文書番号： LK20230216-351-001

LifeKeeper for Windows

QWK Storage モード
ステップバイステップ構築ガイド
【Azure 編】

第 1 版

サイオステクノロジー株式会社

目次

改訂履歴

版	更新日	変更情報
第 1 版	2023/09/10	新規作成

1. はじめに

本ドキュメントに含まれる情報は、公表の日付におけるサイオステクノロジー株式会社の考え方に基づいています。サイオステクノロジー株式会社は記載されている内容をお約束しているわけではありません。また、それらの内容を保証するものでもありません。本ドキュメントは情報提供のみを目的としています。また、記載内容は予告無く変更する場合があります。予めご了承ください。

2. 本ドキュメントについて

本ガイドは、Azure IaaS を基盤とした Windows Server 環境でスプリットブレインの問題を解決する目的で、LifeKeeper for Windows と Quorum Witness Server Support Package for Windows（QWK）の Storage モードを組み合わせる場合の、推奨インフラストラクチャと設定手順を解説します。

ガイドは二部構成になっており、前半では Azure Portal を利用したインフラストラクチャの構築手順、後半ではその構築された環境を用いて、LifeKeeper と DataKeeper でクラスタを形成する手順について説明します。

3. Azure

本章は Azure と Azure Iaas の概要を紹介します。

3.1. Azure の概要

Azure は、Microsoft が提供するクラウドコンピューティングプラットフォームです。世界中のデータセンターで運用されていて世界各地のデータセンターに、仮想マシンやストレージなど、リソースと呼ばれるものを適切に配置することで、Azure 上で稼働するサービスの可用性を高めることができます。

アプリケーションやサービスの開発、実行、管理を支援するための機能を提供しています。Azure を利用することで、ユーザは物理的なサーバを所有することなく、コンピューティングリソース、ストレージ、データベース、ネットワークなどのサービスを利用することができます。

Azure のデータセンターは「ジオ」「リージョン」「リージョンペア」「可用性ゾーン 」という概念でグループ化されています。

ジオ (Geos)

「ジオ」とは、Azure における地理的リージョンのことを指します。
Azure は、世界中に存在する複数のデータセンターによって構成されており、それぞれが異なるジオに位置しています。

リージョン

「リージョン」とは、Azure における地理的な区分のことを指します。各ジオは、複数のリージョンに分割されています。
例えば、「日本」ジオは、東京リージョンと大阪リージョンの 2 つのリージョンがあります。リージョンは、データセンターをより細かく分割することで、より高い可用性を実現するために使用されます。

リージョンペア

「リージョンペア」とは、Azure において、特定のジオ内に存在する 2 つのリージョンを組み合わせたものを指します。
リージョンペアは、主に災害対策の観点から利用されます。1 つのリージョンが災害などで利用不能になった場合でも、もう 1 つのリージョンにデータやアプリケーションをフェイルオーバーすることができます。

可用性ゾーン

「可用性ゾーン」とは、Azure におけるデータセンター内の論理的な区分のことを指します。各リージョンは、複数の可用性ゾーンに分割されています。可用性ゾーンは、物理的に独立した電源、ネットワーク、冷却システムなどを備え、異なる可用性ゾーンに配置されたリソースは、単一障害点を排除し、高い可用性を実現することができます。

3.2. Azure Iaas の概要

Azure IaaS（Infrastructure as a Service）は、Azure におけるクラウドコンピューティングサービスの一つで、物理的なサーバやネットワーク機器などのインフラストラクチャをクラウド上で提供します。

具体的には、Azure IaaS では、仮想マシンやストレージ、ネットワーク、セキュリティ、バックアップ、復元などの機能を提供しています。これにより、ユーザは物理的なサーバを購入、設定、保守する必要がなく、必要なコンピューティングリソースを迅速かつ効率的に利用することができます。

Azure IaaS の主な機能をリソースとして提供されています。

仮想マシン

Windows や Linux などのオペレーティングシステムを実行するための仮想マシンを提供しています。

ストレージ

ファイルやデータの保存、バックアップ、復元を行うためのストレージを提供しています。

ネットワーク

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などを提供し、安全なネットワーク環境を構築することができます。

4. QWK によるスプリットブレイン対策

本節は最初にスプリットブレインについて紹介します。
次に、QWK の概要を紹介し、QWK を使用してスプリットブレインを回避する方法を説明します。
最後に、本ガイドで使用している QWK の Storage モードの概要を紹介します。

4.1. スプリットブレインとは

スプリットブレイン（Split Brain）とは、クラスタノード間の通信が切断され、互いに隔離された状態を指します。
スプリットブレインが発生すると、各ノードは自身が唯一の有効なノードであると認識し、リソースを起動しようとします。

スプリットブレインが起きると、クラスタ内のリソースの整合性やデータの一貫性を損なう可能性があります。そのため、スプリットブレインが発生した場合は、速やかに対処する必要があります。

4.2. QWK によるスプリットブレイン対策

QWK は、ネットワーク全体にわたる障害の恐れがある環境において、より高い信頼性でシステムフェイルオーバーを実行するための機能です。

QWK を使用すると、スプリットブレインの発生リスクを軽減しながら、ローカルサイトのフェイルオーバーと WAN を介したノードへのフェイルオーバーを適切に実行できます。

QWK は、以下の二つの主要なチェックで構成されます。
・Quorum チェック: ノード障害を検知した際、全ノード間で多数決によってフェイルオーバー先を決定します。
・Witness チェック: 第三者サーバに問い合わせ、相手ノードの死活状態を再確認します。

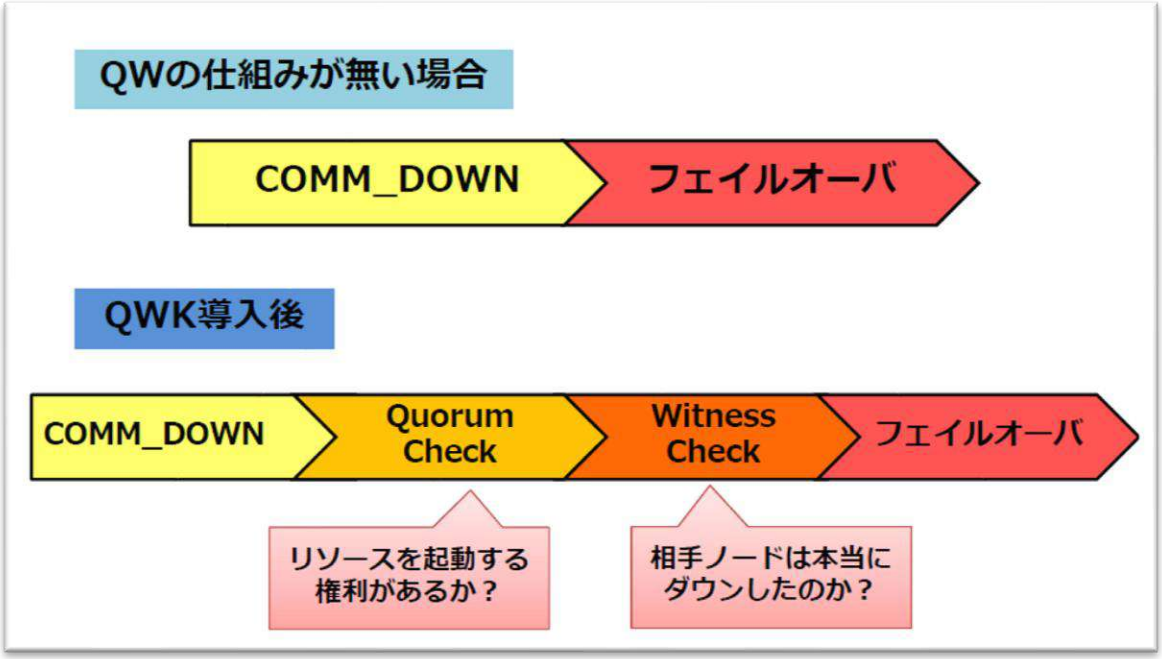


図 4.2 QWK の導入によるチェック

4.3. QWK の Storage モードの概要

「Quorum チェック」には、「Majority モード」「Storage モード」の 2 つのモードが用意されています。

本ガイドでは Storage モードを使用します。
Storage モードは、共有ストレージを Witness デバイスとして利用する Quorum の一形態です。このモードでは、全ノードがアクセス可能な共有ストレージを用いて情報交換を行います。

（1） 基本概念

共有ストレージ: クラスタ内の全ノードがアクセス可能なデータストレージ。
QWK オブジェクト: 各ノードがこの共有ストレージに書き込む、特定の情報を格納するオブジェクト。クラスタを構成するノード分だけこのオブジェクトが必要です。

（2） 動作メカニズム

先に Quorum チェックが行われます。各ノードが定期的に共有ストレージに QWK

オブジェクトとして自身の情報を書き込みます。
次に Witness チェックが行われます。各ノードは、他のノードが書き込んだ QWK オブジェクトを定期的に読み取り、更新されていることをチェックします。
両方のチェックが成功すると、クラスタは正常に動作していると判断されます。

※具体的な障害シナリオについては、テクニカルドキュメンテーションを参照してください。
Storage モード
→シナリオ 1 からシナリオ 3

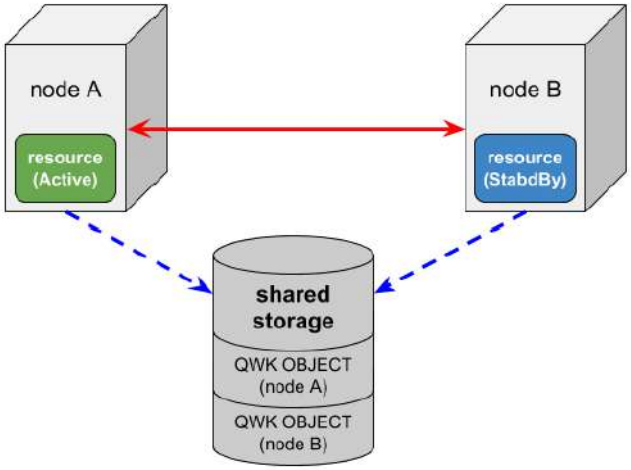


図 4.3 Storage Quorum の標準構成

5. Azure Iaas で環境構築

本章では、Azure Portal を使用して環境を構築する際の必要な設定について説明します。

5.1. 本ガイドの環境構成

本ガイドでは「日本」ジオ、「東日本」リージョンという環境構成になります。

Azure でのシステム構成図は以下のようになります。

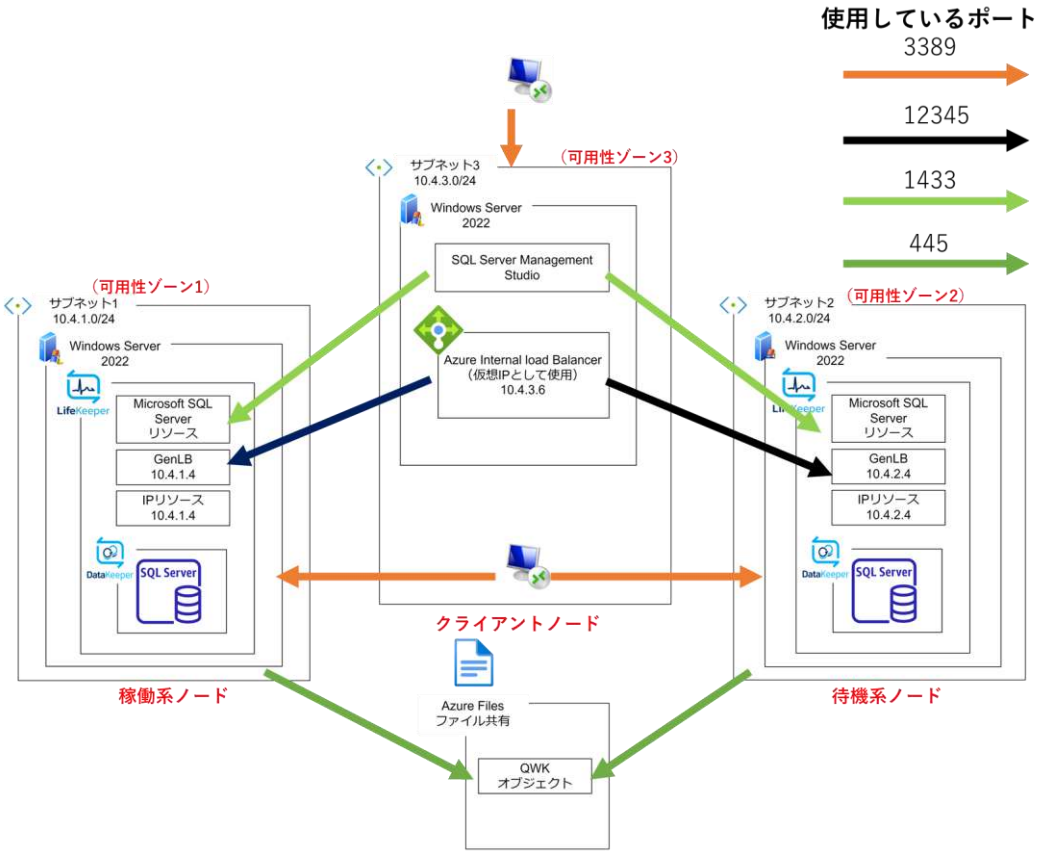


図 **エラー! 指定したスタイルは使われていません。** 本ガイドのシステム構成

5.2. リソースとは

Azure で扱う「リソース」とは、物理的または仮想的な構成要素のことを指します。例としては、仮想マシン（VM）、ネットワークインターフェース、仮想ネットワーク（VNET）などがあります。

5.3. 仮想マシンの利用に必要なリソース

Azure 上でアプリケーションやサービスを実行するためには、通常、仮想マシン（VM）が必要です。ただし、VM を単独で使用せず、VM と一緒に使用するための仮想ネットワーク（VNET）も必要です。

必要なリソースを下記の表にまとめました。

表 5.3　リソース一覧

種類	リソース	説明
仮想ネットワーク（VNET）	仮想ネットワーク	仮想マシン間で通信するための仮想的なネットワーク環境
	サブネット	仮想ネットワーク内で IP アドレスの範囲を制限し、仮想マシンを特定のグループに分けるための仮想的なネットワーク区分
	ネットワークセキュリティグループ（NSG）	サブネットに適用され、特定のトラフィックのフィルタリングや制御ができるファイアウォールルール
仮想マシン（VM）	仮想マシン	オペレーティングシステム（Windows、Linux 等）を実行するための仮想化されたコンピュータ
	ディスク	仮想マシンにアタッチすることでデータを保存する仮想的なストレージデバイス
	ネットワークインターフェース（NIC）	仮想マシンと仮想ネットワークを接続する仮想的なネットワークインターフェース
	パブリック IP アドレス	インターネットから仮想マシンにアクセスする際に必要な外部 IP アドレス
	ネットワークセキュリティグループ（NSG）	仮想マシンに対して、特定のトラフィックのフィルタリングや制御ができるファイアウォールルール

5.4. リソースグループの作成

本節では、Azure 上の複数のリソースを一元管理するための「リソースグループ」の作成方法について説明します。

5.4.1. リソースグループとサブスクリプション

ソースグループの作成と管理には、Azure サブスクリプションが必要です。サブスクリプションとは、Microsoft Azure のサービスやリソースの利用料金を計算し、アクセス制御を行う単位です。

サブスクリプション内で、各種リソースをまとめて管理するための「リソースグループ」を作成します。

リソースグループは、Azure で利用する各種リソースを論理的にグループ化して管理するためのコンテナです。一つのリソースグループ内で、仮想マシン、仮想ネットワーク、データベースなど、複数のリソースを一括で管理できる利点があります。

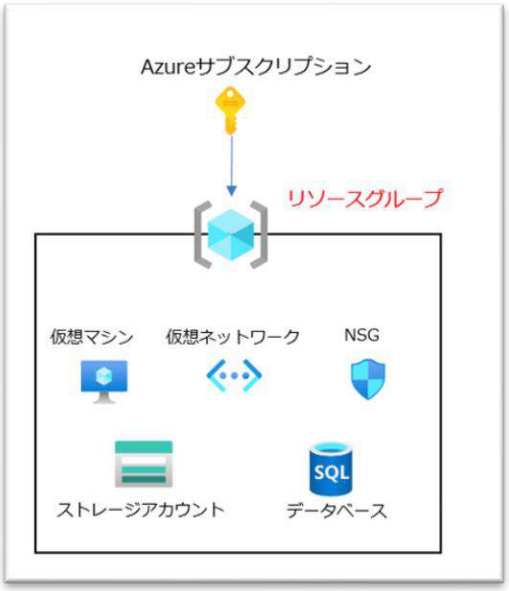


図 5.4.1 リソースグループの概念図

5.4.2. Azure Marketplace へのアクセス

この節では、Azure Marketplace を通じてリソースグループを作成する手順について説明します。

（1） Azure ポータルへのサインイン

Azure ポータルにサインインします。

サインイン後、ポータル画面の左上にある「リソース作成」ボタンをクリックして、Azure Marketplace を開きます。

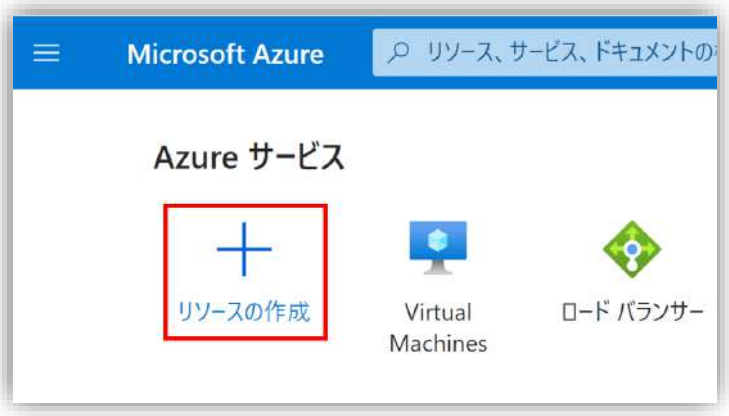


図 5.4.2-1 リソースの作成

（2） リソースグループの作成

Azure Marketplace 内の検索ボックスに「リソースグループ」と入力して検索を行います。

「リソース グループ」（開発元：Microsoft）を選択し、次に表示されるページで「作成」ボタンをクリックします。

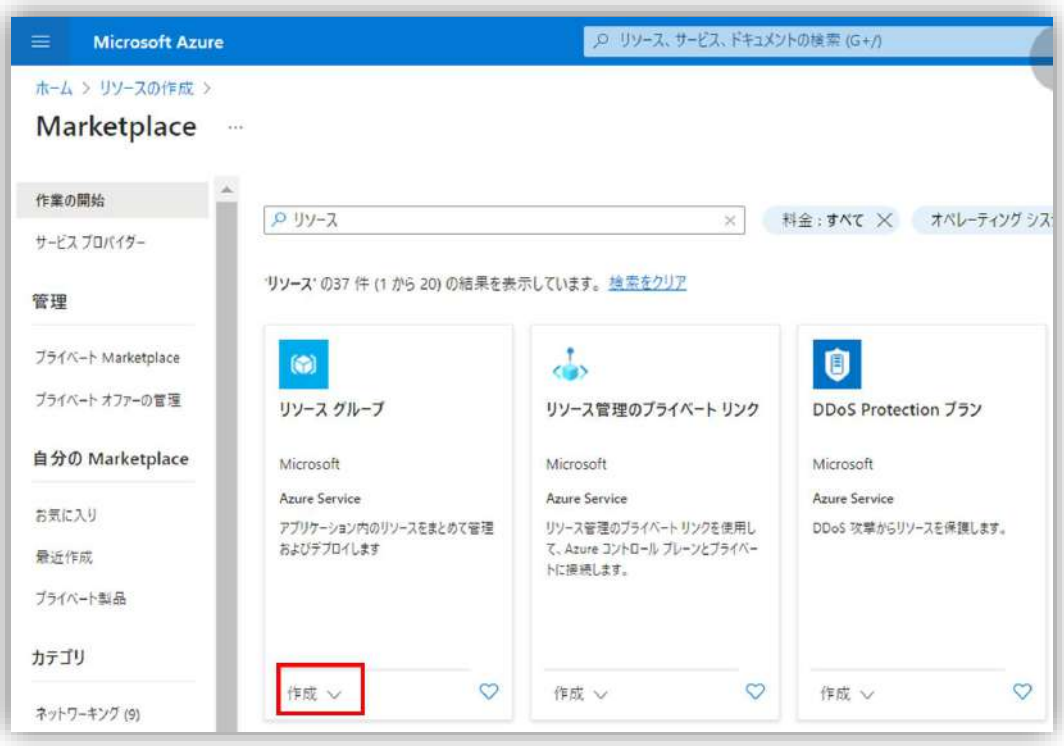


図 5.4.2-2 リソースグループの新規作成

5.4.3. 基本情報の入力

サブスクリプション、リソースグループの名前、およびリージョンを選択した後、「次：タグ」ボタンをクリックします。

図 5.4.3-1 基本情報の入力

設定項目とその対応する値は以下のようになります。

表 5.4.3 設定項目一覧

タブ	設定項目	値	説明
基本	サブスクリプション	<サブスクリプションの名前>	リソースグループを作成するためのサブスクリプション
	リソースグループ	LKW-QWK-Storage	このリソースグループに割り当てる名前
	リージョン	（Asia Pacific）東日本	リソースグループの設定が保存されるリージョン

5.4.4. タグの入力

リソースグループのタグ（キーと値）を設定します。

必須の入力項目を入力し、「次：確認及び作成」をクリックします。

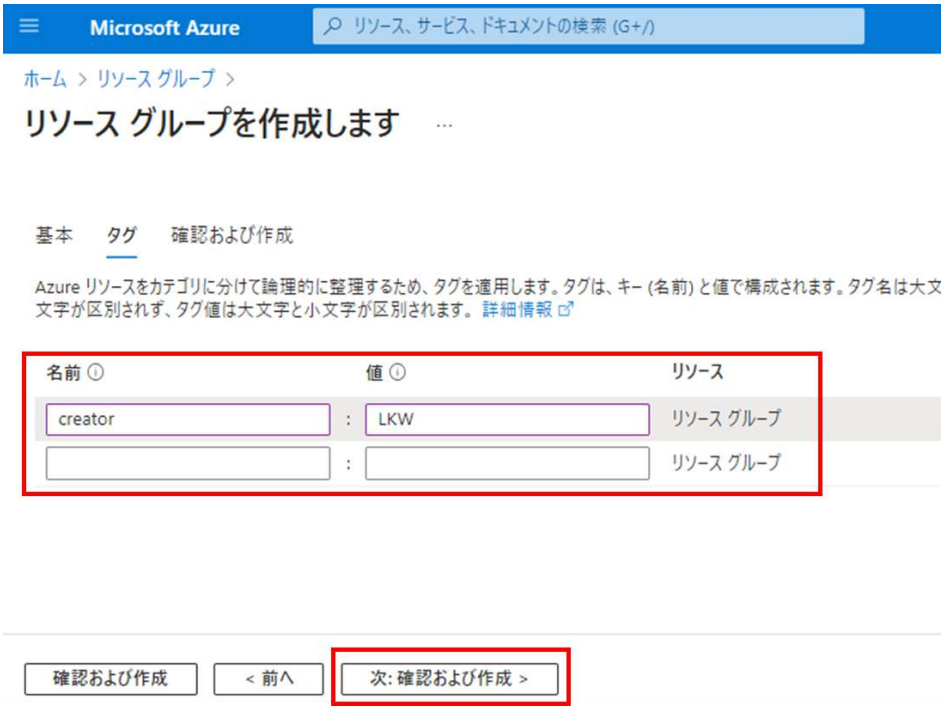


図 5.4.4 タグ設定画面

5.4.5. 入力項目の確認およびリソースグループの作成

入力した情報を確認し、必要に応じて修正します。

問題がなければ、「作成」をクリックします。

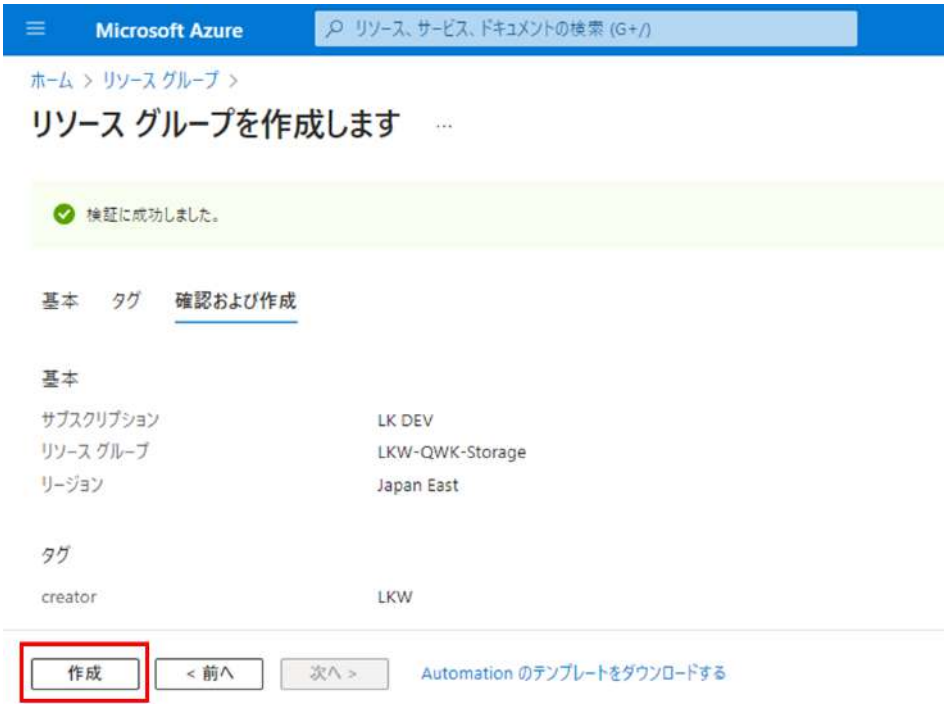


図 5.4.4 リソースグループの確認および作成画面

5.5. 仮想ネットワーク リソースの作成

この章では、Azure での仮想ネットワーク（VNET）とサブネットの作成手順をガイドします。VNET は仮想マシン（VM）が通信するためのネットワーク基盤となります。

5.5.1. 仮想ネットワークの作成

（1） 仮想ネットワークの作成画面にアクセス

Azure ポータルの検索ボックスで「仮想ネットワーク」と入力し、「仮想ネットワーク」を選択します。

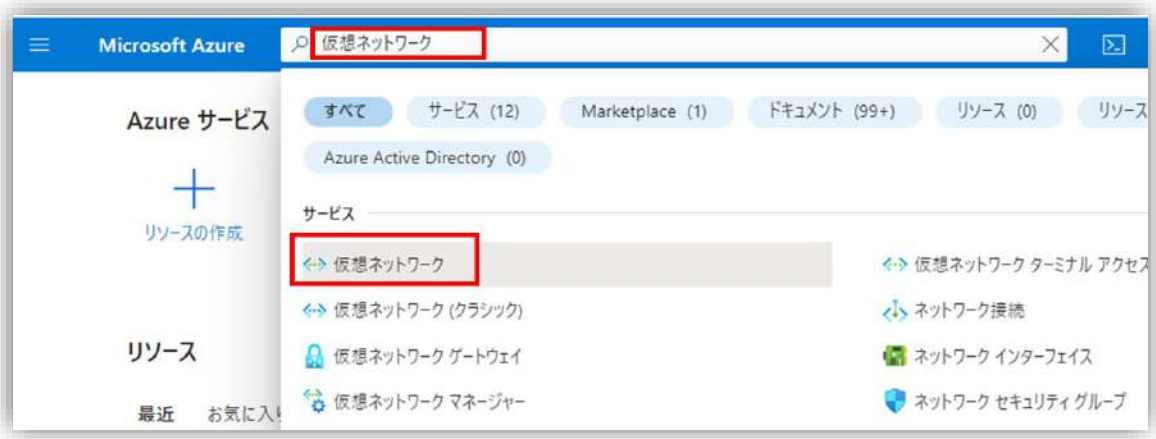


図 5.5.1-1 仮想ネットワークの検索画面

「作成」ボタンをクリックし、新しい仮想ネットワークの設定画面に進みます。

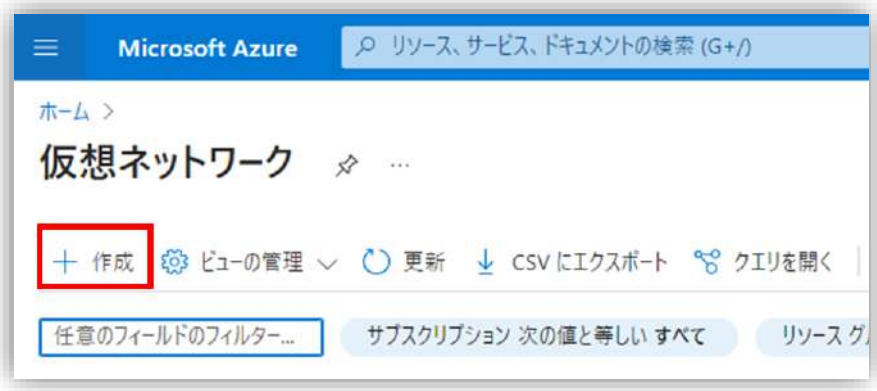


図 5.5.1-2 仮想ネットワークの作成

（2） 基本情報の入力

ここでは仮想ネットワークの基本的な設定を行います。

サブスクリプション、リソースグループの名前、および地域を選択します。

図 5.5.1-3 仮想ネットワークの基本設定

入力が完了したら、「次：IP アドレス」をクリックします。

設定項目と値は以下の表になります。

表 5.5.1 設定項目一覧

タブ	入力項目	値	説明
基本	サブスクリプション	<サブスクリプション名>	使用するサブスクリプション名
	リソースグループ	LKW-QWK-Storage	先ほど作成したリソースグループ
	名前	LKW-QWK-Storage-Vnet	仮想ネットワークに付ける名前
	地域	（Asia Pacific）東日本	仮想ネットワークを設置する地域

（3） IP アドレスの設定

こちらで、仮想ネットワークの IP アドレス範囲とサブネットを設定します。CIDR 形式で入力します。

表 5.5.2 設定項目一覧

タブ	入力項目	値	説明
IP アドレス	IPv4 アドレス空間	10.4.0.0/16	アドレス空間（CIDR 形式）
	サブネットとサブネット範囲	LKW-QWK-Storage-Subnet1：10.4.1.0/24 LKW-QWK-Storage-Subnet2：10.4.2.0/24 LKW-QWK-Storage-Subnet3：10.4.3.0/24	サブネットの範囲（CIDR 形式）

「サブネット追加」ボタンをクリックして、サブネット名とサブネット範囲を入力します。入力が完了したら「追加」ボタンをクリックして、サブネットを追加してください。

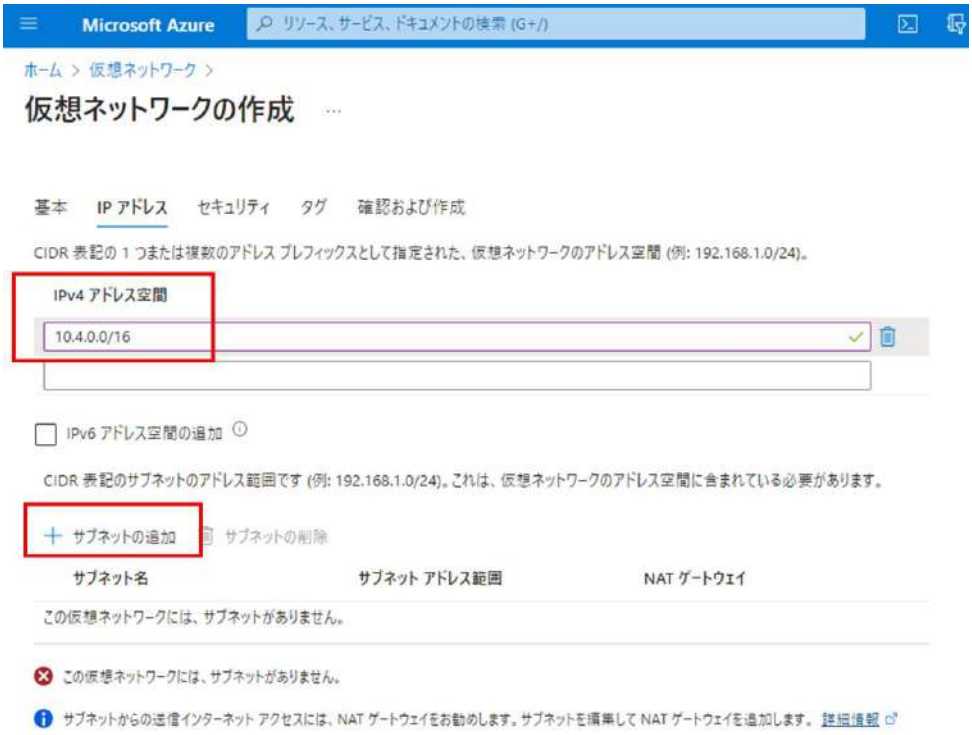


図 5.5.1-4 IPv4 アドレス空間の追加

図 5.5.1-5 サブネットの追加

（4） 設定の確認

設定した IPv4 アドレス空間とサブネットを確認し、「次：セキュリティ」ボタンをクリックして、次の手順に進んでください。

図 5.5.1-6 仮想ネットワークの IPv4 アドレス空間とサブネットを確認

（5） 確認および作成

すべての設定が完了したら、各項目の設定値を確認して「作成」をクリックします。デプロイが開始されます。

デプロイが完了すると、「デプロイが完了しました」と表示されます。

図 5.5.1-7 仮想ネットワークの作成

図 5.5.2-4 仮想ネットワークの設定完了

5.6. マネージドディスクの作成

本節では、SQL Server のデータベースファイルを保存するために使用する、Azure でのマネージドディスクの作成手順を説明します。

（1） マネージドディスクの作成画面にアクセス

Azure ポータルの検索ボックスに「ディスク」と入力して検索します。

検索結果から「ディスク」を選択し、マネージドディスクの管理画面を開きます。

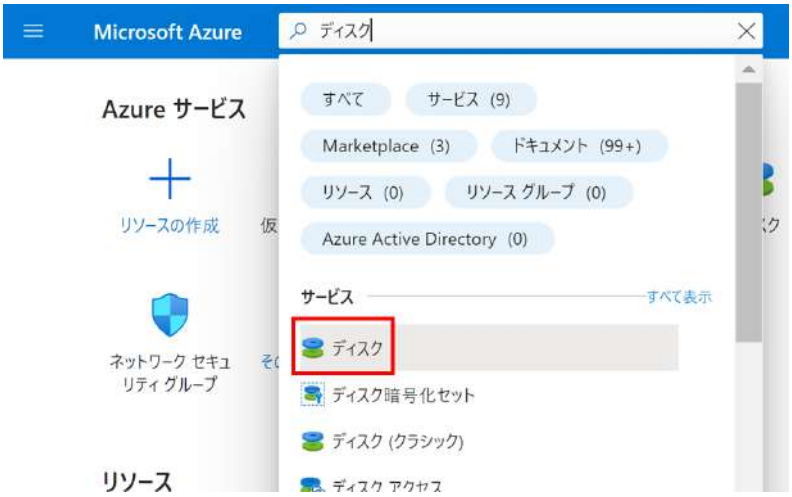


図 5.6-1 マネジッドディスクの管理画面にアクセス

（2） マネジッドディスクの作成

管理画面の右上隅にある「作成」ボタンをクリックしま、新しいマネージドディスクの設定画面が開きます。

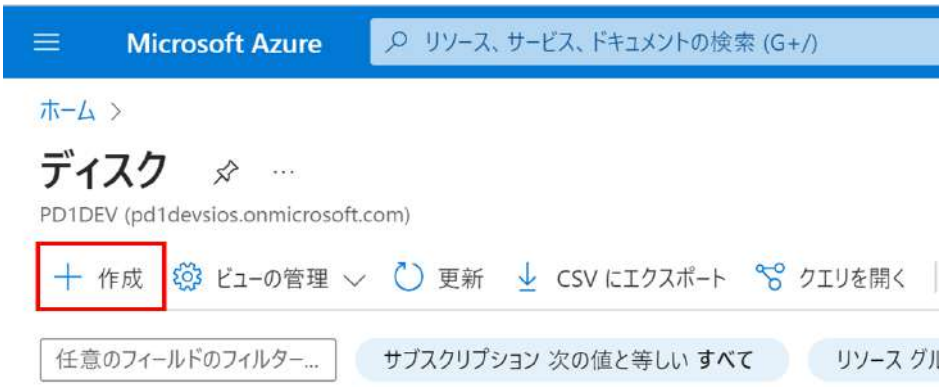


図 5.6-2 マネジッドディスクの新規作成

（3） 基本情報の入力

「サブスクリプション」、「リソースグループ」、「ディスク名」、「地域」を選択します。「可用性ゾーン」で「インフラストラクチャ冗長は必要ありません」を選択します。

必要なフィールドが全て入力されたら、「サイズの変更」をクリックします。

図 5.6-3 基本情報の入力

（4） ストレージ種類とディスクサイズの設定

「ストレージの種類」から「Premium SSD」を選びます。

この設定はデータが 3 つの異なるゾーンにレプリケートされるため、可用性が高いです。

「カスタム ディスク サイズ（GiB）」フィールドに「8」を入力します。 設定が完了したら「OK」をクリックします。

図 5.6-4 ストレージ種類の選択

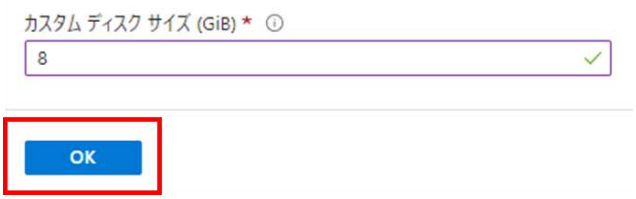


図 5.6-5 ディスクサイズの設定

作成したディスクのサイズと種類を確認します。

確認出来たら、タブにある「詳細」をクリックします。

図 5.6-6 作成したディスクのパラメータの確認

（5） 共有ディスク設定

「共有ディスクを有効にする」のチェックボックスにチェックを入れます。

「最大共有数」フィールドに「2」を入力します。

設定が完了したら、「確認および作成」をクリックします。

図 5.6-7 共有ディスクの有効化と最大共有数の設定

（6） 確認および作成

全ての設定項目を確認します。設定に問題がなければ、「作成」をクリックします。ディスクの作成が開始されます。

「デプロイが完了しました」と表示されれば、マネージドディスクの作成は成功です。

図 5.6-8 ディスクの確認および作成

図 5.6-9 ディスクの作成完了

5.7. 仮想マシンの作成

本節では、Azure で仮想マシンを作成する手順を詳細に説明します。

必要なリソース（CPU、メモリ、ディスクなど）の選定から、ネットワークやストレージの設定まで順を追って解説します。

最初に稼働系ノードが使用する仮想マシンを作成します。

5.7.1. 仮想マシンの作成画面へのアクセス

Azure ポータルの検索ボックスに「Virtual Machines」と入力して検索します。

「Virtual Machines」をクリックし、仮想マシン管理画面が表示されると、「作成」ボタンをクリックします。

「Azure 仮想マシン」オプションを選択し、作成を開始します。

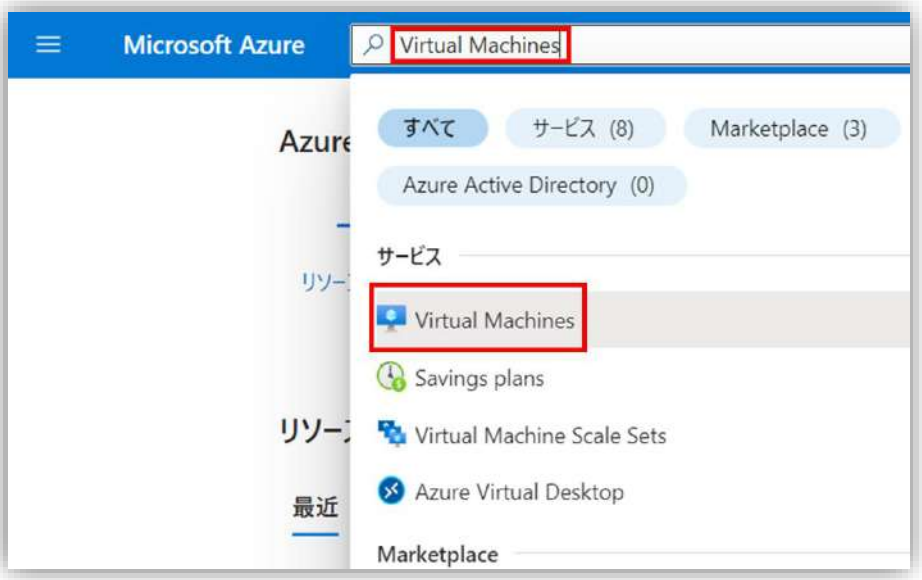


図 5.7.1-1 Azure ポータルから仮想マシンの作成画面にアクセス

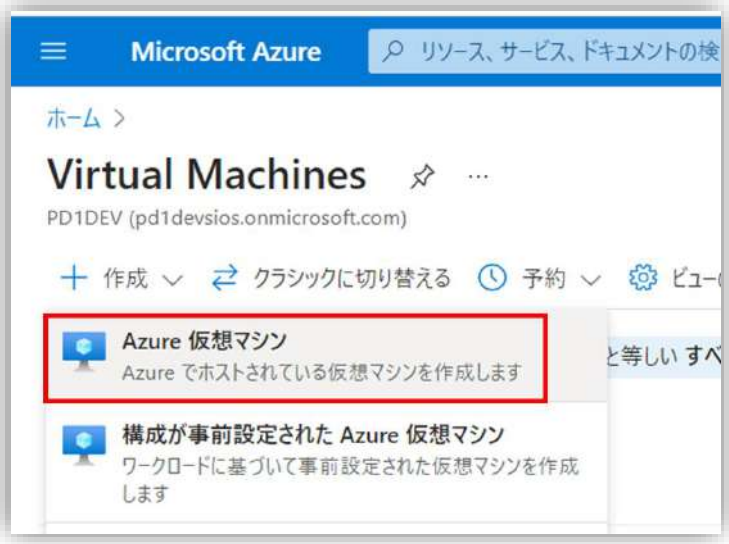


図 5.7.1-2 仮想マシンを作成

5.7.2. 基本情報の入力

（1）基本情報の入力

「基本」タブの設定情報を入力します。

「サブスクリプション」、「リソースグループ」、「ディスク名」、「地域」を入力します。

図 5.7.2-1 設定情報の入力

（1） 可用性に関する設定

次に、Azure の可用性ゾーンについて設定します。

可用性ゾーンは物理的に分離されたデータセンター群であり、一つのゾーンで障害が発生しても他のゾーンは影響を受けません。

ここで、稼働系ノードを「Zone1」に配置し、「セキュリティの種類」は「Standard」に設定します。

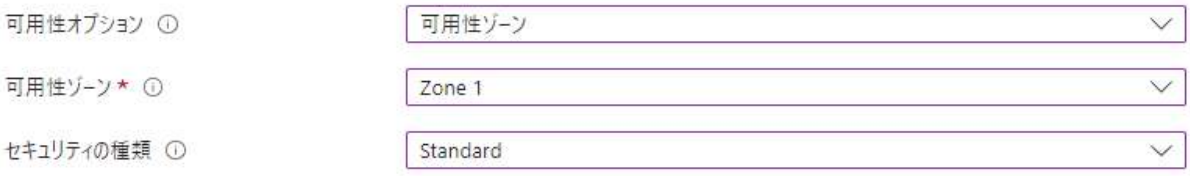


図 5.7.2- 2 可用性に関する設定

（2） OS の設定

本ガイドでは、OS に「Windows Server 2022 Datacenter」を使用します。

そのため、「イメージ」選択欄の下の「すべてのイメージを表示」をクリックして選択します。

仮想マシンのサイズは「Standard_B2s」を選択します。

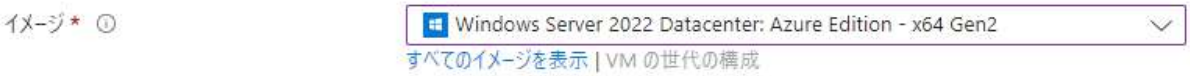


図 5.6.2-3 OS イメージの設定

図 5.7.2-4 OS サイズの選択

（3） ログイン情報設定

仮想マシンへのログインに使用するユーザ名とパスワードを設定します。

図 5.7.2-5 仮想マシンの管理者アカウントの設定

（4） ポート設定

クライアントノードがパブリックネットワークに接続する設定を行います。

リモートデスクトップ（RDP）を用いて仮想マシンにログインします。

そのため、「パブリック受信ポート」の設定を「選択したポートを許可する」にし、

そして RDP 用の「3389」ポートだけを許可します。

図 5.7.2-6 ポートの設定

設定完了したら、「次：ディスク」 をクリックします。

図 5.7.2-7 設定完了

5.7.3. ディスクの作成

ディスクの作成を行います。

（1） OS ディスクの種類の選択

本ガイドは OS ディスクとして、 「Standard SSD」を使用します。

「OS ディスクの種類」で、 「Standard SSD」を選択します。

図 5.7.3-1 OS ディスクの種類の選択

「VM と共に削除」オプションにチェックを入れると、仮想マシンを削除した際にこのディスクも一緒に削除されます。

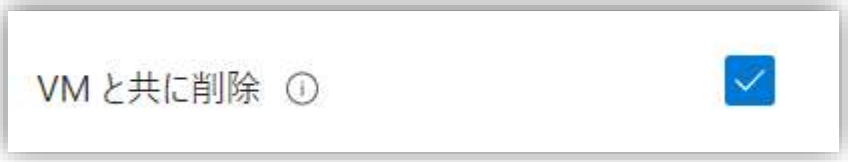


図 5.7.3-2 「VM と共に削除」をチェック

（2） 既存のディスクの接続

次に、「既存のディスクの接続」をクリックし、すでに作成してある共有ディスクを選択します。

図 5.7.3-3 既存のディスクの接続

ディスクの選択が完了したら、「次：ネットワーク」ボタンをクリックして、ネットワークの設定画面へ進んでください。

図 5.7.3-4 既存のディスクの接続

5.7.4. ネットワークの設定作成

ここでは仮想ネットワーク、サブネット、およびパブリック IP の設定を行います。

LifeKeeper がノード間の稼働確認及び通信を行うために、ノード間に特定な IP アドレスを使用し、コミュニケーションパスとして通信お行います。

（1） コミュニケーションパスが使用する IP アドレスの設定

図 5.7.4-1 に示した通り、の主要なコミュニケーションパスは次のようになります。

1 つ目のコミュニケーションパス: IP アドレス 10.4.1.4 と 10.4.2.4
2 つ目のコミュニケーションパス: IP アドレス 10.4.1.5 と 10.4.2.5

このセクションでは、1 つ目のコミュニケーションパスに使用する NIC（ネットワークインターフェースカード）を作成します。
コミュニケーションパスの詳細設定については、セクション「5.1 コミュニケーションパスの設定」を参照してください。

ネットワーク構成図は以下のようになります。

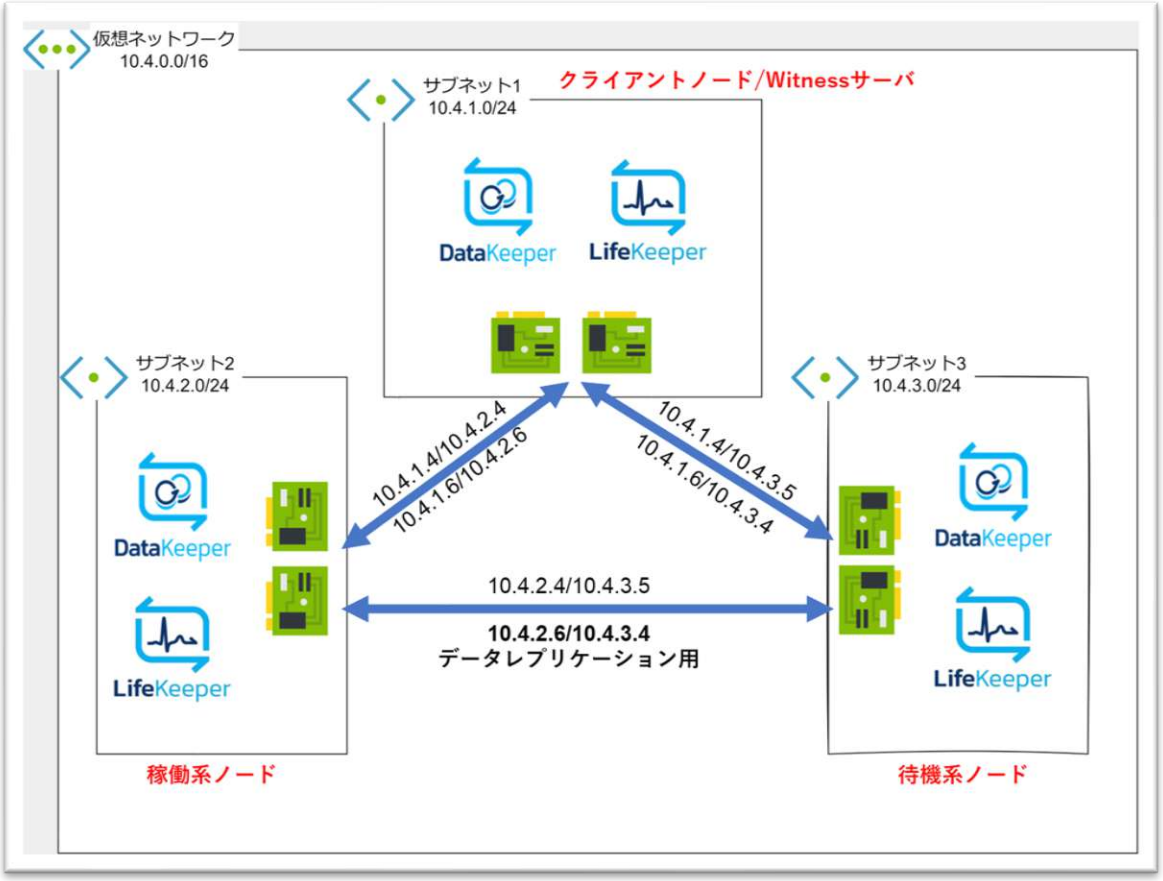


図 5.7.4-1 本ガイドのネットワーク構成図

（2） 仮想マシンが使用する仮想ネットワークとサブネット

稼働系ノードでは、以前に作成した「LKW-QWK-Storage-Vnet」という仮想ネットワークを使用し、サブネット「10.4.1.0/24」に設定します。

図 5.7.4-2 ネットワークとサブネットの選択

（3） パブリック IP アドレスの新規作成

次に、稼働系ノードは外部インターネットに接続しないため、「パブリック IP」の設定を「なし」にします。

図 5.7.4-3 パブリック IP アドレスの新規作成

（4） NIC とセキュリティグループの設定

NIC ネットワーク セキュリティ グループは、ファイアウォールとして機能し、ネットワークトラフィックのフィルタリングや制御に使用されます。

ここでは「Basic」設定を使用し、仮想ネットワーク内とロードバランサからの通信だけを許可します。

図 5.7.4-4 パブリック IP アドレスのセキュリティグループ種類の選択

リモートデスクトップ接続を許可するために、「パブリック受信ポート」を RDP（3389）に設定します。
「VM が削除されたときにパブリック IP と NIC を削除する」にチェックをいれます。

図 5.7.4-5 パブリック IP アドレスの受信ポートの選択

設定完了したら、適宜に「管理」、「Monitoring」、「詳細とタグ」タブを設定し、「確認および作成」をクリックします。

図 5.7.4-6 「確認および作成」をクリック

（5） 仮想マシンの確認と作成

「確認および作成」タブで表示された設定値とコストを確認後、「作成」を押してデプロイが始まります。

図 5.7.4-7 作成した仮想マシンの確認および作成

図 5.7.4-9 デプロイ中

「デプロイが完了しました」が表示されればデプロイが完了しました。

図 5.7.4-8 デプロイ完了

5.7.5. NIC の追加

本節では、稼働系ノードに 2 つ目のコミュニケーション用のネットワークインターフェースカード（NIC）を追加する手順について説明します。2 つ目の NIC の IP アドレスは 10.4.1.5 とします。

LifeKeeper では、冗長性を高めるために 2 本以上のコミュニケーションパスの使用が推奨されています。
稼働系ノードの仮想マシン管理画面にアクセスし、「概要」セクションの中で「停止」ボタンをクリックし、仮想マシンを停止させます。

（1） 仮想マシンの停止

稼働系ノードの仮想マシン管理画面にアクセスし、「概要」セクションの中で「停止」ボタンをクリックし、仮想マシンを停止させます。

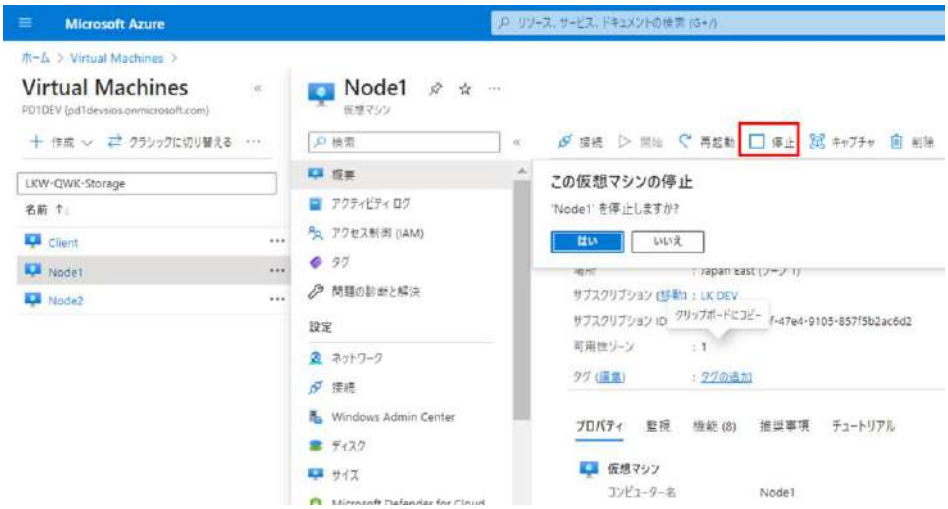


図 5.7.5-1 仮想マシンの停止

（2） NIC の作成と接続

「ネットワーク」タブを選択し、ネットワークの管理画面を開きます。「ネットワーク インターフェースの接続」をクリックし、その後「ネットワーク インターフェースの作成と接続」をクリックします。

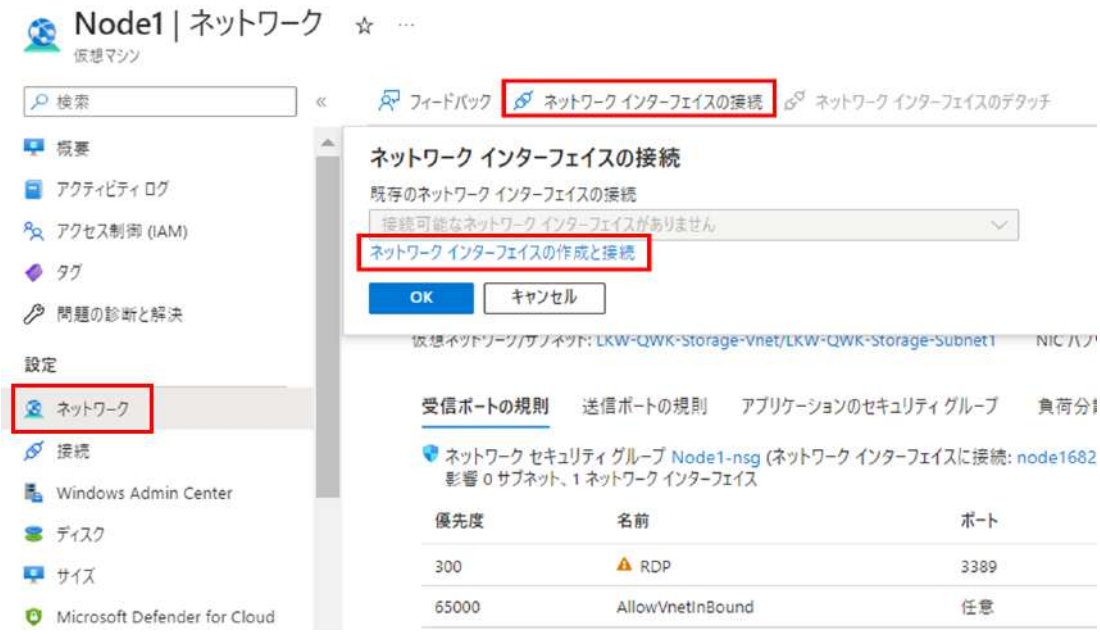


図 5.7.5-2 ネットワークの管理画面にアクセス

（3） NIC 名とサブネットの設定

「サブスクリプション」と「リソースグループ」を選択後、新しい NIC の「名前」を入力し、「サブネット」を選択します。

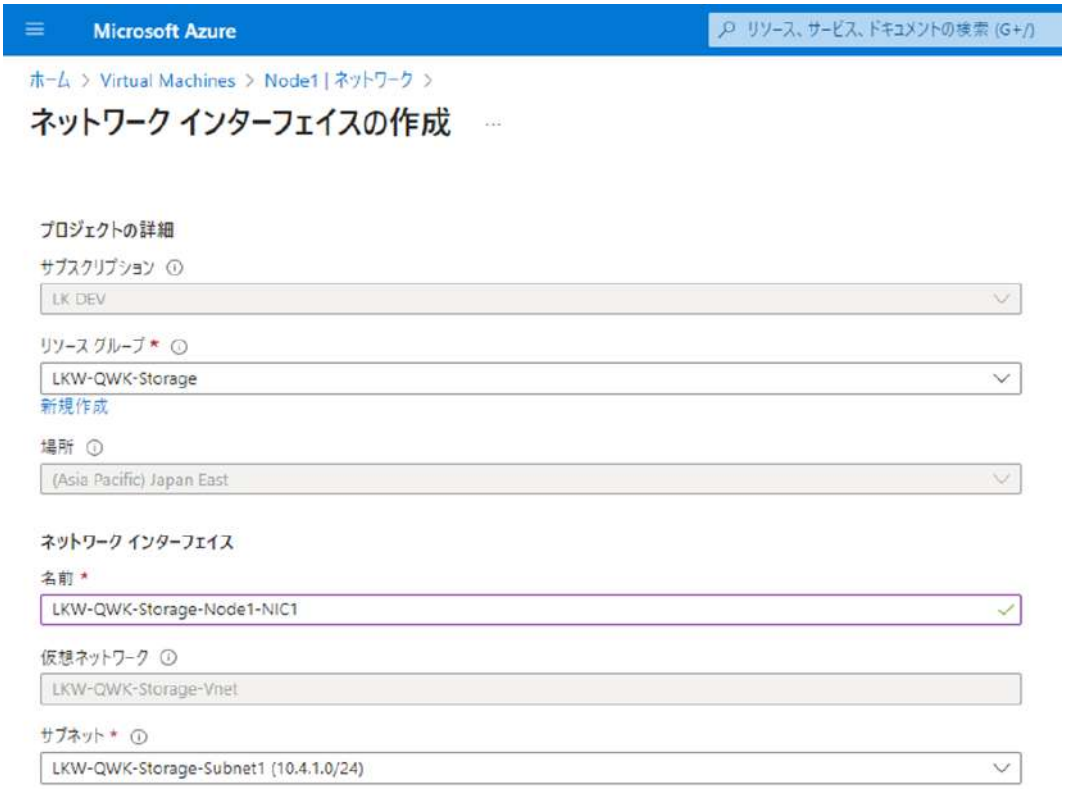


図 5.7.5-3 ネットワークの管理画面にアクセス

（4） セキュリティ グループとパブリック受信ポートの設定

LifeKeeper でセキュリティ設定の部分で、「NIC ネットワーク セキュリティ グループ」は「Basic」に設定します。

「パブリック受信ポート」は「なし」に設定します。

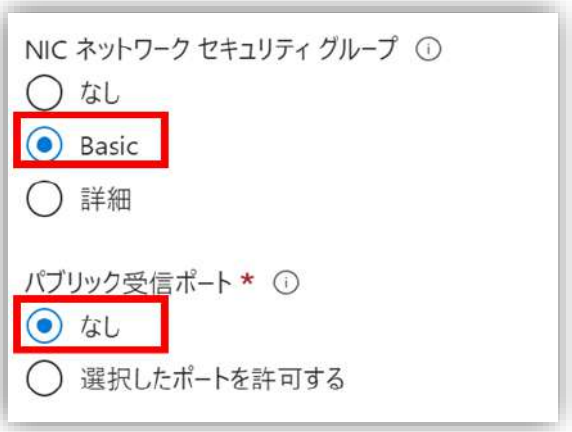


図 5.7.5-4 セキュリティ グループとパブリック受信ポートの設定

（5） プライベート IP アドレスの割り当て方式の設定

最後に、「プライベート IP アドレスの割り当て」オプションで「動的」を選択します。

設定が完了したら、「作成」をクリックして新しい NIC を作成します。

図 5.7.5-5 プライベート IP アドレスの割り当て方式の設定

これで 2 つ目の NIC の IP アドレスは追加されました。

各仮想マシンに追加する NIC の情報は以下の表にまとめています。

表 5.7.5 各仮想マシンに追加する NIC の情報

仮想マシン	IP アドレス	ポート	種類	説明
Node1	20.243.23.86	3389	パブリック	外部インターネットから RDP でアクセスする用
	10.4.1.4	なし	プライベート	コミュニケーションパス用
	10.4.1.5	なし	プライベート	コミュニケーションパス用
Node2	10.4.2.4	3389	プライベート	①クライアントノードから RDP でアクセスする用 ②コミュニケーションパス用
	10.4.2.5	なし	プライベート	コミュニケーションパス用
Client	10.4.3.4	3389	プライベート	①クライアントノードから RDP でアクセスするため

				②コミュニケーションパス用
	10.4.3.5	なし	プライベート	コミュニケーションパス用

5.7.6.1. 仮想マシンの設定値

各ノードで異なった設定は赤い字で書いてあります。

クライアントノード、稼働系ノードと待機系ノード用の仮想マシンを作成したときの値を以下の表にまとめました。

表 5.7.6.1 仮想マシンを作成する際の各タブの入力項目と説明

タブ	入力項目	値			説明
		稼働系	待機系	クライアント	
基本	サブスクリプション	<サブスクリプション名>			リソースグループを作成した時に使ったサブスクリプション
	リソースグループ	LKW-QWK-Storage			先ほど作成したリソースグループを指定
	仮想マシン名	Node1	Node2	Client	仮想マシンに付ける名前
	地域	（Asia Pacific）東日本			仮想ネットワークを作成するリージョン（本ガイドでは東日本に設置
	可用性ゾーン	**Zone 1**	**Zone 2**	**Zone 3**	仮想マシンを展開する可用性ゾーンを指定します。（東日本リージョンでは 3

					つのゾーンが用意されています
	イメージ	Windows Server 2022 Datacenter: Azure Edition - x64 Gen2			仮想マシンが使用数するオペレーティング システム
	セキュリティの種類	Standard			仮想マシンが使用数するセキュリティ種類
	サイズ	Standard_B2s - 2 vcpu 数 4 GiB のメモリ($45.55/月)			仮想マシンに割り当てる CPU、メモリ、ストレージなどのリソースを選択します
	ユーザ名	Client			仮想マシンにログインするためのユーザ名
	パスワード	<設定したパスワード>			仮想マシンにログインするためのパスワード
	パブリック受信ポート	**なし**	**なし**	**選択したポートを許可する**	アクセス許可するポートの選択
	受信ポートを選択	**N/A**	**N/A**	**RDP（3389）**	

ディスク	OS ディスクの種類	Standard SSD (ローカル冗長ストレージ)			仮想マシンで使用する OS ディスクの種類
	ディスク SKU	Standard SSD			OS ディスクの名前
	サイズサイズ (GiB)	8			OS ディスクのサイズ
	データ ディスクの種類	Standard SSD (ローカル冗長ストレージ)			仮想マシンで使用するデータ ディスクの種類
	ディスク SKU	Standard SSD			データ ディスクの名前
	サイズサイズ (GiB)	8			データ ディスクのサイズ
ネットワーク	仮想ネットワーク	LKW-QWK-Storage-Vnet			仮想マシンが使用する仮想ネットワーク
	サブネット	**LKW-QWK-Storage-Subnet1（10.4.1.0/24）**	**LKW-QWK-Storage-Subnet2（10.4.2.0/24）**	**LKW-QWK-Storage-Subnet3（10.4.3.0/24）**	仮想マシンが使用するサブネット
	パブリック IP	**なし**	**なし**	**新規**	外部と通信するためのパブリック IP アドレス

	NIC ネットワーク セキュリティ グループ	Basic			Azure ネットワーク内のトラフィックを制限するために使用されるセキュリティグループ
	パブリック IP の可用性ゾーン	ゾーン冗長			仮想マシンを冗長するためのパブリック IP アドレスを特定した可用性ゾーン
	パブリック受信ポート	**なし**	**なし**	**RDP（3389）**	仮想マシンに対するインターネットからの接続ポート

5.8. 内部ロードバランサ（ILB）の作成

5.8.1. 内部ロードバランサを使用する理由

通常、LifeKeeper は仮想 IP アドレス（Virtual IP, VIP）を用いて、クラスタノードの物理 IP アドレスよりも IP アドレスの正常性を保護し、監視します。この仮想 IP アドレスは、アプリケーションが動作しているノードにリンクされ、通信ルートがそこに割り当てられます。
仮想 IP アドレスは、現在稼働しているノード（アプリケーションが実行されているノード）に常にマッピングされ、通信経路が割り当てられます。

しかし、Azure の仮想ネットワークでは LifeKeeper で設定した仮想 IP アドレスが認識されません。そのため、仮想 IP アドレスを使用したネットワーク通信や保護はできません。
代わりに、Azure では Generic ARK for Load Balancer Probe Reply（GenLB）を使用して、 内部ロードバランサ（Internal Load Balancer、ILB）のバックエンドプールの IP アドレスを稼働系ノードと待機系ノードの NIC の IP アドレスに設定し、ILB がネットワーク通信をアクティブなノードに転送することで ILB のフロントエンド IP アドレスを仮想 IP として利用します。

GenLB により、アクティブなノードの正常性が検出され、ILB はネットワーク通信をアクティブなノードに割り当てます。

このようにして、ILB のフロントエンド IP を仮想 IP アドレスとして利用し、外部インターネットからのトラフィックを受信し、稼働系ノードに転送することができます。仮想 IP を使用してネットワーク通信経路を保護し、伝送することができます。

5.8.2. 内部ロードバランサの作成

Azure ポータルの検索ボックスに「ロードバランサ」と入力し、検索を実行します。表示された「ロードバランサ」をクリックし、その管理画面を開きます。

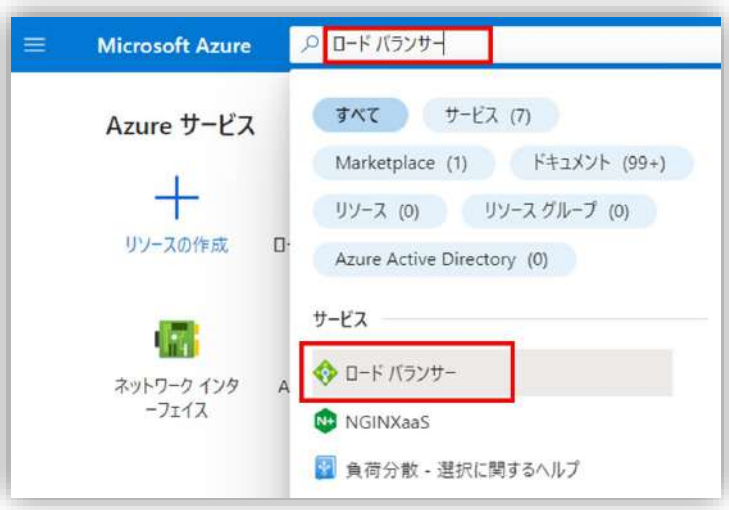


図 5.8.2-1 Azure ポータルからリソースの作成画面にアクセス

次に、画面内で「作成」ボタンをクリックし、新しいロードバランサの設定を開始します。

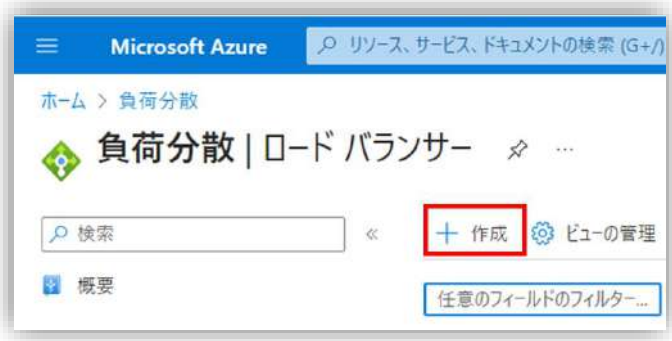


図 5.8.2-2 ロードバランサの作成

（1） 基本情報の入力

サブスクリプション、リソースグループ、およびリージョン（地域）を選択します。

図 5.8.2-3 基本情報の設定

（2）SKU とロードバランサ種類の設定:

SKU を「Standard」に設定します。

このガイドでは内部ロードバランサを利用するため、ロードバランサの「種類」を「内部」に設定します。

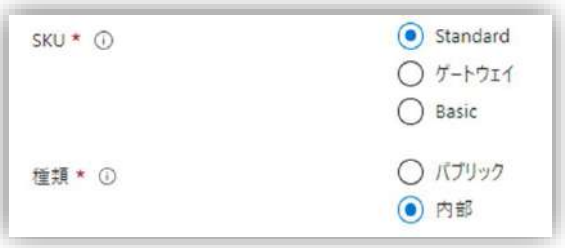


図 5.8.2-4 ロードバランサの SKU と種類の設定

設定完了したら、「次：フロントエンド IP の構成」 をクリックします。

図 5.8.2-5 「次：フロントエンド IP の構成」 へ進む

表 5.8.2 ロードバランサの「基本」タブの入力項目と説明

タブ	入力項目	値	説明
基本	サブスクリプション	サブスクリプション名	このリソースグループを作成した際に使用したサブスクリプション
	リソースグループ	LKW-QWK-Storage	作成済みのリソースグループ
	名前	LKW-QWK-Storage-LB	ロードバランサに設定する名前
	地域	東日本	仮想ネットワークのリージョン
	SKU	Standard	ロードバランサのサービスレベル
	種類	内部	本ガイドでは内部ロードバランサを使用

5.8.3. フロントエンド IP 構成

フロントエンド IP は、クライアントノードから届くリクエストを稼働系ノードとして機能するバックエンドサーバーに転送する IP アドレスです。
この IP は、バックエンドサーバーの直接的なアドレスではありません。ロードバランサを経由してバックエンドへとトラフィックを送ります。

（1） フロンエンド IP の追加
「+ フロントエンド IP 構成の追加」ボタンをクリックします。

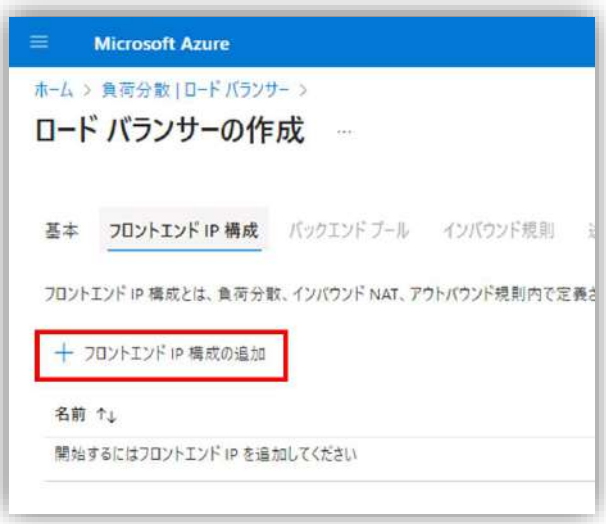


図 5.8.3-1 フロンエンド IP 構成の追加画面

（2） 名前とネットワークの設定

「名前」フィールドでフロンエンド IP の名前を入力し、仮想ネットワークを選択します。

サブネットはクライアントノードが使用しているサブネットに選択します。

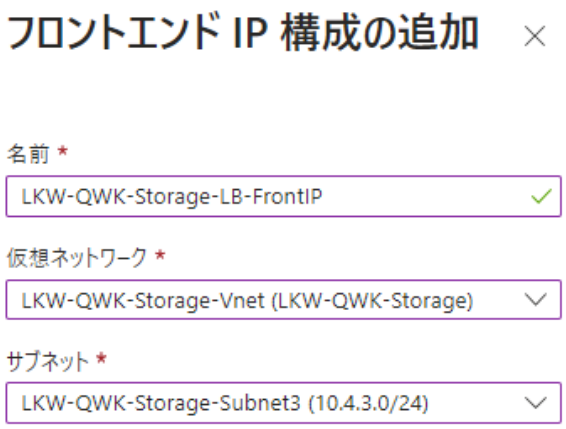


図 5.8.3-2 フロンエンド IP 構成の追加

（3） 割り当て方式と可用性ゾーンの設定

フロントエンド IP は動的に割り当てられます。

そのため、「割り当て」の項目で「動的」を選択します。

さらに、システムの可用性を確保するために、可用性ゾーンはゾーン冗長に設定します。「可用性ゾーン」で 「ゾーン冗長」を選択します。

設定完了したら、「追加」をクリックします。

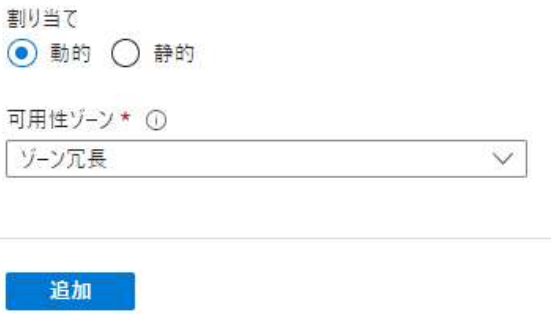


図 5.8.3-3 フロントエンド IP の割り当て方式と可用性ゾーンを選択

フロントエンド IP が作成されました。
設定内容を確認し、「次へ: バックエンド プール」 を選択します。

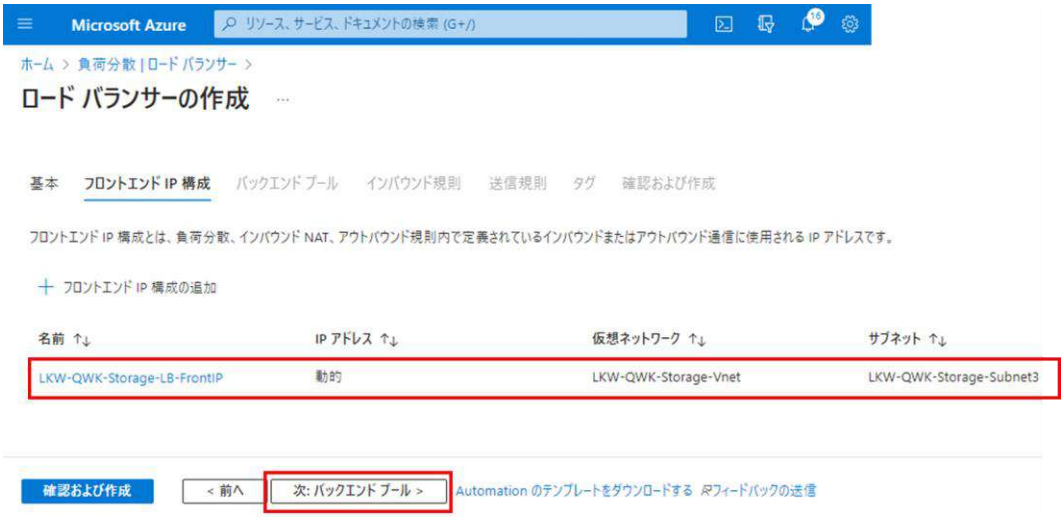


図 5.8.3-4 フロントエンド IP 設定を確認

表 5.8.3 ロードバランサの「フロントエンド IP 構成」タブの入力項目と説明

タブ	入力項目	値	説明
フロントエンド IP 構成	名前	LKW-QWK-Storage-LB-FrontIP	フロントエンド IP の名前

	仮想ネットワーク	LKW-QWK-Storage-Vnet	フロントエンド IP が所属している仮想ネットワーク
	サブネット	LKW-QWK-Storage-Subnet3（10.4.3.0/24）	フロントエンド IP が所属しているサブネット
	割り当て	動的	フロントエンド IP の割り当て方式

5.8.4. バックエンドプール

バックエンドプールは、ロードバランサから受信するトラフィックの転送先となる稼働系ノードと待機系ノードの仮想マシンで構成されています。

（1） バックエンドプールの追加

「+ バックエンドプールの追加」ボタンをクリックし、新しいバックエンドプールの設定画面を開きます。

図 5.8.4-1 バックエンドプールの追加

（2） 仮想マシンの NIC をバックエンド プールに追加

「名前」にバックエンド プールの名前を入力し、「バックエンド プールの構成」は「NIC」を選択します。

図 5.8.4-2 NIC の追加

（3） バックエンド プールに追加する NIC の IP 構成の設定

「IP 構成」に 「+ 追加」 をクリックし、画面の右側に 「バックエンド プールへの IP 構成の追加画面」 が開きます。

図 5.8.4-3 追加する NIC の IP 構成の追加

（4） IP 構成の追加

稼働系ノードと待機系ノードのプライベート IP アドレスをバックエンドプールに追加し、それぞれのチェックボックスを選択します。

設定完了したら、「追加」 をクリックし、選択した仮想マシンをバックエンドプールに追加します。

図 5.8.4-4 IP 構成の追加

（5） 追加した IP 構成の確認

追加したバックエンドプールとその IP 構成を確認します。確認ができたら、「保存」をクリックして、設定を保存します。

図 5.8.4-5 追加したバックエンドプールの IP 構成の確認

（6） バックエンドプール設定の保存

追加した内容を確認します。

確認できたら、「保存」 をクリックし、バックエンド プールの設定を保存します。

図 5.8.4-6 バックエンドプール設定の保存

（7） 作成したバックエンドプールの確認

「ロードバランサの作成」画面で、新しく作成したバックエンドプールと、そのプールに追加した仮想マシンの設定を確認します。

確認できたら、「次：インバウンド規則 >」をクリックします。

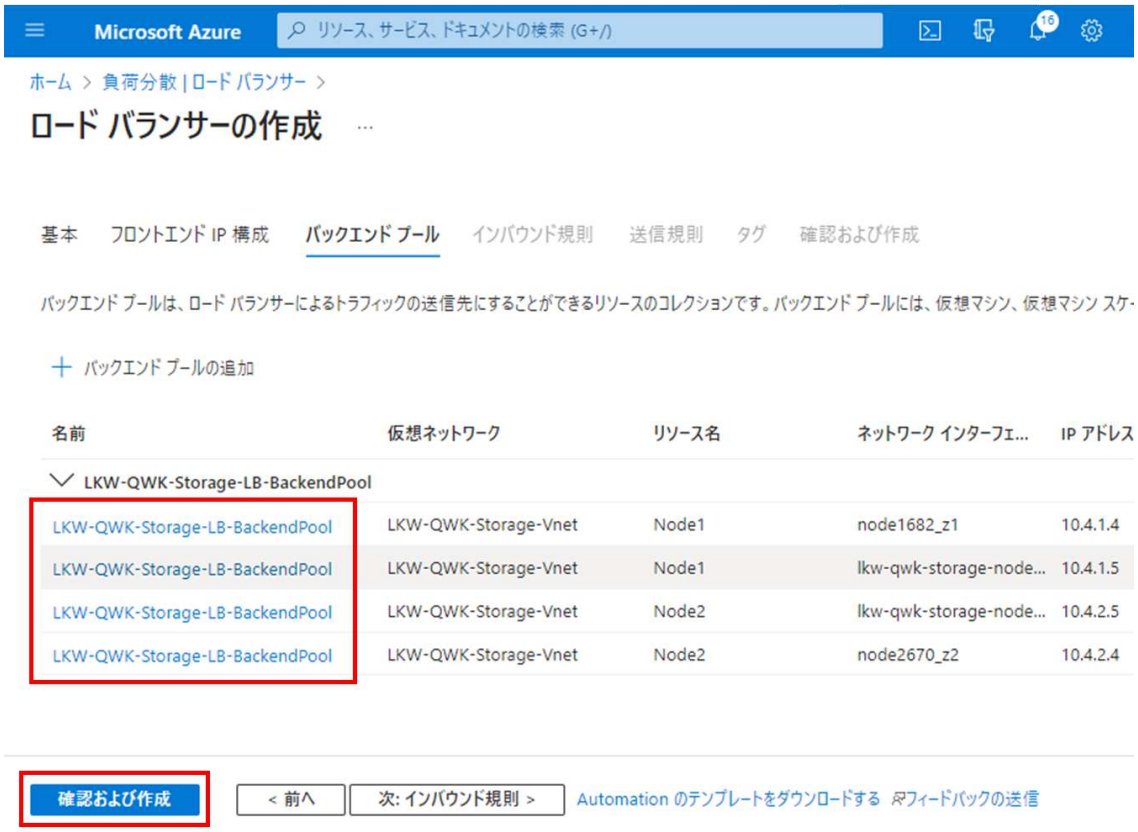


図 5.8.4-7 作成したバックエンドプールの確認

表 5.8.4 ロードバランサの「バックエンド プール」タブの入力項目と説明

タブ	入力項目	値	説明
バックエンド プール	名前	LKW-QWK-Storage-LB-BackendPool	バックエンド プールの名前
	仮想ネットワーク	LKW-QWK-Storage-Vnet	フロントエンド IP が所属している仮想ネットワーク

	バックエンド プールの構成	NIC	バックエンドプールに追加する仮想マシンの NIC または IP アドレスを選択
	バックエンド プールへ IP 構成の追加	Node1 Node2	バックエンドプールに仮想マシンを追加

5.8.5. インバウンド規則（負荷分散規則）

ロードバランサの負荷分散規則は、バックエンドプール内の仮想マシンへのトラフィック分散方法を定義するルールです。

（1） 負荷分散ルールの追加

「インバウンド規則」タブで、バックエンドプール内の仮想マシンへのトラフィック分散方法である負荷分散規則を追加します。

「負荷分散規則」 で、 「+ 負荷分散規則の追加」 をクリックします。画面の右側に 「負荷分散規則の追加」 画面が表示されます。

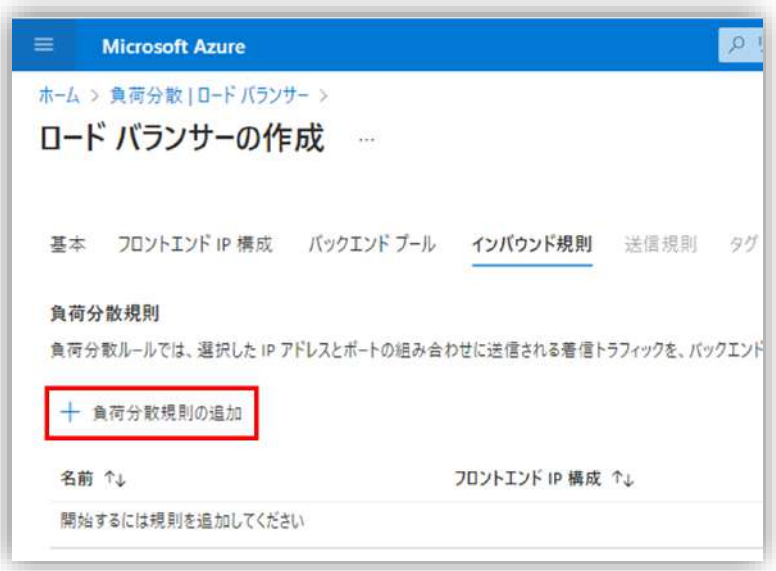


図 5.8.5-1 負荷分散ルールの追加

（2） 名前と使用する IP バージョンを入力

負荷分散ルールの名前と使用する IP バージョンを入力します。

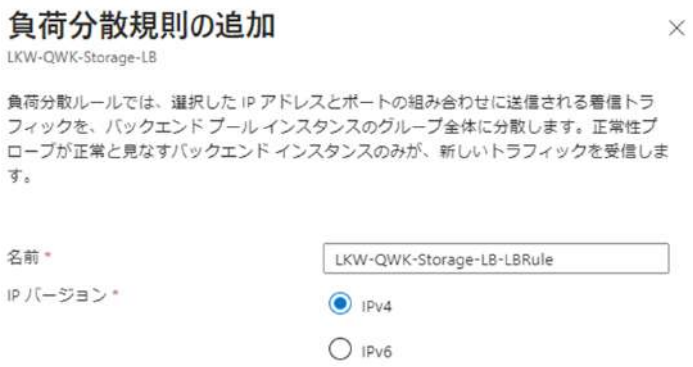


図 5.8.5-2 負荷分散ルールの名前と使用する IP バージョンの入力

（3） フロントエンド IP アドレスの設定

フロントエンド IP アドレスとは負荷分散時にトラフィックを受け取る IP アドレスです。

「フロントエンド IP アドレス」で先ほど作成した 「LKW-QWK-Storage-LB-FrontIP」 を選択します。

（4） バックエンドプールの選択

フロントエンド IP から受け取ったトラフィックを転送するためのバックエンドプールを選択します。

「バックエンド プール」で先ほど作成した 「LKW-QWK-Storage-LB-BackendPool」 を選択します。

図 5.8.5-3 フロントエンド IP アドレスとバックエンドプールの設定

（5） 負荷分散規則のポートとバックエンドポートの設定

ロードバランサの負荷分散規則におけるポートとバックエンドポートの定義は次の通りです。

フロントエンドポート：クライアントノードからの入ってくるトラフィックを受け取るためのポート
バックエンドポート：バックエンドプールの仮想マシンへトラフィックを転送するためのポート

このガイドでは、クライアントノードからのトラフィックが稼働中の SQL サーバのデータベースにアクセスします。そのため、SQL Server のデフォルトのポートである 1433 番を指定します。

「ポート」には 「1433」 入力します。
「バックエンド ポート」にも 「1433」 と入力します。

図 5.8.5-4 ポートとバックエンドポートの設定

（6） 正常性プローブの作成

正常性プローブは定期的にバックエンドプール内の各サーバに送信され、サーバの状態を確認します。
「正常性プローブ」の「新規作成」をクリックして正常性プローブの作成画面が表示されます。

図 5.8.5-5 正常性プローブの作成

正常性プローブのパラメータは以下のようになります。

- 名前：正常性プローブの名前。
- 通信に使用するプロトコル。このガイドでは、「TCP」 を選択します。
- ポート：プローブが使用するポート番号。「12345」 を入力します。
- 間隔（秒）：プローブが定期的に送信される間隔。「5」 秒を設定します。

図 5.8.5-6 正常性プローブの設定値の入力

設定が完了したら、「OK」をクリックして正常性プローブを保存します。

図 5.8.5-7 正常性プローブの作成

柔軟性を高めるために、「Floating IP」を有効にします。

その他の設定はデフォルト値を使用します。

入力した項目を確認した後、「追加」 をクリックします。

図 5.8.5-8 負荷分散ルールの追加

負荷分散規則の作成が完了したら、「確認および作成」 をクリックします。

図 5.8.5-9 負荷分散規則の作成完了

「検証に成功しました」と表示されたら、入力した項目を確認し、「作成」をクリックしてロードバランサのデプロイを開始します。

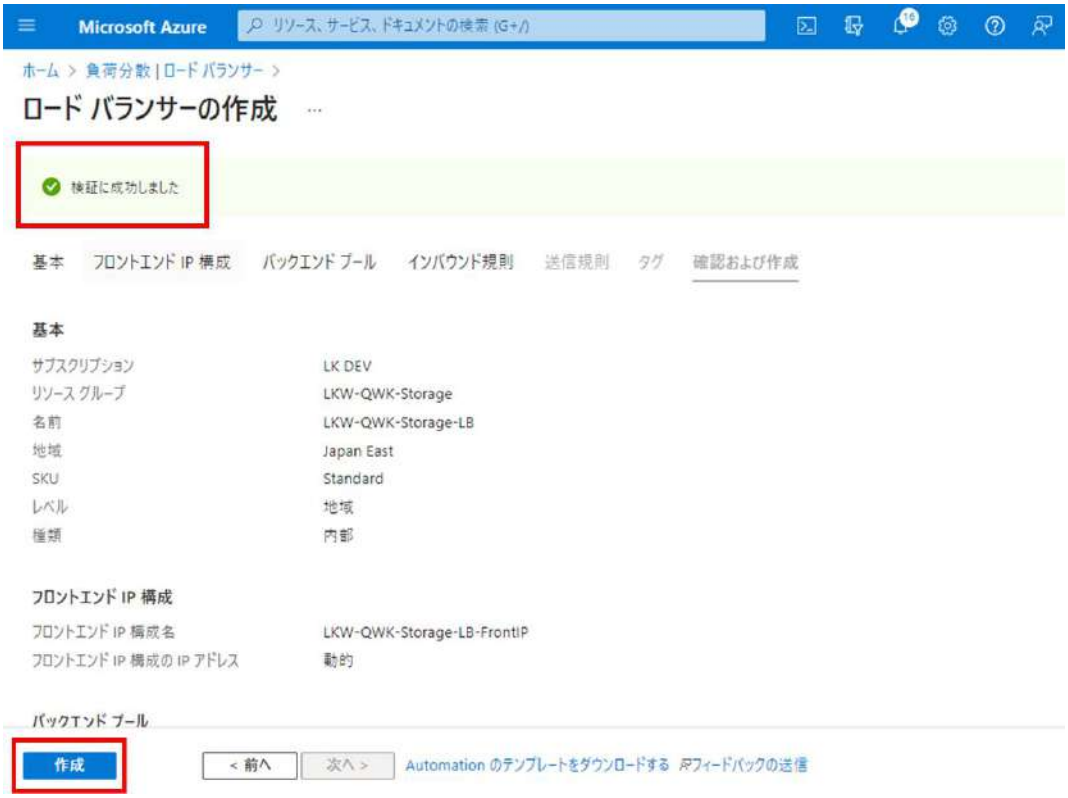


図 5.8.5-10 入力した項目の確認及び作成

「デプロイが完了しました」と表示されたら、ロードバランサの設定は完了です。

図 5.8.5-11 ロードバランサの完了

表 5.8.5 ロードバランサの「インバウンド規則」タブの入力項目と説明

タブ	入力項目	値	説明
インバウンド規則 →負荷分散規則	名前	LKW-QWK-Storage-LB-LBRule	負荷分散規則の名前
	IP バージョン	IPv4	負荷分散規則が使用する IP バージョン
	フロントエンド IP アドレス	LKW-QWK-Storage-LB-FrontIP	負荷分散した時にトラフィックを受け取るフロンエンド IP アドレス 前節で作成したフロンエンド IP アドレスを使用
	バックエンドプール	LKW-QWK-Storage-LB-BackendPool	負荷分散した時にトラフィックを受け取った後に伝送先になるバックエンドプール 前節で作成したバックエンドプールを使用
	ポート	1433	ロードバランサが クライアントノードからのトラフィックを受け取るために使用するポート番号
	バックエンドポート	1433	ロードバランサがバックエンドプールに対してトラフィックを転送するために使用するポート番号
	正常性プローブ	LKW-QWK-Storage-LB-HealthProbe	ロードバランサが管理するバックエンドプール内の各サーバの正常動作を確認

インバウンド規則 →負荷分散規則→ 可用性プローブ	名前	LKW-QWK-Storage-LB-HealthProbe	可用性プローブの名前
	プロトコル	TCP	バックエンドプール内の各サーバとの通信用のプロトコル
	ポート	12345	正常性プローブに使用するポート番号
	間隔（秒）	5	正常性プローブの送信間隔

5.9. ファイル共有の設定

5.9.1. ストレージ アカウントの作成

Azure の共有ファイルサービスを使用して QWK オブジェクトを保存する手続きを説明します。

（1） ストレージ アカウントの管理画面にアクセス

検索ボックスに「ストレージ アカウント」と入力し、該当するオプションをクリックしてストレージ アカウントの管理画面を開きます。

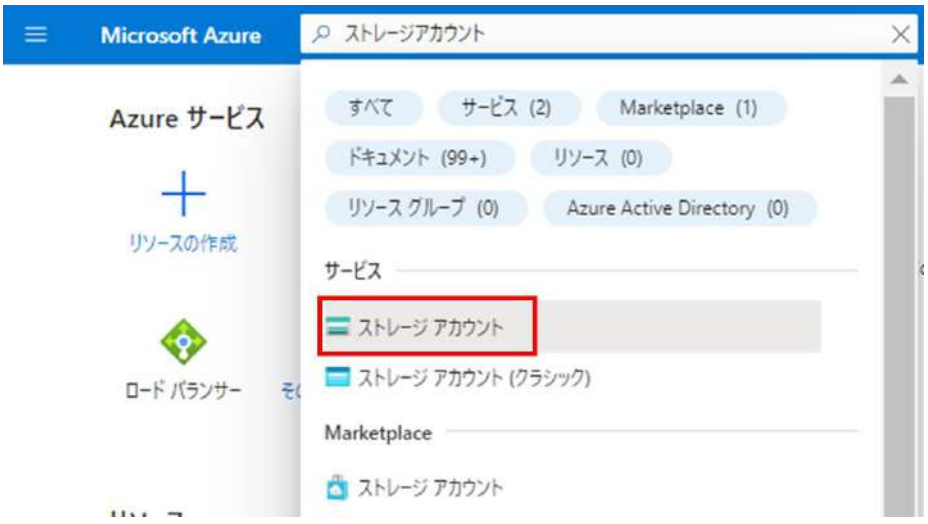


図 5.9.1-1 ストレージ アカウントの管理画面にアクセス

（2） ストレージ アカウントの作成

管理画面で「+ 作成」ボタンをクリックして、新しいストレージ アカウントを作成します。

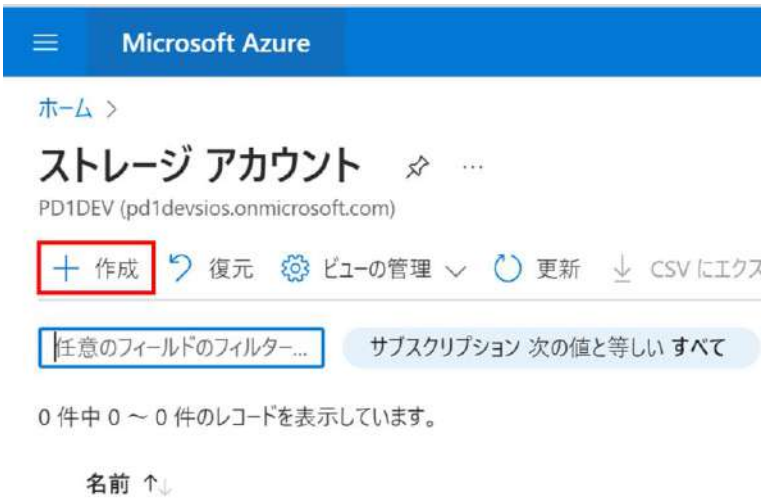


図 5.9.1-2 ストレージ アカウントの作成

（3） 基本設定の入力

サブスクリプションとリソースグループを選択します。

図 5.9.1-3 サブスクリプションとリソースグループの設定

ストレージアカウントの名前を設定し、地域（データセンターの位置）を選択します。

図 5.9.1-4 ストレージ アカウント名と地域の設定

パフォーマンスには「Standard」を、冗長性には「geo 冗長ストレージ（GRS）」を選択します。

設定できたら、「レビュー」をクリックします。

図 5.9.1-5 パフォーマンスと冗長の設定

（4） 設定した内容を確認

設定した内容を確認します。

確認出来たら、「作成」をクリックして、ストレージ アカウントの作成が開始されます。

図 5.9.1-6 設定した内容の確認および作成

5.9.2. 共有ファイルの作成

新しいファイル共有の作成手順について説明します。

（1） ファイル共有の管理画面へのアクセス

先程作成したストレージ アカウントを開きます。

管理画面から「ファイル共有」を選択し、続いて「+ ファイル共有」をクリックして新規のファイル共有を作成します。

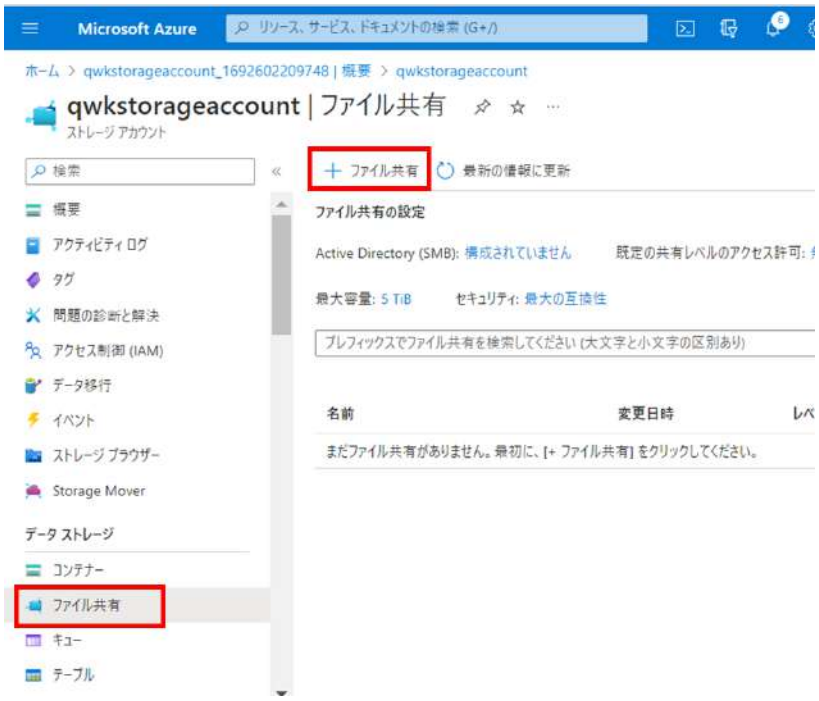


図 5.9.2-1 ファイル共有の管理画面にアクセス

（2） 共有ファイルの基本設定

「名前」フィールドにファイル共有の名称を入力し、「レベル」で「トランザクションが最適化されました」を選択します。

これらの設定が完了したら、「確認および作成」をクリックします。

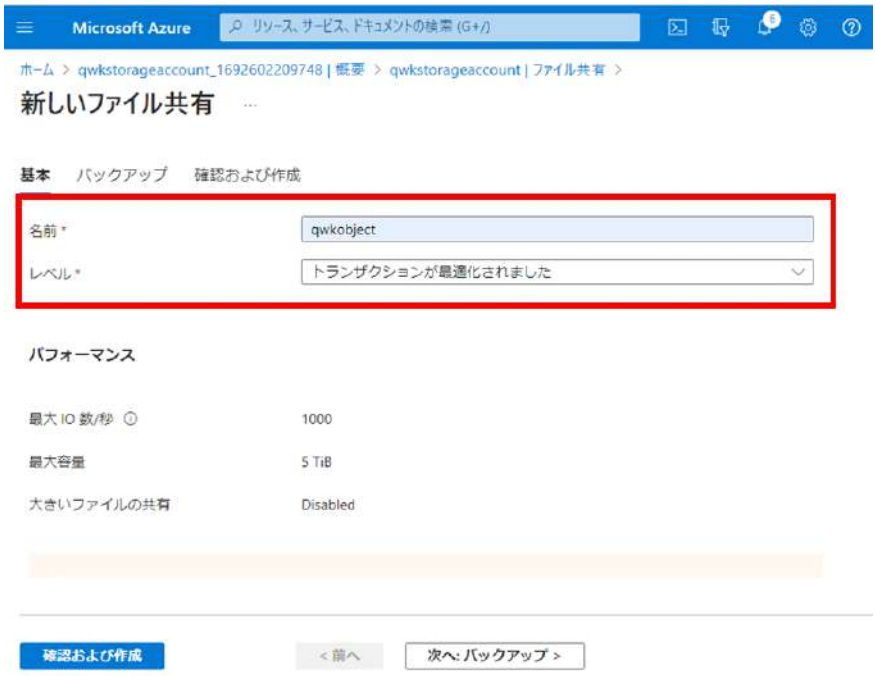


図 5.9.2-2 名前とレベルの設定

（3） 設定の確認とファイル共有の作成

設定項目を確認します。

全ての設定項目を確認した後、「作成」ボタンをクリックして新しいファイル共有を確定します。

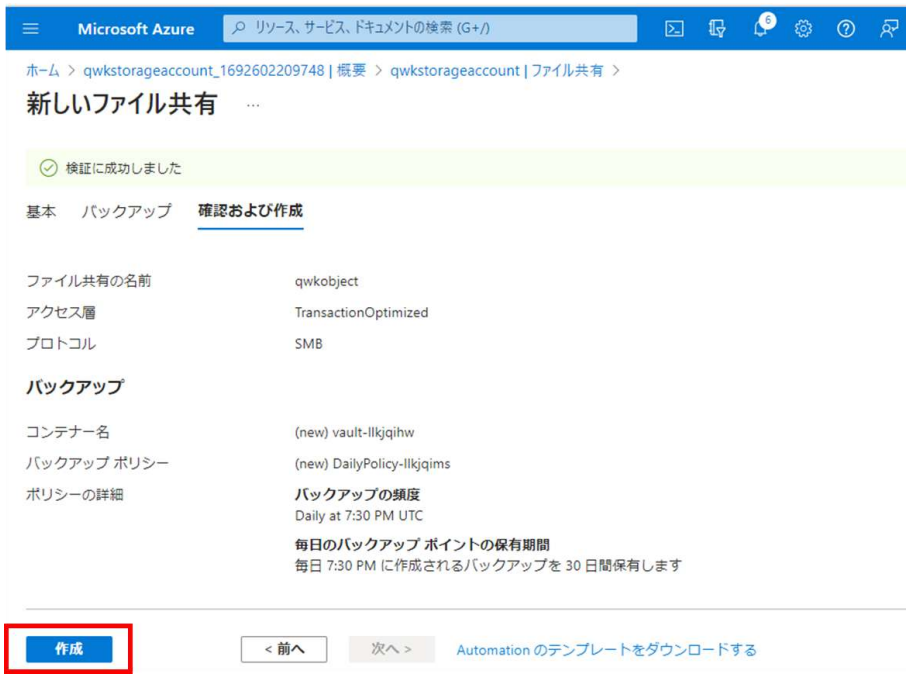


図 5.9.2-3 設定の確認および作成

6. クラスタノードの事前作業

6.1. RDP を用いて仮想マシンに接続する方法

6.1.1. 仮想マシンに接続

RDP (リモート デスクトップ プロトコル) を使用して、クライアントノード上の仮想マシンに接続する手順を説明します。

（1） 接続情報の確認画面にアクセス

クライアントノードの管理画面から接続情報の確認画面を開きます。「接続」をクリックして、接続情報を確認します。RDP 接続で使用する「パブリック IP アドレス」、「ポート番号」、および仮想マシンへのログインアカウントの「ユーザ名」を確認します。

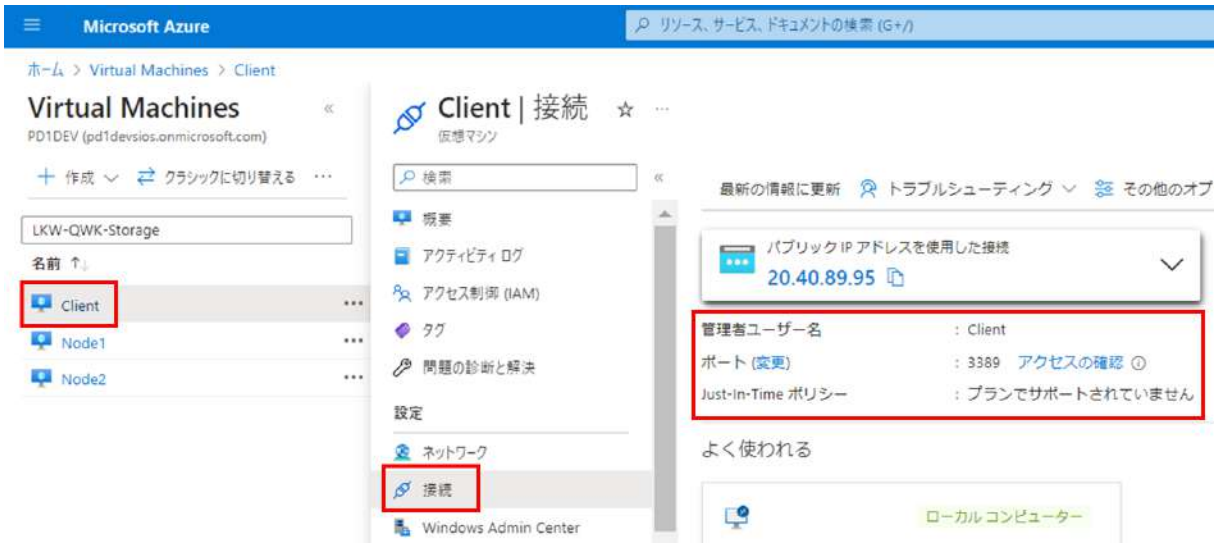


図 6.1.1-1 接続情報の確認画面にアクセス

（2） 「リモート デスクトップ接続」アプリの起動

ローカルマシンで Windows の検索バーを開き、「リモート デスクトップ接続」を検索してアプリを起動します。

図 6.1.1-2 「リモート デスクトップ接続」アプリを開く

（3） 接続情報の入力

先ほど確認した「ユーザ名」と「パブリック IP アドレス：ポート」を「リモート デスクトップ接続」アプリで入力します。

図 6.1.1-3 接続情報の入力

（4） ファイル転送の有効化

ローカルパソコンから仮想マシンへのファイル転送を有効化します。

「ローカルリソース」タブを選択し、「詳細」をクリックしてローカルマシンと仮想マシン間でのファイル転送を許可します。

図 6.1.1-4 ファイル転送の有効化

チェックボックスにて「ドライブ」を選択後、「OK」をクリックして設定を保存します。

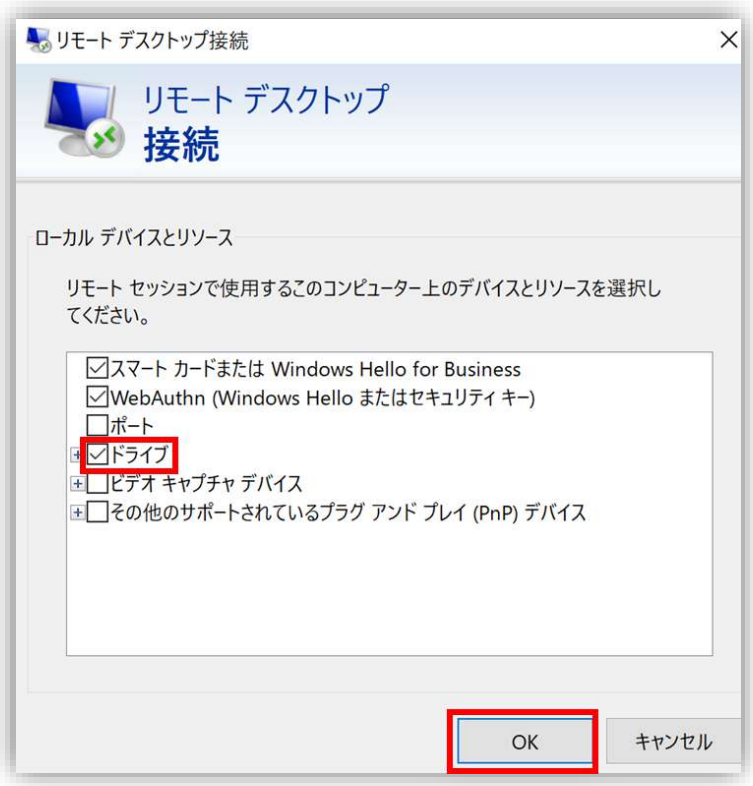


図 6.1.1-5 「ドライブ」 にチェック

「接続」 をクリックし、クライアントノードに接続します。

図 6.1.1-6 クライアントノードの仮想マシンに接続

（5） RDP 接続の信頼に関する画面

「このコンピュータへの接続について今後確認しない」にチェックを入れ、「接続」 をクリックして、クライアントノードに接続します。

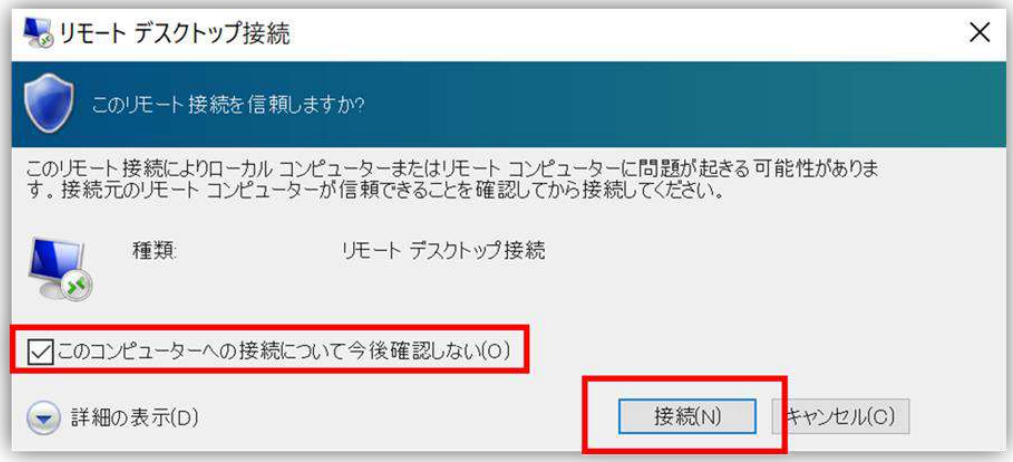


図 6.1.1-7 RDP 接続の信頼に関する画面

（6） 資格情報の入力画面

資格情報の入力画面が表示されます。仮想マシン作成時に設定したユーザ名とパスワードを入力します。

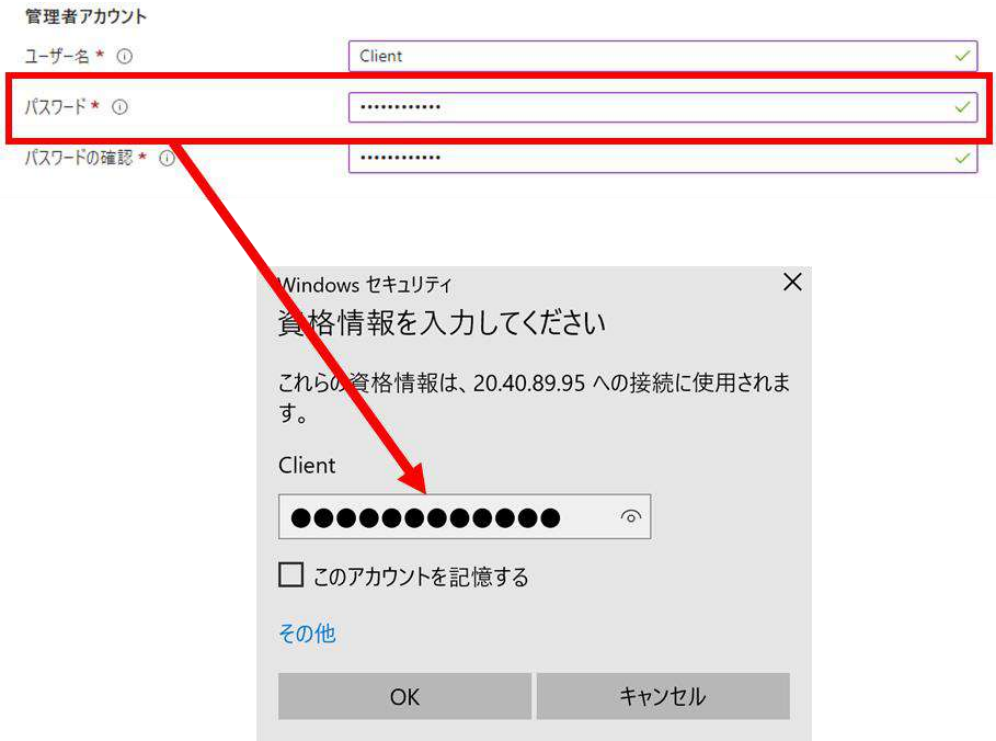


図 6.1.1-8 ログイン

（7） セキュリティに関する確認画面が開きます。
繰り返し接続する場合は、セキュリティ確認をスキップするため「このコンピュータへの接続について今後確認しない」にチェックを入れ、「はい」をクリックします。

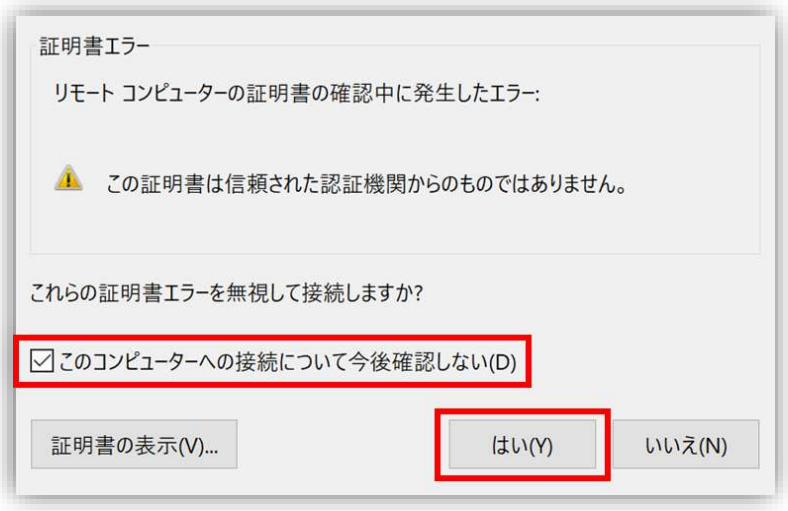


図 6.1.1-9 クライアントノードに接続

クライアントノードのデスクトップ画面が表示されることを確認します。

図 6.1.1-10 クライアントノードのデスクトップ画面に接続

6.2. コンピュータ名を変更

必要に応じてコンピュータ名を適宜変更します。本ガイドでは以下のコンピュータ名を使用します。

表 6.2 各ノードのコンピュータ名

ノード	コンピュータ名
クライアントノード	Client
稼働系ノード	Node1
待機系ノード	Node2

6.3. 新規追加した NIC のデフォルトゲートウェイの設定

稼働系ノードにおいてデフォルトゲートウェイの設定を行います。

（1） Windows PowerShell の起動

デスクトップで Windows アイコンを右クリックし、「Windows PowerShell（Admin）」を選択して管理者権限で PowerShell を開きます。

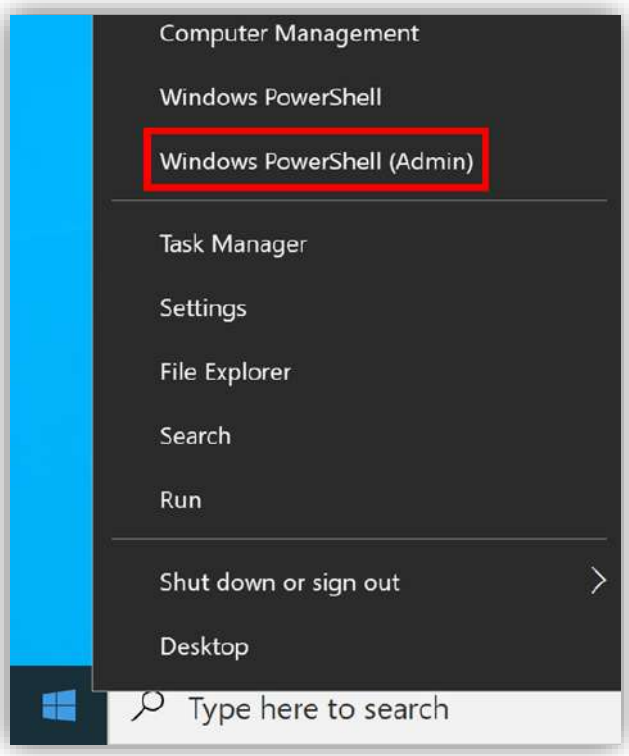


図 6.3-1 Windows PowerShell の起動

（2） ネットワークの設定の確認

PowerShell で Ipconfig コマンドを実行します。

Ethernet 2（新規追加した NIC）のデフォルトゲートウェイが未設定（空白）であれば、次の手順に手動で設定します。

```
PS C:\Users\Client> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : 15lxgvy0akkuvnnjqwx5zqazmg.lx.internal.cloudapp.net
   Link-local IPv6 Address . . . . . : fe80::b729:b2a2:4d72:e0b4%5
   IPv4 Address. . . . . . . . . . . : 10.4.3.4
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.4.3.1

Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . : 15lxgvy0akkuvnnjqwx5zqazmg.lx.internal.cloudapp.net
   Link-local IPv6 Address . . . . . : fe80::edbe:4410:328a:3a0a%10
   IPv4 Address. . . . . . . . . . . : 10.4.3.5
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
PS C:\Users\Client>
```

図 6.3-2 ネットワークの設定の確認

（3） ネットワークステータス表示画面を開く

Windows の検索バーに「View network status and tasks」と入力し、検索結果からそれを選択して開きます。

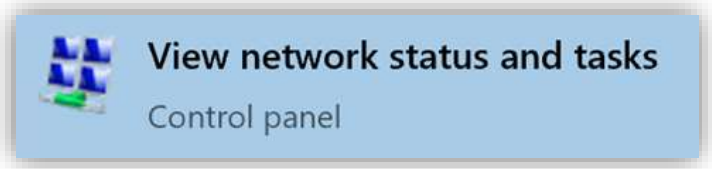


図 6.3-3　View network status and tasks を開く

（4） 追加した NIC のネットワーク状態の確認

Ethernet 2（追加した NIC）が未設定（Unidentified Network）であることが確認できます。

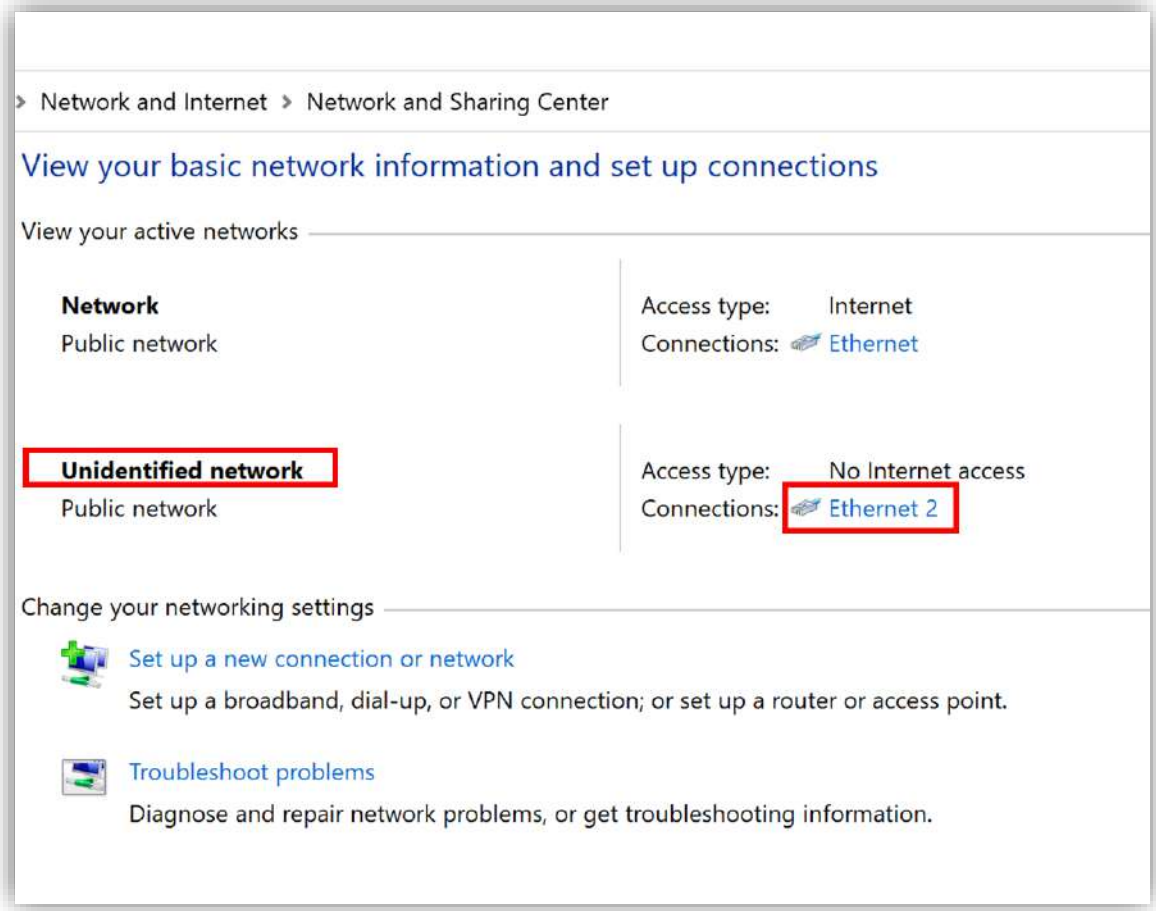


図 6.3-4 NIC のネットワークの設定画面を開く

（5） NIC のネットワーク設定

Ethernet 2 をクリックして「Properties」を選択します。

次に、「Internet Protocol Version 4 (TCP/IPv4)」を選び、「Properties」をクリックしてネットワーク設定を行います。

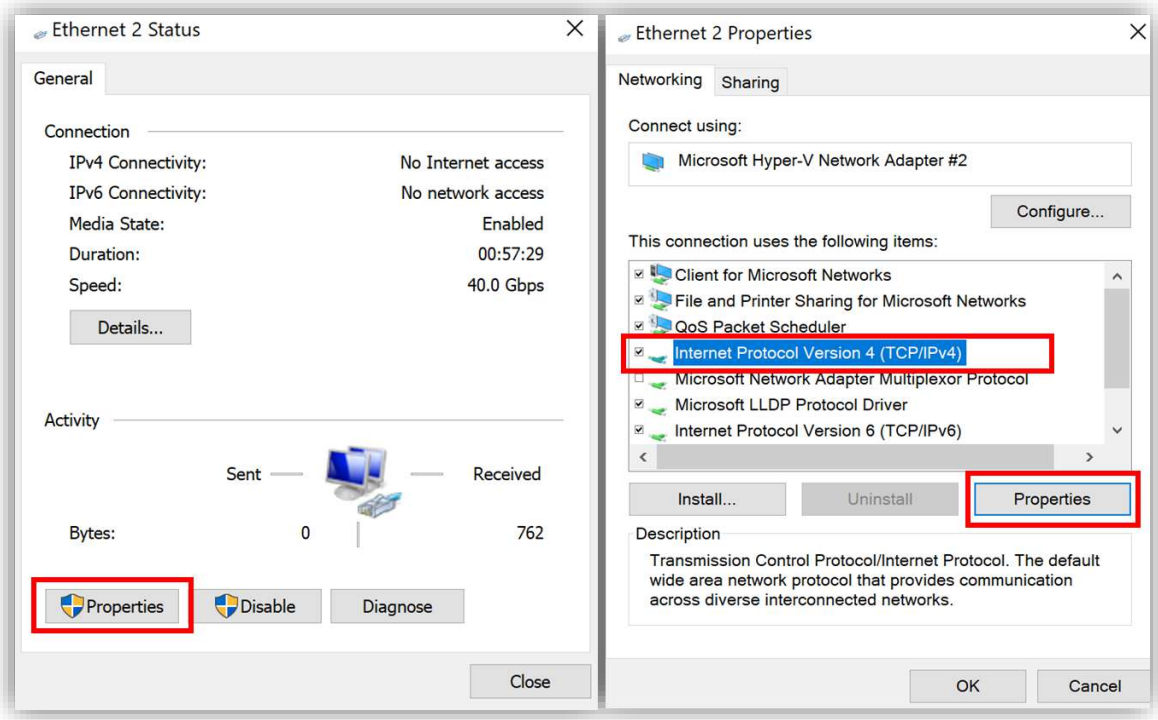


図 6.3-5 NIC のネットワーク設定

（6） NIC のデフォルトゲートウェイ設定

「Internet Protocol Version 4 (TCP/IPv4)」の設定画面にて、「自動的に IP アドレスを取得する」のオプションのチェックを外します。

「次の IP アドレスを使用する」にチェックを入れます。

ipconfig コマンドで表示された情報を参考に、IP アドレス、サブネットマスク、デフォルトゲートウェイを手動で設定します。

全ての設定が完了したら、「OK」をクリックして保存します。

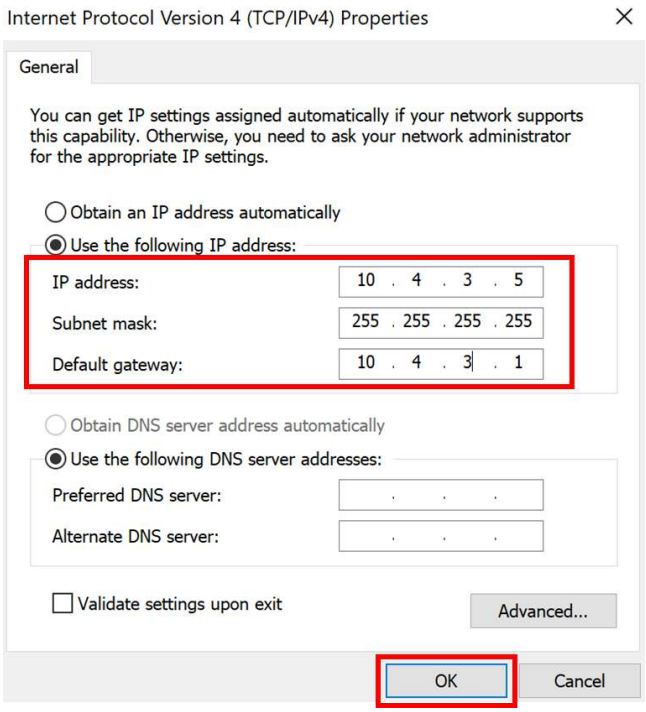


図 6.3-6 NIC のデフォルトゲートウェイの設定

この手順で、稼働系ノードのデフォルトゲートウェイの設定が完了します。待機系ノードも同様の手順で設定してください。

6.4. Ping の有効化

Ping を使用して、ネットワークの疎通確認を行います。
そのため、ファイアウォールで Ping リクエストを有効化します。

（1） Ping リクエストの有効化

Windows の検索バーで「Windows Defender Firewall with Advanced Security」を検索して開きます。

図 6.4-1 ファイアウォールの設定画面を開く

次に、「File and Printer Sharing (Echo Request - ICMPv4-In)」を右クリックし、「Enable Rule」を選択します。
これで IPv4 用の Ping リクエストが有効になります。

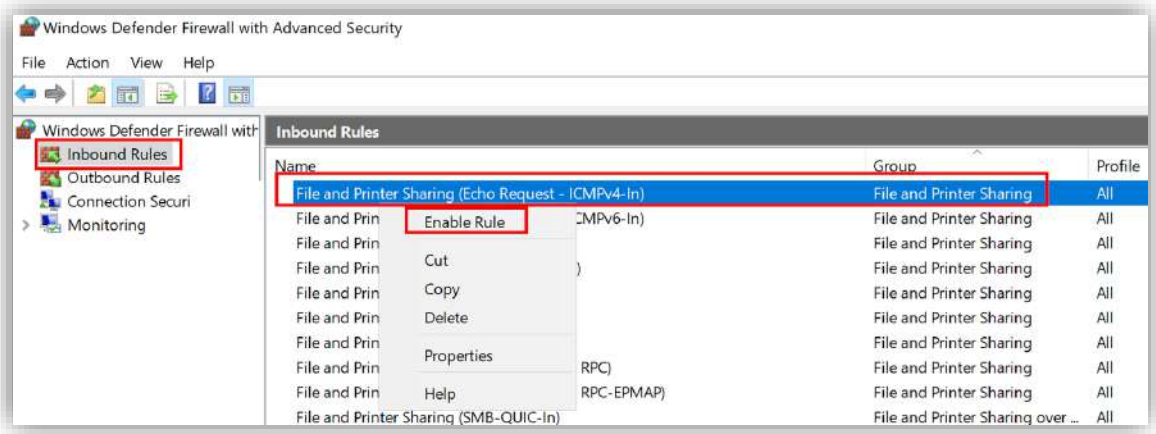


図 6.4-2 IPv4 による Ping リクエストの有効化

（2） ネットワークの疎通確認

PowerShell で Ping を実行して管理者権限で PowerShell を開きます。
クライアントノードから稼働系ノードに対して、IP アドレスを指定して Ping を実行します。
これでネットワークの疎通状態を確認できます。

```
PS C:\Users\Client> ping 10.4.3.4

Pinging 10.4.3.4 with 32 bytes of data:
Reply from 10.4.3.4: bytes=32 time<1ms TTL=128
Reply from 10.4.3.4: bytes=32 time<1ms TTL=128
Reply from 10.4.3.4: bytes=32 time<1ms TTL=128
Reply from 10.4.3.4: bytes=32 time<1ms TTL=128

Ping statistics for 10.4.3.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

図 6.4-3 ネットワークの疎通確認

6.5. ホストファイルにホスト情報を記入する

クラスタ内の各ノードの IP アドレスとドメイン名の対応を設定するため、ホストファイルに必要な情報を記入します。

（1） ホスト情報の記入
Windows Server 2022 のホストファイルは以下の場所にあります：
C:¥Windows¥System32¥drivers¥etc¥hosts

以下に示すように、クライアントノード、稼働系ノード、および待機系ノードの IP アドレスと対応するホスト名を追加します。

10.4.1.4 Client
10.4.1.5 Client

10.4.2.4 Node1
10.4.2.5 Node1

10.4.3.4 Node2
10.4.3.5 Node2

（2） Ping での名前解決テスト
ホスト情報が記入された後、Ping コマンドを使って名前解決が正しく行われるかテストします。
ホスト名を用いて Ping を実行し、正常に応答があれば設定は成功です。
（Ping への応答を有効にする手段は前節で説明した通りです。）

応答（Reply from <IP アドレス>）が表示されれば、ホストファイルによる名前解決が正常に行われています。

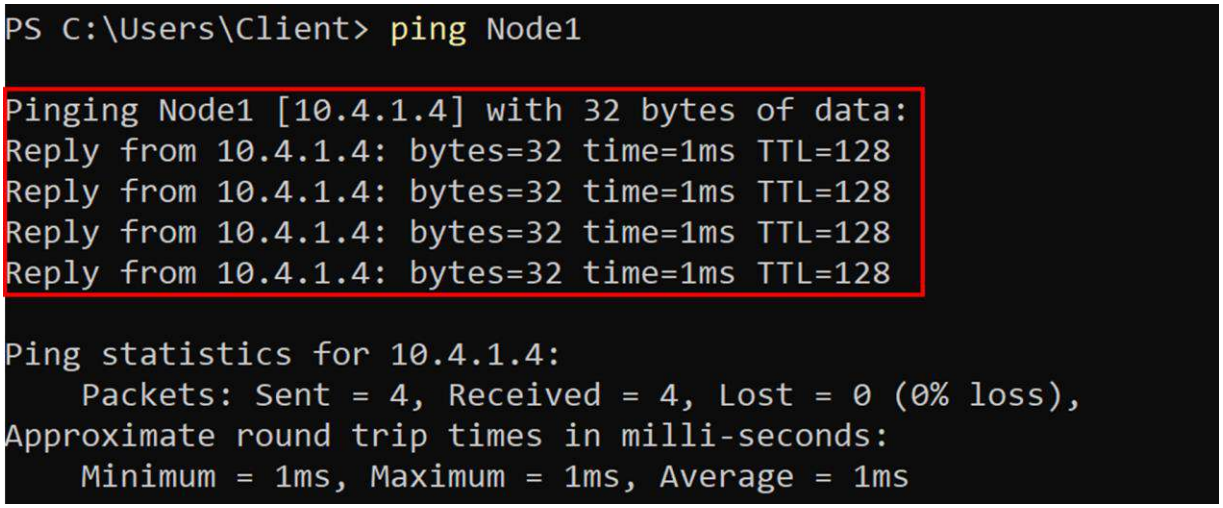


図 6.5 Ping の実行

6.6. AD DS を構築する

6.6.1. AD DS サービスをクライアントノードにインストールする

Active Directory Domain Services (AD DS) は、ログオンアカウントの一括管理やファイル共有時の認証に必要なサービスです。

このセクションでは、AD DS サービスをクライアントノードにインストールする手順を説明します。

（1） Server Manager の起動

Server Manager を開きます。

「Add roles and features」をクリックして、AD DS サービスをインストールする画面に進みます。

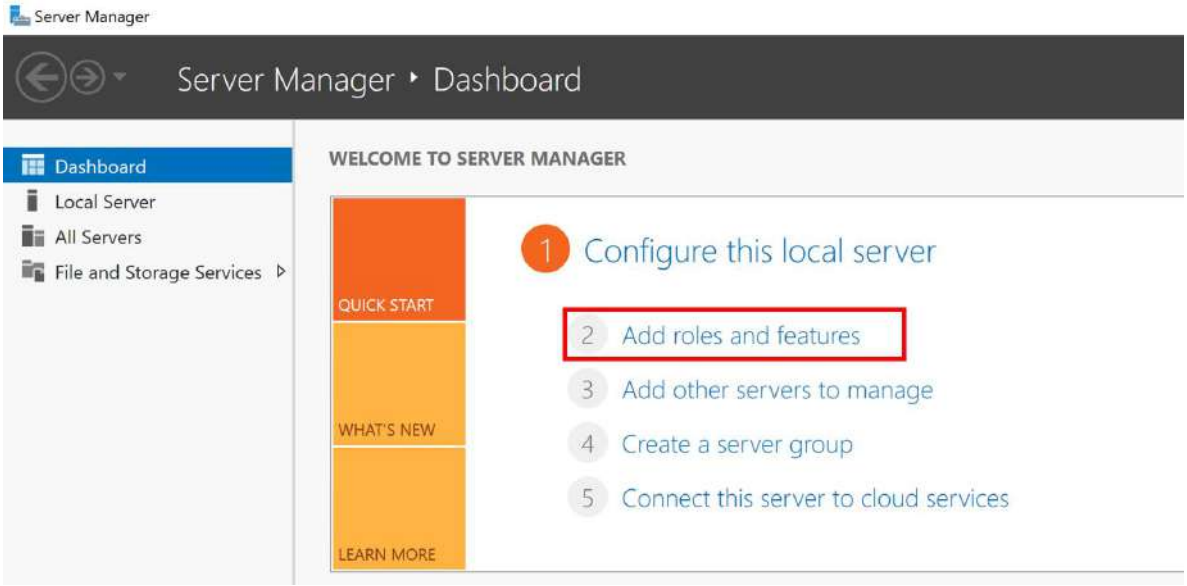


図 6.6.1-1 役割と機能の追加

（2） インストール前の確認

インストール前の確認事項を確認します。

すべての項目が問題なければ、「Next >」をクリックします。

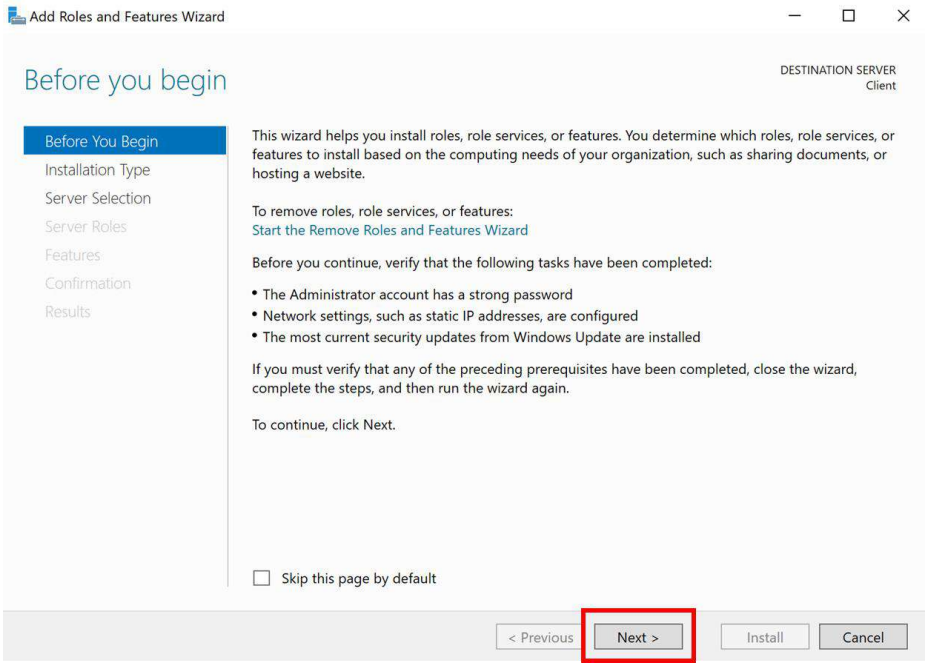


図 6.6.1-2 インストール前の確認

（3） インストールの種類の選択

インストールの種類を選択します。

AD DS はサーバのロールとしてインストールされます。

「Role-based or feature-based installation」にチェックを入れ、「Next >」をクリックします。

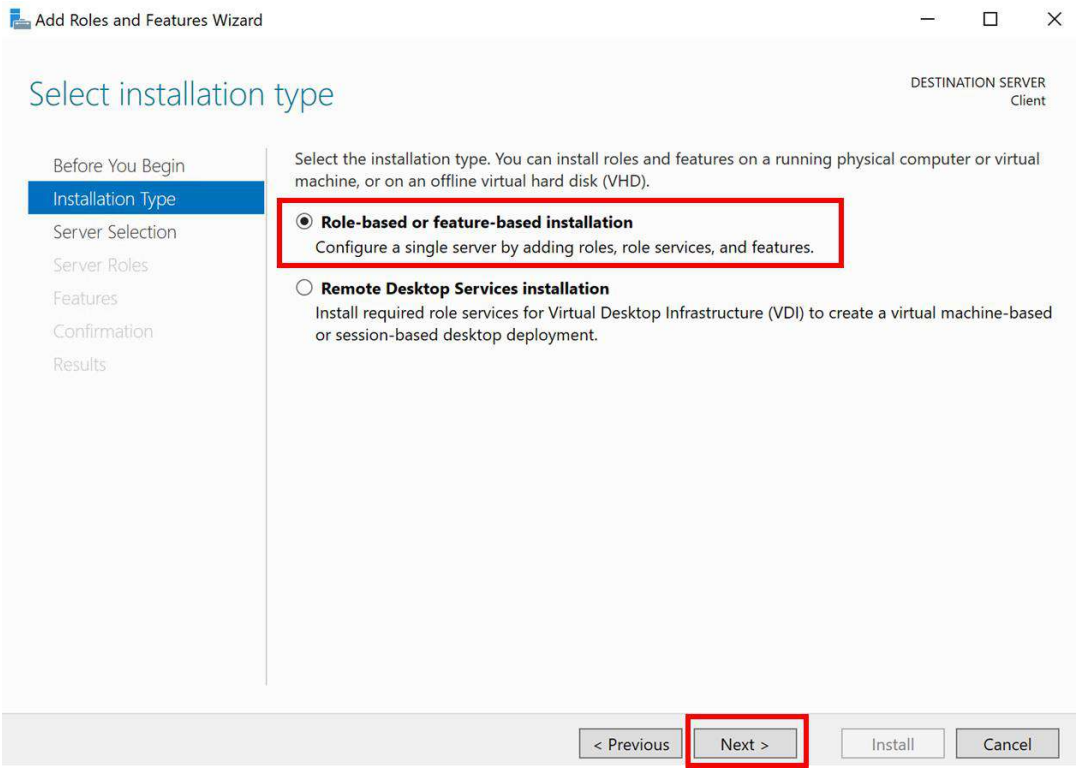


図 6.6.1-3 インストールの種類の選択

（4） 役割を追加する対象のサーバの選択

インストールするサーバを選択します。このケースではクライアントノードが対象ですので、「Client」を選択し、「Next >」をクリックします。

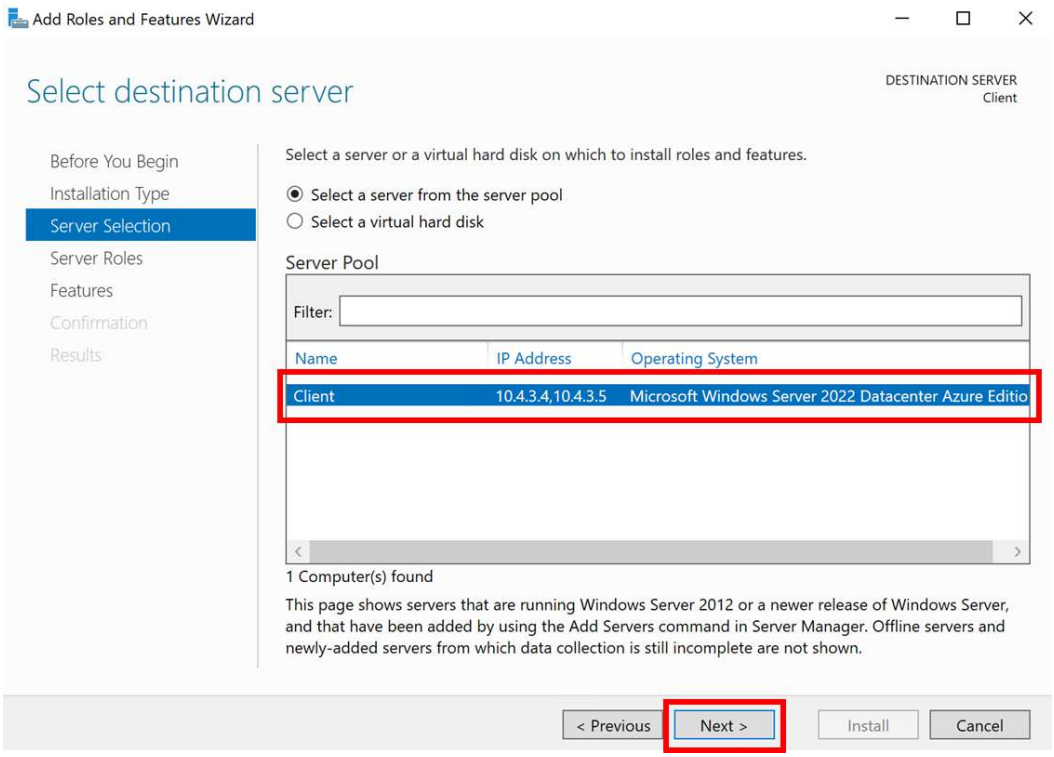


図 6.6.1-4 役割を追加する対象のサーバの選択

（5） サーバの役割の選択

「Active Directory Domain Services」にチェックマークを付け、にチェックを入れ、「Next >」をクリックします。

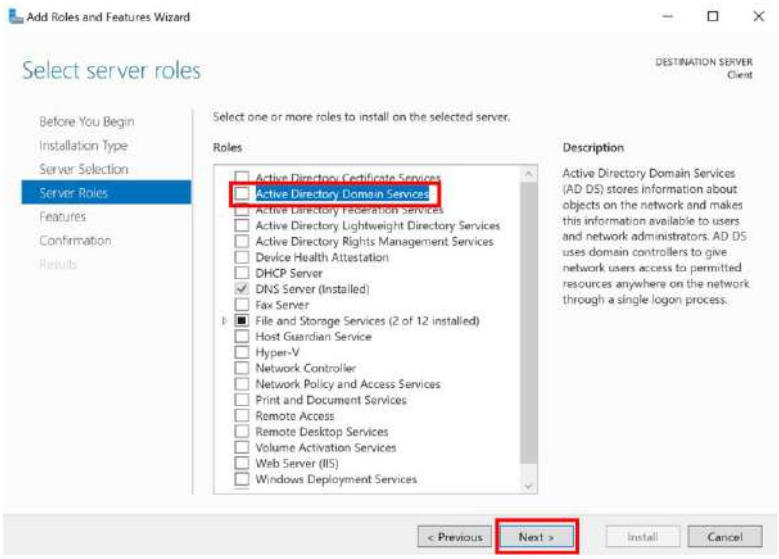


図 6.6.1-5 サーバの役割の選択

（6） 役割と機能の追加

Active Directory Domain Services に必要な追加機能が表示されます。

「Add Features」をクリックして、次へ進みます。

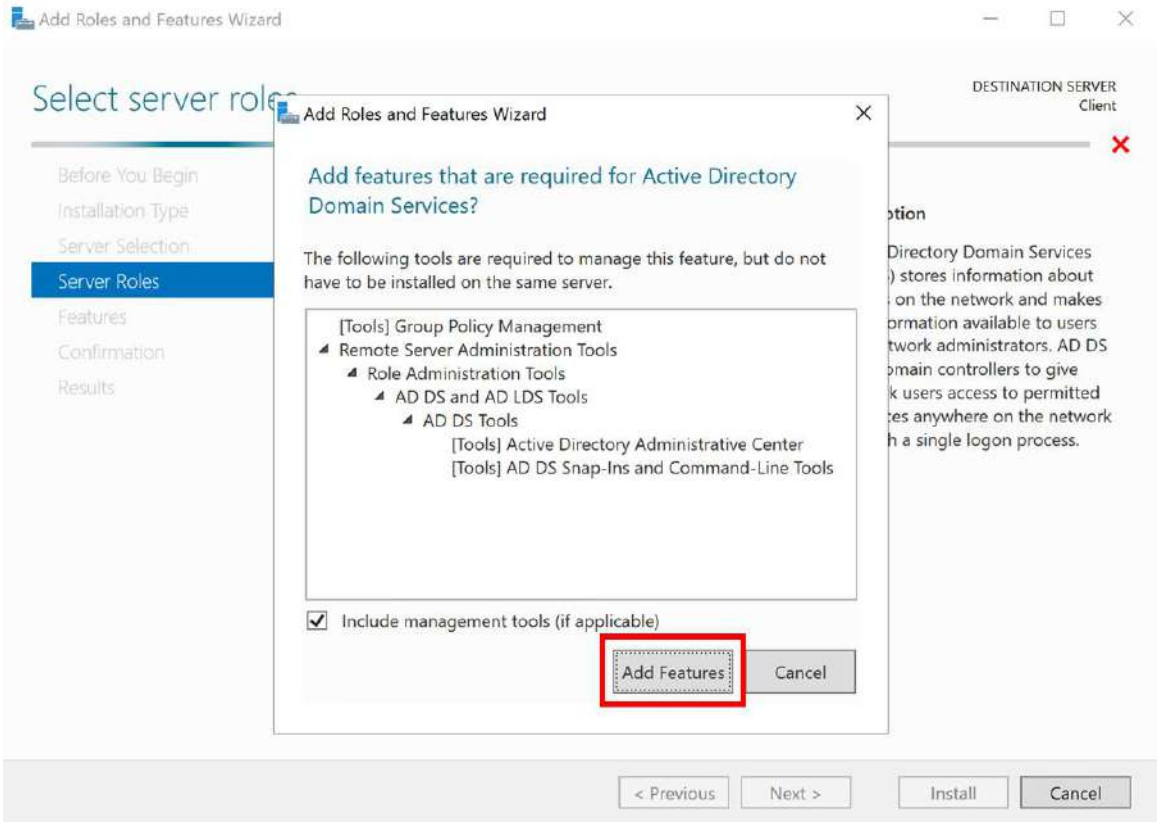


図 6.6.1-6 役割と機能の追加

「Active Directory Domain Services」にチェックが入れています。

「Next >」をクリックします。

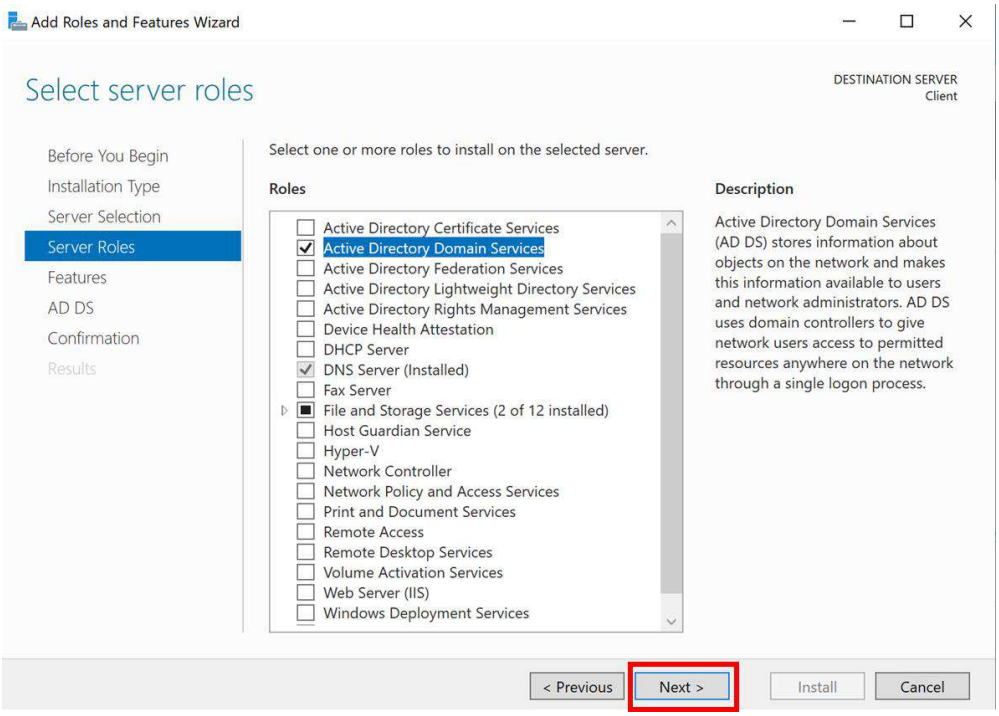


図 6.6.1-7 役割と機能の追加

（7） 機能の選択

特に追加の機能は必要ないため、そのまま「Next >」をクリックします。

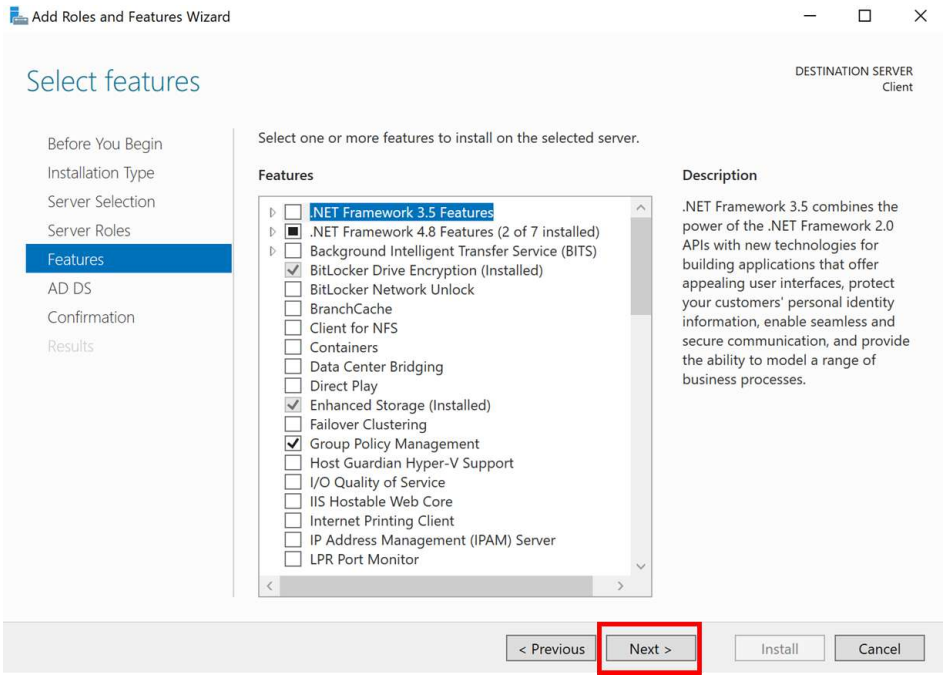


図 6.6.1-8 機能の選択

（8） AD DS の注意事項

AD DS に関する重要な注意事項が表示されます。

これを確認後、「Next >」をクリックします。

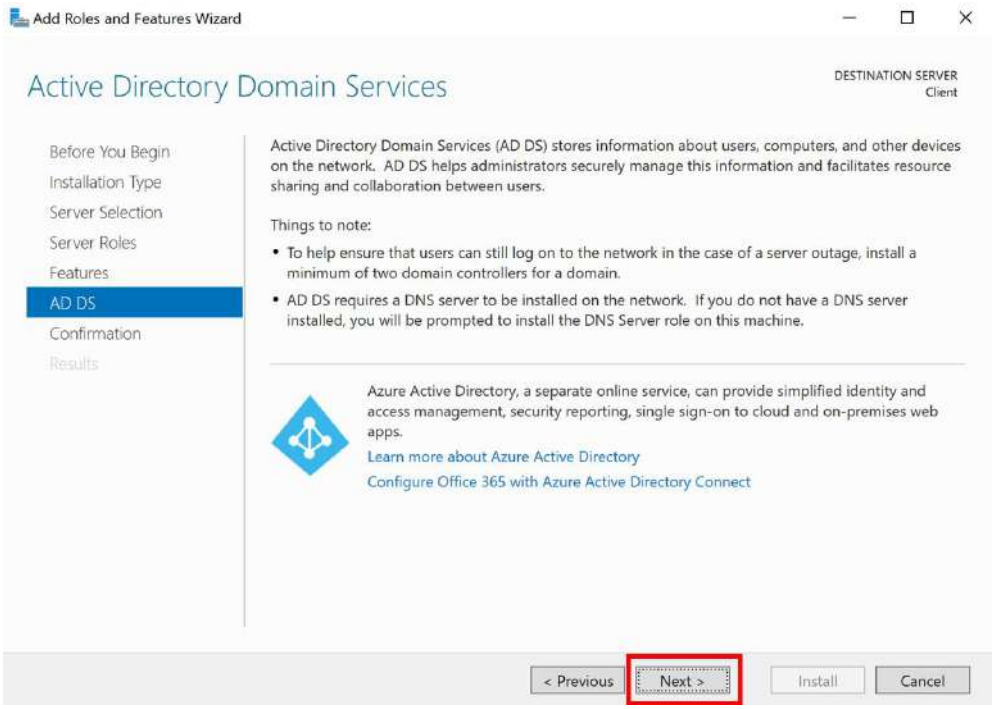


図 6.6.1-9 AD DS に関する注意事項

（9） インストールの確認

すべての設定が完了したら、表示される確認事項を再度確認し、「Install」をクリックしてインストールを開始します。

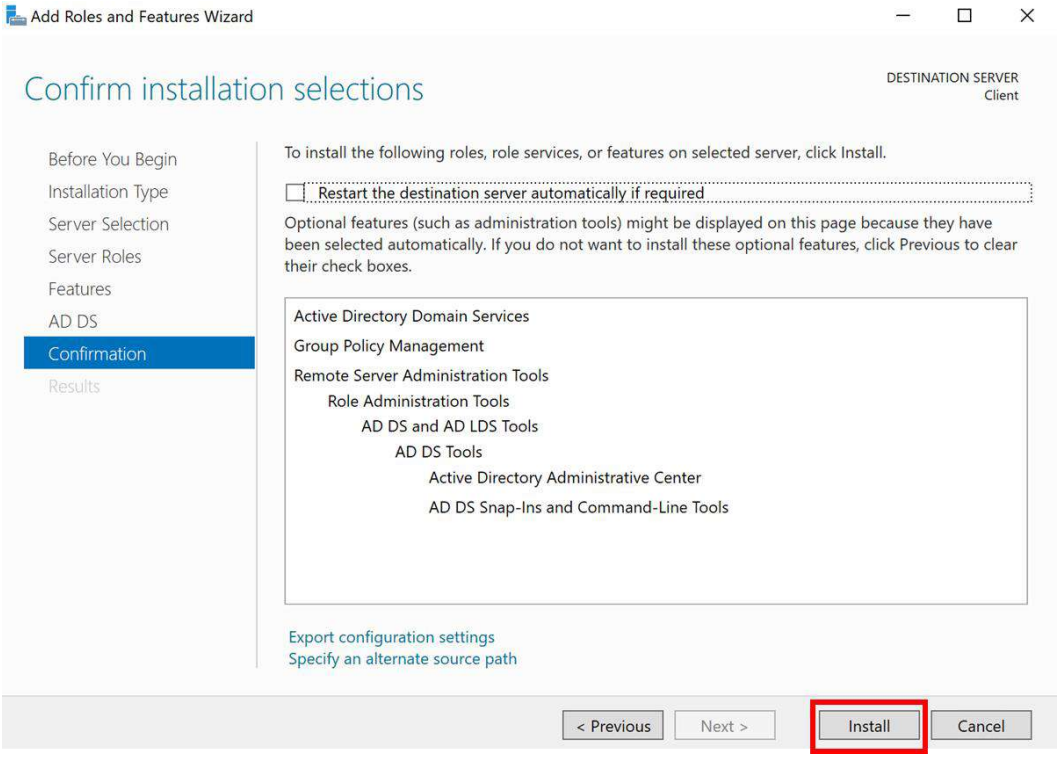


図 6.6.1-10 インストールの確認

6.6.2. DC (ドメインコントローラー) の新規構成

（1） ドメインコントローラーの設定

Server Manager を起動して、左側のペインで「AD DS」を選択します。
次に、右側のペインの画面右上部に表示される「More…」をクリックし、クライアントノードをドメインコントローラー（DC）に昇格させるオプションへ進みます。

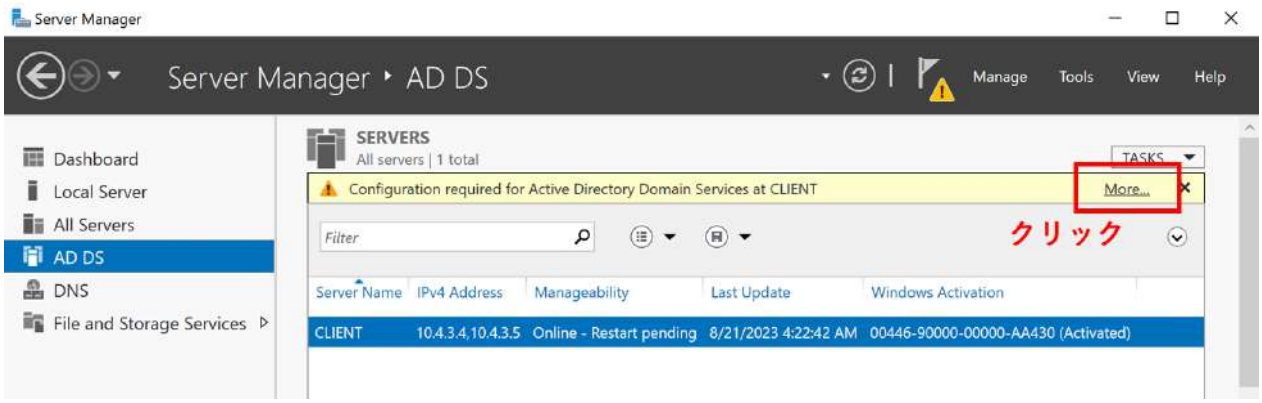


図 6.6.2-1 ドメインコントローラーの昇格画面にアクセス

（2） DC に昇格

画面の右上の「Promote this server to a domain controller...」というオプションをクリックします。

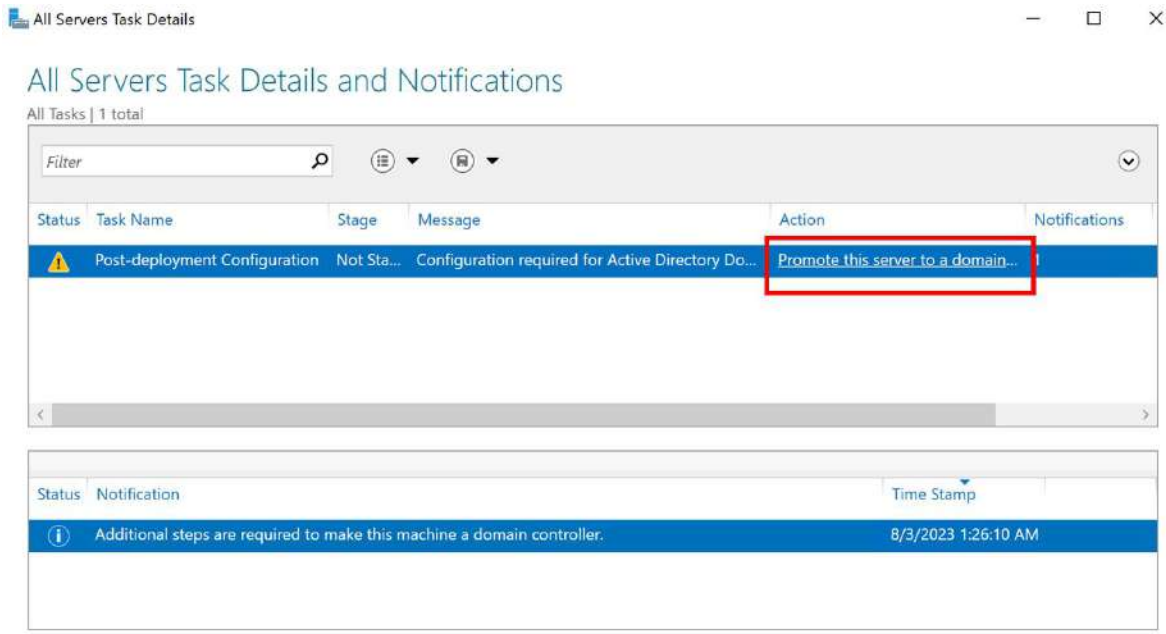


図 6.6.2-2 ドメインコントローラーに昇格

（3） DC の構成の設定

新しいドメインを作成するため、「Add a new forest」にチェックを入れます。ドメイン名を指定してから、「Next >」をクリックします。

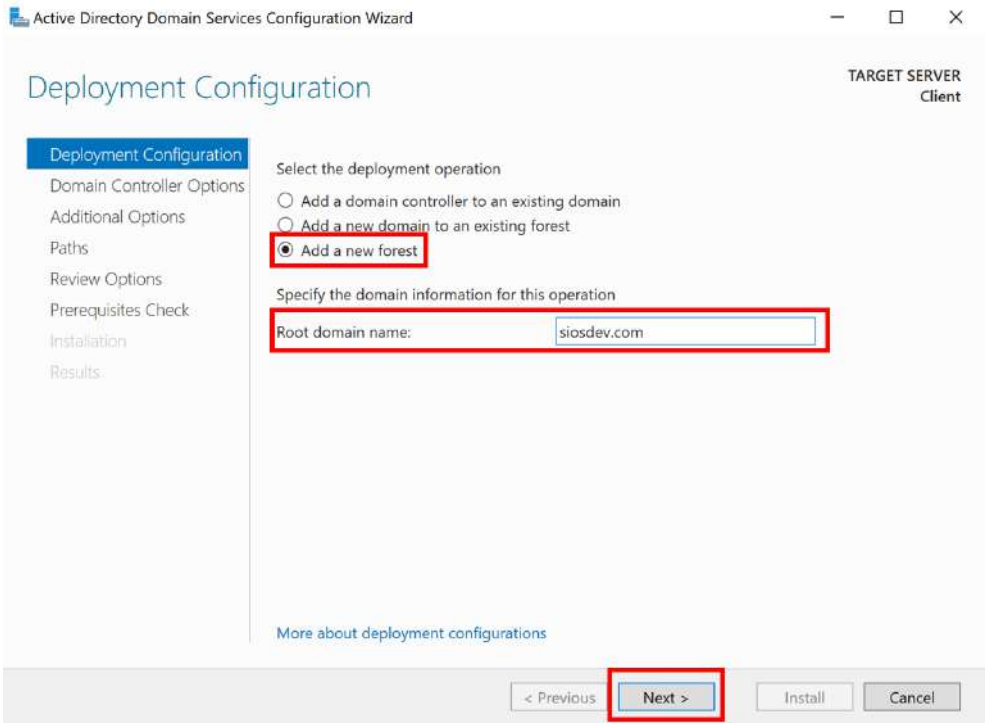


図 6.6.2-3 DC の構成の設定

（4） DC のオプション

「Password」フィールドには、ディレクトリサービス復元モード（DSRM）のパスワードを入力します。

入力後、「Next」をクリックします。

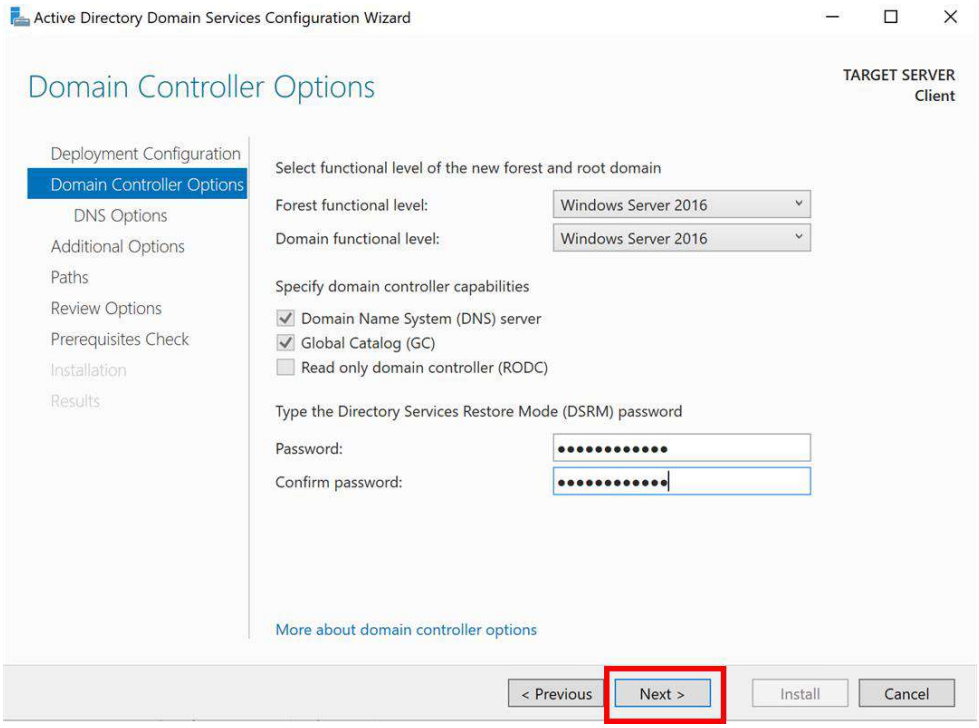


図 6.6.2-4 DC のオプション

（5） DNS オプション

この設定では DNS を設定しません。そのまま「Next >」をクリックします。

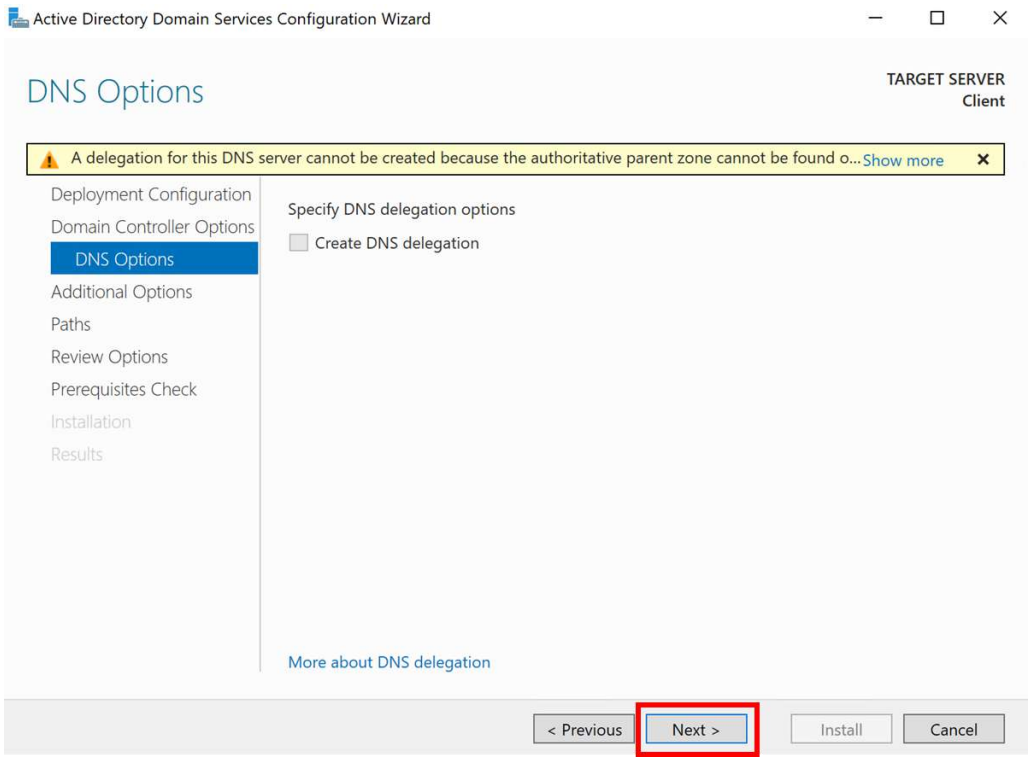


図 6.6.2-5 DC のオプション

（6） NetBIOS 名の設定

任意の NetBIOS 名を設定後、「Next >」をクリックします。

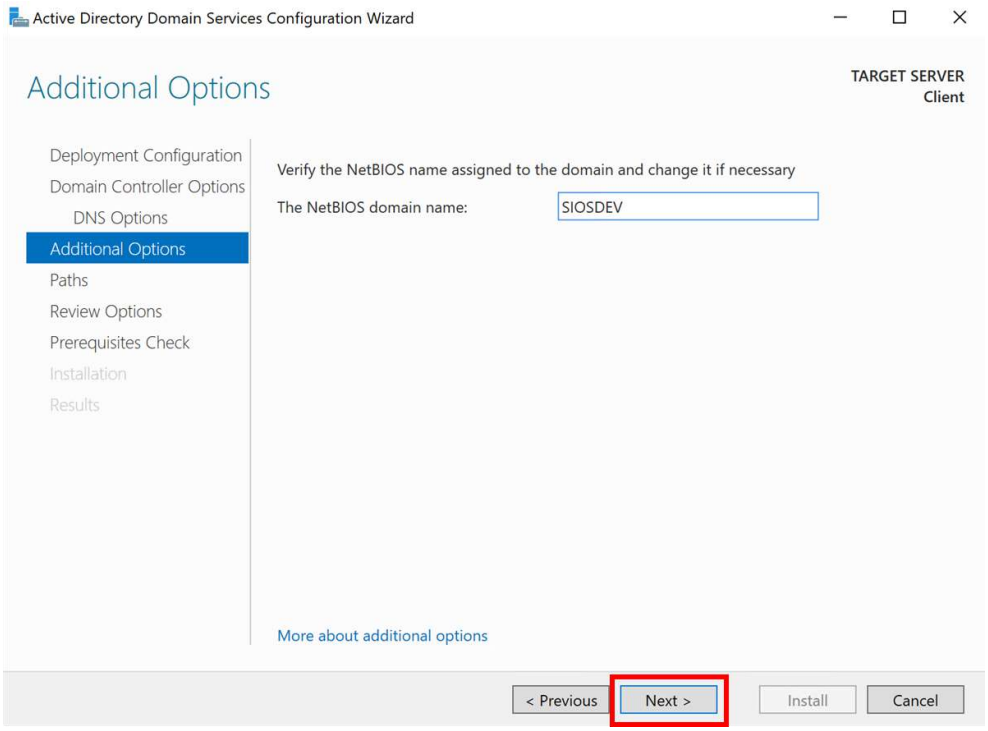


図 6.6.2-6 NetBIOS 名の設定

（7） 保存先パスの設定

AD DS のデータベースやログファイルを保存するディレクトリを指定します。
特別な要件がなければ、そのまま「Next >」をクリックします。

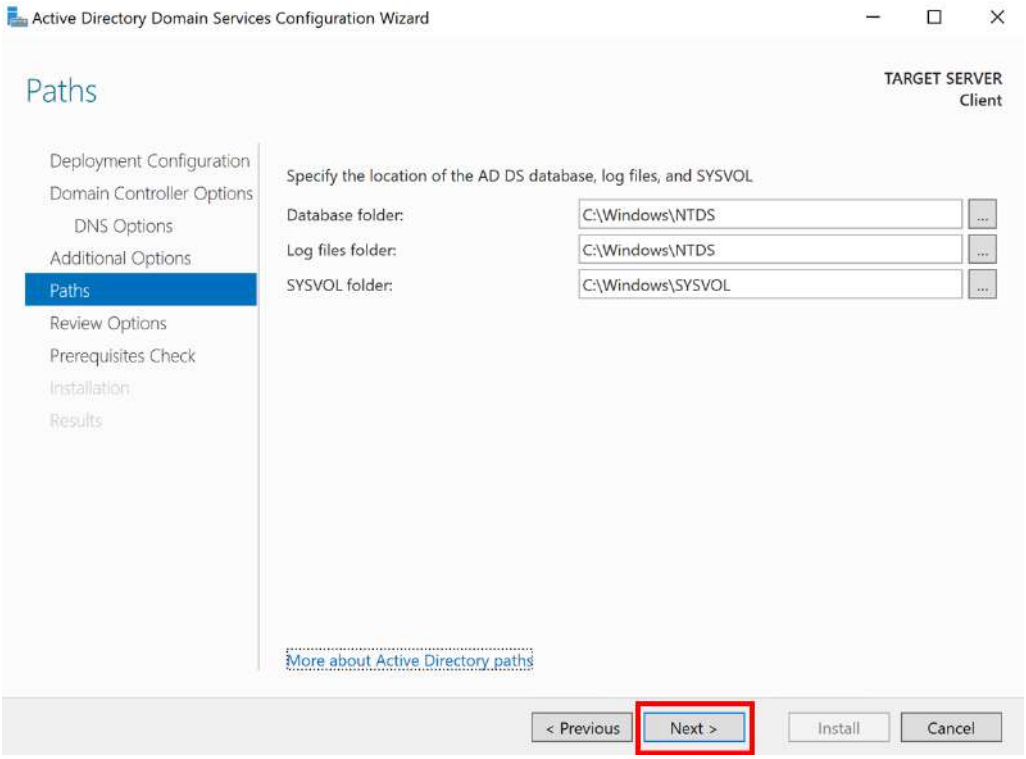


図 6.6.2-7 保存先パスの設定

（8） 設定の確認

DC の設定内容を確認する画面が表示されます。問題がなければ、「Next >」をクリックして次へ進みます。

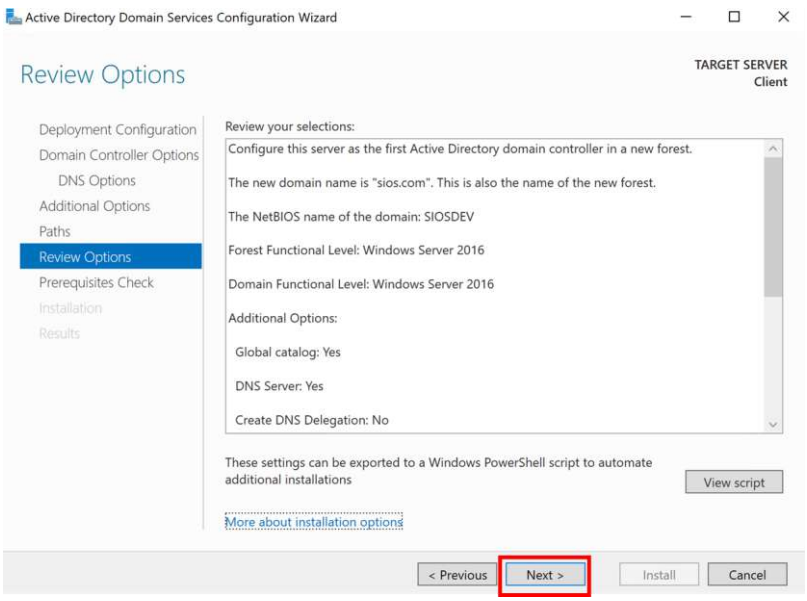


図 6.6.2-8 DC 設定の最終確認

（9） DC のインストール開始

「Install」ボタンをクリックすると、DC のインストールプロセスが始まります。

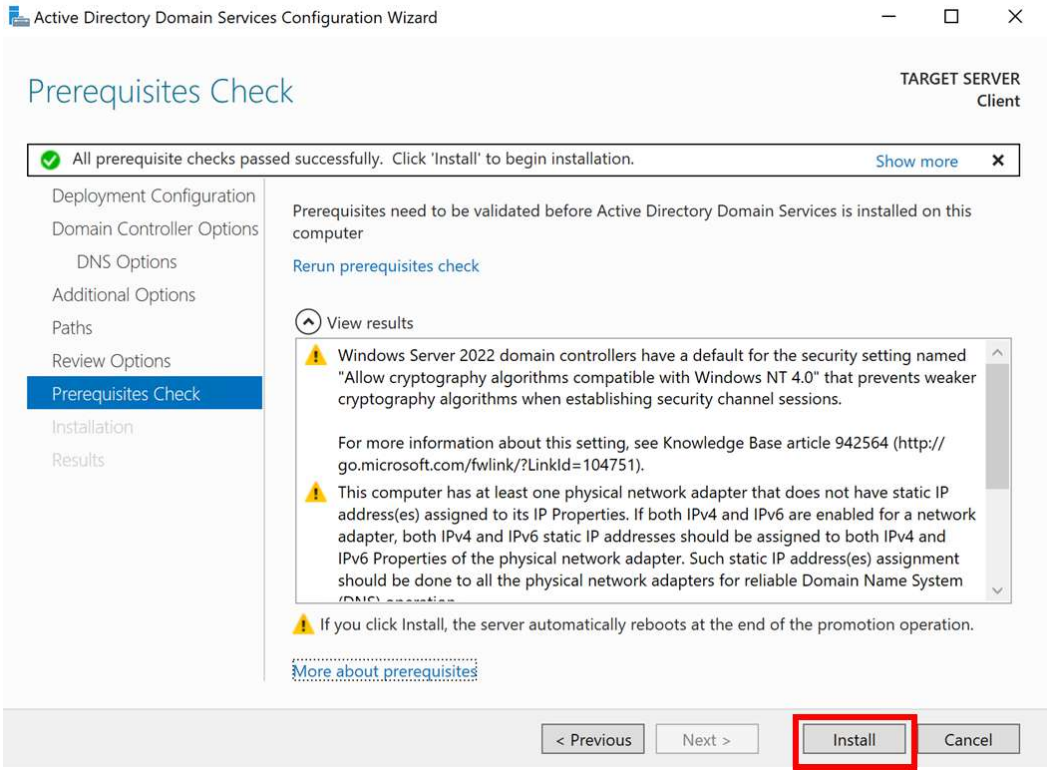


図 6.6.2-9 インストール開始

インストールが完了したら、システムは自動的に再起動します。

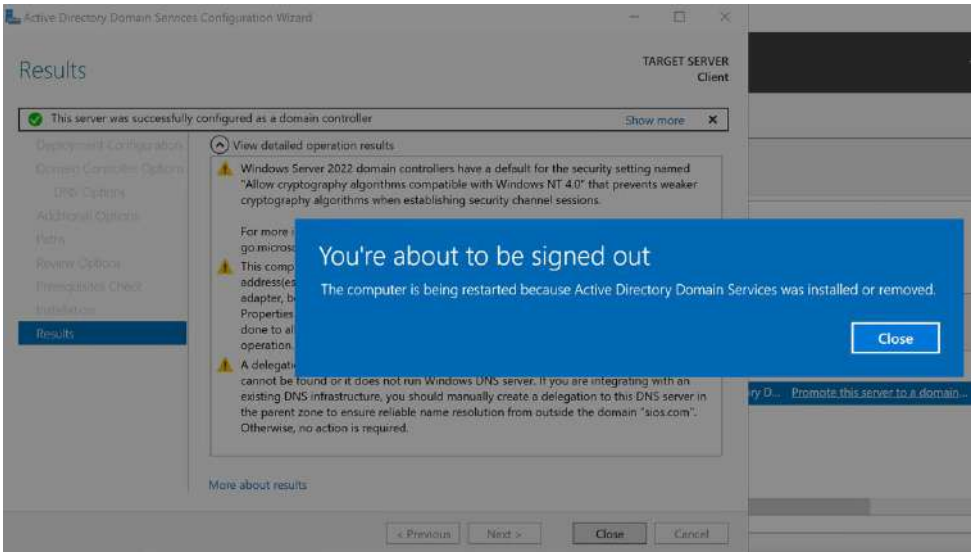


図 6.6.2-10 インストール開始

（10） DC 構成の確認

システムが再起動した後、Server Manager の「Local Server」タブを開き、Domain 情報を確認します。

Domain が先ほど設定したドメイン名に変更されていたら、DC の設定は成功です。

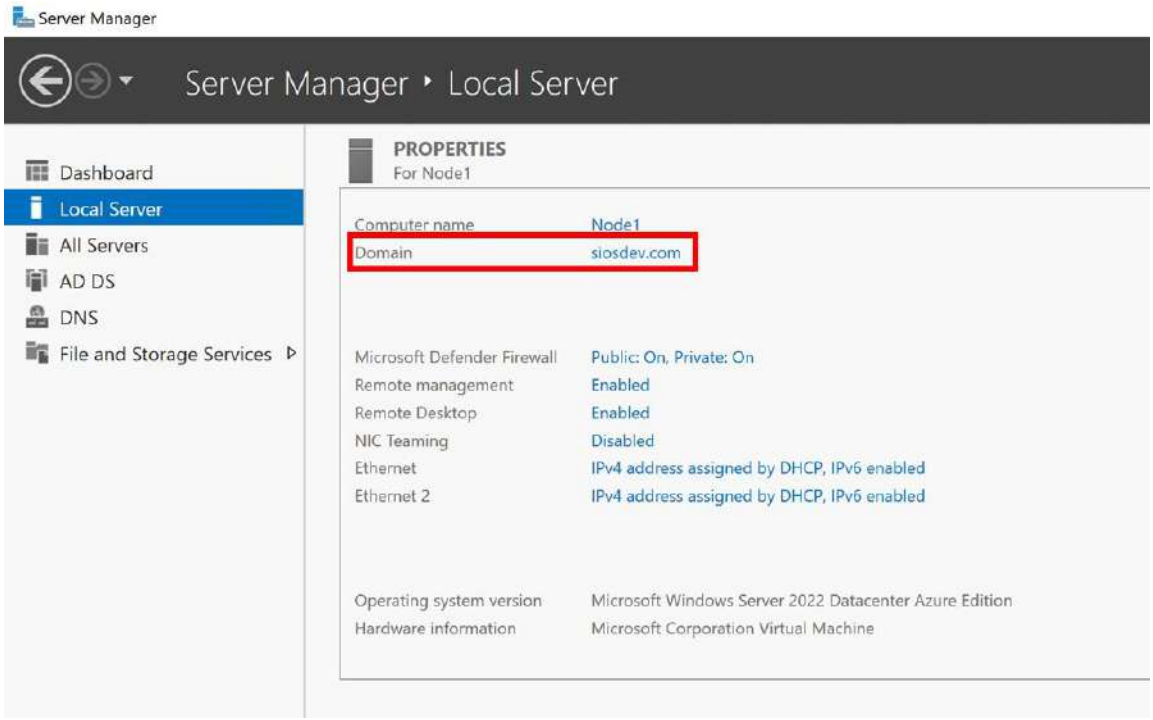


図 6.6.2-11 ドメインを確認

6.6.3. 稼働系と待機系をドメインに参加させる

（1） ネットワークステータスにアクセス

Windows の検索バーで「View network status and tasks」を検索して開きます。

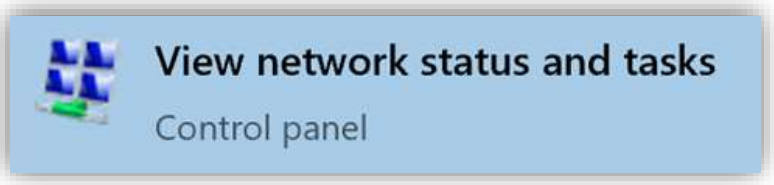


図 6.6.3-1 ネットワークステータスにアクセス

（2） NIC のネットワーク設定に移動

一覧から「Ethernet」を選択し、NIC のネットワーク設定画面を開きます。

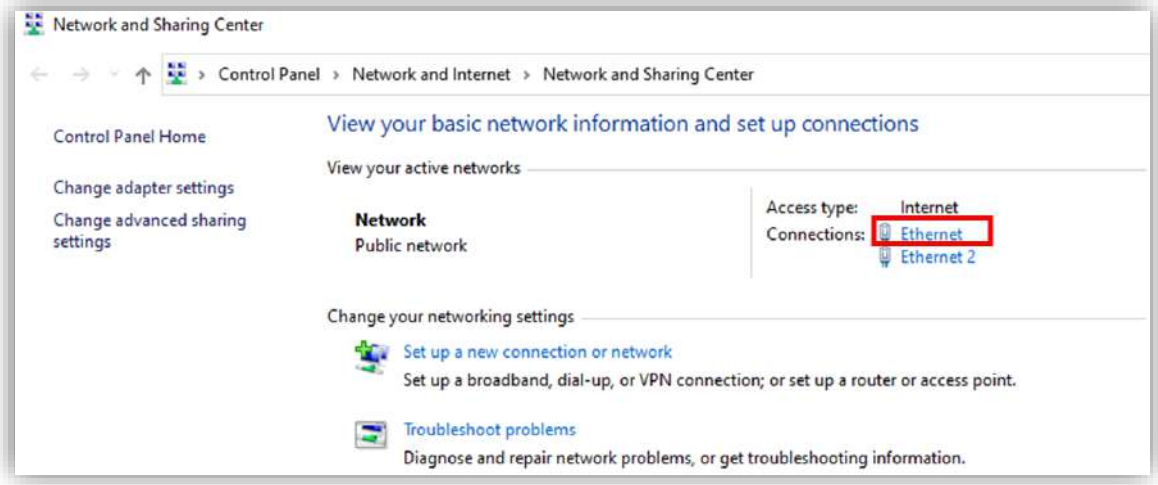


図 6.6.3-2 NIC のネットワークの設定画面

「Properties」をクリック後、「Internet Protocol Version 4 (TCP/IPv4)」を選び、開かれた画面の「Properties」をクリックして設定を開きます。

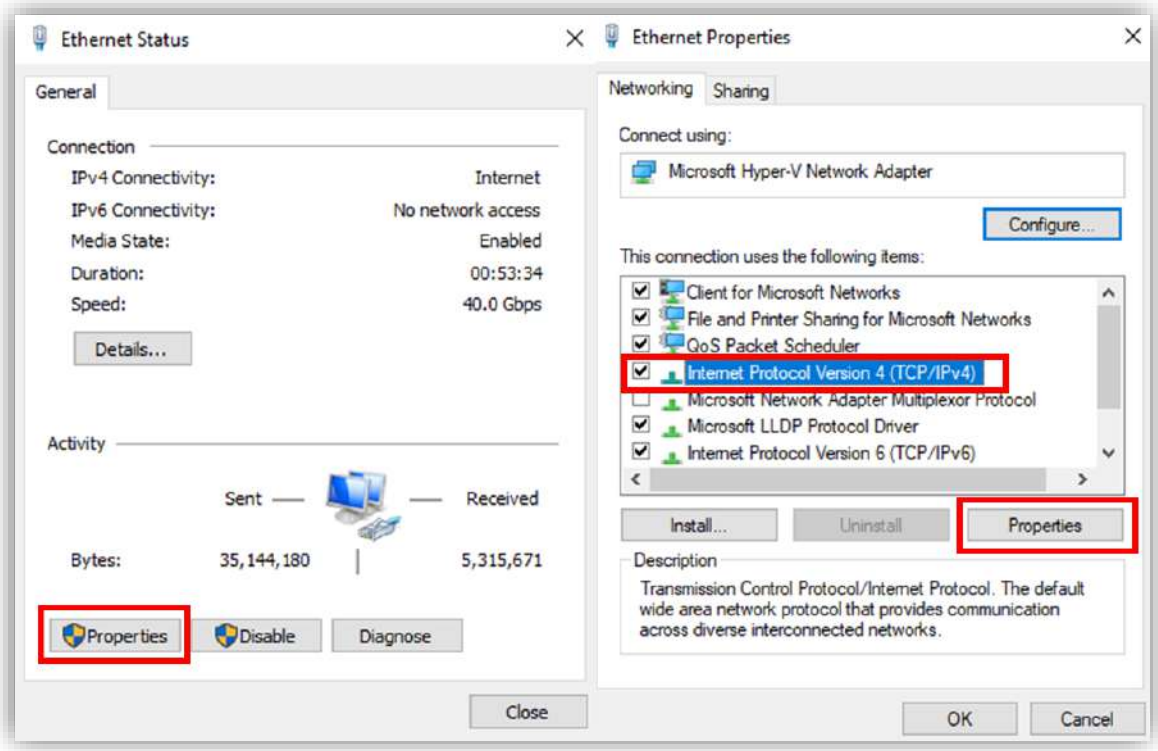


図 6.6.3-3 NIC のネットワーク設

（3） ドメイン情報の入力

「Preferred DNS server」のフィールドに、DC（ドメインコントローラ）の IP アドレスを入力します。

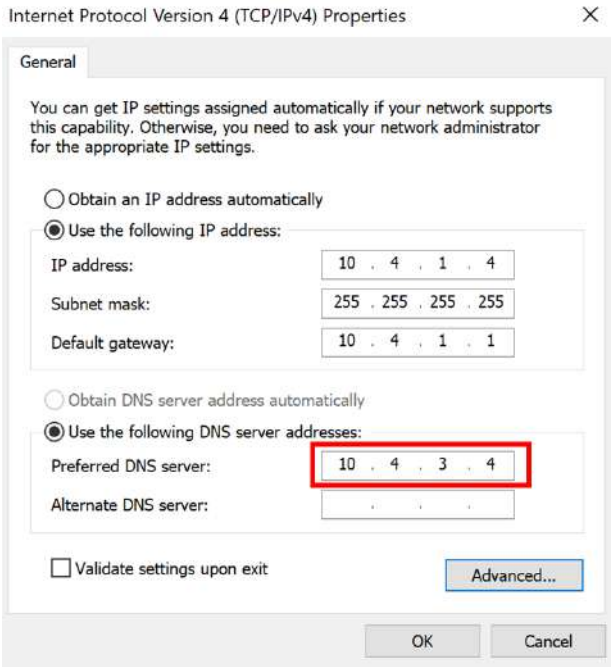


図 6.6.3-4 ドメイン情報の入力

6.6.4. ドメインに参加

次に、サーバマネージャーを使用して各ノードをドメインに参加させます。

（1） Server Manager を開く

Windows の検索バーで「Server Manager」を検索して開きます。

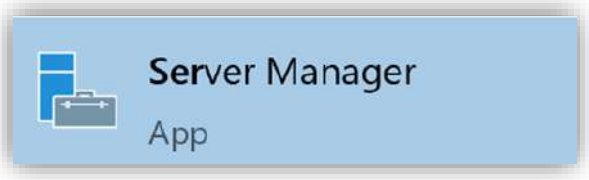


図 6.6.4-1 サーバマネージャーの管理画面を開く

（2） ローカルサーバの管理画面にアクセス

左側のメニューバーで「Local Server」をクリックして、ローカルサーバの設定画面に移動します。

現在の設定ではローカルの「Workgroup」が使用されています。その横に表示される「WORKGROUP」をクリックし、システムプロパティウィンドウを開きます。

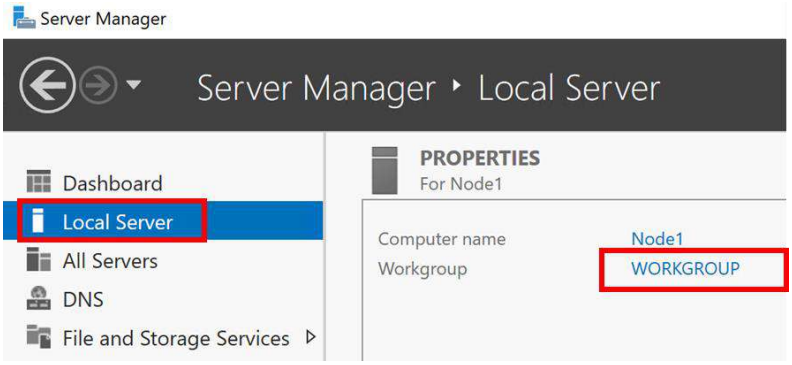


図 6.6.4-2 ローカルサーバの管理画面を開く

（3） Workgroup から Domain への変更

「Change...」をクリックして、サーバをドメインメンバーに変更します。

「Domain」のオプションにチェックを入れ、ドメイン名を入力後、「OK」をクリックします。

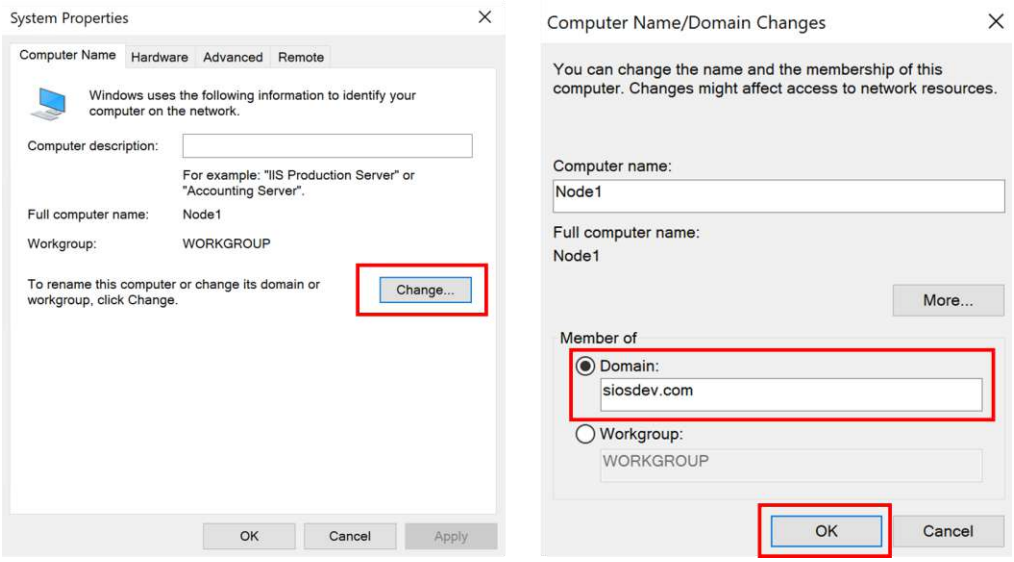


図 6.6.4-3 Workgroup メンバーからドメインメンバーに変更する

（4） ドメイン参加の認証

ドメインに参加するためのアカウント入力画面が表示されます。

ここで DC（ドメインコントローラ）に設定されたクライアントノードのアカウント情報を使用します。

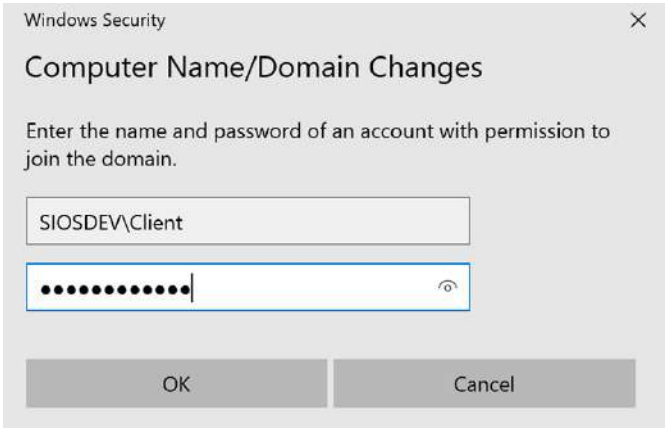


図 6.6.4-4 ドメイン参加

「Welcome to <ドメイン名> domain」と表示されるメッセージボックスが現れたら、ドメインへの参加が成功したと確認できます。

（5） オペレーティングシステム（OS）の再起動

ドメインの追加後には OS を再起動します。

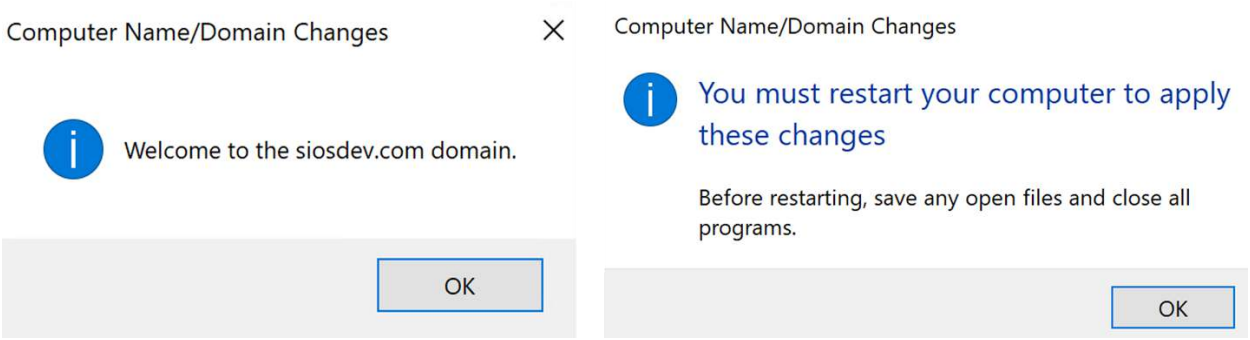


図 6.6.4-5 OS の再起動

これでドメインへの参加が完了しました。

待機系ノードに対しても同様の手順を適用してドメインを追加してください。

6.7. LifeKeeper 用の管理者アカウントの作成と追加

6.7.1. 管理者アカウントの作成

LifeKeeper 用の管理者アカウントは、ドメインコントローラ（DC）であるクライアントノードで作成します。

（1） AD のユーザ管理画面にアクセス

Windows アイコンを右クリックして、「Active Directory Users and Computers」を検索し、該当する管理画面を開きます。

図 6.7.1-1 AD のユーザ管理画面にアクセス

（2） 新しいユーザアカウントの作成

画面の左側ペインで「ドメイン名」を選択した後、「User」フォルダを右クリックします。「New」を選び、続いて「User」をクリックします。

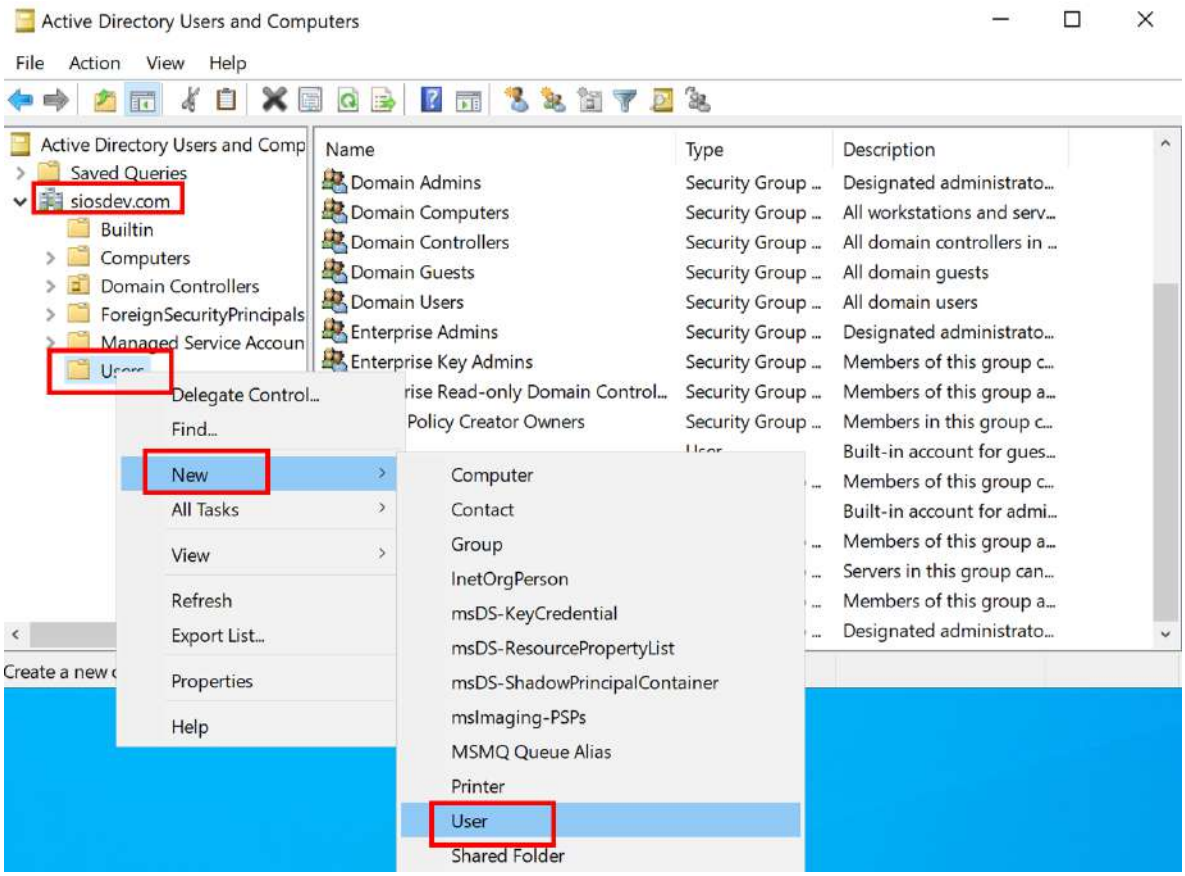


図 6.7.1-2 新しいユーザアカウントの作成

（3） 使用者名とユーザ名の入力

「First name」フィールドに使用者名（実名または任意の名前）を入力します。

「User logon name」フィールドにログインする際に使用するユーザ名を入力します。

これらの情報が正確に入力されたら、「Next >」をクリックして次に進みます。

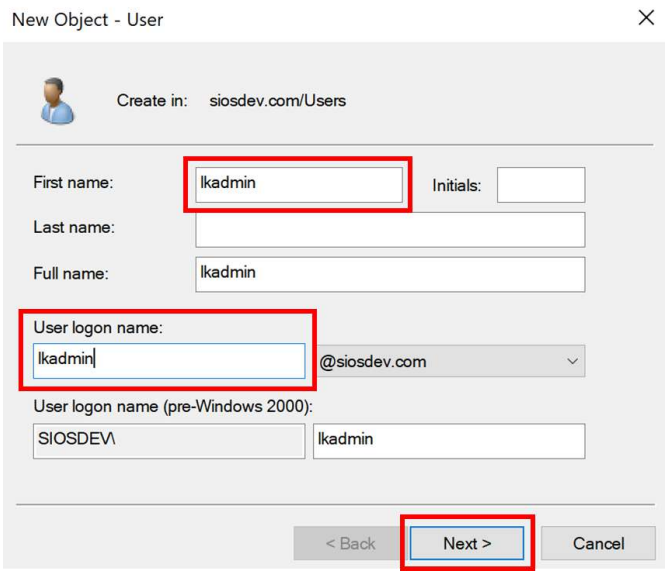


図 6.7.1-3 使用者名とユーザ名の入力

（4） パスワードの入力

パスワードを入力します。

入力できたら、「Next >」をクリックします。

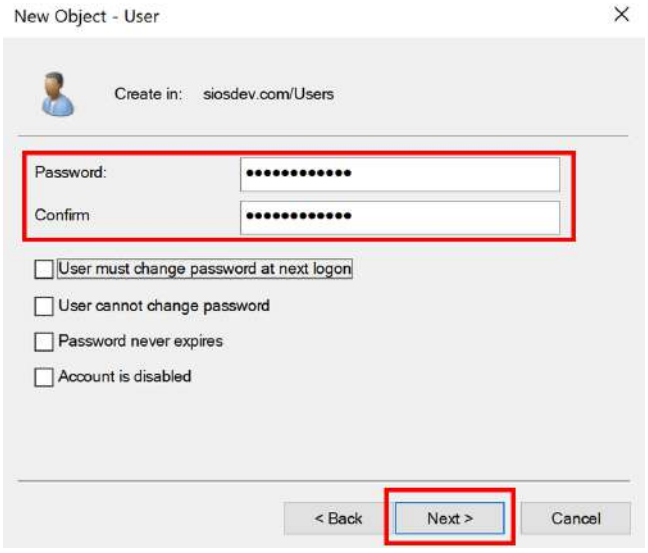


図 6.7.1-4　ユーザ名の入力

（5） 入力内容の確認

入力内容を確認します。

確認できたら、「Finish」をクリックします。

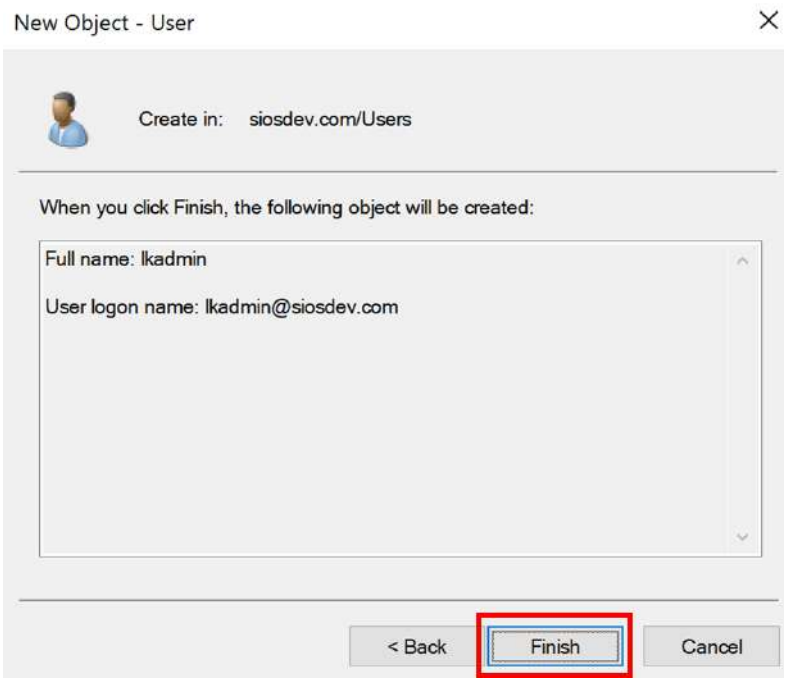


図 6.7.1-5　入力内容の確認

6.7.2. 作成したユーザを管理者アカウントに設定

（1）「Builtin」フォルダへの移動

先ほど作成したユーザを管理者アカウントに設定します。

左側のペインで「ドメイン名」を展開し、「Builtin」フォルダをクリックします。

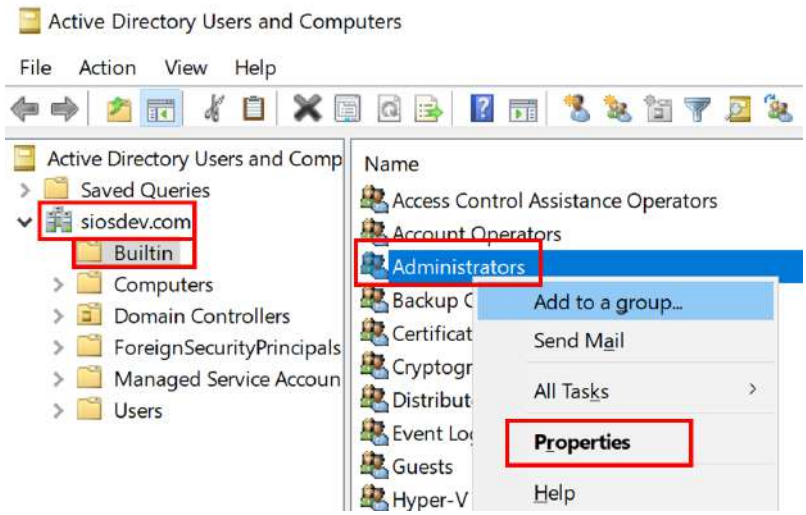


図 6.7.2-1　管理者グループの設定

（2）新規ユーザを管理者グループに追加

作成したユーザを管理者グループに追加します。

「Builtin」フォルダへの移動「Add」ボタンをクリックします。

「From this location」でドメイン名を選択します。

「Enter the object names to select」に、先ほど作成したユーザ名を入力します。 入力が完了したら、「OK」をクリックします。

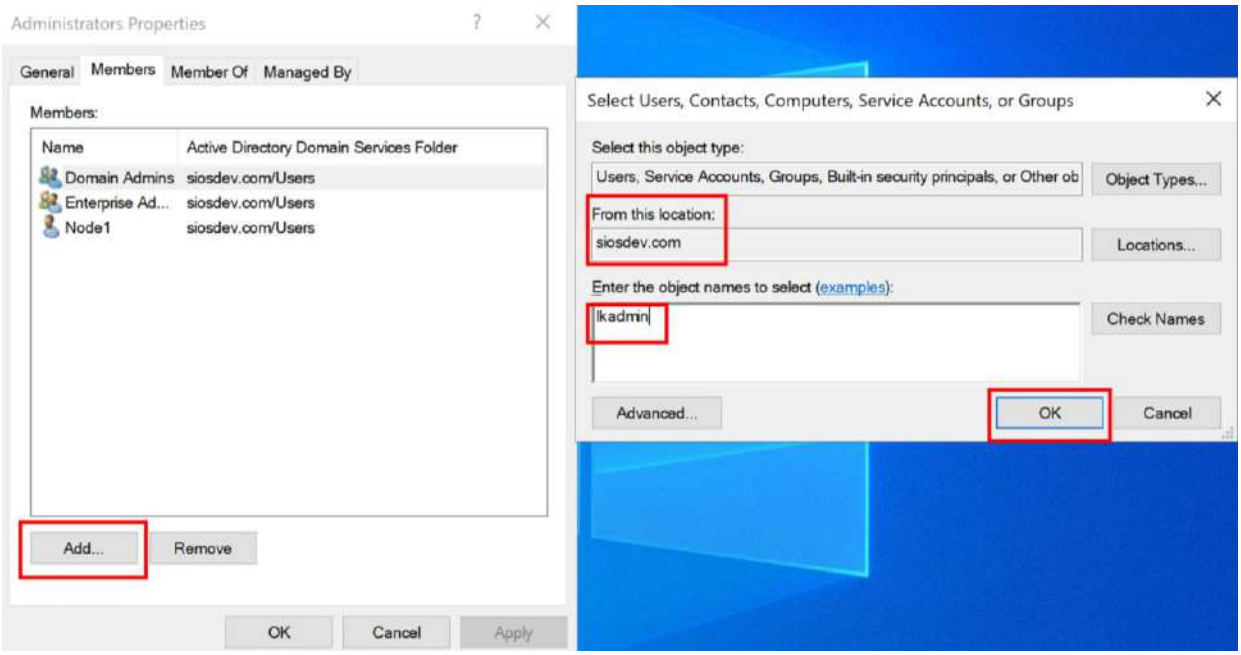


図 6.7.2-2　管理者グループに追加

（3） 管理者グループへの追加確認

追加されたユーザ名が「Administrators」グループに表示されているか確認します。

確認ができたら、「OK」をクリックして設定を完了します。

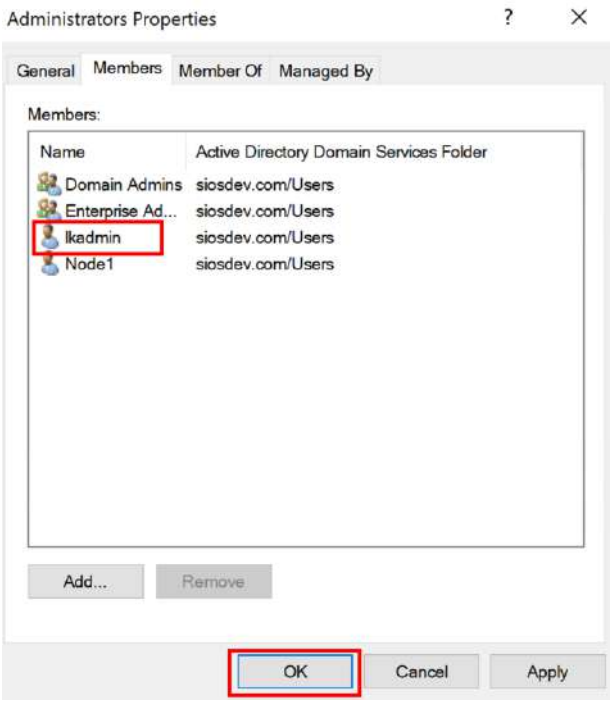


図 6.7.2-3 管理者グループに追加された

6.7.3. 待機系と稼働系ノードに管理者アカウントに追加

（1） ローカルユーザとグループの管理画面にアクセス

「Local Users and Groups (Local)」の管理画面に移動します。

（2） 「Administrators」グループ設定画面へ

「Groups」タブを選択し、その中から「Administrators」を右クリックして、「Properties」を選びます。

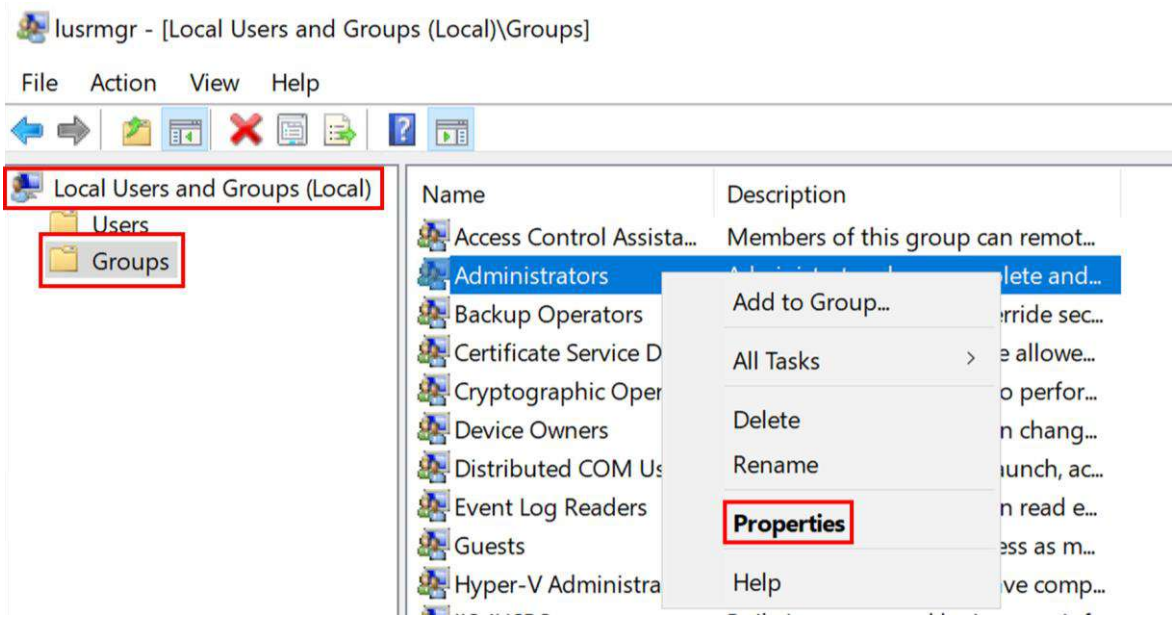


図 6.7.3-1 「Administrators」グループの設定

（3） 新規ユーザを管理者グループに追加

「Add」ボタンをクリックします。

「From this location」で、ドメイン名を選択します。

「Enter the object names to select」フィールドに作成したユーザ名を入力します。

入力後、「OK」ボタンをクリックします。

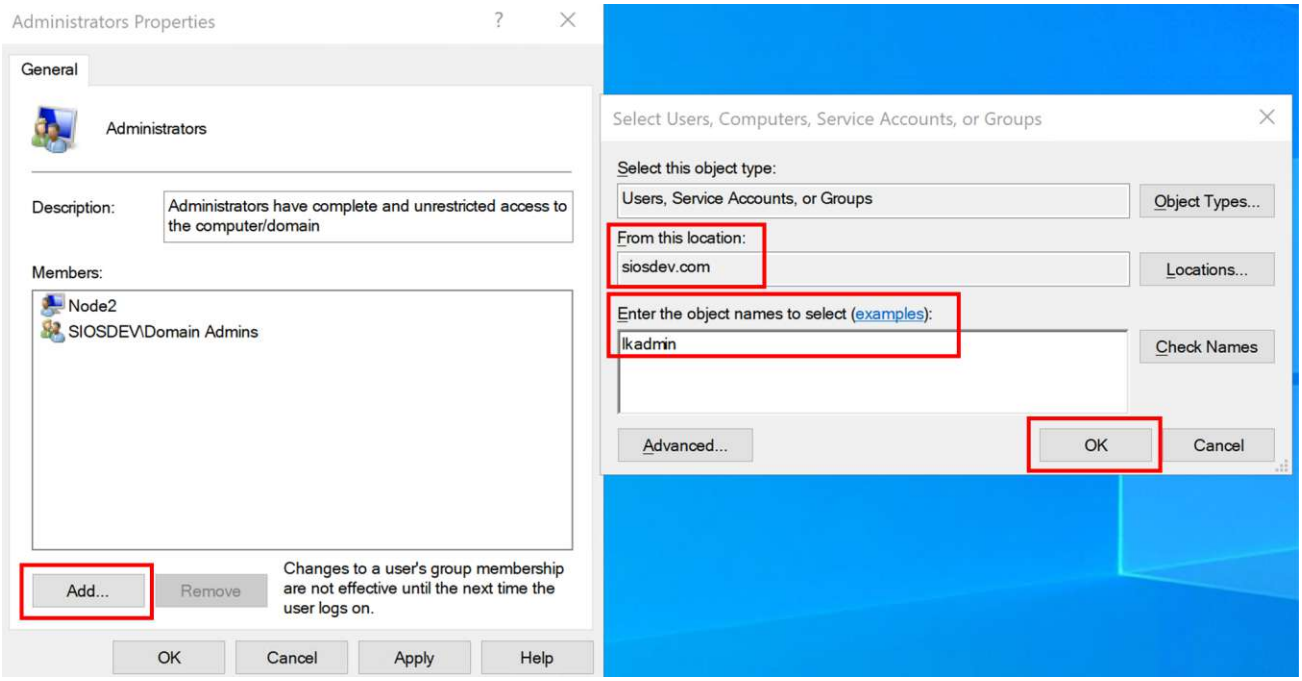


図 6.7.3-2 管理者グループへ新規ユーザの追加

「Administrators」グループ内に新規ユーザ名が表示されているか確認します。
確認ができたら、「OK」をクリックして設定を保存します。

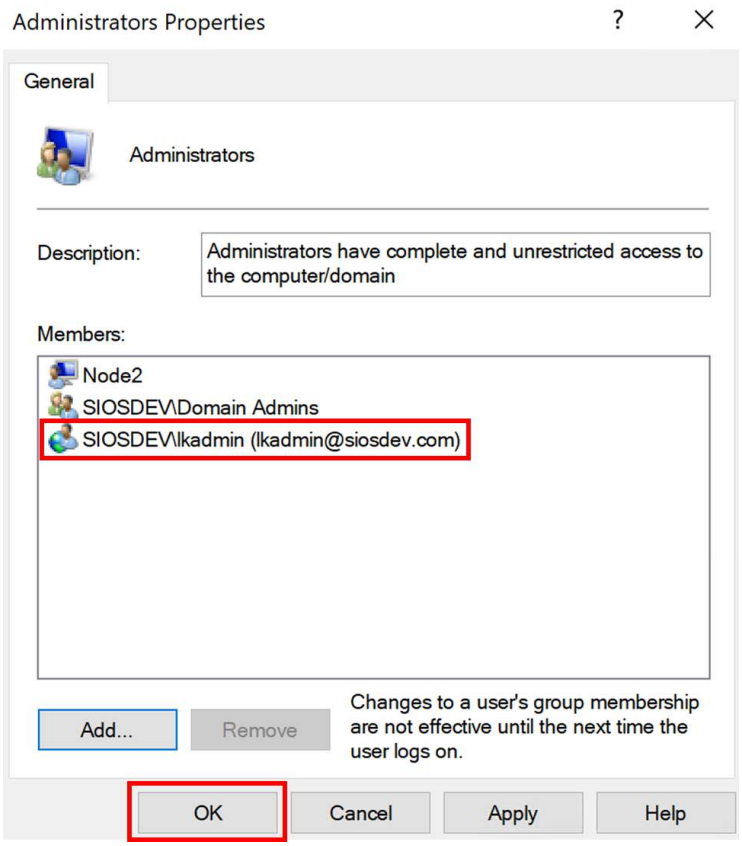


図 6.7.3-3 管理者グループへのユーザ追加確認

6.8. Azure 共有ファイルへの接続

6.8.1. Azure ファイル共有の AD DS 認証を有効にする

Azure 共有ファイルへの適切なアクセス制御を行うため、Azure ファイル共有の AD DS（Active Directory Domain Services）認証を有効にする手順を説明します。

詳細に関しましては以下の URL をご参照ください。

Azure ファイル共有の AD DS 認証を有効にする

→オプション 1 (推奨):AzFilesHybrid PowerShell モジュールを使用する

（1） AzFilesHybrid PowerShell モジュールのダウンロードと解凍

AzFilesHybrid PowerShell モジュールをダウンロードして解凍します。

URL：AzFilesHybrid モジュールで最新バージョンのダウンロード URL

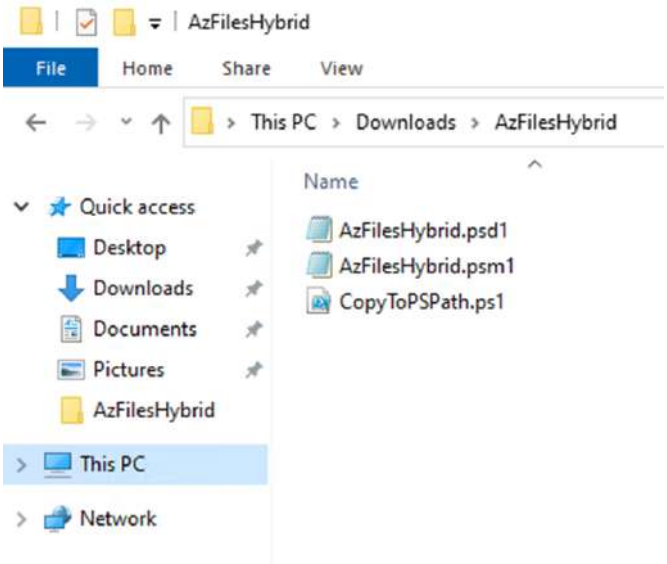


図 6.8.1-1 AzFilesHybrid PowerShell モジュール

（2） PowerShell 実行ファイルの作成

解凍したディレクトリ内で、AD 認証に使う PowerShell 実行ファイル「ADStorageAccountAuth.ps1」を作成します。

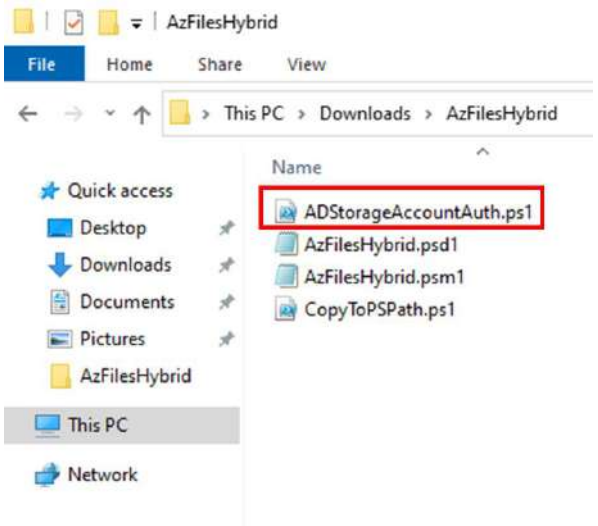


図 6.8.1-2 AD DS 認証用の PowerShell 実行ファイルの作成

以下の内容を ADStorageAccountAuth.ps1 に書き込みます。

URL：AzFilesHybrid モジュールで最新バージョンのダウンロード URL

図 6.8.1-3 実行ファイルの内容

（3） AD 認証用の PowerShell 実行ファイルの内容の書き換え

以下のパラメータを書き換えます。

パラメータと説明は以下の表にまとめました。

表 6.8.1 AD 認証用の PowerShell 実行ファイルの内容

$SubscriptionId	Azure サブスクリプション ID
$ResourceGroupName	リソースグループの名前
$StorageAccountName	AD に参加させるストレージアカウント名
$SamAccountName	AD によって識別されるオブジェクトのログオン名。**lkadmin を使用します。**
$DomainAccountType	ドメインアカウントタイプを指定します。ComputerAccount または ServiceLogonAccount
$OuDistinguishedName	OU（組織単位）の識別名を指定します。
$EncryptionType	Kerberos 認証に使用される暗号化アルゴリズムを指定します。AES256, RC4, AES256,RC4 のいずれかを使用できます。AES256 の使用が推奨されます。

PowerShell で OU の識別名を確認するコマンドは以下のようになります:

Import-Module ActiveDirectory

Get-ADOrganizationalUnit -Filter * | Select-Object Name, DistinguishedName

（4） Azure ファイル共有の AD DS 認証を行う

PowerShell を管理者権限で開きます。

解凍した AzFilesHybrid PowerShell モジュールのディレクトリに cd コマンドを用いて移動し、AD 認証用の PowerShell 実行ファイルを実行します。

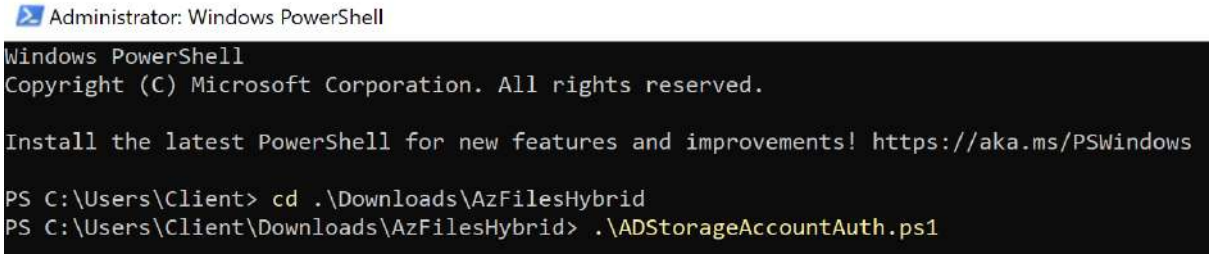


図 6.8.1-4 Azure ファイル共有の AD DS 認証を行う

（5） セキュリティの確認

認証処理中にセキュリティ確認画面が出ます。

「Add」ボタンをクリックして、信頼されるサイトリストにアクセスする URL を追加します。

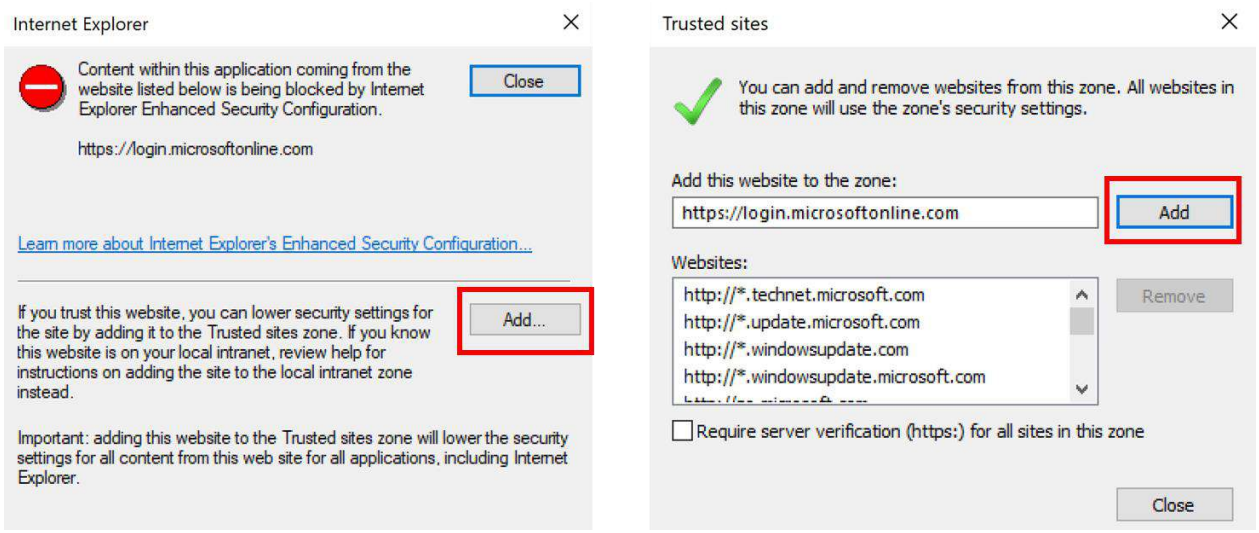


図 6.8.1-5 アクセスする URL を信頼されているサイトに追加

（6） Azure へのログイン画面

Azure へのログイン画面が開かれます。

すでに持っている Azure アカウントの認証情報を用いてログインします。

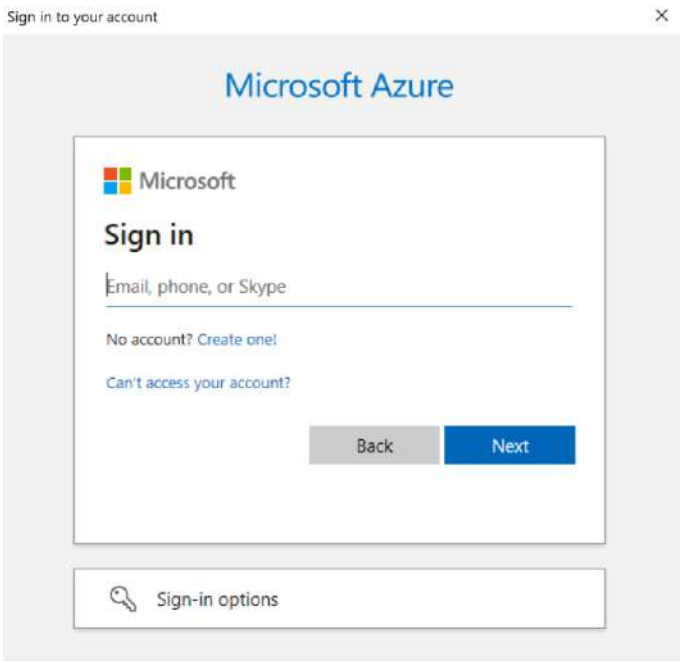


図 6.8.1-6 Azure へのログイン画面

（7） インストール完了

インストール完了画面が表示されます。

ここで「SMB share-level」が許可されていない場合があります。これは次のセクションで設定します。

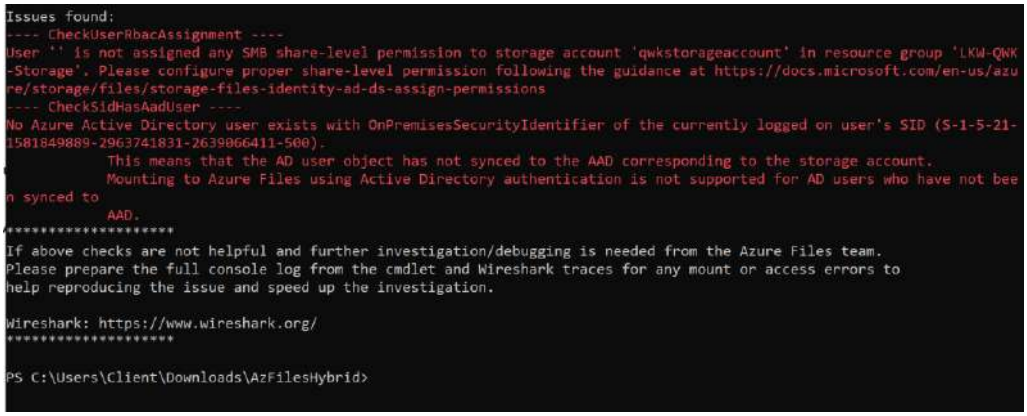


図 6.8.1-7 インストールの完了画面

6.8.2. Azure ファイル共有の共有レベルの設定

Azure ファイル共有の管理画面を開きます。

管理画面を開いて、確認します。「Active Directory (SMB)」が「構成済み」と表示

されていることを確認します。

図 6.8.2-1 ファイル共有の設定

「既定の共有レベルのアクセス許可」がデフォルトで「無効」になっている場合、これをクリックして設定します。

「手順 2」に「既定の共有レベルのアクセス許可」に「認証されているすべてのユーザとグループについてアクセス許可を有効にする」を選択します。

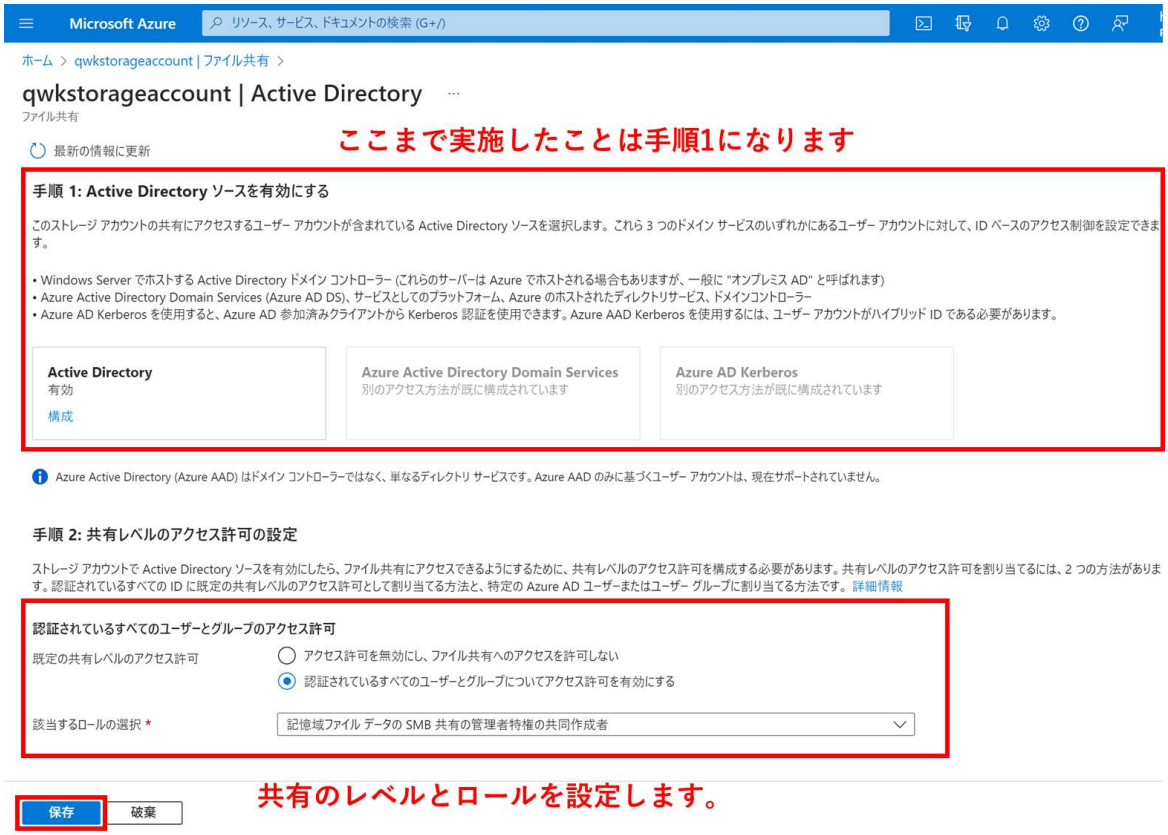


図 6.8.2-2 ファイル共有の設定

「既定の共有レベルのアクセス許可」は「有効」になっていれば、Azure ファイル共有の共有レベルの設定が完了です。

図 6.8.2-3 設定完了

6.8.3. Azure ファイル共有に接続する

（1） ファイル共有の管理画面にアクセス

ファイル共有の管理画面にアクセスします。

「接続」をクリックします。

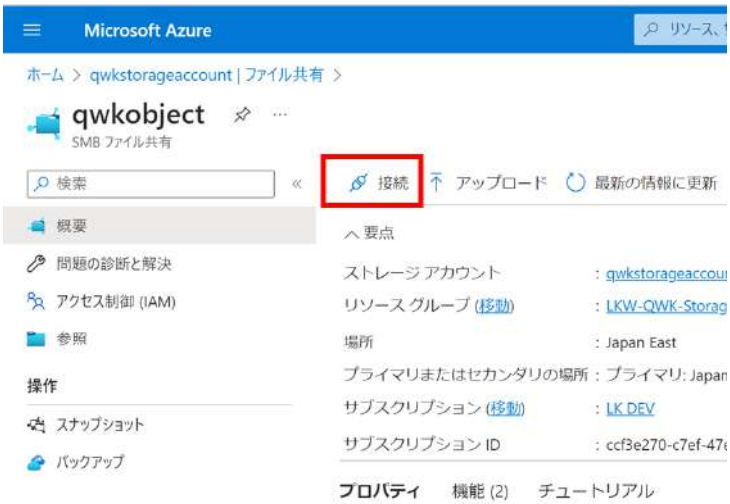


図 6.8.3-1 ファイル共有の管理画面

「ドライブ文字」を選択し、「認証方法」は「ストレージ アカウント キー」を指定します。

図 6.8.3-2 ドライブ文字と認証方法の設定

ファイル共有に接続する PowerShell の実行コマンドが表示されます。

右下のコピーアイコンをクリックして、コマンドをコピーします。

図 6.8.3-3 ファイル共有に接続する PowerShell コマンド

（2） PowerShell でコマンドの実行

PowerShell を管理者権限で開き、コピーしたコマンドをペーストして実行します。「Credential added successfully」が表示されれば、Azure ファイル共有に正しく接続できました。

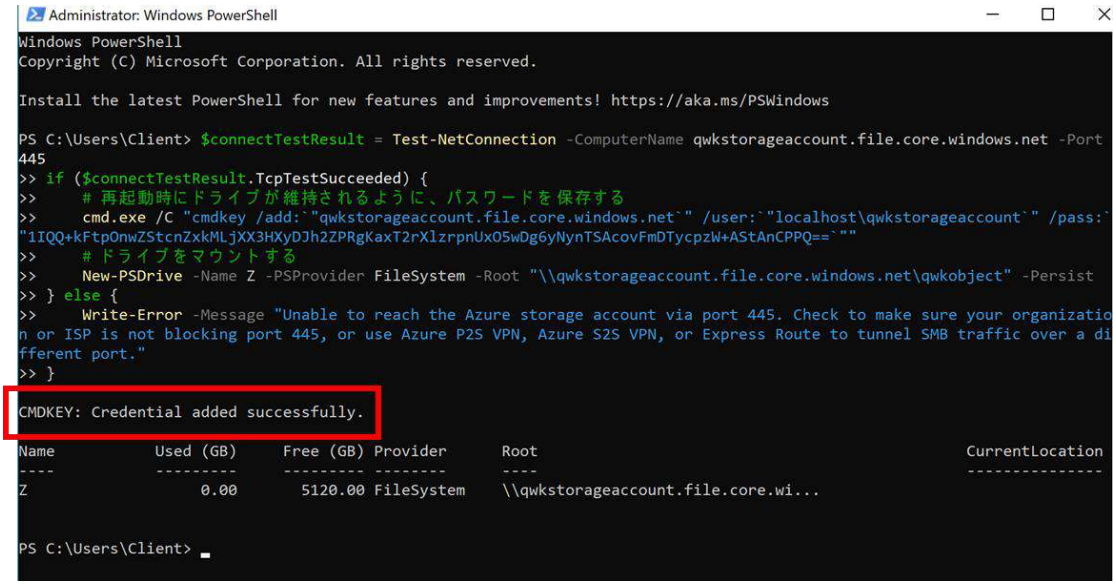


図 6.8.3-4 ファイル共有に接続する PowerShell コマンドの実行

エクスプローラーを開き、Azure ファイル共有に接続されていることを確認します。確認できたら、設定が完了です。

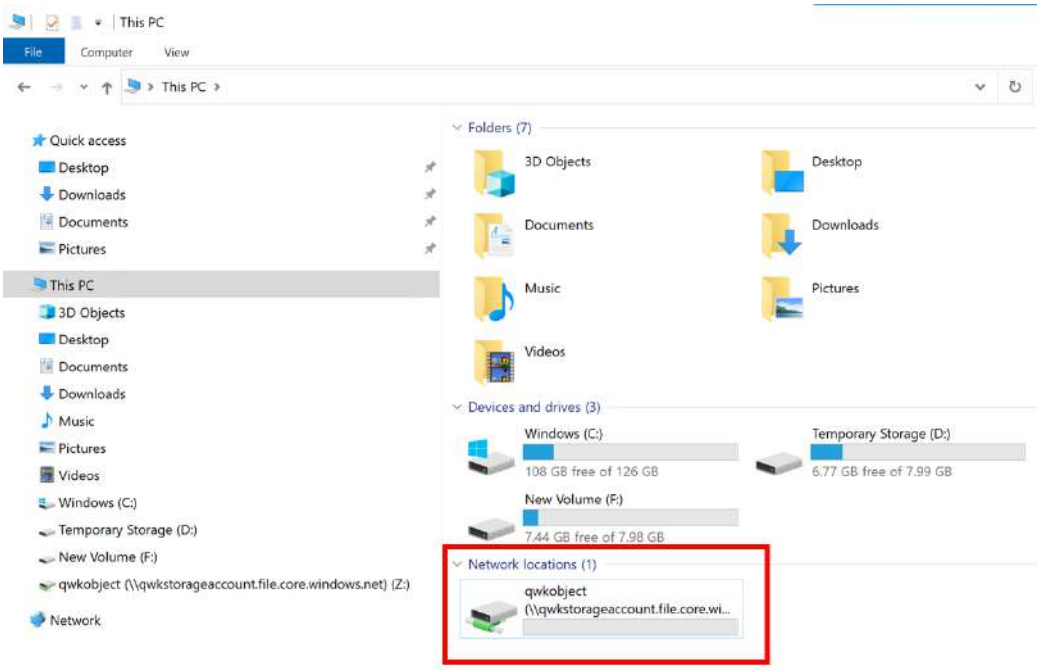


図 6.8.3-5 ファイル共有に接続完了

7. LifeKeeper/DataKeeper、SQL Server のインストール

7.1. インストールメディアの準備

本ガイドでは、LifeKeeper for Windows v8.9.2 および DataKeeper for Windows v8.9.2 を使用してクラスタを構築する方法を解説します。

（1） クライアントノードにインストールメディアとライセンスを準備

LifeKeeper と DataKeeper のインストールメディアおよびライセンスをクライアントノードに保存します。

RDP のドライブアクセス機能を利用するか、ダウンロードサイトから直接取得してください。

図 7.1-1 クライアントノードでのインストールメディアとライセンスの配置

稼働系ノードからクライアントノードのディスクにアクセスする場合、

パスは以下のようになります：

This PC¥C:¥AZURE-LKW-CLIENT¥Users¥Client¥Desktop

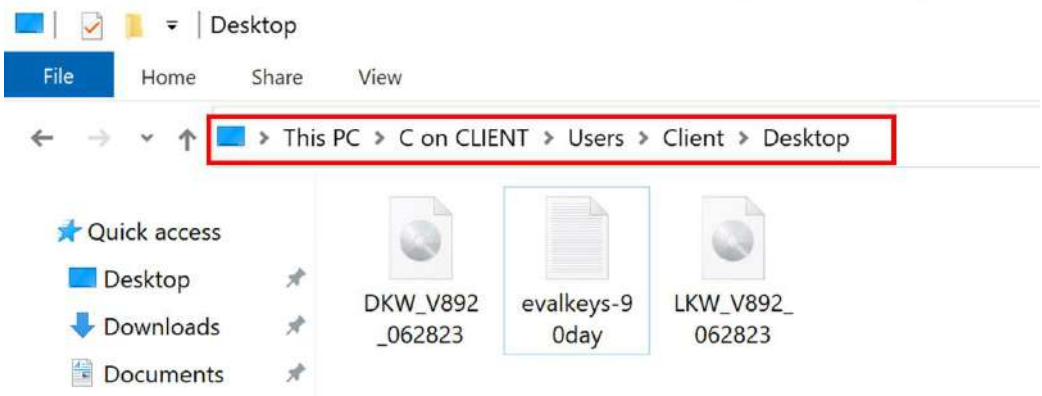


図 7.1-2 稼働系ノードからクライアントノードへのアクセスパス

（2） インストールメディアとライセンスを稼働系ノードにコピー

LifeKeeper と DataKeeper のインストールメディアとライセンスファイルを稼働系ノードに転送します。このガイドでは、それらをデスクトップにコピーします。

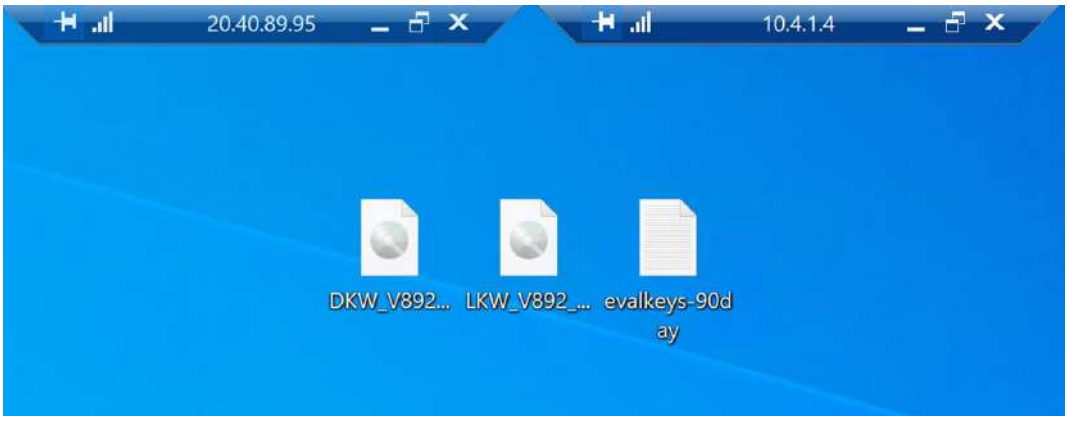


図 7.1-3 稼働系ノードでのインストールメディアとライセンスの配置

7.2. LifeKeeper のインストール手順

LifeKeeper のインストール手順について説明します。

（1） LifeKeeper のインストールファイルの実行

LifeKeeper のインストールファイルは以下のパスにあります。

<LifeKeeper のイメージファイルのパス>¥Core¥LK-8.9.2-Setup

この実行ファイルをダブルクリックして開きます。

（2） ライセンス契約書の確認と承認

インストールの進行画面が表示されます。「Next」をクリックして先に進んでください。

ライセンス契約書の内容をよく読み、「Yes」をクリックして同意します。

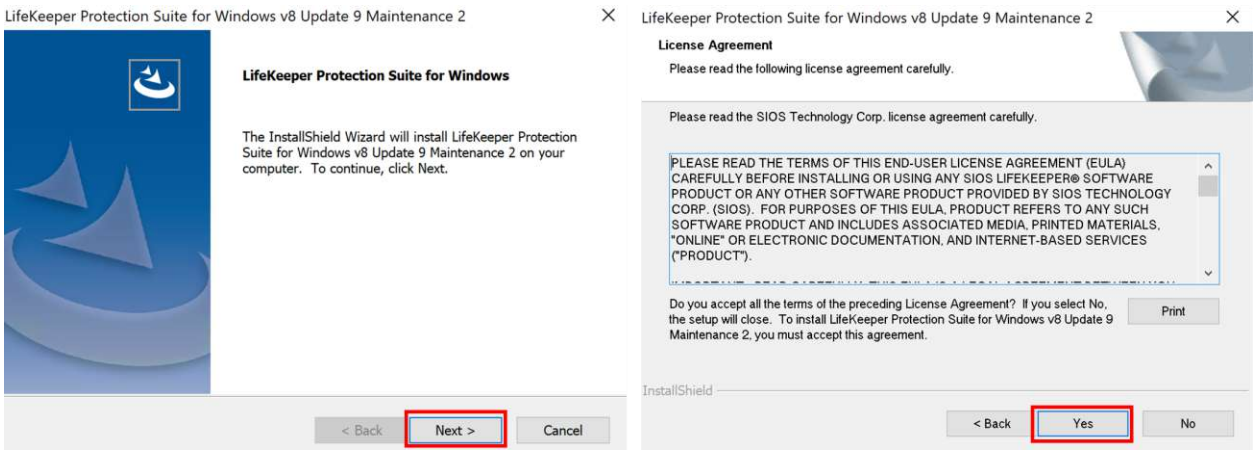


図 7.2-1 ライセンス契約書の確認と承認

（3） インストール機能の選択

インストール機能の選択画面で、「SIOS DataKeeper for Windows」にチェックマークを入れます。

この設定を選択すると、LifeKeeper のインストールが完了した後、自動的に DataKeeper のインストールが始まります。

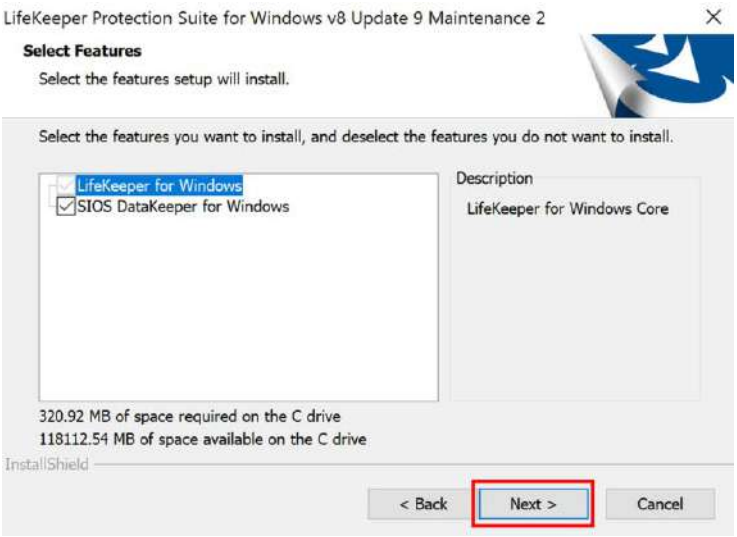


図 7.2-2 インストール機能の選択

（4） インストールファイルのコピー

インストールに必要なファイルが自動的にコピーされます。

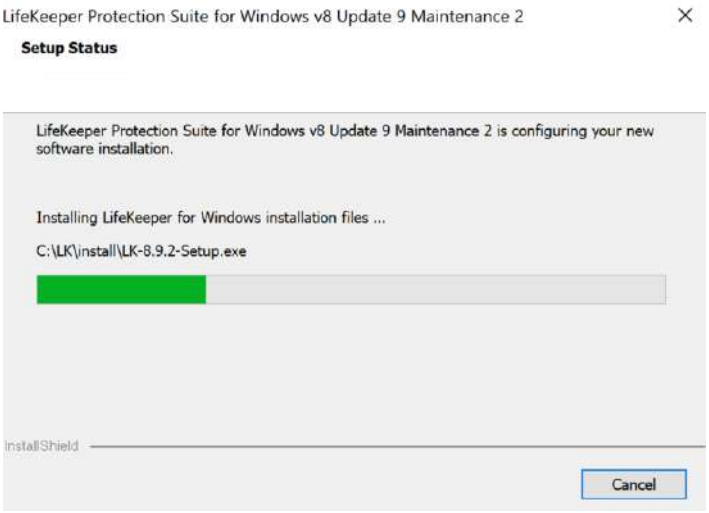


図 7.2-3 インストールファイルのコピー

（5） インストール先のパスの設定

インストール先のディレクトリを必要に応じて変更できます。

このガイドでは、デフォルトのディレクトリ C:¥LK にインストールします。

設定が完了したら、「Next」ボタンをクリックします。

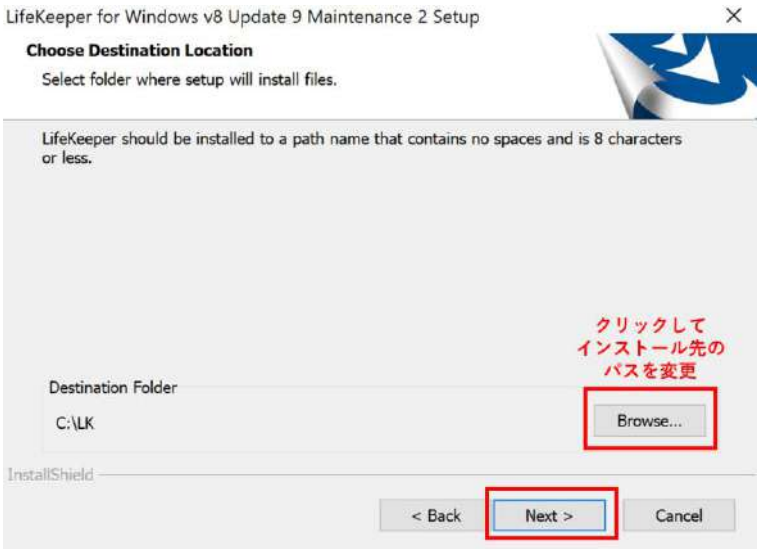


図 7.2-4 インストール先のパスの設定

（6） インストールタイプの選択

インストールするコンポーネントを選択する画面が表示されます。

個別のツールを選択してインストールしたい場合は、「Custom」を選択してください。

このガイドでは、デフォルト設定である「Typical」を選び、「Next」をクリックします。

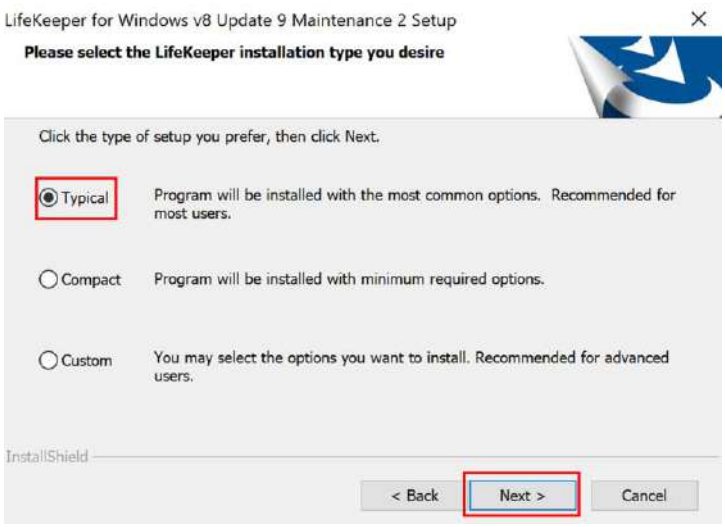


図 7.2-5 インストールタイプを選択する

（7） LifeKeeper GUI の表示速度に関する注意

このステップでは、オペレーティングシステムの NIC 設定によっては、LifeKeeper GUI の表示が遅くなる可能性について説明されます。

もし、インストール後に LifeKeeper GUI の表示が遅いと感じた場合、LifeKeeper for Windows のオンラインドキュメント内の「GUI ネットワーク関連 – Windows プラットフォーム上の長期接続遅延」を参照して設定を行ってください。

「OK」ボタンをクリックして進めます。

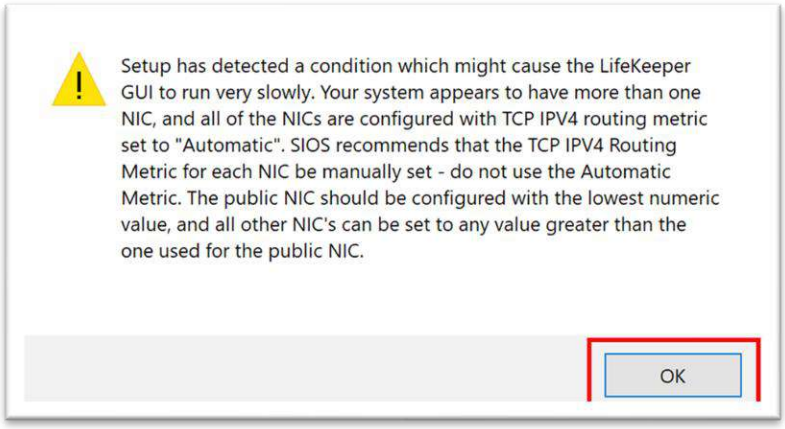


図 7.2-6 LifeKeeper GUI の表示速度に関する画面

（8） ポート解放を許可

ファイアウォールの設定画面が開き、必要なポートを解放するための許可を求められます。

「Yes」をクリックして許可してください。

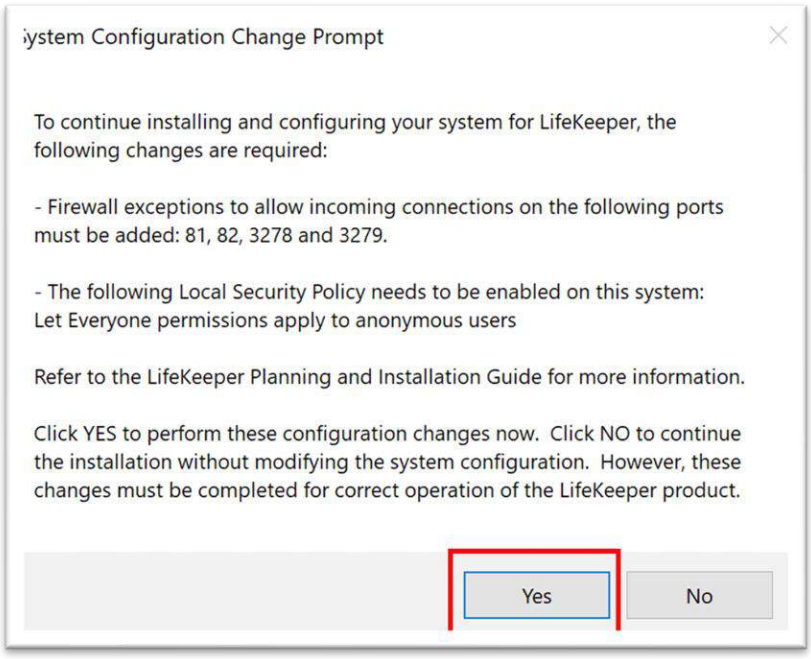


図 7.2-7 ポート解放を許可

（9） DHCP Media Sense for TCP/IP の無効化

DHCP Media Sense for TCP/IP を無効にする必要があります。

「Yes」をクリックして、この機能を無効にしてください。

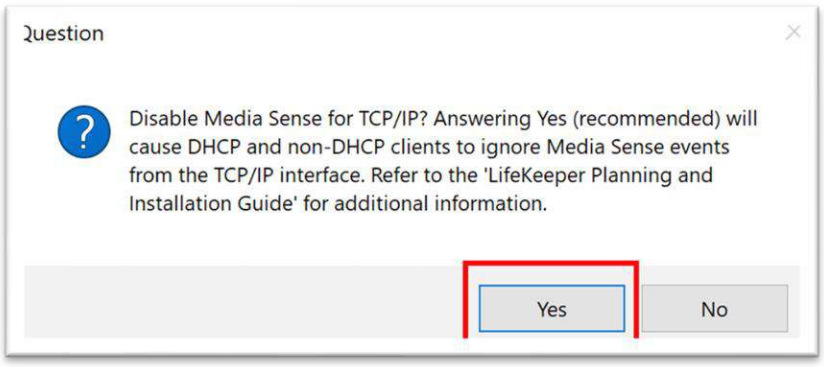


図 7.2-8 DHCP Media Sense for TCP/IP の無効化

（10） Distributed Link Tracking Client サービスの無効化

Distributed Link Tracking Client サービスを無効にするための許可を求める画面が表示されます。

「Yes」をクリックして、このサービスを無効にします。

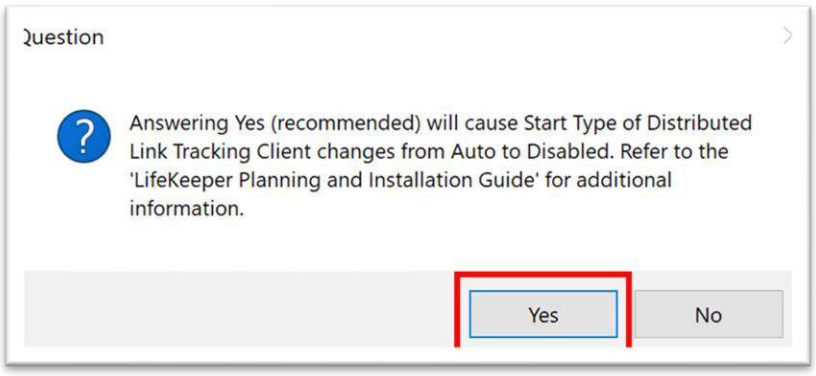


図 7.2-9 Distributed Link Tracking Client サービスの無効化

（11） LifeKeeper のインストールが開始

以上の設定が完了したら、LifeKeeper のインストールが開始されます。

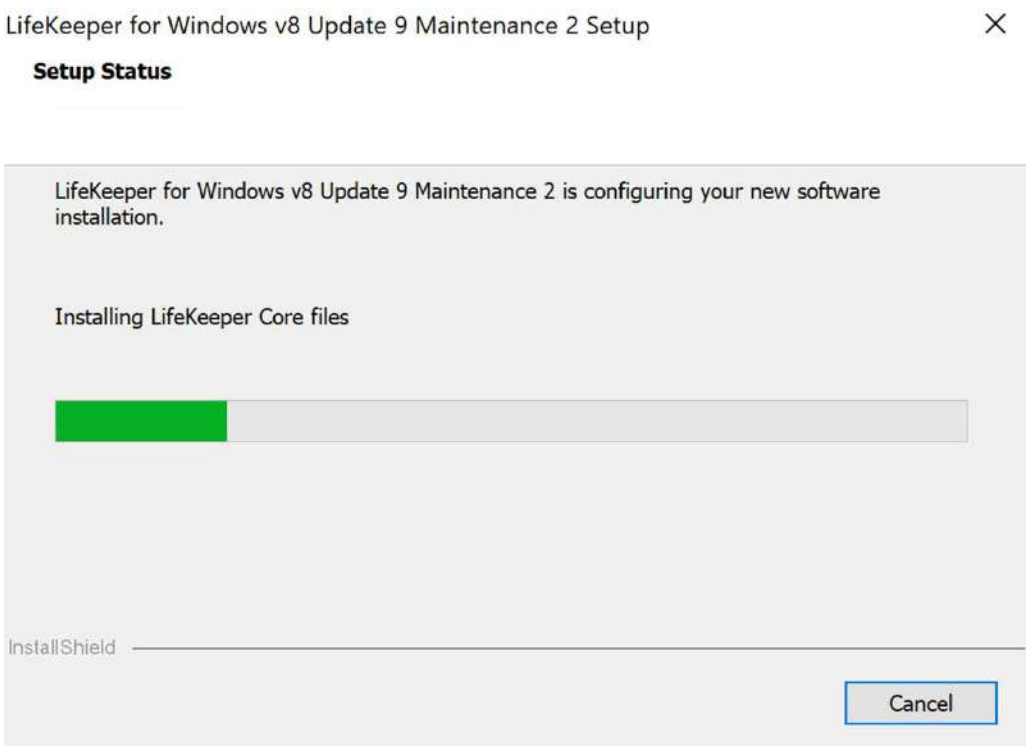


図 7.2-10 LifeKeeper のインストールが開始

（12） インストール完了

インストールが完了しました。「Finish」をクリックします。

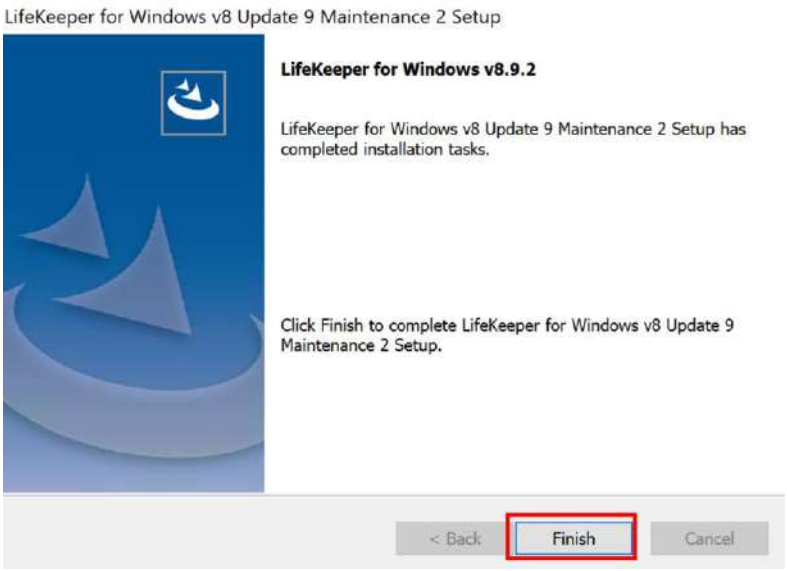


図 7.2-11 インストール完了

7.3. DataKeeper のインストール

LifeKeeper のインストールが完了すると、DataKeeper のインストールが自動的に開始されます。

（1） ライセンス契約書の内容の確認と承認

インストールの進行画面が表示されます。「Next」をクリックして先に進んでください。

ライセンス契約書の内容をよく読み、「Yes」をクリックして同意します。

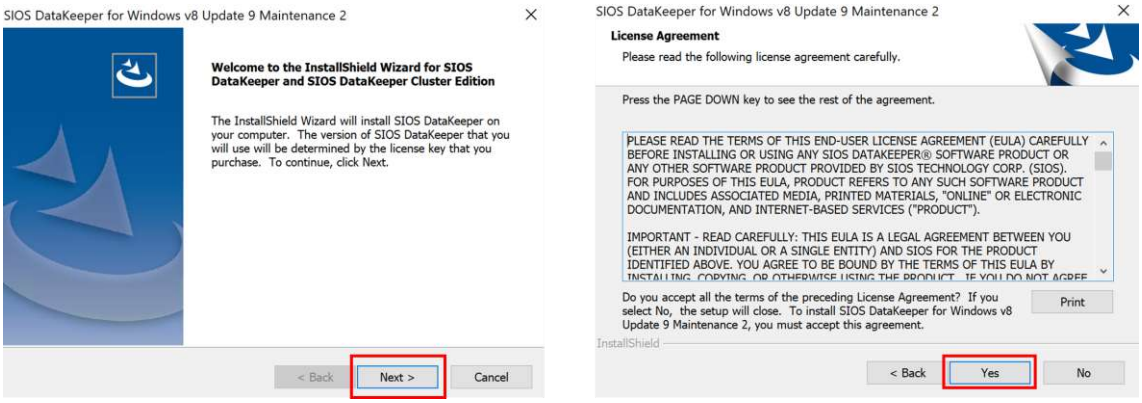


図 7.3-1 ライセンス契約書の内容の確認と承認

（2） インストール機能の選択

インストール機能の選択画面において、DataKeeper の GUI「SIOS DataKeeper User Interface」にチェックマークを入れます。

「Next>」をクリックします。

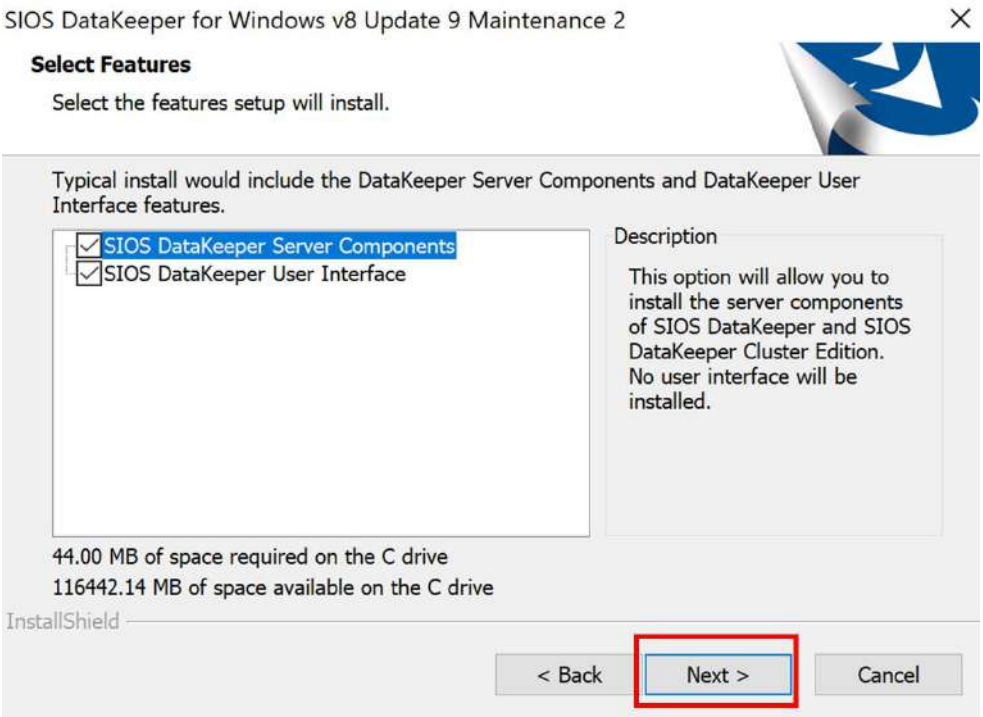


図 7.3-2 インストール機能を選択する

（3） インストール先のパスの設定

インストール先のパスを指定します。

本ガイドでは、デフォルトのパス C:¥Program Files (x86)¥SIOS¥DataKeeper を指定します。

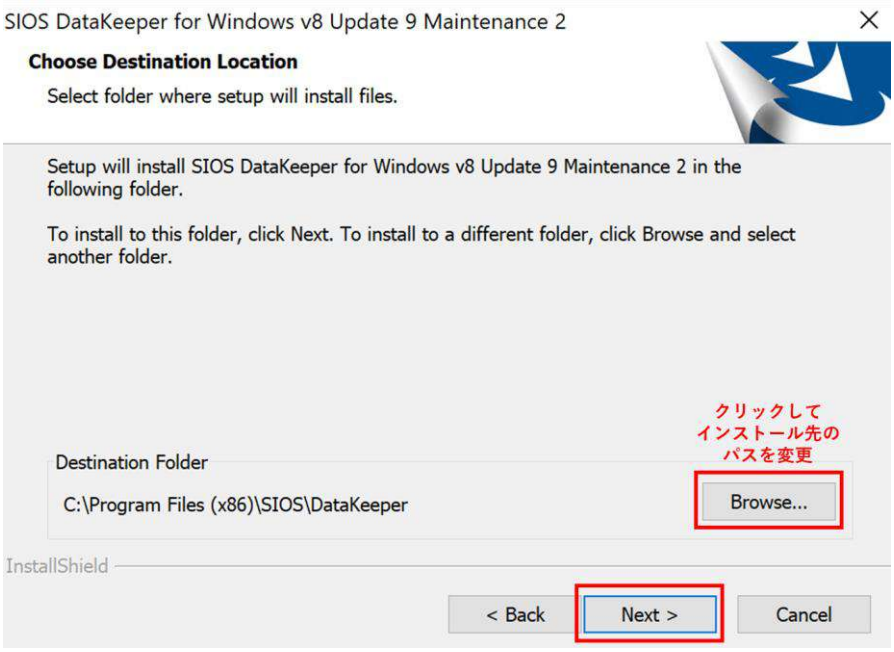


図 7.3-4 インストール先のパスの設定

（4） ポート開放の確認

DataKeeper が使用するポートの設定に関する画面が表示されます。

「Yes」をクリックして、ファイアウォールの受信ルールに必要なポートを解放します。

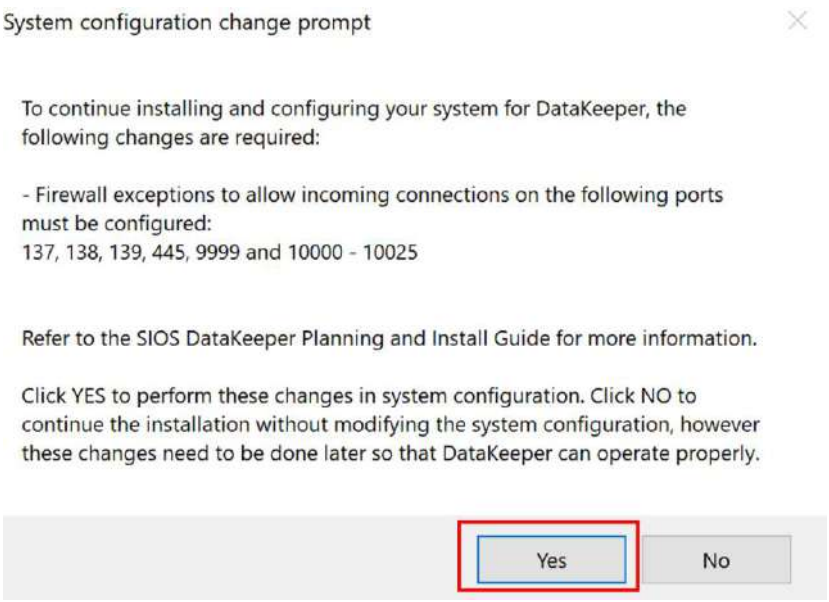


図 7.3-5 ポート開放の確認

（5） サービスを起動するアカウントの設定

DataKeeper のサービスを起動するアカウントを設定します。

本ガイドでは、「Domain or Server account」を選択します（Local System アカウントは推奨されません）。

選択した後、「Next>」をクリックしてください。

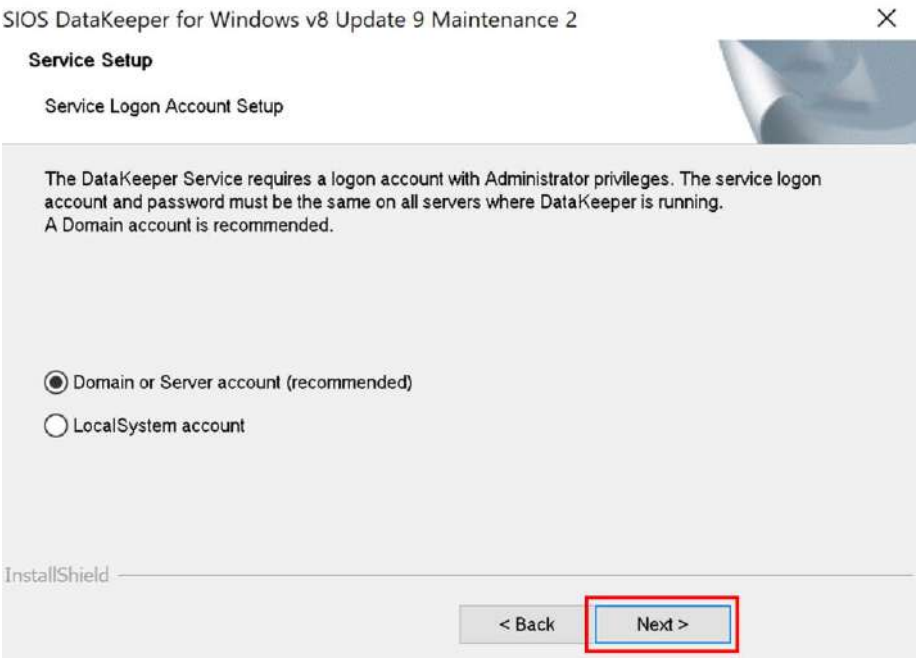


図 7.3-6 サービスを起動するアカウントの設定

（6） ドメインアカウントとパスワードの設定

「User ID」 の入力欄には、<ドメイン名>¥<ドメインアカウント> 形式でドメインアカウントを入力します。本ガイドでは SIOSDEV¥lkadmin です。

ログオンパスワードは適切に設定してください。

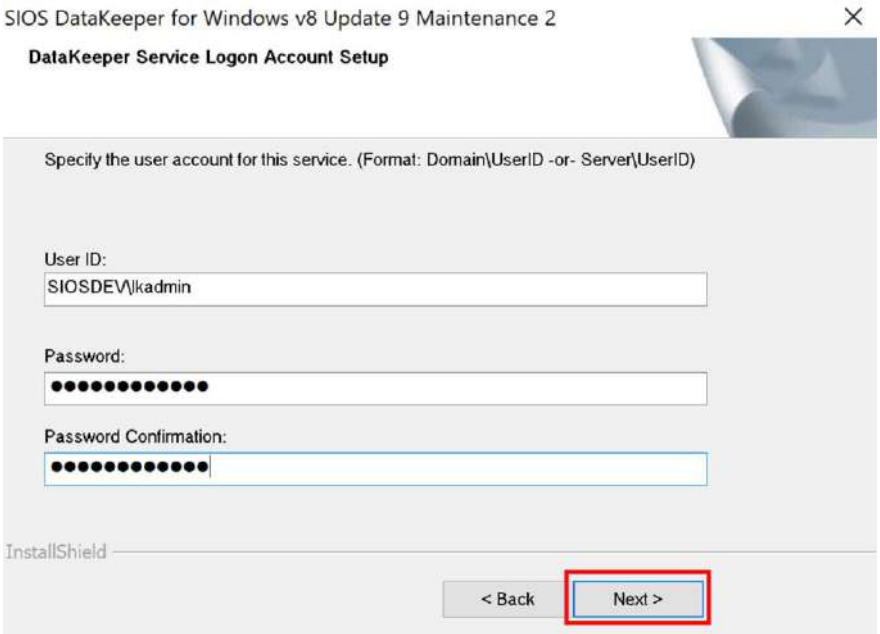


図 7.3-7 ドメインアカウントとパスワードの設定

（7） LifeKeeper と DataKeeper の共通アカウント設定

LifeKeeper に対しても、DataKeeper と同じアカウント情報を設定します。

「Synchronize LifeKeeper Account (recommended)」のチェックを入れて「Next>」をクリックします。

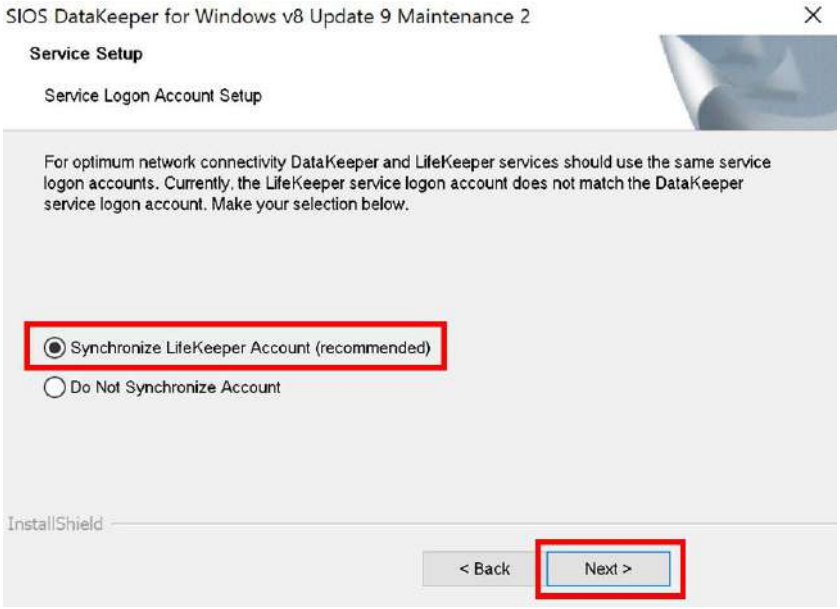


図 7.3-8 LifeKeeper と DataKeeper を同じアカウントで管理

（8） LifeKeeper の User ID の設定

この画面では、DataKeeper で設定した User ID が LifeKeeper 用の User ID として表示されます。

表示された情報を確認した後、「Next>」をクリックします。

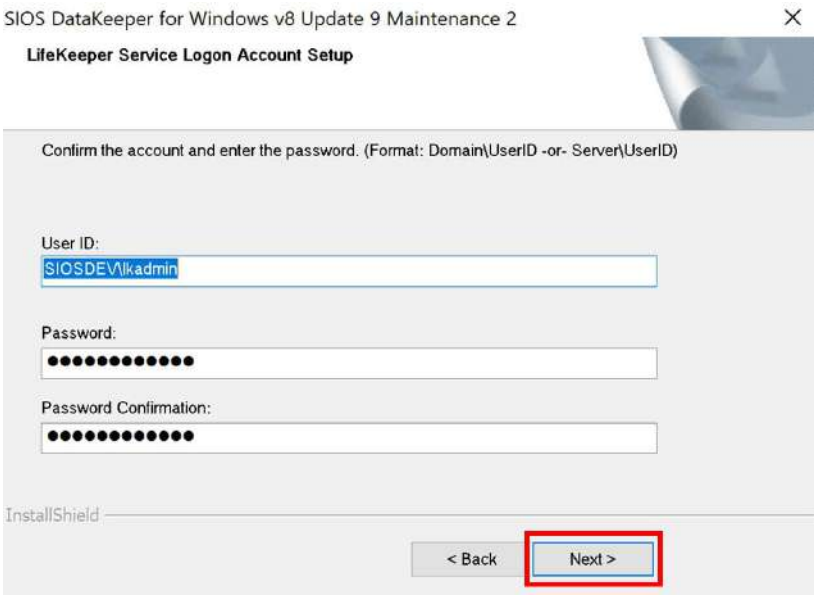


図 7.3-9 LifeKeeper の User ID の設定

（9） Bitmap ファイルの保存先ディレクトリの確認

DataKeeper で使用する Bitmap ファイルの保存先ディレクトリを確認します。

本ガイドではデフォルト設定を使用します。

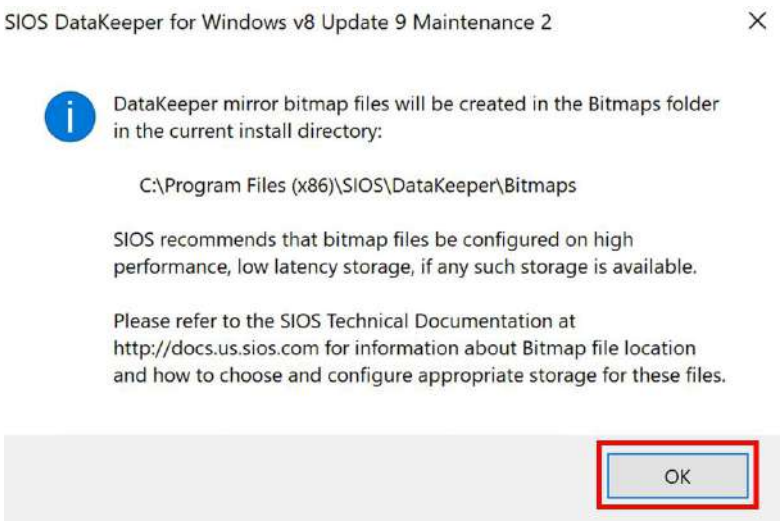


図 7.3-10 Bitmap ファイルの保存先ディレクトリの確認

（10） インストール完了

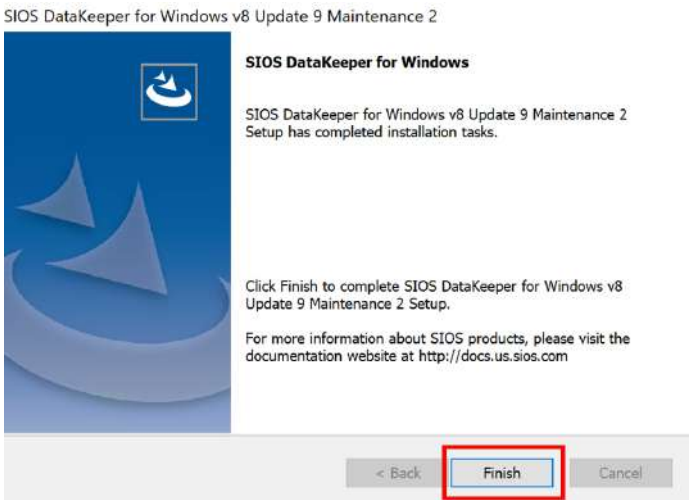


図 7.3-10 インストール完了

（11） ライセンスのインストール

インストール完了後、ライセンス管理画面が表示されます。

「Install License File」を選択し、必要なライセンスファイルをインストールします。

インストール後には、ライセンスファイルの種類と有効期限が表示されるので、これを確認します。

確認が終われば、「Exit」をクリックしてライセンスのインストールを閉じます。

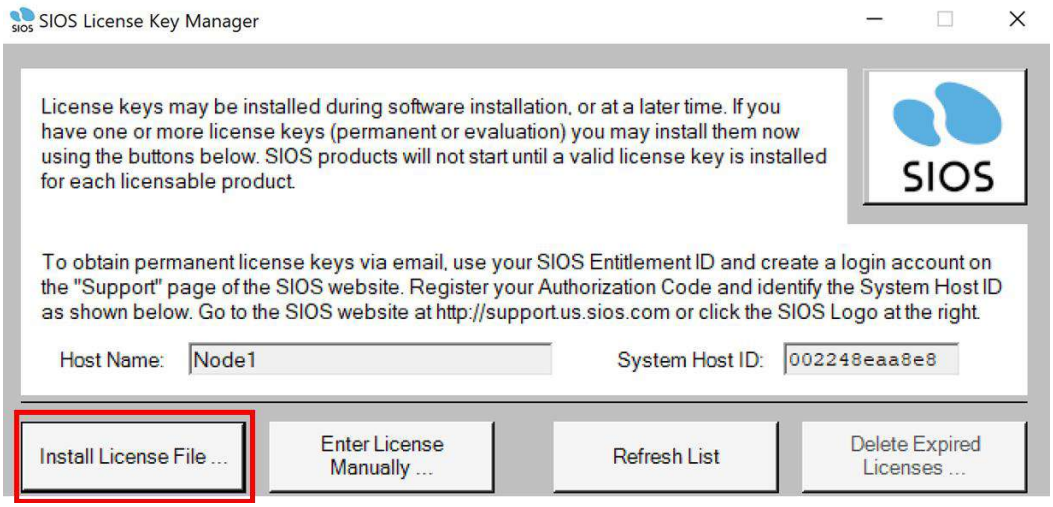


図 7.3-11 ライセンスのインストール

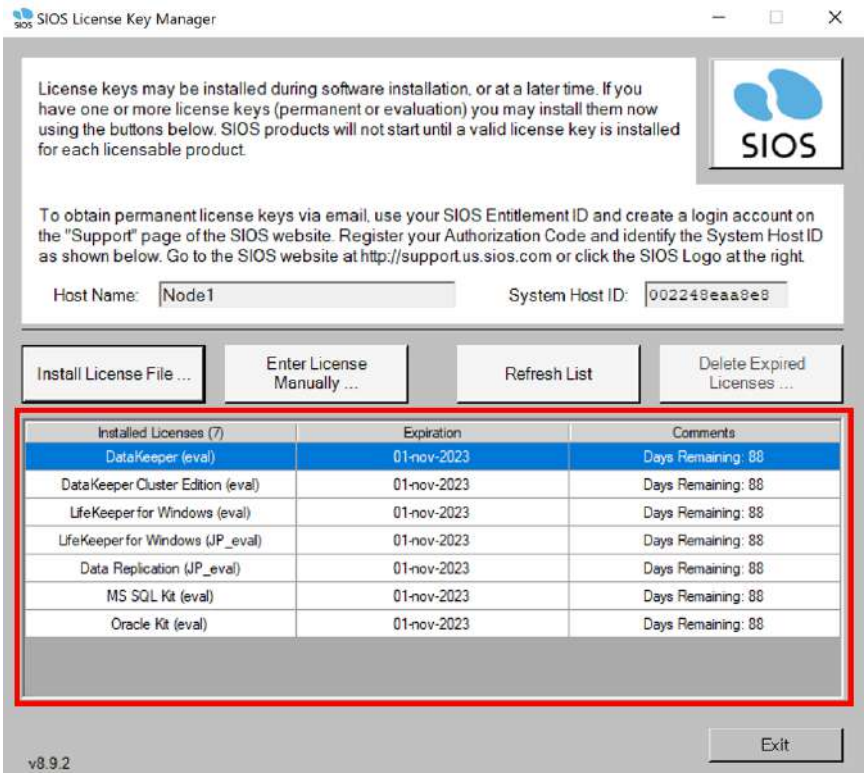


図 7.3-12 インストールされたライセンス

これで DataKeeper for Windows のインストールが完了しました。

（12） システムの再起動

DataKeeper のインストールが完了した後、システムを再起動する必要があります。即時に再起動する場合は、「Yes, I want to restart my computer now.」を選択し、クリックしてください。

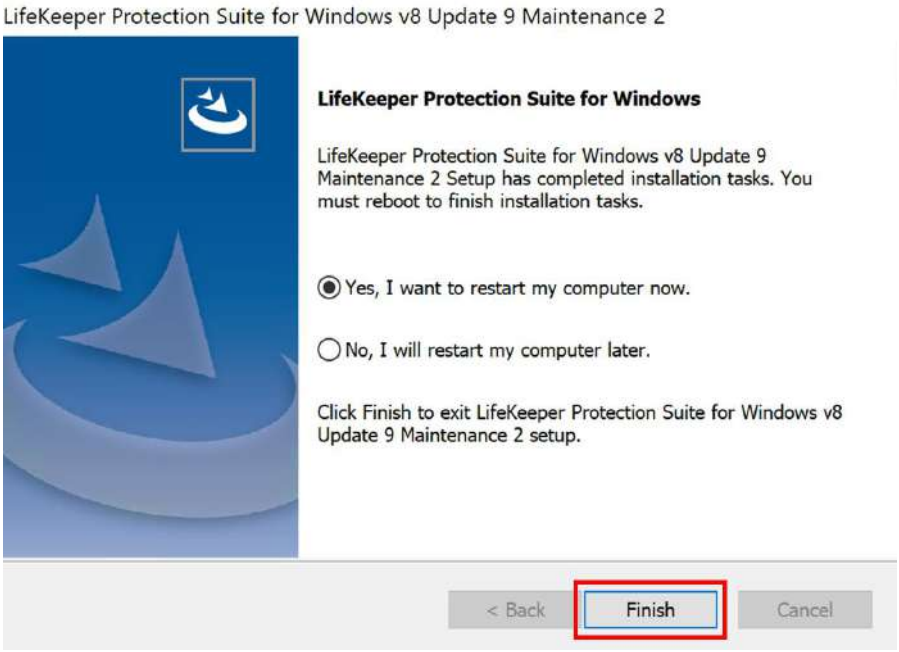


図 7.3-13 システムの再起動

これで、DataKeeper for Windows のインストールが全て完了しました。

7.4. SQL Server 2019 と SSMS のインストールメディアのダウンロード

このセクションでは、SQL Server 2019 と SSMS（SQL Server Management Studio）のインストールメディアをダウンロードします。
ボリュームリソースの作成後にインストールを行います。

（1） SQL Server 2019 のインストールメディアをダウンロード
クライアントノードにアクセスし、「Download Media」をクリックして SQL Server 2019 のインストールメディアをダウンロードします。

SQL Server 2019 のダウンロードサイド
https://www.microsoft.com/en-us/download/confirmation.aspx?id=101064

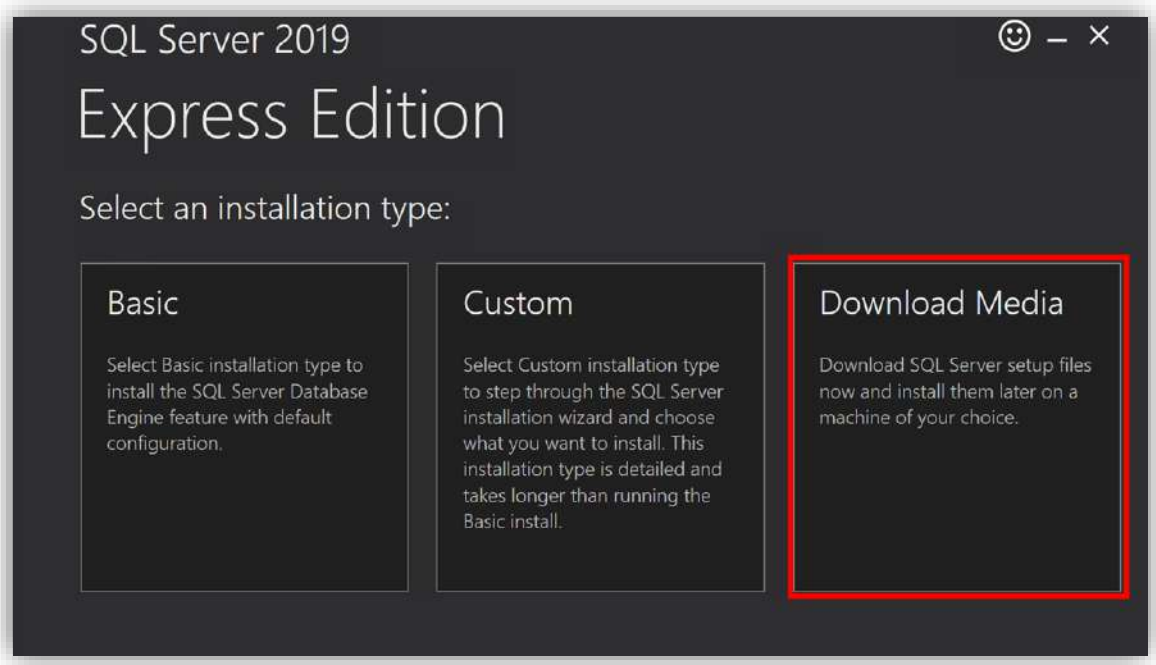


図 7.4-1 SQL Server のインストールメディアのダウンロード画面

（2） 保存先の指定

「Express Advanced」オプションを選択した後、「Browse」をクリックし、ダウンロードするメディアファイルの保存場所を指定します。

このガイドでは、C:¥Users¥<コンピュータ名>¥Downloads に保存します。

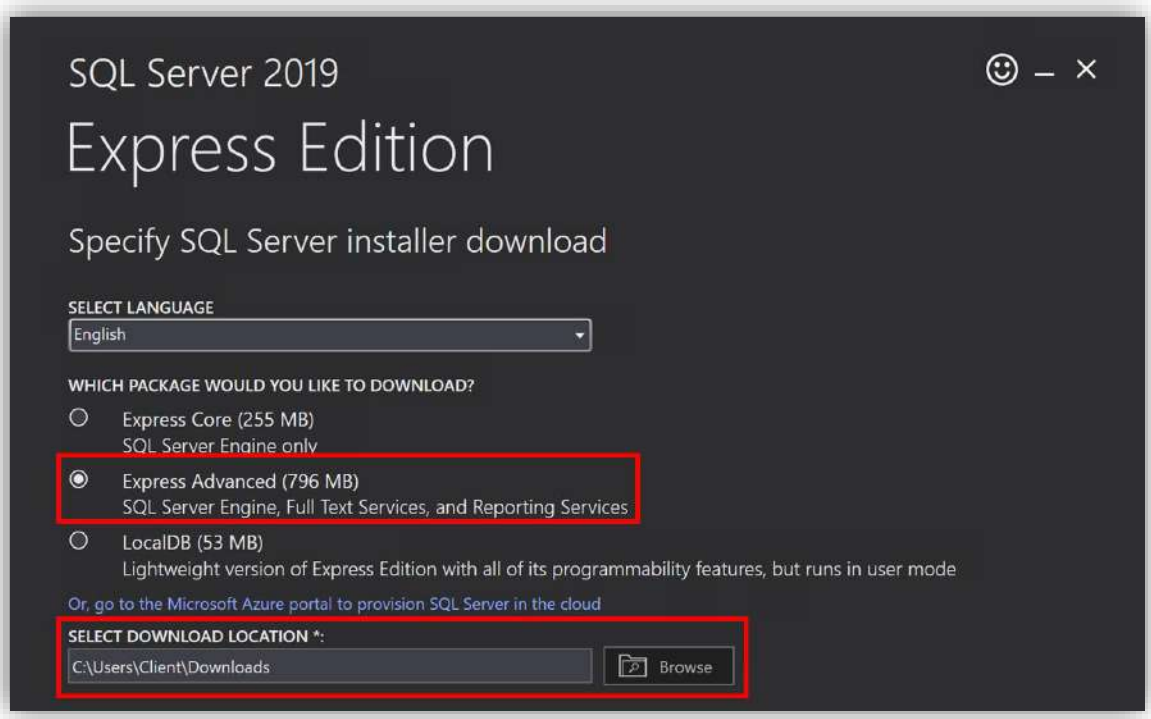


図 7.4.1-2 メディアファイルの保存場所の指定

（3） ダウンロード開始

設定が完了したら、「Download」をクリックしてダウンロードを始めます。

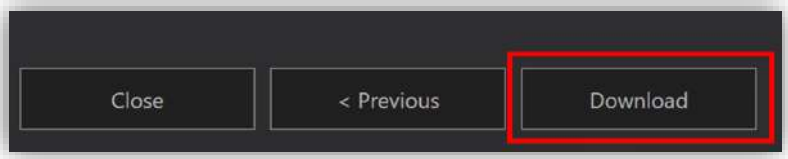


図 7.4-3 ダウンロード開始

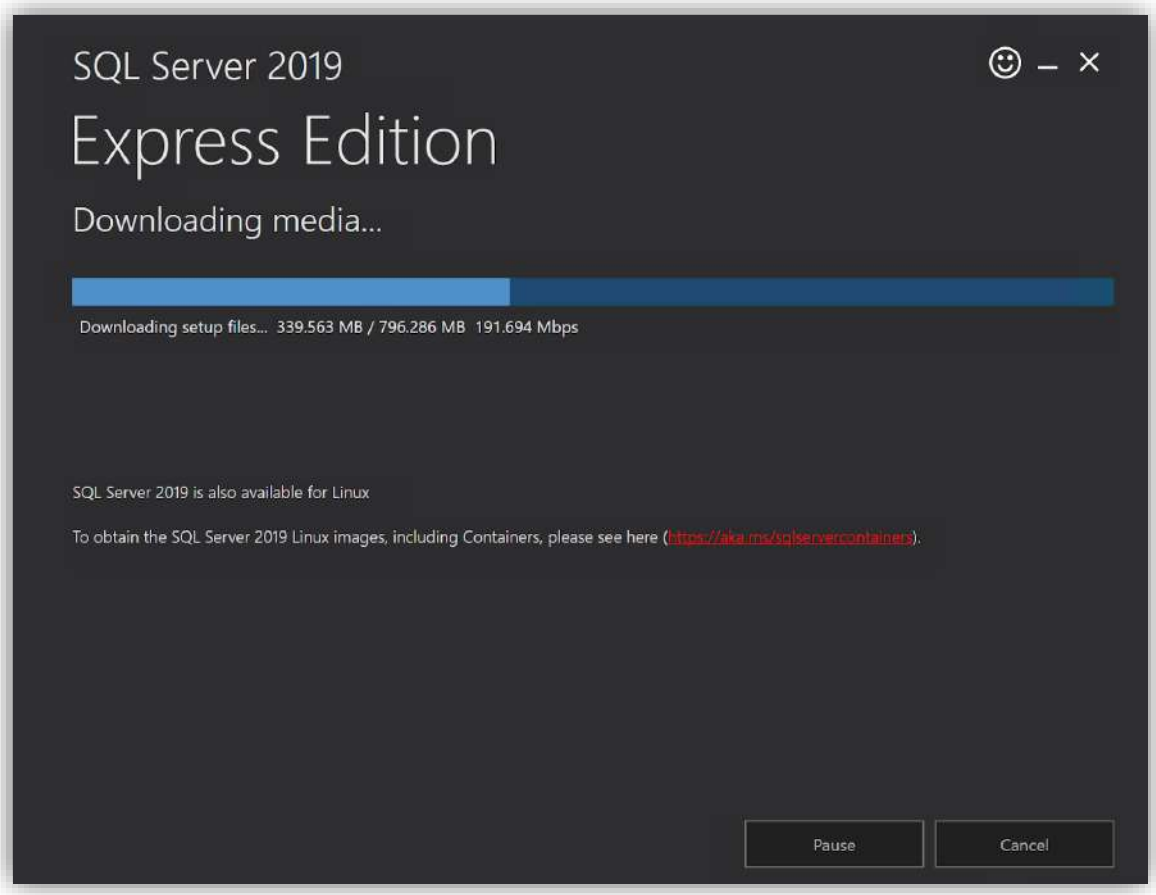


図 7.4-4 ダウンロード中

「Download successful」と表示されたら、ダウンロードが完了しています。その後、「Open folder」をクリックし、ダウンロードしたファイルが保存された場所を開いて確認します。

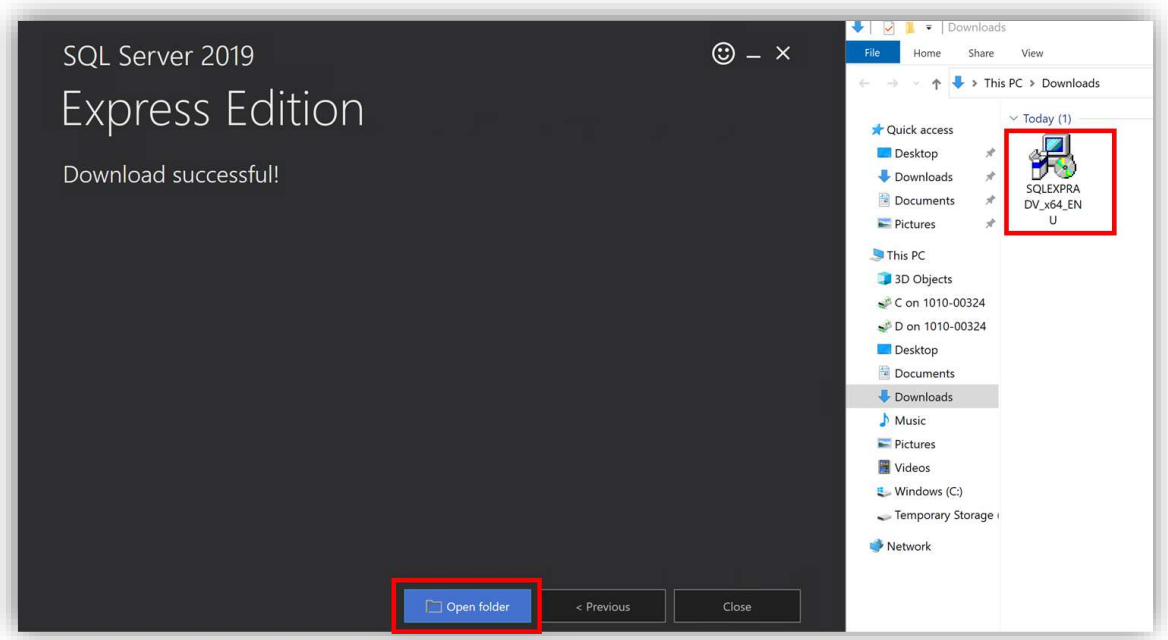


図 7.4-5 ダウンロード完了

ダウンロードがクライアントノードで完了したら、インストールメディアを稼働系ノードと待機系ノードにコピーします。

（4） SSMS のインストールメディアのダウンロード

SSMS のインストールメディア（SSMS-Setup-ENU.exe）をダウンロードして SQL Server 2019 のインストールメディア（SQLEXPRADV_x64_EN_ENU.exe）と同じ場所に移動します。

以下のサイトからダウンロードしてください。

https://learn.microsoft.com/ja-jp/sql/ssms/download-sql-server-management-studio-ssms

（5） インストールメディアの稼働系ノードと待機系ノードへのコピー

SQL Server 2019 と SSMS のインストールメディアを稼働系ノードと待機系ノードにコピーします。

RDP を使用して、稼働系ノードと待機系ノードに接続します。次に、クライアント

ノードのストレージからダウンロードした SQL Server 2019 と SSMS のインストールメディアをこれらのノードにコピーして、ローカルに保存します。

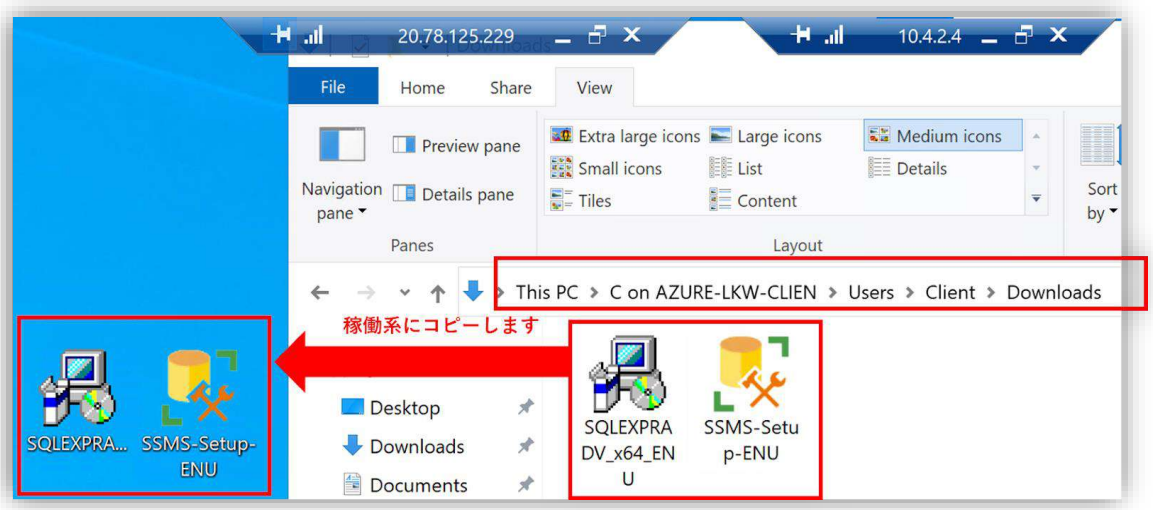


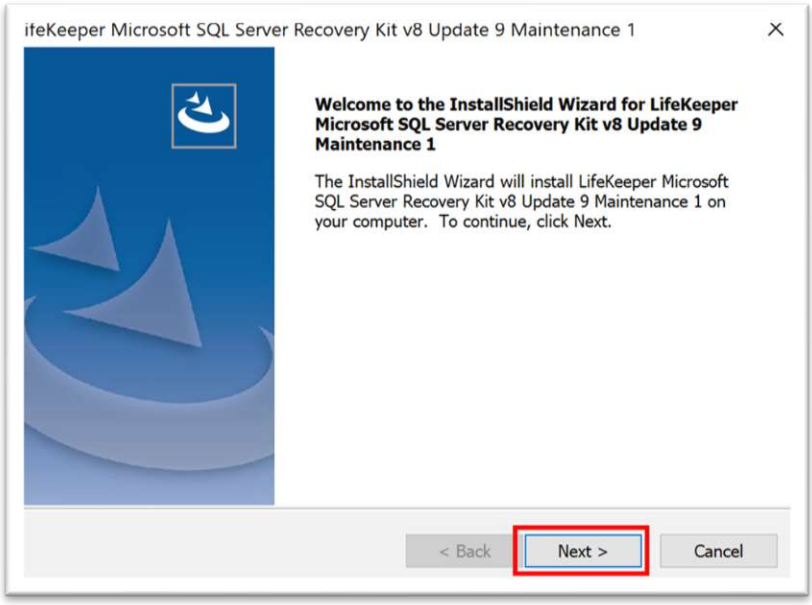
図 7.4-6 インストールメディアを稼働系ノードにコピー

7.5. LifeKeeper for Windows Microsoft SQL Server Recovery Kit のインストール

本節では、LifeKeeper for Windows Microsoft SQL Server Recovery Kit（以後、SQL Server RK）のインストール手順を説明します。
SQL Server RK を使用することで、Microsoft SQL Server 上のデータベースデータの完全性が保たれ、さらに LifeKeeper for Windows によるシステム可用性も高まります。

（1） 実行ファイルの実行
インストールに使用する実行ファイルは以下のディレクトリに格納されています。
<LifeKeeper のイメージファイル>¥Core¥LKSQL-8.9.1-Setup。
上記の実行ファイルをダブルクリックしてインストールウィザードを開きます。

（2） ライセンス規約の確認
インストールウィザードが起動したら、「Next」ボタンをクリックします。
次に表示されるライセンス規約を読み、同意する場合は「Yes」ボタンをクリックし、インストールが開始されます。



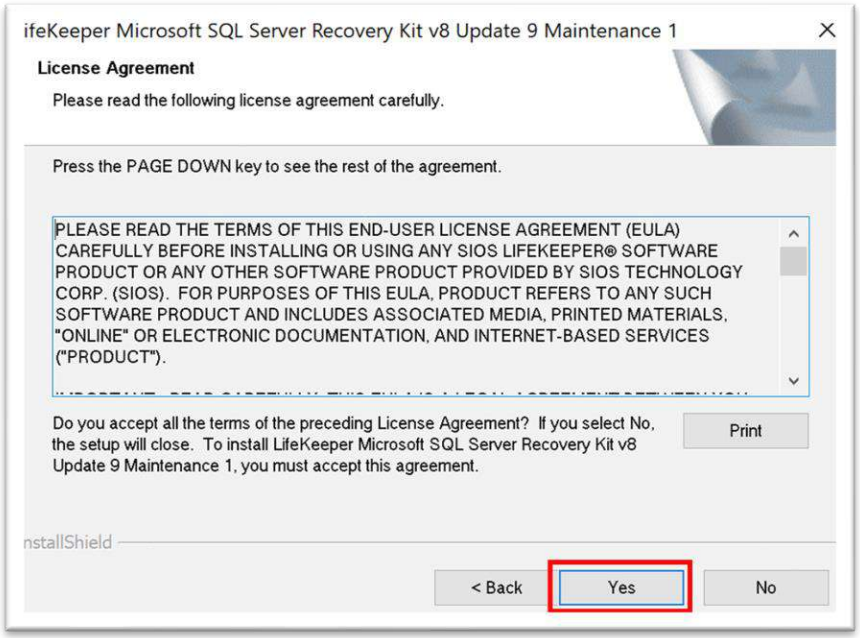


図 7.5-1 SQL Server RK のインストール

インストールが完了しました。「Finish」 をクリックしてインストールを閉じます。

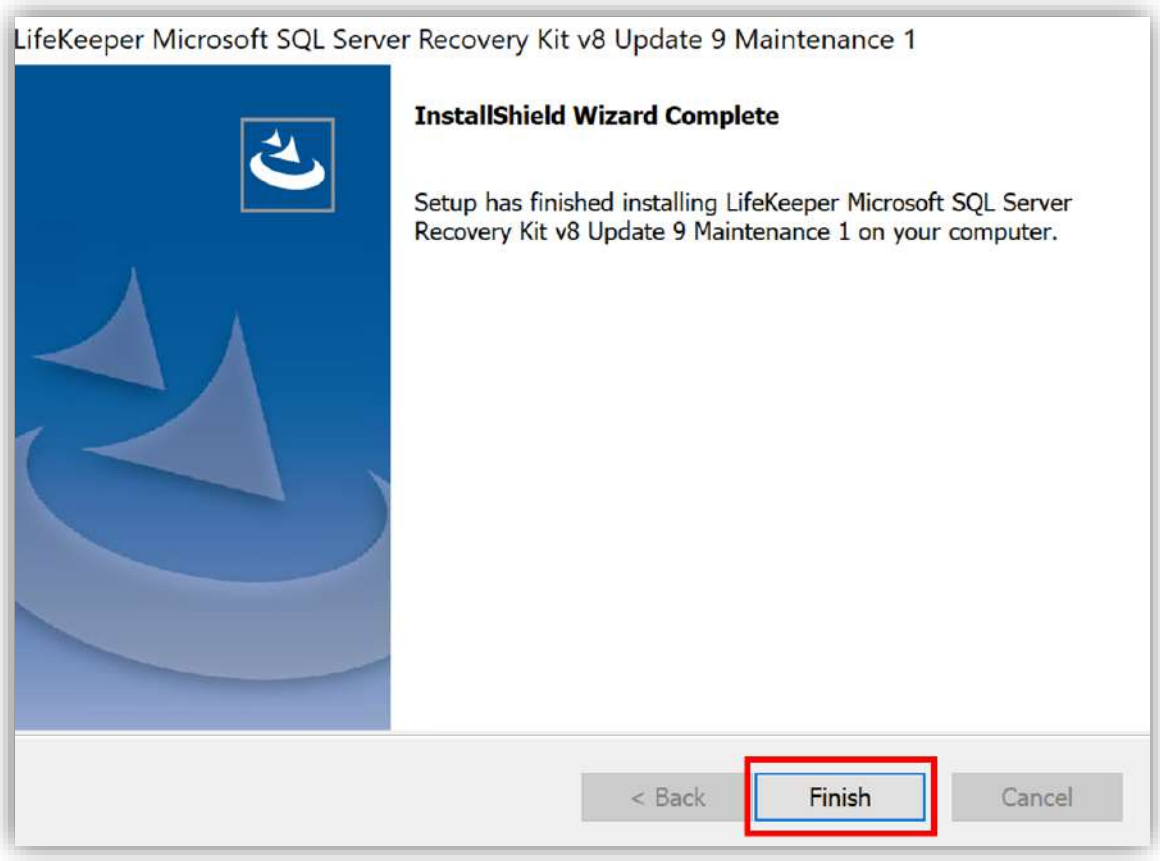


図 7.5.1-2 インストール完了

これで SQL Server RK のインストールが完了しました。

次に、稼働系ノードにも同じく SQL Server RK をインストールしてください。

8. リソース作成

本節は LifeKeeper の GUI を使用してコミュニケーションパスおよびリソースの作成手順を説明します。

8.1. コミュニケーションパスの作成

最初のステップでは、「10.4.1.4」と「10.4.2.4」の IP アドレスを使用して稼働系ノードと待機系ノード間のコミュニケーションパスを確立します。
ここでは、稼働系ノードをローカルサーバとし、待機系ノードをリモートサーバとして設定します。

ネットワークの構成は以下のようになります。

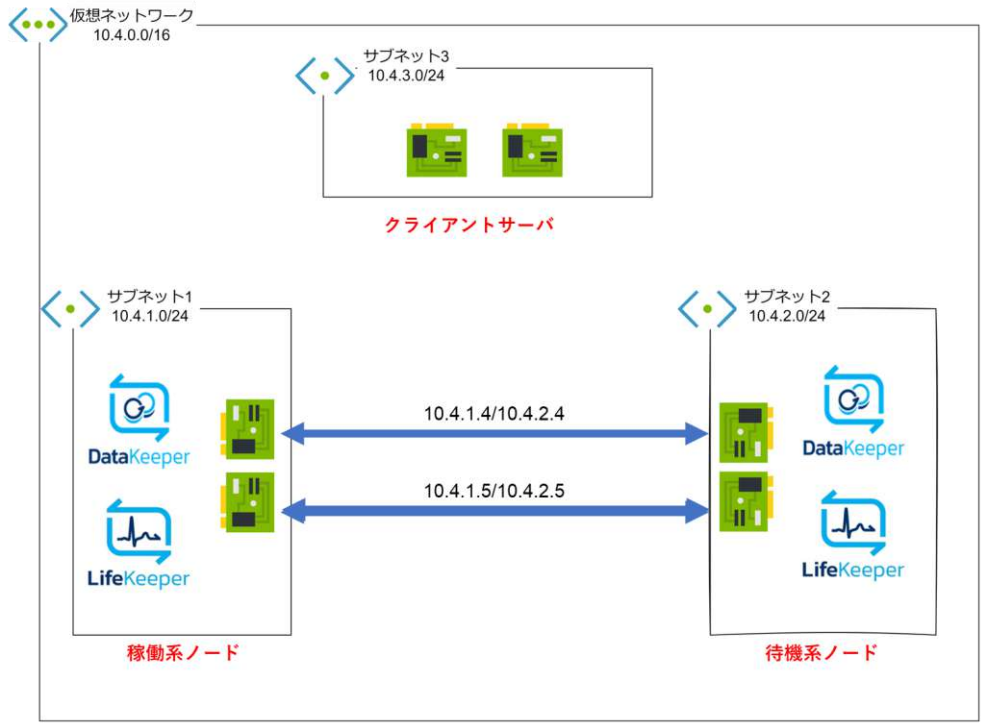


図 8.1-1 ネットワークの構成図

（1） LifeKeeper GUI の起動

Windows の検索バーで 「LifeKeeper (Admin Only) 」 を検索して管理者権限で LifeKeeper GUI を開きます。

図 8.1-2 LifeKeeper GUI の起動

（2） LifeKeeper GUI にログイン

ログイン画面にて、「Login」と「Password」のフィールドにドメインアカウントとパスワードを入力し、ログインします。

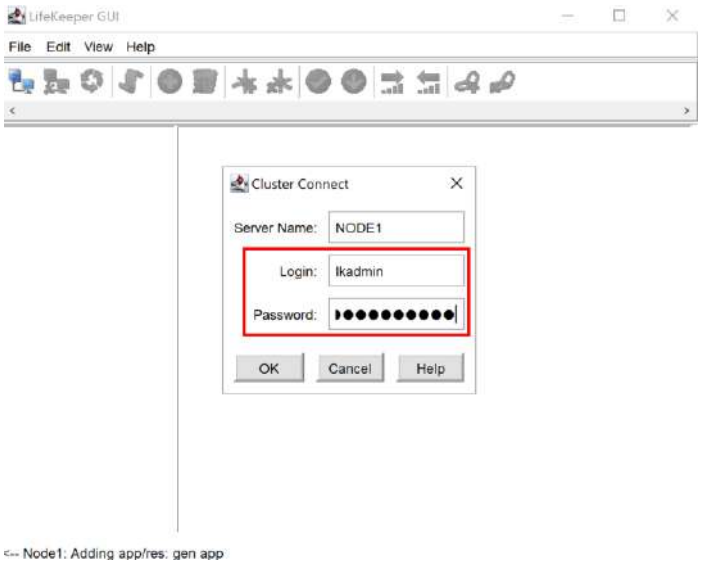


図 8.1-3 ログイン

（3） コミュニケーションパスの初期設定

「Create Comm Path」ボタンをクリックし、コミュニケーションパスの設定ウィンドウを開きます。

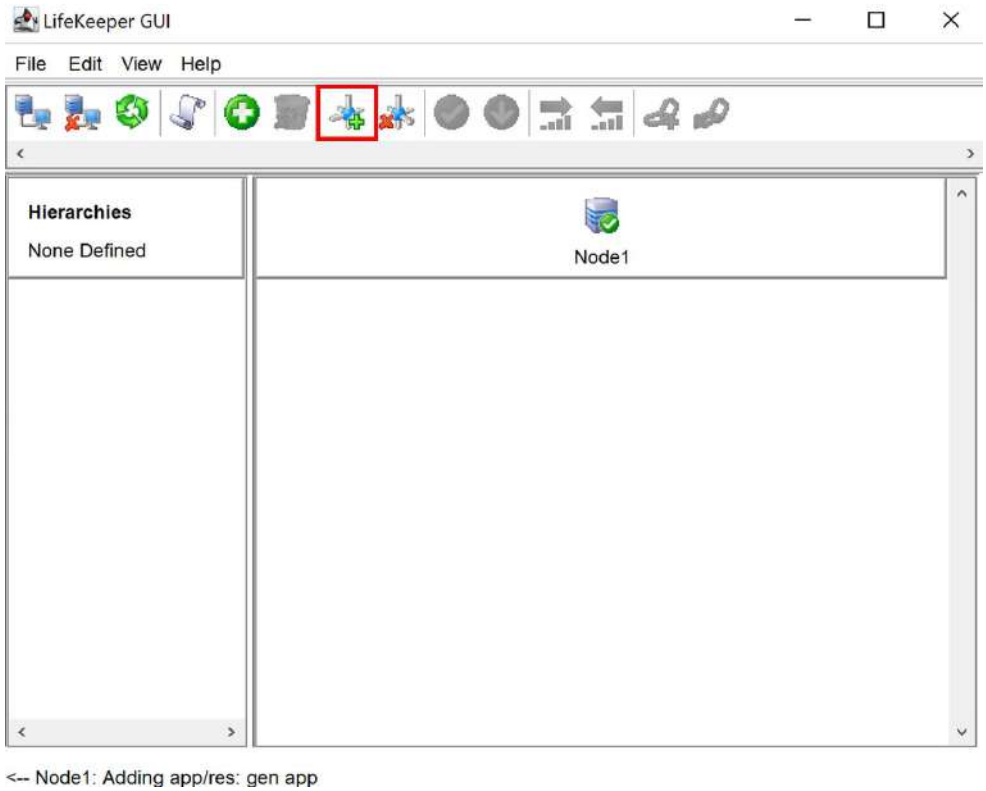


図 8.1-4 コミュニケーションパスの作成

（4） ローカルサーバ（稼働系ノード）を選択する

「Local Server」リストボックスから、ローカルサーバのコンピュータ名を選択します。

選択後は「Next >」をクリックします。

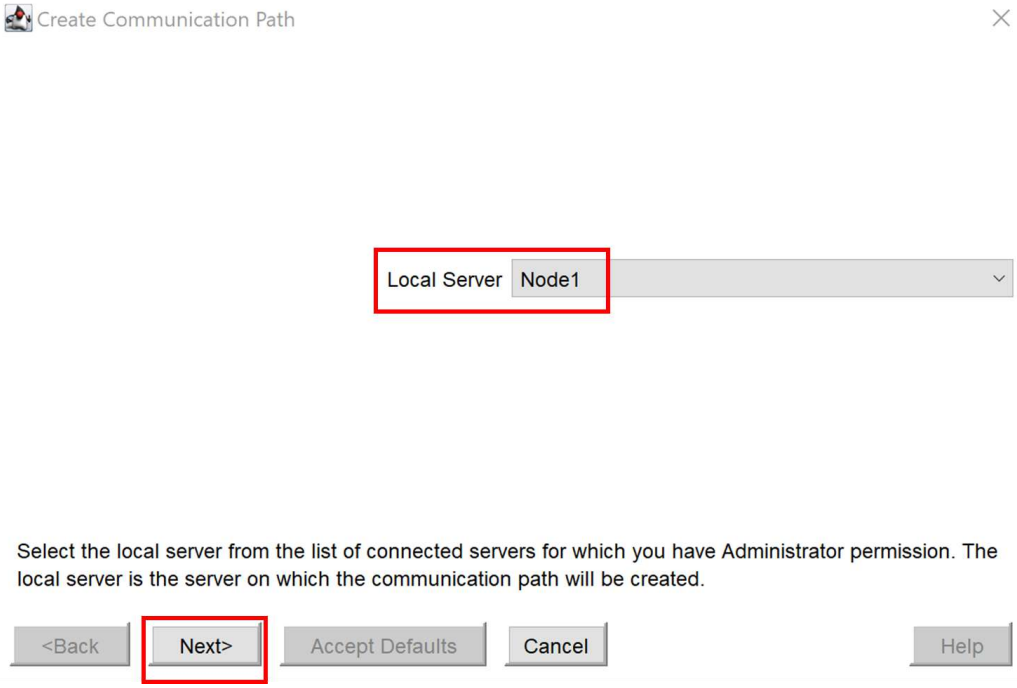


図 8.1-5 ローカルサーバの選択

（5） リモートサーバ（待機系ノード）を追加・選択する

「Add Server」ボタンの隣のテキストボックスにリモートサーバの IP アドレスを入力し、「Add Server」をクリックします。

追加が完了したら、「Remote Servers」のリストボックスから追加したサーバの IP アドレスを選択し、次に進むため「Next >」をクリックします。

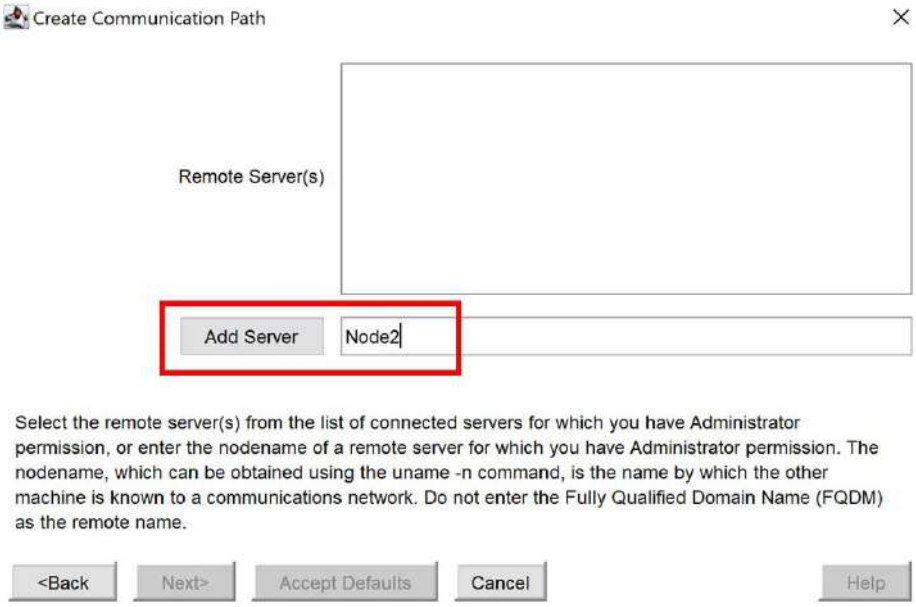


図 8.1-6 リモートサーバの追加

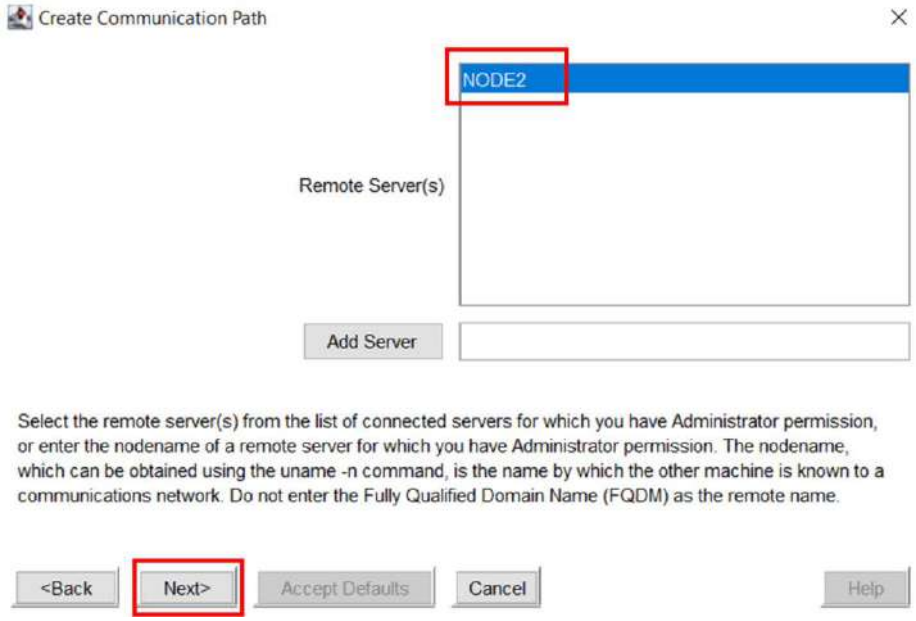


図 8.1-7 リモートサーバの選択

（6） 通信プロトコルの選択

本ガイドでは TCP プロトコルを使用します。

「TCP」 を選択し、「Next >」 をクリックします。

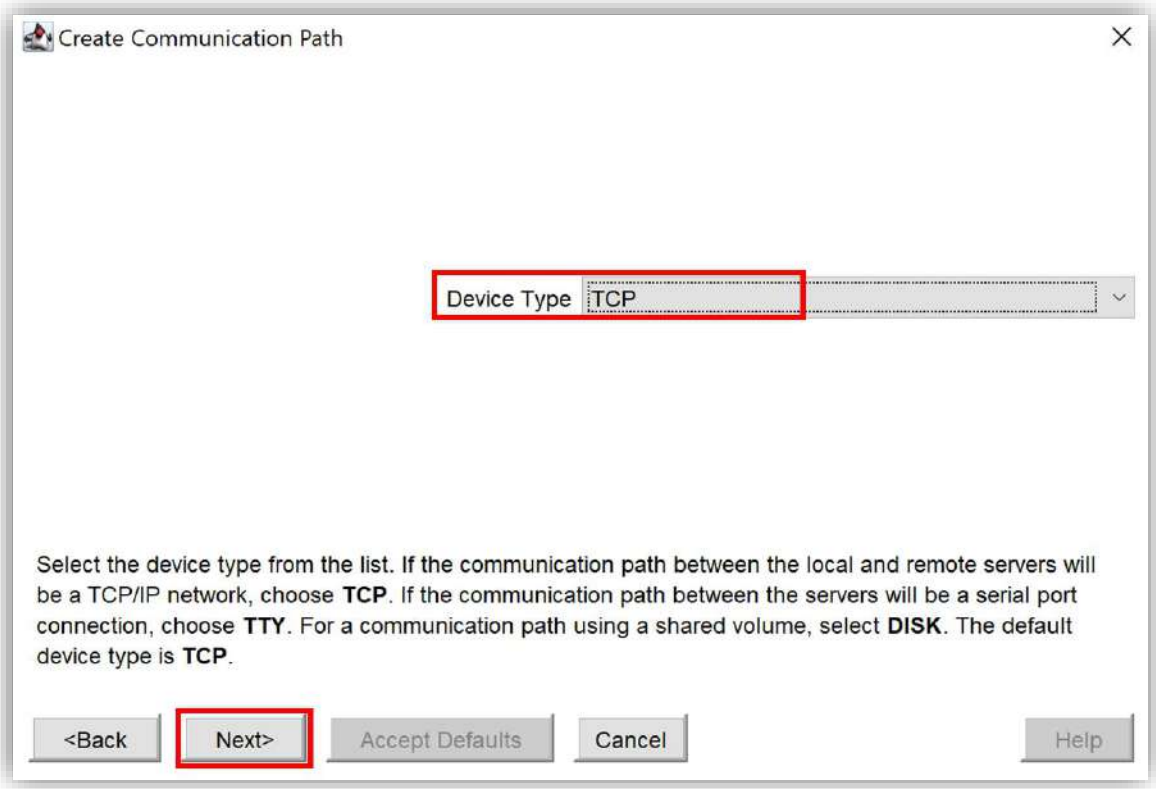


図 8.1-8 通信プロトコルの選択

（7） ハートビートの間隔（秒）の設定

ハートビートは、各ノード間で定期的なポーリングを行い、状態を監視する仕組みです。もしハートビートが途絶えた場合（DEAD ステータス）、システムは対象のノードが故障していると判断し、フェイルオーバーが実施されます。

ハートビートの設定には、「間隔」と「最大欠落数」という二つの主要なパラメータがあります。"間隔"はハートビートの送信間隔を、"最大欠落数"は連続してハー

トビートが失敗した場合の許容回数を指します。デフォルト設定では、5 秒ごとにハートビートが送信され、3 回の失敗で DEAD ステータスが確定します。

このガイドでは、デフォルトの 6 秒に設定します。「Heartbeat interval (in seconds)」欄に「6」を入力し、「Next >」をクリックします。

入力が完了したら、「Next >」 をクリックします。

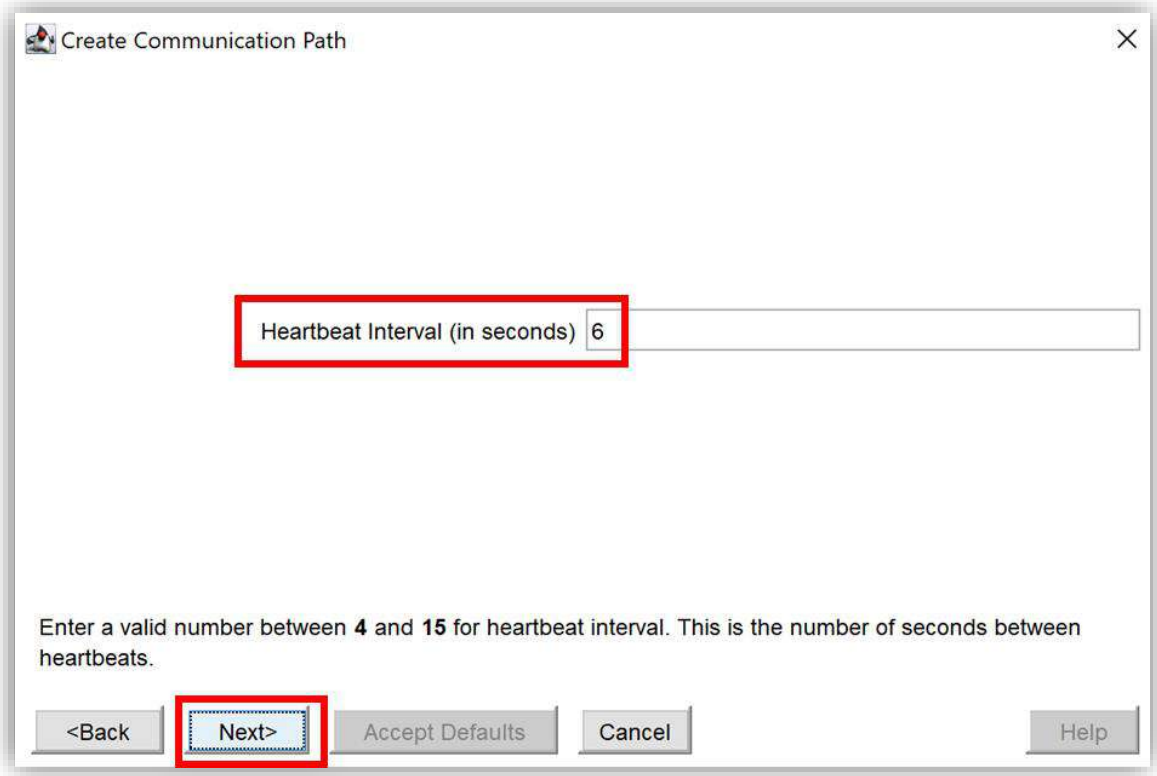


図 8.1-9 ハートビート間隔設定画面

（8） ハートビートの最大欠落数の設定

本ガイドではデフォルトの 5 回に設定します。「Maximum Heartbeat Misses」欄に「5」を入力した後、[Next >]をクリックします。 入力が完了したら、「Next >」をクリックします。

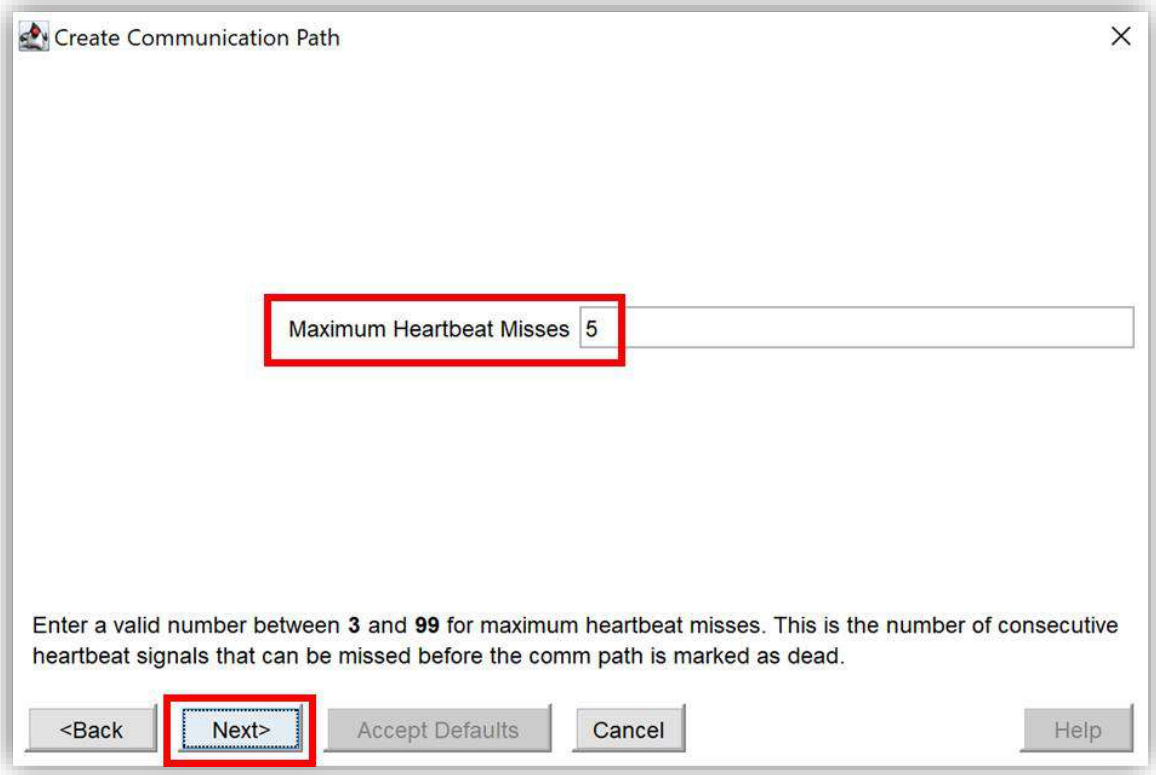


図 8.1-10 ハートビートの最大欠落数の設定

（9） ローカルサーバの IP アドレスの選択

ローカルサーバの全ての IP アドレスを選択します。

優先度の高い IP アドレスからコミュニケーションパスを設定します。このガイドでは、10.4.1.4 が優先度の高いアドレスとして設定します。

「Local IP Address(es)」リストから「10.4.1.4」を選択し、「Next >」をクリックします。

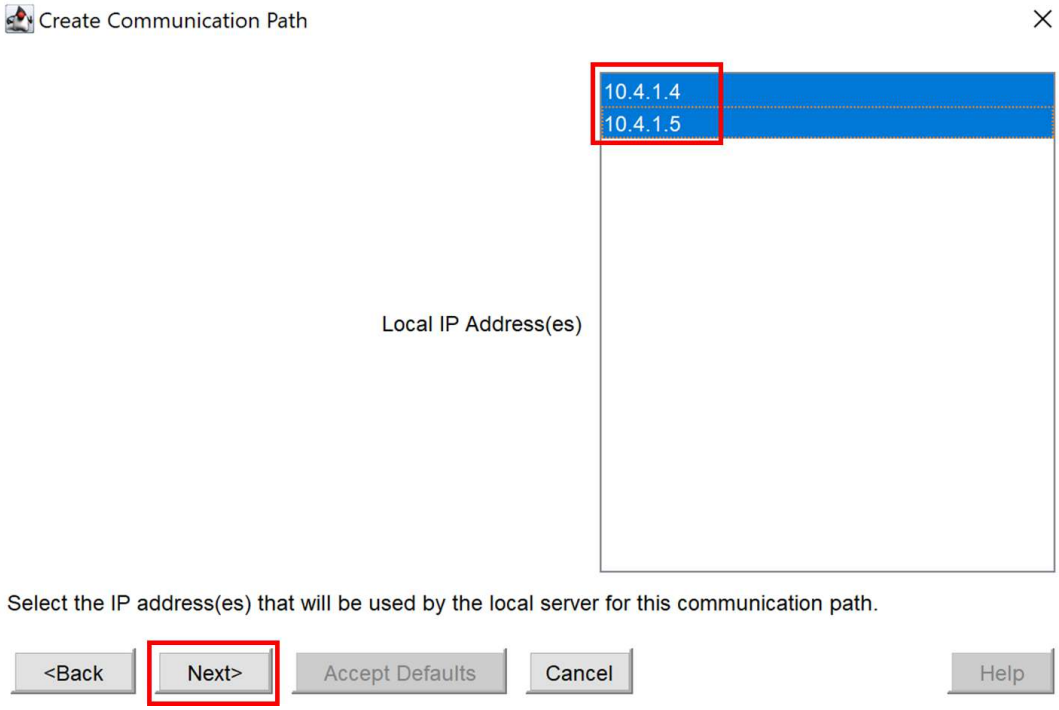


図 8.1-11 ローカルサーバの IP アドレスの選択

（10） ローカルサーバの優先度の指定

優先度は、サーバ間のコミュニケーションパスの優先順位を決定するために使用されます。

IP アドレス 10.4.1.4 を優先的に使用するように設定します。左上に表示された Local IP を確認し、「Priority」に 1 を入力します。（1 は最優先です）

入力が完了したら、「Next >」 をクリックします。

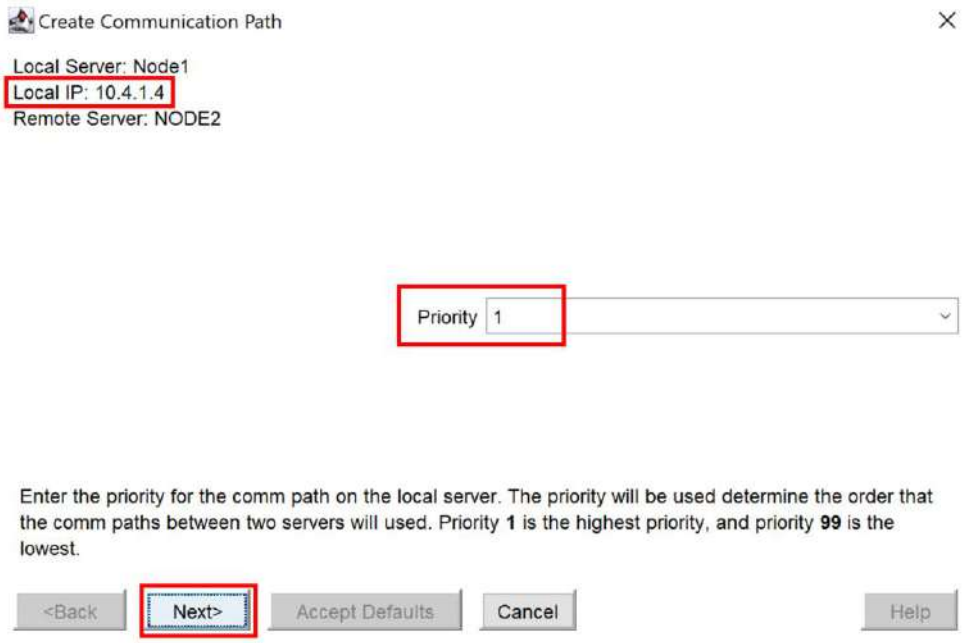


図 8.1-12 優先度の指定

（11） リモートサーバの IP アドレスの選択

左上に表示されたローカルサーバの IP アドレス「Local IP」 とリモートサーバの IP アドレスの間にコミュニケーションパスを作成します。

ローカルサーバの IP アドレス 10.4.1.4 とリモートサーバの IP アドレス 10.4.2.4 の間にコミュニケーションパスを作成します。

「Remote IP Address on <リモートサーバのコンピュータ名> に 「10.4.2.4」 を選択します。

選択したら 「Next >」 をクリックします。

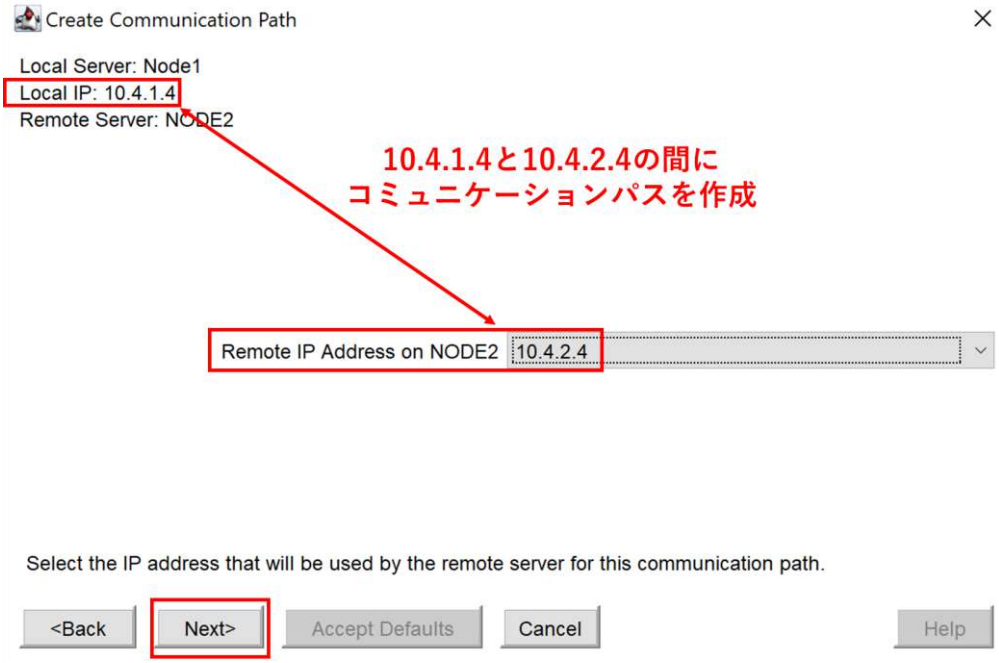


図 8.1-13 リモートサーバの IP アドレスの選択

（12） ロハートビートによる通信確認で使用するポート番号の入力

ハートビートによる通信確認で使用するポート番号の範囲は 1500～10000 です。

デフォルト値の 1500 を使用します。

「Port#」に 「1500」 入力します。

入力が完了したら、「Create」 をクリックして上記の設定でコミュニケーション

パスを作成します。

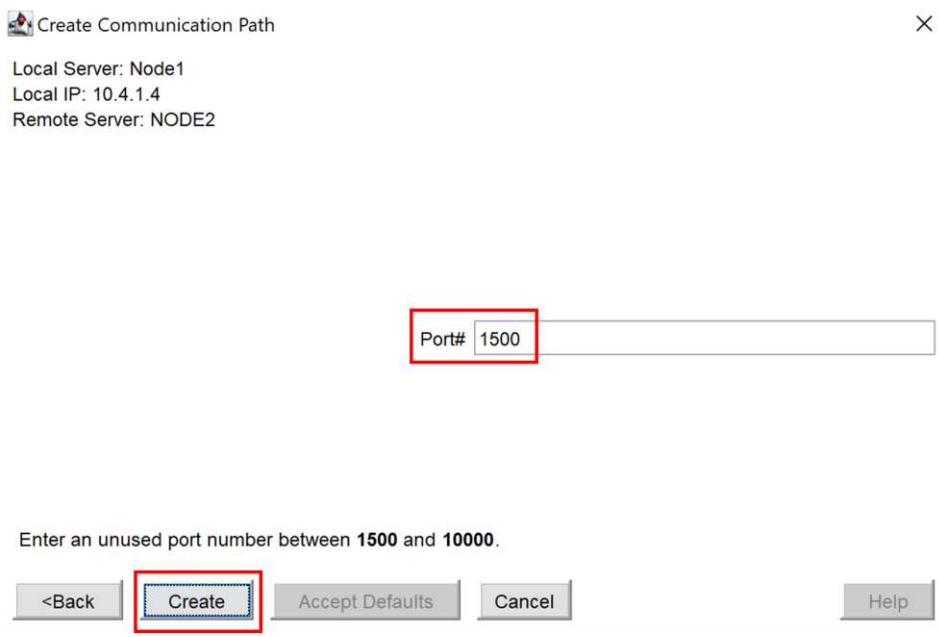


図 8.1-14 ポート番号の入力

（13） ロハートビートによる通信確認で使用するポートの開放

表示された情報を確認したら、「Next >」 をクリックします。

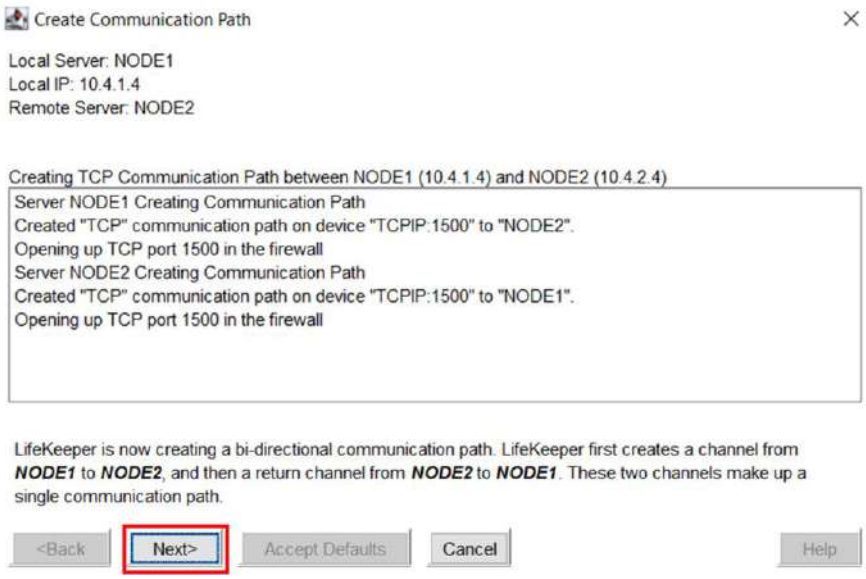


図 8.1-15 ポートの開放

（14） LifeKeeper GUI でコミュニケーションパスの状態の確認

各ノード間で 2 つのコミュニケーションパスが正常に作成された場合、GUI 上でサーバのアイコンが緑色になります。この状態を確認するには、LifeKeeper GUI を開き、サーバのアイコンを右クリックして「Properties」を選択します。

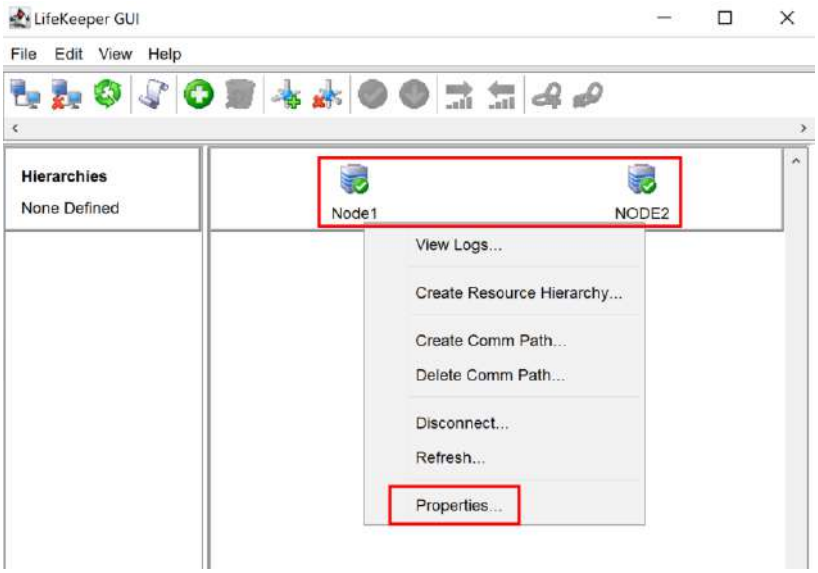


図 8.1-16 コミュニケーションパスの状態の確認

「Server」で稼働系ノードと待機系ノードを選択します。

「CommPaths」タブを開き、通信の状態を確認します。ここで、

「Address/Device」はハートビート通信に使用されているローカルとリモートの IP アドレスを示します。

「Status」がすべて 「ALIVE」 であれば、サーバ間はコミュニケーションパスを通じてハートビートを正常に受信しています。

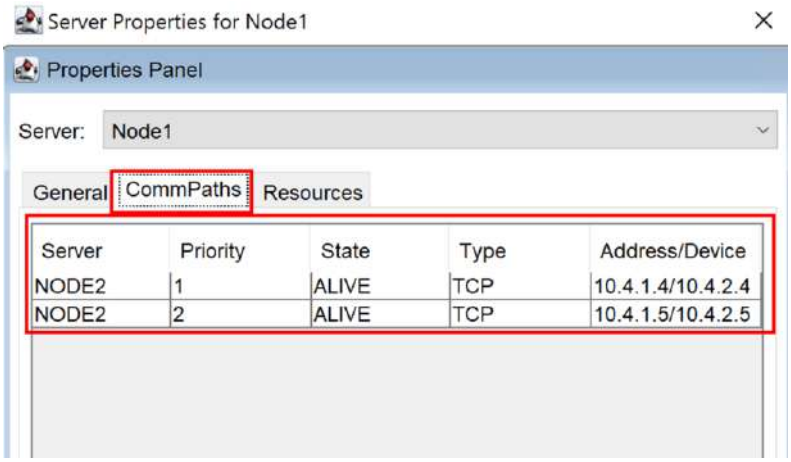


図 8.1-17 コミュニケーションパスの状態の確認

これで「10.4.1.5」と「10.4.2.5」間のコミュニケーションパスの作成が完了しました。
次に、同じ手順で「10.4.1.5」と「10.4.2.5」の IP アドレスを使用して稼働系ノードと待機系ノード間のコミュニケーションパスを作成してください。

稼働系ノードと待機系ノードの間のコミュニケーションパス情報は以下のようになります。

表 8.1 ノード間のコミュニケーションパス情報

	稼働系	待機系
稼働系		10.4.1.4/10.4.1.5
待機系	10.4.2.4/10.4.2.5	

8.2. Quorum Witness Server Support Package for Windows (QWK) Storage モードの設定

本節は、QWK Storage モードを有効にするために必要な設定ファイルの編集手順を説明します。

8.2.1. QWK Storage モードの有効化

（1） QWK オブジェクトを保存するフォルダの作成

共有ファイルのルートディレクトリに qwk_object という名前のフォルダを作成し、そこに QWK オブジェクトを格納します。

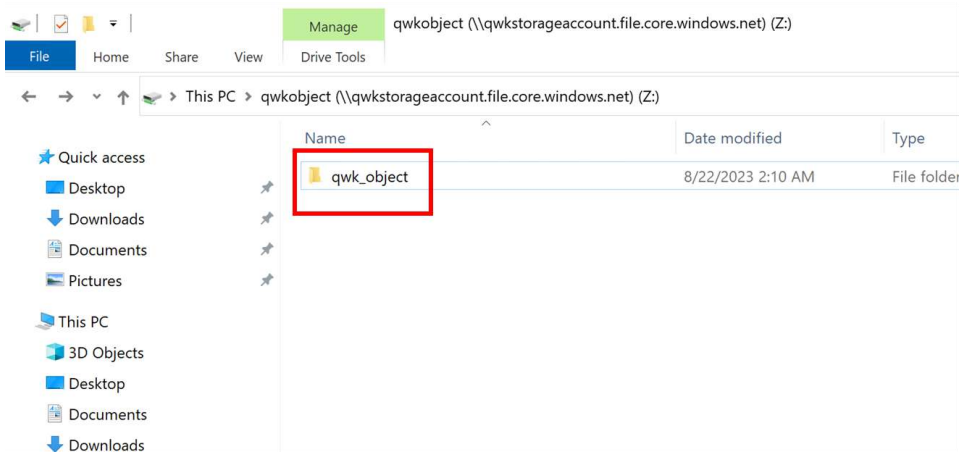


図 8.2-1 qwk オブジェクトを保存するディレクトリ

（2） 設定ファイルの編集

QWK の各設定は、%LKROOT%/etc/default/LifeKeeper という設定ファイルで行います。このファイルを編集することにより、クライアントノード、稼働系ノード、および待機系ノードのモードを次のように指定します。

QUORUM_MODE=storage

WITNESS_MODE=storage

（3） Storage モード用のパラメータの追加

設定ファイルの末尾に、以下のストレージ関連のパラメータを追加します。

QWK_STORAGE_TYPE=file

QWK_STORAGE_HBEATTIME=6

QWK_STORAGE_NUMHBEATS=9

QWK_STORAGE_OBJECT_NODE1=//qwkstorageaccount.file.core.windows.net/qwkobject/qwk_object/NODE1_object

QWK_STORAGE_OBJECT_NODE2=//qwkstorageaccount.file.core.windows.net/qwkobject/qwk_object/NODE2_object

ここで、「//qwkstorageaccount.file.core.windows.net/qwkobject/」は、Azure でホストされている共有ファイルの URL です。

「qwk_object/NODE1_object」と「qwk_object/NODE2_object」は、それぞれ稼働系ノードと待機系ノードが持つ QWK オブジェクトの名前です。

図 8.2-2 共有ファイルの URL

これらのパラメータは変更した後にすぐに適用されます。

8.3. GenLB リソースの作成

Azure の環境では、内部ロードバランサ（Internal Load Balancer、略して ILB）を設置することが可能です。ILB はフロントエンド IP アドレスを仮想 IP として持ち、これを使ってネットワーク通信のルーティングを制御します。LifeKeeper の Generic ARK for Load Balancer probe reply（以下 GenLB）を用いると、ILB がアクティブなノードだけに通信を割り当てるように制御できます。Azure の環境では、この GenLB リソースが必須となります

本節では GenLB リソースについて説明します。

8.3.1. ILB の正常性プローブで使用されるポート番号の確認と開放

Azure 内部ロードバランサの正常性プローブに使用するポート番号を確認します。

（1） 正常性プローブに使用するポート番号の確認

Azure Portal で作成したロードバランサのリソース管理画面を開き、「正常性プローブ」タブを選択して使用されているヘルスプローブのポート番号を確認します。

本ガイドでは、ヘルスプローブのポート番号は 12345 を使用します。

図 8.3.1-1 正常性プローブに使用するポート番号の確認

（2） 正常性プローブに使用するポート番号の開放

稼働系と待機系に正常性プローブに使用するポートを開放します。

8.3.2. GenLB リソースの作成

LifeKeeper GUI を使用して GenLB リソースを作成します。

まず、GenLB のスクリプトファイルをダウンロードし、RDP のドライブ接続機能を使用して稼働系ノードにコピーします。

GenLB は以下のサイトで入手できます。

「Windows」Generic ARK for Load Balancer probe reply の提供

（1） GenLB のスクリプトファイルの用意

GenLB のスクリプトファイルを C:¥LK¥GenArk¥GenLB-W にコピーしました。

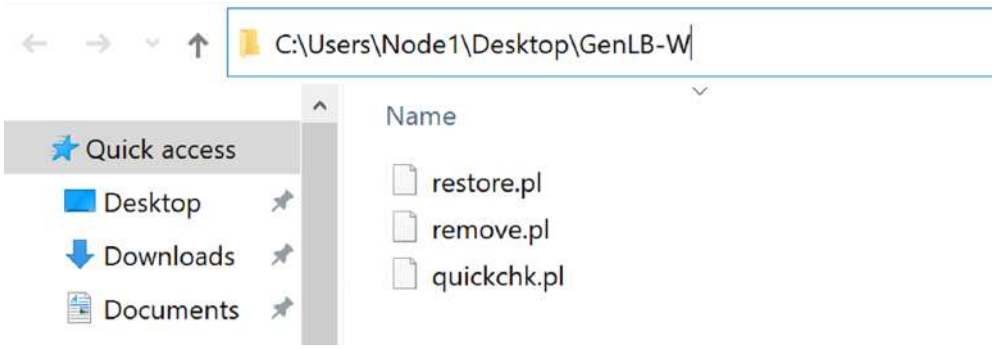


図 8.3.2-1 GenLB のスクリプトファイルの用意

（2） LifeKeeper GUI でリソース作成

LifeKeeper GUI を開き、メニューから「Create Resource Hierarchy」アイコンをクリックして、新しい GenLB リソースのリソース階層を作成します。

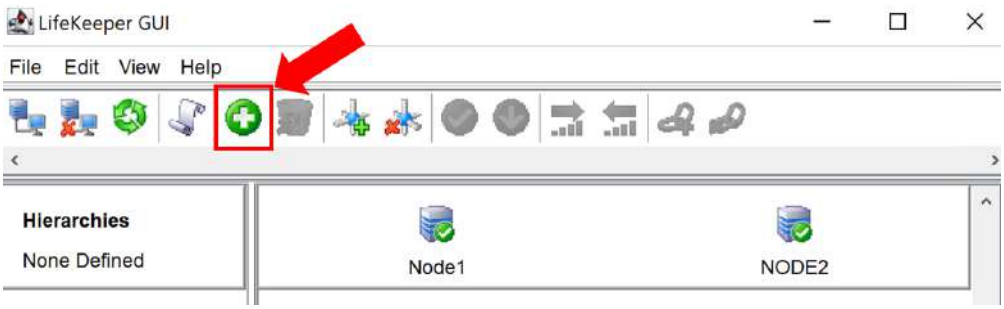


図 8.3.2-2 LifeKeeper GUI でリソース作成

（3） 稼働系ノードと待機系ノードの選択

画面に表示されるリストボックスから、Primary Server（稼働系ノード）と Backup Server（待機系ノード）を選択します。

選択が完了したら、「Next>」ボタンをクリックします。

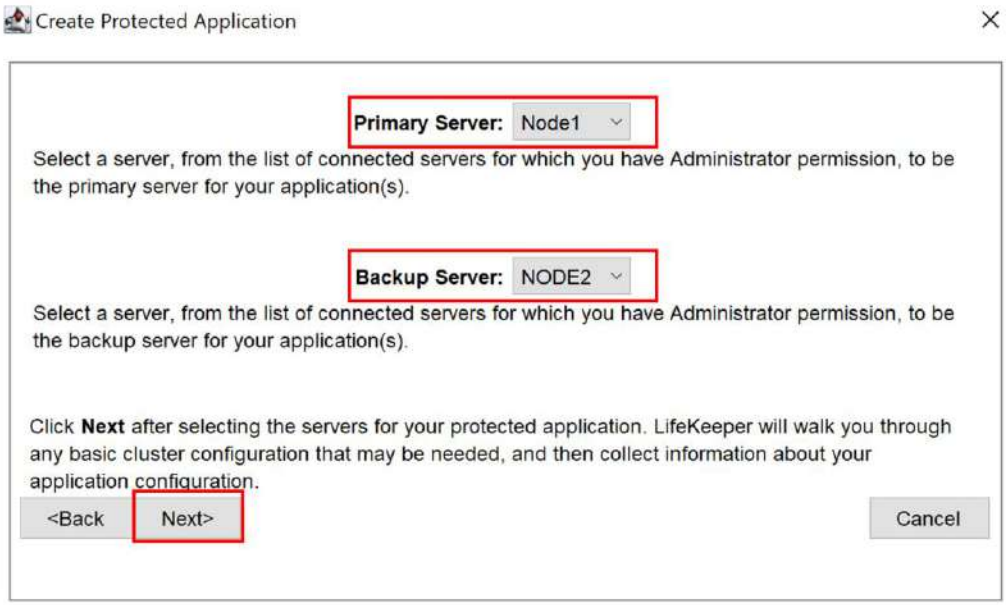


図 8.3.2-3 稼働系と待機系の選択

（4） 保護するアプリケーションの選択

保護するアプリケーション「Application to protect」のリストボックスで「Generic Application」 を選択します。「Next >」 をクリックします。

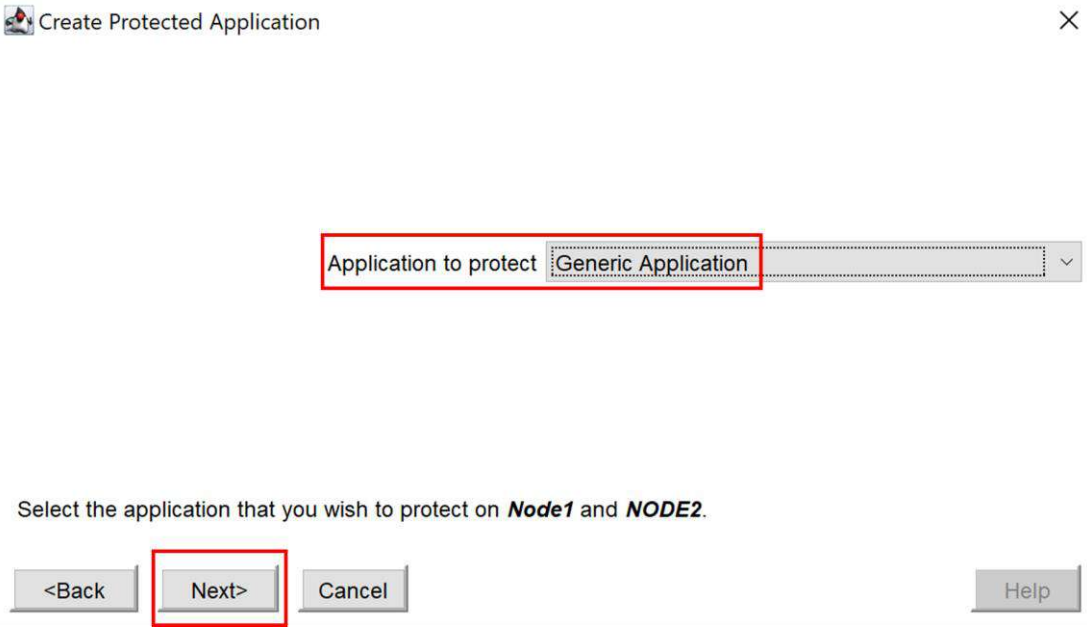


図 8.3.2-4 保護するアプリケーションを選択する

(5) Restore 用のスクリプトの選択

「Restore Script」のテキストボックスに、Restore 用のスクリプトが保存されているディレクトリのパス「C:¥LK¥GenArk¥GenLB-W¥restore.pl」を入力します。

設定が完了したら、「Next >」ボタンをクリックします。

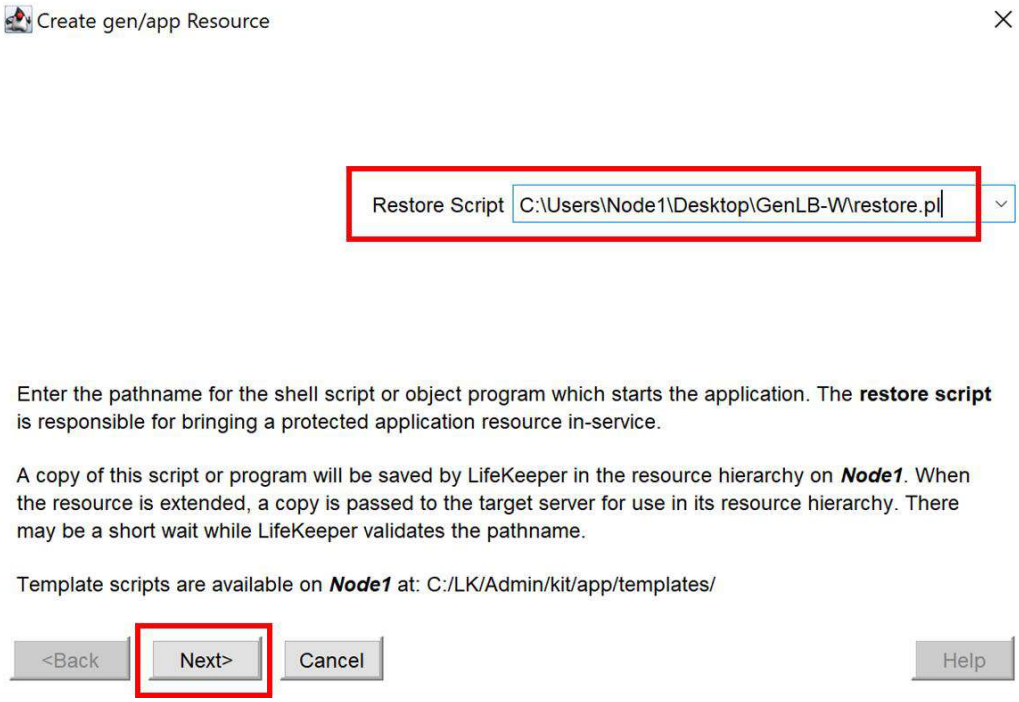


図 8.3.2-5 Restore 用のスクリプトの選択

（5） Remove 用のスクリプトの選択

「Remove Script」のテキストボックスに、Remove 用のスクリプトが保存されているディレクトリのパス「C:¥LK¥GenArk¥GenLB-W¥remove.pl」を入力します。

入力できたら、「Next >」 をクリックします。

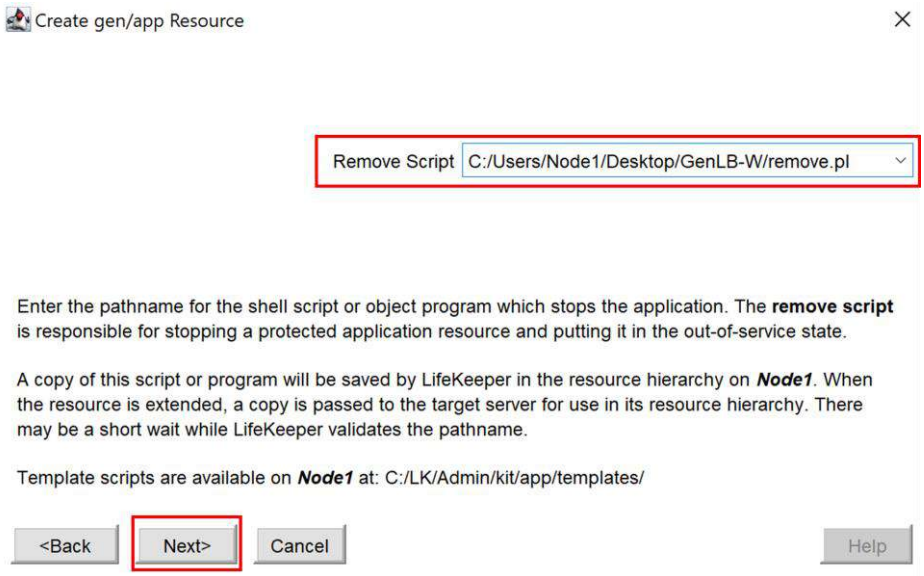


図 8.3.2-6 Remove 用のスクリプトの選択

（6） QuickChek 用のスクリプトの選択

「Quick Check Script [optional]」の入力欄に QuickChek 用のスクリプトのディレクトリ 「C:¥LK¥GenArk¥GenLB-W¥quickchk.pl」 を入力します。

入力できたら、「Next >」 をクリックします。

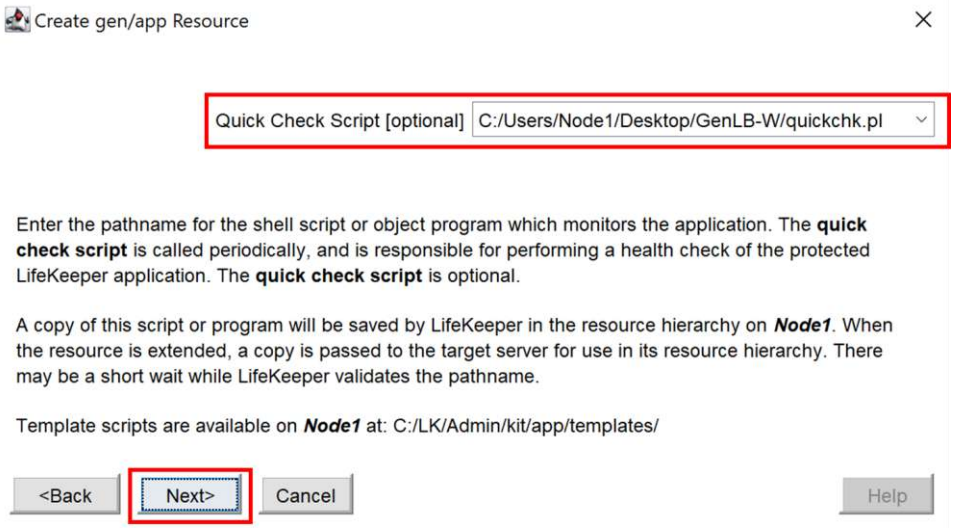


図 8.3.2-7 QuickChek 用のスクリプトの選択

（7） Deepcheck と Local Recovery

GenLB リソースにおいて、Deepcheck と Local Recovery は実施しないため、入力欄を空白のままにして 「Next >」 をクリックします。

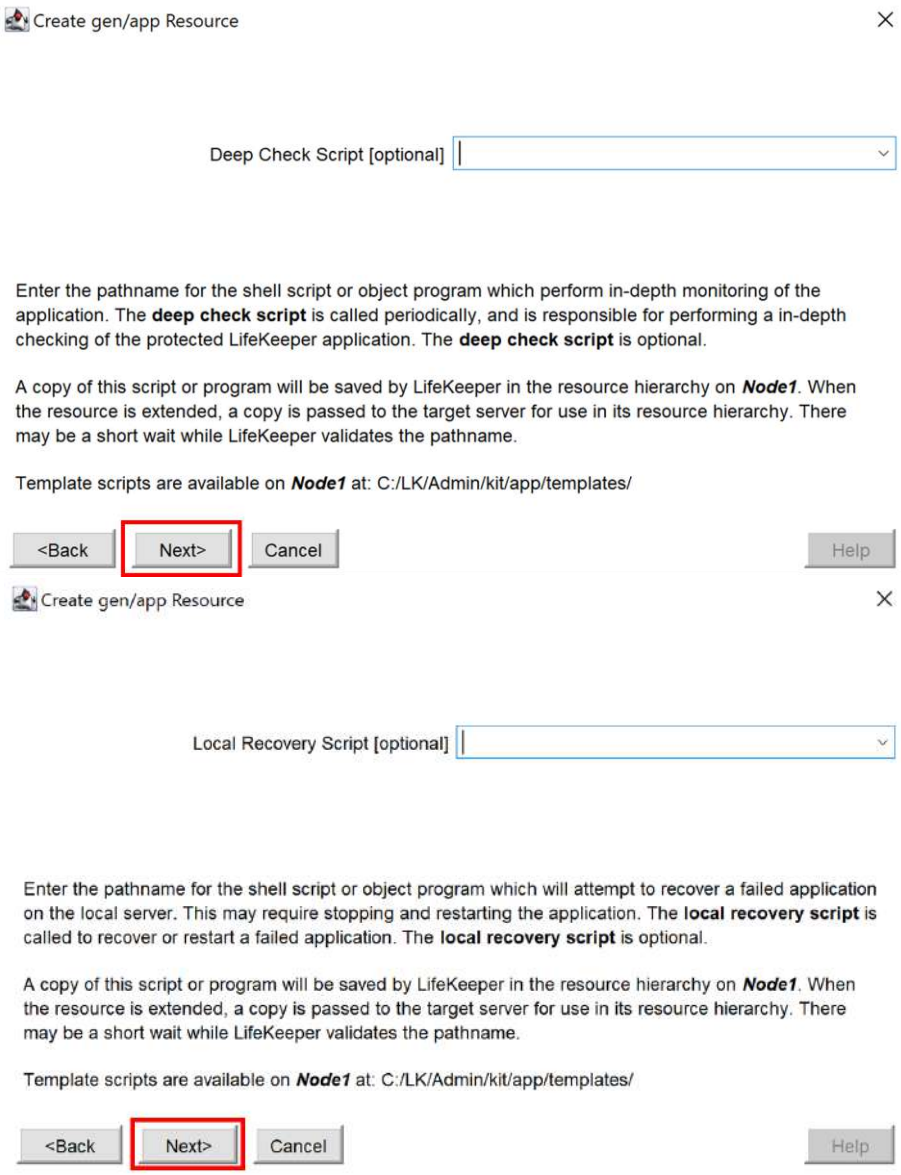


図 8.3.2-8 Deepcheck と Local Recovery は入力しない

（8） Application Info の入力

GenLB リソースでは、Application Info は正常性プローブが使用しているポート番号になります。「Application Info 「optional」」の入力欄に正常性プローブが使用しているポート番号 「12345」 を入力します。

入力できたら、「Next >」 をクリックします。

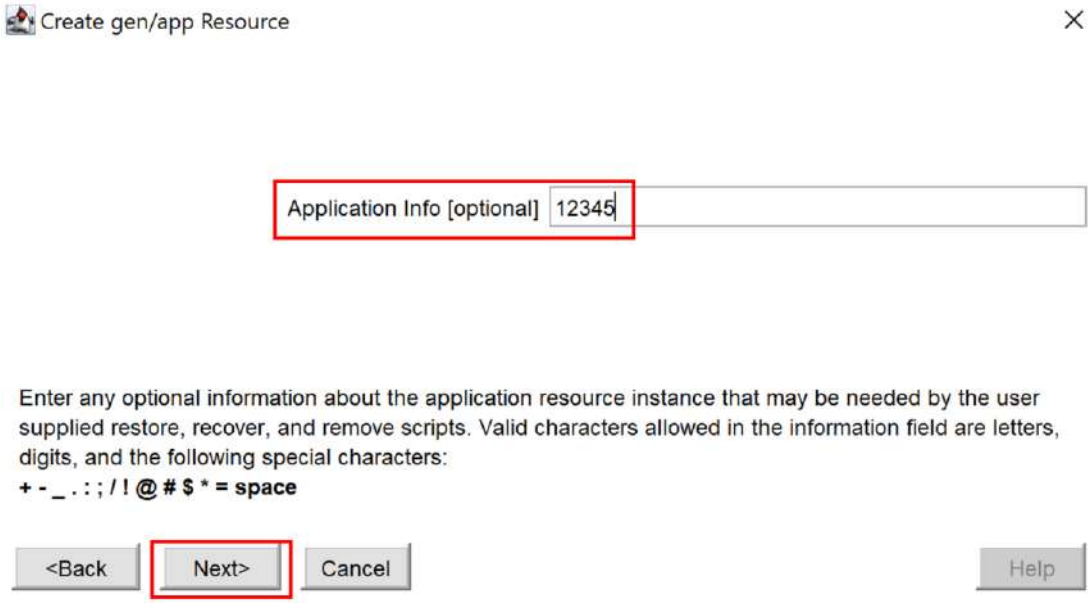


図 8.3.2-9 Application Info の入力

（9） リソースのタグ名の入力

「Resource Tag Name」にリソースのタグ名 「GenLB」 を入力します。

入力できたら、「Create Instance」 をクリックしてリソースを作成します。

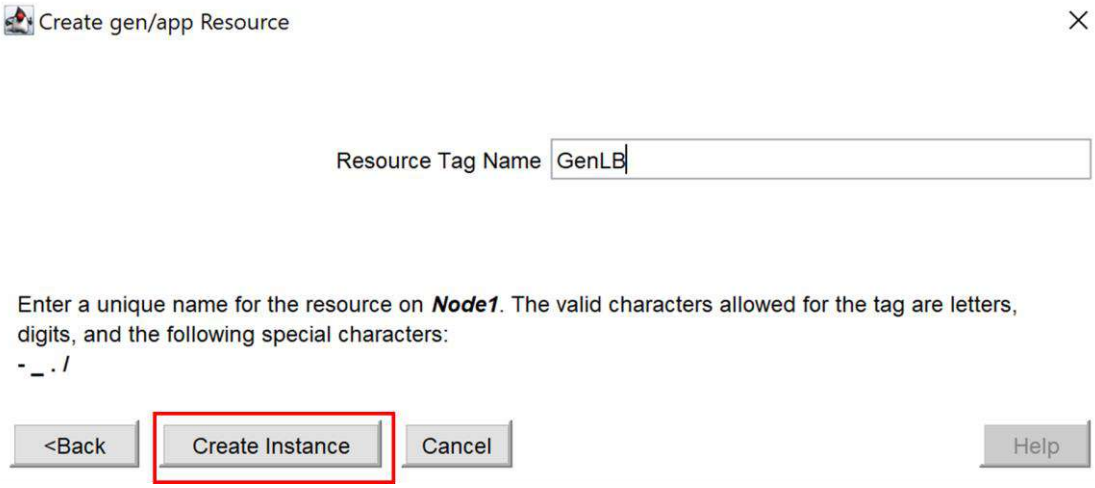


図 8.3.2-10 リソースのタグ名の入力

（10） 待機系ノードでリソースの作成

待機系ノードにてリソースが作成されていることを示す画面が開きます。
作成が完了したら、「Next>」をクリックします。

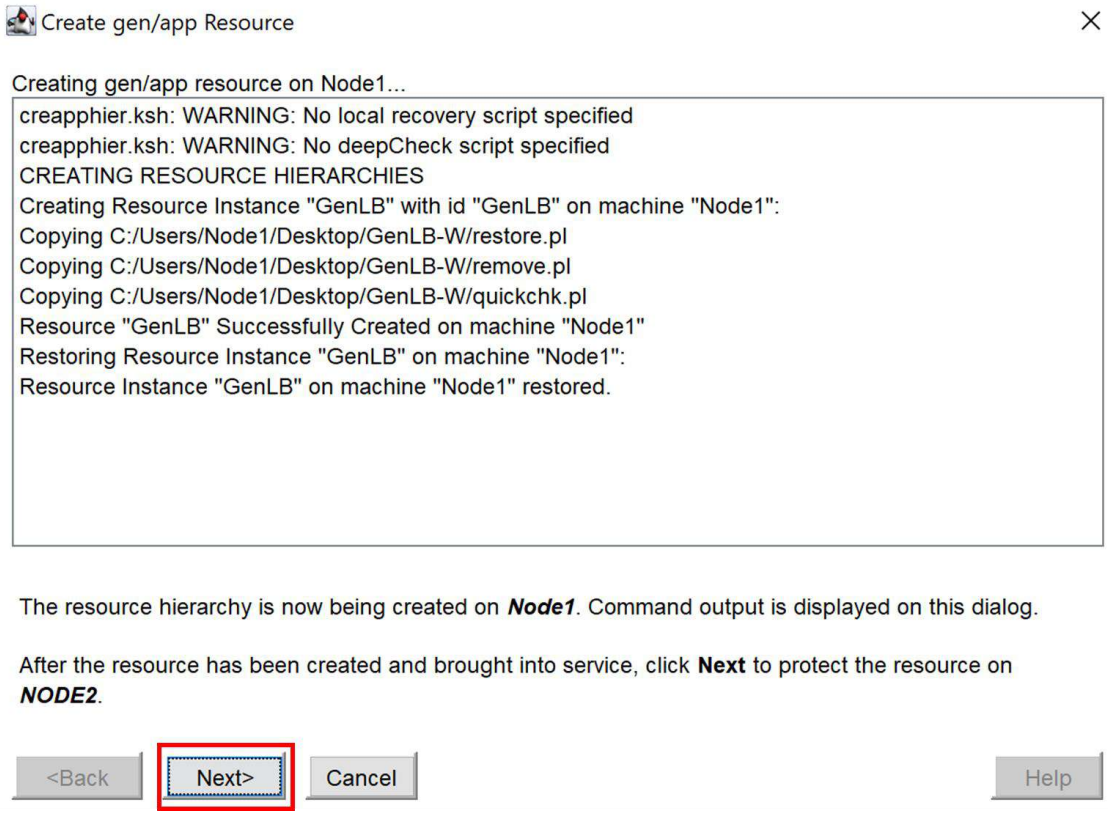


図 8.3.2-11 Primary Server にリソースが作成される

（11） PreExtend チェック

待機系ノードへの拡張可能か（PreExtend）をチェックする画面が開きます。
待機系ノードへ拡張するとは、リモートサーバにリソースを追加することを指します。

「PreExtend checks were successful」が表示されれば、待機系ノードへ拡張可能であることを確認できました。「Next >」 をクリックします。

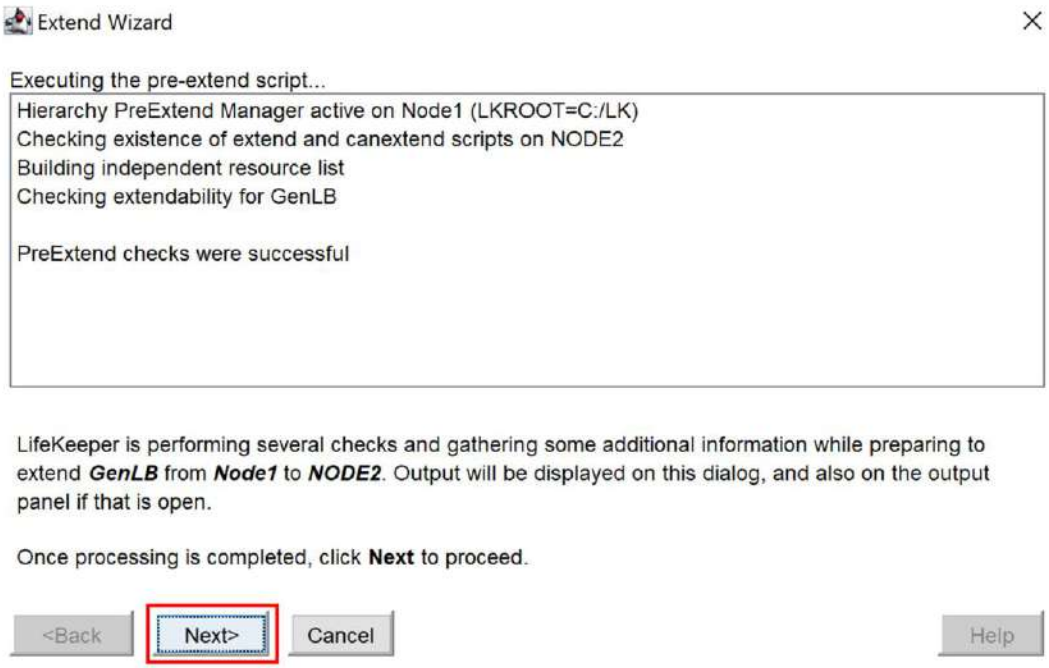


図 8.3.2-12 PreExtend チェック

（12） 待機系ノードのバックアップ優先度の設定

バックアップの優先度（Backup Priority）は、フェイルオーバーが発生した場合にリソースの起動優先度を示します。

同じ階層に複数のリソースが存在する場合、優先度の高いリソースが先に起動されます。

「Backup Priority」に 「10」 と入力します。

入力が完了したら、「Next >」 をクリックします。

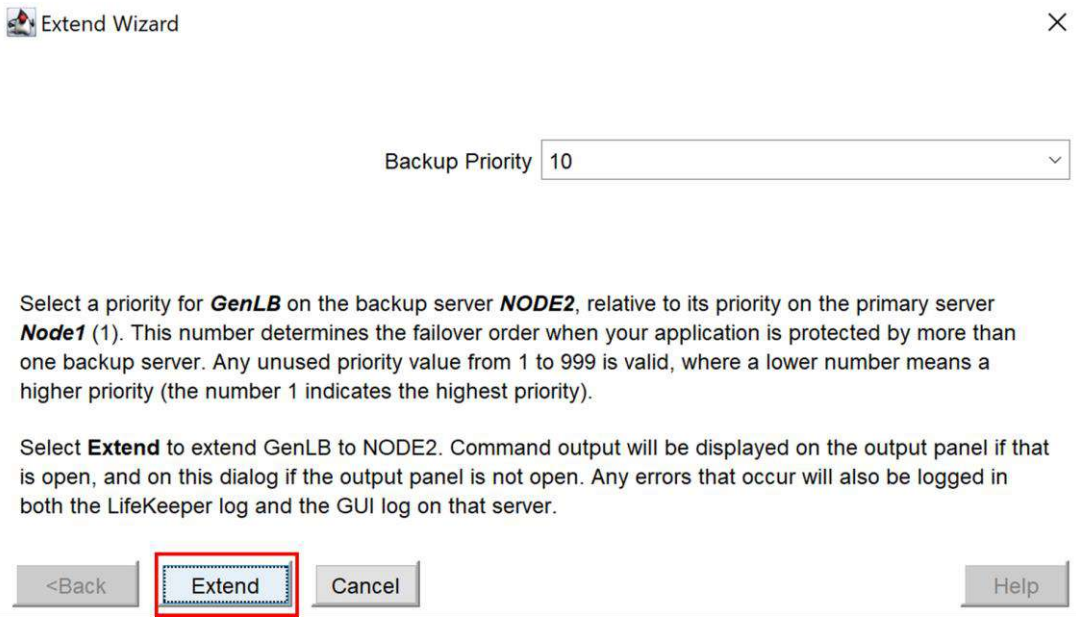


図 8.3.2-13 バックアップ優先度の設定

（13） GenLB リソースの拡張完了

「Hierarchy extend operation completed」というメッセージが表示された場合、GenLB リソースが待機系ノードに正常に拡張されたことを確認できます。これにより、GenLB リソースが LifeKeeper によって保護され、障害が発生した場合に対向ノードにフェイルオーバーすることが可能になります。

「Finish」 をクリックして GenLB リソースの作成を完了します。

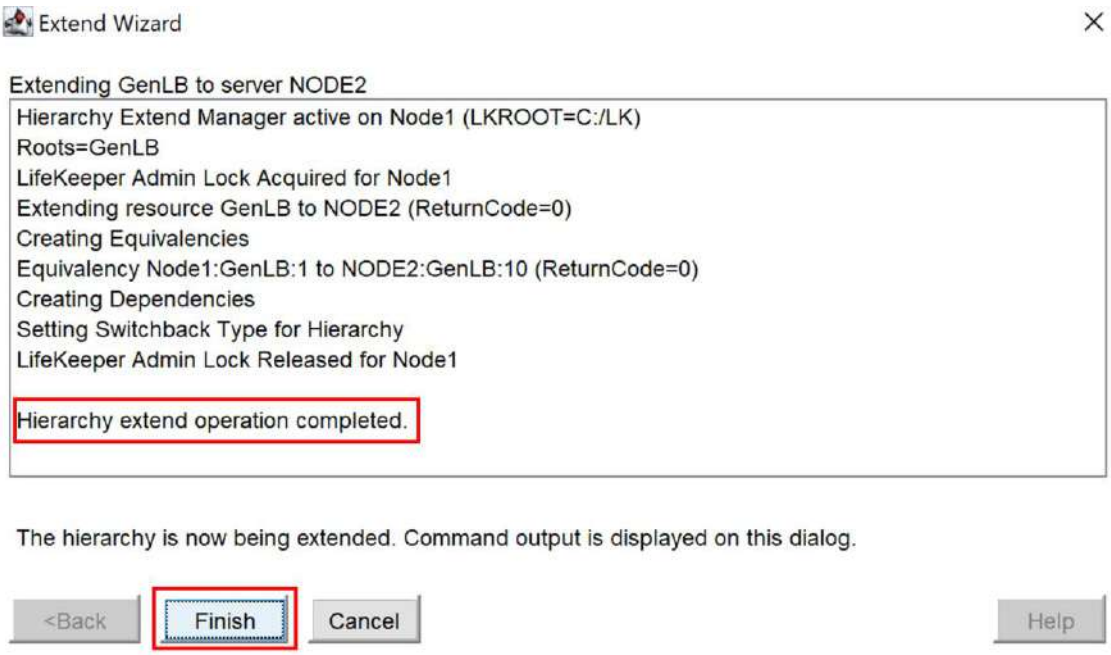


図 8.3.2-14 GenLB リソースの拡張が完了

（14） GenLB リソースが作成完了

リソースが作成された後、LifeKeeper の GUI は以下の画面のように GenLB リソースは稼働系ノードに 「Active」 ステータスで、待機系ノードに「StandBy」ステータスが表示されます。

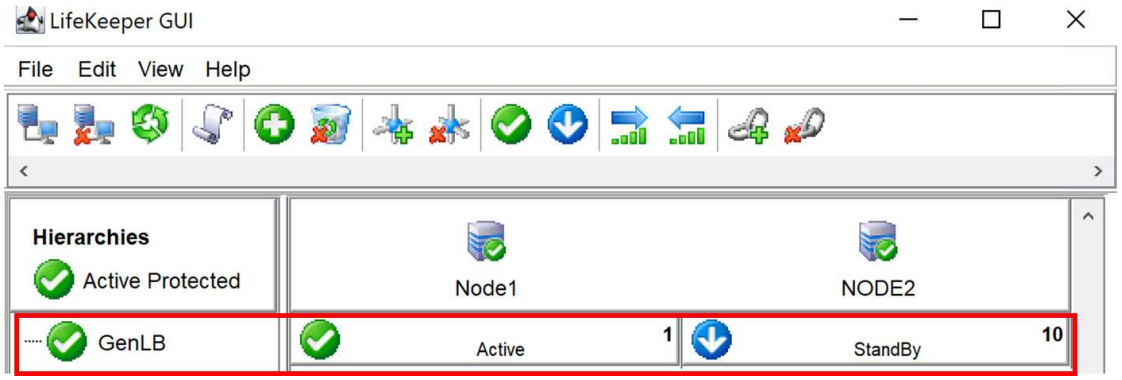


図 8.3.2-15 GenLB リソースが作成完了

8.4. IP リソースの作成

8.4.1. IP リソースの概要

LifeKeeper は、クラスタノードの IP アドレスを直接使用せず、代わりに仮想 IP アドレスを活用して IP の正常性を監視し、保護します。この仮想 IP は、常に動作して

いるノードにマッピングされ、通信ルートが確保されます。 しかし、Azure の仮想ネットワークでは、この仮想 IP が使用している IP アドレスは認識されません。

このため、LifeKeeper for Windows が元々想定していたような仮想 IP アドレスを使用したネットワーク通信や保護は行えません。 その代替手段として、Azure では内部ロードバランサ（ILB）を設置します。ILB のフロントエンド IP アドレスを仮想 IP として用い、バックエンドプールの IP アドレス（実際にトラフィックが転送される IP アドレス）を動作ノードと待機ノードの NIC の IP アドレス（仮想 IP が保護する IP アドレス）に設定することで、ネットワーク通信ルートを確保し転送することが可能です。

IP リソースを作成することで、仮想 IP アドレスを活用してネットワーク通信ルートを保護し、転送することができます。その前に、ILB が使用しているフロントエンドとバックエンドプールの IP アドレスを確認する必要があります。

8.4.2. ILB が使用している IP アドレスの確認

ILB が使用しているフロントエンド IP アドレスを確認します。

（1） フロントエンド IP アドレスの確認

Azure Portal で作成したロードバランサリソースの管理画面を開きます。
「フロントエンド IP 構成」タブを選択し、ILB が使用しているフロントエンド IP アドレスを確認します。

図 8.4.2-1 フロントエンド IP の確認

（2） バックエンド IP アドレスの確認

ILB が使用しているバックエンド IP アドレスを確認します。

Azure Portal で作成したロードバランサリソースの管理画面を開き、「Backend Pools」タブを選択し、ILB が使用しているバックエンドプールの IP アドレスを確認します。

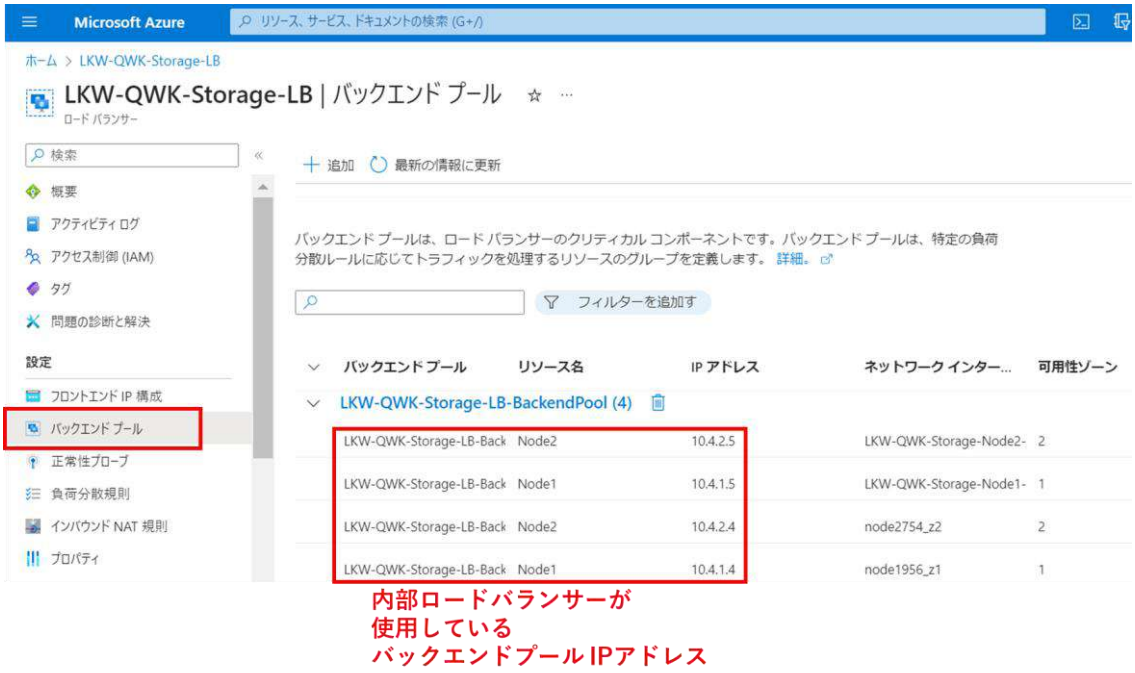


図 8.4.2-2 バックエンド IP アドレスの確認

（3） バックエンドプール IP アドレスの NIC 名の確認

仮想 IP アドレスが保護するバックエンドプールの IP アドレスの NIC 名を確認します。

稼働ノードおよび待機ノードでそれぞれ PowerShell を開き、ipconfig コマンドを実行して NIC 名と IP アドレスの情報を取得します。

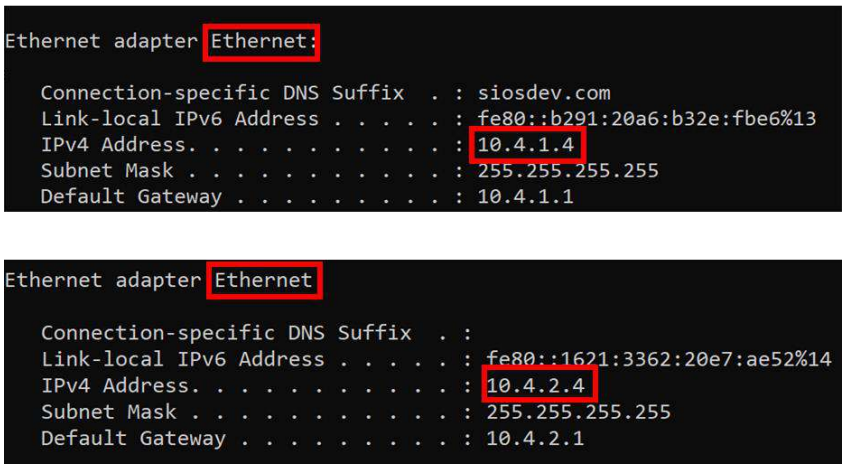


図 8.4.2-3 バックエンドプール IP アドレスの NIC 名の確認

8.4.3. IP リソースの作成

稼働系ノードは Primary Server、待機系ノードは Backup Server として設定します。

（1） リソース階層の作成

GUI 画面からリソース階層の作成アイコン 「Create Resource Hierarchy」 をクリックして、リソース階層の作成ウィザードを開きます。

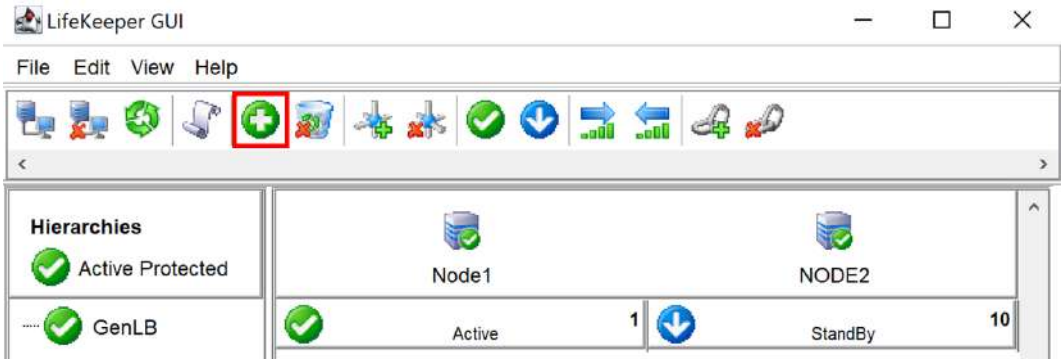


図 8.4.3-1 リソース階層の作成

（2） 稼働系ノードと待機系ノードの選択

Primary Server と Backup Server をリストボックスから選択し、 「Next >」 をクリックします。

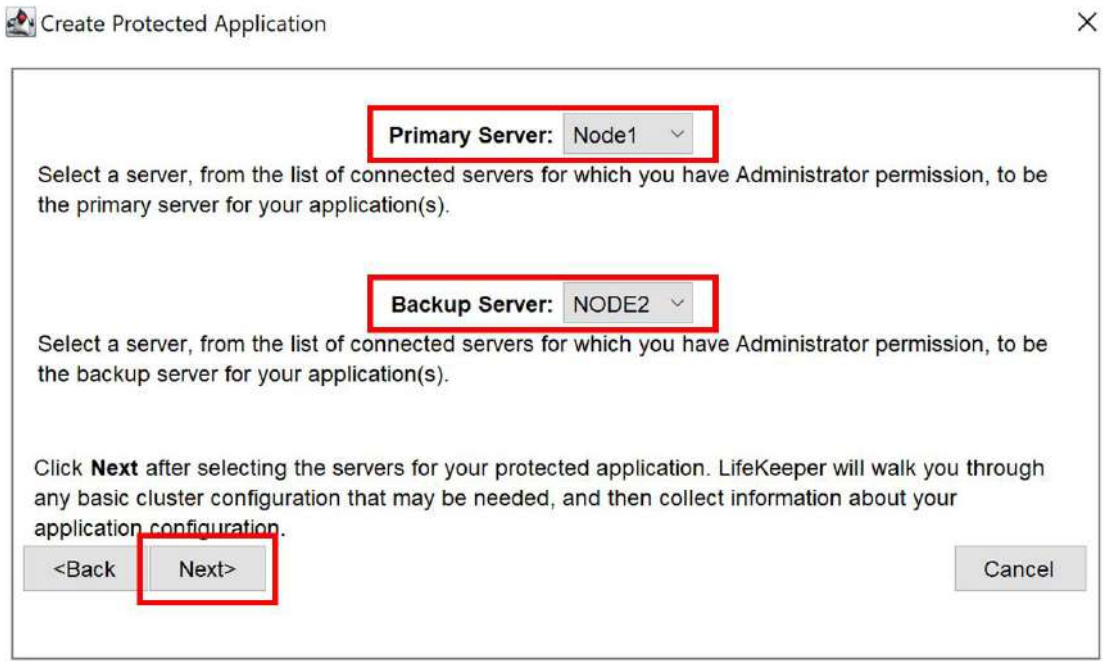


図 8.4.3-2 稼働系ノードと待機系ノードの選択

（3） 保護するアプリケーションの選択

保護するアプリケーションを選択します。

「Application to protect（保護するアプリケーション）」のリストボックスから「IP Address」を選択し、「Next >」ボタンをクリックします。

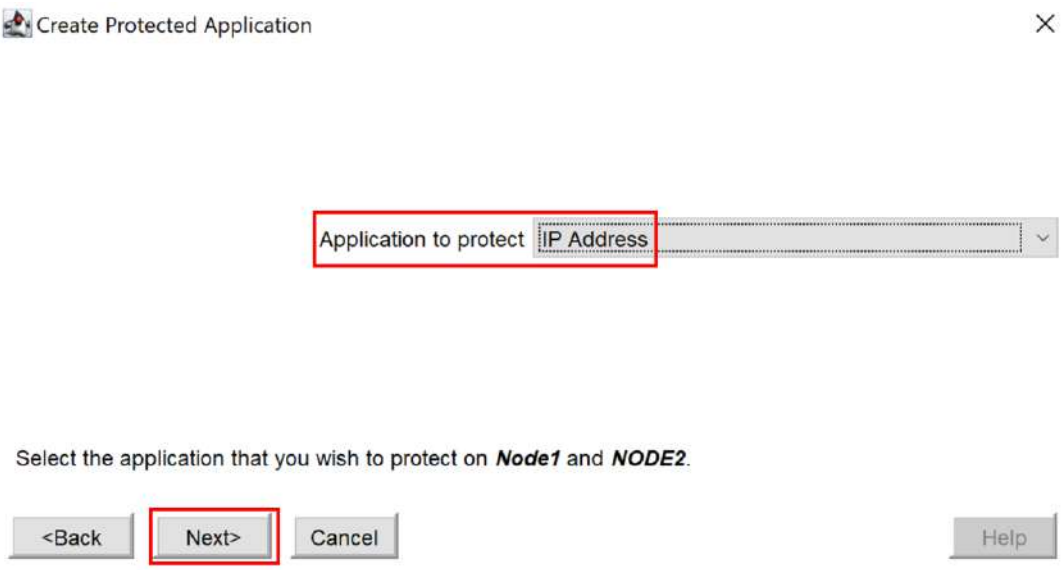


図 8.4.3-3 保護するアプリケーションの選択

（4） 仮想 IP アドレスの設定

IP アドレスリソースで保護する仮想 IP アドレスを設定します。

「IP Address」欄に 内部ロードバランサが使用しているフロントエンド IP アドレスを入力します。

入力できたら、「Next >」 をクリックします。

図 8.4.3-4 仮想 IP アドレスの設定

（5） 保護する IP アドレスのサブネットマスクの入力

IP リソースによる保護対象となる稼働系ノードの IP アドレスのサブネットマスクを設定します。

「Subnet Mask」 欄に 「255.255.255.255」 と入力します。入力が完了したら、「Next >」 をクリックします。

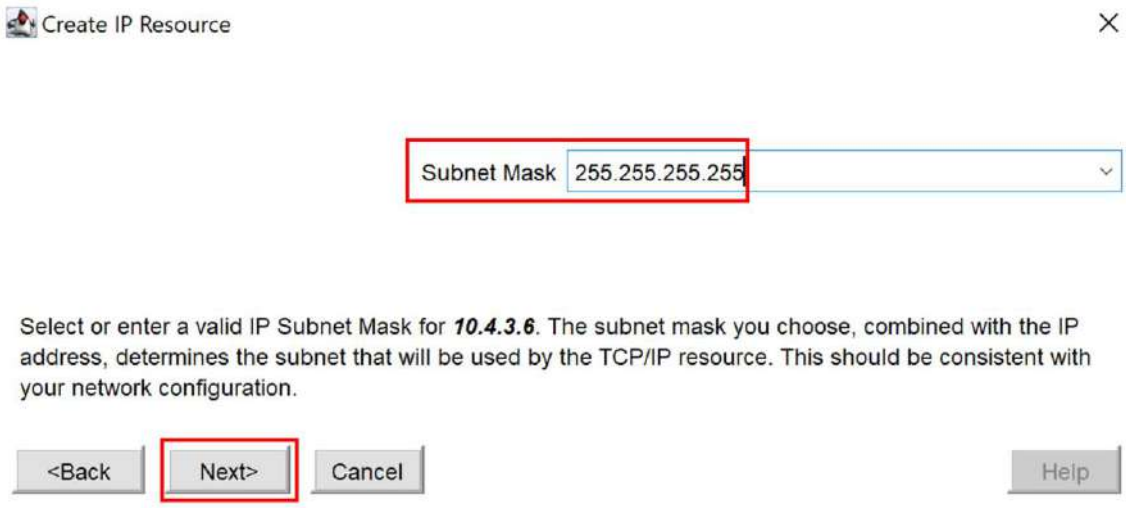


図 8.4.3-5 保護する IP アドレスのサブネットマスクの入力

（6） IP リソースのタグ名の入力

作成する IP リソースのタグ名を入力します。

「IP Resource Tag」にタグ名を入力します。

入力できたら、「Next >」 をクリックします。

図 8.4.3-6 IP リソースのタグ名の入力

（7） 保護する IP アドレスの NIC の選択

仮想 IP アドレス「10.4.3.6」を保護するためのローカルサーバの NIC 名を選択します。

選択できたら、「Next >」 をクリックします。

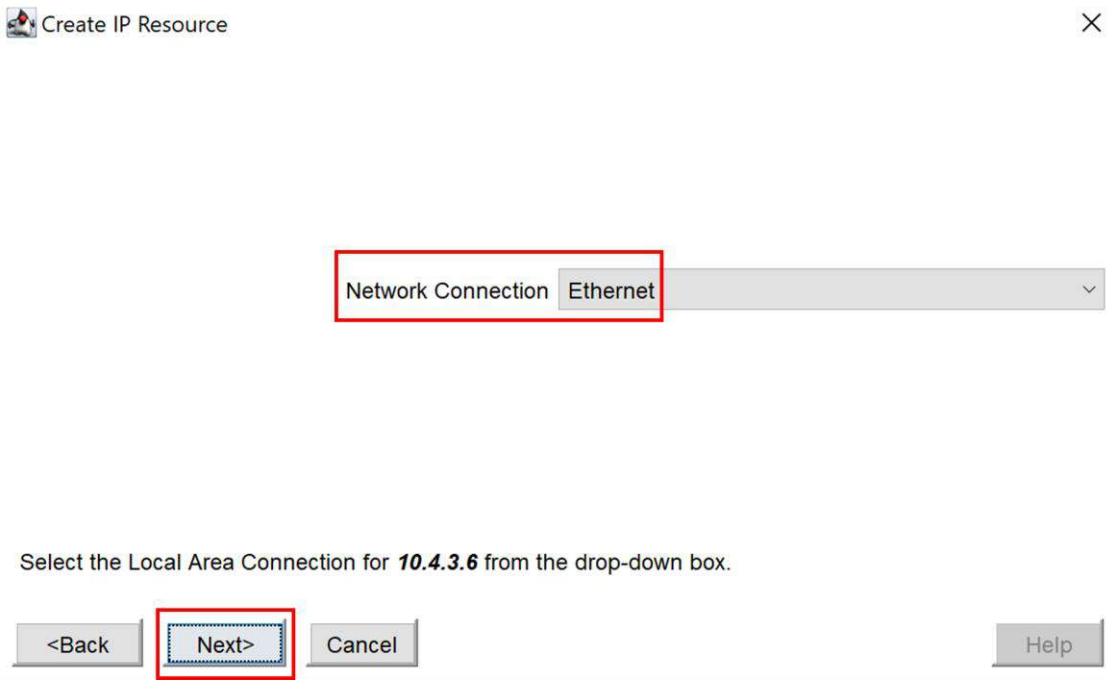


図 8.4.3-7 保護する IP アドレスの NIC の選択

（8） Local Recovery の設定

Local Recovery の設定画面が開きます。
Local Recovery は、障害が発生した場合にそのノードで回復作業を行う機能です。
このガイドでは、Local Recovery を無効にします。「Local Recovery」で「No」を選択し、「Next >」をクリックします。

図 8.4.3-8 Local Recovery の設定

（9） 稼働系ノードでリソースとリソース階層の作成
稼働系ノードでリソースとリソース階層を作成しています。

「INFO (No. xxx) Restore IP Address <仮想 IP アドレス> End: Successful」と表示されたら、稼働系ノードでリソースが正しく作成されました。

「Next >」 をクリックします。

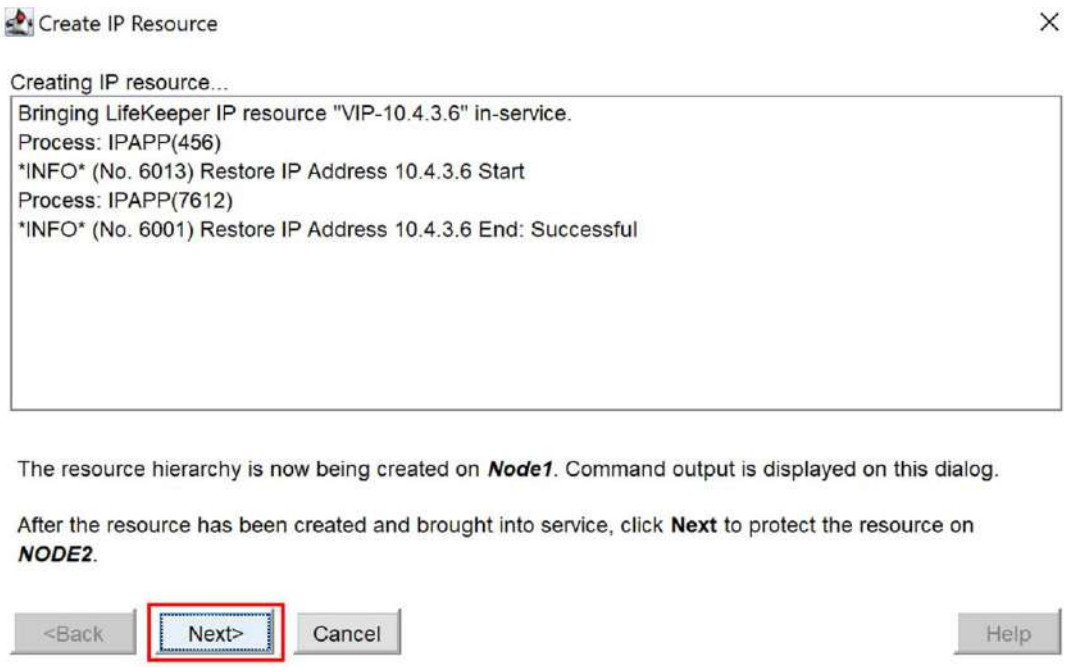


図 8.4.3-9 稼働系ノードでリソースとリソース階層の作成

（10） PreExtend のチェック

待機系ノードへの拡張の可否（PreExtend）を確認する画面が開きます。「PreExtend checks were successful」と表示された場合、IP リソースが待機系ノードに正常に拡張できることが確認されます。

「Next >」をクリックします。

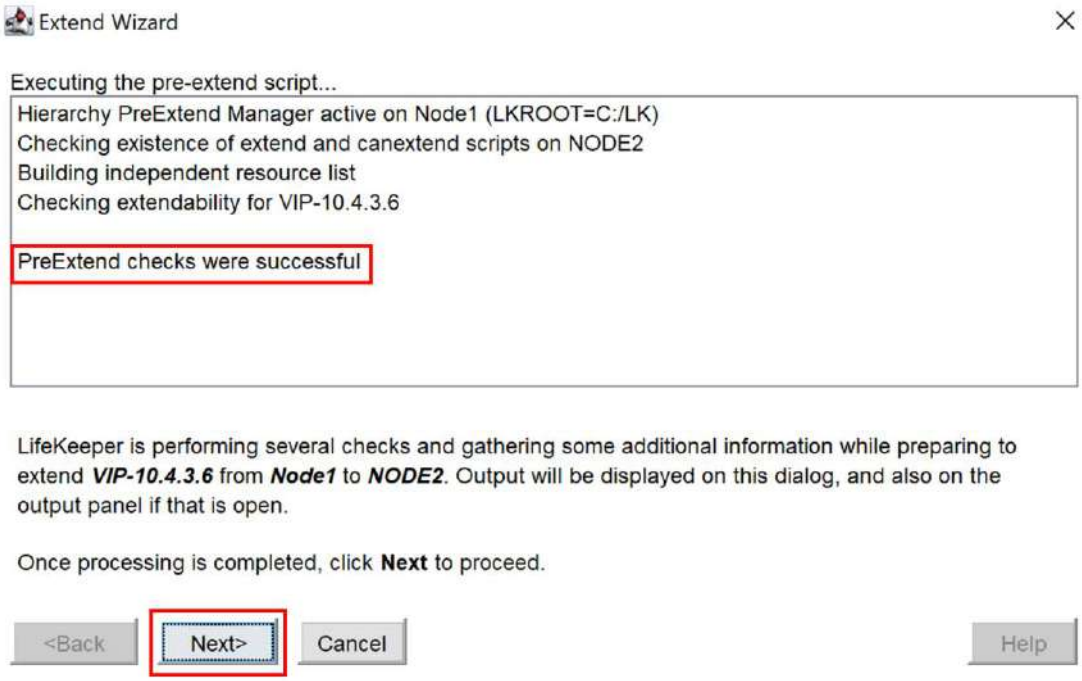


図 8.4.3-10 PreExtend のチェック

次 IP リソースを待機系ノードへ拡張します。
入力項目は稼働系ノードを設定した時と同じです。

（11） 保護する IP アドレスのサブネットマスクの入力
IP リソースによる保護対象となるバックアップサーバの IP アドレスのサブネットマスクを設定します。
「Subnet Mask」に 「255.255.255.255」 を入力します。
入力できたら、「Next>」 をクリックします。

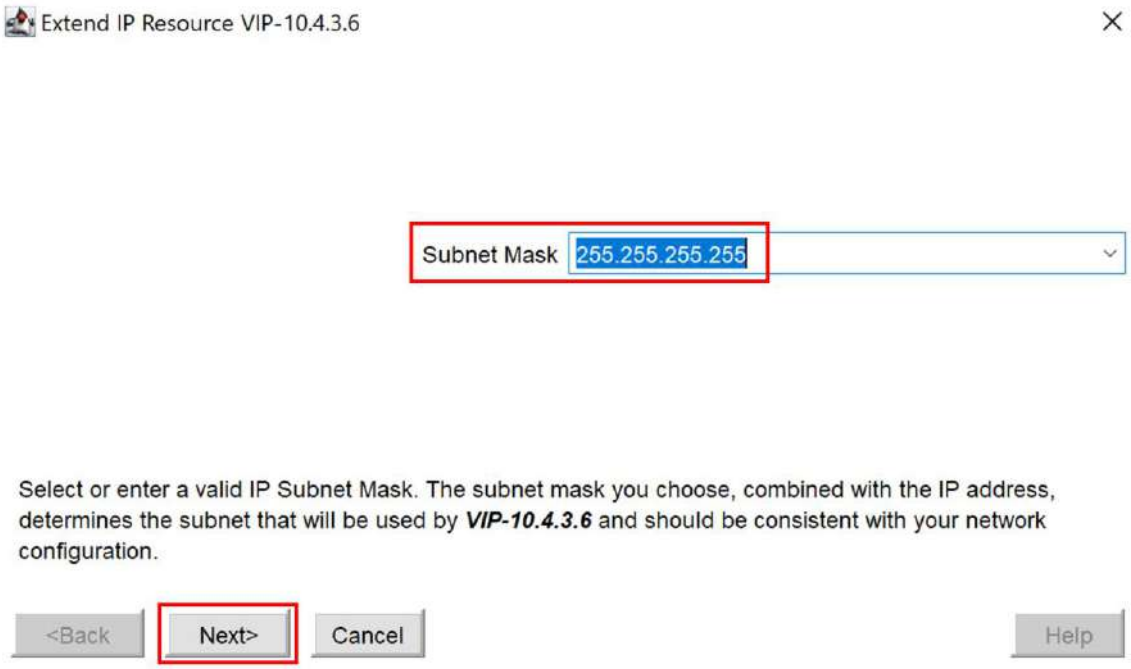


図 8.4.3-11 保護する IP アドレスのサブネットマスクの入力

（12） 保護する IP アドレスの NIC の選択
仮想 IP アドレス 10.4.3.6 を使用して保護する待機系ノードの NIC 名の選択画面が開きます。

選択できたら、「Next >」 をクリックします。

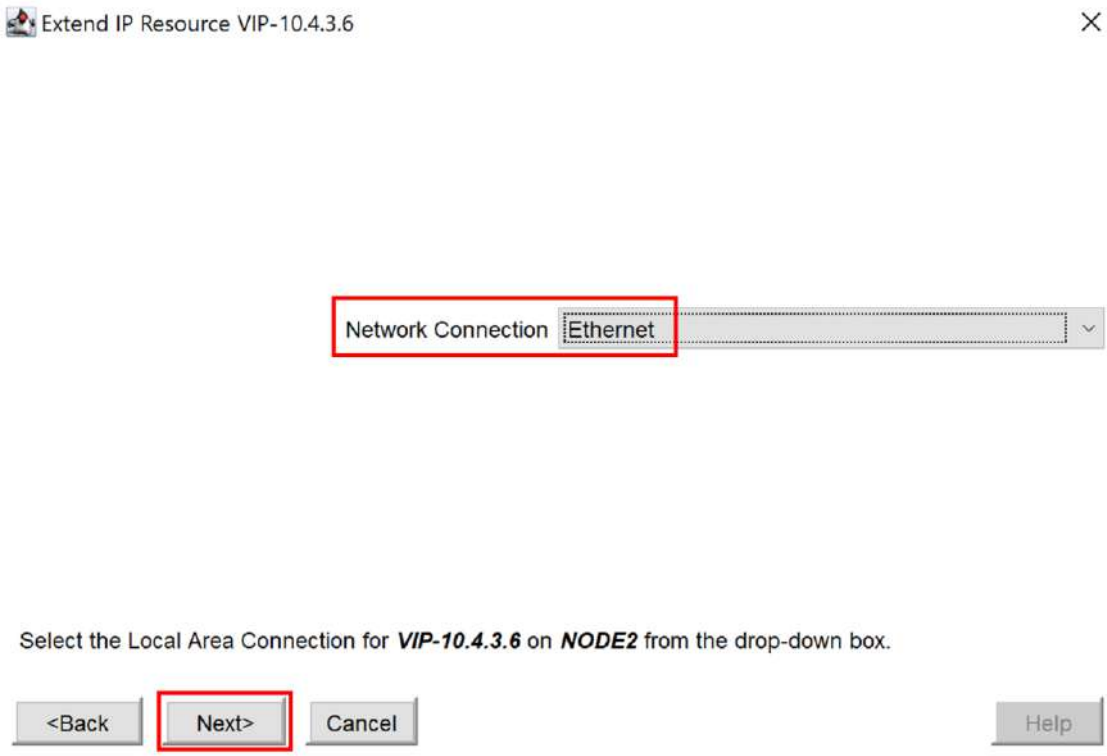


図 8.4.3-12 保護する IP アドレスの NIC の選択

（13） 待機系のリストアモードの選択

IP リソースの Target Restore Mode は、保護対象の IP アドレスがフェイルオーバー後のバックアップサーバで使用可能かどうかを制御する設定です。

本ガイドでは、Target Restore Mode を有効にします。

「Target Restore Mode」で 「Enable」 を選択します。

選択したら、「Next >」 をクリックします。

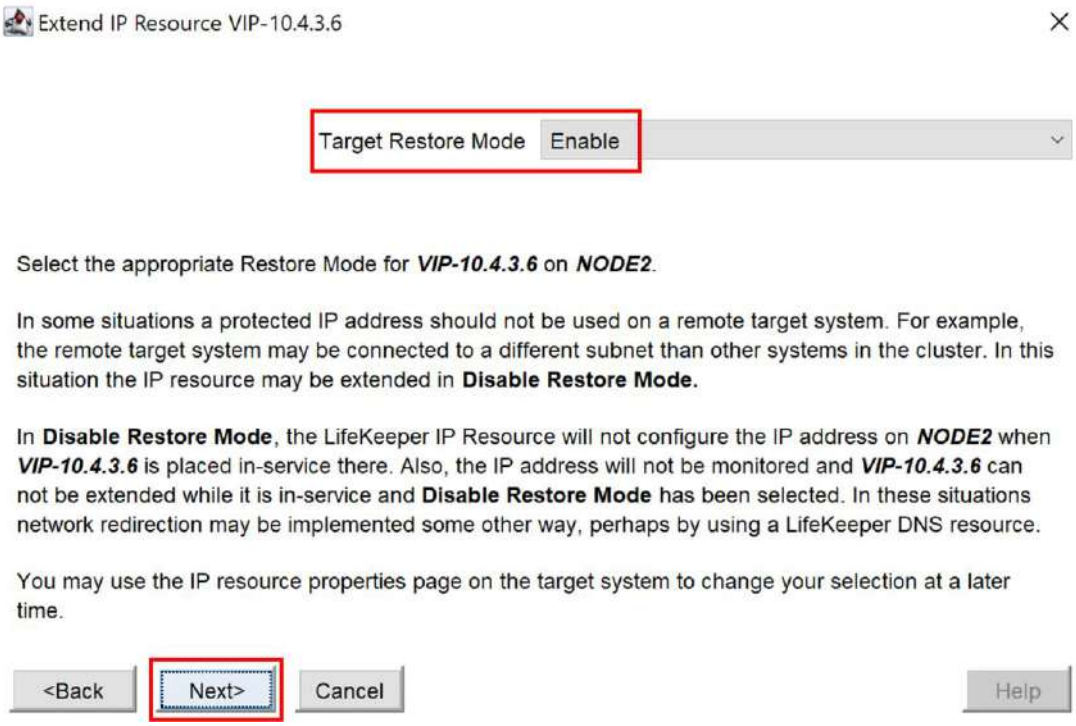


図 8.4.3-13 待機系のリストアモードの選択

（14） Local Recovery の設定

待機系ノードでの Local Recovery 設定画面が開きます。Local Recovery は、障害発生時に待機系ノードでの回復を試みる機能です。

このガイドでは Local Recovery を「No」と設定します。選択後、「Next >」をクリックします。

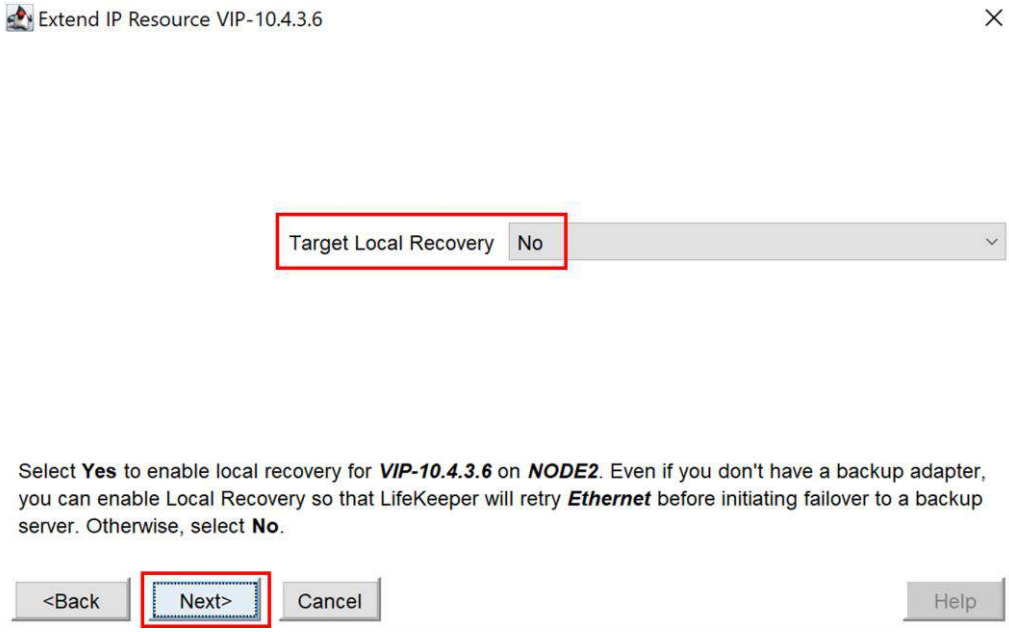


図 8.4.3-14 Local Recovery の設定

（15） 待機系ノードの優先度の設定

待機系ノードの優先度（Backup Priority）を設定します。「Backup Priority」欄に「9」と入力し、「Extend >」をクリックします。

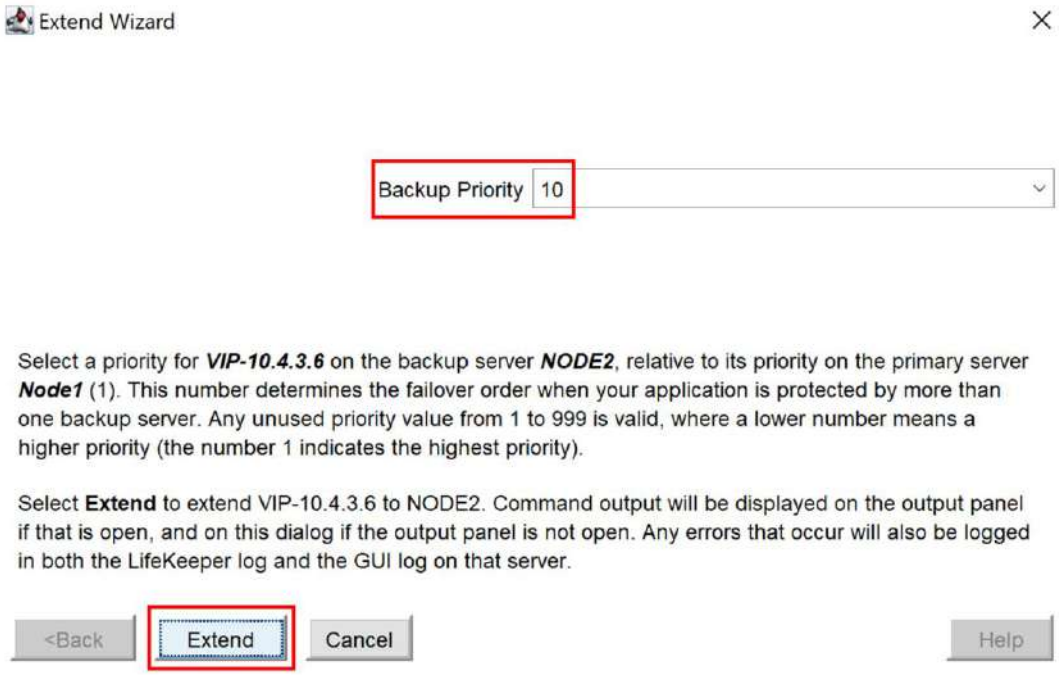


図 8.4.3-15 待機系ノードの優先度の設定

（16） IP リソースの拡張完了

「Hierarchy extend operation completed」と表示されたら、IP リソースが正常にリモートサーバに拡張されました。

「Finish」をクリックして、IP リソースの設定を完了します。

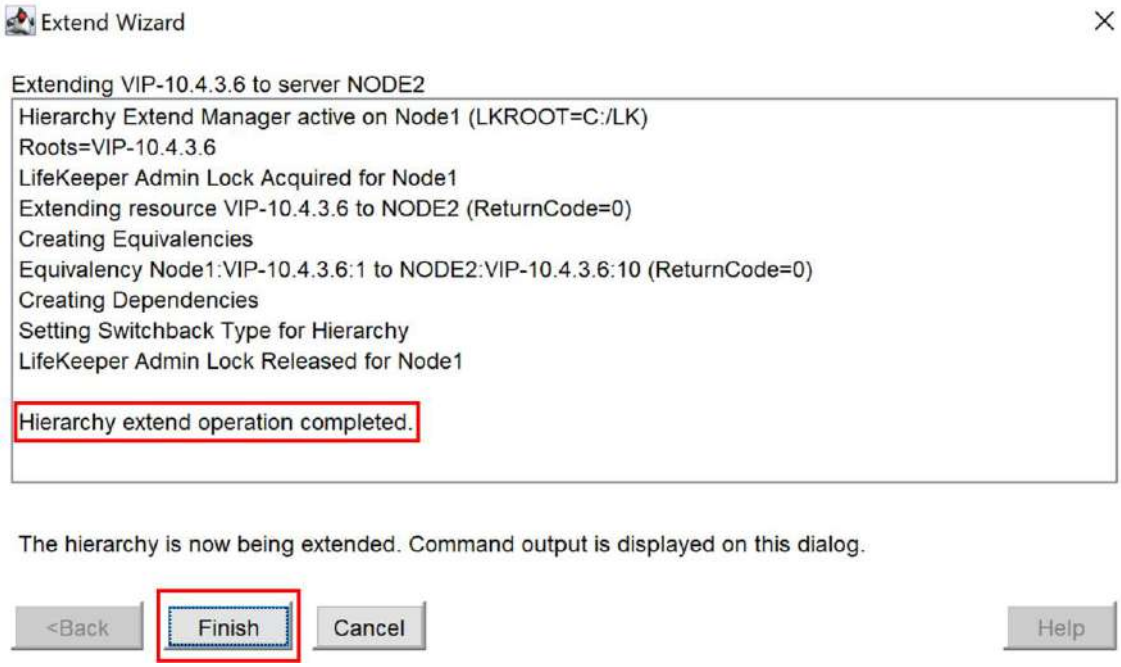


図 8.4.3-16 IP リソースの拡張完了

これで仮想 IP アドレス 10.4.3.6 を使用して、稼働系の IP アドレス 10.4.1.1 と待機系の IP アドレス 10.4.2.4 の正常性を監視し、保護することができます。

8.5. ボリューム リソースの作成

本節では、SQL Server のデータベースを格納する共有ディスクを保護するためのボリュームリソースの作成手順を説明します。

（1） LifeKeeper GUI でリソース作成

リソース階層を作成します。

メニューからリソース階層の作成アイコン［Create Resource Hierarchy］をクリックします。

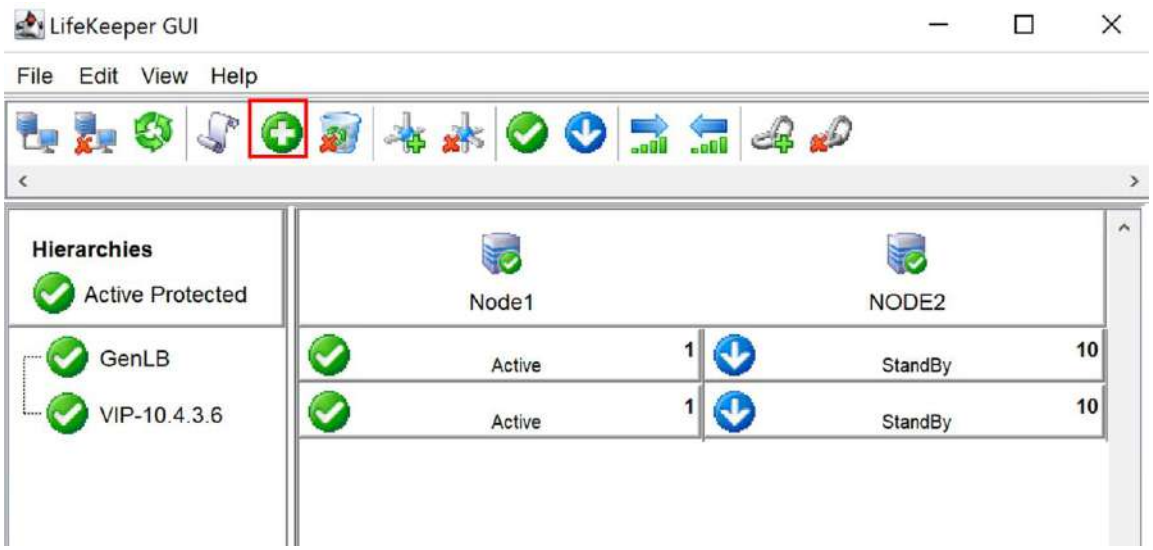


図 8.5.3-1 リソース作成

（2） 稼働系ノードと待機系ノードの選択

稼働系ノードと待機系ノードの選択

Primary Server と Backup Server をリストボックスから選択し、 「Next >」 をクリックします。

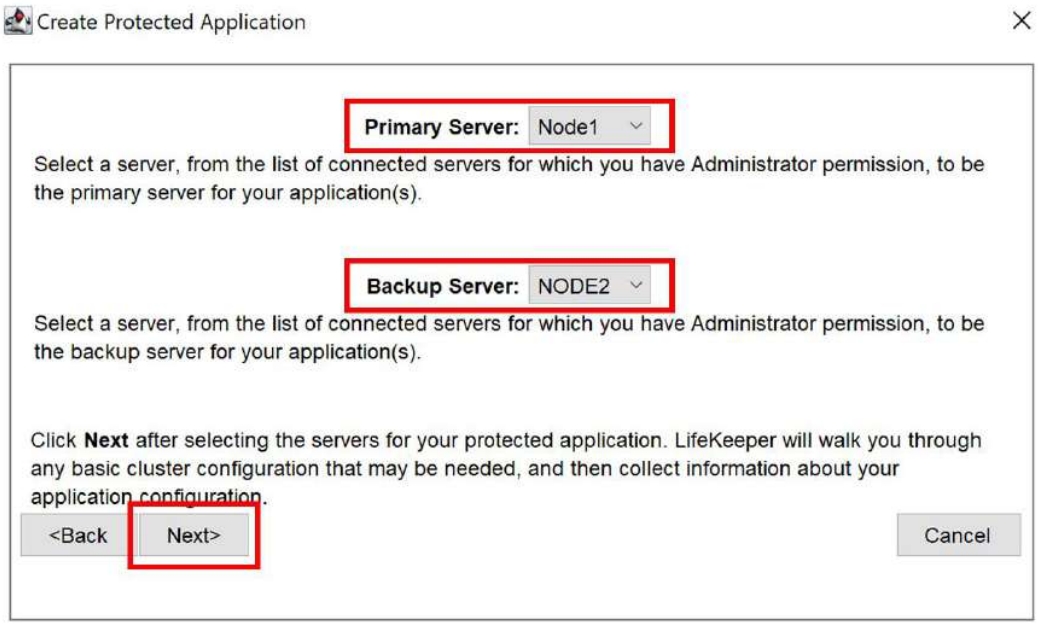


図 8.5.3-2 稼働系ノードと待機系ノードの選択

（3） 保護するアプリケーションの選択

保護するアプリケーション「Application to protect」のリストボックスで「Volume」 を選択し、「Next>」 をクリックします。

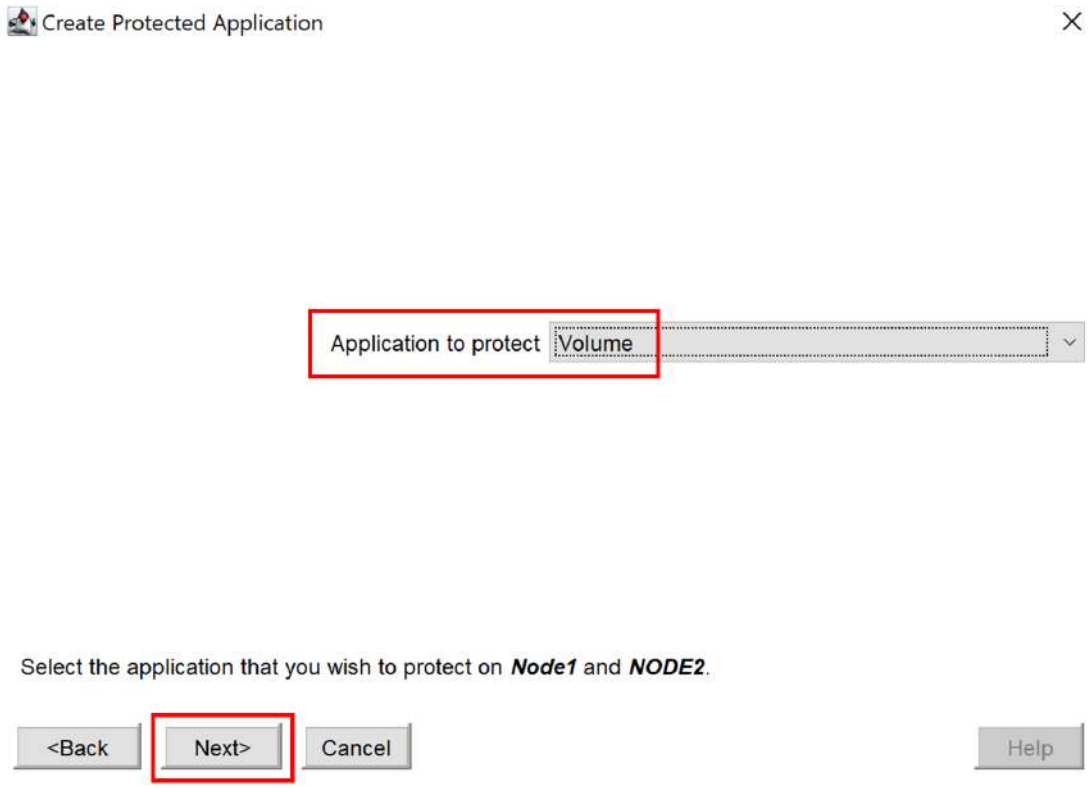


図 8.5.3-3 ボリュームリソースの作成

（4） ボリューム番号の選択

ボリュームリソースが保護するボリュームのドライブ番号を選択し、「Next>」 をクリックします。

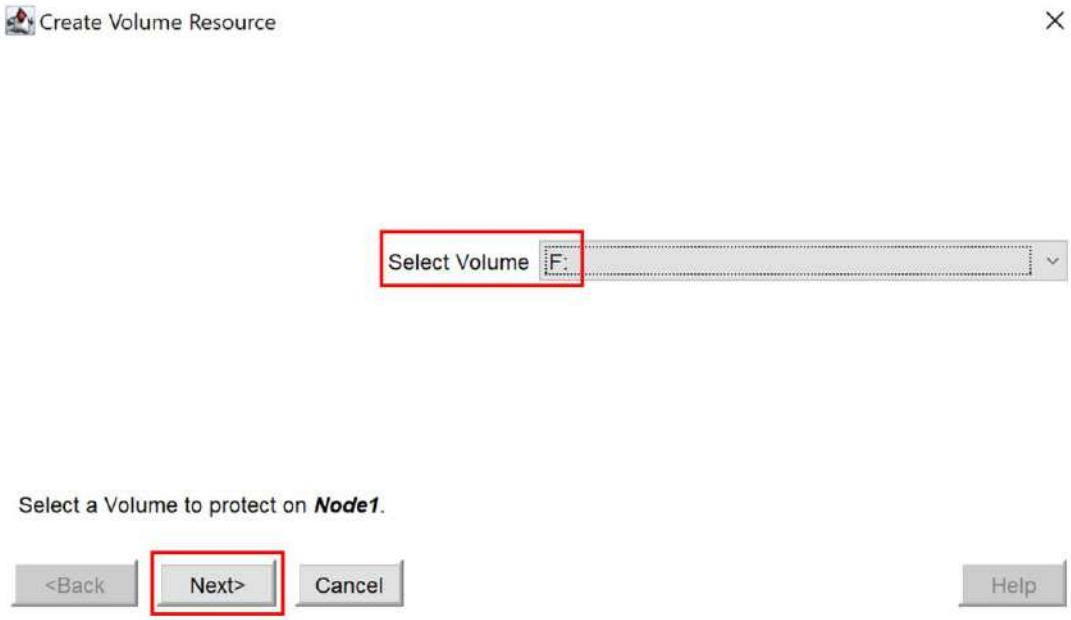


図 8.5.3-4 ボリューム番号の選択

（5） タグ名の入力

「Volume Tag」にタグ名を入力します。

入力できたら、「Next >」 をクリックします。

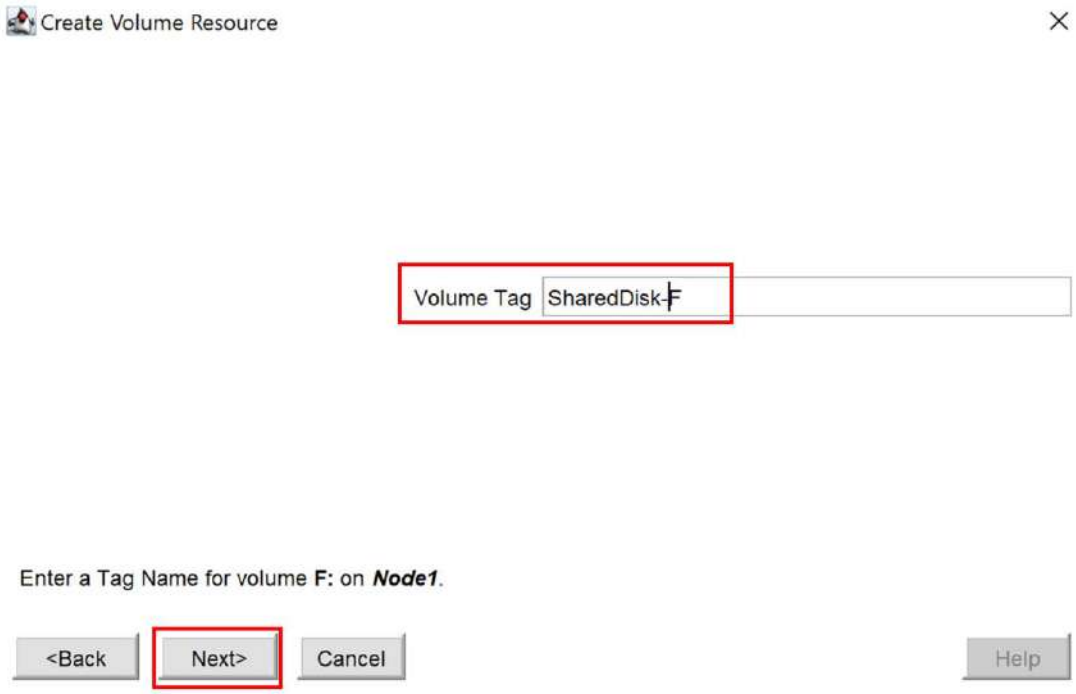


図 8.5.3-5 タグ名の入力

（6） 稼働系ノードでリソース階層の作成

稼働系ノードでリソースとリソース階層を作成しています。

「successfully created」と表示されたら、稼働系ノードでボリュームリソースが正しく作成されました。

「Next >」 をクリックします。

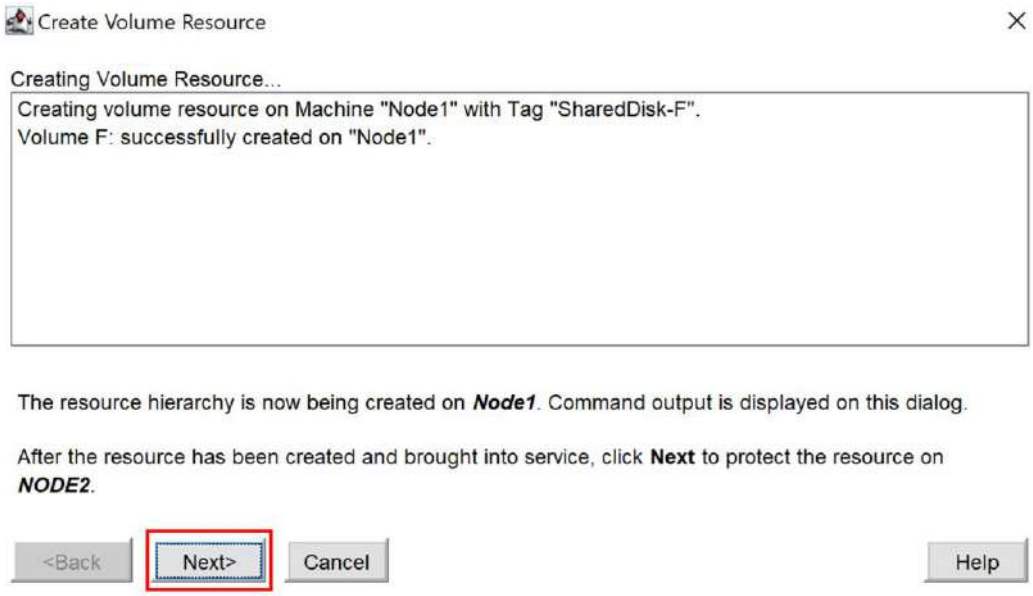


図 8.5.3-6 リソース階層の作成

（7） 待機系ノードへの PreExtend チェック

待機系ノードへの拡張の可否（PreExtend）を確認する画面が開きます。

「PreExtend checks were successful」と表示された場合、リソースが待機系ノードに正常に拡張できることが確認されます。

「Next >」をクリックします。

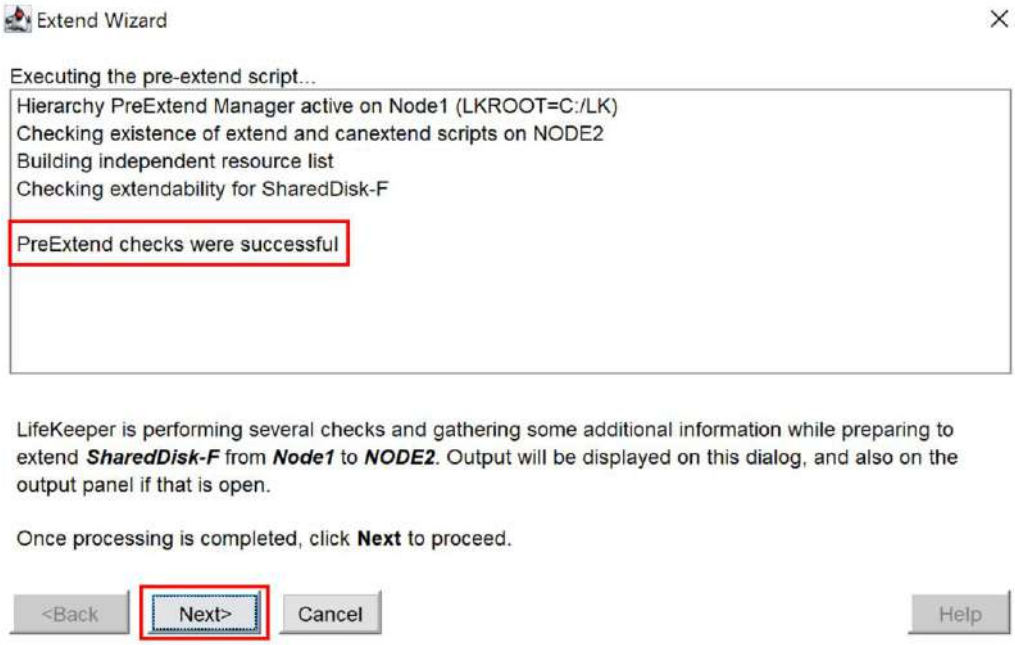


図 8.5.3-7 PreExtend チェック

（8） ボリュームリソースの種類の選択

ボリュームリソースの種類を選択します。

共有ディスクを保護しますので、「Volume Type」に「Shared Disk」を選択し、「Next >」をクリックします。

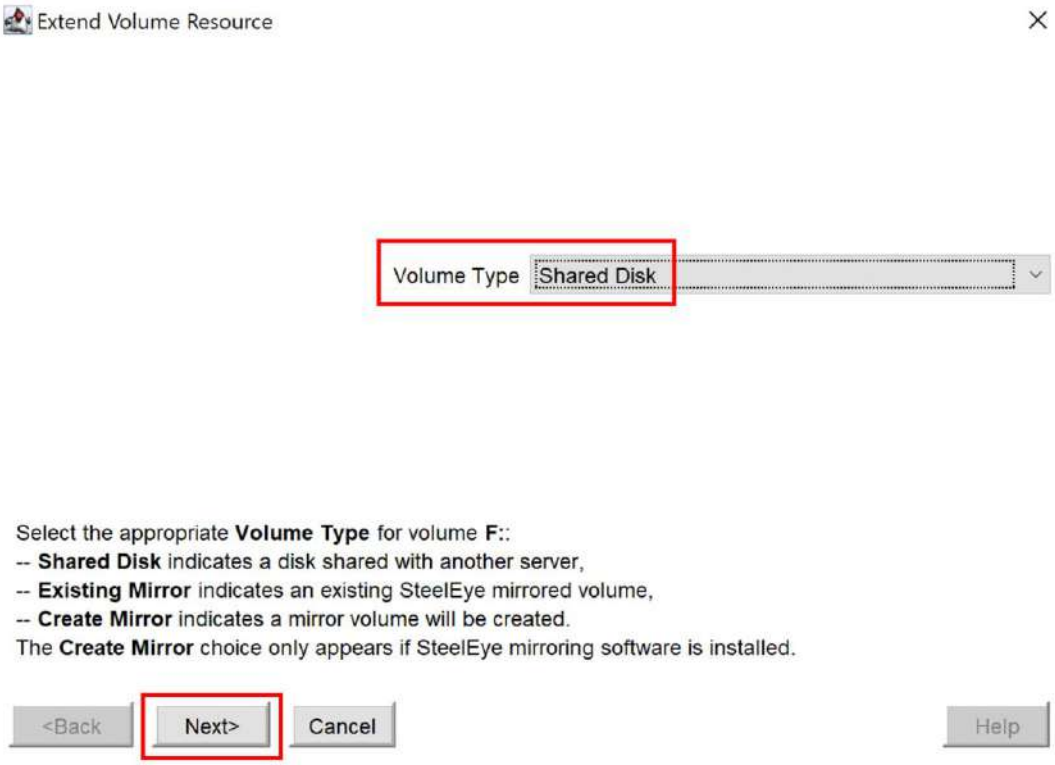


図 8.5.3-8 ボリュームリソースの種類の選択

（9） 優先度の設定

待機系ノードの優先度（Backup Priority）を設定します。「Backup Priority」欄に「10」と入力し、「Extend >」をクリックします。

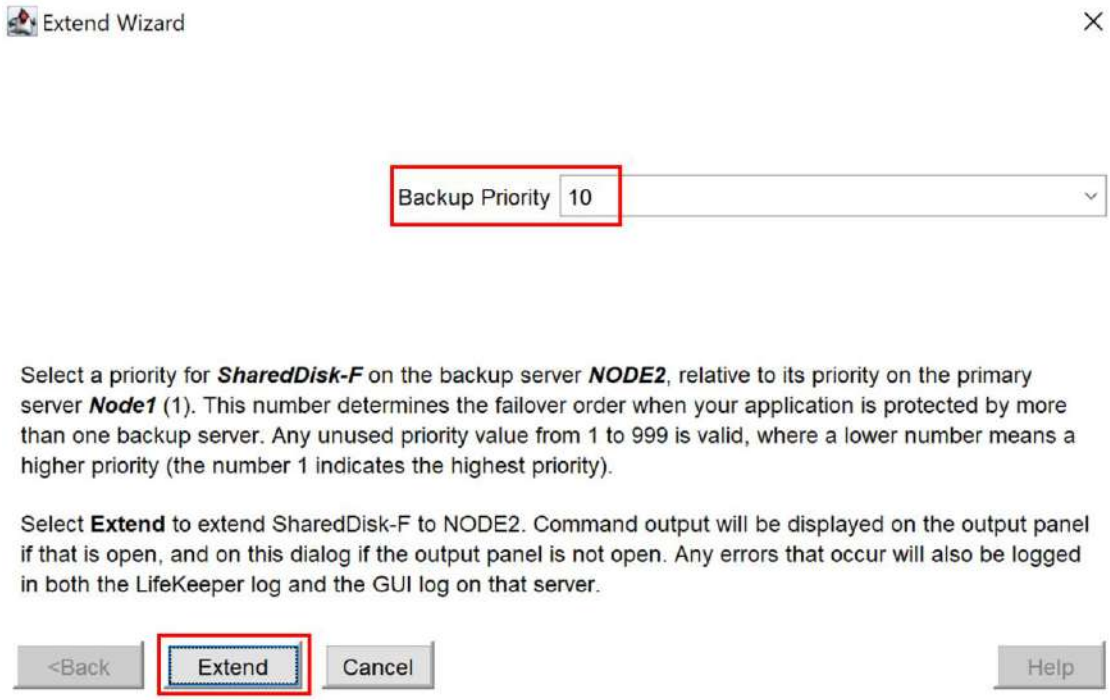


図 8.5.3-9 待機系ノードの優先順位の設定

（10） ボリュームリソースの拡張

ボリュームリソースを待機系ノードに拡張します。

「Hierarchy extend operation completed」というメッセージが表示された場合、ボリュームリソースは待機系ノードに正しく拡張されました。

「Finish」 をクリックします。

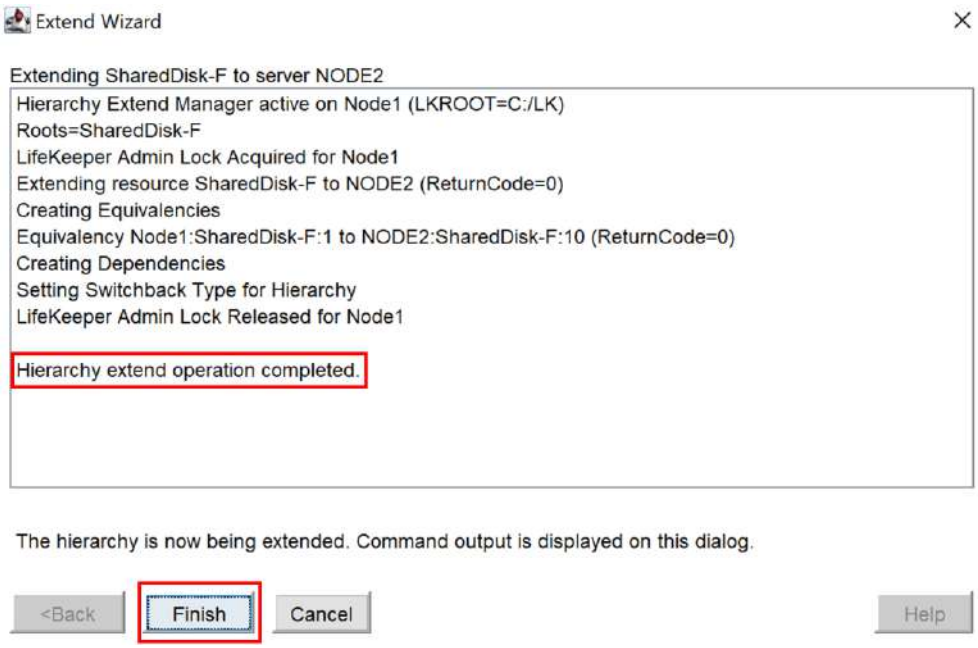


図 8.5.3-10 ミラーボリュームの拡張

これでボリュームリソースが作成されました。

リソース階層は自動的に作成され、調整されます。

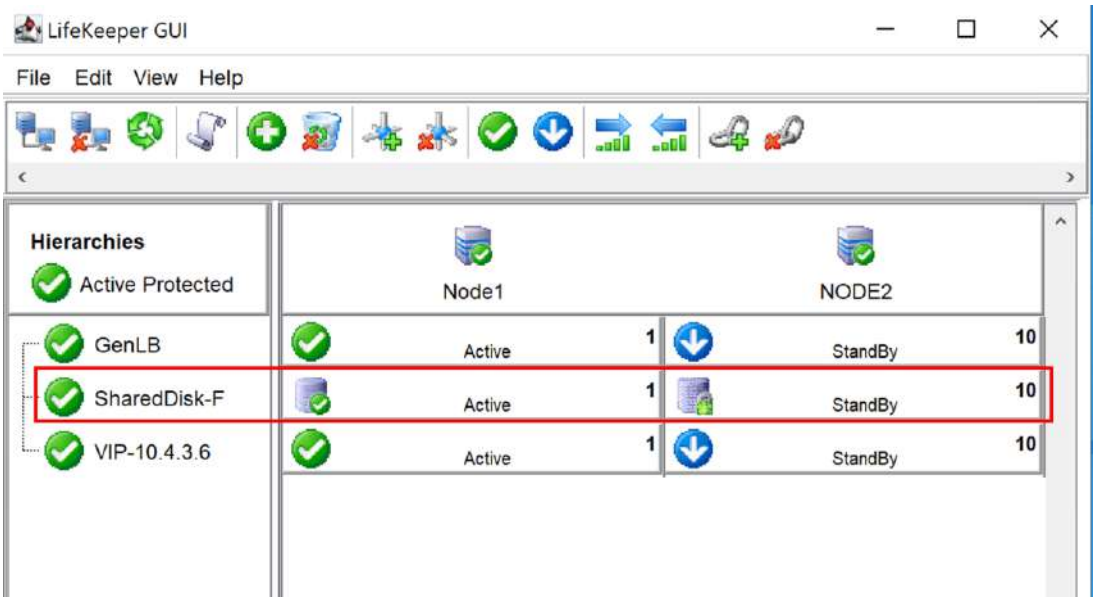


図 8.5.3-11 ミラーボリュームの作成完了

8.6. SQL Server 2019 のダウンロードとインストール

本節では、共有ディスクに SQL Server 2019 をダウンロードおよびインストールする手順について説明します。

8.6.1. 共有ディスク リソースのスイッチオーバー

まず、待機系ノードにインストールを行います。そのため、全リソースを待機系にスイッチオーバーして共有ディスクにアクセスできる状態にします。

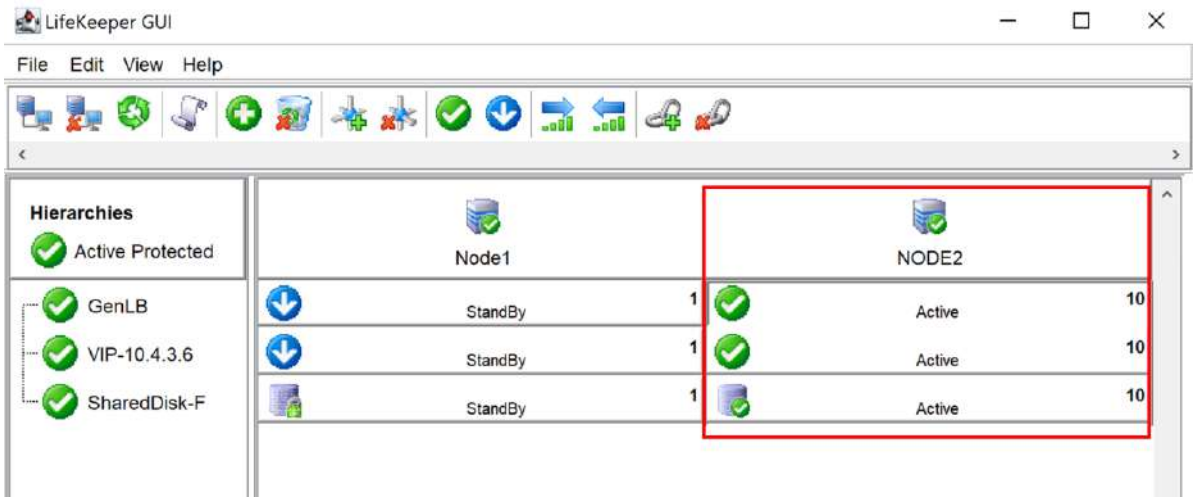


図 8.6.1 すべてのリソースを待機系にスイッチオーバー

8.6.2. SQL Server 2019 のインストール

待機系ノードに SQL Server 2019 をインストールする手順を説明します。

（1） SQL Server のインストールメディアの展開

待機系ノードでローカルに保存した SQL Server 2019 のインストールメディア（SQLEXPRADV_x_ENU.exe）を開いて、解凍します。

「Browse...」をクリックして、解凍に使用するディレクトリを選択します。

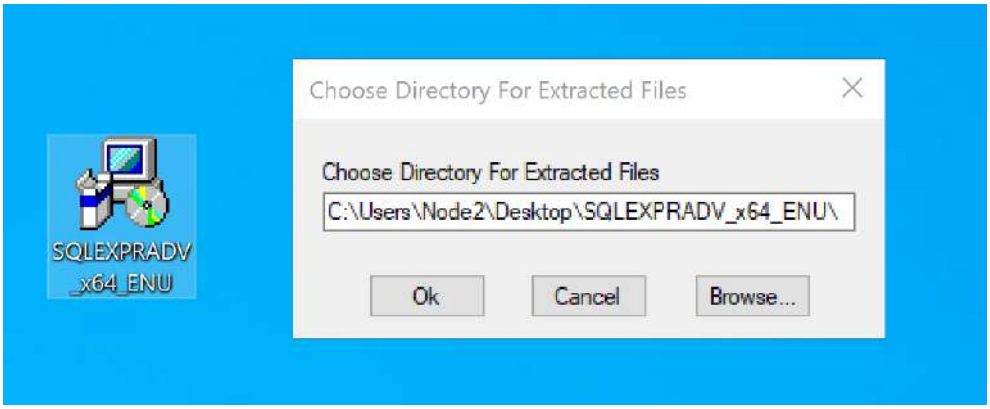


図 8.6.2-1 インストールメディアの展開

（2） SQL Server 2019 のインストール

展開後、「SQL Server Installation Center」が表示されます。「New SQL Server stand-alone installation or add features to an existing installation」をクリックします。

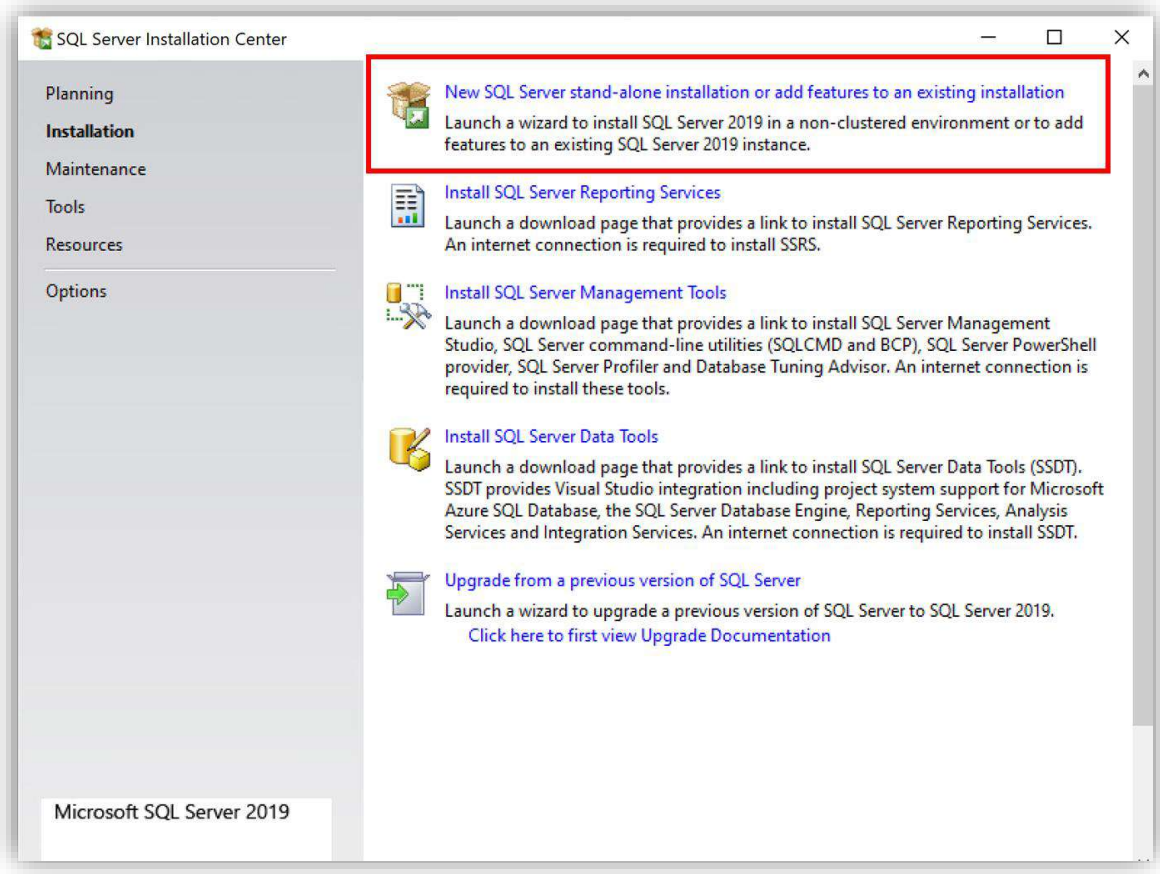


図 8.6.2-2 SQL Server 2019 のインストール

（3） ライセンス条項に同意

ライセンス条項が表示されます。

「I accept the license terms and Privacy Statement」にチェックを入れ、「Next >」をクリックして進みます。

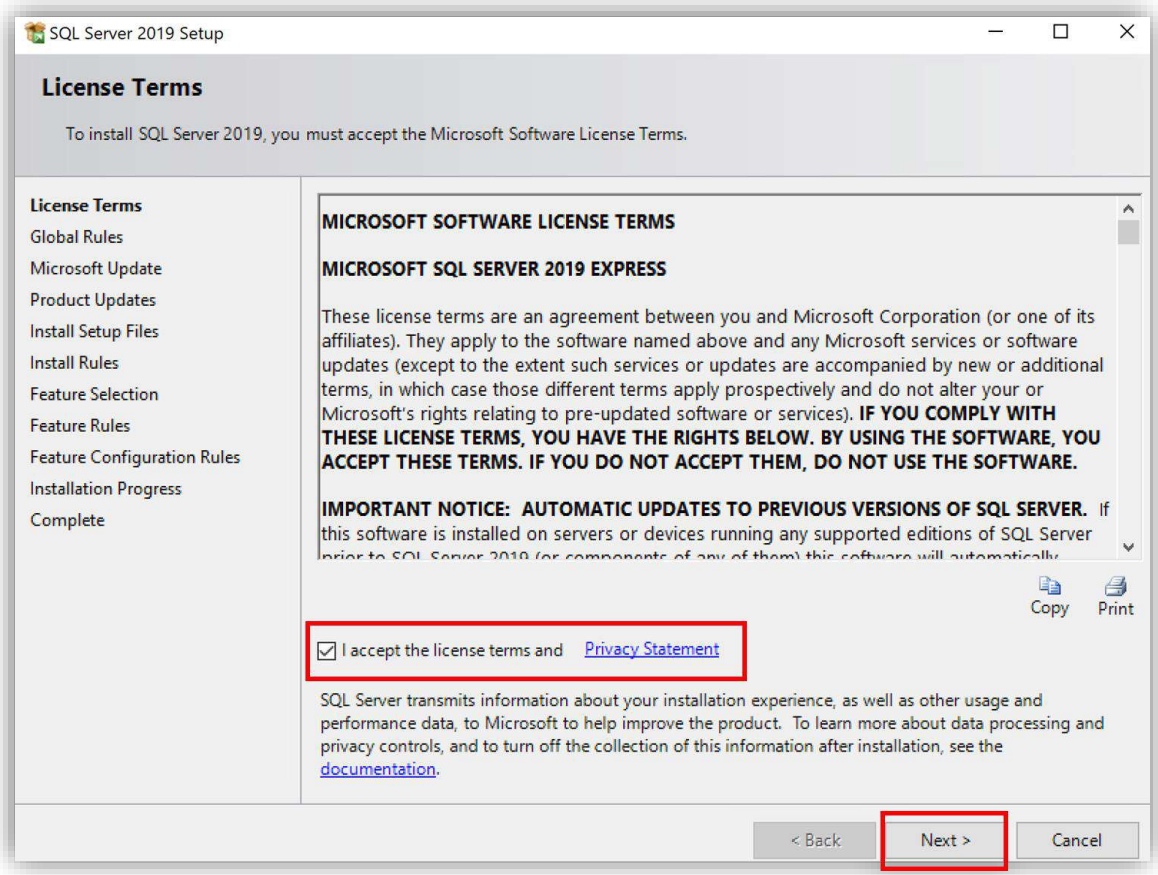


図 8.6.2-3 ライセンス条項に同意

（4） 自動アップデート機能の選択

SQL Server 2019 の自動アップデート機能の使用を選択します。

本ガイドではチェックを外して、「Next >」をクリックします。

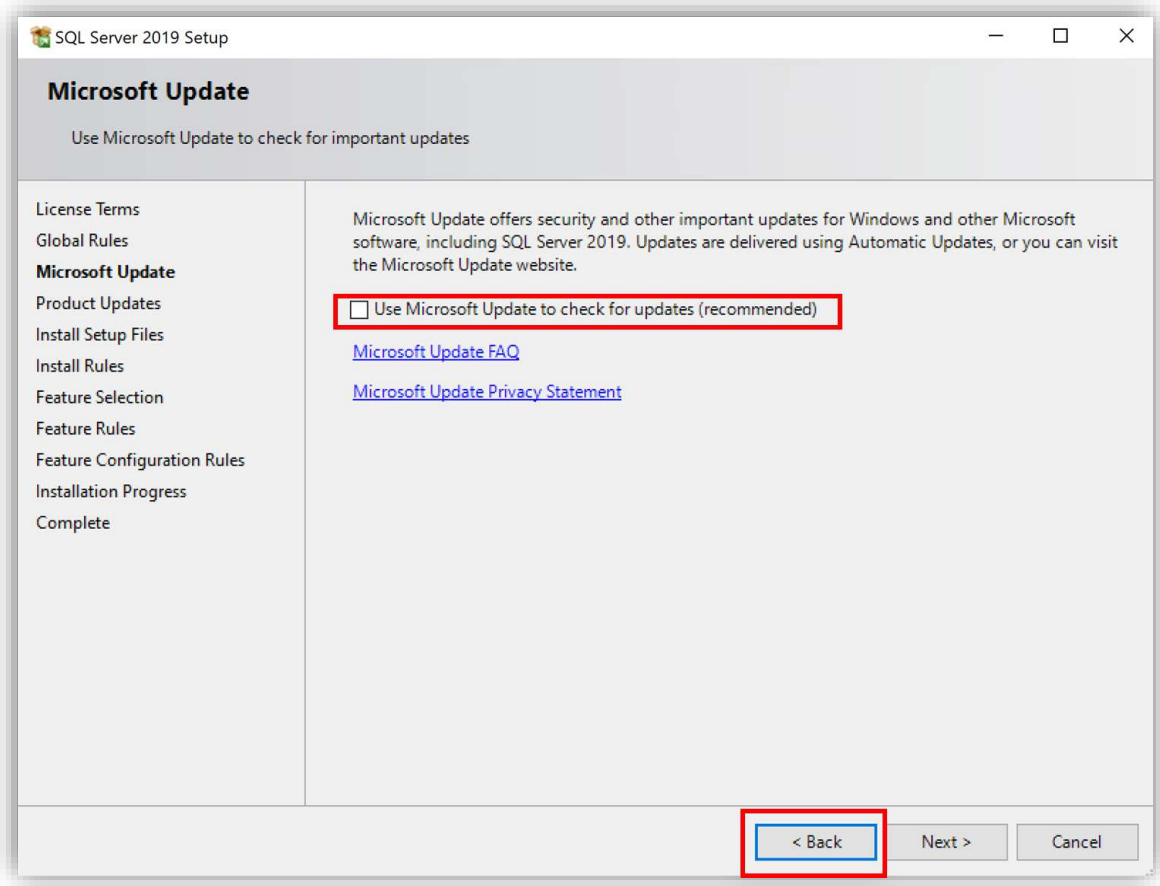


図 8.6.2-4 自動アップデート機能の選択

（5） インストール前のルールチェック

インストール前のルールチェックを行います。

「Next >」 をクリックして次のステップに進みます。

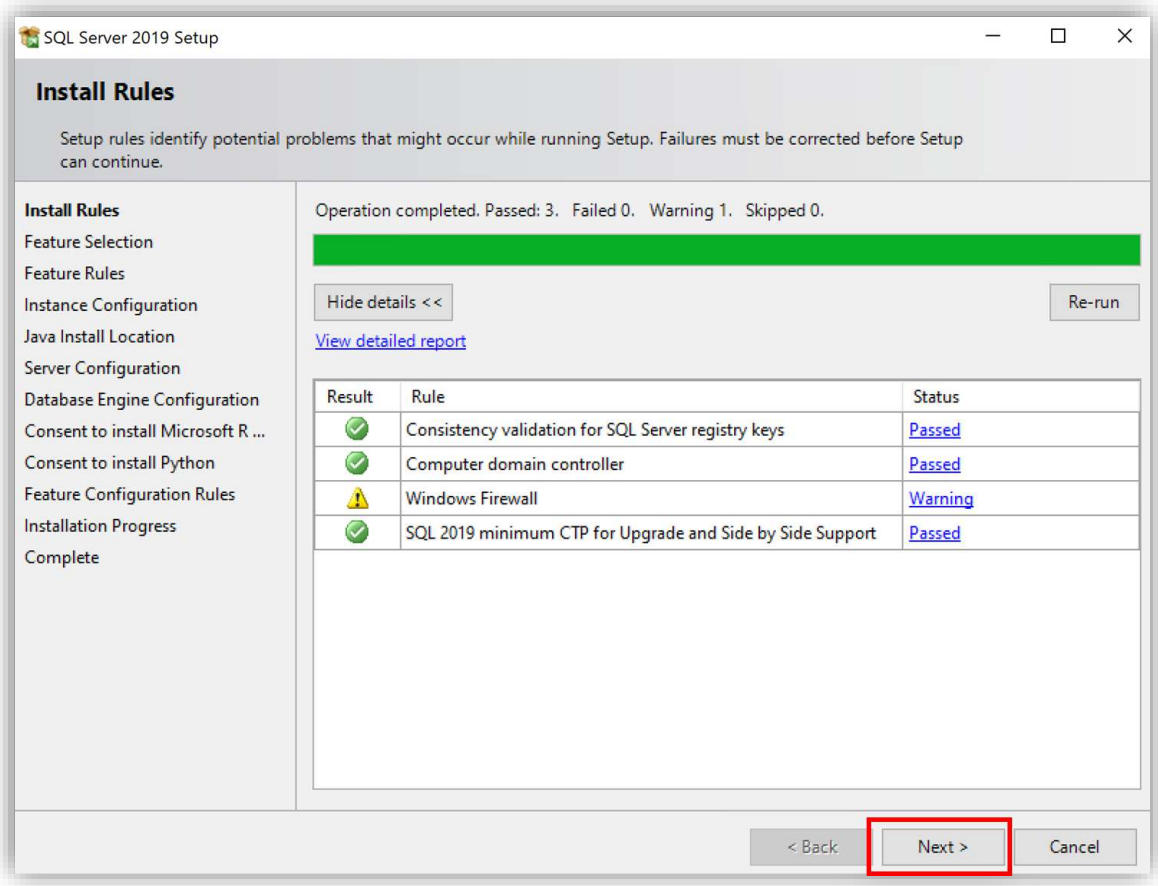


図 8.6.2-5 インストール前のルールチェック

（6） インストール機能の選択。

必要な機能にチェックを入れます。このガイドでは、「Database Engine Services」のみを選択します。

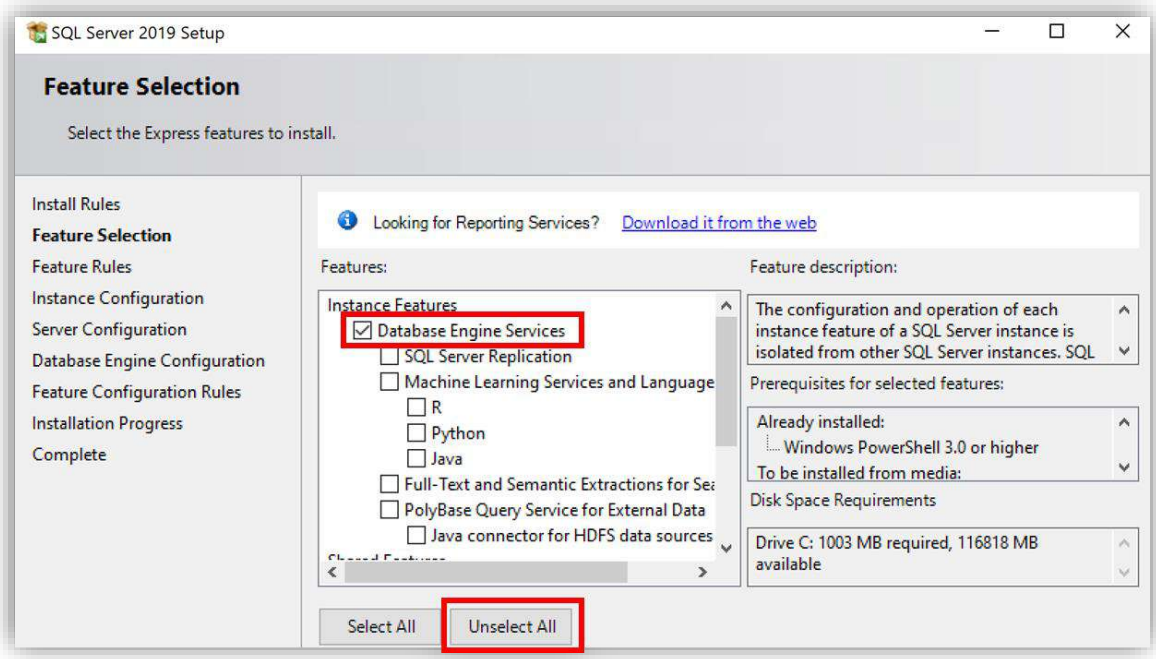


図 8.6.2-6 インストール機能の選択

（7） SQL Server インスタンスのインストールの選択

「...」をクリックして、インストール先のディレクトリを選択します。

インストールディレクトリを選択したら、「次へ >」をクリックして、次のステップに進みます。

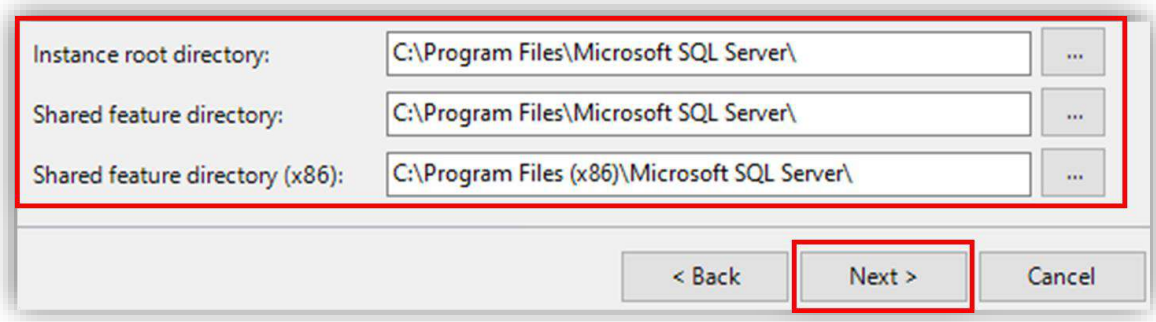


図 8.6.2-7 SQL Server インスタンスのインストール先の選択

（8） SQL インスタンス ID の入力

SQL インスタンス ID を入力します。

入力ができたら、「Next >」 をクリックして次のステップに進みます。

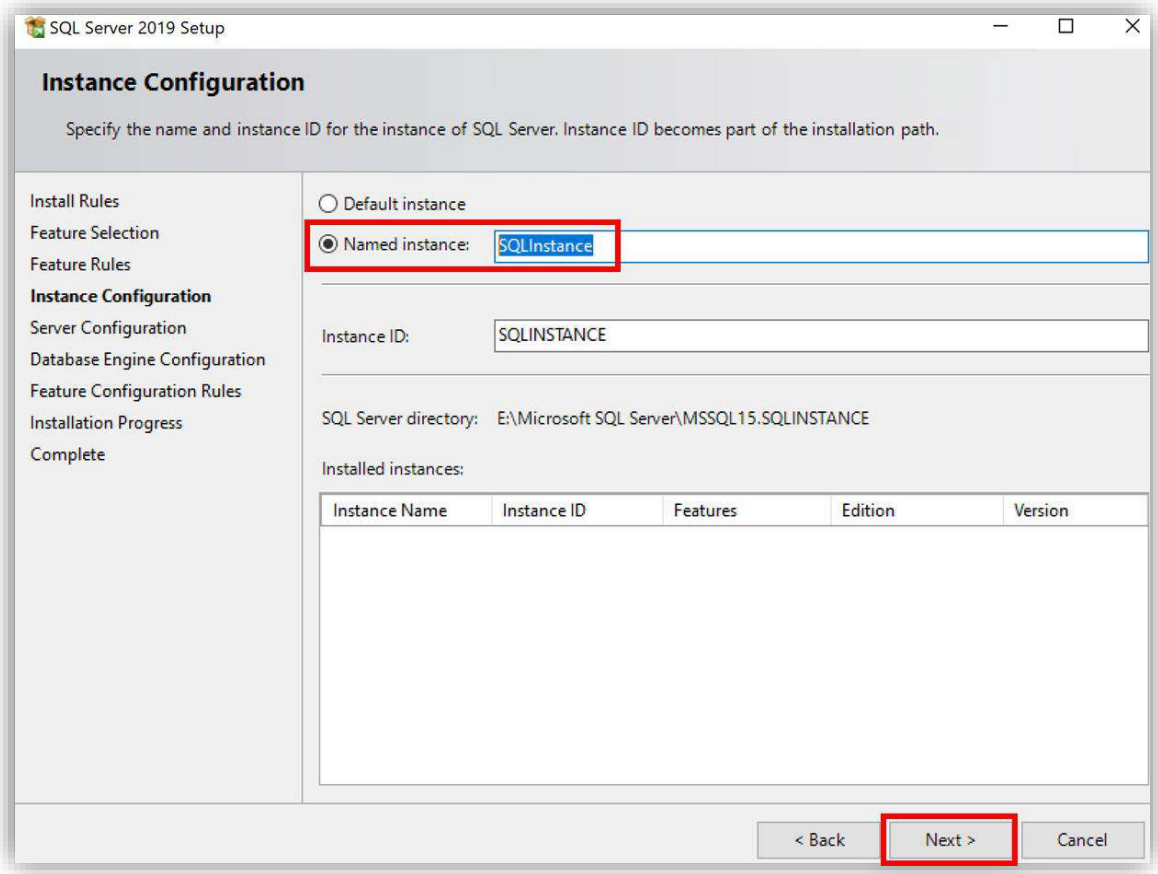


図 8.6.2-8 SQL インスタンス ID の入力

（9） サーバコンフィグレーションの設定

ここではデフォルトの設定のままにします。SQL データベースエンジンはサーバが起動したときに自動的に起動されるようにします。

「次へ >」 をクリックして次のステップに進みます。

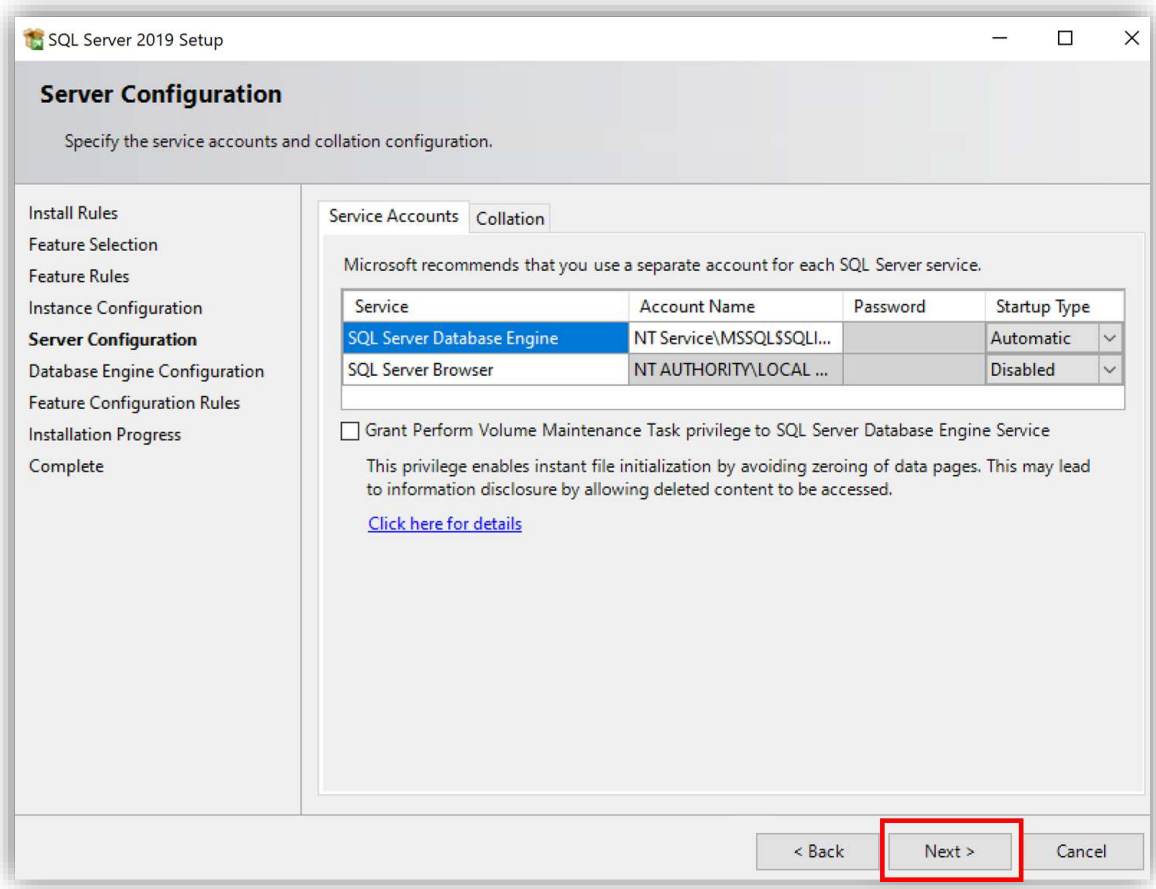


図 8.6.2-9 サーバコンフィグレーションの設定

（10） データベースエンジンの構成の設定

Windows 認証と SQL Server 認証の両方を使用するため、混合モード（Mixed mode）にチェックを入れます。

SQL Server 認証では、sa（System Administrator）アカウントを使用します。

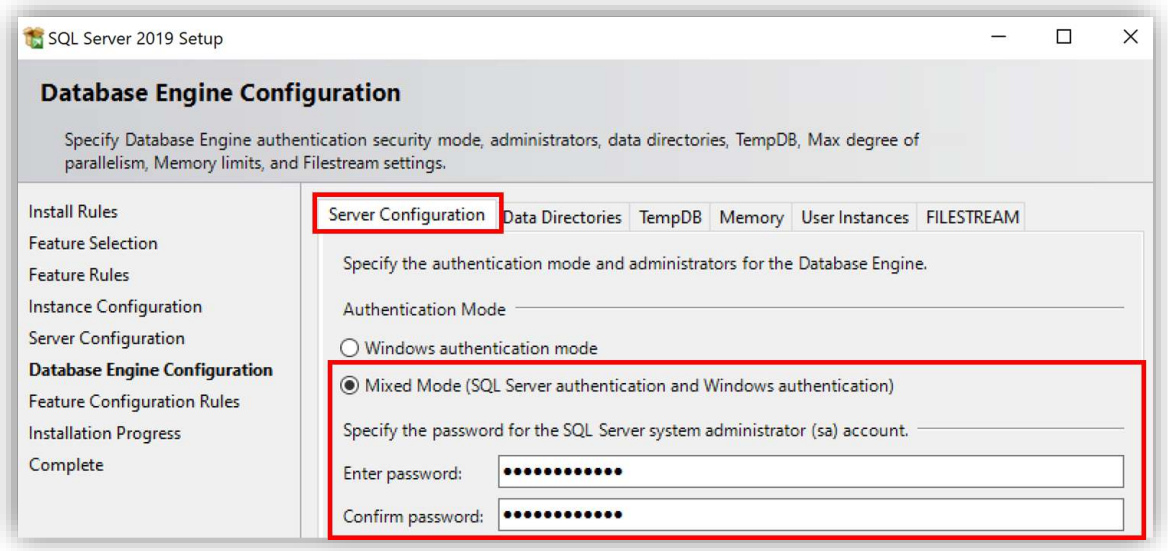


図 8.6.2-10 データベースエンジンの構成の設定

（11） SQL Server の管理者アカウントの設定

管理者アカウントを設定します。

「Specify SQL Server Administrators」で、ドメイン管理者アカウントを設定します。

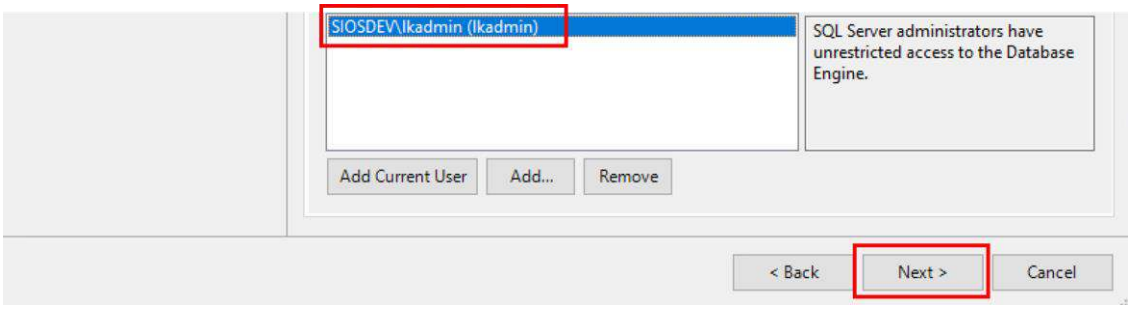


図 8.6.2-11 SQL Server の管理者アカウントの設定

（11） SQL Server のインストールディレクトリの設定

入力が完了したら、「Data Directories」 タブを開きます。

ここで SQL Server のインストールディレクトリを確認できます。データディスクに設定します。

DataKeeper のデータレプリケーションを使用するためには、待機系ノードにもインストール時に完全に同じディレクトリにインストールする必要がありますので、

インストールディレクトリのメモを取っておいてください。

（12） インストールが開始されます

「Data Directories」タブを開いて、SQL Server のインストールディレクトリが共有ディスクになっていることを確認します。

確認できたら、「次へ >」 をクリックします。

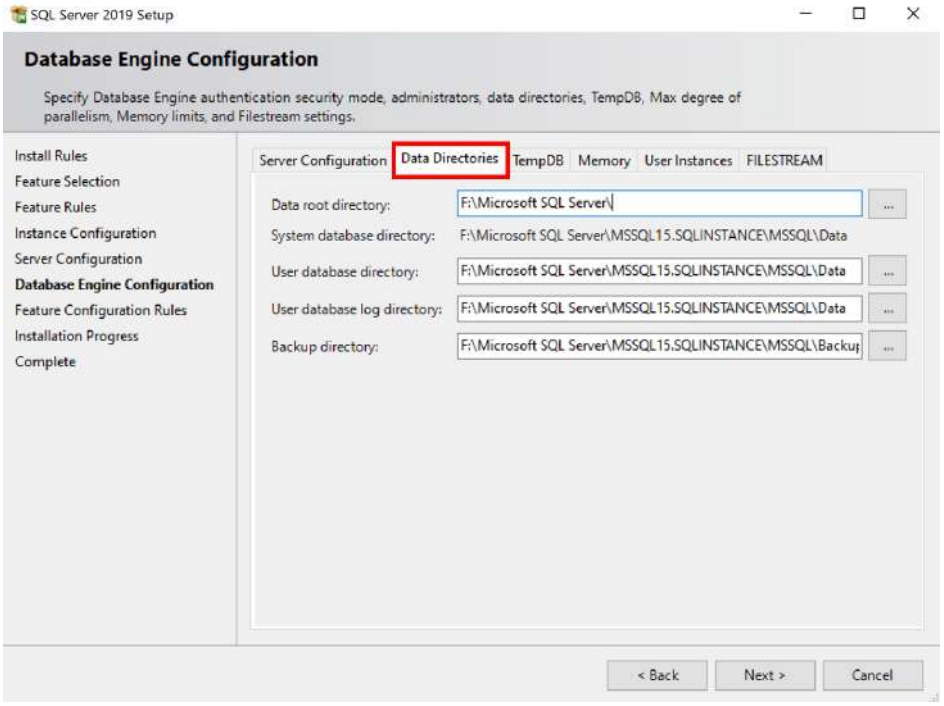


図 8.6.2-12 SQL Server のインストールディレクトリの設定

（13） インストール完了

待機ノードでのインストールが完了しました。各項目が「Succeeded」と表示されていることを確認すれば、全ての機能が正しくインストールされています。

「Close」 をクリックして、インストール画面を閉じます。

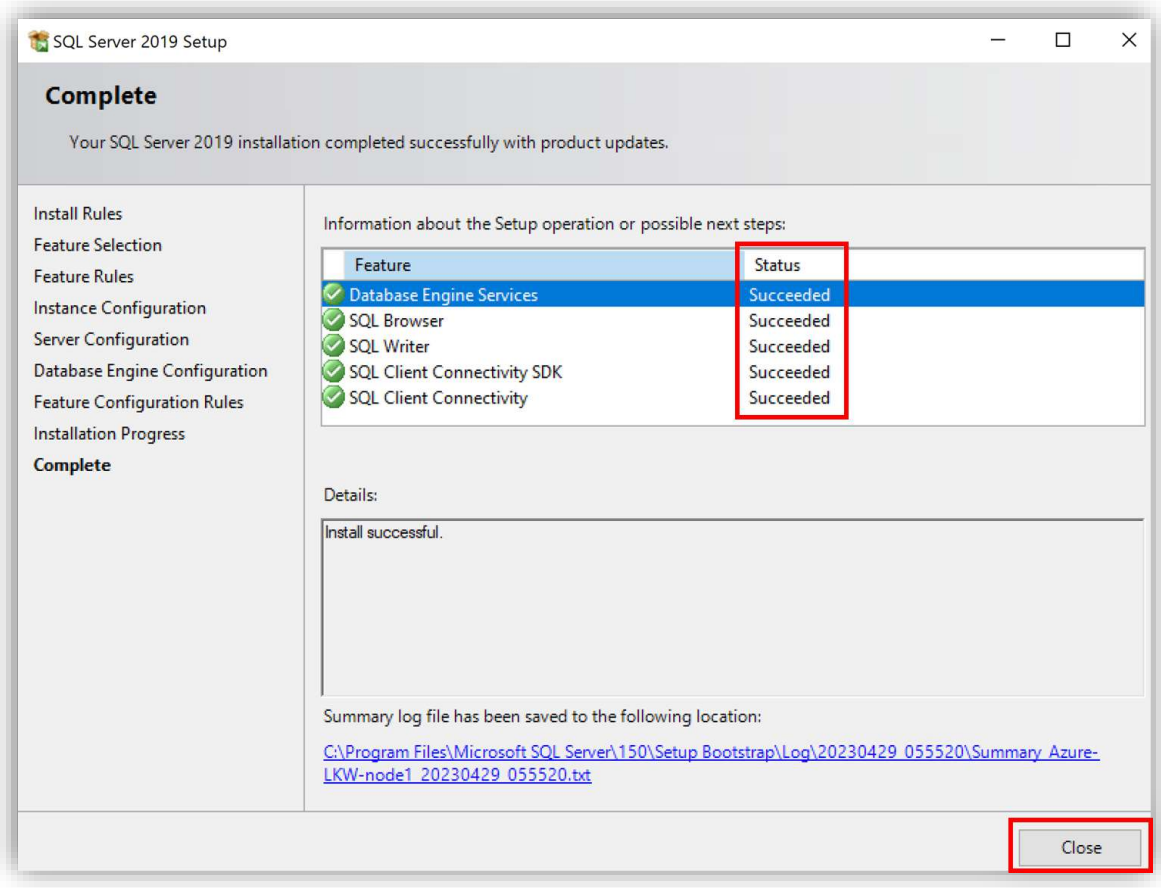


図 8.6.2-13 インストール完了

次に、稼働系に SQL Server をインストールします。

以下のような手順で行います。

- LifeKeeper の GUI ですべてのリソースを待機系にスイッチオーバーします。
- 共有ディスクの SQL データをすべて削除します。
- 同じ内容で SQL Server を待機系にインストールします。

8.6.3. SQL Server Management Studio のインストール

続いて、SQL Server Management Studio（SSMS）をインストールします。

（1） SSMS のインストールメディアの実行

SSMS-Setup-ENU.exe ファイルをダブルクリックして起動します。

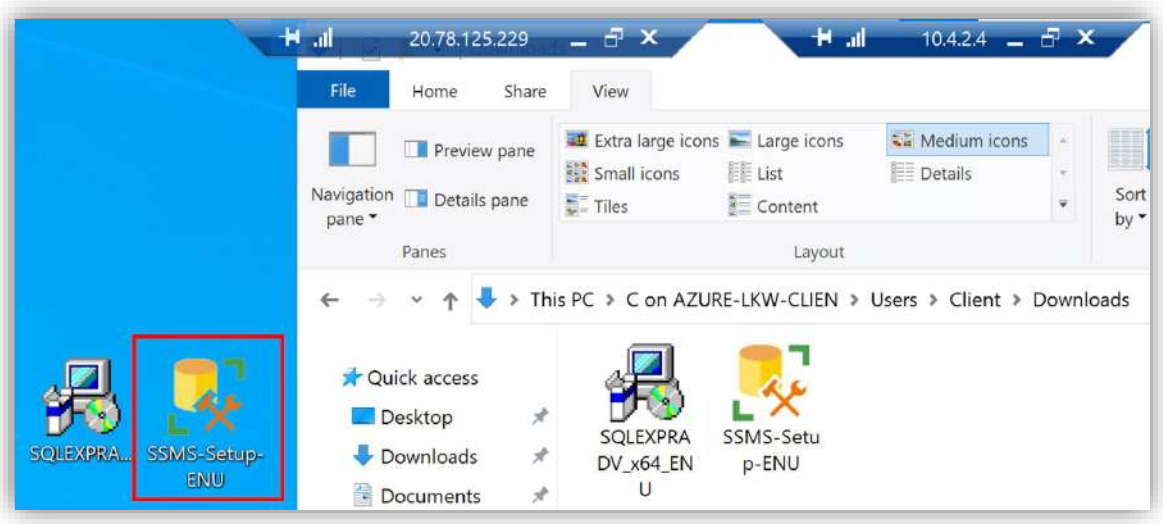


図 8.6.3-1 SSMS のインストールメディアの行

（2） SSMS のインストールディレクトリの指定

デフォルトのインストール先を変更したい場合は、「Change」をクリックしてください。

設定が完了したら、「Install」をクリックし、インストールを開始します。

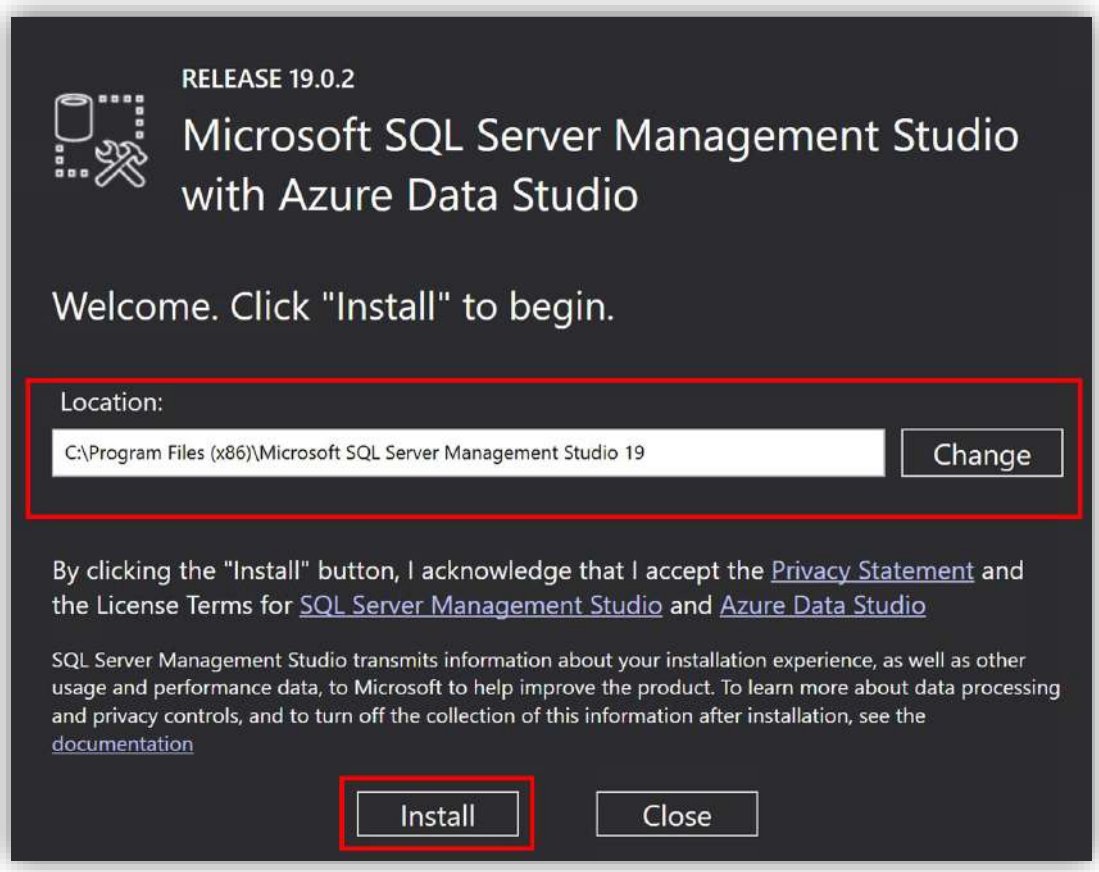


図 8.6.3-2 SSMS のインストールディレクトリの指定

（3） インストール完了

インストールが完了したら、システムを再起動してください。

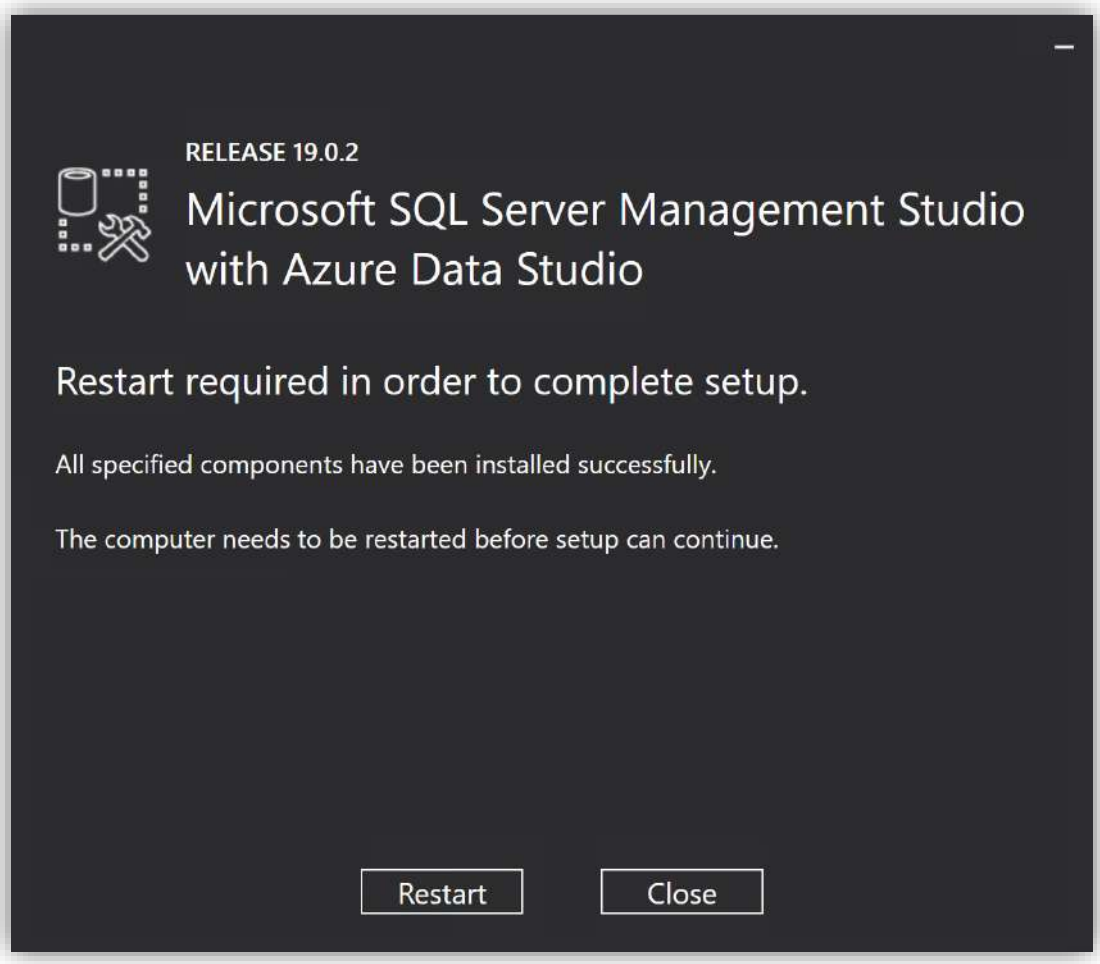


図 8.6.3-3 インストール完了

これにより、SSMS のインストールは完了しました。

同じ手順で SQL Server Management Studio を稼働系ノードにインストールします。

8.6.4. SSMS の TCP/IP 通信の有効化

この節では、SQL Server にアクセスするための TCP/IP 通信設定について説明します。

（1） SQL Server 2019 Configuration Manager の起動

Windows の検索バーから 「SQL Server 2019 Configuration Manager」 を検索し、起動します。

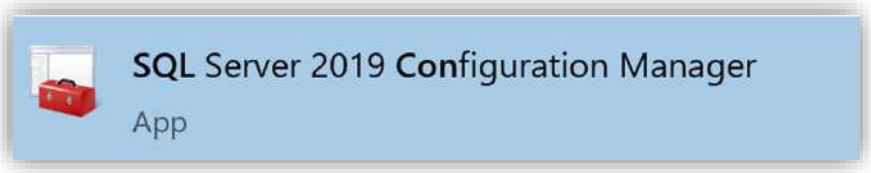


図 8.6.4-1 SQL Server 2019 Configuration Manager の起動

（2） TCP/IP 通信の有効化

「SQL Server Network Configuration」を展開し、「Protocols for <SQL Server インスタンス名>」を選択。

TCP/IP を右クリックし、「Enable」を選択して有効化します。

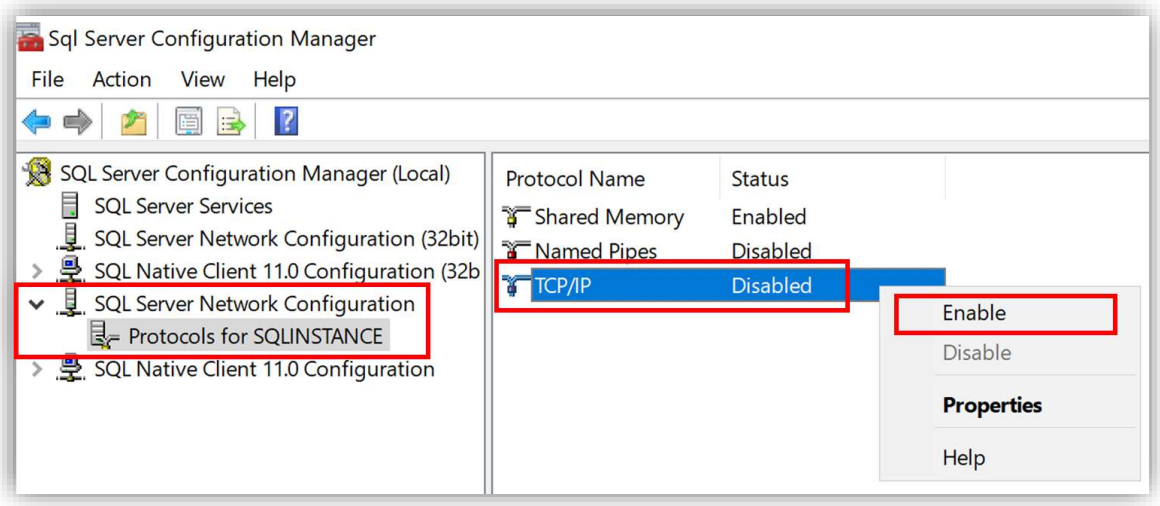


図 8.6.4-2 TCP/IP 通信の有効化

（3） SQL Server の TCP/IP 通信の詳細設定

「TCP/IP」を右クリックし、「Properties」 を起動します。

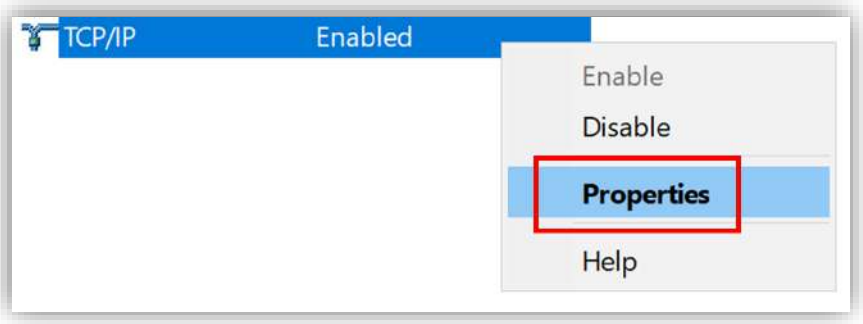


図 8.6.4-3 SQL Server の TCP/IP 通信の詳細設定

（4） TCP ポートの設定

「IP Addresses」タブから、「IPALL」の「TCP Port」に 1433 を指定します。設定が完了したら、「OK」 をクリックします。

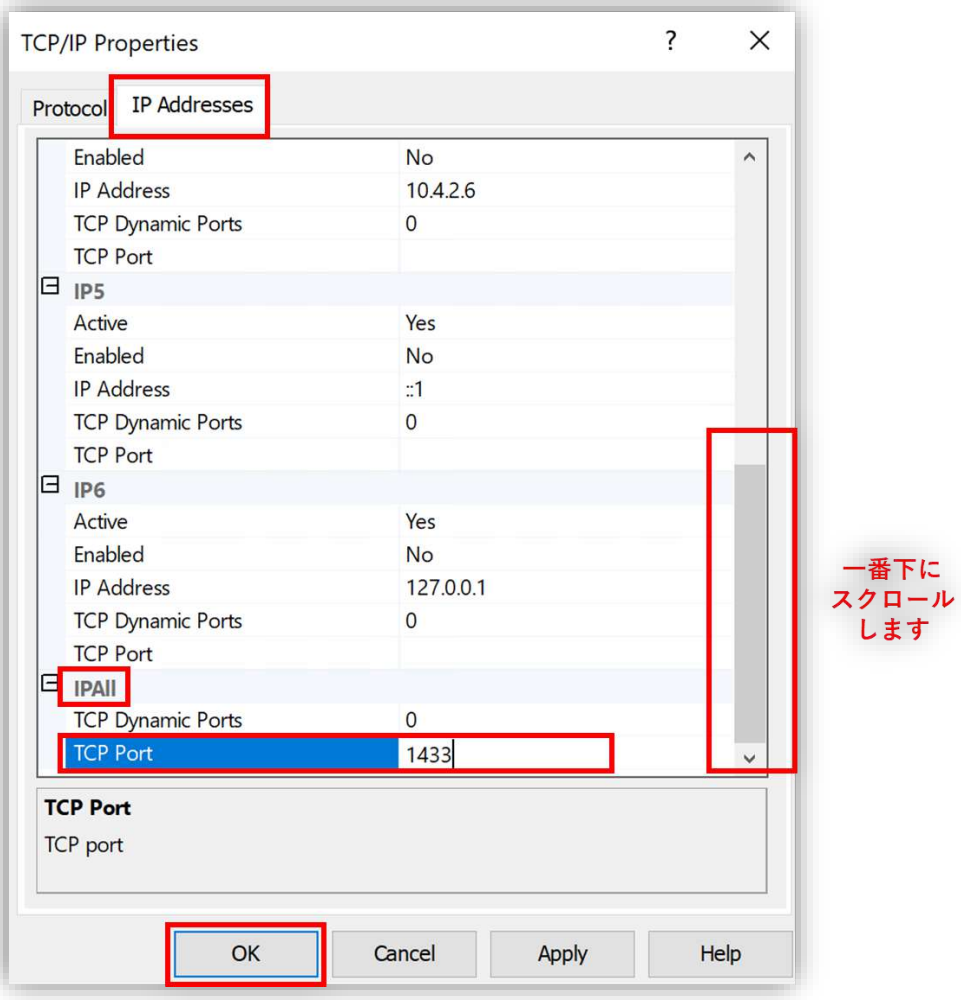


図 8.6.4-4 SQL Server インスタンスが使用する TCP ポートの設定

（5） SQL Server の再起動

設定を反映させるには、SQL Server インスタンスを再起動する必要があります。「SQL Server Network Configuration」 の 「SQL Server Services」（SQL Server のサービス）で SQL Server インスタンスの起動状態を管理できます。

「SQL Server Services」 を選択し、「SQL Server <SQL Server インスタンス名>」を右クリックして、「Restart」 をクリックして SQL Server サービスを再起動します。

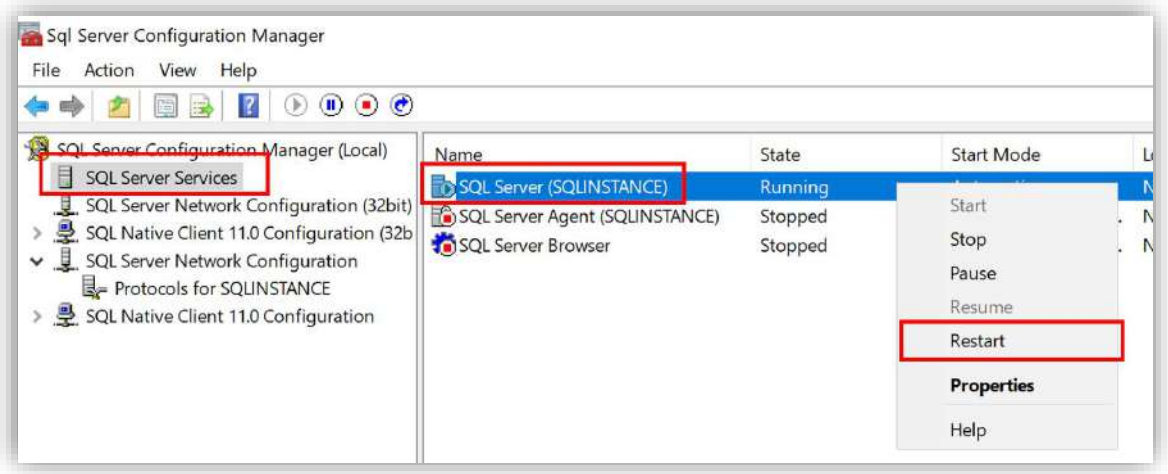


図 8.6.4-5 SQL Server サービスを再起動

SQL Server サービスが再起動されます。

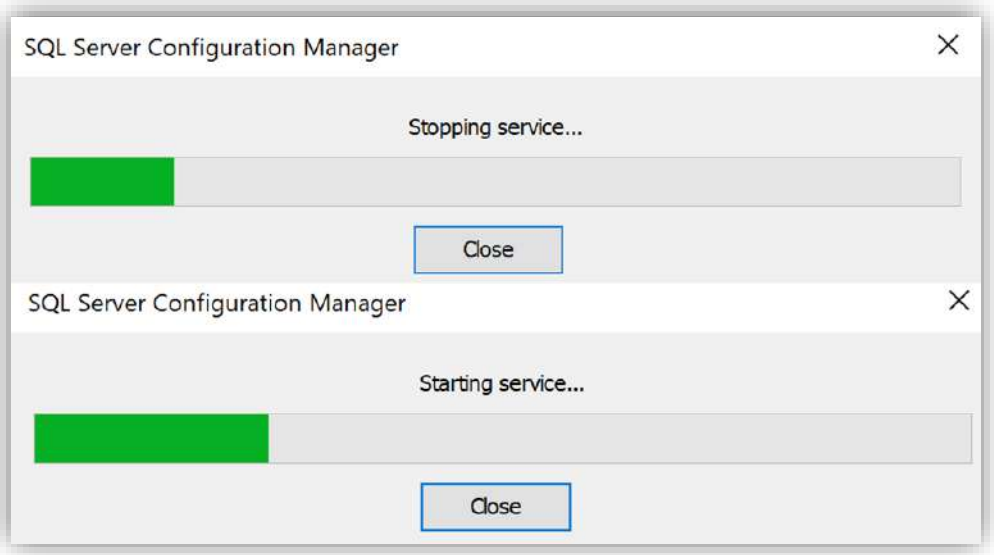


図 8.6.4-6 SQL Server サービス再起動中

SQL Server サービスの再起動が完了したら、TCP/IP および TCP ポート 1433 での通信を有効にしました。
これにより、TCP ポート 1433 使用して SQL Server インスタンスにアクセスできるようになります。

（6） TCP 1433 番ポートの開放
ファイアウォールで SQL Server が使用している 1433 番ポートを開放します。

8.6.5. SQL Server への接続確認テスト

本節では、SSMS を用いて SQL Server インスタンスへの接続確認テストを行う手順を説明します。

（1） SSMS の起動
スタートメニューから「SQL Server Management Studio 19」を選択して起動します。

図 8.6.5-1 SSMS の起動

（2） 認証情報の入力

起動後、認証情報の入力画面が現れます。

ここでは、IP アドレスとポートを指定して接続します。具体的には「Server Name」フィールドに「IP アドレス,ポート番号」の形式で入力します。

認証方式「Authentication」は「SQL Server Authentication」に指定し、sa アカウントとパスワードを入力します。

入力できたら、「Connect」をクリックして、接続を行います。

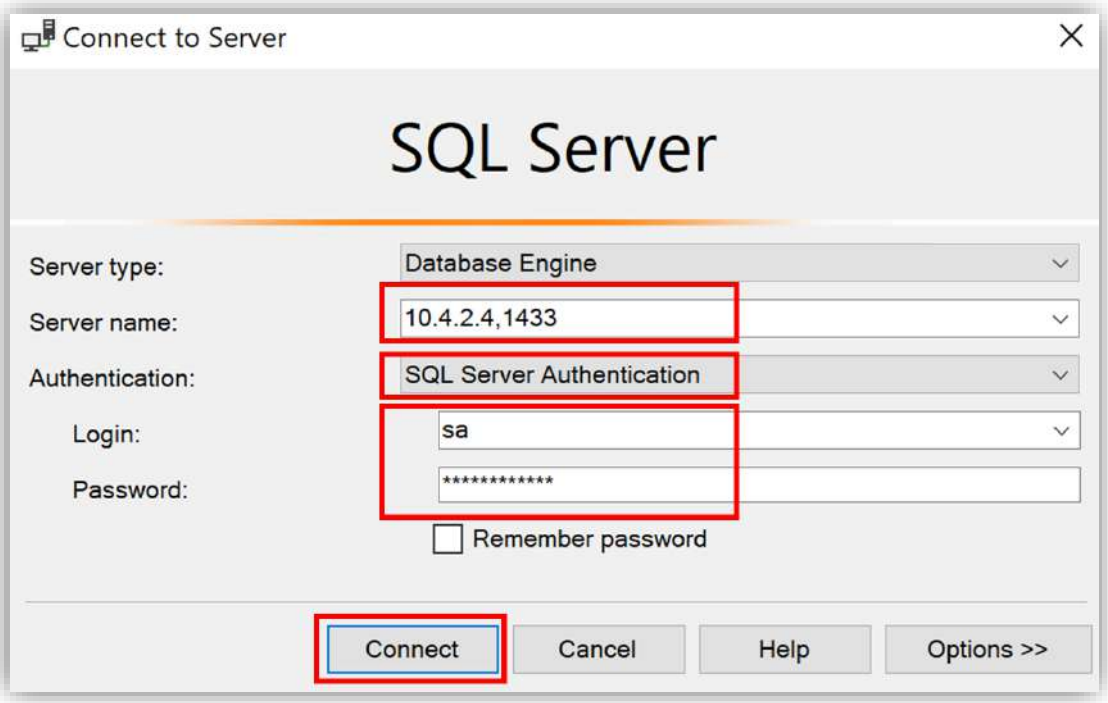


図 8.6.5-2 認証情報の入力

接続が成功すると、画面の左上にある「Object Explorer」に SQL Server インスタンスが表示されます。

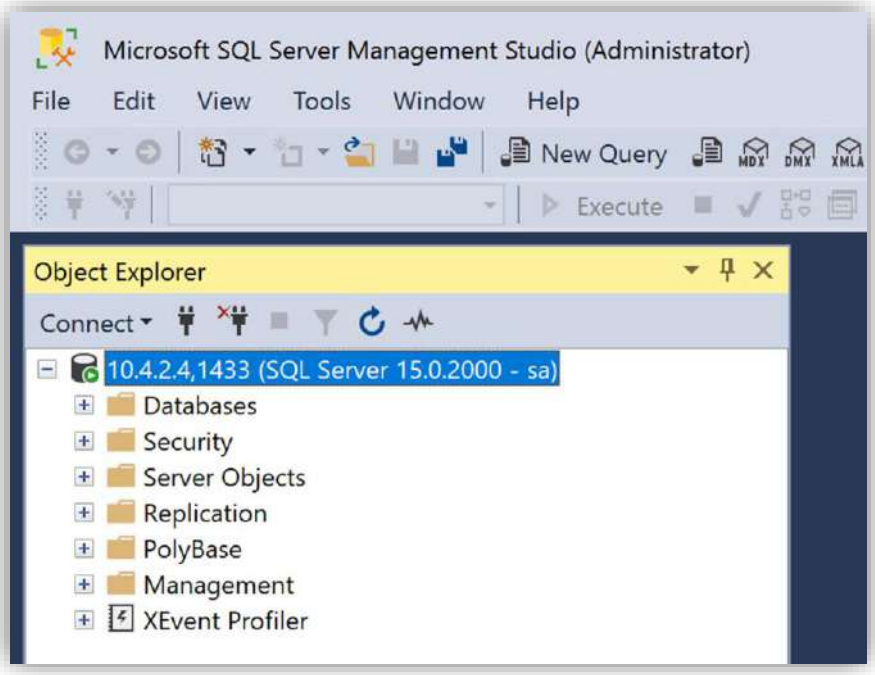


図 8.6.5-3 SQL Server インスタンスに接続成功

8.7. Microsoft SQL Server リソースを作成

本節は Microsoft SQL Server リソースを作成して、SQL Server のデータベースを保護します。

（1） リソースを作成する前の確認事項

リソースを作成する前に、稼働系ノードと待機系ノードに以下の項目をチェックしてください

- SQL Server インスタンスが起動している
- TCP/IP が有効である
- 使用するポート（通常は 1433）が開放されている
- LifeKeeper for Windows Microsoft SQL Server Recovery Kit がインストールされている

（2） リソースの作成

LifeKeeper GUI のメニューから「Create Resource Hierarchy」アイコンをクリッ

クして、リソース階層の作成画面を開きます。

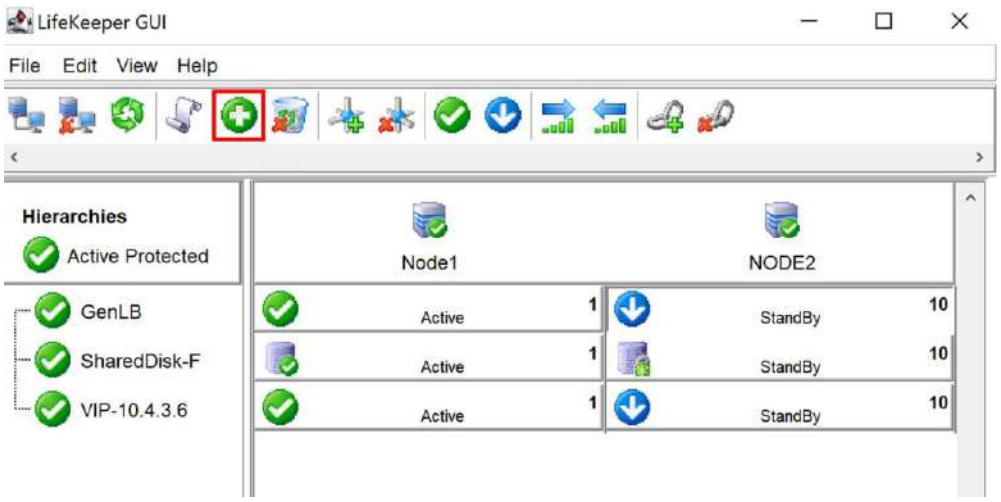


図 8.7-1 リソースの作成

（3） 稼働系ノードと待機系ノードの選択

「Primary Server」は稼働系ノードとして、「Backup Server」は待機系ノードとして選択します。「Next >」をクリックします。

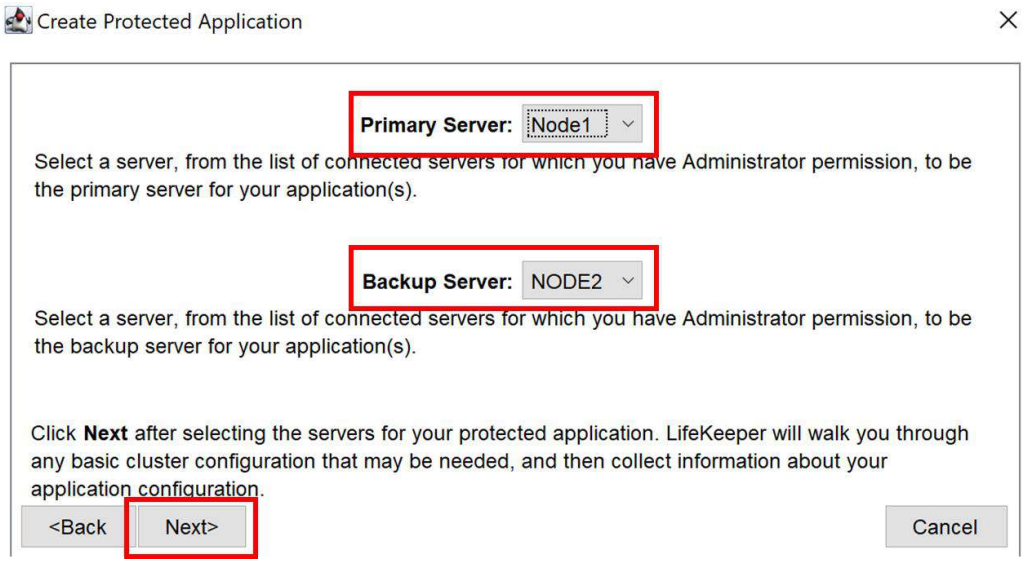


図 8.7-2 稼働系ノードと待機系ノードの選択

（4） 保護するアプリケーションの選択

Microsoft SQL Server リソースを作成して SQL Server インスタンスを保護します。

「Application to protect」リストボックスから「MS SQL Server」を選び、「Next >」をクリックします。

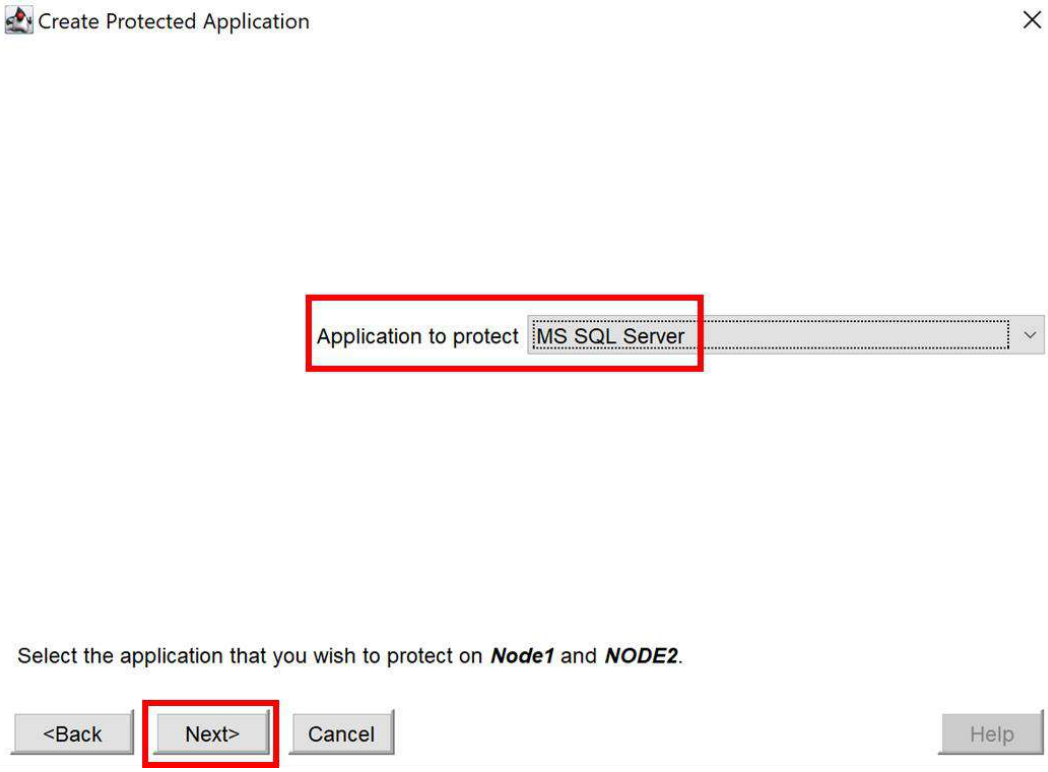


図 8.7-3 保護するアプリケーションの選択

（5） 保護する SQL Server インスタンスの選択

SQL Server のインスタンスの選択画面が開き、保護する SQL Server のインスタンスを選択します。

「Select Microsoft SQL Server Instance」に 「SQLINSTANCE（SQL Server のインスタンス名）」 を選択します。

選択できたら、 「Next >」 をクリックします。

（※）SQL Server のインスタンス名が表示されていない場合は、SQL Server のインスタンスの起動状態を確認してください。

SQL Server のインスタンスが起動していない場合は、起動してから再度リソースの作成を実行してください。SQL Server のインスタンス名と SQL Server の起動

状態は、「SQL Server Network Configuration」を起動し、「SQL Server Network Configuration」の「SQL Server Services」で SQL Server のサービスを確認できます。

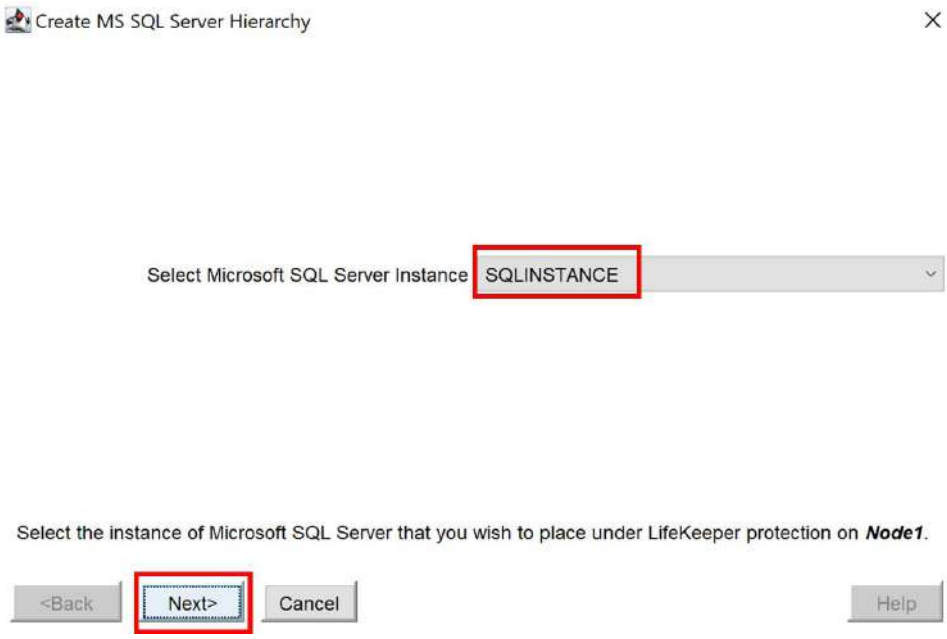


図 8.7-4 保護する SQL Server インスタンスの選択

（6） 管理アカウントのユーザ名の入力

SQL Server インスタンスの管理アカウントのユーザ名を入力します。

「Enter Administrative User Name for SQL <SQL Server のインスタンス名>」の下の入力欄に 「sa」 を入力します。

入力できたら、「Next >」 をクリックします。

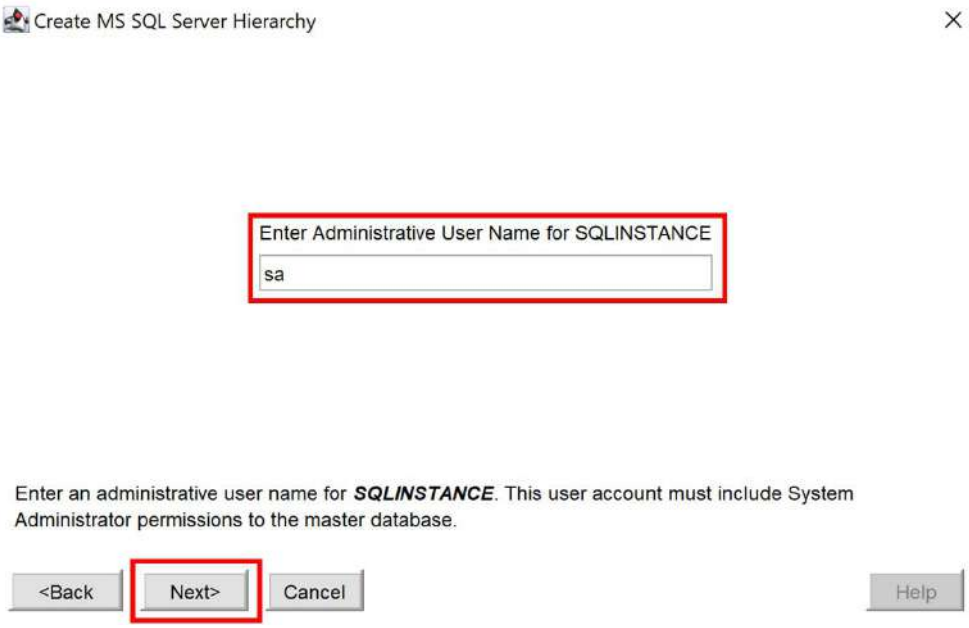


図 8.7-5 管理アカウントのユーザ名の入力

（7） 管理アカウントのパスワードの入力

先ほど指定した SQL Server インスタンスの管理アカウントのパスワードを入力します。

「Enter Password for <指定した管理ユーザ>」の下の入力欄にパスワードを入力します。

入力できたら、「Next >」 をクリックします。

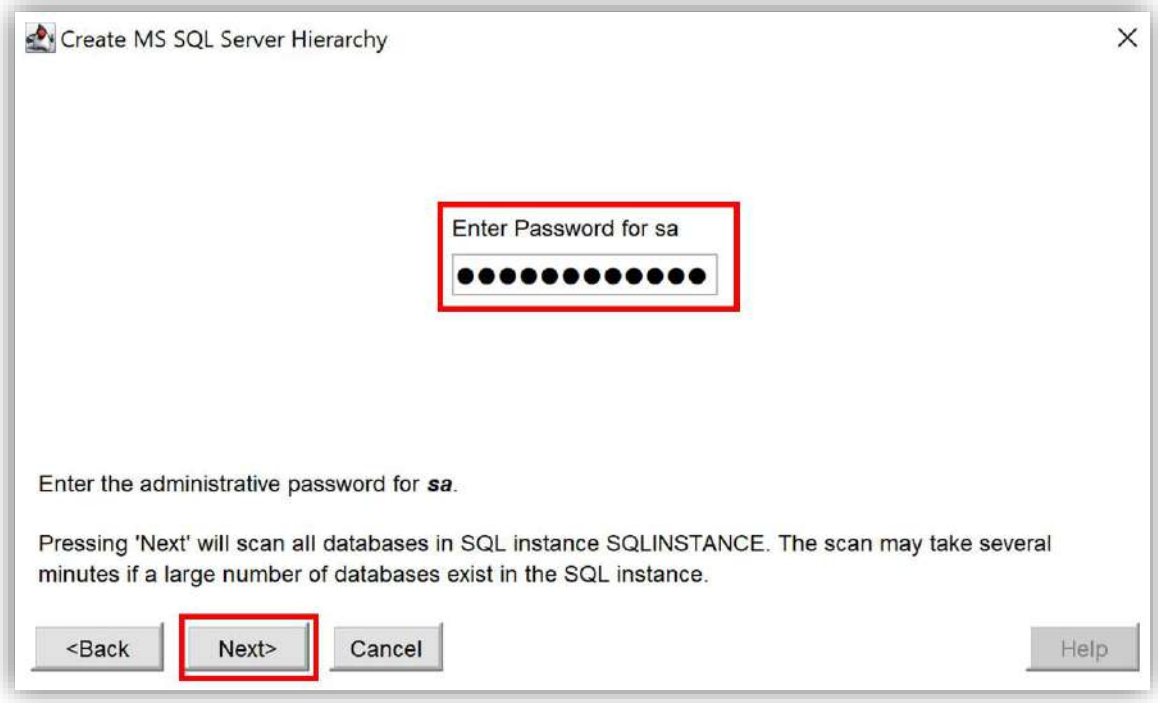


図 8.7-6 管理アカウントのパスワードの入力

（8） ディスク情報の確認

データベースファイルが共有ディスクに格納されていることを確認し、

「Continue」 をクリックします。

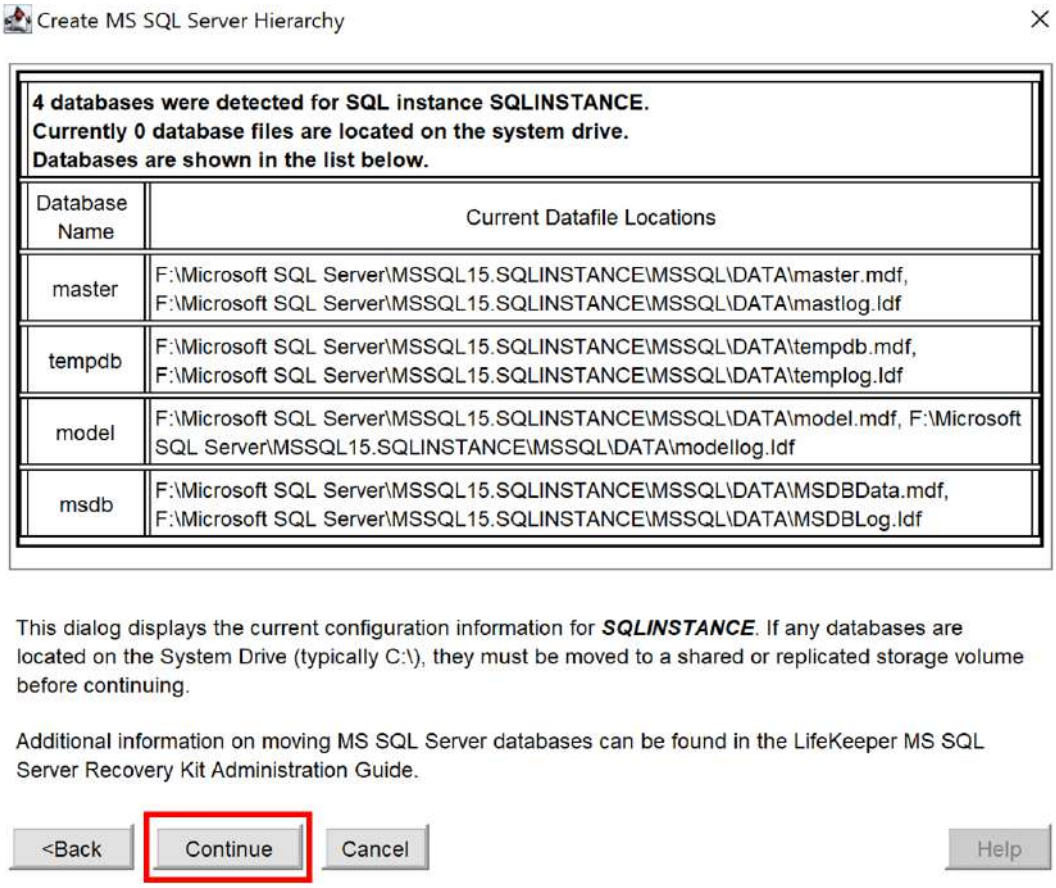


図 8.7-7 レプリケーションを行うディスクの確認

（9） オプショナルサービスの選択

保護するデータベースと一緒に保護したいオプショナルサービスを選択します。このガイドでは「None」を選択しています。

選択したら 「Next >」 をクリックします。

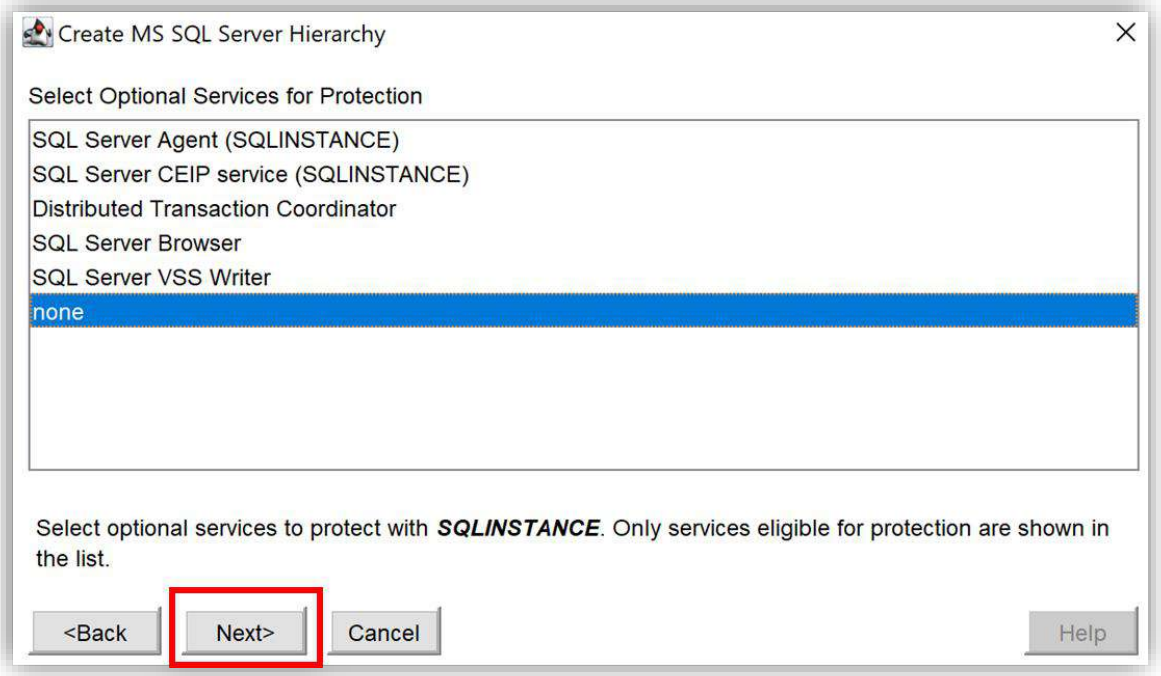


図 8.7-8 オプショナルサービスの選択

（10） データベースにアクセスするための IP リソースの選択

SQL Server データベースに接続するために使用する IP リソース（このガイドでは「VIP-10.4.3.6」）を選択します。

「Next >」をクリックします。

図 8.7-9 データベースにアクセスするための仮想 IP アドレスの入力

（11） パイプのエイリアスの入力

名前付きパイプのエイリアスを選択することができますが、このガイドでは使用しません。「none」を選択し、「Next >」をクリックします。

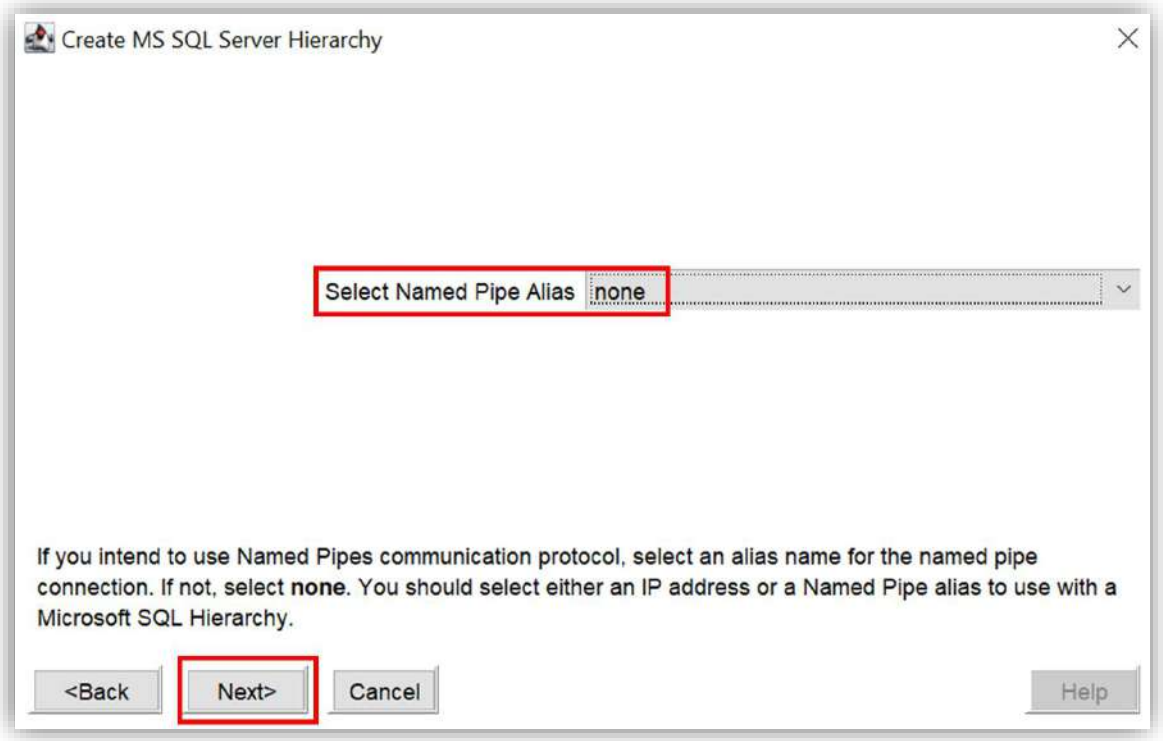


図 8.7-10 パイプのエイリアスの入力

（12） リソースのタグ名の設定

SQL Server リソースのタグ名を設定します。

初期値をそのまま利用します。

「Create」をクリックして SQL Server リソースを作成します。

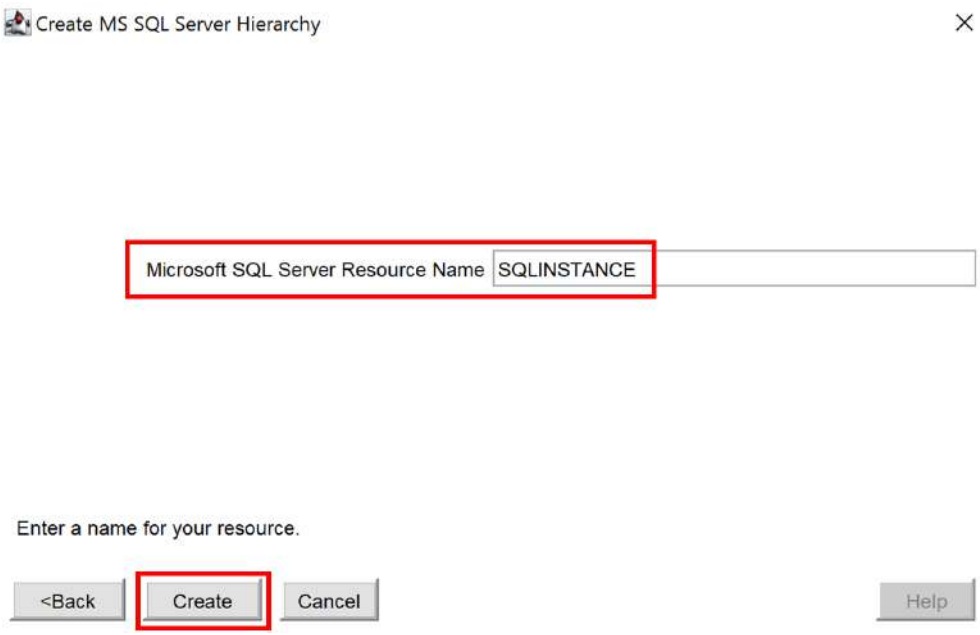


図 8.7-11 リソースのタグ名の設定

（13） 稼働系ノードでリソースの階層作成

稼働系ノードでリソースの階層が作成されることを確認します。

「Next >」をクリックします。

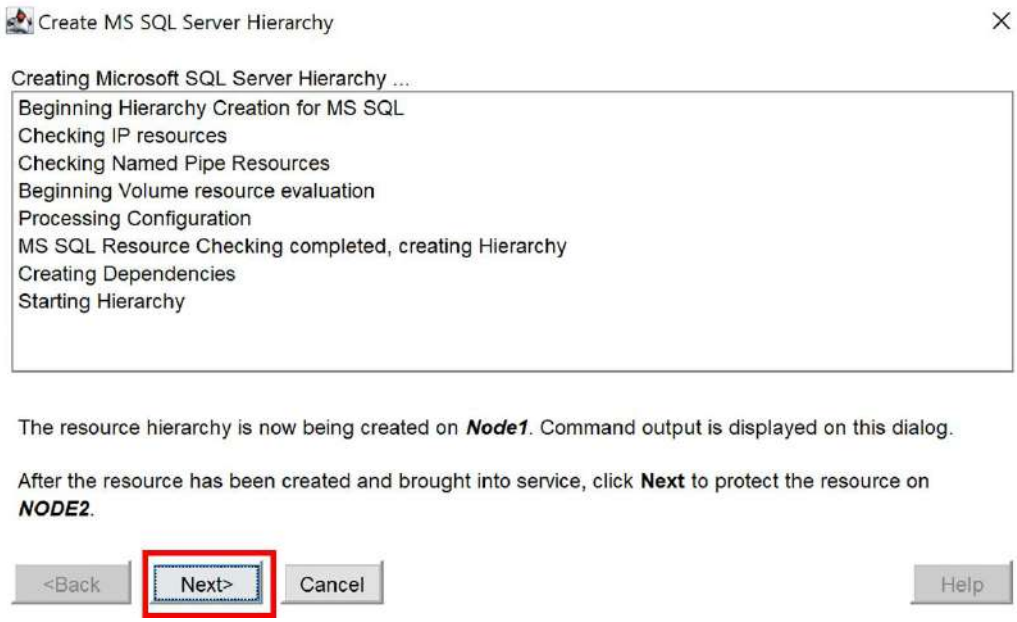


図 8.7-12 稼働系ノードでリソースの階層が作成される

（14） PreExtend のチェック

待機系ノードへリソースが拡張可能かどうかを確認します。

「PreExtend checks were successful」が表示されれば、リソースが待機系ノードへ拡張可能であると確認できます。

「Next >」をクリックします。

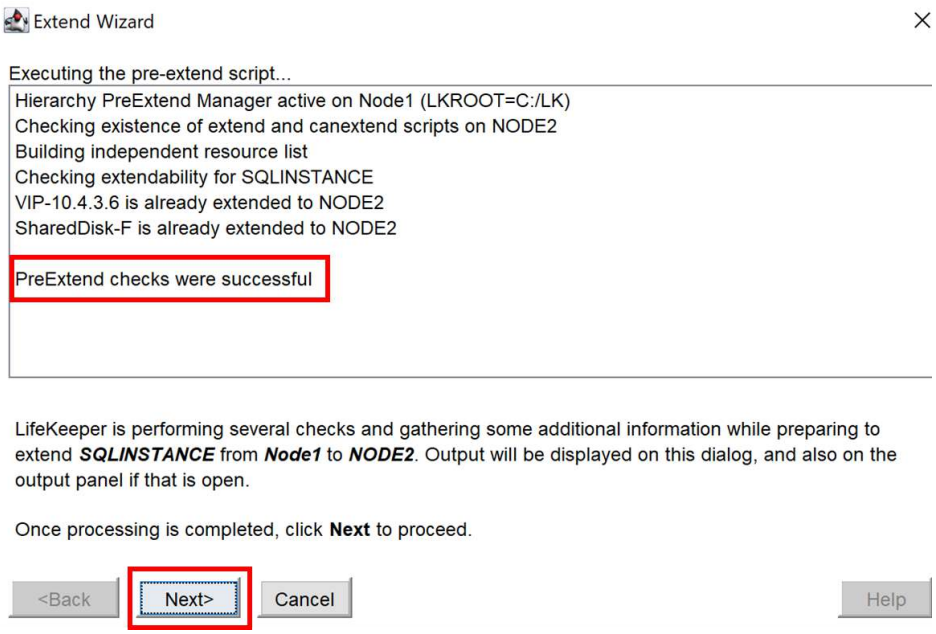


図 8.7-13 PreExtend のチェック

8.8. 仮想 IP を利用して SQL Server に接続確認

前節で設定した仮想 IP アドレスを使用して、SQL Server インスタンスに正常に接続できるかどうかを確認する手順をこの節で説明します。

（3） SSMS の実行

SSMS をクライアントノードで開きます。

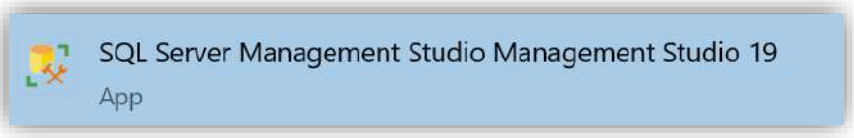


図 8.8-1 SSMS の実行

（4） 仮想 IP アドレスを使用してログイン

次に、先ほど設定した仮想 IP アドレスを使用して、システム管理者（sa）アカウントでログインします。

このステップで正常にログインできると、仮想 IP アドレスの設定が成功していることが確認できます。

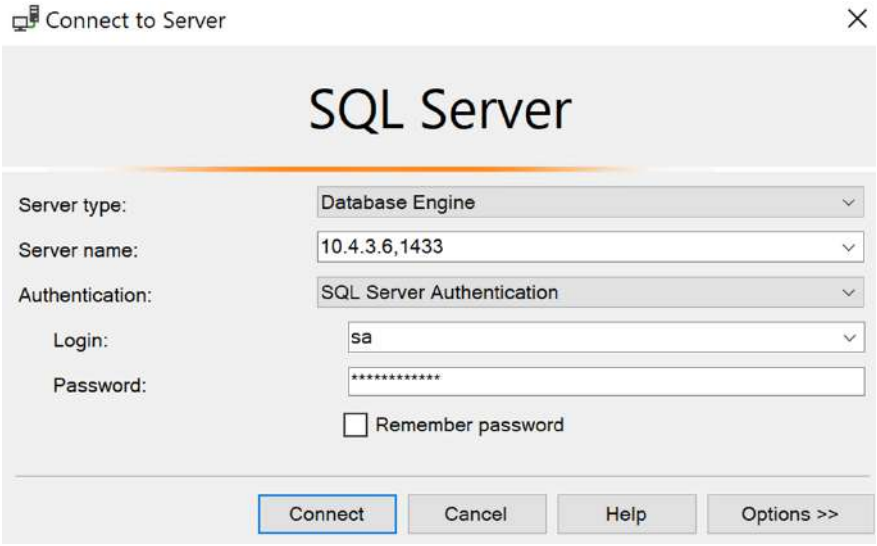


図 8.8-2 仮想 IP アドレスを使用してログイン

（5） ログイン完了

ログインが成功した場合、クライアントノードで仮想 IP アドレスを使用して SQL Server インスタンスを管理できるようになります。これで動作検証は完了です。

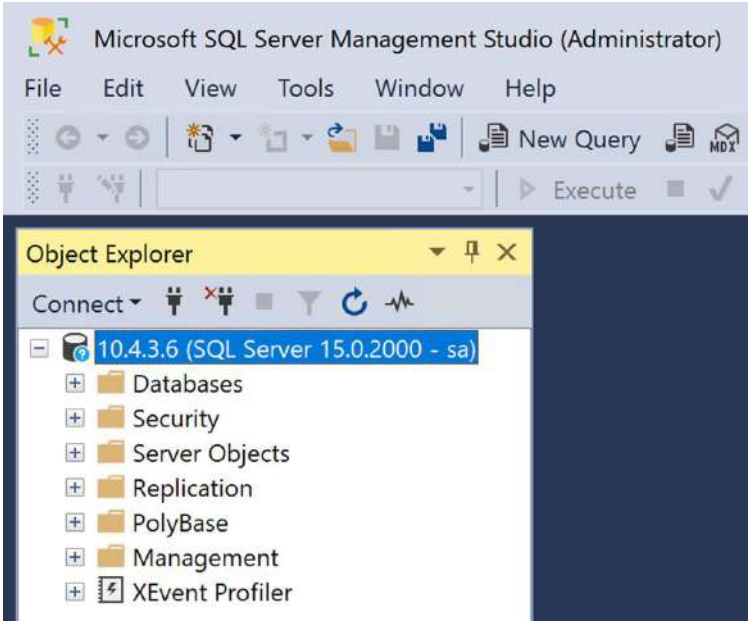


図 8.8-3 ログイン完了

9. お問い合わせ

本書の記載内容についてのお問い合わせ先

■ LifeKeeper 製品の導入を検討中のお客様

弊社パートナー営業部までお問い合わせください。

お問い合わせメールフォーム

https://mk.sios.jp/BC_Web_Free-entry_Inquiry.html

■ LifeKeeper 製品をご購入済みのお客様

弊社 LifeKeeper 製品サポート窓口までお問い合わせください。

購入後のお問い合わせ

https://bc.sios.jp/support_lk.html

10. 免責事項

- **本書に記載された情報は予告なしに変更、削除される場合があります。最新のものをご確認ください。**
- **本書に記載された情報は、全て慎重に作成され、記載されていますが、本書をもって、その妥当性や正確性についていかなる種類の保証もするものではありません。**
- **本書に含まれた誤りに起因して、本書の利用者に生じた損害については、サイオステクノロジー株式会社は一切の責任ｓｓを負うものではありません。**
- **第三者による本書の記載事項の変更、削除、ホームページ及び本書等に対する不正なアクセス、その他第三者の行ためにより本書の利用者に生じた一切の損害について、サイオステクノロジー株式会社は一切の責任を負うものではありません。**
- **システム障害などの原因によりメールフォームからのお問い合せが届かず、または延着する場合がありますので、あらかじめご了承ください。お問い合せの不着及び延着に関し、サイオステクノロジー株式会社は一切の責任を負うものではありません。**

サイオステクノロジー株式会社
住所 ： 〒106-0047
東京都港区南麻布 2 丁目 12-3　サイオスビル

URL: https://sios.jp