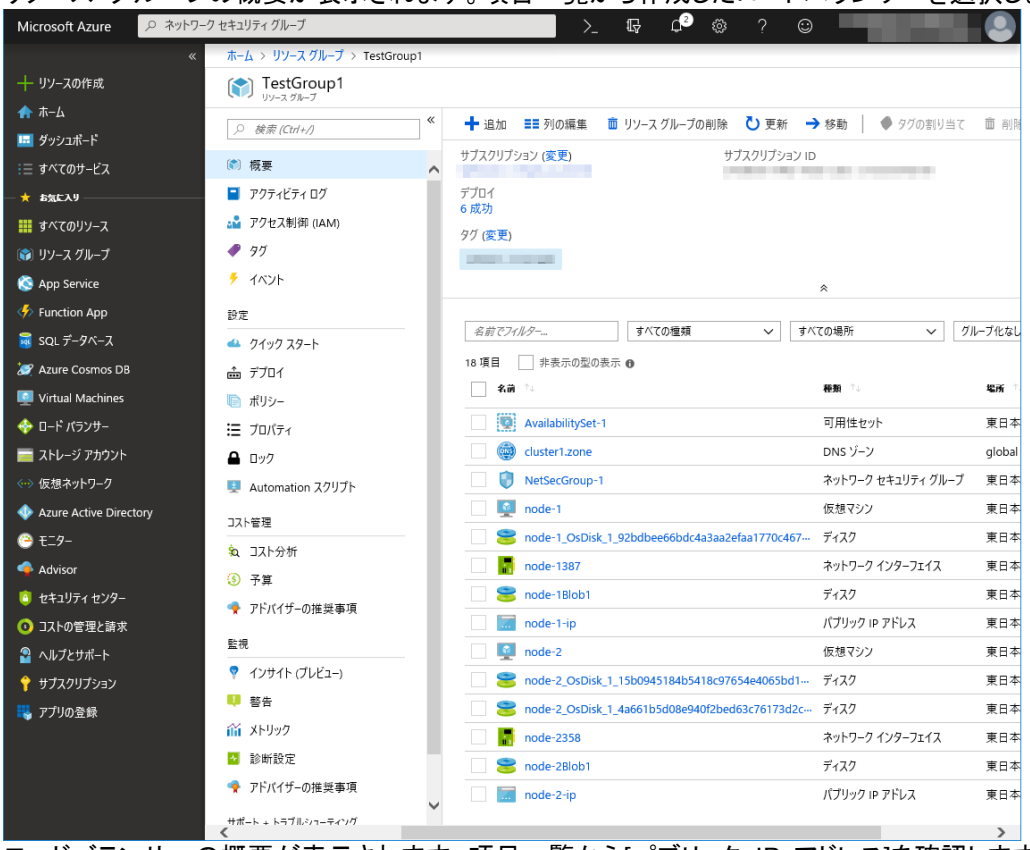
1. 画面左側のメニューにある[リソース グループ]もしくはリソース グループアイコンを選択します。



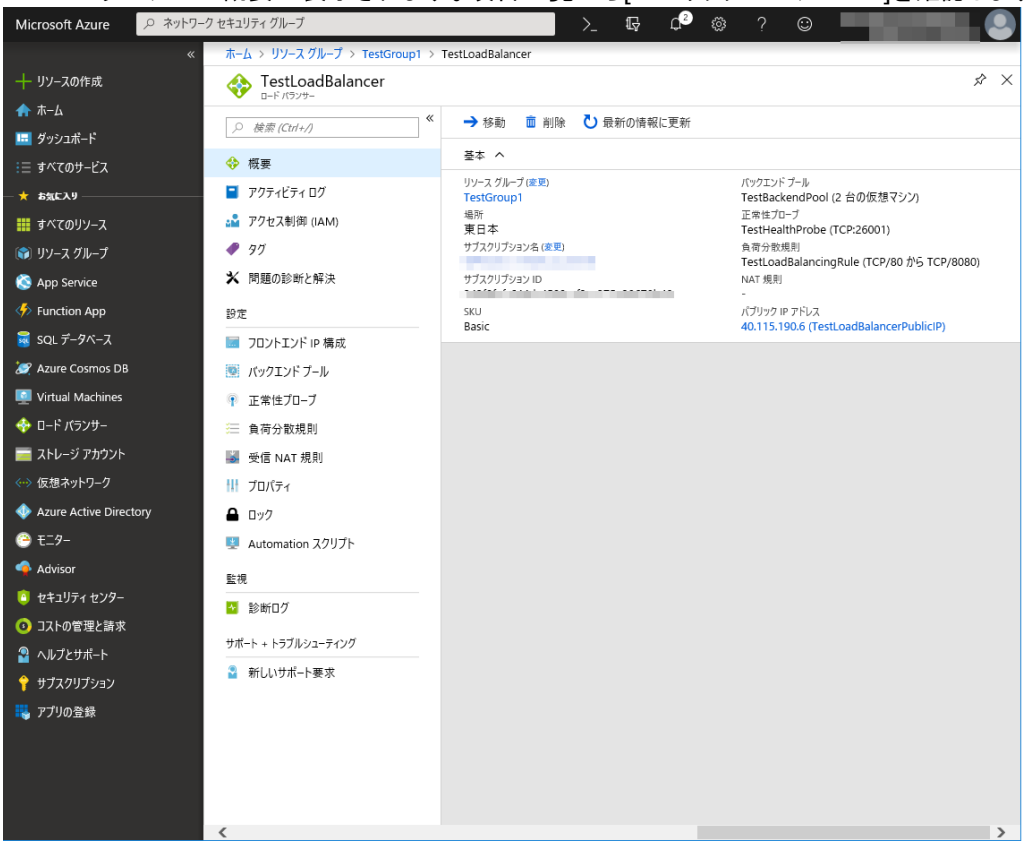
2. リソース グループ一覧から作成したロードバランサーが所属するリソース グループを選択します。



3. リソース グループの概要が表示されます。項目一覧から作成したロードバランサーを選択します。



4. ロードバランサーの概要が表示されます。項目一覧から[パブリック IP アドレス]を確認します。



11) OS 起動時間の調整、ネットワーク設定の確認、ファイアウォールの設定を確認、サーバの時刻を同期、パワーセービング機能をオフ

各手順は『インストール&設定ガイド』-「第 1 章 システム構成を決定する」-「ハードウェア構成後の設定」を参照してください。

12) CLUSTERPRO のインストール

インストール手順は『インストール&設定ガイド』を参照してください。
インストール完了後、OS の再起動を行ってください。

13) CLUSTERPRO のライセンスを登録

ライセンス登録手順は『インストール&設定ガイド』を参照してください。

4.3 CLUSTERPRO の設定

Cluster WebUI のセットアップ、および接続方法は『インストール&設定ガイド』-「第5章 クラスタ構成情報を作成する」を参照してください。

以下のリソース/監視リソースを追加する手順を記述します。

- ミラーディスクリソース
- Azure プローブポートリソース
- Azure プローブポート監視リソース
- Azure ロードバランス監視リソース
- カスタム監視リソース(NP 解決用)
- IP 監視リソース(NP 解決用)
- マルチターゲット監視リソース(NP 解決用)

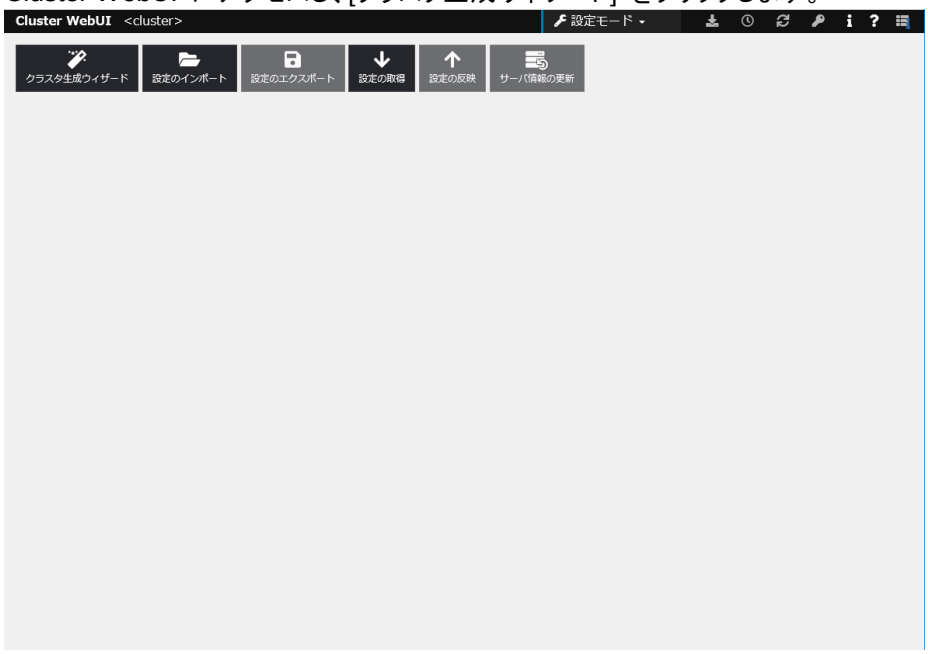
上記以外の設定は、『インストール&設定ガイド』、『リファレンスガイド』を参照してください。

1) クラスタの作成

最初に、クラスタ生成ウィザードを開始し、クラスタを構築します。

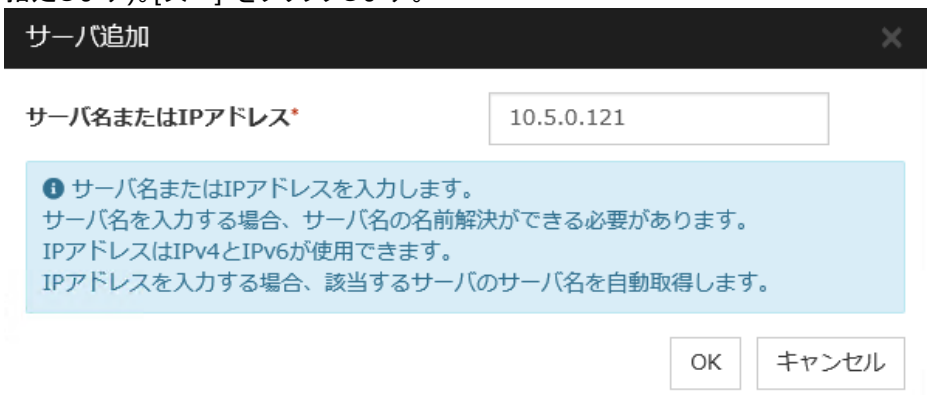
◇ クラスタの構築

1. Cluster WebUI にアクセスし、[クラスタ生成ウィザード] をクリックします。



2. [クラスタ生成ウィザード]画面の[クラスタ]画面が表示されます。
[クラスタ名] に任意のクラスタ名を入力します。
[言語] を適切に選択します。[次へ] をクリックします。

3. [基本設定]画面が表示されます。
Cluster WebUI に接続したインスタンスがマスタサーバとして登録済みの状態で表示されます。
[追加] をクリックし、残りのインスタンスを追加します(インスタンスの Private IP アドレスを指定します)。[次へ] をクリックします。



4. [インタコネクト] 画面が表示されます。
   インタコネクトのために使用する IP アドレス(各インスタンスの Private IP アドレス)を指定します。また、後で作成するミラーディスクリソースの通信経路として [MDC] に mdc1 を選択します。[次へ] をクリックします。

5. [NP 解決] 画面が表示されます。
   ただし、NP 解決は本画面では設定せず、 別途 IP 監視リソース、カスタム監視リソース、マルチターゲット監視リソースを追加することによって同等のことを実現します。NP 解決の設定は、後述の「3) **監視リソースの追加**」で行います。
   クラスタシステムにアクセスするクライアントの配置やオンプレミス環境との接続条件(専用線接続など)によって、NP 解決先や NP 解決の方法は、その都度 検討する必要があります。NP 解決にネットワークパーティション解決リソースを利用することも可能です。
   [次へ] をクリックします。

2) グループリソースの追加

◇ グループの定義
フェイルオーバグループを作成します。

1. [グループ一覧] 画面が表示されます。
[追加]をクリックします。

2. [グループの定義] 画面が表示されます。
[名前] にフェイルオーバグループ名(failover1)を設定します。[次へ] をクリックします。

3. [起動可能サーバ] 画面が表示されます。
何も指定せず [次へ] をクリックします。
4. [グループ属性] 画面が表示されます。
何も指定せず [次へ] をクリックします。
5. [グループリソース一覧] 画面が表示されます。
以降の手順で、この画面でグループリソースを追加していきます。

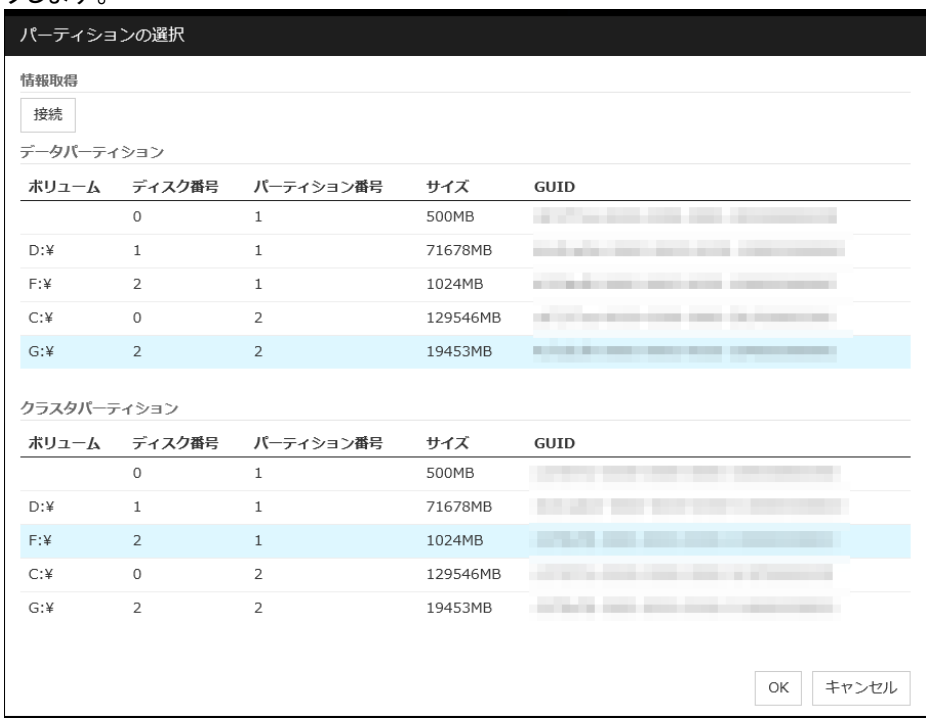
◇ ミラーディスクリソース
ミラーディスクリソースを作成します。
詳細は『リファレンスガイド』-「ミラーディスクリソースを理解する」を参照してください。

1. [グループリソース一覧] で [追加] をクリックします。

2. [グループのリソース定義 | failover1] 画面が開きます。
   [タイプ] ボックスでグループリソースのタイプ(ミラーディスクリソース) を選択し、[名前] ボックスにグループ名 (md) を入力します。[次へ] をクリックします。

3. [依存関係] 画面が表示されます。
   何も指定せず [次へ] をクリックします。
4. [復旧動作] 画面が表示されます。[次へ] をクリックします。
5. [詳細] 画面が表示されます。
   [起動可能サーバ]で[名前]列中のサーバ名を選択し[追加]をクリックします。

6. [パーティションの選択]ダイアログボックスが表示されます。[接続]をクリックし、「5) **仮想マシンの設定**」で作成したデータパーティションと、クラスタパーティションを選択し、[OK]をクリックします。



7. node-1について5と6を設定、次に node-2について5と6を設定し、[完了]をクリックします。

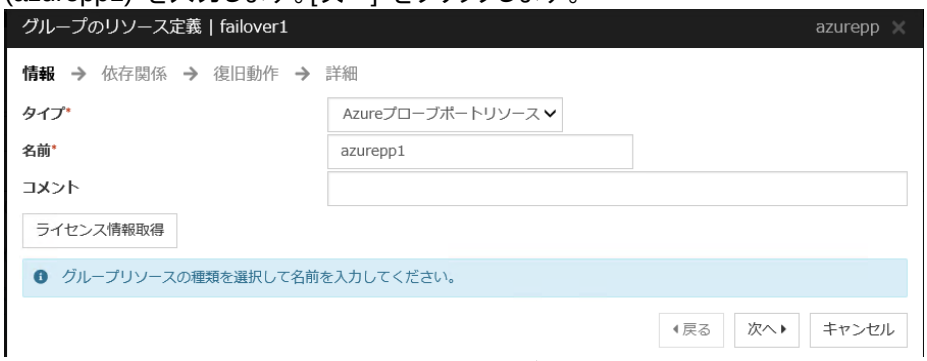
◇ Azure プローブポートリソース

Microsoft Azure 上で CLUSTERPRO を利用する場合、業務が稼働するノードの特定のポートでロードバランサーからの死活監視を待ち受ける仕組みを提供します。

Azure プローブポートリソースの詳細は『リファレンスガイド』-「Azure プローブポートリソースを理解する」を参照してください。

1. [グループリソース一覧] で [追加] をクリックします。

2. [グループのリソース定義 | failover1] 画面が開きます。[タイプ] ボックスでグループリソースのタイプ (Azure プローブポートリソース) を選択して、[名前] ボックスにグループ名 (azurepp1) を入力します。[次へ] をクリックします。



3. [依存関係] 画面が表示されます。何も指定せず [次へ] をクリックします。
4. [復旧動作] 画面が表示されます。[次へ] をクリックします。
5. [プローブポート] にロードバランサーの設定(正常性プローブの設定)時に [ポート] として指定した値を入力します。

6. [完了] をクリックします。

3) 監視リソースの追加

◇ Azure プローブポート監視リソース
Microsoft Azure プローブポートリソースが起動しているノードに対して、死活監視のためのポートの監視機構を提供します。

Azure プローブポート監視リソースの詳細は『リファレンスガイド』-「Azure プローブポート監視リソースを理解する」を参照してください。

Azure プローブポートリソースを1つ追加すると、Azure プローブポート監視リソースが1つ自動的に作成されます。

◇ Azure ロードバランス監視リソース
Microsoft Azure プローブポートリソースが起動していないノードに対して、プローブポートと同じポート番号が開放されていないかの監視機構を提供します。

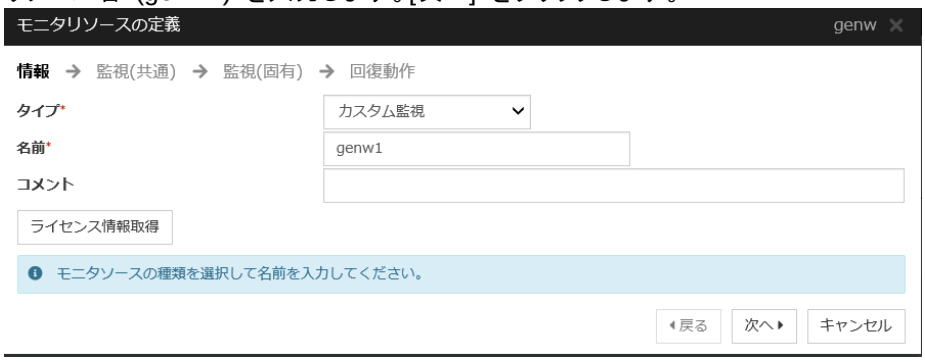
Azure ロードバランス監視リソースの詳細は『リファレンスガイド』-「Azure ロードバランス監視リソースを理解する」を参照してください。

Azure プローブポートリソースを1つ追加すると、Azure ロードバランス監視リソースが1つ自動的に作成されます。

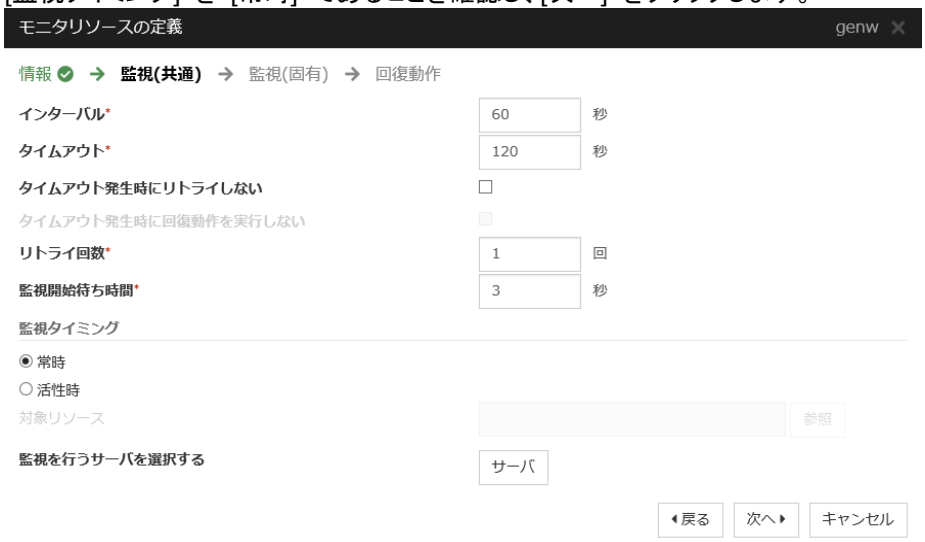
◇ カスタム監視リソース
Microsoft Azure の Service Management API へ疎通可能かどうかを監視し、外部ネットワークとの通信の健全性を監視するためのスクリプトを設定します。

カスタム監視リソースの詳細は『リファレンスガイド』-「カスタム監視リソースを理解する」を参照してください。

1. [モニタリソース一覧] で [追加] をクリックします。
2. [タイプ] ボックスでモニタリソースのタイプ (カスタム監視) を選択し、[名前] ボックスに監視リソース名 (genw1) を入力します。[次へ] をクリックします。



3. [監視(共通)] 画面が表示されます。
[監視タイミング] を [常時] であることを確認し、[次へ] をクリックします。



4. [監視(固有)] 画面が表示されます。
[この製品で作成したスクリプト] をチェックします。
作成するスクリプトのサンプルは以下のとおりです。

<*CLUSTERPRO インストールパス*>¥bin¥clpazure_port_checker -h management.core.windows.net -p 443
EXIT %ERRORLEVEL%

[監視タイプ] を [同期] にチェックします。[次へ] をクリックします。

5. [回復動作] 画面が表示されます。
[回復動作] に [最終動作のみ実行]、[回復対象] に [LocalServer]、[最終動作] に [何もしない]を設定します。

6. [完了] をクリックして設定を終了します。

◇ IP 監視リソース
仮想マシンで構成されたクラスタ間の通信を監視し、内部ネットワークとの通信の健全性を監視する IP 監視リソースを作成します。

IP 監視リソースの詳細は『リファレンスガイド』-「IP 監視リソースを理解する」を参照してください。

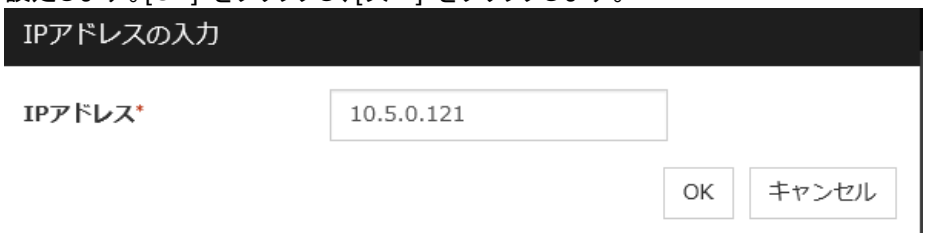
1. [モニタリソース一覧] で [追加] をクリックします。
2. [タイプ] ボックスでモニタリソースのタイプ (IP 監視) を選択し、[名前] ボックスに監視リソース名 (ipw1) を入力します。[次へ] をクリックします。

3. [監視(共通)] 画面が表示されます。
[監視タイミング] が [常時] であることを確認します。

[監視を行うサーバを選択する] で起動可能なサーバをひとつ選択し追加します。[OK] をクリックし、[次へ] をクリックします。

4. [監視(固有)] 画面が表示されます。

[IP アドレス一覧] で [追加] を選択し、3 で選択したサーバとは別のサーバの IP アドレスを設定します。[OK] をクリックし、[次へ] をクリックします。



5. [回復動作] 画面が表示されます。
   [回復動作] に [最終動作のみ実行]、[回復対象] に [LocalServer]、[最終動作] に [何もしない] を設定します。

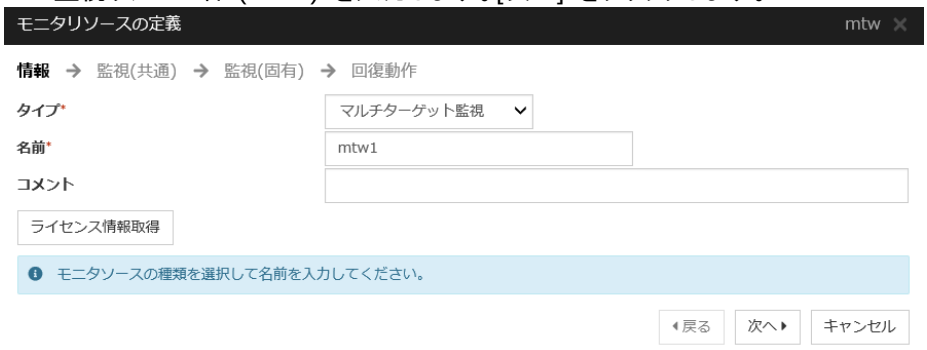
6. [完了] をクリックして設定を終了します。
7. 次にもう一方のサーバでも、同様の監視リソースを作成します。[モニタリソース一覧] で [追加] をクリックします。
8. [タイプ] ボックスでモニタリソースのタイプ (IP 監視) を選択し、[名前] ボックスに監視リソース名 (ipw2) を入力します。[次へ] をクリックします。
9. [監視(共通)] 画面が表示されます。
   [監視タイミング] が [常時] であることを確認します。
   [監視を行うサーバを選択する] で起動可能なサーバをひとつ選択し追加します。
   [OK] をクリックし、[次へ] をクリックします。
10. [監視(固有)] 画面が表示されます。
    [共通] タブの [IP アドレス一覧] で [追加] を選択し、9 で選択したサーバとは別のサーバの IP アドレスを設定します。[OK] をクリックし、[次へ] をクリックします。
11. [回復動作] 画面が表示されます。
    [回復動作] に [最終動作のみ実行]、[回復対象] に [LocalServer]、[最終動作] に [何もしない] を設定します。
12. [完了] をクリックして設定を終了します。

◇ マルチターゲット監視リソース

Microsoft Azure の Service Management API への通信を監視するカスタム監視リソースと、仮想マシンで構成されたクラスタ間の IP 監視リソースの両方の状態を確認するマルチターゲット監視リソースを作成します。両方の監視リソースの状態が異常となった際に、NP 解決用の処理を記載したスクリプトを実行します。

マルチターゲット監視リソースの詳細は『リファレンスガイド』-「マルチターゲット監視リソースを理解する」を参照してください。

1. [モニタリソース一覧] で [追加] をクリックします。
2. [タイプ] ボックスでモニタリソースのタイプ (マルチターゲット監視) を選択し、[名前] ボックスに監視リソース名 (mtw1) を入力します。[次へ] をクリックします。



3. [監視(共通)] 画面が表示されます。
[監視タイミング] が [常時] であることを確認し、[次へ] をクリックします。

4. [監視(固有)] 画面が表示されます。
利用可能なモニタリソース一覧から [追加] を選択し、Service Management API への疎通確認用カスタム監視リソース、両サーバに設定したそれぞれの IP 監視リソースの3つの監視リソースを追加します(genw1、ipw1、ipw2)。[次へ] をクリックします。

5. [回復動作] 画面が表示されます。
[回復動作] に [最終動作のみ実行]、[最終動作前にスクリプトを実行する]をチェック、[回復対象] に [LocalServer]、[最終動作] に [何もしない] を設定します。
[スクリプト設定] をクリックし、マルチターゲット監視リソースが異常検出時に実行するスクリプトを作成します。

6. スクリプトの編集ダイアログが表示されます。
[この製品で作成したスクリプト] をチェックし、スクリプトを [編集] します。作成するスクリプトのサンプルは以下のとおりです。
以下は「4.1 構築例について」を参照して設定してください。ポートは業務により異なります。
・ロードバランサーの負荷分散規則 - バックエンドポート
・ロードバランサーの負荷分散規則 - ポート
以下は「10) **受信セキュリティ規則の設定**」でメモしたパブリック IP アドレスを設定してください。
・ロードバランサーのフロントエンド IP(パブリック IP アドレス)

```
-----
rem ********************
rem Check Active Node
rem ********************
<CLUSTERPRO インストールパス>¥bin¥clpazure_port_checker -h 127.0.0.1 -p <ロードバランサーの負荷分散規則 - バックエンドポート>
IF NOT "%ERRORLEVEL%" == "0" (
    GOTO CLUSTER_SHUTDOWN
)

rem ********************
rem Check DNS
rem ********************
<CLUSTERPRO インストールパス>¥bin¥clpazure_port_checker -h <ロードバランサーのフロントエンド IP(パブリック IP アドレス)> -p <ロードバランサーの負荷分散規則 - ポート>
IF "%ERRORLEVEL%" == "0" (
    GOTO EXIT
)

rem ********************
rem Cluster Shutdown
rem ********************
:CLUSTER_SHUTDOWN
clpdown

rem ********************
rem EXIT
rem ********************
:EXIT
EXIT 0
-----
```

[タイムアウト] は clpazure_port_checker のタイムアウト値(5秒固定)より長く設定します。
上記のサンプルスクリプトでは clpazure_port_checker を2回実行するため、10秒より大きな値を推奨します。
[OK] をクリックします。

7. [完了] をクリックして設定を終了します。

4) クラスタプロパティの設定

クラスタプロパティの詳細は『リファレンスガイド』-「クラスタプロパティ」を参照してください。

◇ クラスタプロパティ

Microsoft Azure と CLUSTERPRO の連携用に、クラスタプロパティ内の設定を以下のように設定します。

1. Cluster WebUI から設定モードへ移動し、クラスタ名のプロパティアイコンをクリックします。

2. [タイムアウト] タブを選択します。ハートビートの[タイムアウト]に以下の「A + B + C」の結果を設定します。

   A :NP 解決用のマルチターゲット監視リソースで監視している監視リソースの[インターバル] × ([リトライ回数] + 1)

   ※3つある監視リソースのうち上記計算式の結果が大きい方を選択してください。

   B :マルチターゲット監視リソースの [インターバル] × ([リトライ回数] + 1)

   C :30秒(マルチターゲット監視リソースでの異常検出前にハートビートがタイムアウトしないようにするための猶予時間。適宜変更可能)

注:ハートビートのタイムアウト値が、NP 解決用のモニタで異常を検出する時間より短い場合、NP 解決処理が動作する前にハートビートのタイムアウトを検出します。この場合、待機サーバでサービスが起動され、クラスタ内でサービスの二重起動が発生する可能性があります。

3. [OK] をクリックします。

5) 設定の反映とクラスタの起動

1. Cluster WebUI の設定モード から、[設定の反映] をクリックします。
   [設定を反映しますか。] というポップアップメッセージが表示されますので、[OK] をクリックします。
   アップロードに成功すると、[反映に成功しました。] のメッセージが表示されますので、[OK] をクリックします。
   アップロードに失敗した場合は、表示されるメッセージに従って操作を行ってください。
2. Cluster WebUI の ツールバーのドロップダウンメニューで [操作モード] を選択して、操作モードに切り替えます。
3. Cluster WebUI の[ステータス] タブから [クラスタ開始] をクリックし、確認画面で [開始] をクリックします。

詳細は『インストール&設定ガイド』-「クラスタを生成するには」を参照してください。

4.4 動作確認

構築した環境が正常に動作するかを、監視異常(擬似)を発生させフェイルオーバグループがフェイルオーバすることにより確認します。
既にクラスタが正常に起動している状態からの確認手順は以下のとおりです。

1. フェイルオーバグループ(failover1)が、現用系ノードの node-1で起動します。Cluster WebUI [ステータス]タブにおいて failover1が node-1で[起動済]になっていることを確認します。
2. Cluster WebUI のプルダウンより[操作モード]から[検証モード]に変更します。
3. Cluster WebUI [ステータス]タブにおいて azureppw1の [擬似障害発生]アイコンを選択します。
4. Azure プローブポートリソース(azurepp1)が3回再活性後に、フェイルオーバグループ(failover1)が異常になり、ノード node-2へフェイルオーバします。Cluster WebUI [ステータス]タブにおいて failover1が node-2で[起動済]になっていることを確認します。
   また、Azure ロードバランサーのフロントエンド IP、ポートに対してフェイルオーバ後も正常にアクセスできることを確認します。

以上で、擬似障害の場合におけるフェイルオーバの動作確認は完了です。その他の障害発生時の動作確認については適宜実施してください。

第 5 章　構築手順(内部ロードバランサーを使用した HA クラスタの場合)

5.1 構築例について

本書では、Microsoft Azure において、CLUSTERPRO を使用した2ノードでの片方向スタンバイクラスタの構築手順を紹介します。本手順は、node-1 を現用系サーバとしたミラーディスク型の構成を対象としています。
以下の表は既定値が存在しないパラメータ、および既定値から変更したパラメータについて記載しています。

- Microsoft Azureの設定(node-1、node-2で共通の設定)

設定項目	設定値
リソース グループの設定	
名前	TestGroup1
リソース グループの場所	東日本
仮想ネットワークの設定	
名前	Vnet1
アドレス空間	10.5.0.0/24
サブネット名	Vnet1-1
サブネットアドレス範囲	10.5.0.0/24
リソース グループ名	TestGroup1
場所	東日本
ロードバランサーの設定	
名前	TestLoadBalancer
種類	内部
仮想ネットワーク	Vnet1
サブネット	Vnet1-1
IPアドレスの割り当て	静的
プライベートIPアドレス	10.5.0.200
Resource group	TestGroup1
場所	東日本
バックエンドプール - 名前	TestBackendPool
関連付け先	可用性セット
ターゲット仮想マシン	node-1 node-2
ネットワークIP 構成	10.5.0.120 10.5.0.121
正常性プローブ - 名前	TestHealthProbe
正常性プローブ - ポート	26001
負荷分散規則 - 名前	TestLoadBalancingRule
負荷分散規則 - ポート	80(業務を提供しているポート番号)
負荷分散規則 - バックエンドポート	8080(業務を提供しているポート番号)

- Microsoft Azureの設定(node-1、node-2でそれぞれ設定)

設定項目	設定値	
	node-1	node-2
仮想マシンの設定		
ディスクの種類	Standard HDD	
ユーザー名	testlogin	

パスワード	PassWord_123	
リソース グループ名	TestGroup1	
場所	東日本	
ネットワーク セキュリティ グループの設定		
名前	NetSecGroup-1	
可用性セットの設定		
名前	AvailabilitySet-1	
更新ドメイン	5	
障害ドメイン	2	
診断ストレージアカウントの設定		
名前	自動生成(testgroup1diag679)	
パフォーマンス	Standard	
レプリケーション	ローカル冗長ストレージ(LRS)	
IP構成の設定		
IPアドレス	10.5.0.120	10.5.0.121
Blobの設定		
名前	node-1Blob1	node-2Blob1
ソースの種類	なし(空のディスク)	
アカウントの種類	Standard HDD	
サイズ	20	

- CLUSTERPROの設定(クラスタプロパティ)

設定項目	設定値	
	node-1	node-2
クラスタ名	Cluster1	
サーバ名	node-1	node-2
NP解決タブ - 種別	Ping	
NP解決タブ - Pingターゲット	10.5.0.5	
NP解決タブ - [サーバ] 列	使用する	使用する

- CLUSTERPROの設定(フェイルオーバグループ)

リソース名	設定項目	設定値
ミラーディスクリソース	リソース名	md
	詳細タブ - データパーティションのドライブ文字	G:
	詳細タブ - クラスタパーティションのドライブ文字	F:
Azure プローブポートリソース	リソース名	azurepp1
	プローブポート	26001(正常性プローブ - ポートで指定した値)
スクリプトリソース(DSRを使用する場合)	リソース名	script1

- CLUSTERPROの設定(監視リソース)

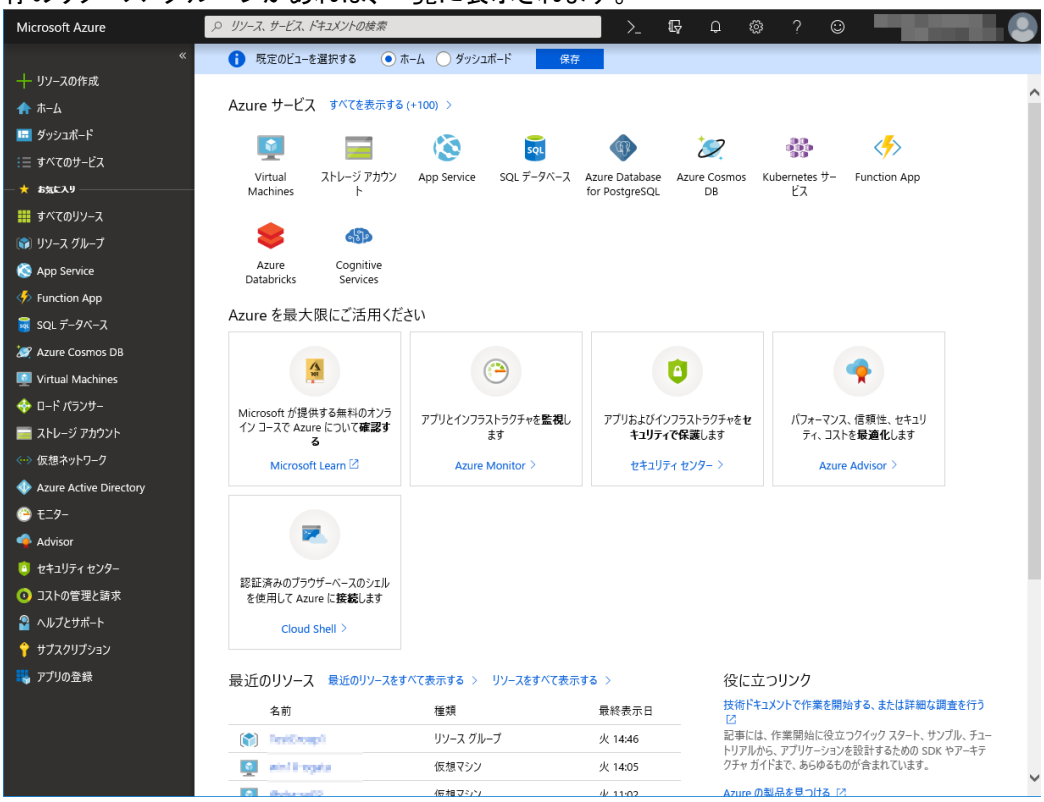
監視リソース名	設定項目	設定値
ミラーディスク監視リソース	－	－
Azure プローブポート監視リソース	監視リソース名	azureppw1
	回復対象	azurepp1
Azure ロードバランス監視リソース	監視リソース名	aurelbw1
	回復対象	azurepp1

5.2 Microsoft Azure の設定

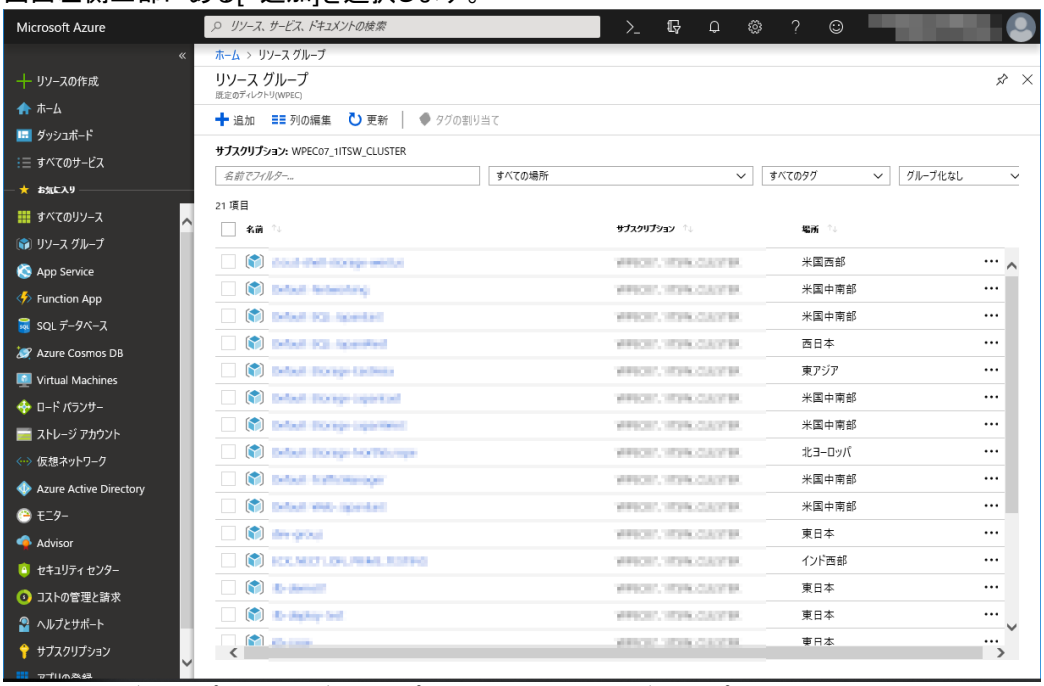
1) リソースグループの作成

Microsoft Azure ポータル(https://portal.azure.com/)にログインし、以下の手順でリソース グループを作成します。

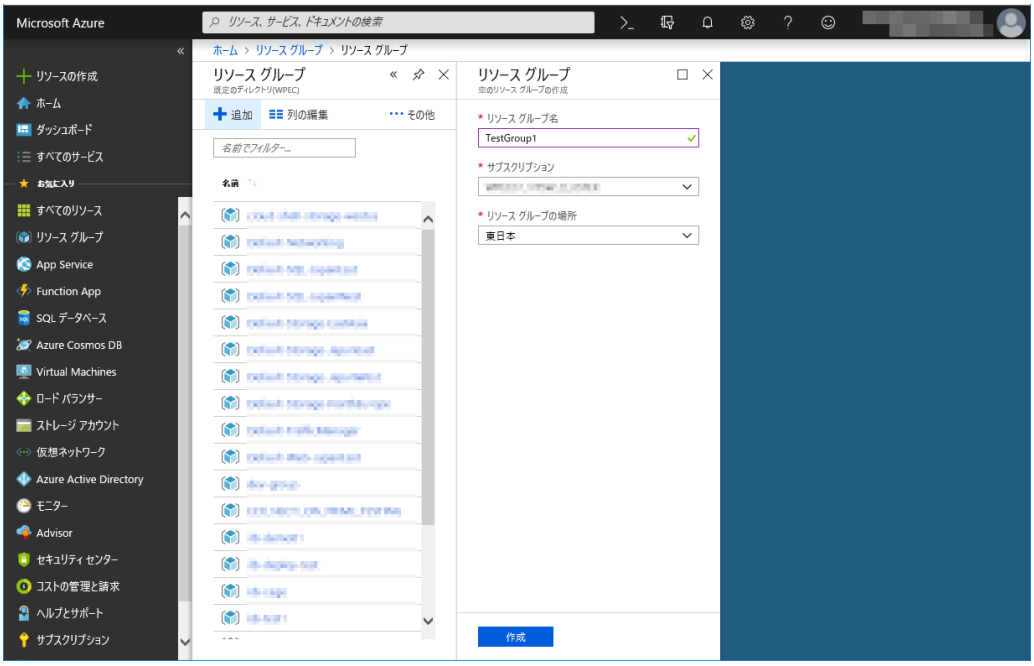
1. 画面左側のメニューにある[リソース グループ]もしくはリソース グループアイコンを選択します。既存のリソース グループがあれば、一覧に表示されます。



2. 画面左側上部にある[+追加]を選択します。



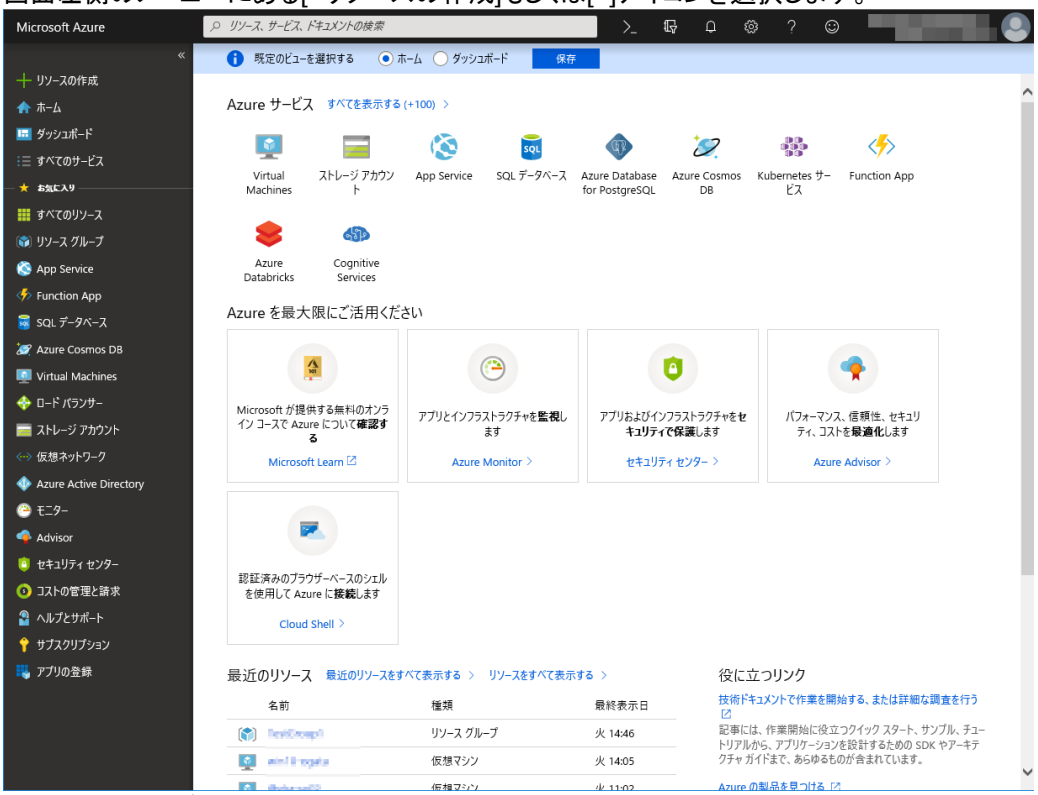
3. [リソース グループ名]、[サブスクリプション]、[リソース グループの場所]を設定し、[作成]を選択します。



2) 仮想ネットワークの作成

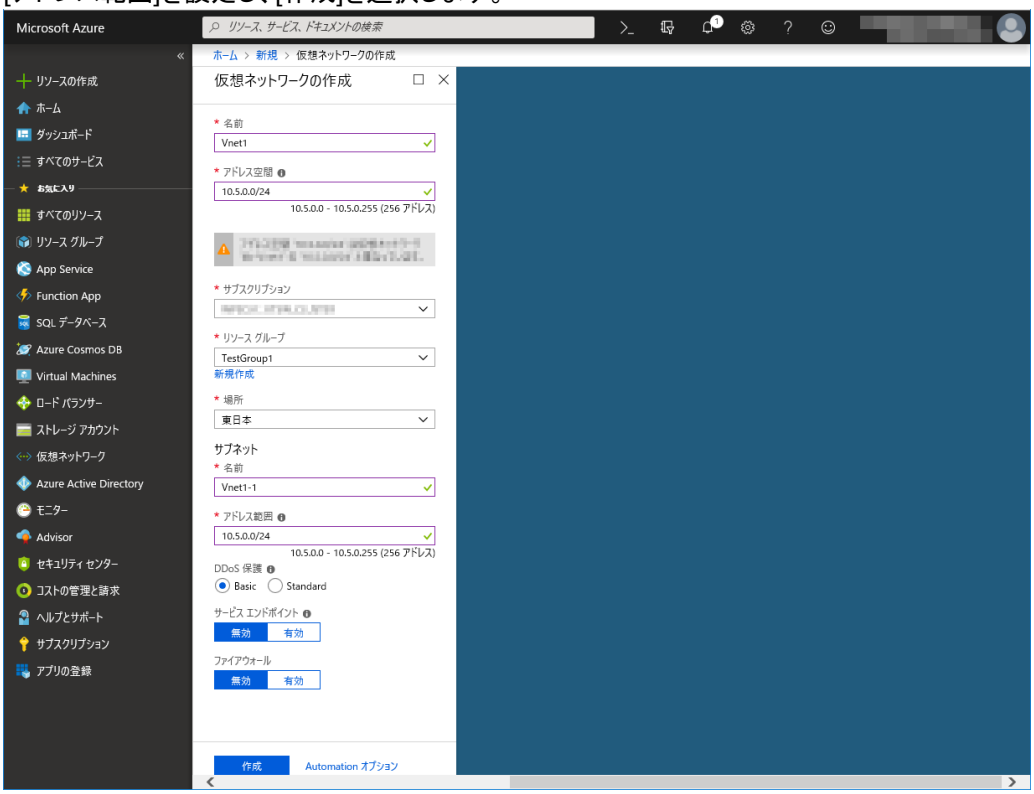
Microsoft Azure ポータル(https://portal.azure.com/)にログインし、以下の手順で仮想ネットワークを作成します。

1. 画面左側のメニューにある[+リソースの作成]もしくは[+]アイコンを選択します。



2. [ネットワーキング]>[仮想ネットワーク]を選択します。

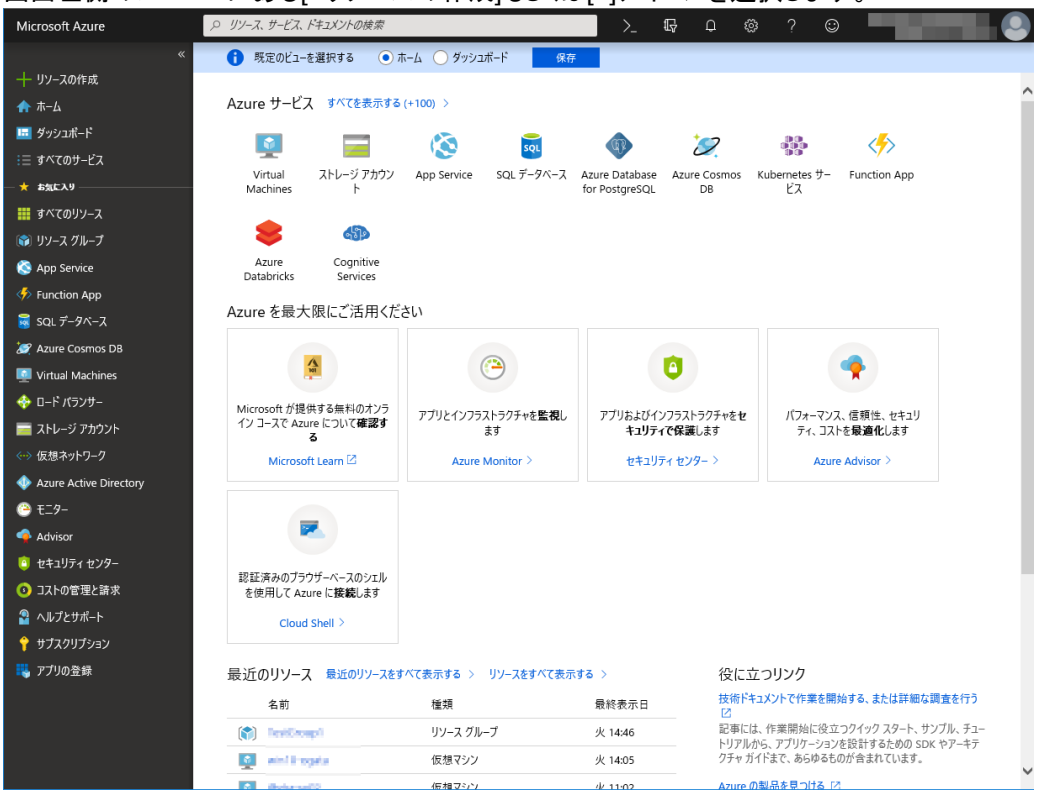
3. [名前]、[アドレス空間]、[サブスクリプション]、[リソース グループ名]、[場所]、サブネットの[名前]、[アドレス範囲]を設定し、[作成]を選択します。



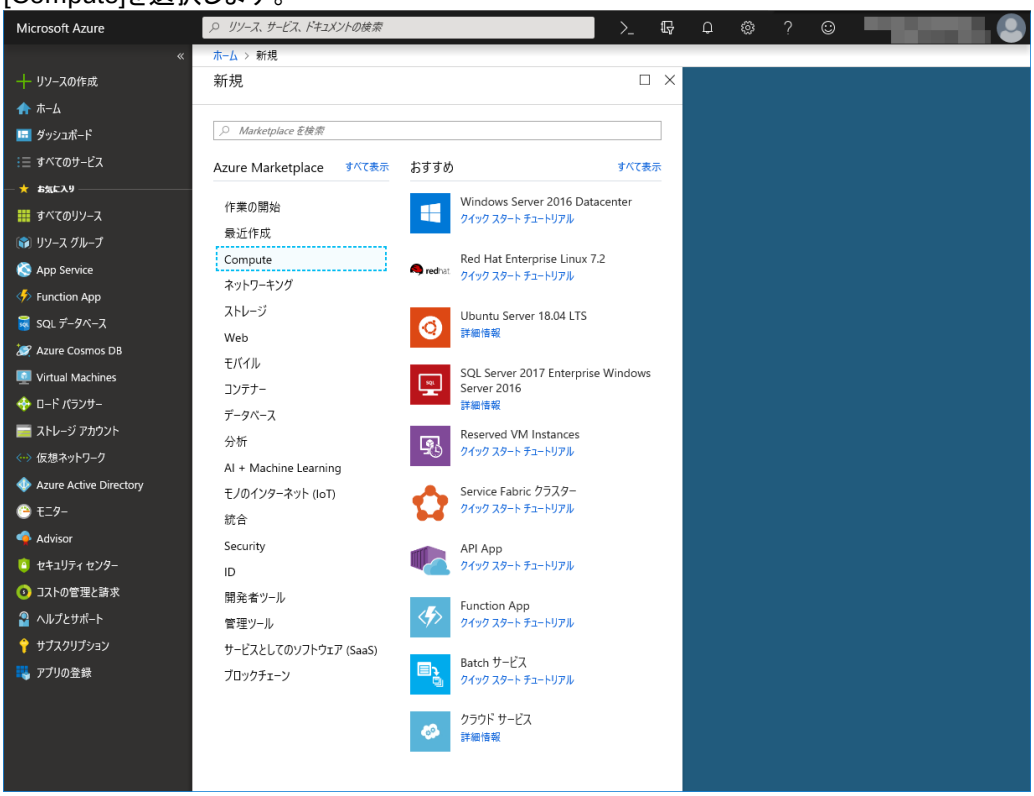
3) 仮想マシンの作成

Microsoft Azure ポータル(https://portal.azure.com/)にログインし、以下の手順で仮想マシンおよびディスクを追加します。
クラスタを構成する仮想マシンを必要な数だけ作成します。node-1、node-2 の順に作成します。

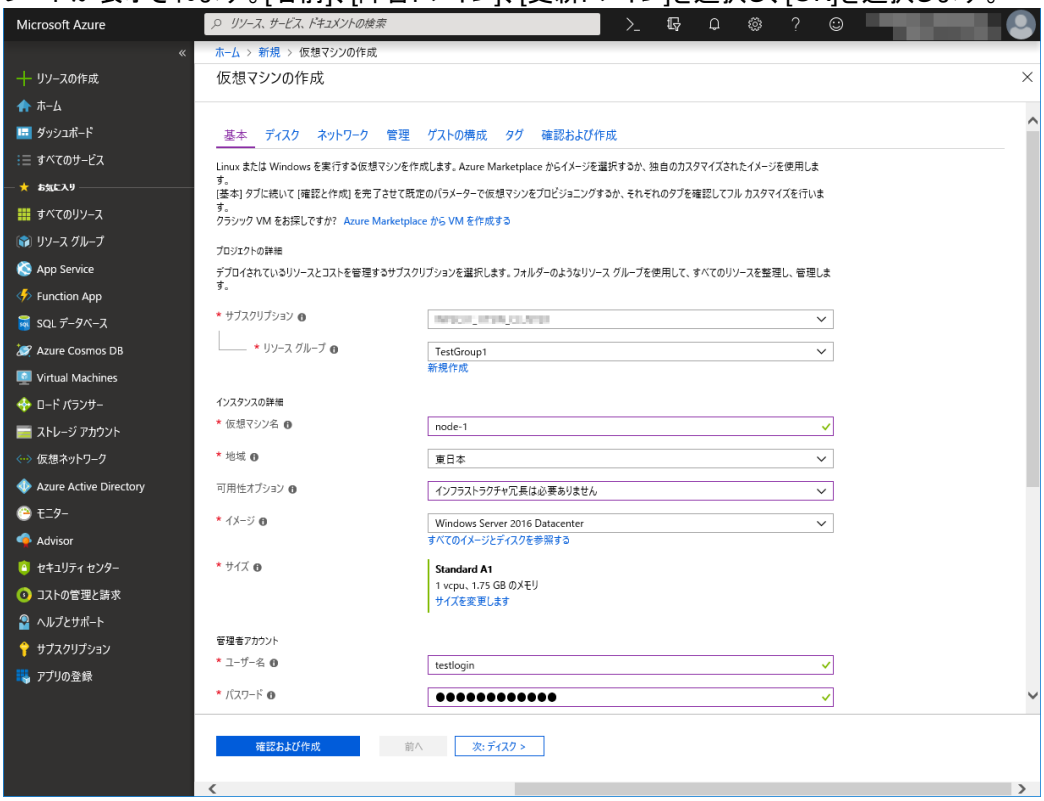
1. 画面左側のメニューにある[+リソースの作成]もしくは[+]アイコンを選択します。



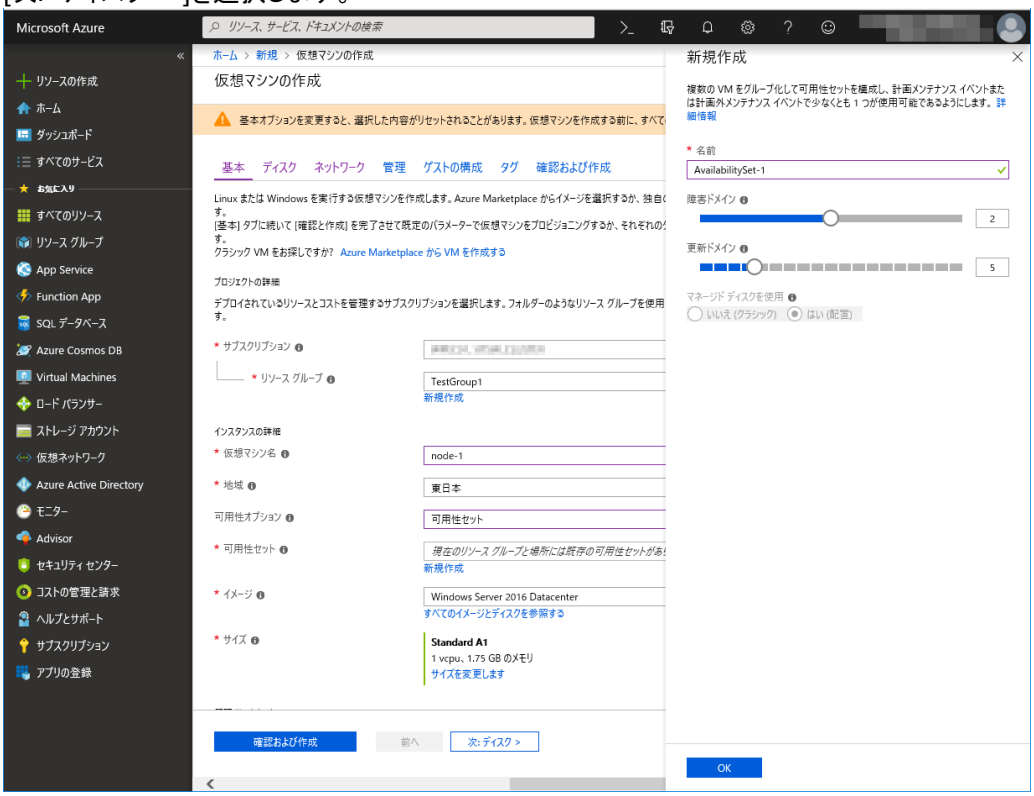
2. [Compute]を選択します。

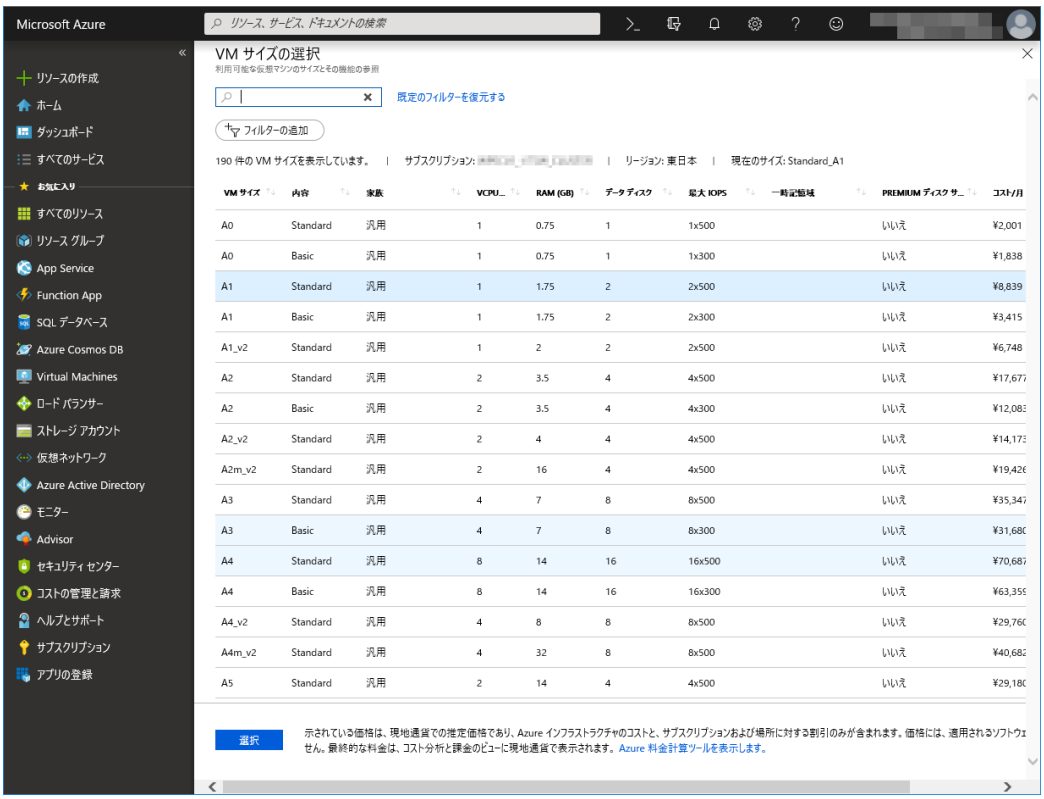


3. [Windows Server 2016 Datacenter]を選択します。
4. [基本]タブが表示されますので、[サブスクリプション]、[リソース グループ]、[仮想マシン名]、[地域]、[イメージ]、[サイズ]、[ユーザー名]、[パスワード]、[パスワードの確認]を設定します。
[可用性オプション]で可用性セットを選択し、[可用性セット]で新規作成を選択すると、[新規作成]ブレードが表示されます。[名前]、[障害ドメイン]、[更新ドメイン]を選択し、[OK]を選択します。

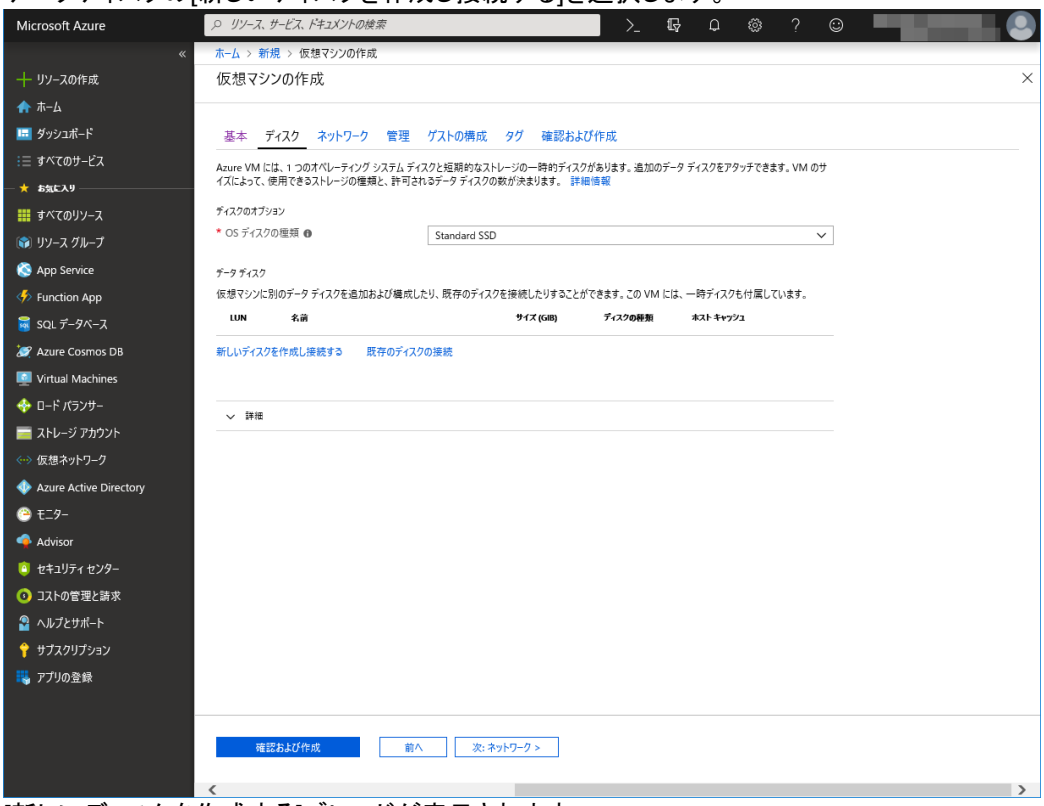


[サイズを変更します]を選択すると、[VM サイズの選択]ブレードが表示されます。
仮想マシンの目的に合ったサイズを一覧から選択し、[選択]を選択します。本書では[A1 Standard]を選択します。
[仮想マシン名]は、node-1 の場合は node-1、node-2 の場合は node-2 です。
[次: ディスク >]を選択します。

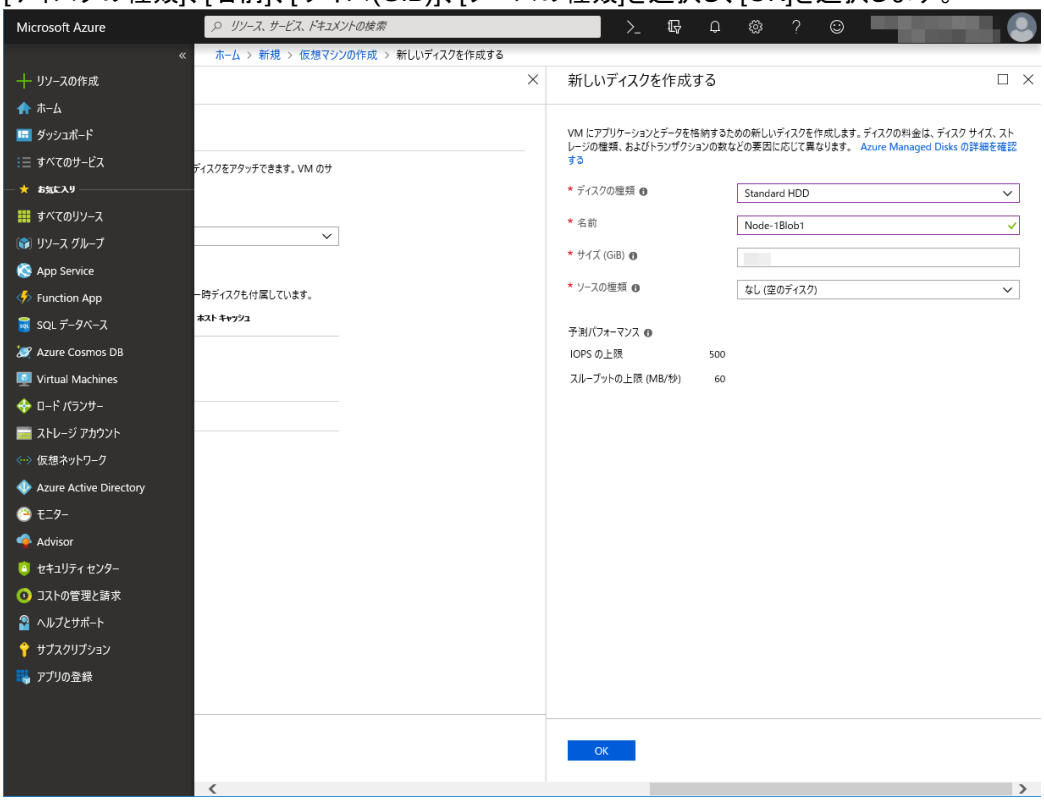




5. [ディスク]タブが表示されますので、以下の手順でミラーディスク(クラスタパーティション、データパーティション)に使用する Blob を追加します。
データディスクの[新しいディスクを作成し接続する]を選択します。

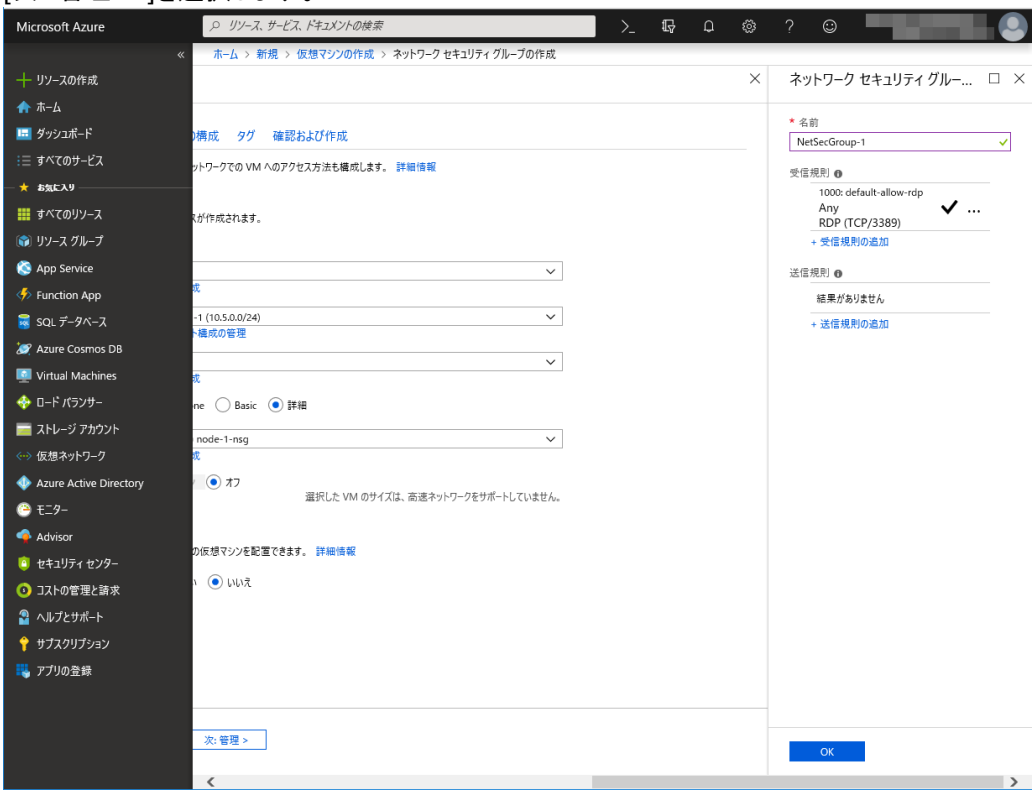


6. [新しいディスクを作成する]ブレードが表示されます。
[ディスクの種類]、[名前]、[サイズ(GiB)]、[ソースの種類]を選択し、[OK]を選択します。

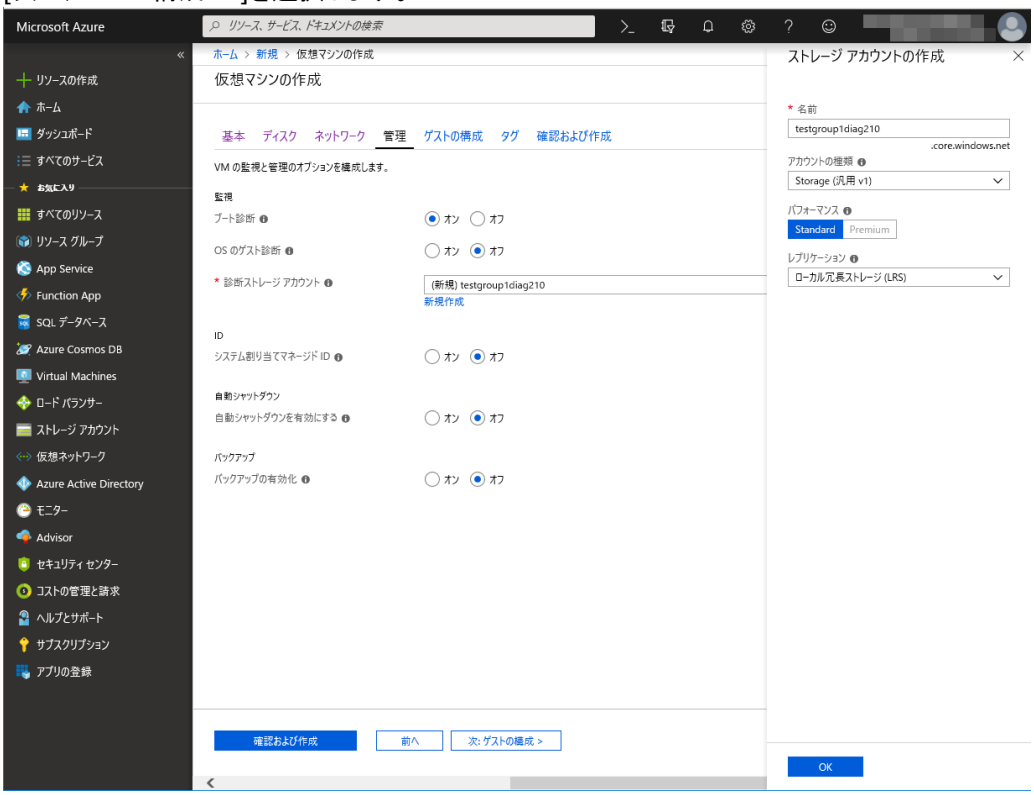


7. [次: ネットワーク >]を選択します。

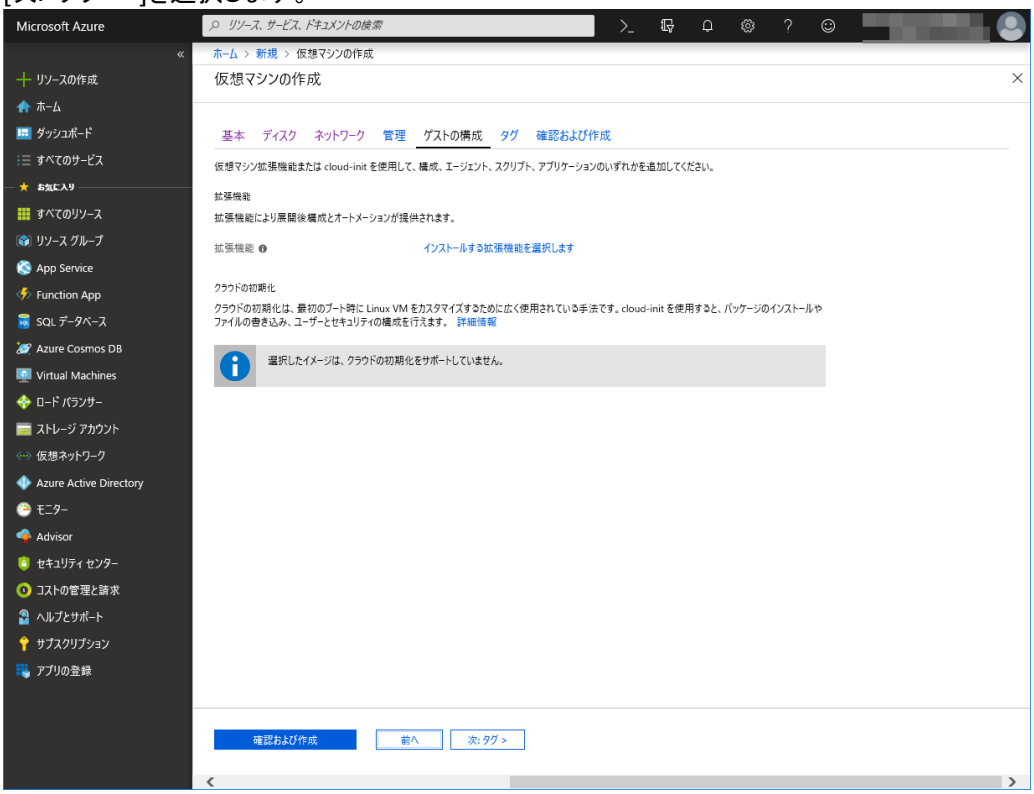
8. [ネットワーク]タブが表示されます。
[仮想ネットワーク]、[サブネット]、[ネットワーク セキュリティ グループ]、[ネットワーク セキュリティ グループの構成]を選択します。
[ネットワーク セキュリティ グループの構成]の新規作成を選択すると、[ネットワーク セキュリティ グループの作成]ブレードが表示されますので、[名前]を選択し、[OK]を選択します。
[次: 管理 >]を選択します。



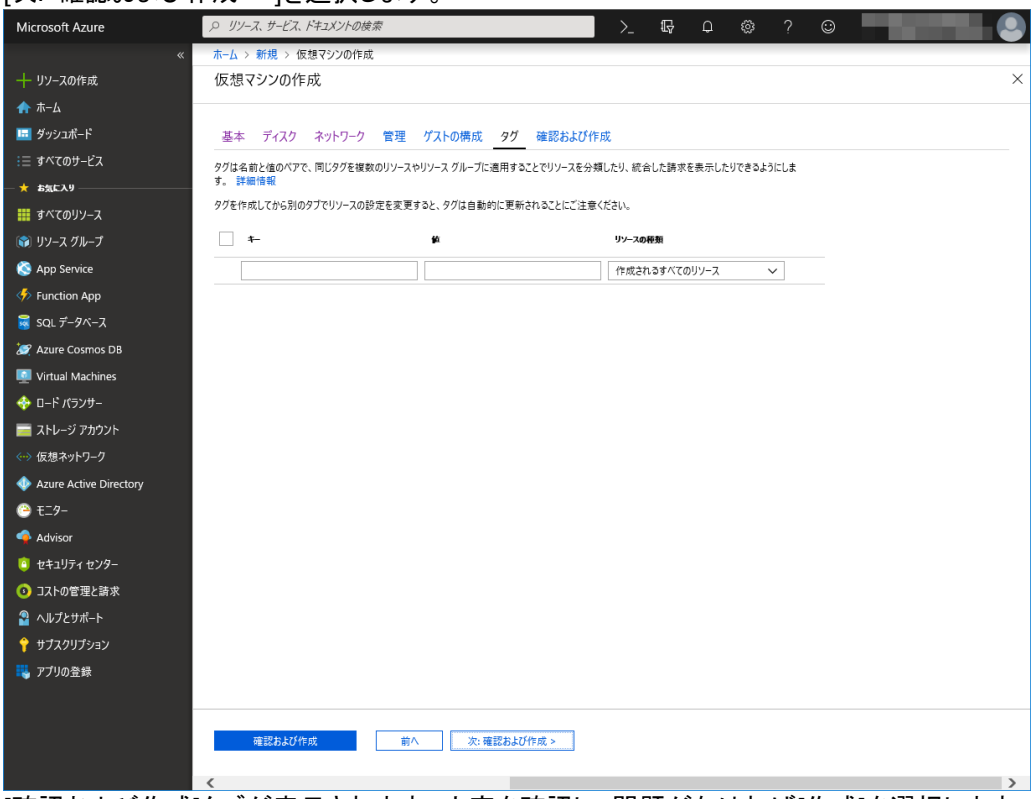
9. [管理]タブが表示されます。
[診断ストレージアカウント]で[新規作成]を選択すると、[ストレージアカウントの作成]ブレードが表示されます。
[名前]、[アカウントの種類]、[レプリケーション]を選択し、[OK]を選択します。
[診断ストレージアカウント]は、自動生成される既定値が入力されています。
[次: ゲストの構成 >]を選択します。



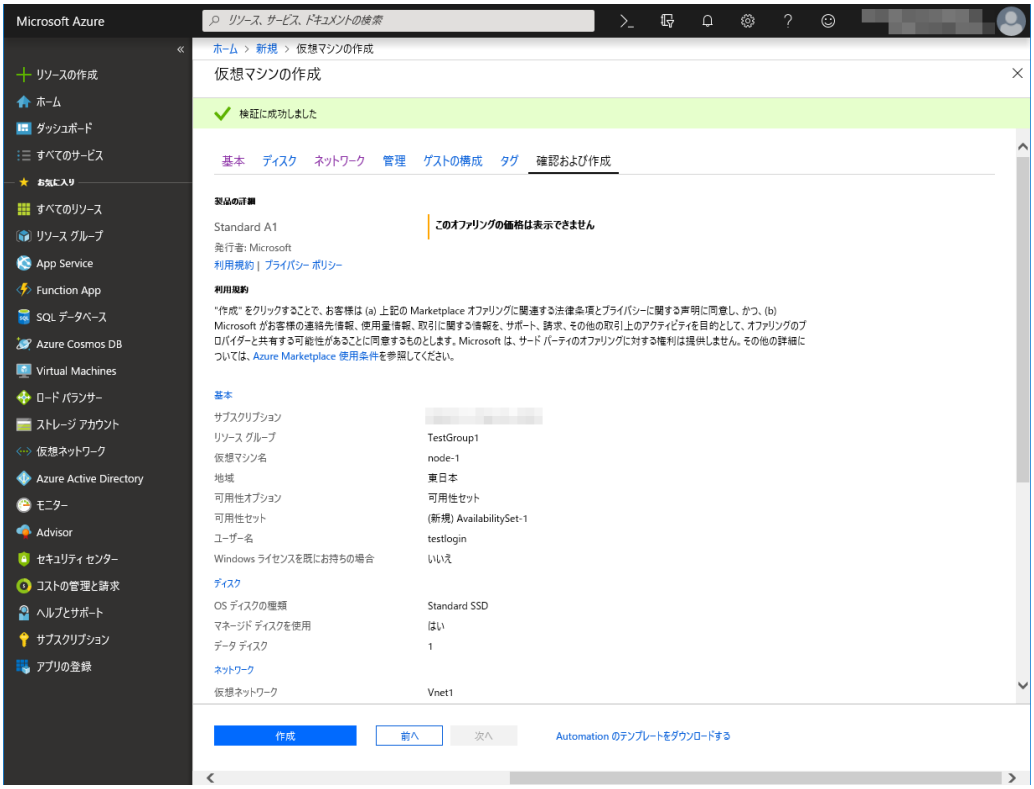
10. [次: タグ >]を選択します。



11. [次: 確認および作成 >]を選択します。



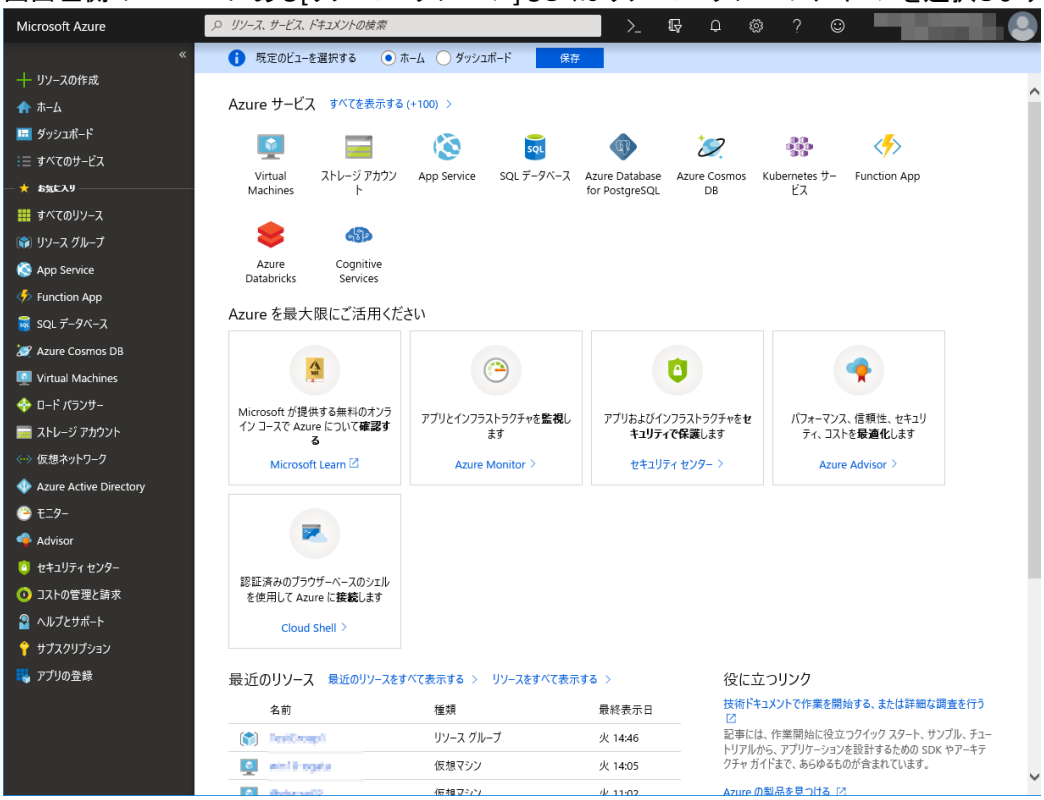
12. [確認および作成]タブが表示されます。内容を確認し、問題がなければ[作成]を選択します。デプロイが開始されます。デプロイには数分時間が掛かります。



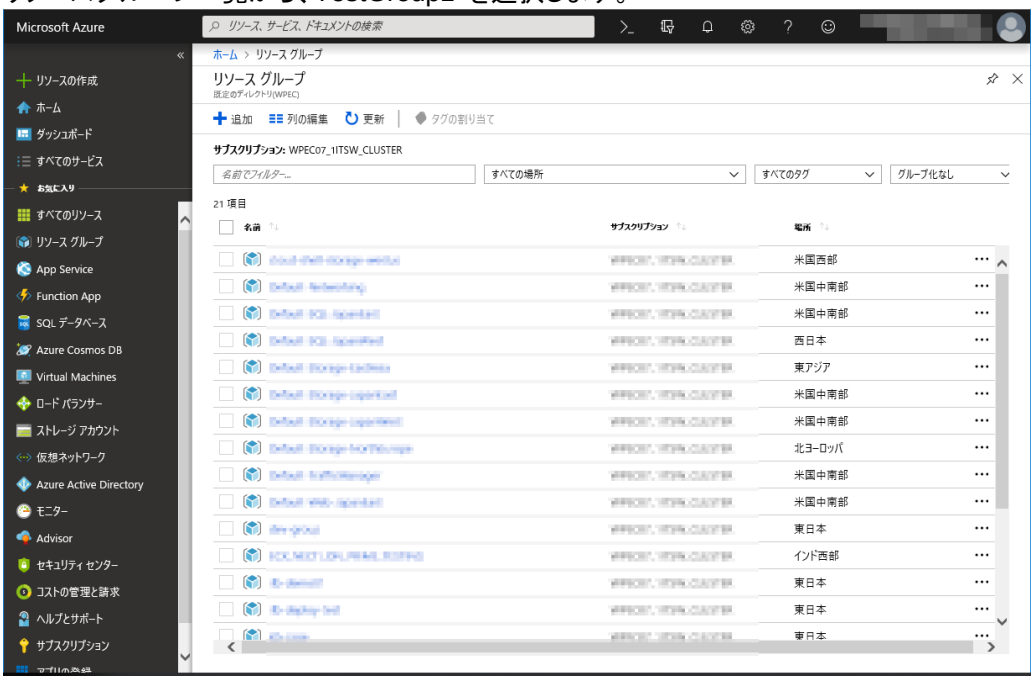
4) プライベート IP アドレスの設定

Microsoft Azure ポータル(https://portal.azure.com/)にログインし、以下の手順でプライベート IP アドレスの設定を変更します。IP アドレスは初期設定では動的割り当てとなっているため、静的割り当てに変更します。node-1、node-2 の順に実行します。

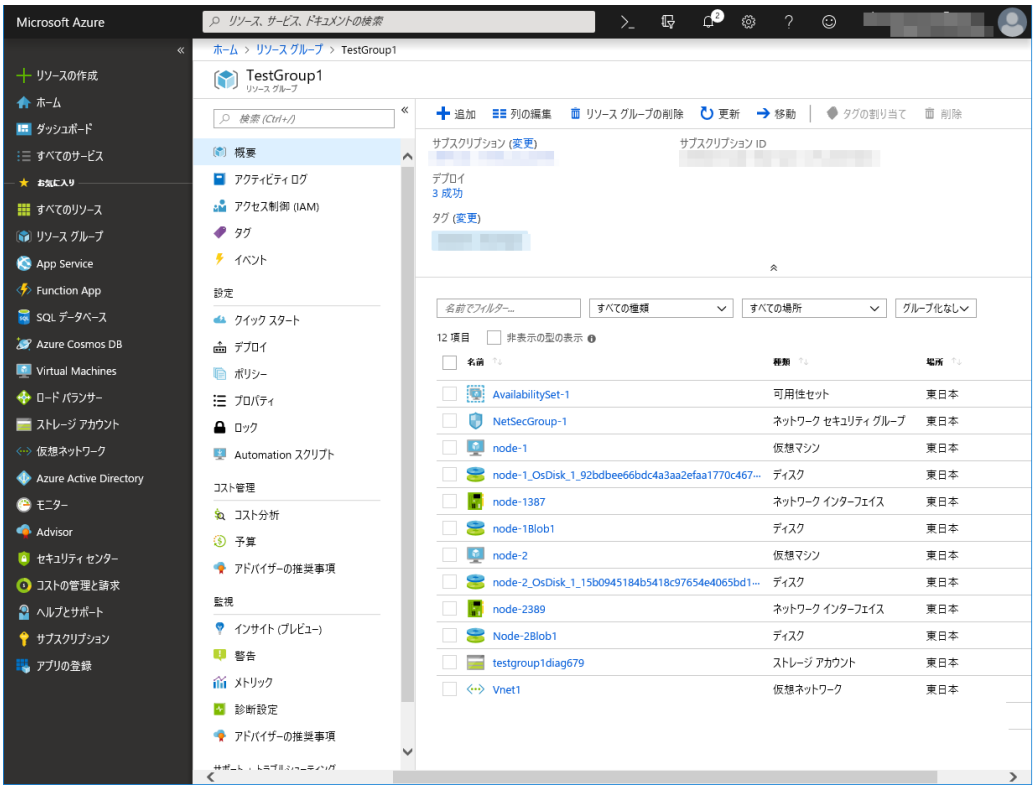
1. 画面左側のメニューにある[リソース グループ]もしくはリソース グループアイコンを選択します。



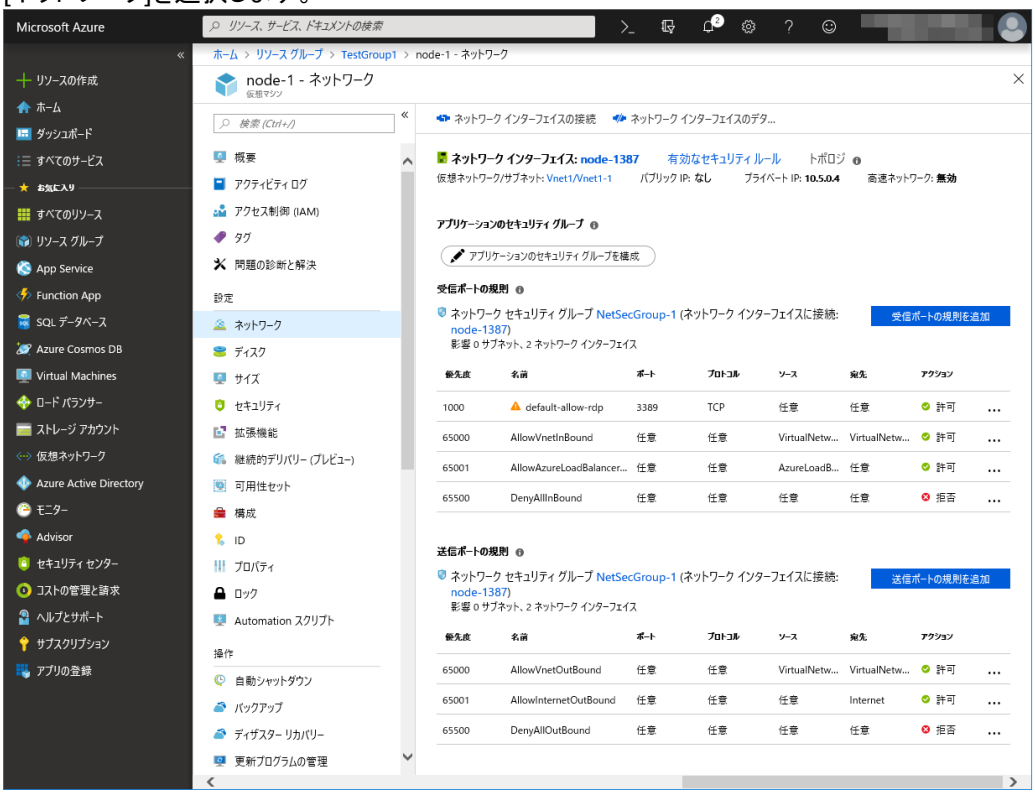
2. リソースグループ一覧から、TestGroup1 を選択します。



3. TestGroup1 の概要が表示されます。項目一覧から仮想マシン node-1 もしくは node-2 を選択します。

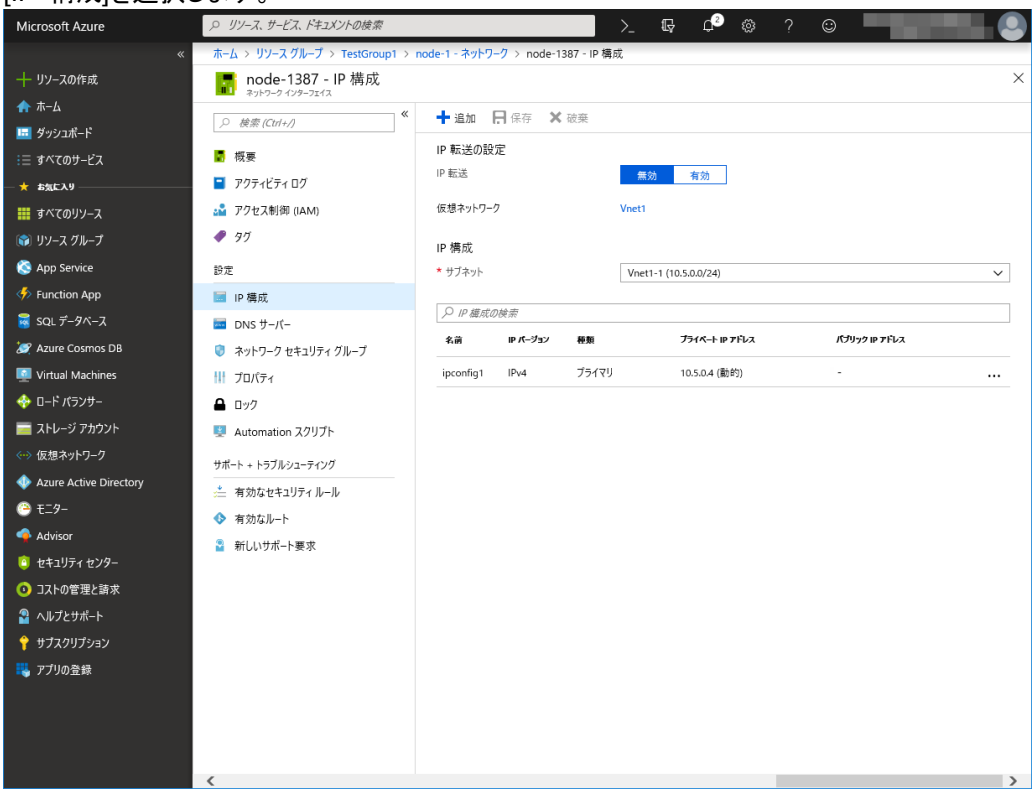


4. [ネットワーク]を選択します。

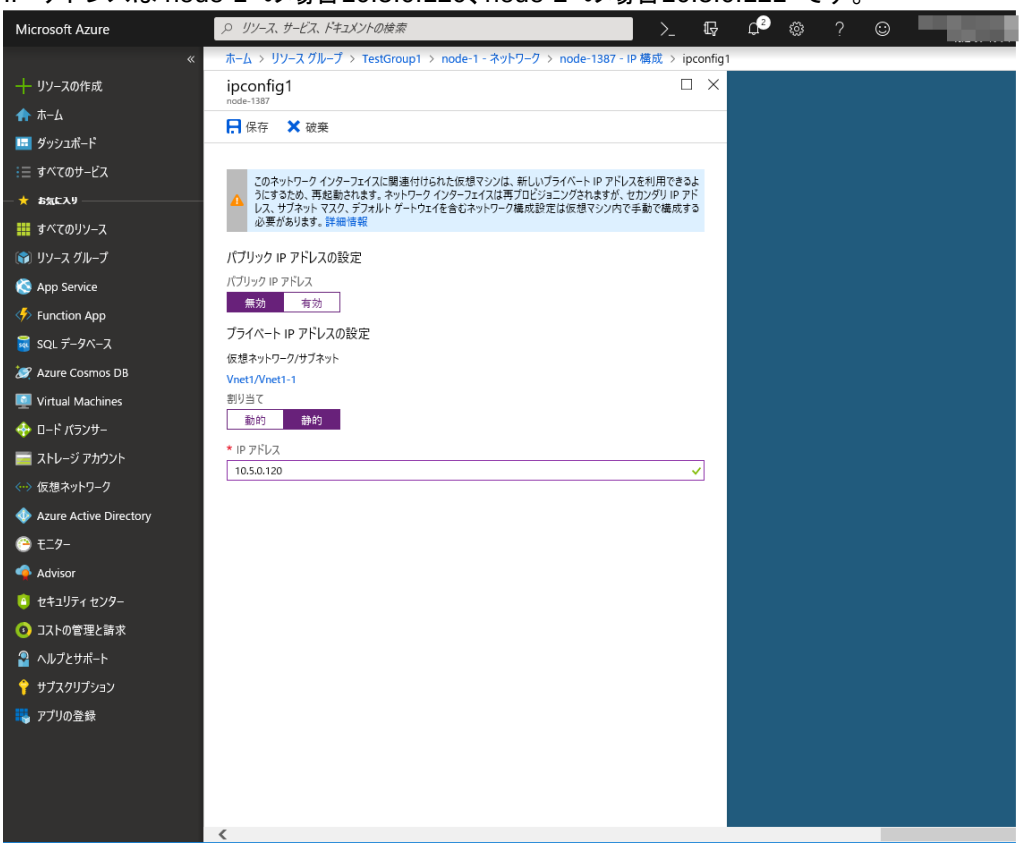


5. 一覧に1 つ表示されているネットワーク インターフェイスを選択します。ネットワーク インターフェイス名は自動生成されます。

6. [IP 構成]を選択します。



7. 一覧に1 つ表示されている ipconfig1 を選択します。
8. [プライベート IP アドレスの設定]の下に表示されている[割り当て]を、[静的]に変更します。その下にある[IP アドレス]に、静的に割り当てる IP アドレスを入力し、画面上部にある[保存]を選択します。IP アドレスは node-1 の場合10.5.0.120、node-2 の場合10.5.0.121 です。



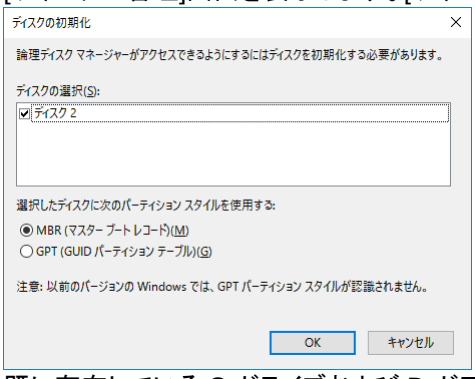
9. 新しいプライベートIP アドレスを利用できるようにするために、仮想マシンが自動的に再起動されます。

5) 仮想マシンの設定

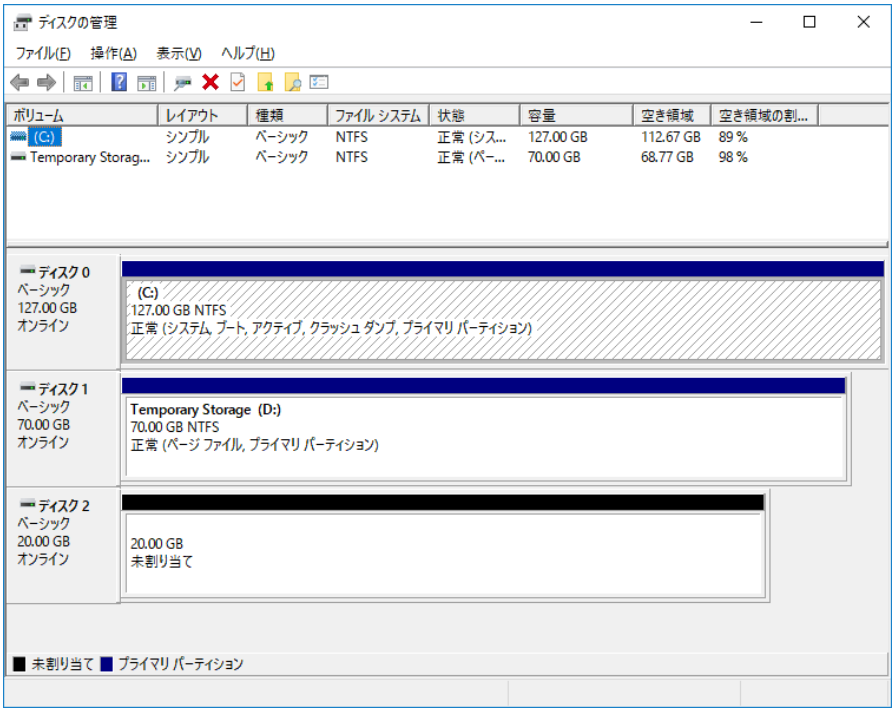
作成した node-1、node-2 へログインし、以下の手順で設定します。
必要な場合、OS を日本語化します。node-1、node-2 の順に実行してください。

次にミラーディスクリソース用のパーティションを設定します。追加した Blob にファイルシステムを作成します。
ミラーディスクリソース用のパーティションについては、『インストール&設定ガイド』-「第1章 システム構成を決定する」-「ハードウェア構成後の設定」-「2. ミラー用パーティションを設定する (ミラーディスク使用時は必須)」を参照してください。

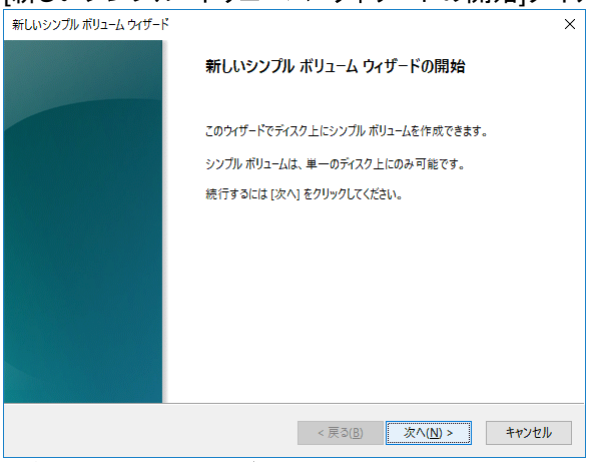
1. [ディスクの管理]画面を表示します。[ディスクの初期化]ダイアログが表示されます。



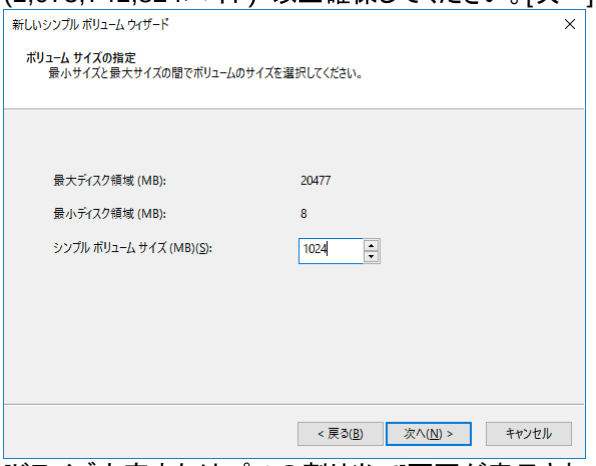
2. 既に存在している C ドライブおよび D ドライブの下に追加ディスクがディスク2 として未割り当て状態で表示されていることを確認します。



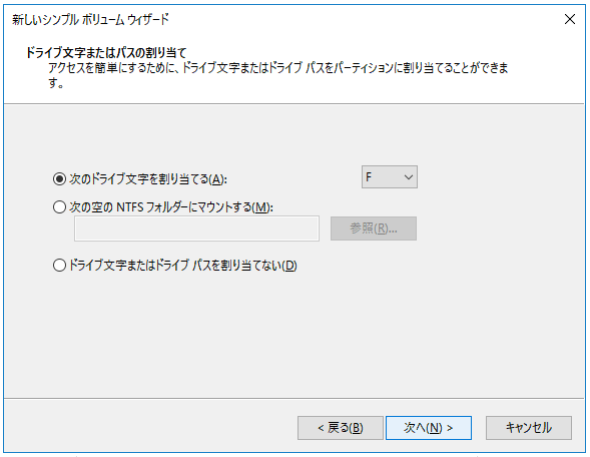
3. クラスタパーティションを作成します。[ディスク2]上で右クリックし、[新しいシンプル ボリューム]を選択します。
4. [新しいシンプル ボリューム ウィザードの開始]ダイアログが表示されます。[次へ]を選択します。



5. [ボリューム サイズの指定]画面が表示されます。クラスタパーティションは 1024MB (1,073,741,824バイト) 以上確保してください。[次へ]を選択します。

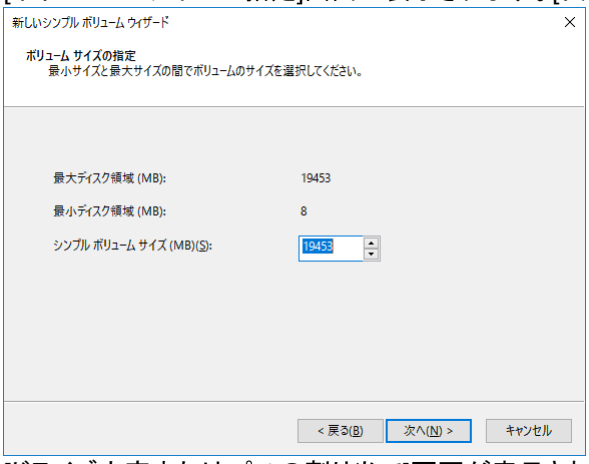


6. [ドライブ文字またはパスの割り当て]画面が表示されます。[次のドライブ文字を割り当てる]にF ドライブを選択します。フォーマットは行わず RAW パーティションのまま使用します。

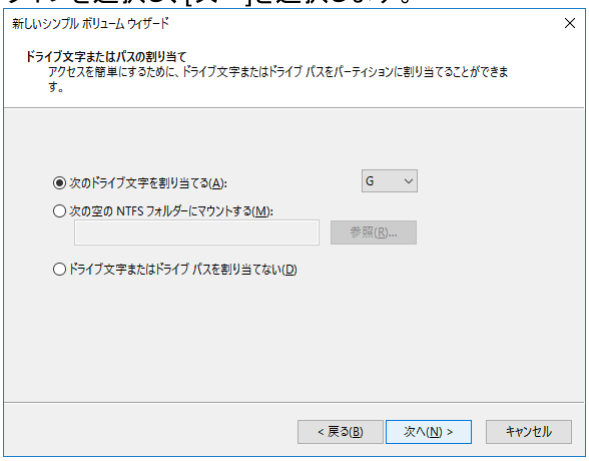


7. 次にデータパーティションを作成します。[ディスク2]上で右クリックし、[新しいシンプル ボリューム]を選択します。
8. [新しいシンプル ボリューム ウィザードの開始]ダイアログが表示されます。[次へ]を選択します。

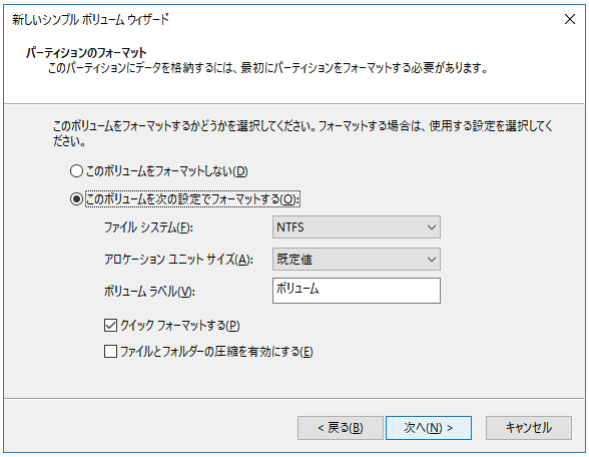
9. [ボリューム サイズの指定]画面が表示されます。[次へ]を選択します。



10. [ドライブ文字またはパスの割り当て]画面が表示されます。[次のドライブ文字を割り当てる]に G ドライブを選択し、[次へ]を選択します。

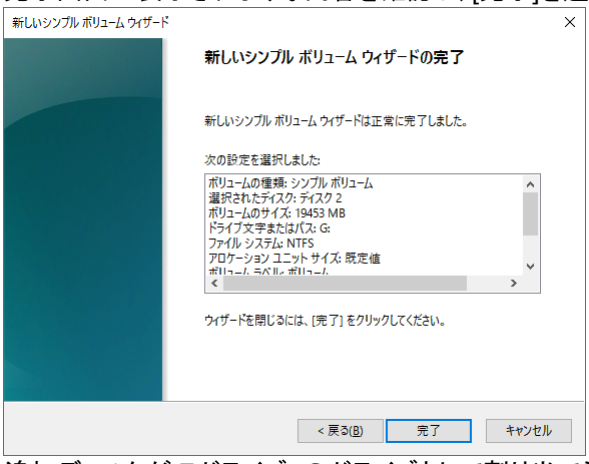


11. [パーティションのフォーマット]画面が表示されます。[ファイル システム]が NTFS であることを確認します。

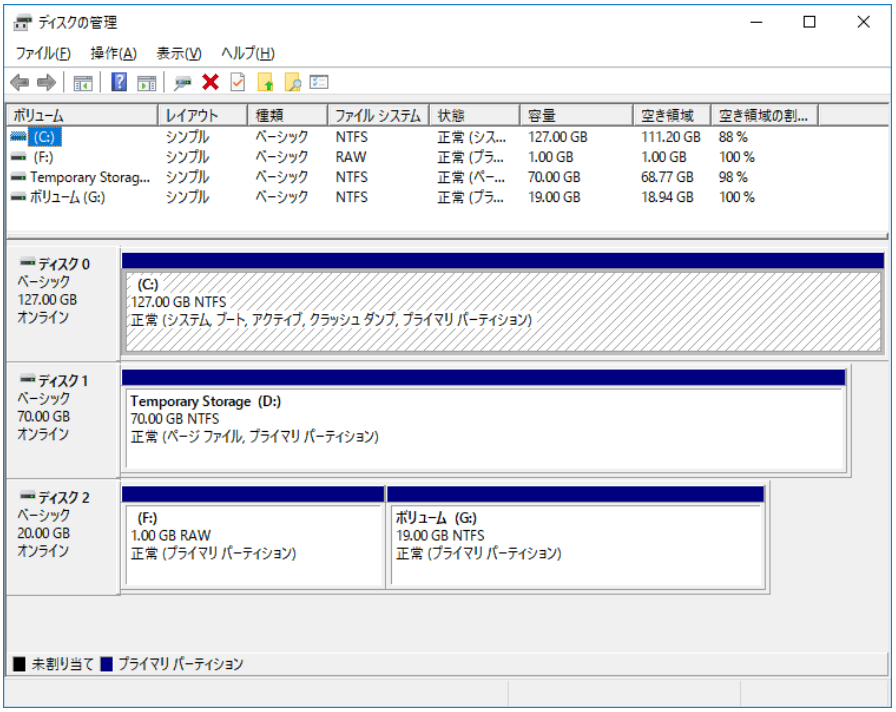


12. [次へ]を選択します。

13. 完了画面が表示されます。内容を確認し、[完了]を選択します。



14. 追加ディスクが F ドライブ、G ドライブとして割り当てられていることを確認します。



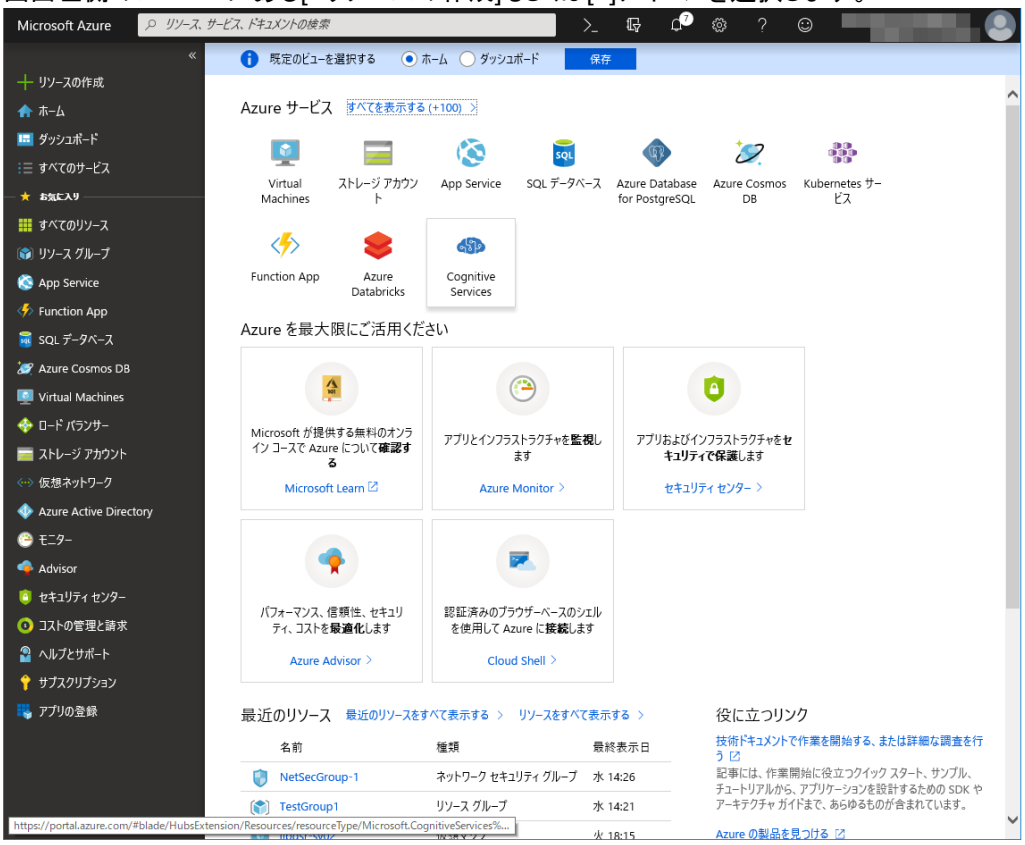
次に DSR を使用する場合、クラスタを構成する各ノードにおいてループバックアダプタを追加します。
DSR 構成を作成する場合は以下を参照してください。
https://jpn.nec.com/clusterpro/blog/20181031.html

6) ロードバランサーの作成

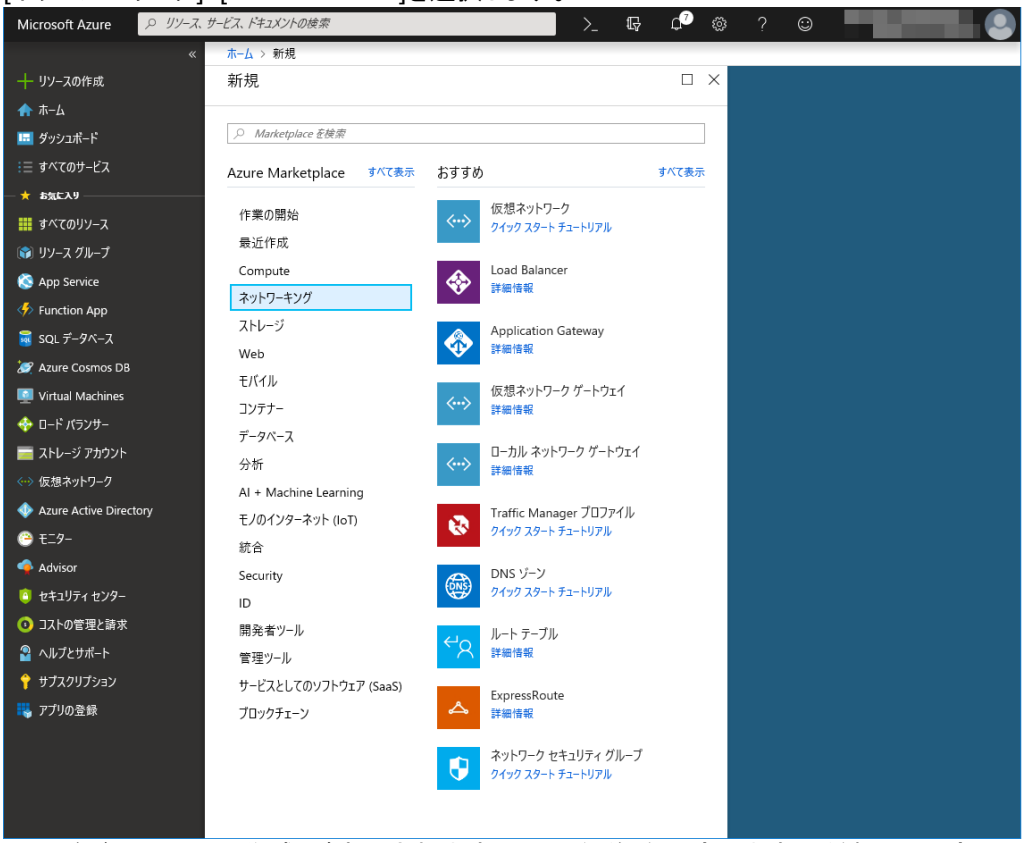
Microsoft Azure ポータル(https://portal.azure.com/)にログインし、以下の手順で内部ロードバランサーを追加します。
詳細は以下の Web サイトを参照してください。

- Load Balancer :
  https://docs.microsoft.com/ja-jp/azure/load-balancer/

1. 画面左側のメニューにある[+リソースの作成]もしくは[+]アイコンを選択します。

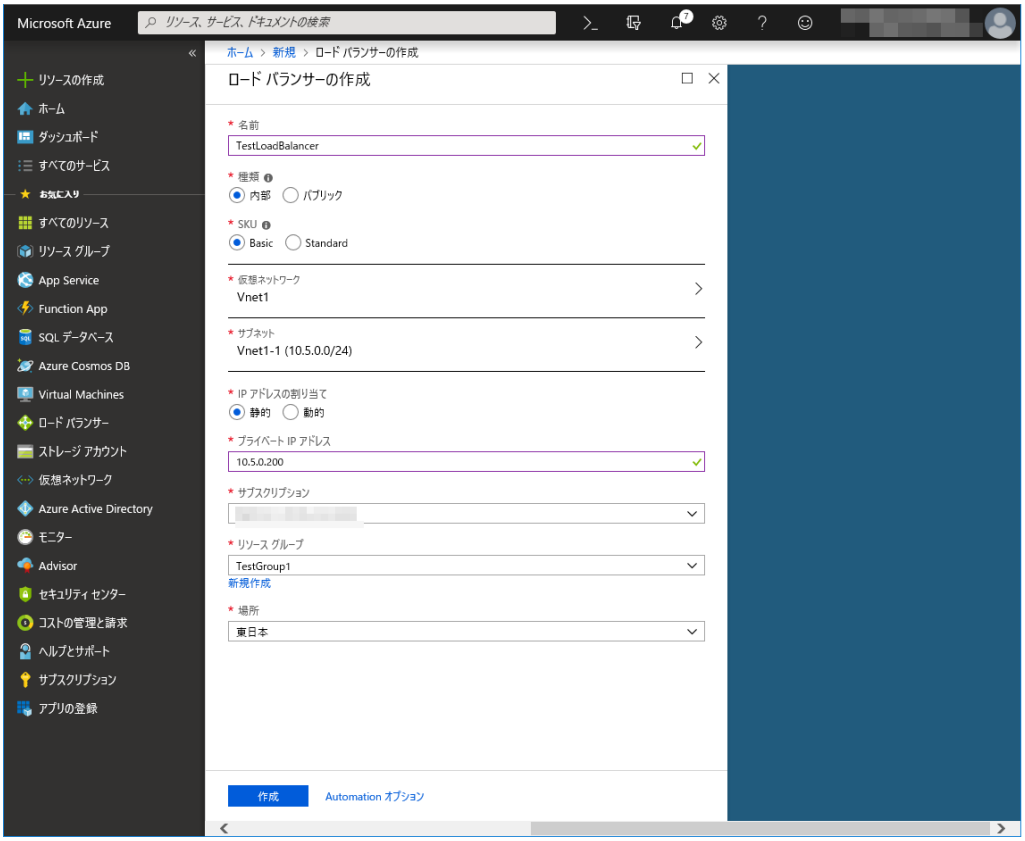


2. [ネットワーキング]>[Load Balancer]を選択します。



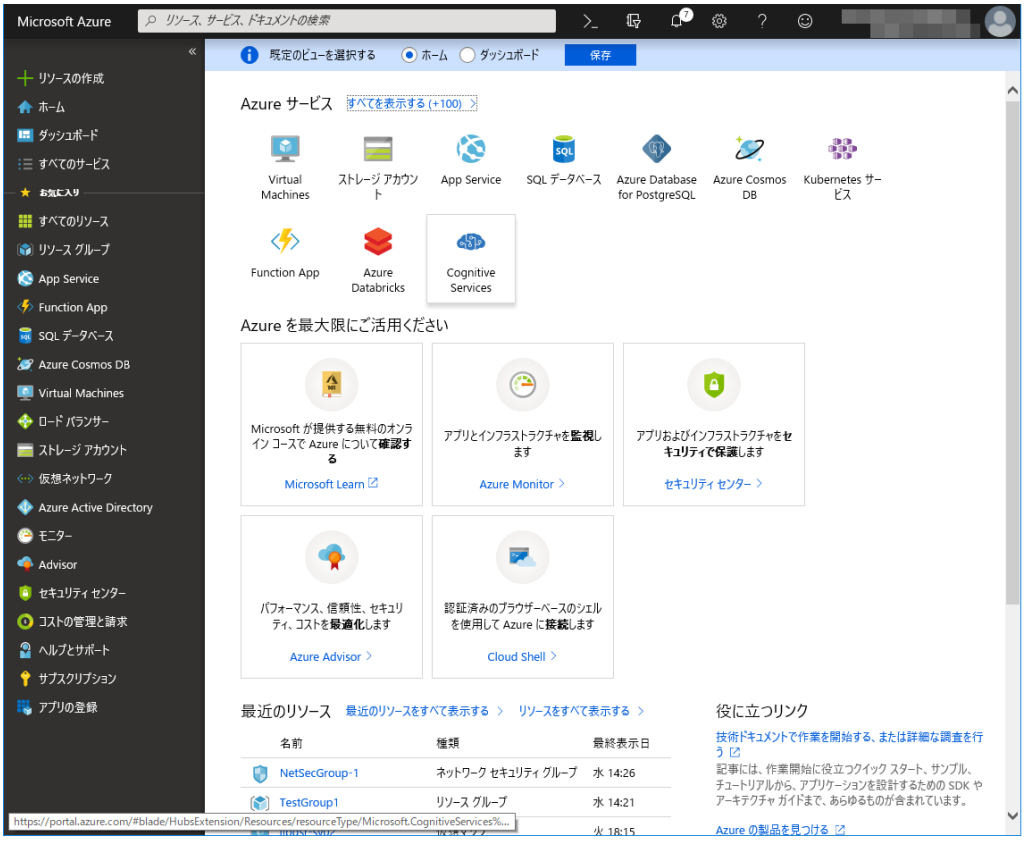
3. [ロードバランサーの作成]が表示されますので、[名前]を設定します。[種類]は[内部]、[SKU]は[Basic]を選択します。
4. [仮想ネットワーク]、[サブネット]は、「2) **仮想ネットワークの作成**」にて作成した[仮想ネットワーク]、[サブネット]を選択します。

5. [IP アドレスの割り当て]、[プライベート IP アドレス]、[サブスクリプション]、[リソースグループ]、[場所]を設定し、[作成]を選択します。ロードバランサーのデプロイが開始されます。デプロイには数分掛かります。

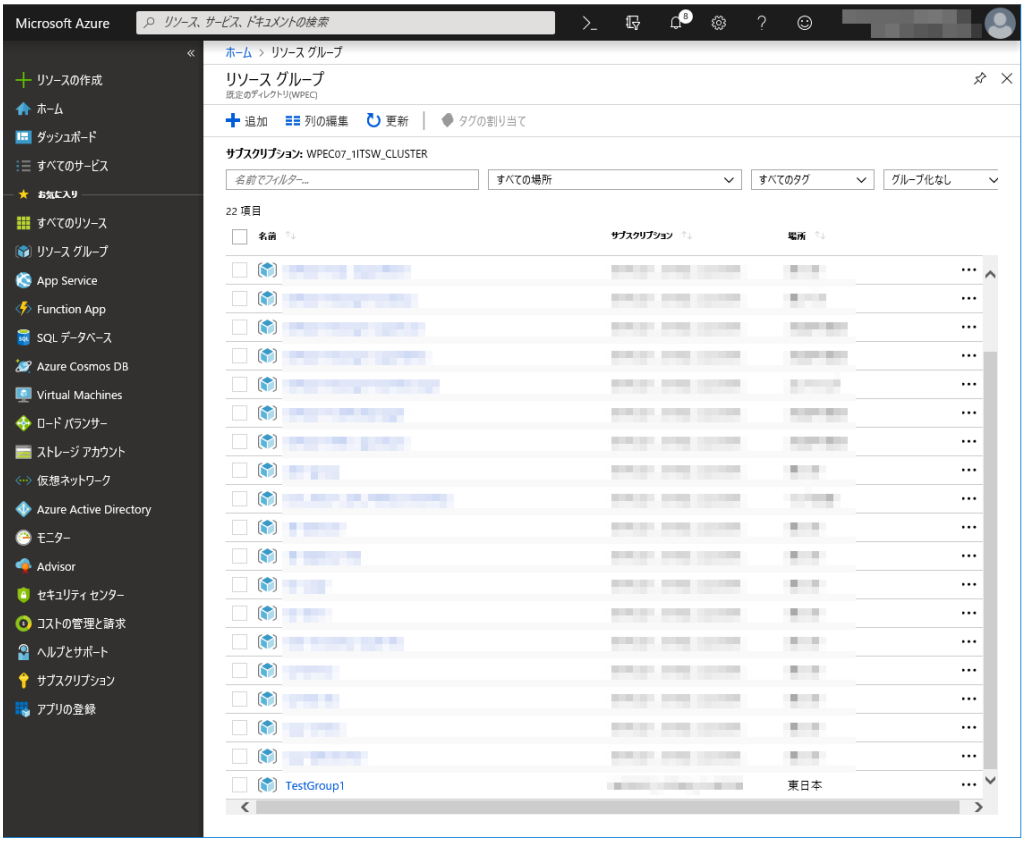


7) ロードバランサーの設定(バックエンドプールの設定)

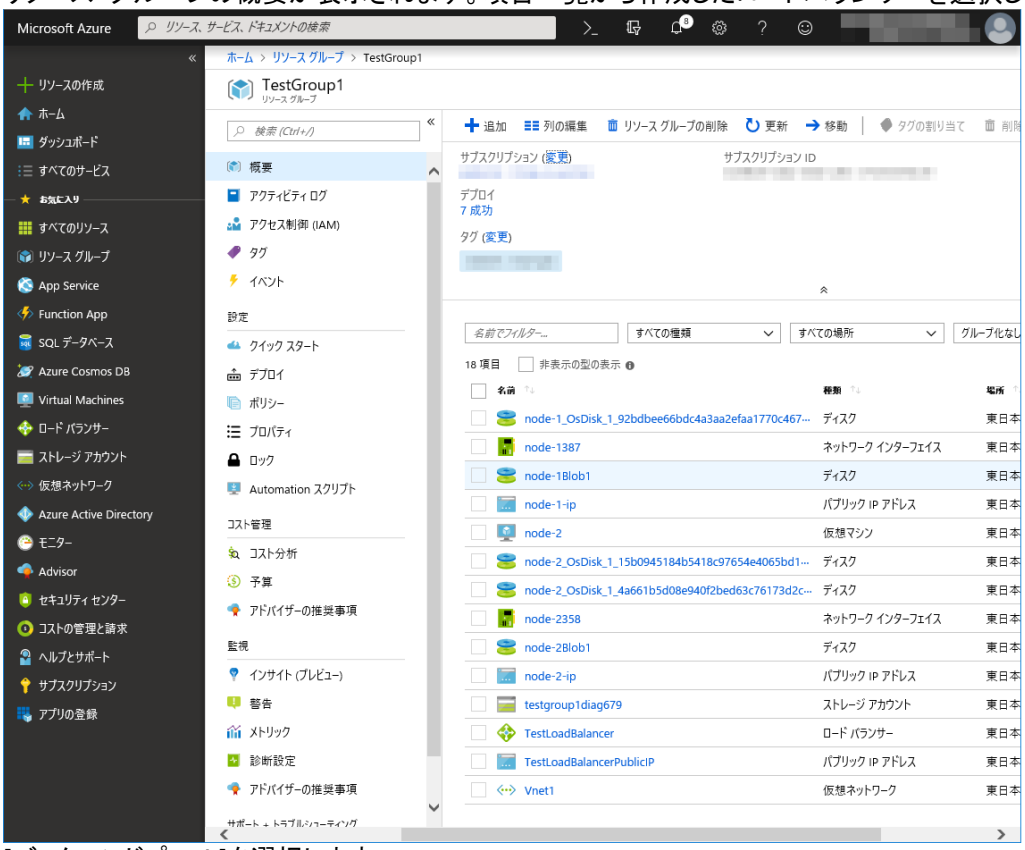
1. 次に可用性セットに登録されている仮想マシンをロードバランサーに紐付けます。ロードバランサーのデプロイが完了したら、画面左側のメニューにある[リソース グループ]もしくはリソース グループアイコンを選択します。



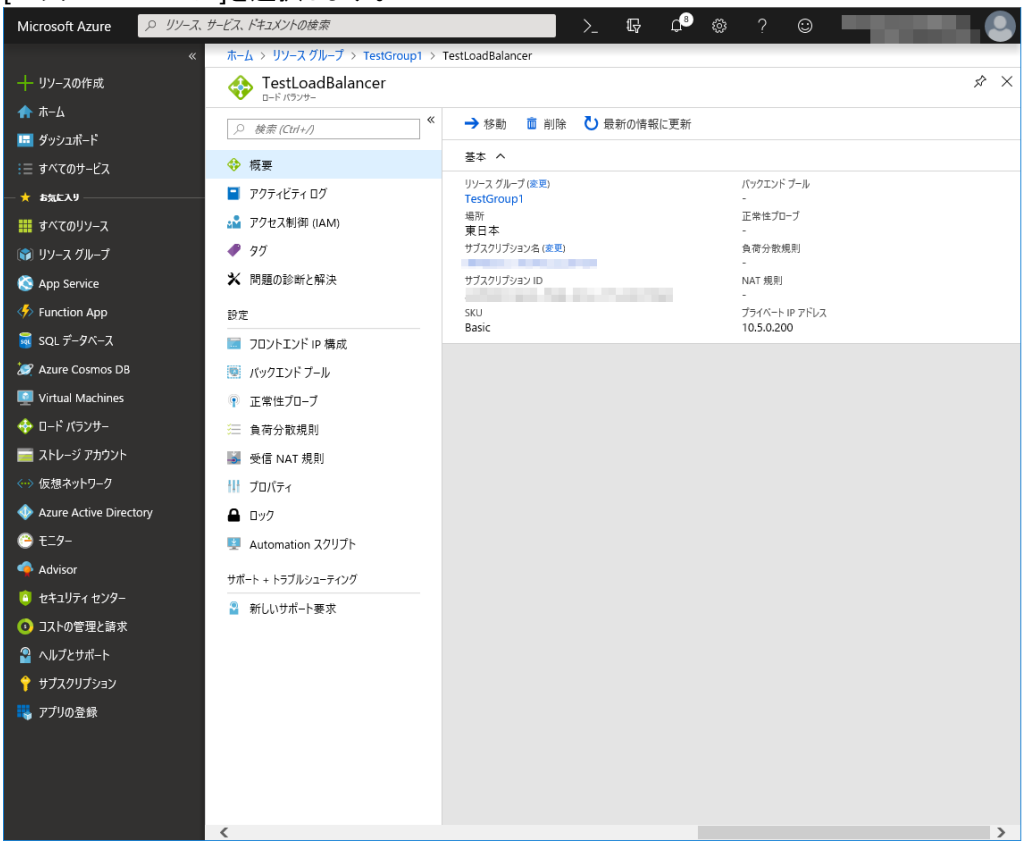
2. リソース グループ一覧から作成したロードバランサーが所属するリソース グループを選択します。



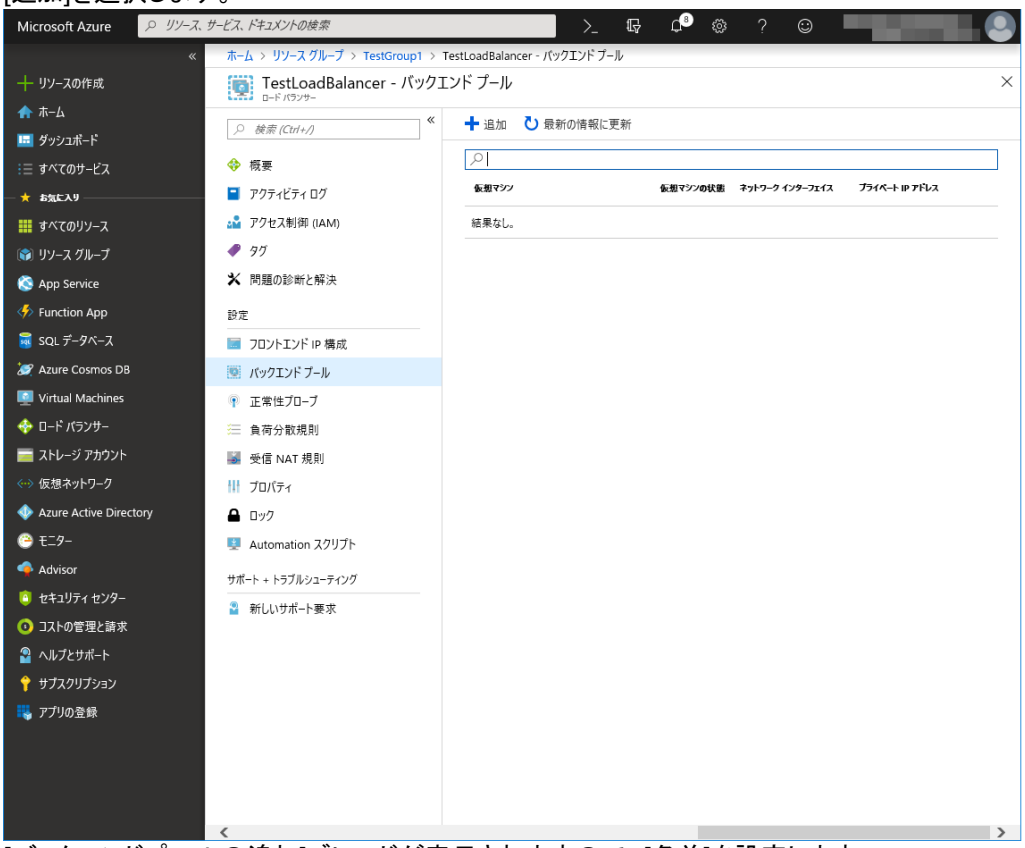
3. リソース グループの概要が表示されます。項目一覧から作成したロードバランサーを選択します。



4. [バックエンドプール]を選択します。

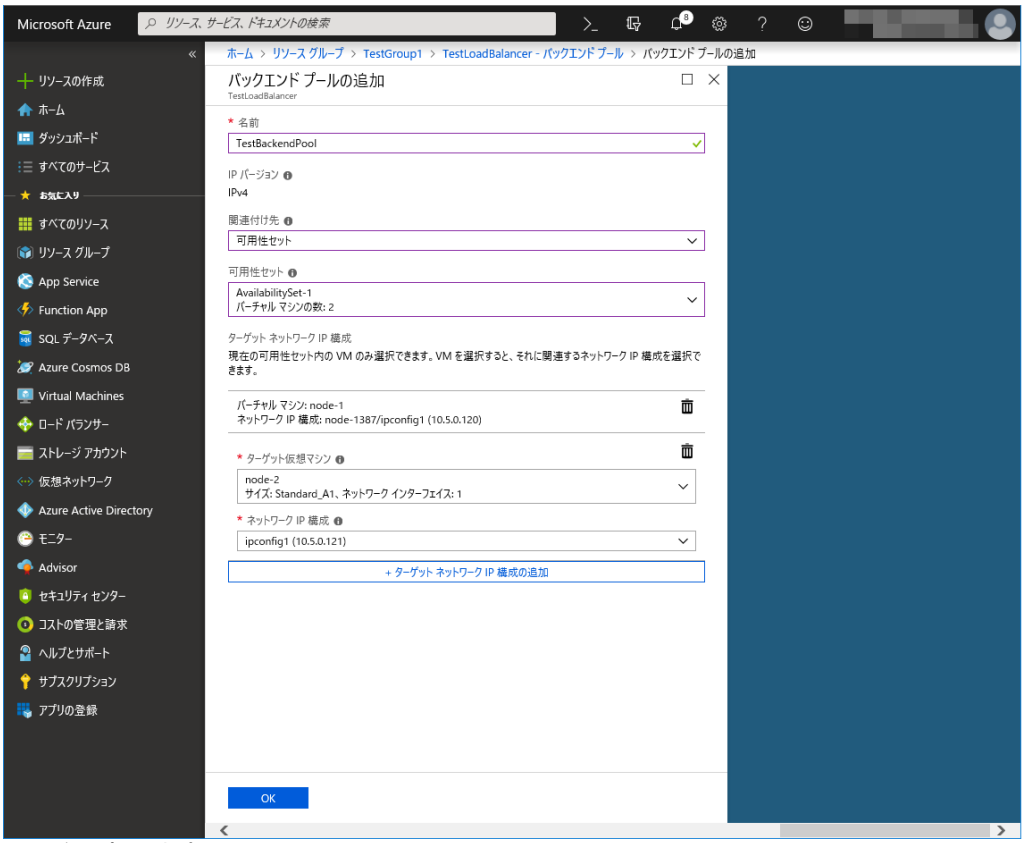


5. [追加]を選択します。



6. [バックエンドプールの追加]ブレードが表示されますので、[名前]を設定します。
7. [関連付け先]は、[可用性セット]を設定します。
8. [可用性セット]を設定します。
9. [+ ターゲットネットワーク IP 構成の追加]を選択します。
10. [ターゲット仮想マシン]、[ネットワーク IP 構成]に対象の仮想マシンを設定します。

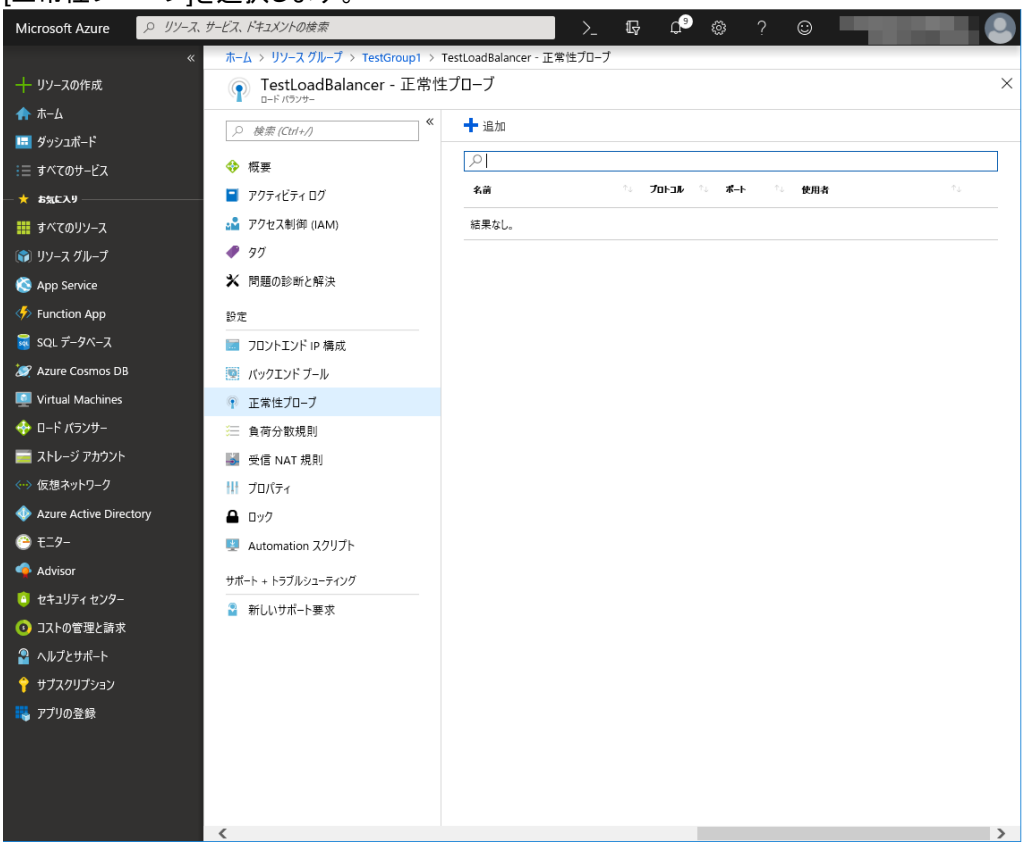
11. 9-10を対象の仮想マシン数分繰り返します。



12. [OK]を選択します。

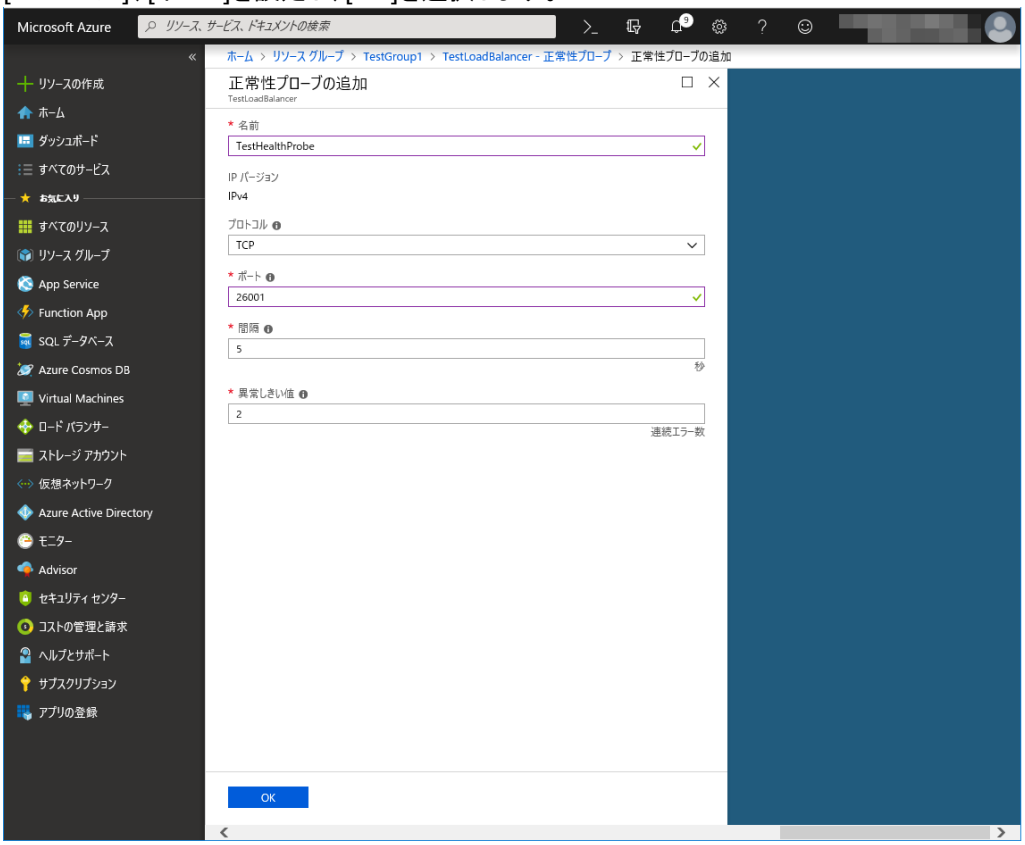
8) ロードバランサーの設定(正常性プローブの設定)

1. [正常性プローブ]を選択します。



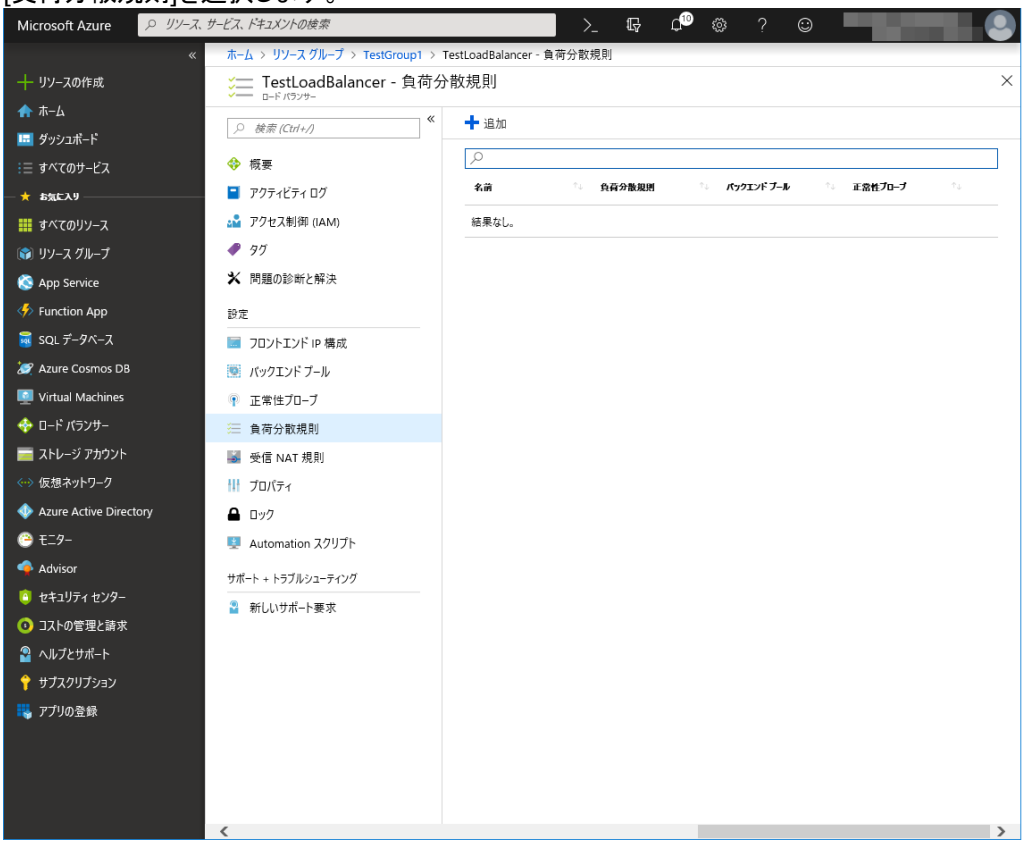
2. [追加]を選択します。
3. [正常性プローブの追加]ブレードが表示されますので、[名前]を設定します。

4. [プロトコル]、[ポート]を設定し、[OK]を選択します。



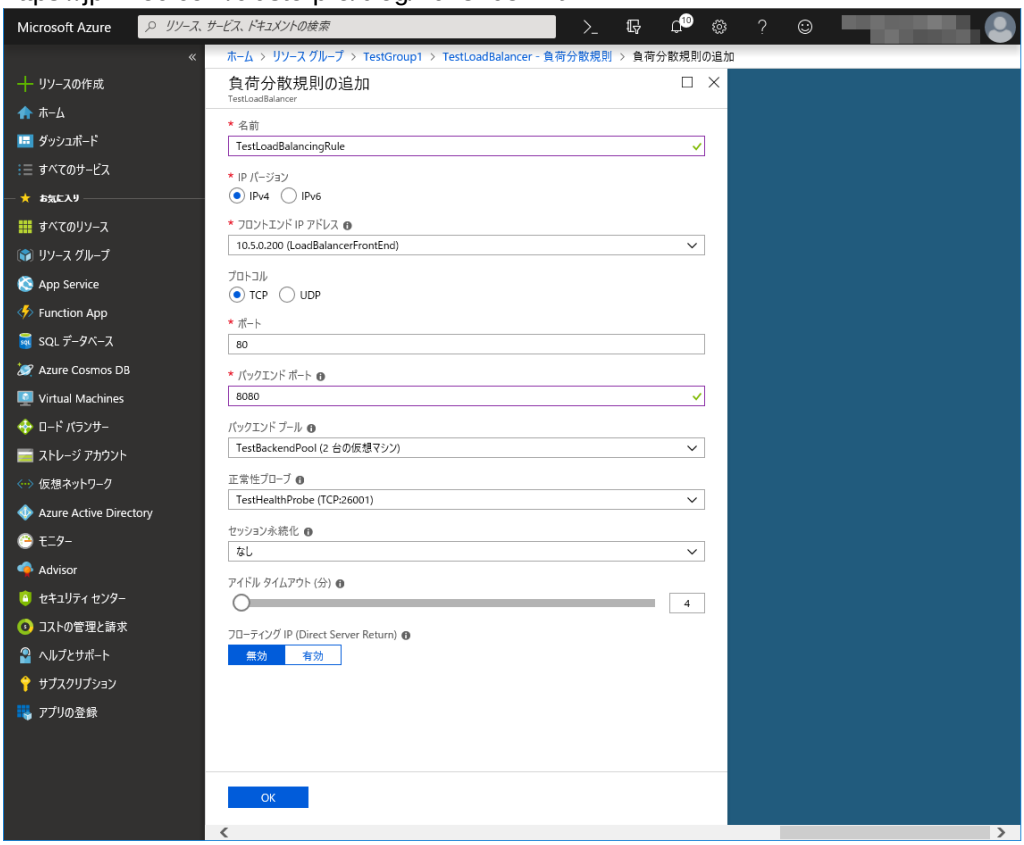
9) ロードバランサーの設定(負荷分散規則の設定)

1. [負荷分散規則]を選択します。



2. [追加]を選択します。
3. [負荷分散規則の追加]が表示されますので、[名前]を設定します。

4. [ポート]、[バックエンドポート]を設定し、[OK]を選択します。
DSR を使用する場合は、[ポート]と[バックエンドポート]に同一のポート番号を設定、[フローティング IP(Direct Server Return)]を有効に設定し、[OK]を選択します。その際指定するポート番号は、業務を提供するアプリケーションへの接続に使用するポート番号を指定します(例.80)。
DSR 構成を作成する場合は以下を参照してください。
https://jpn.nec.com/clusterpro/blog/20181031.html



10) OS 起動時間の調整、ネットワーク設定の確認、ファイアウォールの設定を確認、サーバの時刻を同期、パワーセービング機能をオフ

各手順は『インストール&設定ガイド』-「第 1 章 システム構成を決定する」-「ハードウェア構成後の設定」を参照してください。

11) CLUSTERPRO のインストール

インストール手順は『インストール&設定ガイド』を参照してください。
インストール完了後、OS の再起動を行ってください。

12) CLUSTERPRO のライセンスを登録

ライセンス登録手順は『インストール&設定ガイド』を参照してください。

5.3 CLUSTERPRO の設定

Cluster WebUI のセットアップ、および接続方法は『インストール&設定ガイド』-「第5章 クラスタ構成情報を作成する」を参照してください。

以下のリソース/監視リソースを追加する手順を記述します。

- ミラーディスクリソース
- Azure プローブポートリソース
- Azure プローブポート監視リソース
- Azure ロードバランス監視リソース
- PING ネットワークパーティション解決リソース(NP 解決用)

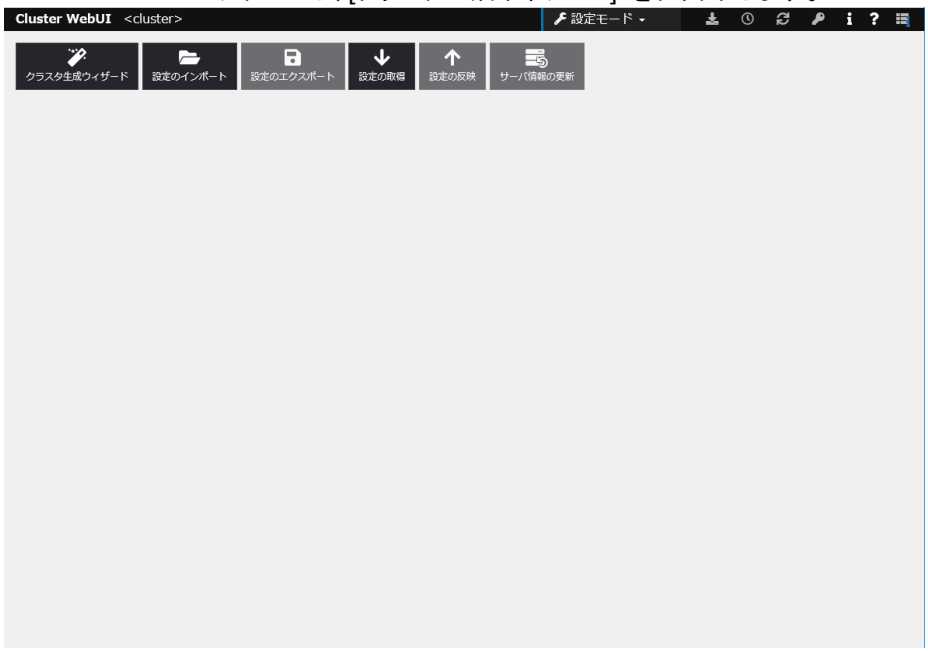
上記以外の設定は、『インストール&設定ガイド』、『リファレンスガイド』を参照してください。

1) クラスタの作成

最初に、クラスタ生成ウィザードを開始し、クラスタを構築します。

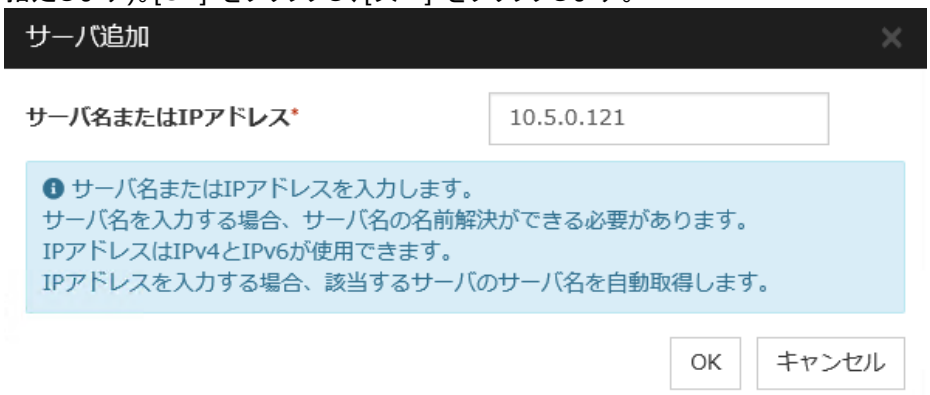
◇ クラスタの構築

1. Cluster WebUI にアクセスし、[クラスタ生成ウィザード] をクリックします。



2. [クラスタ生成ウィザード]画面の[クラスタ] 画面が表示されます。
[クラスタ名] に任意のクラスタ名を入力します。
[言語] を適切に選択します。[次へ] をクリックします。

3. [基本設定] 画面が表示されます。
Cluster WebUI に接続したインスタンスがマスタサーバとして登録済みの状態で表示されます。
[追加] をクリックし、残りのインスタンスを追加します(インスタンスの Private IP アドレスを指定します)。[OK] をクリックし、[次へ] をクリックします。



4. [インタコネクト] 画面が表示されます。
インタコネクトのために使用する IP アドレス(各インスタンスの Private IP アドレス)を指定します。また、後で作成するミラーディスクリソースの通信経路として [MDC] に mdc1 を選択します。[次へ] をクリックします。

5. [NP 解決] 画面が表示されます。
PING 方式の NP 解決を行う場合、[追加] をクリックして [NP 解決一覧] に行を追加します。[種別] 列のセルをクリックし、[Ping] を選択します。Ping ターゲット列のセルをクリックして Ping を送信する対象となる機器の IP アドレスを設定します。IP アドレスは、Microsoft Azure の仮想ネットワーク内部に存在するクラスタサーバ以外のサーバを設定して下さい。各サーバ列のセルをクリックして [使用する] [使用しない] を設定します。[次へ] をクリックします。

2) グループリソースの追加

◇ グループの定義
フェイルオーバグループを作成します。

1. [グループ一覧] 画面が表示されます。
[追加]をクリックします。

2. [グループの定義] 画面が表示されます。
[名前] にフェイルオーバグループ名(failover1)を設定します。[次へ] をクリックします。

3. [起動可能サーバ] 画面が表示されます。
何も指定せず [次へ] をクリックします。
4. [グループ属性] 画面が表示されます。
何も指定せず [次へ] をクリックします。
5. [グループリソース一覧] 画面が表示されます。
以降の手順で、この画面でグループリソースを追加していきます。

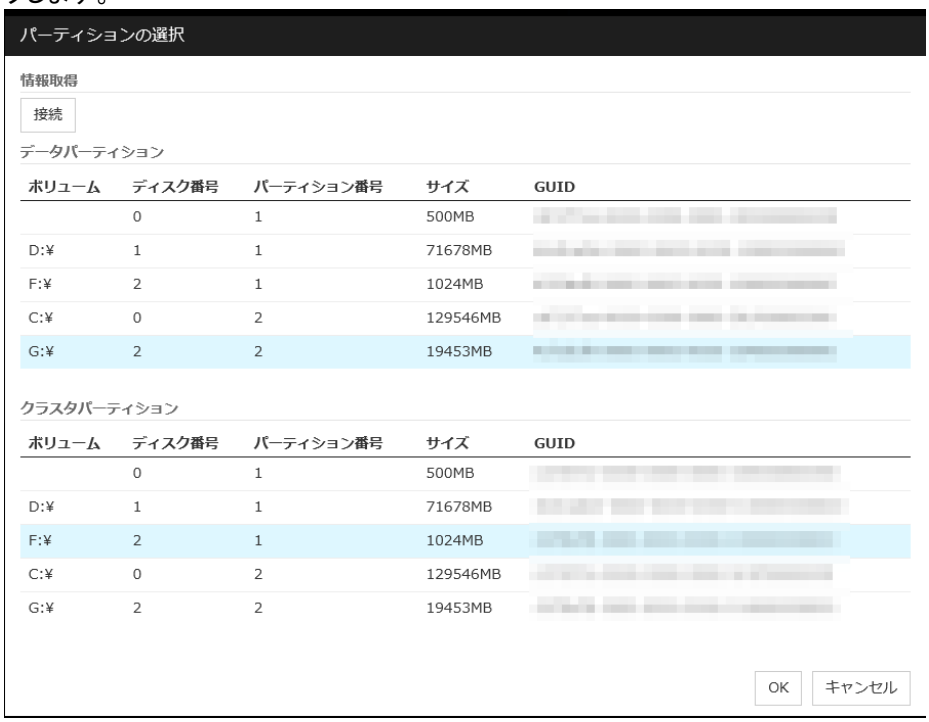
◇ ミラーディスクリソース
ミラーディスクリソースを作成します。
詳細は『リファレンスガイド』-「ミラーディスクリソースを理解する」を参照してください。

1. [グループリソース一覧] で [追加] をクリックします。

2. [グループのリソース定義 | failover1] 画面が開きます。
[タイプ] ボックスでグループリソースのタイプ(ミラーディスクリソース) を選択し、[名前] ボックスにグループ名 (md) を入力します。[次へ] をクリックします。

3. [依存関係] 画面が表示されます。
何も指定せず [次へ] をクリックします。
4. [復旧動作] 画面が表示されます。[次へ] をクリックします。
5. [詳細] 画面が表示されます。
[起動可能サーバ]で[名前]列中のサーバ名を選択し[追加]をクリックします。

6. [パーティションの選択]ダイアログボックスが表示されます。[接続]をクリックし、「5) **仮想マシンの設定**」で作成したデータパーティションと、クラスタパーティションを選択し、[OK]をクリックします。



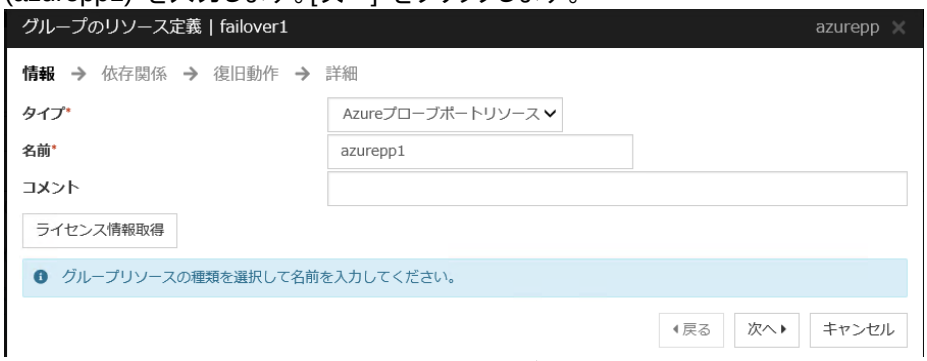
7. node-1について5と6を設定、次に node-2について5と6を設定し、[完了]をクリックします。

◇ Azure プローブポートリソース
Microsoft Azure 上で CLUSTERPRO を利用する場合、業務が稼働するノードの特定のポートでロードバランサーからの死活監視を待ち受ける仕組みを提供します。

Azure プローブポートリソースの詳細は『リファレンスガイド』-「Azure プローブポートリソースを理解する」を参照してください。

1. [グループリソース一覧] で [追加] をクリックします。

2. [グループのリソース定義 | failover1] 画面が開きます。[タイプ] ボックスでグループリソースのタイプ (Azure プローブポートリソース) を選択して、[名前] ボックスにグループ名 (azurepp1) を入力します。[次へ] をクリックします。



3. [依存関係] 画面が表示されます。何も指定せず [次へ] をクリックします。
4. [復旧動作] 画面が表示されます。[次へ] をクリックします。
5. [プローブポート] にロードバランサーの設定(正常性プローブの設定)時に [ポート] として指定した値を入力します。

6. [完了] をクリックします。

◇ スクリプトリソース(DSR を使用する場合)
スクリプトリソースを追加することにより、ロードバランサーの切り替えに合わせて、ループバックアダプタにフロントエンド IP アドレスを追加/削除する仕組みを提供します。

スクリプトリソースの詳細は『リファレンスガイド』-「スクリプトリソースを理解する」を参照してください。

1. [グループリソース一覧] で [追加] をクリックします。
2. [グループのリソース定義 | failover1] 画面が開きます。[タイプ] ボックスでグループリソースのタイプ (スクリプトリソース) を選択して、[名前] ボックスにグループ名 (script1) を入力します。
3. [次へ] をクリックします。
4. [依存関係] 画面が表示されます。何も指定せず [次へ] をクリックします。
5. [復旧動作] 画面が表示されます。[次へ] をクリックします。
6. start.bat、stop.bat を選択し、[編集] をクリックします。スクリプトは CLUSTERPRO オフィシャルブログ(https://jpn.nec.com/clusterpro/blog/20181031.html)を参考に設定してください。CLUSTERPRO オフィシャルブログに掲載のスクリプトはサンプルです。環境に合わせてカスタマイズしてください。
7. [完了] をクリックします。

3) 監視リソースの追加

◇ Azure プローブポート監視リソース
Microsoft Azure プローブポートリソースが起動しているノードに対して、死活監視のためのポートの監視機構を提供します。

Azure プローブポート監視リソースの詳細は『リファレンスガイド』-「Azure プローブポート監視リソースを理解する」を参照してください。

Azure プローブポートリソースを1つ追加すると、Azure プローブポート監視リソースが1つ自動的に作成されます。

◇ Azure ロードバランス監視リソース
Microsoft Azure プローブポートリソースが起動していないノードに対して、プローブポートと同じポート番号が開放されていないかの監視機構を提供します。

Azure ロードバランス監視リソースの詳細は『リファレンスガイド』-「Azure ロードバランス監視リソースを理解する」を参照してください。

Azure プローブポートリソースを1つ追加すると、Azure ロードバランス監視リソースが1つ自動的に作成されます。

4) 設定の反映とクラスタの起動

1. Cluster WebUI の設定モード から、[設定の反映] をクリックします。
   [設定を反映しますか。] というポップアップメッセージが表示されますので、[OK] をクリックします。
   アップロードに成功すると、[反映に成功しました。] のメッセージが表示されますので、[OK] をクリックします。
   アップロードに失敗した場合は、表示されるメッセージに従って操作を行ってください。
2. Cluster WebUI の ツールバーのドロップダウンメニューで [操作モード] を選択して、操作モードに切り替えます。
3. Cluster WebUI の[ステータス] タブから [クラスタ開始] をクリックし、確認画面で [開始] をクリックします。

詳細は『インストール&設定ガイド』-「クラスタを生成するには」を参照してください。

5.4 動作確認

構築した環境が正常に動作するかを、監視異常(擬似)を発生させフェイルオーバグループがフェイルオーバすることにより確認します。
既にクラスタが正常に起動している状態からの確認手順は以下のとおりです。

1. フェイルオーバグループ(failover1)が、現用系ノードの node-1で起動します。Cluster WebUI [ステータス]タブにおいて failover1が node-1で[起動済]になっていることを確認します。
   DSR を使用する場合は、パケットキャプチャを実施し、クライアントの IP アドレスとロードバランサーのフロントエンド IP アドレスで通信が行われていることもあわせて確認します。
2. Cluster WebUI のプルダウンより[操作モード]から[検証モード]に変更します。
3. Cluster WebUI [ステータス]タブにおいて azureppw1の [擬似障害発生]アイコンを選択します。
4. Azure プローブポートリソース(azurepp1)が3回再活性後に、フェイルオーバグループ(failover1)が異常になり、ノード node-2へフェイルオーバします。Cluster WebUI [ステータス]タブにおいて failover1が node-2で[起動済]になっていることを確認します。
   また、Azure ロードバランサーのフロントエンド IP、ポートに対してフェイルオーバ後も正常にアクセスできることを確認します。
   DSR を使用する場合は、パケットキャプチャを実施し、クライアントの IP アドレスとロードバランサーのフロントエンド IP アドレスで通信が行われていることもあわせて確認します。

以上で、擬似障害の場合におけるフェイルオーバの動作確認は完了です。その他の障害発生時の動作確認については適宜実施してください。

DSR 構成を作成する場合は以下を参照してください。
https://jpn.nec.com/clusterpro/blog/20181031.html

第 6 章　エラーメッセージ一覧

各リソース/モニタリソースのエラーメッセージについては、以下のマニュアルを参照してください。

- 『リファレンスガイド』-「第 9 章 エラーメッセージ一覧」

第 7 章　注意・制限事項

7.1 Azure DNS を使用した HA クラスタの場合

7.1.1 Microsoft Azure の注意事項

- マルチテナントのクラウド環境では、物理環境や一般的な仮想化環境(非クラウド環境)に比べて性能の差が大きくなる(性能の劣化率が大きくなる)傾向があります。性能を重視するシステムでは、設計フェーズにおいて、この点に留意する必要があります。
- 仮想マシンをシャットダウンしただけでは、仮想マシンの状態は[停止済み]となり課金状態が継続されます。Microsoft Azureポータルの仮想マシンの設定画面の[停止]を実行し、仮想マシンの状態を[停止済み(割り当て解除済み)]にしてください。
- 可用性セットは、仮想マシンの作成時にのみ設定できます。 可用性セットの内外に仮想マシンを移動するには、仮想マシンを再作成する必要があります。
- CLUSTERPROがMicrosoft Azureと連携するためには、Microsoft Azureの組織アカウントが必要となります。組織アカウント以外のアカウントはAzure CLI実行時に対話形式でのログインが必要となるため使用できません。

7.1.2 CLUSTERPRO の注意事項

以下のマニュアルを参照してください。
- 『スタートアップガイド』-「第 5 章 注意制限事項」-「CLUSTERPRO インストール前」-「通信ポート番号」
- 『スタートアップガイド』-「第 5 章 注意制限事項」-「CLUSTERPRO インストール前」-「Azure DNS リソースについて」
- 『スタートアップガイド』-「第 5 章 注意制限事項」-「CLUSTERPRO の構成情報作成時」-「Azure DNS リソースの設定について」
- 『リファレンスガイド』-「Azure DNS リソースに関する注意事項」
- 『リファレンスガイド』-「Azure DNS 監視リソースの注意事項」

Azure のメモリ保持メンテナンスにより、仮想マシンは最大で 30 秒間一時停止状態になる場合があります。
メモリ保持メンテナンスについての詳細は以下を参照してください。
https://docs.microsoft.com/ja-jp/azure/virtual-machines/windows/maintenance-and-updates
[クラスタプロパティ]-[タイムアウト]タブ-[ハートビートタイムアウト]はメモリ保持メンテナンスを考慮した値を設定してください。
また、[ハートビートタイムアウト]と併せて以下も調整してください。
- OS の起動時間は[ハートビートタイムアウト]より長くなるよう調整してください。

以下のマニュアルも参照してください。
- 『リファレンスガイド』-「クラスタプロパティ」-「タイムアウトタブ」
- 『スタートアップガイド』-「第 5 章 注意制限事項」-「CLUSTERPRO インストール前」-「OS 起動時間の調整」

7.2 ロードバランサーを使用した HA クラスタの場合

7.2.1 Microsoft Azure の注意事項

- マルチテナントのクラウド環境では、物理環境や一般的な仮想化環境(非クラウド環境)に比べて性能の差が大きくなる(性能の劣化率が大きくなる)傾向があります。性能を重視するシステムでは、設計フェーズにおいて、この点に留意する必要があります。
- 仮想マシンをシャットダウンしただけでは、仮想マシンの状態は[停止済み]となり課金状態が継続されます。Microsoft Azureポータルの仮想マシンの設定画面の[停止]を実行し、仮想マシンの状態を[停止済み(割り当て解除済み)]にしてください。
- 可用性セットは、仮想マシンの作成時にのみ設定できます。 可用性セットの内外に仮想マシンを移動するには、仮想マシンを再作成する必要があります。

7.2.2 CLUSTERPRO の注意事項

以下のマニュアルを参照してください。
- 『スタートアップガイド』-「第 5 章 注意制限事項」-「CLUSTERPRO インストール前」-「通信ポート番号」
- 『スタートアップガイド』-「第 5 章 注意制限事項」-「CLUSTERPRO インストール前」-「Azure プローブポートリソースについて」
- 『スタートアップガイド』-「第 5 章 注意制限事項」-「CLUSTERPRO の構成情報作成時」-「Azure プローブポートリソースの設定について」
- 『スタートアップガイド』-「第 5 章 注意制限事項」-「CLUSTERPRO の構成情報作成時」-「Azure ロードバランス監視リソースの設定について」
- 『リファレンスガイド』-「Azure プローブポートリソースに関する注意事項」
- 『リファレンスガイド』-「Azure プローブポート監視リソースの注意事項」
- 『リファレンスガイド』-「Azure ロードバランス監視リソースの注意事項」

Azure のメモリ保持メンテナンスにより、仮想マシンは最大で 30 秒間一時停止状態になる場合があります。
メモリ保持メンテナンスについての詳細は以下を参照してください。
https://docs.microsoft.com/ja-jp/azure/virtual-machines/windows/maintenance-and-updates
[クラスタプロパティ]-[タイムアウト]タブ-[ハートビートタイムアウト]はメモリ保持メンテナンスを考慮した値を設定してください。
また、[ハートビートタイムアウト]と併せて以下も調整してください。
- OS の起動時間は[ハートビートタイムアウト]より長くなるよう調整してください。

以下のマニュアルも参照してください。
- 『リファレンスガイド』-「クラスタプロパティ」-「タイムアウトタブ」
- 『スタートアップガイド』-「第 5 章 注意制限事項」-「CLUSTERPRO インストール前」-「OS 起動時間の調整」