



Microsoft Azure

Microsoft Azure 自習書シリーズ No.7

企業内システムと Microsoft Azure の VPN 接続、ファイルサーバー連携

Published: 2014 年 5 月 30 日

Updated: 2014 年 9 月 30 日

Cloudlive, Inc.



本書に含まれる情報は本書の制作時のものであり、将来予告なしに変更されることがあります。提供されるソフトウェアおよびサービスは市場の変化に対応する目的で隨時更新されるため、本書の内容が最新のものではない場合があります。本書の記述が実際のソフトウェアおよびサービスと異なる場合は、実際のソフトウェアおよびサービスが優先されます。Microsoft および Cloudlive は、本書の内容を更新したり最新の情報を反映することについて一切の義務を負わず、これらを行わないことによる責任を負いません。また、Microsoft および Cloudlive は、本書の使用に起因するいかなる状況についても責任を負いません。この状況には、過失、あらゆる破損または損失（業務上の損失、収益または利益などの結果的な損失、間接的な損失、特別の事情から生じた損失を無制限に含む）などが含まれます。

Microsoft、SQL Server、Visual Studio、Windows、Windows Server、MSDN は米国 Microsoft Corporation および、またはその関連会社の、米国およびその他の国における登録商標または商標です。

その他、記載されている会社名および製品名は、各社の商標または登録商標です。

© Copyright 2014 Microsoft Corporation. All rights reserved.

本ドキュメントの更新について

バージョン	更新日	内容
v1.00	2014/6/30	・初版リリース
v1.10	2014/9/30	・2014年9月現在の情報に更新
v1.20	2015/1/30	・2015年1月現在の情報に更新

目次

STEP 1. 仮想ファイルサーバーの概要と本書の目的について	5
1.1 仮想ファイルサーバーの概要	6
1.2 シナリオ	7
1.3 ゴール	8
STEP 2. 実習の前提について	9
2.1 前提条件	10
STEP 3. VPN 接続を設定する	11
3.1 仮想ネットワークの作成	12
3.2 仮想ゲートウェイの作成	19
3.3 社内ネットワークの構成	23
STEP 4. ストレージアカウントを作成する	24
4.1 ストレージアカウントの作成	25
STEP 5. 仮想マシンを作成する	28
5.1 仮想サーバーの作成	29
5.2 仮想マシンへの RDP 接続	37
5.3 日本語化	40
5.4 タイムゾーン	50
5.5 Windows Update の設定	53
5.6 ディスクを追加する	56
5.7 ユーザーとグループを作成する	65
STEP 6. Microsoft Azure 上にファイルサーバーを導入する	73
6.1 ファイルサーバーの構成	74
6.2 共有フォルダーの作成	79
6.3 アクセス権の設定	84
6.4 ネットワーク共有	92

STEP 1. 仮想ファイルサーバーの概要と本書の目的について

この STEP では、仮想ファイルサーバーの概要と本書の目的について説明します。

この STEP では、次のことを学習します。

- ✓ 仮想ファイルサーバーの概要
- ✓ シナリオ
- ✓ ゴール

1.1 仮想ファイルサーバーの概要

◆ 仮想ファイルサーバーの概要

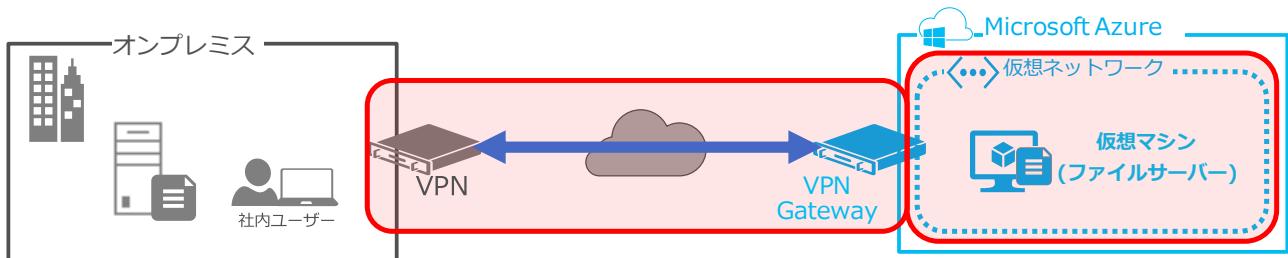
Azure 上で仮想マシンを作成し、ファイルサーバーとして構成して、オンプレミス ネットワークと相互接続する事で、Azure ファイルサーバーに自社のネットワークの一部としてアクセスする事ができます。

1.2 シナリオ

◆ 構築範囲について

本自習書では、下記赤枠内の構築を行います。

オンプレミス側に VPN、Azure 側に VPN ゲートウェイ、仮想ネットワーク、仮想マシン(ファイルサーバー)を導入します。



1.3 ゴール

➔ 本自習書のゴールについて

上記のシナリオで環境を構築し、以下が確認できたことをもってゴールとします。

- ・オンプレミス側から Azure 仮想ファイルサーバーのフォルダーにアクセスできるであること。

STEP 2. 実習の前提について

この STEP では、この自習書で実習を行うために必要な前提について説明します。

この STEP では、次のことを学習します。

- ✓ 前提条件

2.1 前提条件

◆ 前提条件について

本自習書は下記環境を前提に記載されています。そのため、オンプレミス側のファイルサーバーの構築や Microsoft Azure へのサインインアカウントの作成及びサインイン方法については記載いたしません。

- ・ インターネット回線が存在している。
- ・ オンプレミス環境にて Site-to-Site を実現できるルーター(ファイアフォール等)が存在している。
- ・ Microsoft Azure へのサインインアカウントを持っている。
- ・ VPN 接続用の回線は、固定グローバル IP アドレスが必要とする。
- ・ Azure 仮想ネットワークとオンプレミスを VPN 接続するには、オンプレミス側に VPN デバイスを設置する必要がある。(Point to Site 接続を除く)
- ・ Azure 上のファイルサーバーにアクセスするため、オンプレミス上にクライアント PC を用意すること。

STEP 3. VPN 接続を設定する

この STEP では、VPN 接続のために仮想ネットワーク、仮想ゲートウェイの作成について説明します。

この STEP では、次のことを学習します。

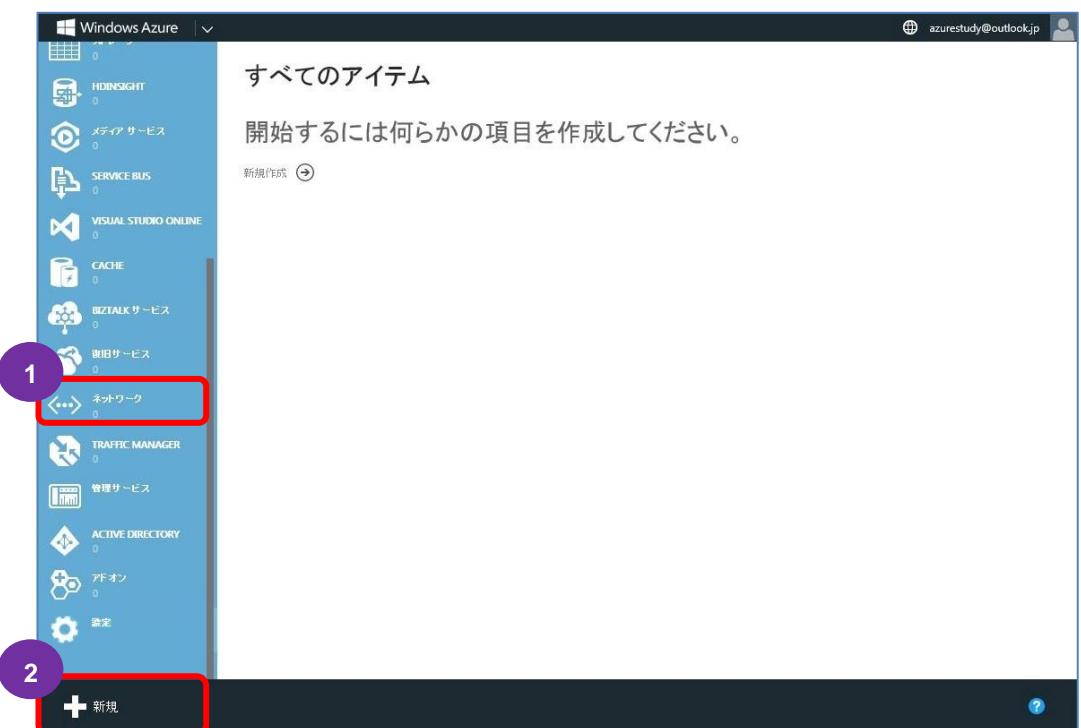
- ✓ 仮想ネットワークの作成
- ✓ 仮想ゲートウェイの作成
- ✓ 社内ネットワークの構成

3.1 仮想ネットワークの作成

◆ 仮想ネットワークの作成

仮想ネットワークは、仮想マシンを社内ネットワークへ接続し、社内のコンピューターのように操作することができます。仮想ネットワークの接続形態には、「サイト間 VPN」と「ポイント対サイトVPN」があります。ここでは、サイトとサイトを接続するサイト間 VPN を作成します。

1. 画面左側のメニューから[ネットワーク]をクリックし、画面左下の [+新規] をクリックします。



2. [ネットワークサービス]→[仮想ネットワーク]→[カスタム作成]をクリックします。



企業内システムと Microsoft Azure の VPN 接続、ファイルサーバー連携

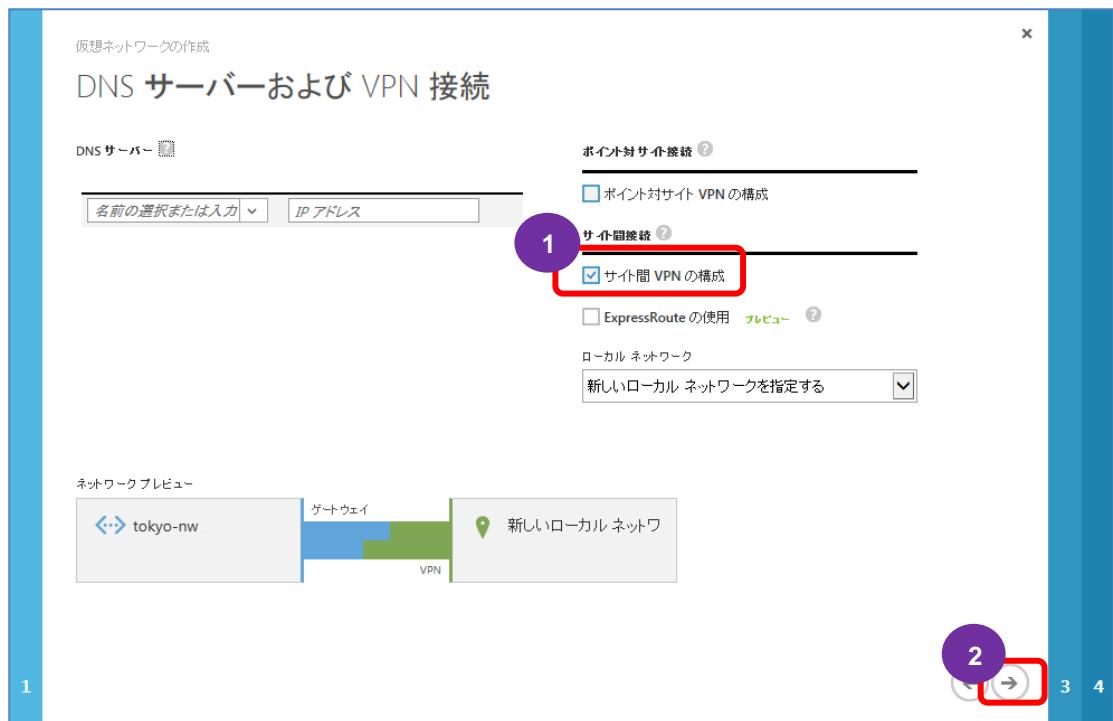
3. [仮想ネットワークの作成 > 仮想ネットワークの詳細]が表示されます。次の設定値を入力および選択し、[⊕] をクリックします。

項目	設定値
名前	tokyo-nw
場所	日本(東)



企業内システムと Microsoft Azure の VPN 接続、ファイルサーバー連携

4. [DNS サーバーおよび VPN 接続]が表示されます。[サイト間 VPN の構成]に☑を入れ、[⊕]をクリックします。



企業内システムと Microsoft Azure の VPN 接続、ファイルサーバー連携

5. [サイト間接続]が表示されます。次の設定値を入力および選択し、[⊕] をクリックします。

項目	設定値
名前	local-nw
VPN デバイスの IP アドレス	<プロバイダーから割り当てられた WAN 側の IP アドレス>
アドレス空間	・開始 IP : 192.168.118.0



企業内システムと Microsoft Azure の VPN 接続、ファイルサーバー連携

6. [仮想ネットワークアドレス空間] が表示されます。次の設定値を入力および選択し、[⊕]をクリックします。

項目	設定値
名前	tokyo-Subnet1
サブネットの開始 IP	10.1.1.0
CIDR (アドレス数)	/24 (256)

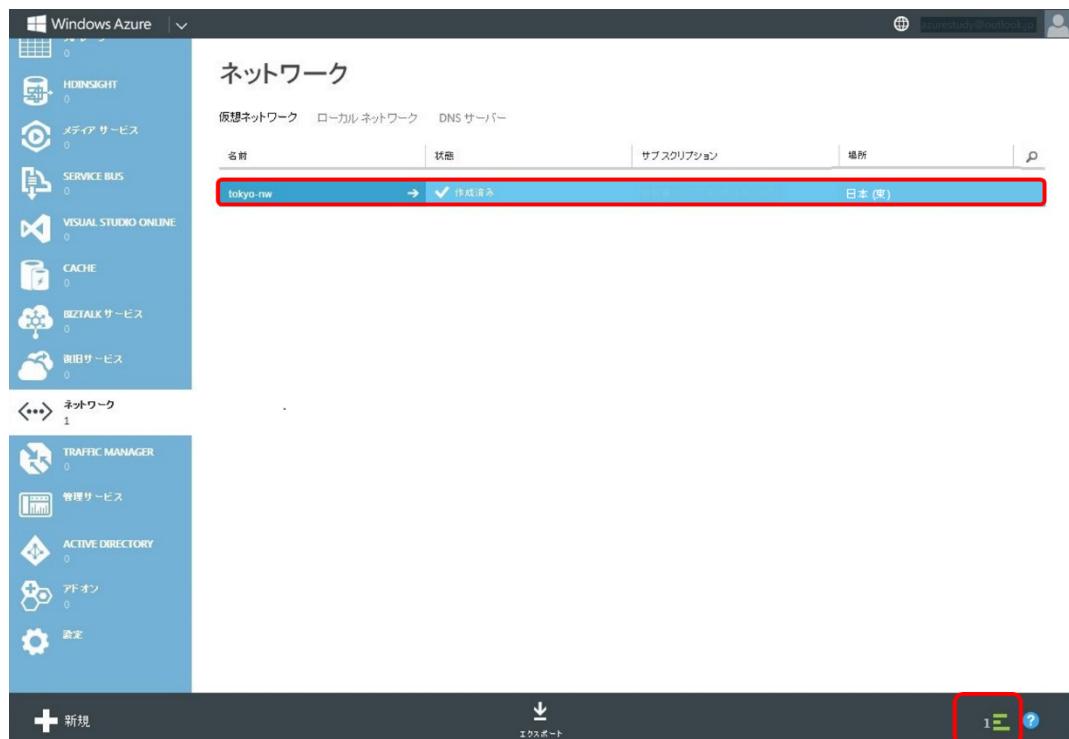


企業内システムと Microsoft Azure の VPN 接続、ファイルサーバー連携

7. 引き続き、[ゲートウェイサブネットの追加]をクリックします。サブネットの行に[ゲートウェイ]が追加されますので、[ゲートウェイの開始 IP]を入力し、[ゲートウェイの CIDR(アドレス数)]を選択します。(今回はデフォルト値を使用します。) 入力および選択が終わったら、右下のをクリックします。

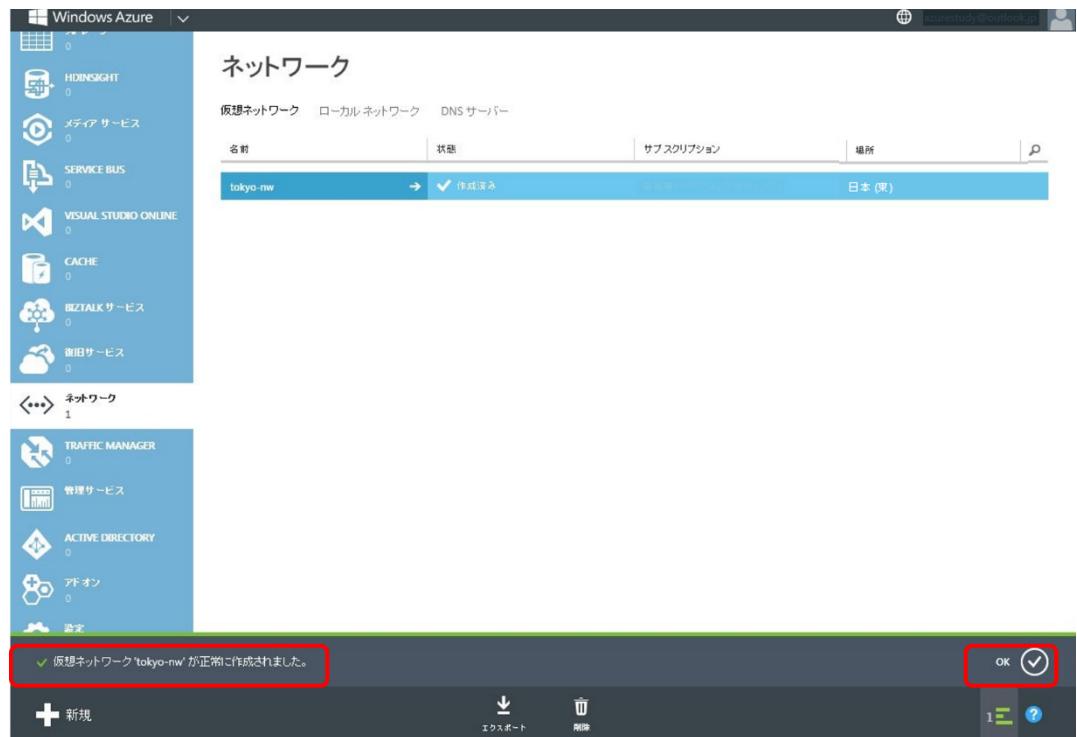


8. [ネットワーク > 仮想ネットワーク]画面に戻ります。作成中の仮想ネットワークがリストに表示されます。右下に**作成中**であることを示すアイコンが表示されます。



企業内システムと Microsoft Azure の VPN 接続、ファイルサーバー連携

9. [仮想ネットワーク “tokyo-nw” が正常に作成されました]のメッセージが表示されたら、[OK (✓)]チェックをクリックしてメッセージをクリアします。

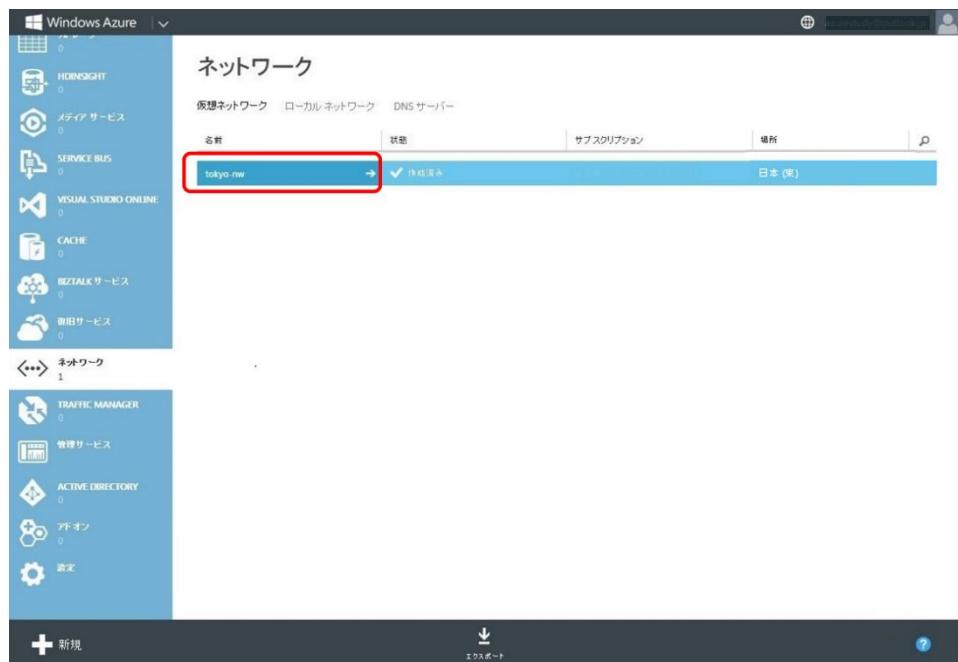


3.2 仮想ゲートウェイの作成

➔ 仮想ゲートウェイの作成

仮想ゲートウェイを作成します。

1. 作成した仮想ネットワーク名、「tokyo-nw」をクリックします。

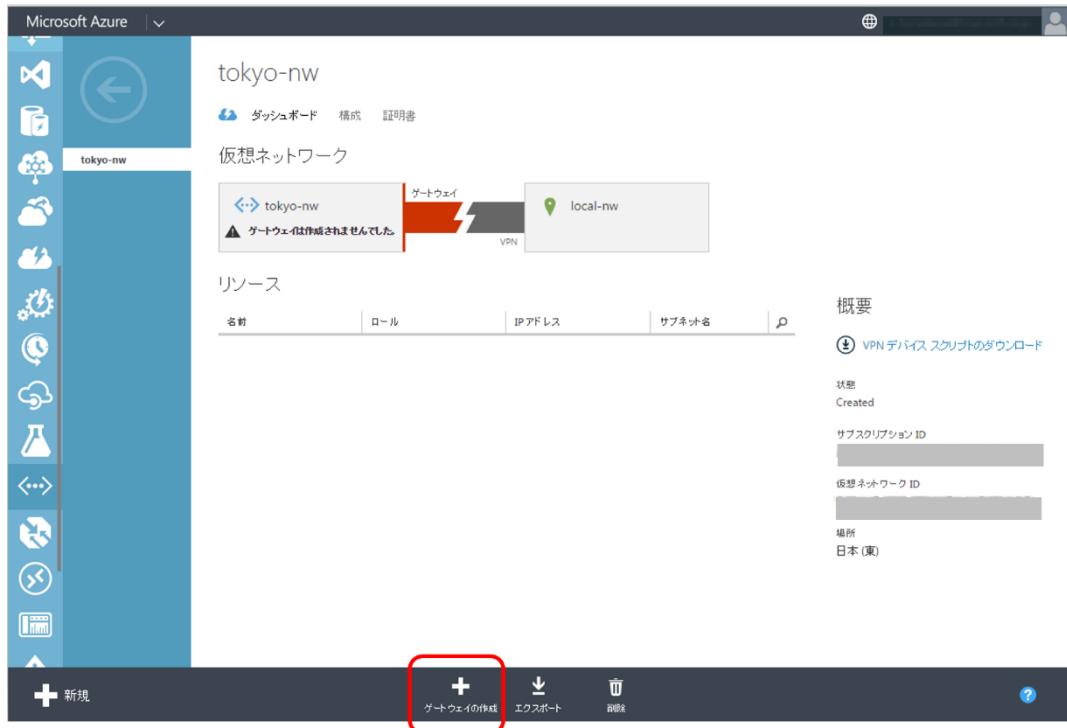


2. [クイックスタート]が表示されます。次に[ダッシュボード]をクリックします。

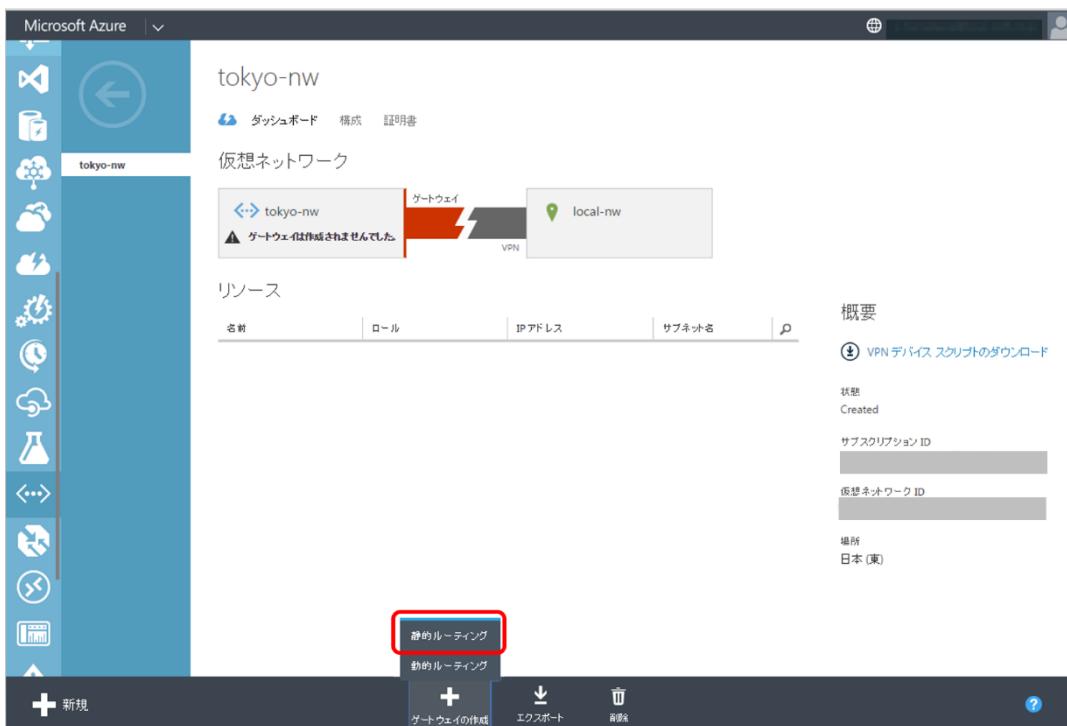


企業内システムと Microsoft Azure の VPN 接続、ファイルサーバー連携

3. [ダッシュボード]が表示されます。次に画面下部の[+ゲートウェイの作成]をクリックします。



4. [静的ルーティング/動的ルーティング]のリストが表示されます。今回は[静的ルーティング]をクリックします。

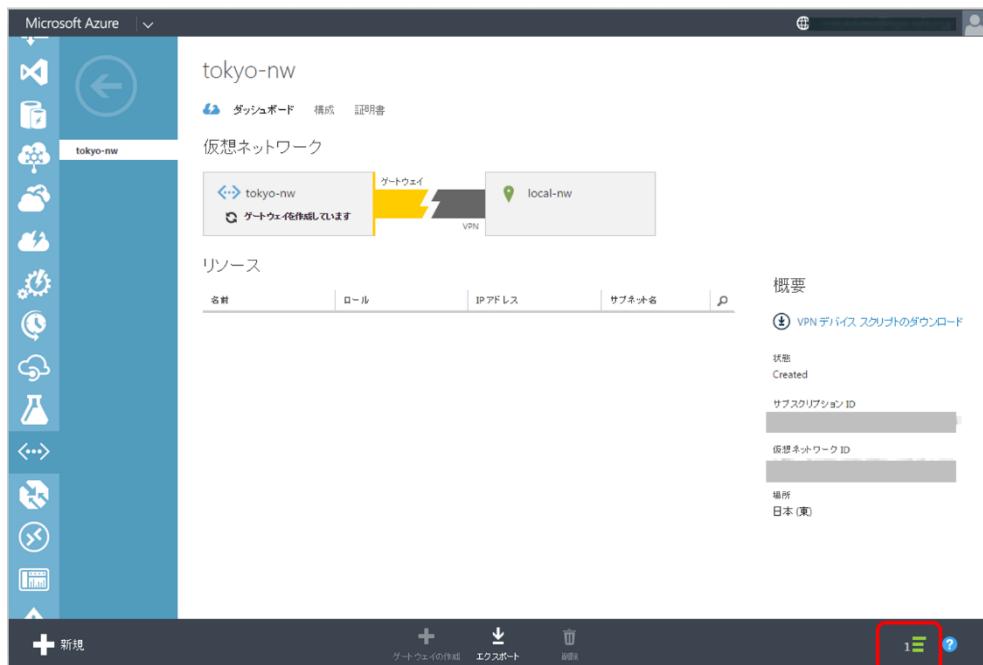


企業内システムと Microsoft Azure の VPN 接続、ファイルサーバー連携

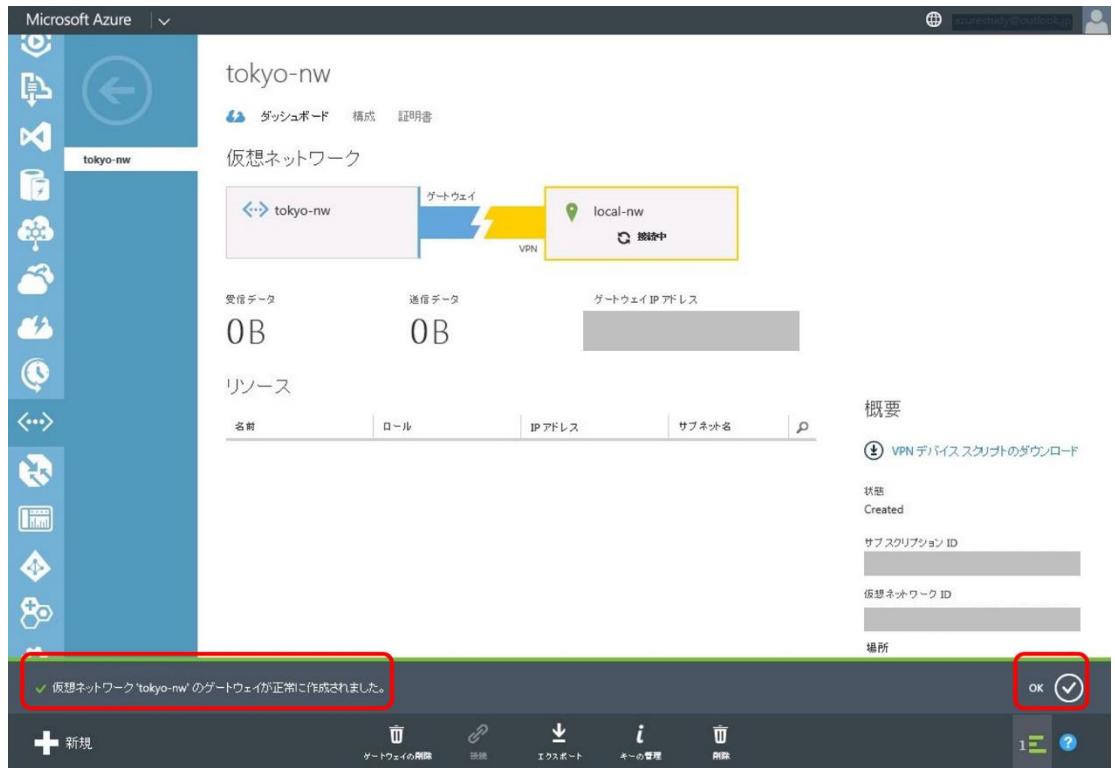
5. 画面下部に[仮想ネットワーク "tokyo-nw" にゲートウェイを作成しますか?]というメッセージが表示されますので、[はい]をクリックします。



6. [ダッシュボード]に戻ります。右下に**作成中**であることを示すアイコンが表示されます。



7. [仮想ネットワーク “tokyo-nw” のゲートウェイが正常に作成されました]のメッセージが表示されたら、[OK]をクリックしてメッセージをクリアします。



3.3 社内ネットワークの構成

◆ 社内ネットワークの構成

Azure と接続するための VPN 機器の設定を行います。

Note : VPN 機器関連参照先

- VPN 接続検証済み ルーター一覧

<http://msdn.microsoft.com/ja-jp/windowsazure/dn132612.aspx>

- 一般的な VPN 機器の必須要件と Cisco 社と Juniper 社のルーターについては、こちらをご確認ください。

<http://msdn.microsoft.com/en-us/library/windowsazure/jj156075.aspx>

◆ 社内ネットワークの構成手順

社内ネットワークの作成手順については別途自習書、「企業内システムと Microsoft Azure の VPN 接続」の「STEP 8 . ASA の設定」をご参照願います。

STEP 4. ストレージアカウントを作成する

この STEP では、仮想マシンを作成するためにストレージアカウントの作成について説明します。

この STEP では、次のことを学習します。

- ✓ ストレージアカウントの作成

4.1 ストレージアカウントの作成

ストレージアカウントは Azure のストレージを使用するために必要なアカウントです。事前にストレージアカウントを作成せずに仮想マシンを作成することも可能ですが、その場合、ランダムな名称が用いられます。

今後の管理の面なども考慮して本自習書では、仮想マシンを作成する前に明示的にストレージアカウントを作成します。

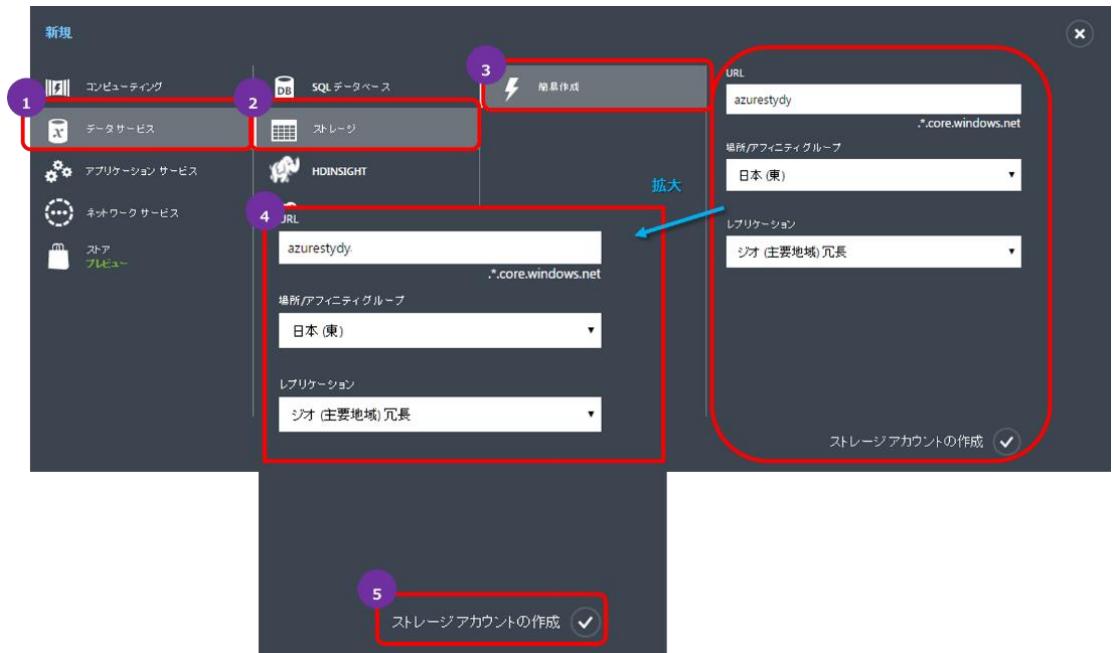
1. Azure 管理ポータルにサインインし、右のメニューから[ストレージ]をクリックします。画面左下に表示される[+新規]をクリックします。



企業内システムと Microsoft Azure の VPN 接続、ファイルサーバー連携

2. [データサービス]→[ストレージ]→[簡易作成]の順にクリックします。

さらに、[URL]に「azurestudy」(任意の文字列)を入力、[場所/アフィニティグループ]に「日本(東)」を選択、[レプリケーション]に「ジオ(主要地域)冗長」(任意のレプリケーション)を選択し、[ストレージアカウントの作成]をクリックします。



項目	説明								
URL	<ul style="list-style-type: none"> ストレージアカウント内に格納されたオブジェクトにアクセスするための URL を決めます。 一意である必要があります。一意であることが確認されると[URL]の右に「」が表示されます。 								
場所/アフィニティグループ	<ul style="list-style-type: none"> Microsoft Azure 内で展開する地域を指定します。 								
レプリケーション	<ul style="list-style-type: none"> 以下の 4 つからレプリケーション方法を選択することができます。 <table border="1"> <tr> <td>ローカル冗長</td><td> <ul style="list-style-type: none"> 1 つのリージョンにデータのレプリカを複数保持することで、高い持続性を達成します。 </td></tr> <tr> <td>ジオ(主要地域)冗長</td><td> <ul style="list-style-type: none"> 同じ Geo 内の遠く離れた 2 つのリージョン間で非同期的にレプリケーションを行うことによって、データ継続性を高めます。両方のリージョンで、複数のデータのレプリカを保持します。 なお、既定で選択されます。 </td></tr> <tr> <td>読み取りアクセス Geo 冗長</td><td> <ul style="list-style-type: none"> Geo 冗長ストレージに加え、プライマリ ストレージのデータとまったく同じコピーが格納される、セカンダリ リージョンのストレージ アカウントに読み取り専用でアクセスすることができます。プライマリ リージョンのストレージ アカウントが利用できなくなった場合、お客様はこのサービスを使ってご自分のデータにアクセスすることができます。 ジオ(主要地域)冗長に比べ容量あたりの価格が上がります。 </td></tr> <tr> <td>ゾーン冗長</td><td> <ul style="list-style-type: none"> 単一リージョン内のデータの持続性を保証します。 1 つのリージョン内、または 2 つのリージョンにまたがって、2 カ所から 3 カ所の施設にわたって 3 回レプリケートされるため、ローカル冗長より持続性が高くなります。 ロック BLOB のみで使用できます。 </td></tr> </table>	ローカル冗長	<ul style="list-style-type: none"> 1 つのリージョンにデータのレプリカを複数保持することで、高い持続性を達成します。 	ジオ(主要地域)冗長	<ul style="list-style-type: none"> 同じ Geo 内の遠く離れた 2 つのリージョン間で非同期的にレプリケーションを行うことによって、データ継続性を高めます。両方のリージョンで、複数のデータのレプリカを保持します。 なお、既定で選択されます。 	読み取りアクセス Geo 冗長	<ul style="list-style-type: none"> Geo 冗長ストレージに加え、プライマリ ストレージのデータとまったく同じコピーが格納される、セカンダリ リージョンのストレージ アカウントに読み取り専用でアクセスすることができます。プライマリ リージョンのストレージ アカウントが利用できなくなった場合、お客様はこのサービスを使ってご自分のデータにアクセスすることができます。 ジオ(主要地域)冗長に比べ容量あたりの価格が上がります。 	ゾーン冗長	<ul style="list-style-type: none"> 単一リージョン内のデータの持続性を保証します。 1 つのリージョン内、または 2 つのリージョンにまたがって、2 カ所から 3 カ所の施設にわたって 3 回レプリケートされるため、ローカル冗長より持続性が高くなります。 ロック BLOB のみで使用できます。
ローカル冗長	<ul style="list-style-type: none"> 1 つのリージョンにデータのレプリカを複数保持することで、高い持続性を達成します。 								
ジオ(主要地域)冗長	<ul style="list-style-type: none"> 同じ Geo 内の遠く離れた 2 つのリージョン間で非同期的にレプリケーションを行うことによって、データ継続性を高めます。両方のリージョンで、複数のデータのレプリカを保持します。 なお、既定で選択されます。 								
読み取りアクセス Geo 冗長	<ul style="list-style-type: none"> Geo 冗長ストレージに加え、プライマリ ストレージのデータとまったく同じコピーが格納される、セカンダリ リージョンのストレージ アカウントに読み取り専用でアクセスすることができます。プライマリ リージョンのストレージ アカウントが利用できなくなった場合、お客様はこのサービスを使ってご自分のデータにアクセスすることができます。 ジオ(主要地域)冗長に比べ容量あたりの価格が上がります。 								
ゾーン冗長	<ul style="list-style-type: none"> 単一リージョン内のデータの持続性を保証します。 1 つのリージョン内、または 2 つのリージョンにまたがって、2 カ所から 3 カ所の施設にわたって 3 回レプリケートされるため、ローカル冗長より持続性が高くなります。 ロック BLOB のみで使用できます。 								

3. ストレージアカウントが作成されると[状態]が[オンライン]になります。

名前	状態
azurestudy	→ オンライン

STEP 5. 仮想マシンを作成する

この STEP では、Azure 上に仮想サーバーを作成するための手順について説明します。

この STEP では、次のことを学習します。

- ✓ 仮想サーバーの作成
- ✓ 仮想サーバーに RDP 接続する
- ✓ 日本語化する
- ✓ タイムゾーンを変更する
- ✓ Windows Update の設定
- ✓ ディスクを追加する
- ✓ ユーザーとグループを作成する

5.1 仮想サーバーの作成

◆ 仮想サーバーの作成

ファイルサーバーのベースとなる仮想マシンを作成します。

1. Azure 管理ポータルにサインインし、右のメニューから[仮想マシン]をクリックします。画面左下に表示される[+新規]をクリックします。

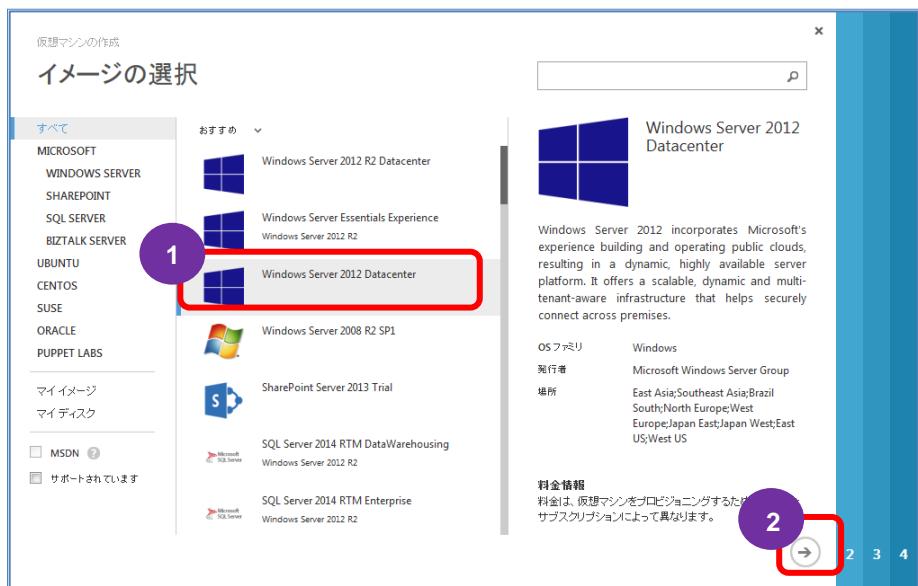


2. 簡易ウィザードが表示されます。

[コンピューティング]→[仮想マシン]→[ギャラリーから]の順にクリックします。



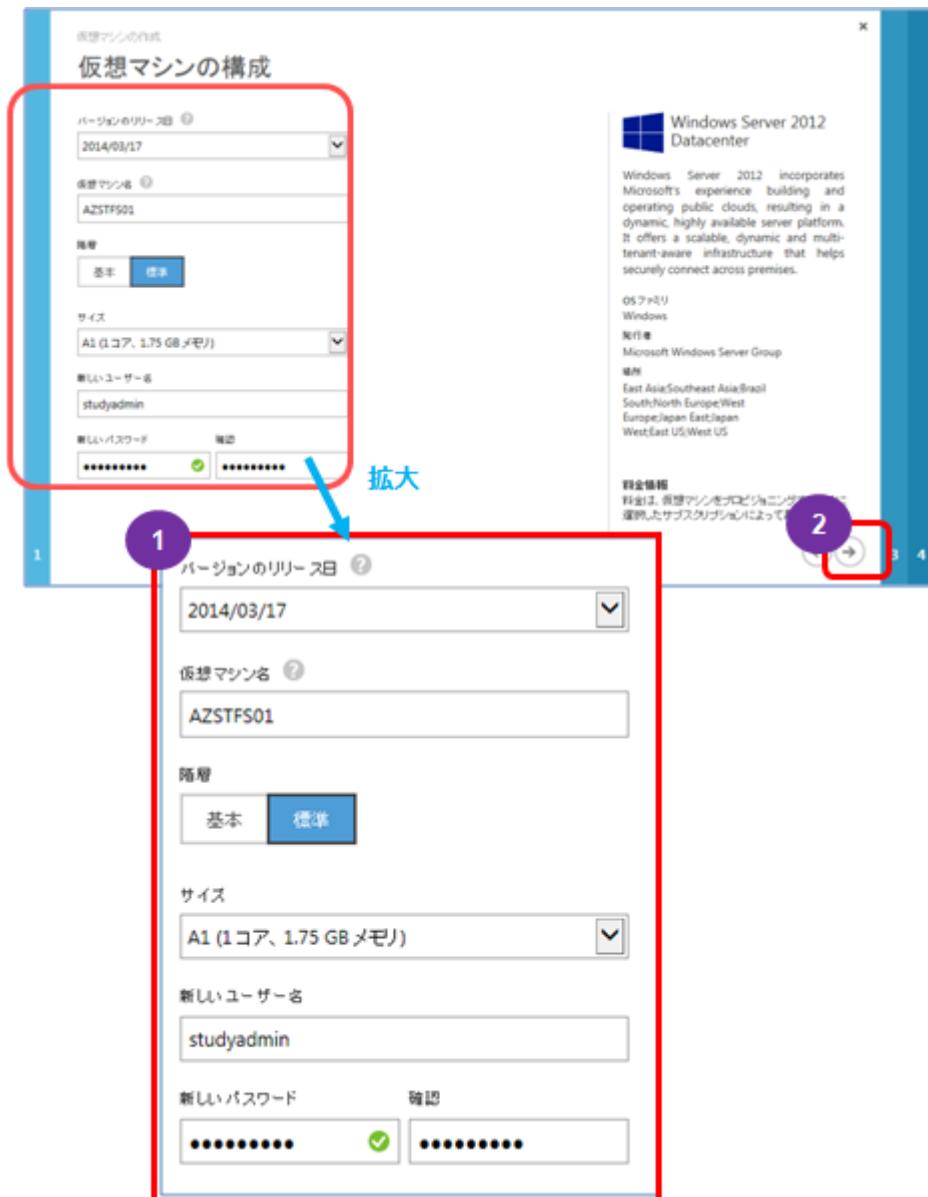
3. インストールする OS[Windows Server 2012 Datacenter]を選択し[④]をクリックします。



企業内システムと Microsoft Azure の VPN 接続、ファイルサーバー連携

4. 仮想マシンの構成の 2 ページ目が表示されます。

[バージョンのリリース日]に「2014/03/17」を選択(リリース日は更新されていくので、作成時点の最新の日付を選択します)、[仮想マシン名]に「AZSTFS01」(任意の文字列)を入力、[階層]に「標準」を選択、[サイズ]に「A1(1コア、1.75GB メモリ)」を選択、[新しいユーザー名]に「studyadmin」(任意の文字列)を入力、[新しいパスワード]および[確認]に「studyP@ss」(任意の文字列)を入力し、[④]をクリックします。

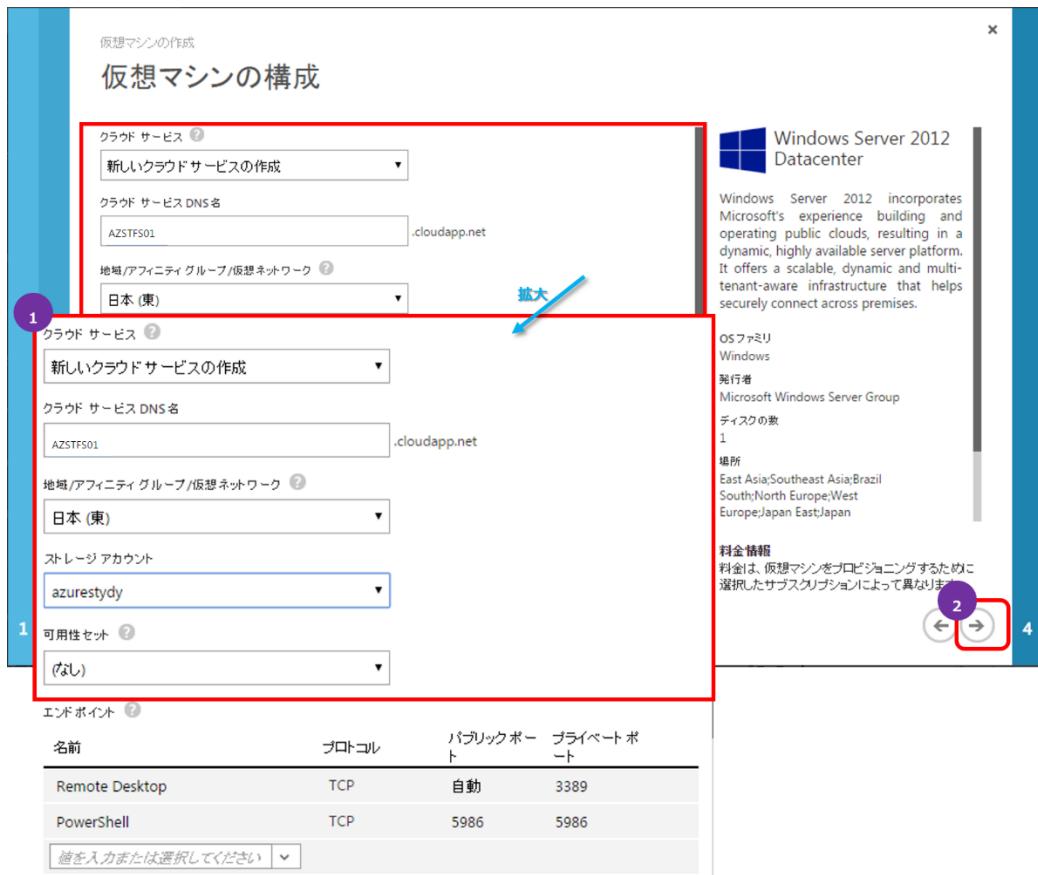


項目	説明
バージョンのリリース日	<ul style="list-style-type: none"> ベースとなる OS のイメージのバージョンを選択します。 2 世代のバージョンから選択できます。
仮想マシン名	<ul style="list-style-type: none"> 仮想マシン名を入力します。 予約文字列もしくは、既に同じ仮想ネットワーク内で使用されている仮想マシン名を使用することは出来ません。
階層	<ul style="list-style-type: none"> 以下の 2 つから選択することが出来ます。
基本(基本コンピューティング レベル)	<ul style="list-style-type: none"> 負荷分散と自動調整の機能は含まれません。 このような機能が不要な、单一インスタンスの運用アプリケーション、開発ワークロード、テスト サーバー、バッチ処理アプリケーションに適しています。現在、基本コンピューティング レベルは汎用目的インスタンスでのみ利用できます。
	<ul style="list-style-type: none"> 幅広いアプリケーションを実行するために最適なコンピューティング リソース、メモリ リソース、IO リソースを備えています。自動調整と負荷分散の機能を利用できます。 標準コンピューティング レベルは、汎用目的インスタンス、メモリ集中型インスタンス、コンピューティング集中型インスタンスで利用できます。
サイズ	<ul style="list-style-type: none"> サイズは A0～A7 の中から選択できます。各サイズの説明は別途「仮想マシンのサイズについて」を参照ください。
新しいユーザー名	<ul style="list-style-type: none"> ユーザー名を入力します。 予約文字列の場合には使用することが出来ません。 なお、ここで指定した名前で管理者権限を持ったユーザー アカウントが作成されます。
新しいパスワード／確認	<ul style="list-style-type: none"> パスワードを入力します。 複雑さや非汎用的な文字列、非予約文字列であるかなどが検査されます。 これをクリアできない文字列の場合、仮想マシンの作成を続けることが出来ません。

企業内システムと Microsoft Azure の VPN 接続、ファイルサーバー連携

5. 仮想マシンの構成の 3 ページ目が表示されます。

[クラウド サービス]に「新しいクラウドサービス」を選択、[クラウド サービス DNS 名]に「AZSTFS01」(任意の文字列)を入力、[地域/アフィニティグループ/仮想ネットワーク]に「日本 (東)」を選択、[ストレージアカウント]に「azurestudy」(事前に作成したストレージアカウント)を選択、[可用性セット]に「なし」を選択し、[④]をクリックします。



項目	説明
クラウドサービス	<ul style="list-style-type: none"> ・ クラウドサービスを選択します。 <p>クラウドサービスとは、1つまたは複数の仮想マシンを配置する箱を意味します。同じクラウド サービス内に複数の仮想マシンを作成すると、仮想マシンの相互通信、仮想マシン間での負荷分散、仮想マシンの高可用性を実現できます。</p> <p>先にクラウドサービスが作成している場合に選択できます。また、既存のクラウドサービスが存在しない、もしくは選択しなかった(「新しいクラウドサービスの作成」を選択した)場合には、新規にクラウドサービスが作成されます。</p>
クラウドサービス DNS 名	<ul style="list-style-type: none"> ・ クラウドサービス DNS 名を入力します。 <p>インターネット経由でアクセスする際に使用する DNS 名となります。世界で一意の名前を入力する必要があります。</p>
地域/アフィニティグループ/仮想ネットワーク	<ul style="list-style-type: none"> ・ 地域、アフィニティグループ、仮想ネットワークのいずれから仮想マシンが所属する場所を選択します。
仮想ネットワーク サブネット	<ul style="list-style-type: none"> ・ 仮想ネットワークサブネットを選択します。 <p>「リージョン/アフィニティグループ/仮想ネットワーク」の選択で「仮想ネットワーク」を選択した際に表示されます。</p>
ストレージ アカウント	<ul style="list-style-type: none"> ・ ストレージアカウントを選択します。 <p>ストレージアカウントは Microsoft Azure のストレージを使用するために必要なアカウントです。先にストレージアカウントを作成している場合に選択できます。また、既存のストレージアカウントが存在しない、もしくは選択しなかった(「自動的に生成されたストレージ アカウントを使用」を選択した)場合には、新規にストレージアカウントが作成されます。</p>
可用性セット	<ul style="list-style-type: none"> ・ 可用性セットの利用有無を選択します。 <p>同サービスで複数台のサーバーを運用している際に、利用するデータセンターの1系統のクラスタの障害により、複数台が同時に停止しないようにするための設定になります。</p> <p>先に可用性セットを作成している場合には既存の可用性セットを選択することができます。新規に可用性のセットを作成する場合には「可用性セットの作成」を選択します。</p>
可用性セット名	<ul style="list-style-type: none"> ・ 可用性セット名を入力します。 <p>「可用性セット」で「可用性セットの作成」を選択した際に表示されます。</p>
エンドポイント	<ul style="list-style-type: none"> ・ インターネットに対して公開するサービス(ポート)と仮想マシンのサービス(ポート)の紐付けを設定できます。

企業内システムと Microsoft Azure の VPN 接続、ファイルサーバー連携

6. 仮想マシンの構成の 4 ページ目が表示されます。[VM エージェントのインストール]にチェックを付け、[②]をクリックします。



項目	説明
VM エージェント	<ul style="list-style-type: none"> インストールが推奨されます。 誤ってリモートデスクトップ接続の設定を無効にしたり、パスワードを忘れてしまったりした際の復旧を可能にします。
Puppet	<ul style="list-style-type: none"> 本エージェントについては別途 Puppet Labs のサイトをご確認ください。
Enterprise エージェント	
Chef	<ul style="list-style-type: none"> 本エージェントについては別途 Chef Software のサイトをご確認ください。
カスタム スクリプト	<ul style="list-style-type: none"> 本エージェントについては別途 Microsoft のサイトをご確認ください。
Microsoft Antimalware	<ul style="list-style-type: none"> 本セキュリティについては別途 Microsoft のサイトをご確認ください。
Symantec	<ul style="list-style-type: none"> 本セキュリティについては別途 Symantec のサイトをご確認ください。
Endpoint Protection	
Trend Micro	<ul style="list-style-type: none"> 本セキュリティについては別途 Trend Micro のサイトをご確認ください。
Deep Security Agent	

7. 仮想マシンが作成されると[状態]が[実行中]になります。

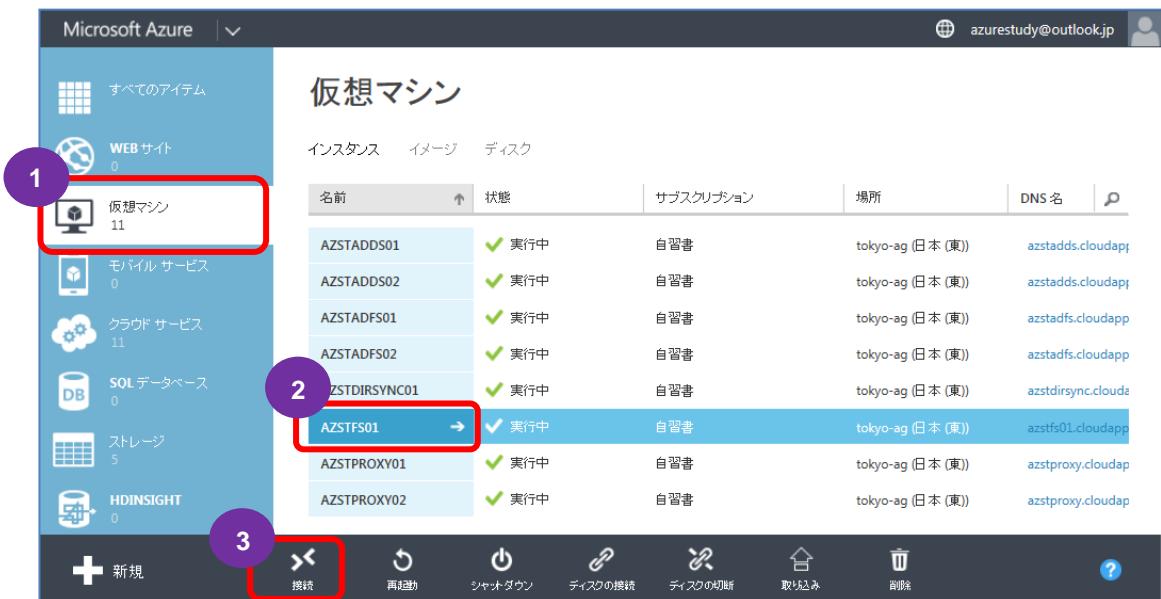
仮想マシン		
名前	↑	状態
AZSTFS01	→	✓ 実行中

5.2 仮想マシンへの RDP 接続

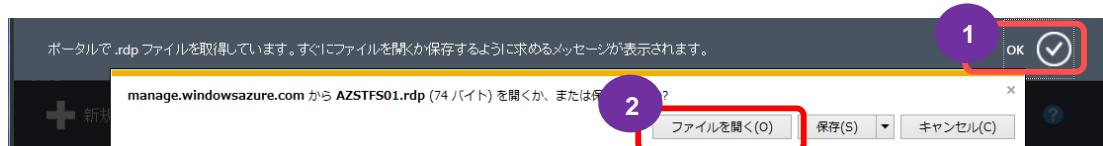
◆ 仮想サーバーに RDP 接続する

Azure に配置した仮想マシンは、RDP (リモートデスクトッププロトコル) により接続して操作することができます。

1. Azure 管理ポータルにサインインし、左バナーの [仮想マシン] をクリックします。上記で作成した仮想マシンの名前(AZSTFS01)を選択し、[接続]ボタンをクリックします。

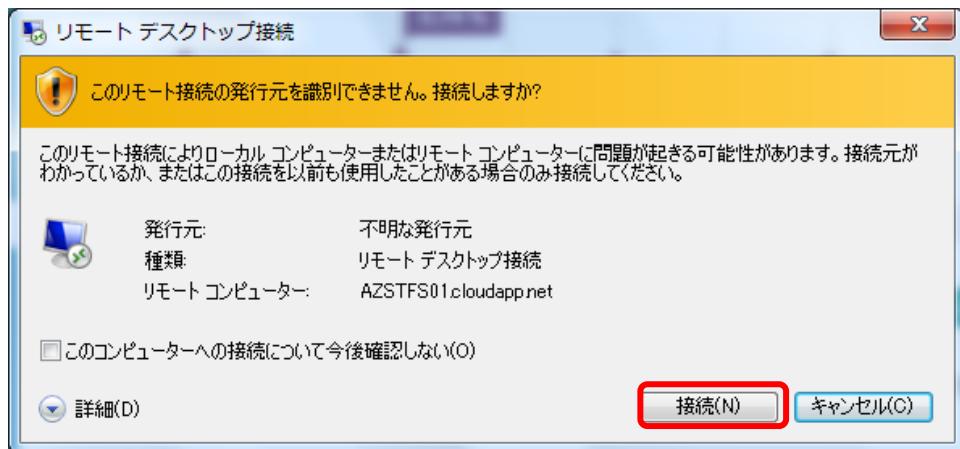


2. 画面下段に[ポータルで.rdp ファイルを取得しています。すぐにファイルを開くか保存するように求めるメッセージが表示されます]というメッセージが表示されたら、[OK?]をクリックします。RDP 接続の設定ファイルが表示されますので [ファイルを開く] をクリックします。

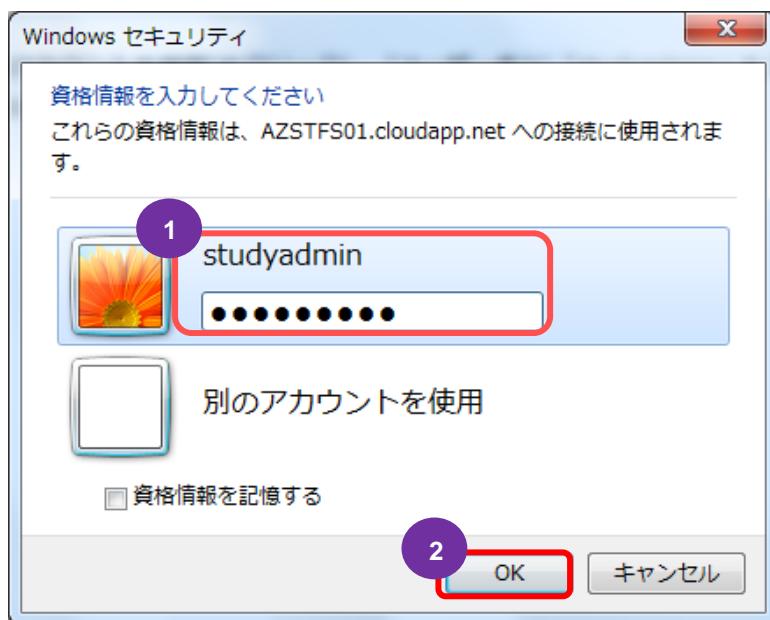


企業内システムと Microsoft Azure の VPN 接続、ファイルサーバー連携

3. RDP 接続の確認画面が表示されますので、[接続]をクリックします。

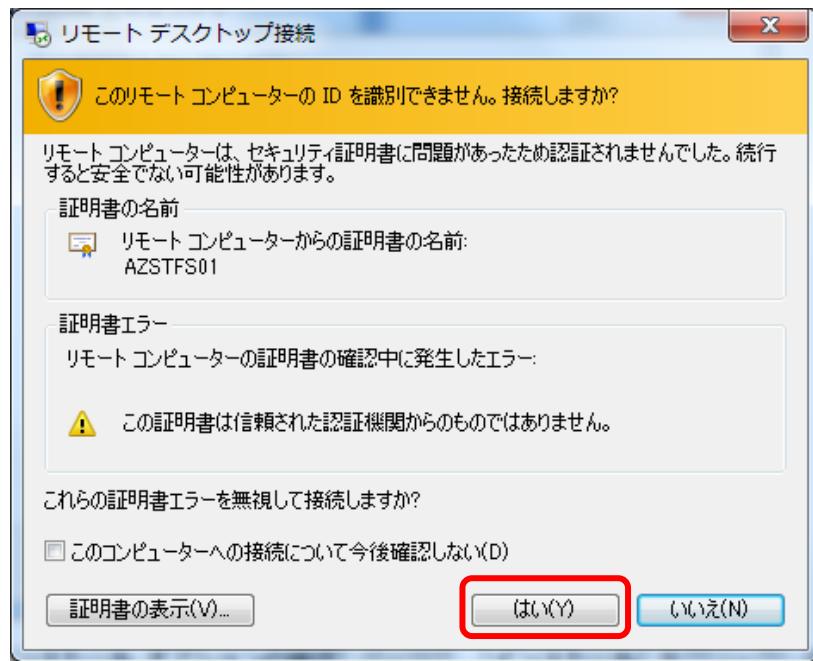


4. 仮想マシンへのログオン画面が表示されます。[ユーザー名]に「studyadmin」を入力、[パスワード]に「studyP@ss」を入力し、[OK]をクリックします。

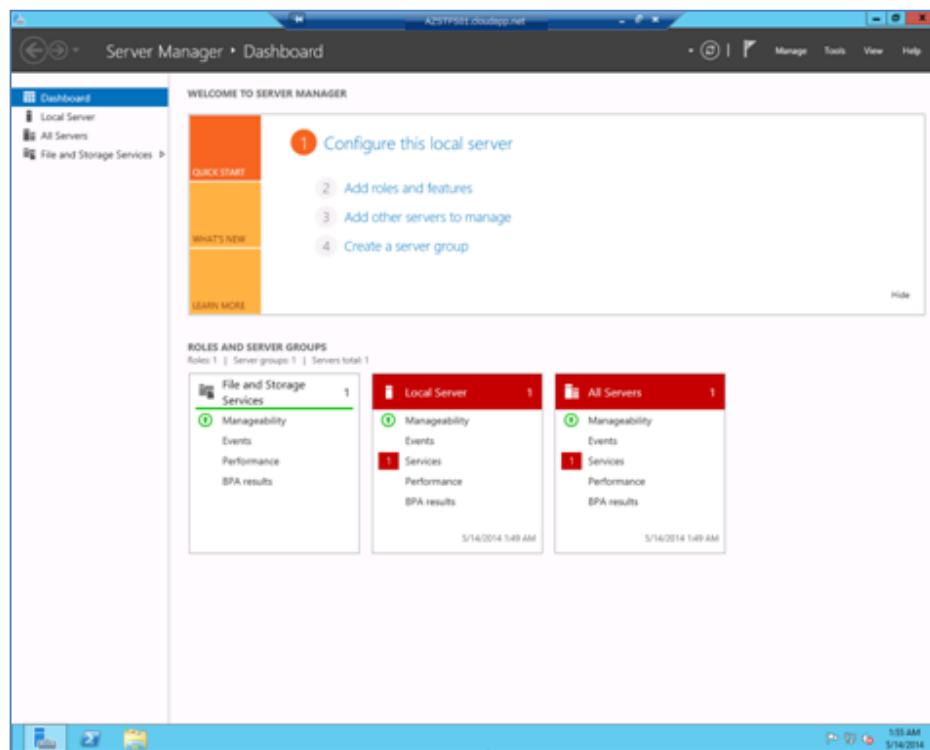


企業内システムと Microsoft Azure の VPN 接続、ファイルサーバー連携

5. セキュリティ証明書の確認エラーが表示される場合は [はい] をクリックします。



6. リモートデスクトップ接続の画面が立ち上ります。Windows Server 2012 がインストールされた仮想マシンに接続されたことを確認します。



5.3 日本語化

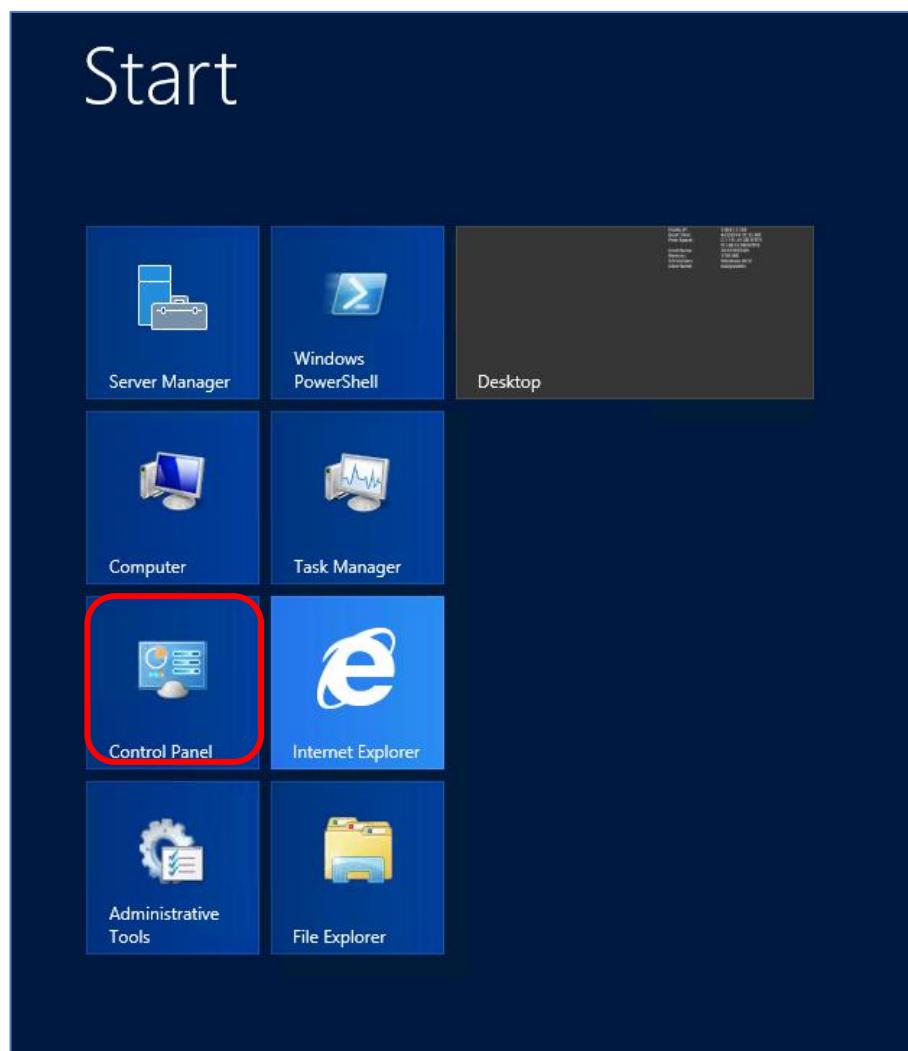
◆ 日本語化する

Azure で作成される仮想マシンの言語は既定で英語になっているため日本語化を行います。

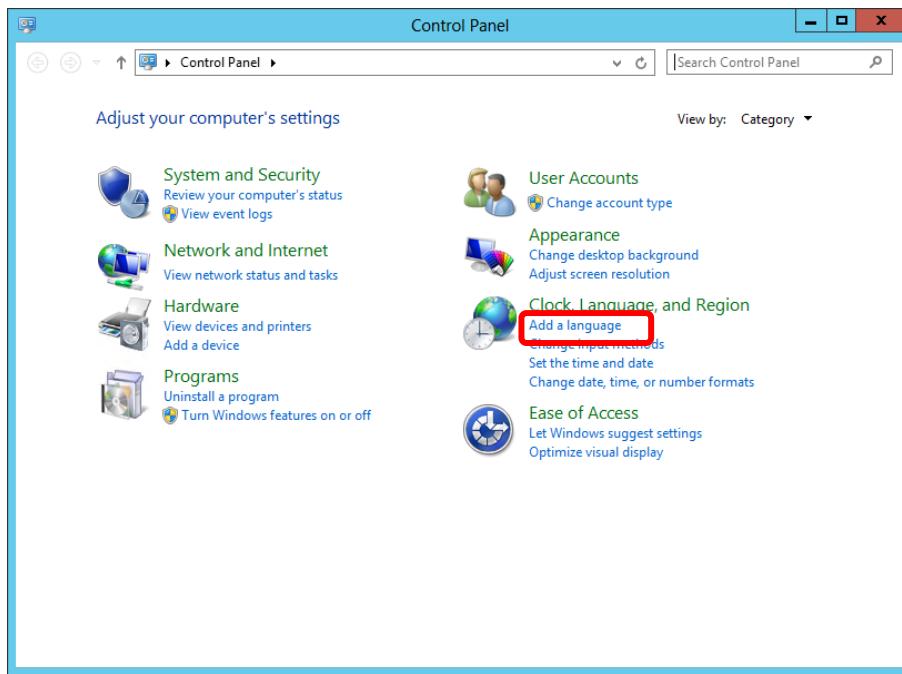
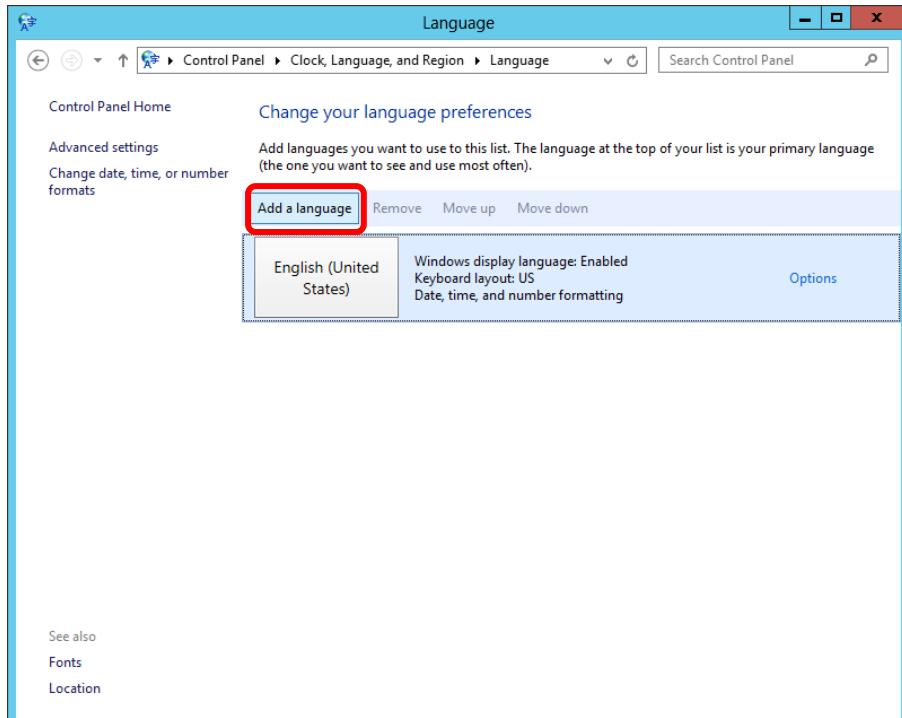
1. デスクトップ画面左下にマウスカーソルを移動し [Start] を表示させクリックします。



2. [Control Panel] をクリックします。

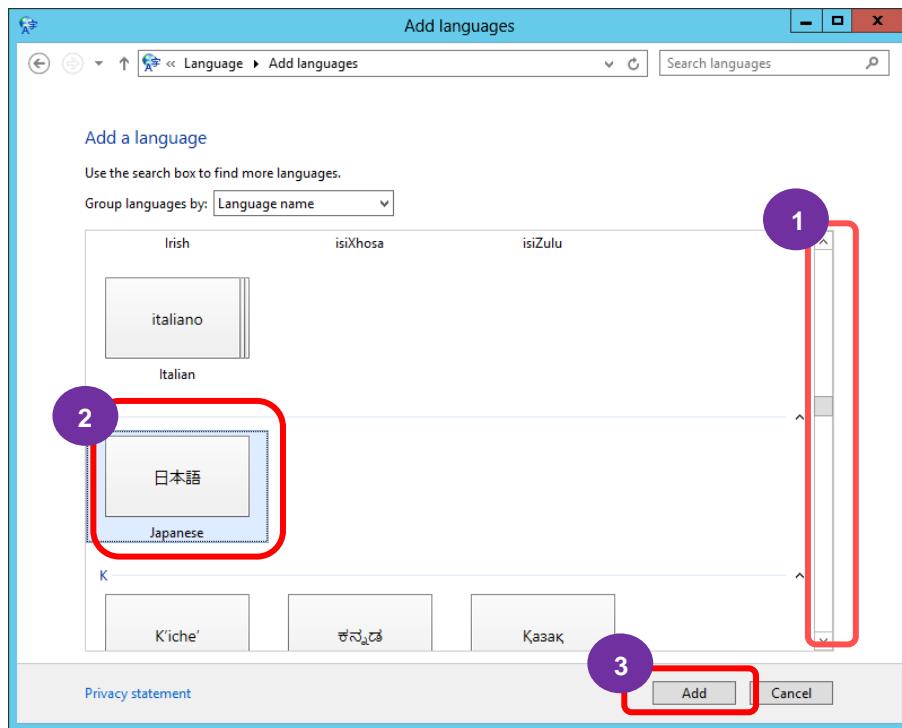


企業内システムと Microsoft Azure の VPN 接続、ファイルサーバー連携

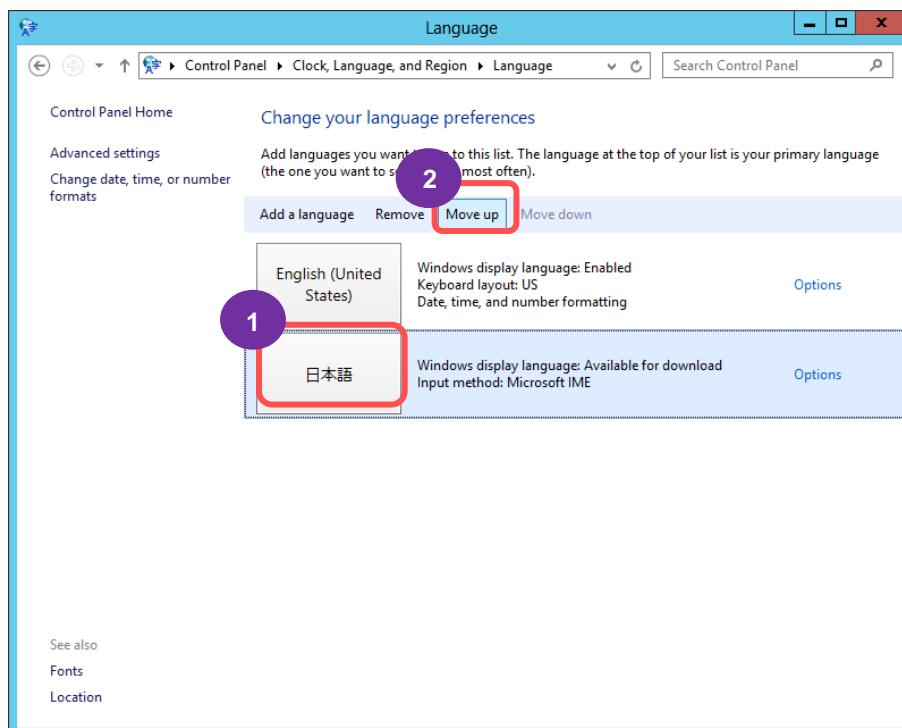
3. [Clock, Language, and Region]配下、[Add a language]をクリックします。**4. [Add a language]をクリックします。**

企業内システムと Microsoft Azure の VPN 接続、ファイルサーバー連携

5. 画面の右のスクロールバーを下にスクロールし[日本語]を選択し、[Add]をクリックします。

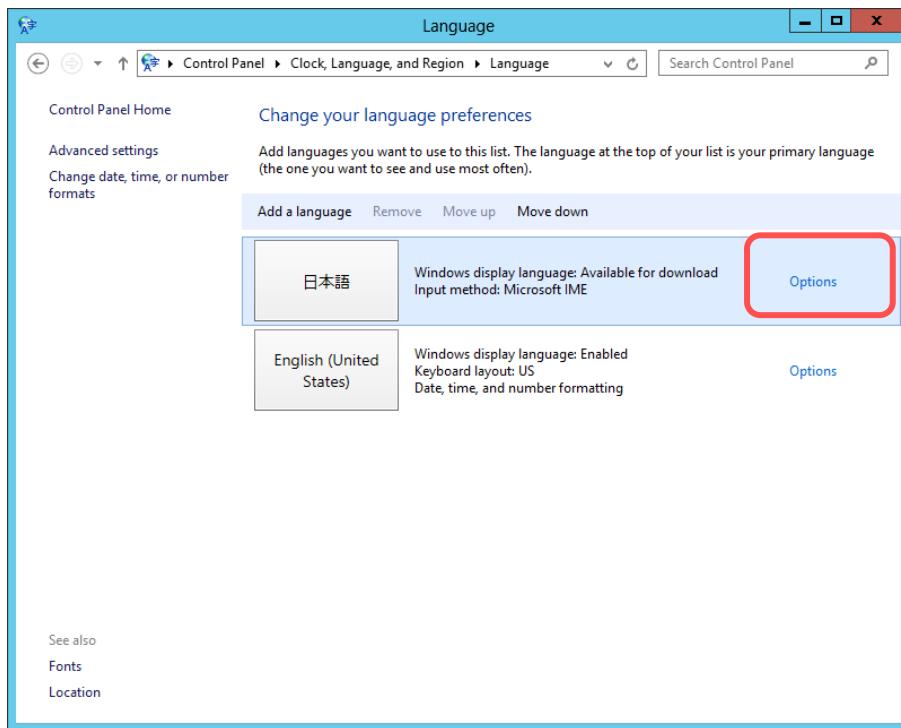


6. [日本語]を選択し[Move up]をクリックします。

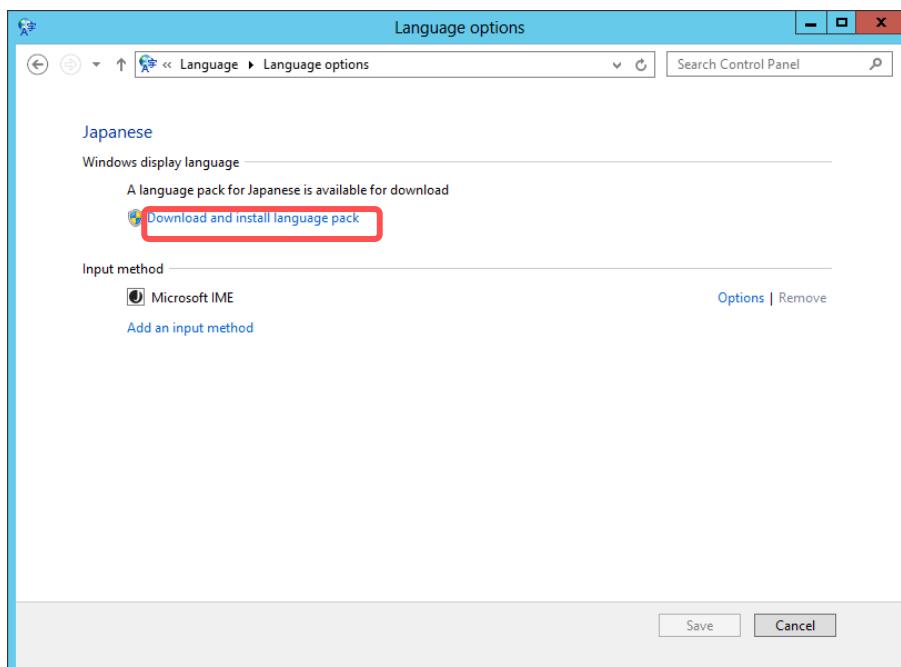


企業内システムと Microsoft Azure の VPN 接続、ファイルサーバー連携

7. [日本語]の[Options]をクリックします。

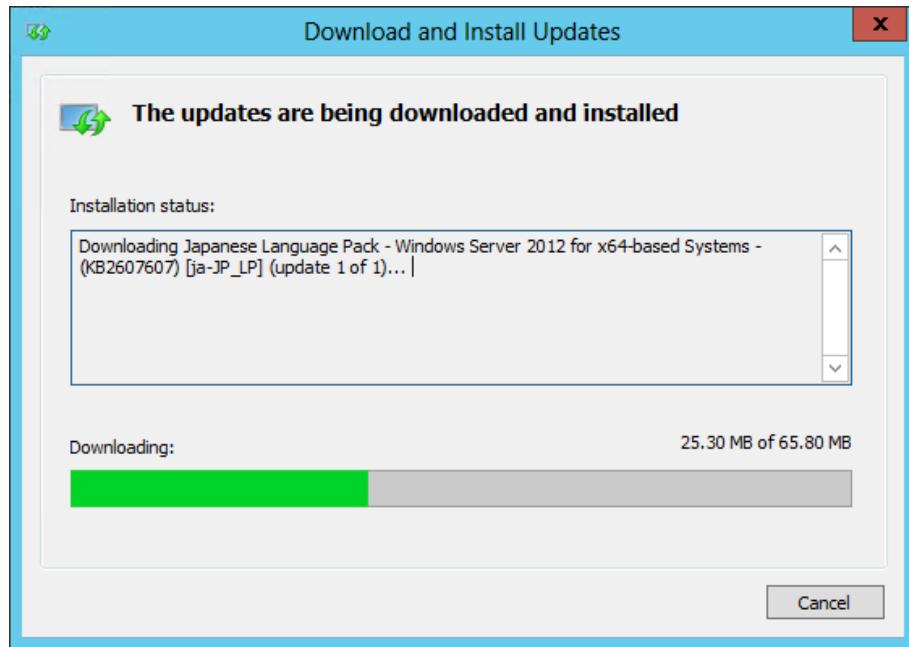


8. [Download and install language pack]をクリックします。

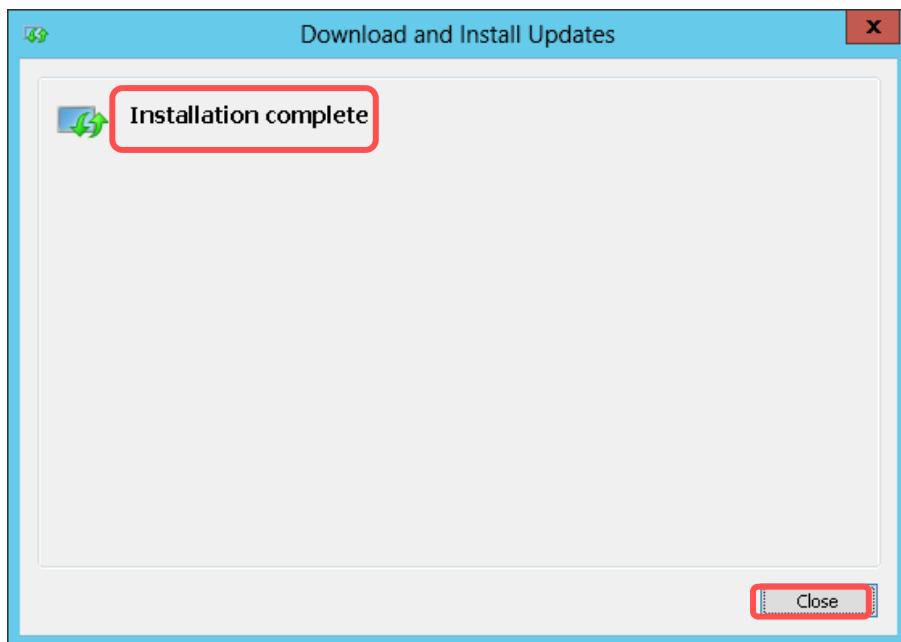


企業内システムと Microsoft Azure の VPN 接続、ファイルサーバー連携

9. インストールが完了するのを待ちます。環境にもよりますが 30 分程度かかります。



10. [Installation complete]画面が表示されたら、[Close]をクリックします。



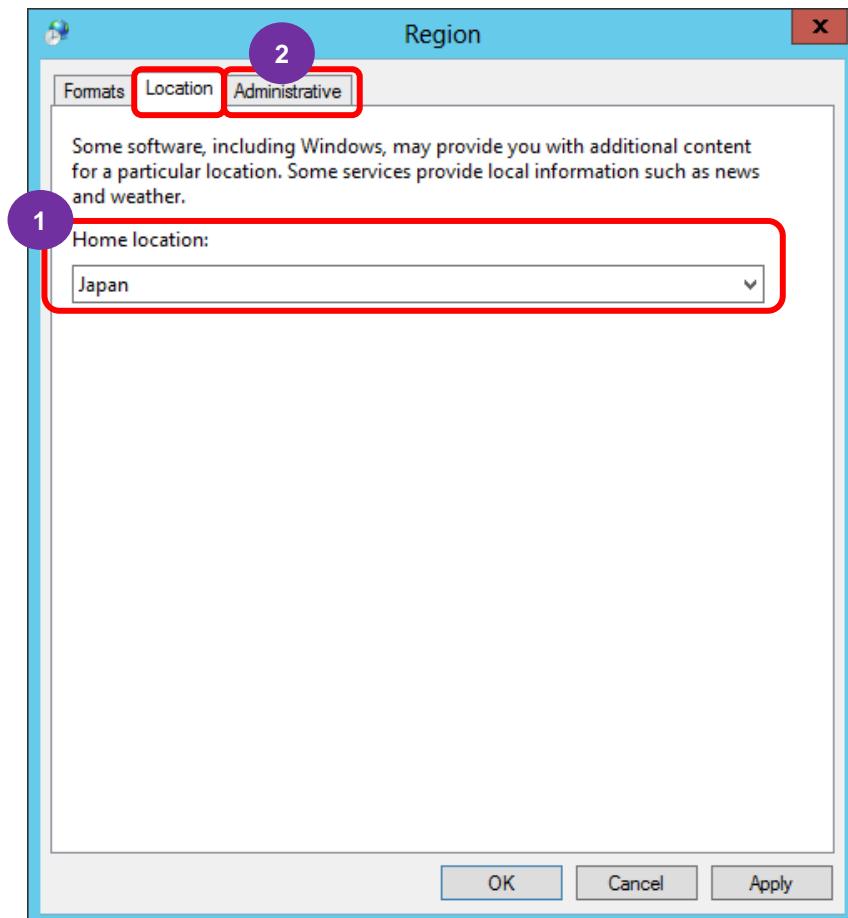
企業内システムと Microsoft Azure の VPN 接続、ファイルサーバー連携

11. 場所(Location)を変更し、サインイン画面の日本語化や PowerShell やコマンドプロンプトで日本語が使えるように設定を変更します。

[Language] ウィンドウの[Location]をクリックします。

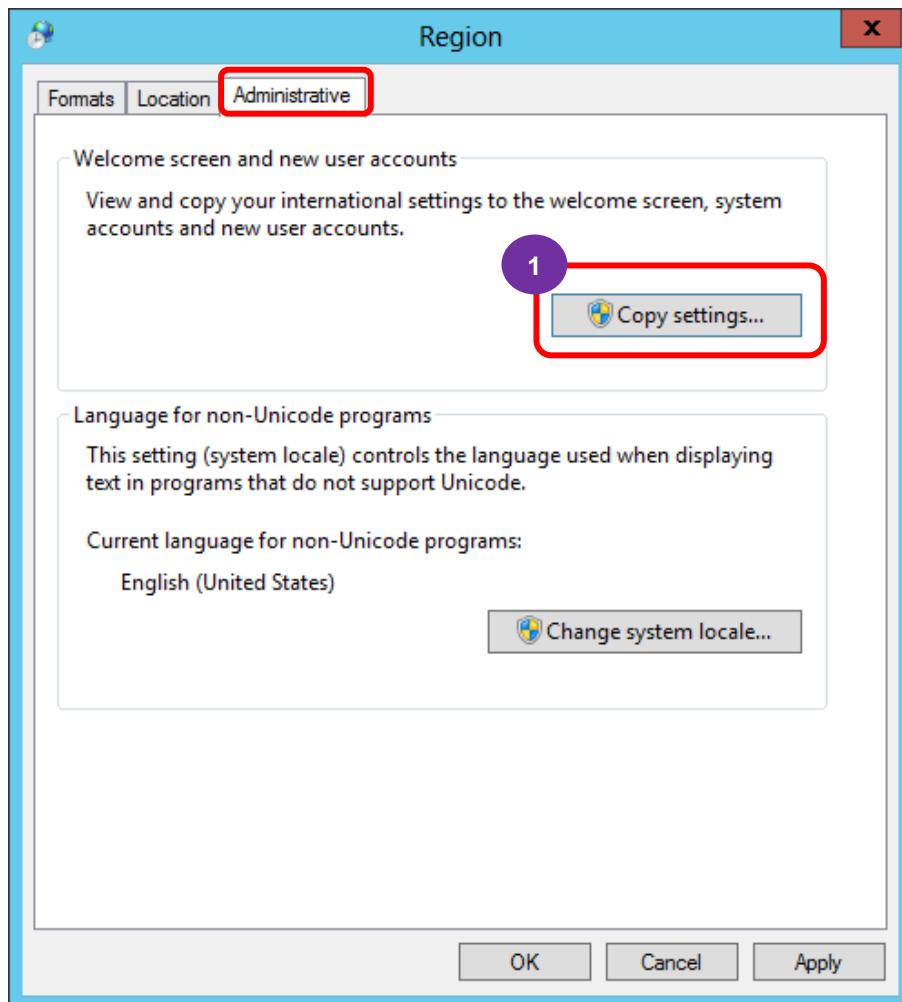


12. [Location]タブが表示されます。[Home location]のプルダウンメニューから「Japan」を選択し[Administrative]タブをクリックします。



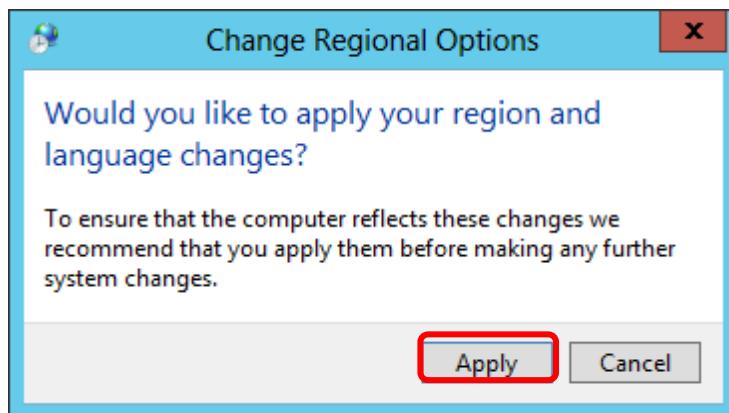
企業内システムと Microsoft Azure の VPN 接続、ファイルサーバー連携

13. [Administrative]タブが表示されるので、[Copy settings]をクリックします。



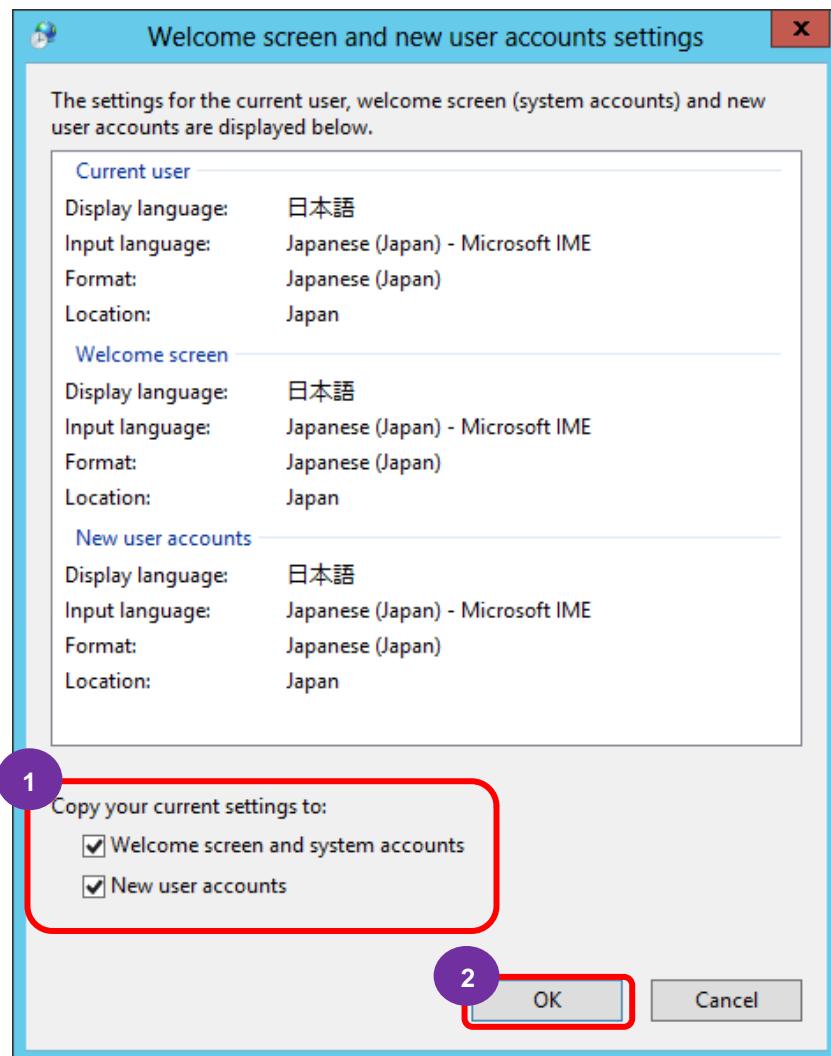
14. 場所と言語の変更を適用するか確認のウィンドウが開きます。

[Apply]をクリックします。



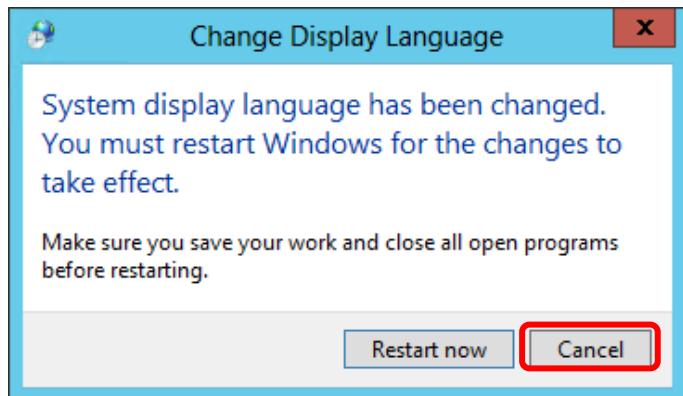
企業内システムと Microsoft Azure の VPN 接続、ファイルサーバー連携

15. 「Welcome screen and system accounts」(「ようこそ画面」の日本語化)と「New user accounts」(ユーザー追加時のデフォルト言語(及び場所)の日本語化)にチェックを付け[OK]をクリックします。

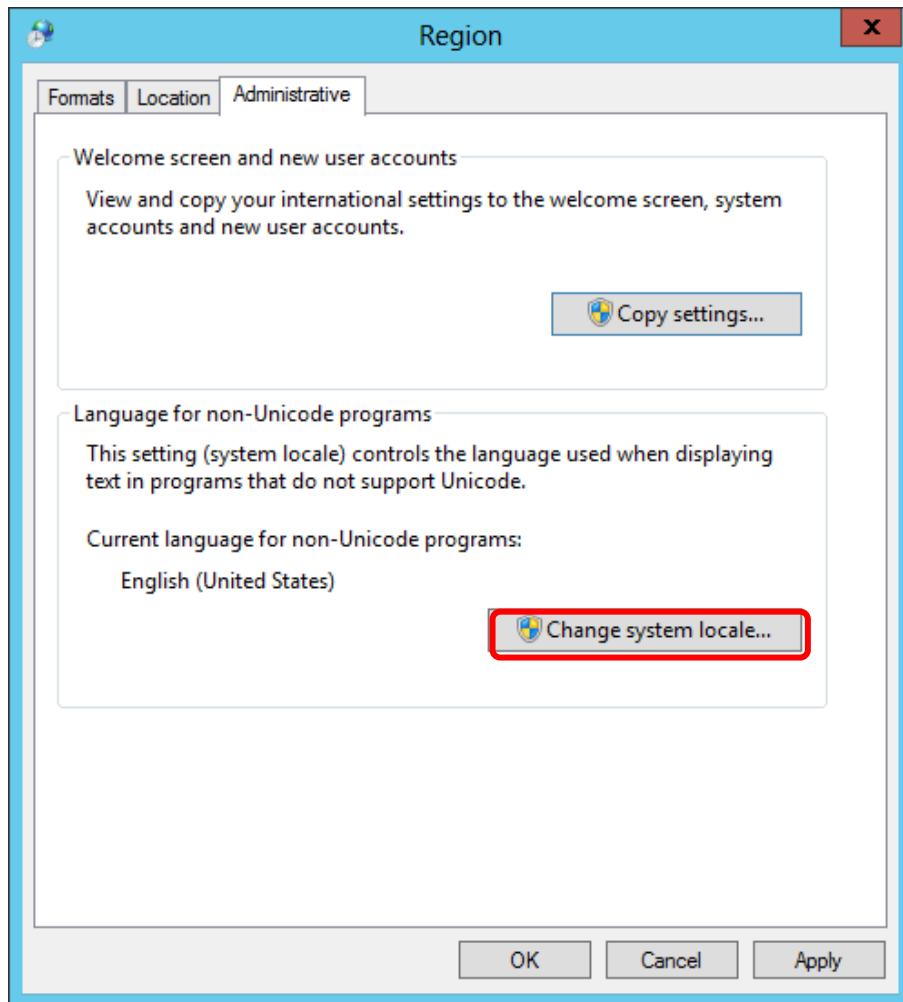


企業内システムと Microsoft Azure の VPN 接続、ファイルサーバー連携

16. 再起動を薦めるウィンドウが表示されますが、続けて作業を行うため「Cancel」をクリックします。

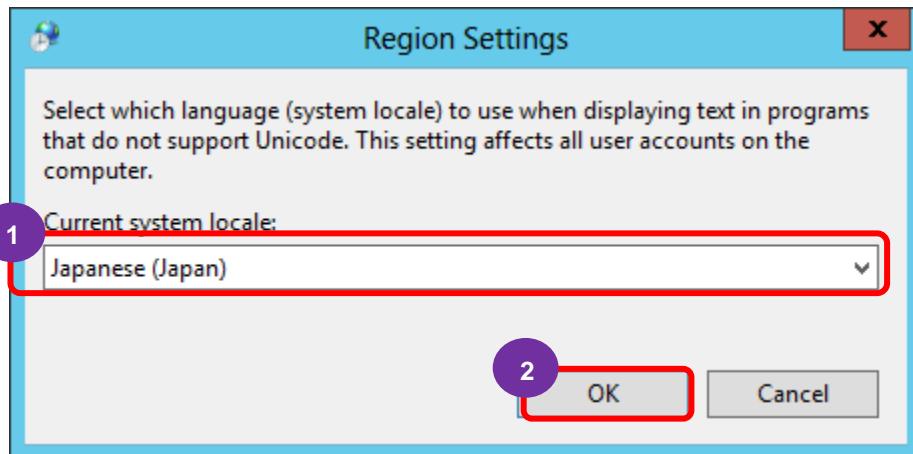


17. [Change system locale]をクリックします。

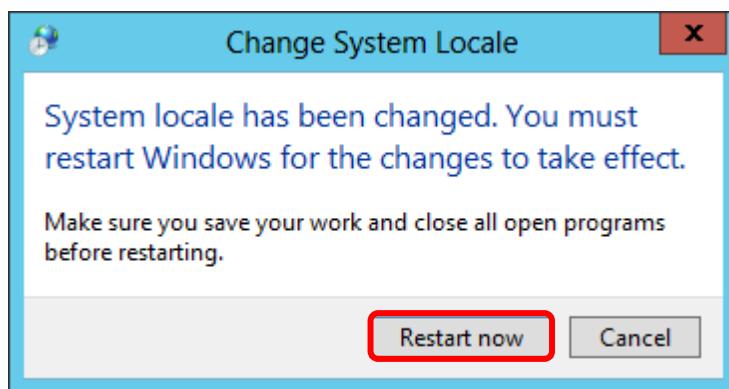


企業内システムと Microsoft Azure の VPN 接続、ファイルサーバー連携

18. [Current system locale:] のプルダウンメニューから「Japanese (Japan)」を選択し[OK]をクリックします。



19. 再起動を薦めるウィンドウが表示されます。[Restart now]をクリックします。



20. 再起動後 RDP で仮想マシンに接続しなおすと日本語が適用されます。



5.4 タイムゾーン

◆ タイムゾーンの設定

既定で世界標準時となっているためこれを日本時間に変更します。

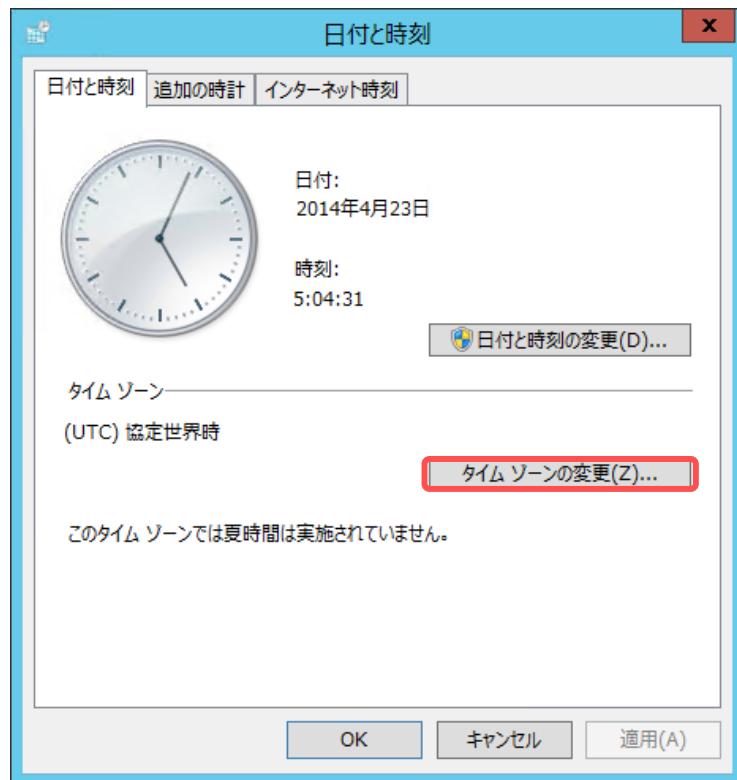
1. デスクトップ画面右下の時計をクリックします。



2. [日付と時刻の設定の変更]をクリックします。

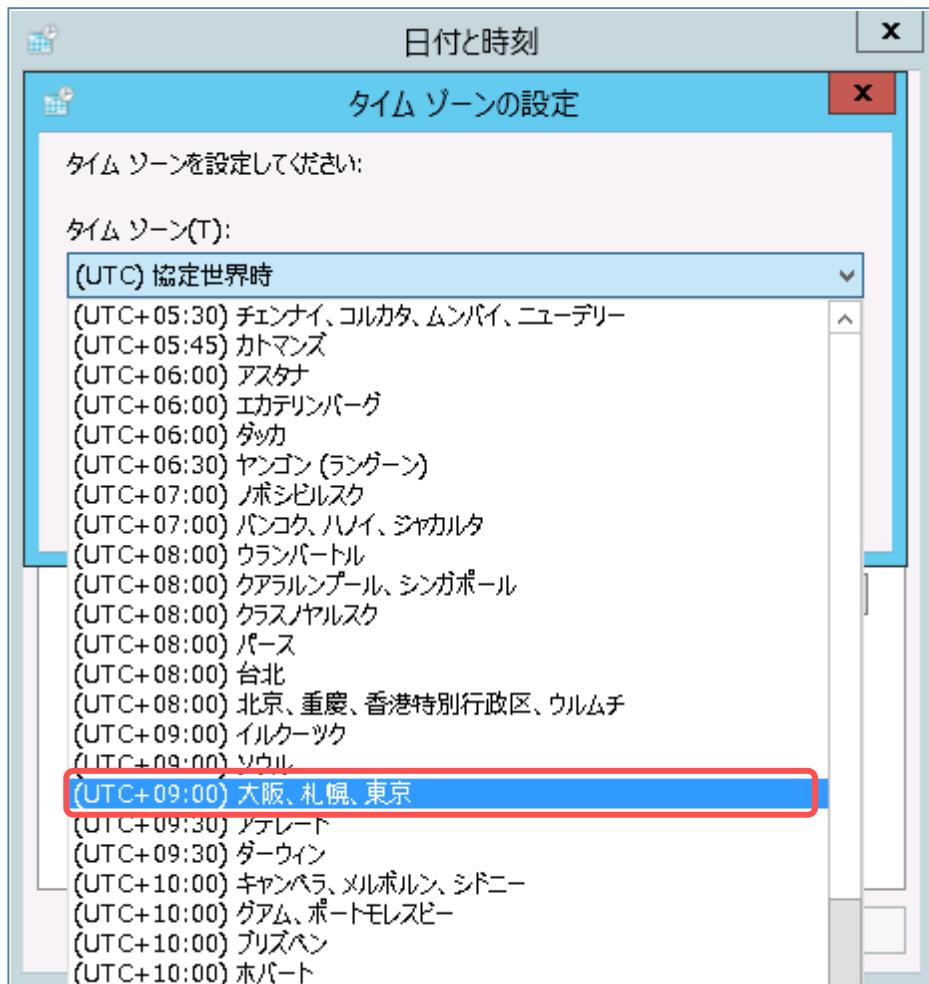


3. [タイムゾーンの変更]をクリックします。

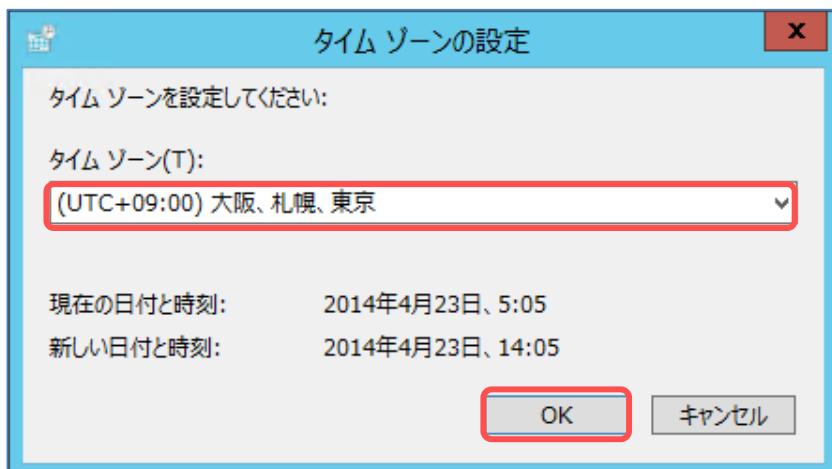


企業内システムと Microsoft Azure の VPN 接続、ファイルサーバー連携

4. [タイムゾーン]のプルダウンから[(UTC+9:00)大阪、札幌、東京]を選択し[OK]をクリックします。



5. タイムゾーンが変更されたことを確認して[OK]をクリックします。



5.5 Windows Update の設定

◆ Windows Update の設定

Windows Update を行い、サーバーを最新の状態にします。また、更新プログラムのインストール方法の選択では自社のセキュリティポリシーや運用形態などに合わせて設定します。本自習書では Windows Update が自動で実行されないように設定します。更新プログラムがインストールされると、システムの再起動を伴う場合があります。

1. デスクトップ画面左下の[サーバー マネージャー]をクリックします。

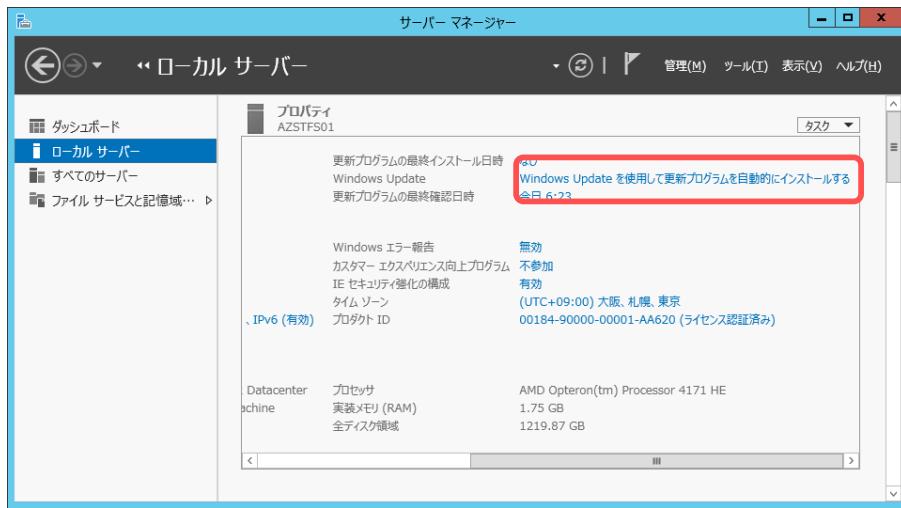


2. [ローカル サーバー]をクリックします。

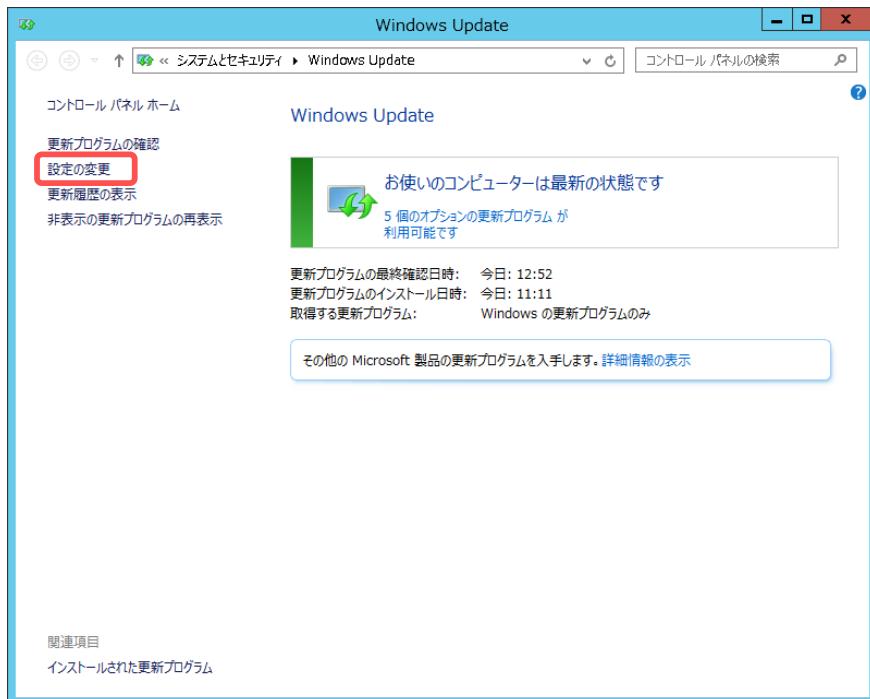


企業内システムと Microsoft Azure の VPN 接続、ファイルサーバー連携

3. 画面をスクロールし[Windows Update を使用して更新プログラムを自動的にインストールする]をクリックします。

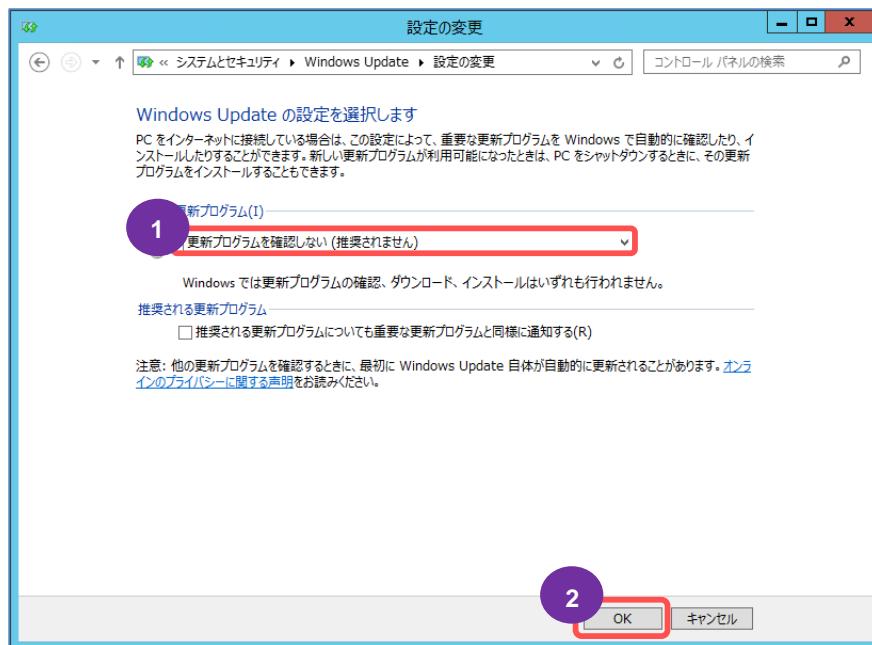


4. 更新プログラムがある場合にはインストール及び再起動後に、ない場合には[設定の変更]をクリックします。



企業内システムと Microsoft Azure の VPN 接続、ファイルサーバー連携

5. [重要な更新プログラム]のプルダウンから[更新プログラムを確認しない(推奨されません)]を選択し、[OK]をクリックします。



6. [更新プログラムを確認しない]になっていることを確認します。



Note : Windows Update について

なお、章の始めにも記載したとおり、この設定は Windows Update を行わないことを推奨するものではなく、意図しない再起動を抑止するための設定となります。サービスとして本運用を行う際には適宜アップデートを行うよう運用設計を行ってください。

5.6 ディスクを追加する

5.6.1 Azure 上での追加

→ Azure 管理ポータルでの作成と追加

Azure 管理ポータルにて BLOB ストレージの接続を行います。ファイルサーバーのデータを格納するために使用します。

1. ファイルサーバー仮想マシン(AZSTFS01)を選択し、[ディスクの接続]をクリックします。

新規にディスクを作成する場合は[空のディスクの接続]を選択します。

名前	状態	サブスクリプション	場所	DNS 名
AZSTADDS01	実行中	自習書	tokyo-ag (日本(東))	azstadds.cloudapp.jp
AZSTADDS02	実行中	自習書	tokyo-ag (日本(東))	azstadds.cloudapp.jp
AZSTADFS01	実行中	自習書	tokyo-ag (日本(東))	azstadfs.cloudapp.jp
AZSTADFS02	実行中	自習書	tokyo-ag (日本(東))	azstadfs.cloudapp.jp
AZSTDIRSYNC01	実行中	自習書	tokyo-ag (日本(東))	azstdirsync.cloudapp.jp
AZSTFS01	実行中	自習書 (シグマゴンサルティング)	tokyo-ag (日本(東))	azstfs01.cloudapp.jp
AZSTPROXY01	実行中	自習書	tokyo-ag (日本(東))	azstproxy.cloudapp.jp
AZSTPROXY02	実行中	自習書	tokyo-ag (日本(東))	azstproxy.cloudapp.jp

ディスクの接続
空のディスクの接続

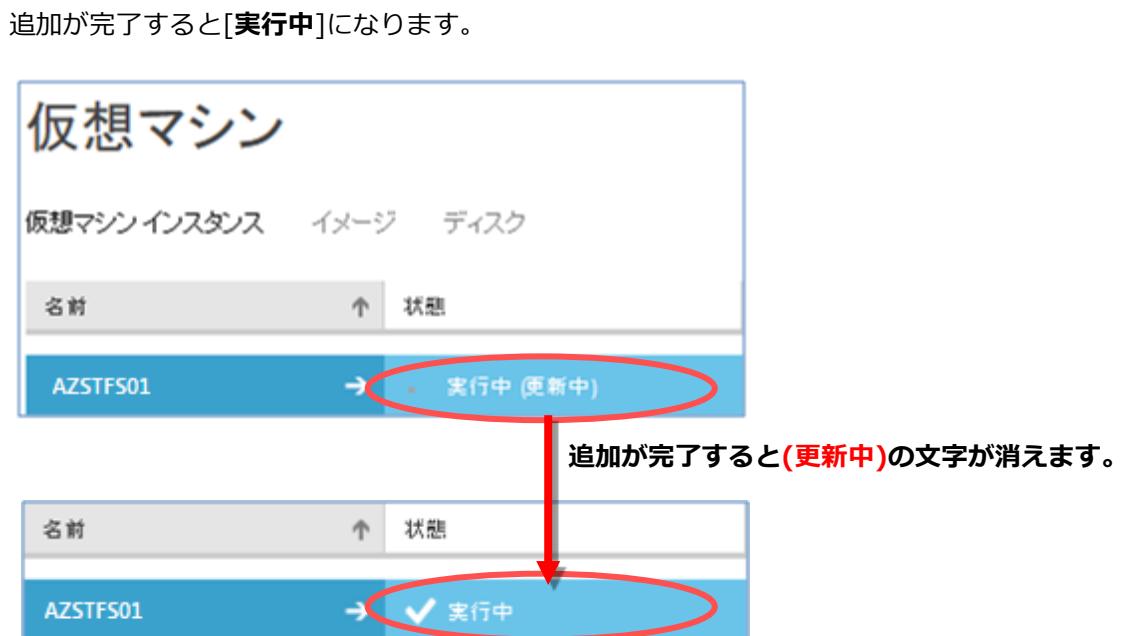
2. [サイズ(GB)]に「1023」を入力し、[ホスト キャッシュ機能]が「なし」になっていることを確認して「②」をクリックします。



項目	説明
仮想マシン名	・接続対象の仮想マシン名が表示されます。
ストレージの場所	・接続するストレージ(VHD ファイル)を格納する場所を指定します。 自動で入力されます。
ファイル名	・VHD ファイル名を入力します。 自動で入力されます。
サイズ(GB)	・1~1023 の間で選択します。 なお、ディスクは一度小さく設定すると後からサイズを変更することが出来ません。一旦、大きく取り、仮想マシン上でパーティションを設定するなどして使用することを推奨いたします。
ホストキャッシュ設定	・以下の 3つから選択します。
なし	・ホストキャッシュ機能を使用しません。 AD DS のデータベースや SQL データベースなど書き込みの整合性確保が必要なデータを扱う場合に有効です。
読み取り専用	・データの読み取りのみキャッシュ機能を使用します。
読み取り/書き込み	・データの読み込み書き込みにキャッシュ機能を使用します。 キャッシュ機能により、データの書き込み読み込みの処理が速くなります BUT、障害等によりディスクに書き込めない状態が発生した場合、キャッシュ上のデータを損失します。

企業内システムと Microsoft Azure の VPN 接続、ファイルサーバー連携

3. ディスクの作成と追加が始まると対象の仮想マシンの状態が[実行中(更新中)]になります。



5.6.2 仮想サーバー上での追加とフォーマット

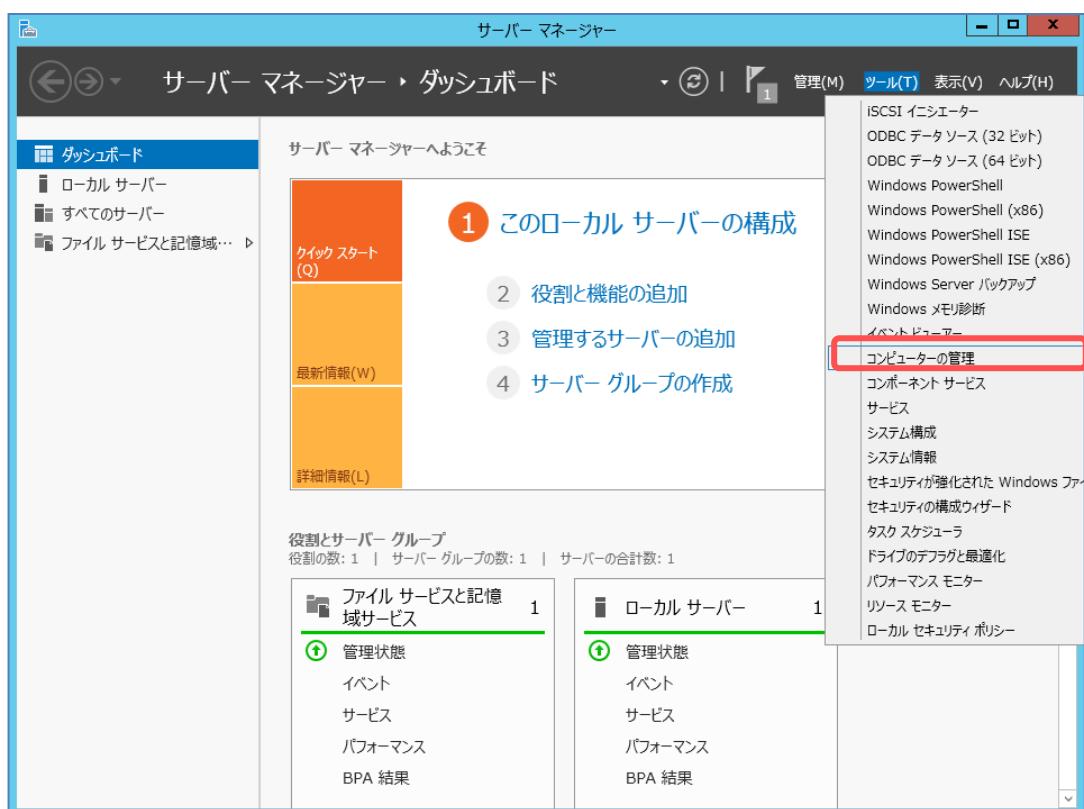
→ 仮想サーバー上でのディスク追加とフォーマット

Azure 上の仮想サーバー上でのディスク追加とフォーマットを行います。

1. デスクトップ画面左下の[サーバー マネージャー]をクリックします。



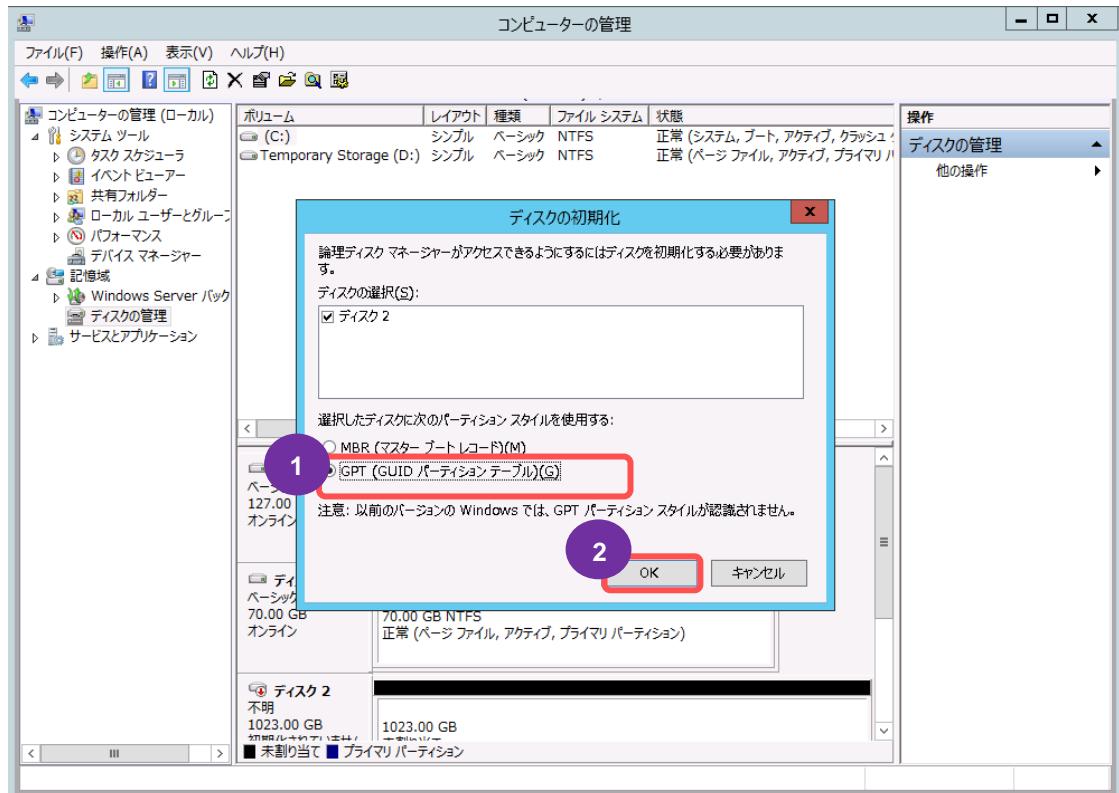
2. [ツール]→[コンピューターの管理]を選択します。



企業内システムと Microsoft Azure の VPN 接続、ファイルサーバー連携

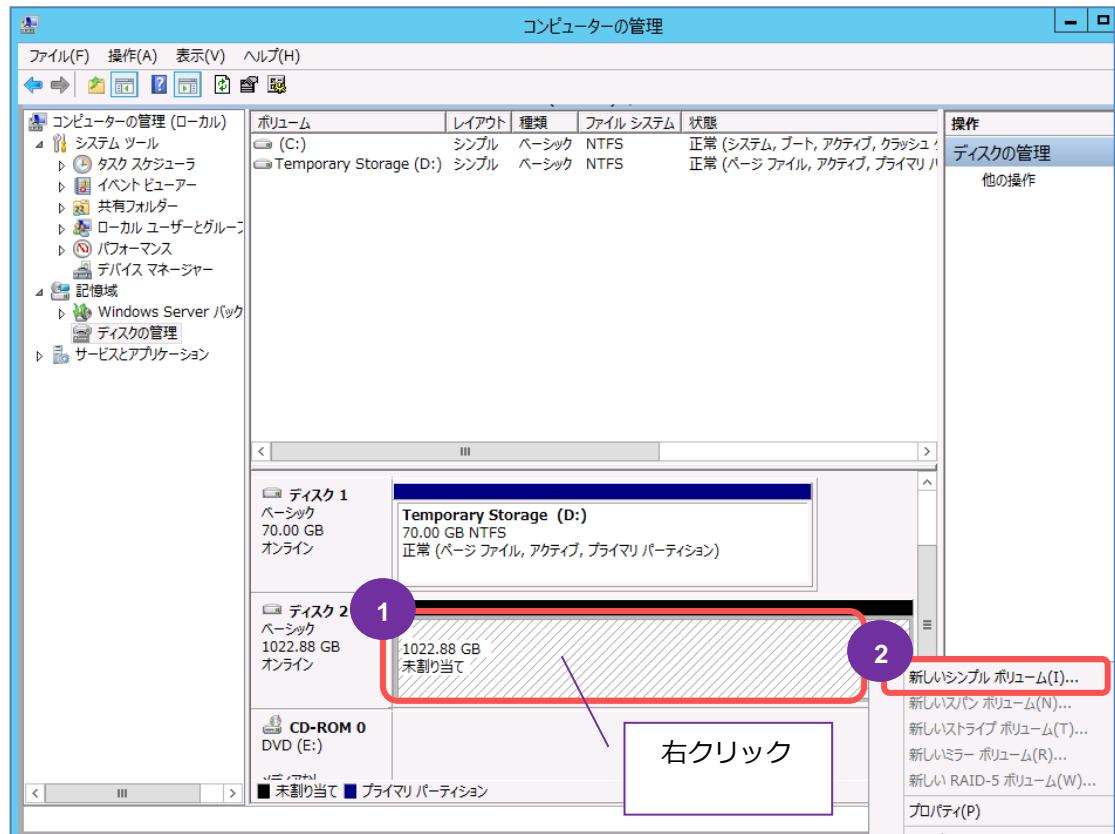
3. [ディスクの初期化]画面が表示されます。

選択したディスクに[GPT(GUID パーティションテーブル)]パーティションスタイルを使用し、[OK]をクリックします。

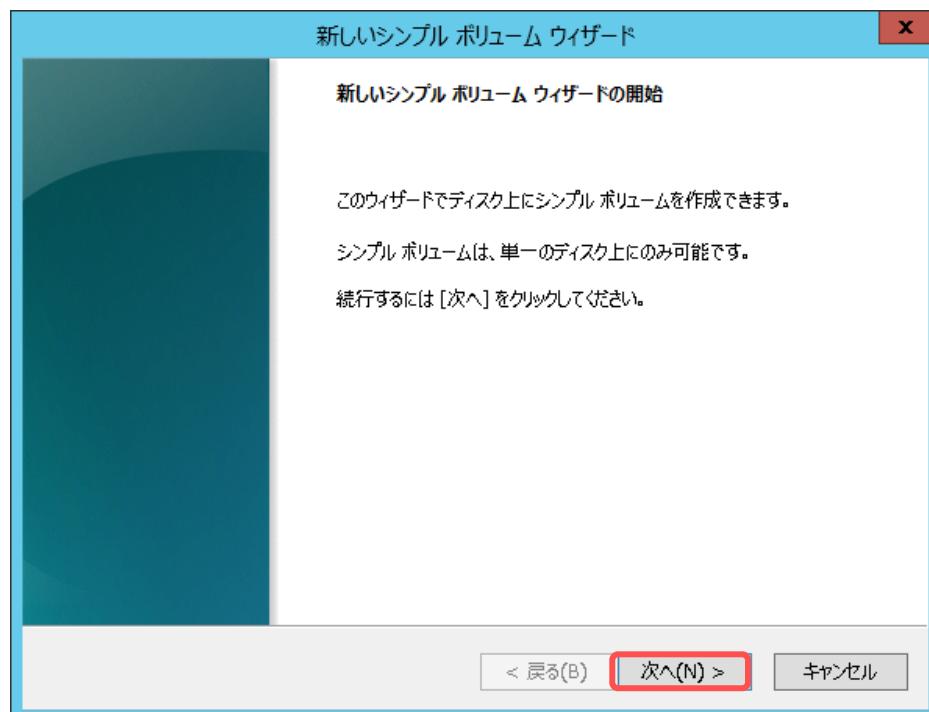


企業内システムと Microsoft Azure の VPN 接続、ファイルサーバー連携

4. 初期化したディスクの[未割り当て]となっている箇所(黒帯で表示されている箇所)を右クリックし「新しいシンプルボリューム」を選択します。

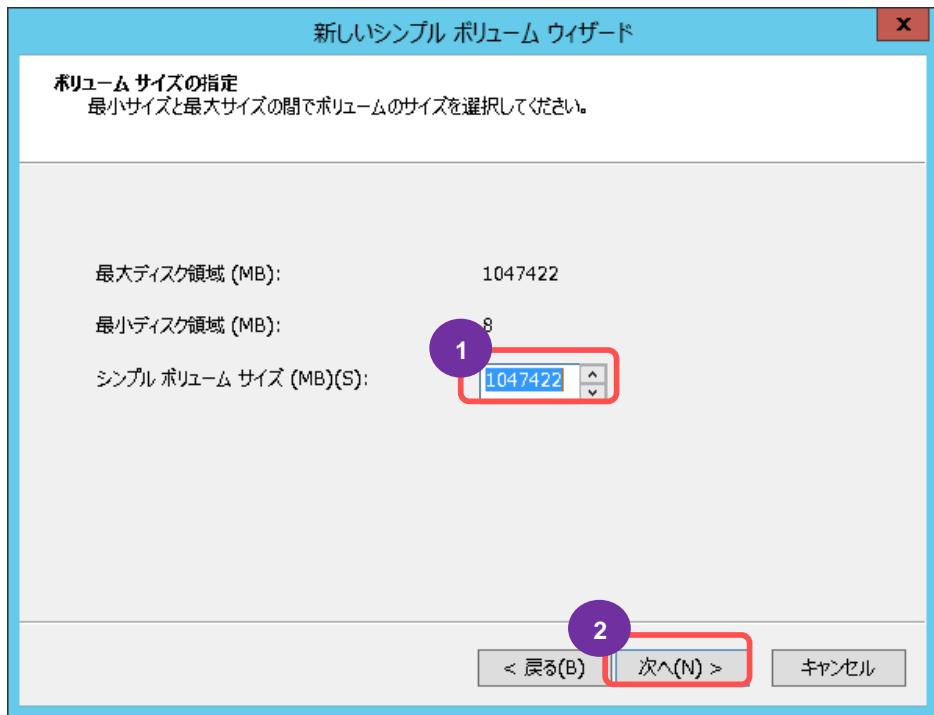


5. [新しいシンプルボリュームウィザード]画面が表示されますので、[次へ]をクリックします。

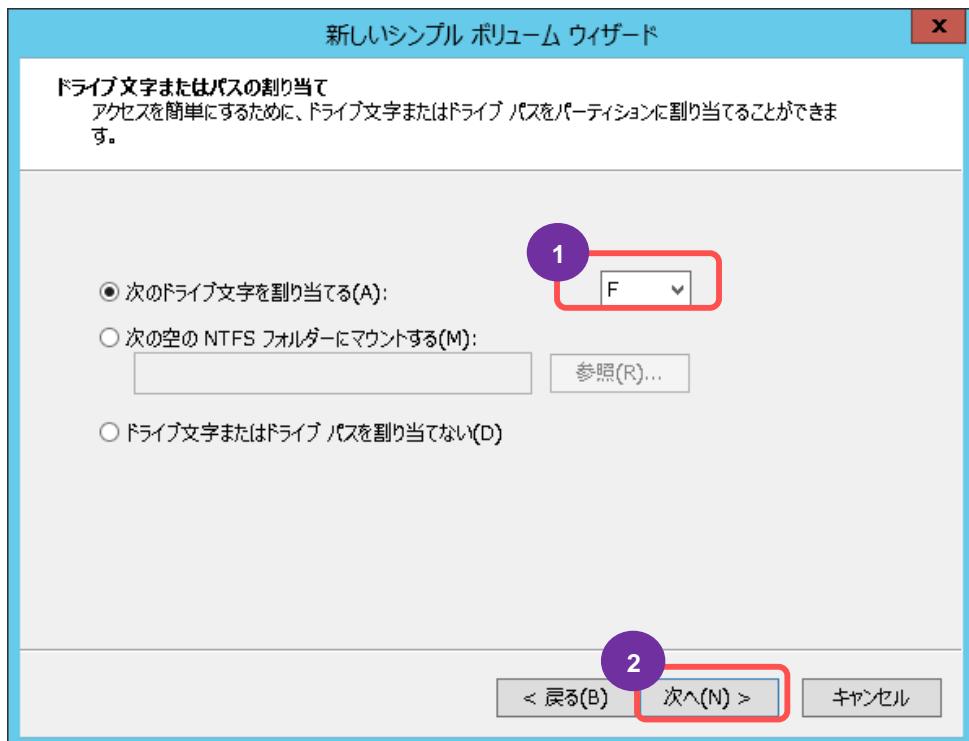


企業内システムと Microsoft Azure の VPN 接続、ファイルサーバー連携

6. [ボリューム サイズの指定]では、シンプルボリュームサイズが最大ディスク領域になっているのを確認し[次へ]ボタンをクリックします。



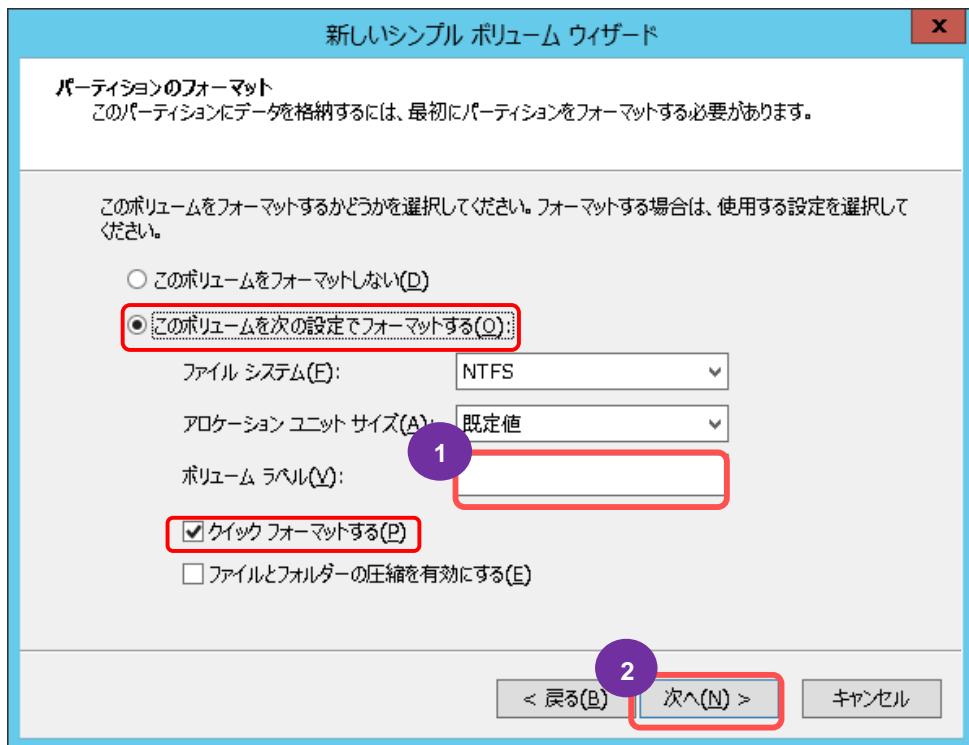
7. [ドライブ文字またはパスの割り当て]では、[次のドライブに割り当てる]にチェックが入っているのを確認し[次へ]ボタンをクリックします。(本例ではマシン上に既に C・D・E ドライブが存在していますので F ドライブに割り当てられています。)



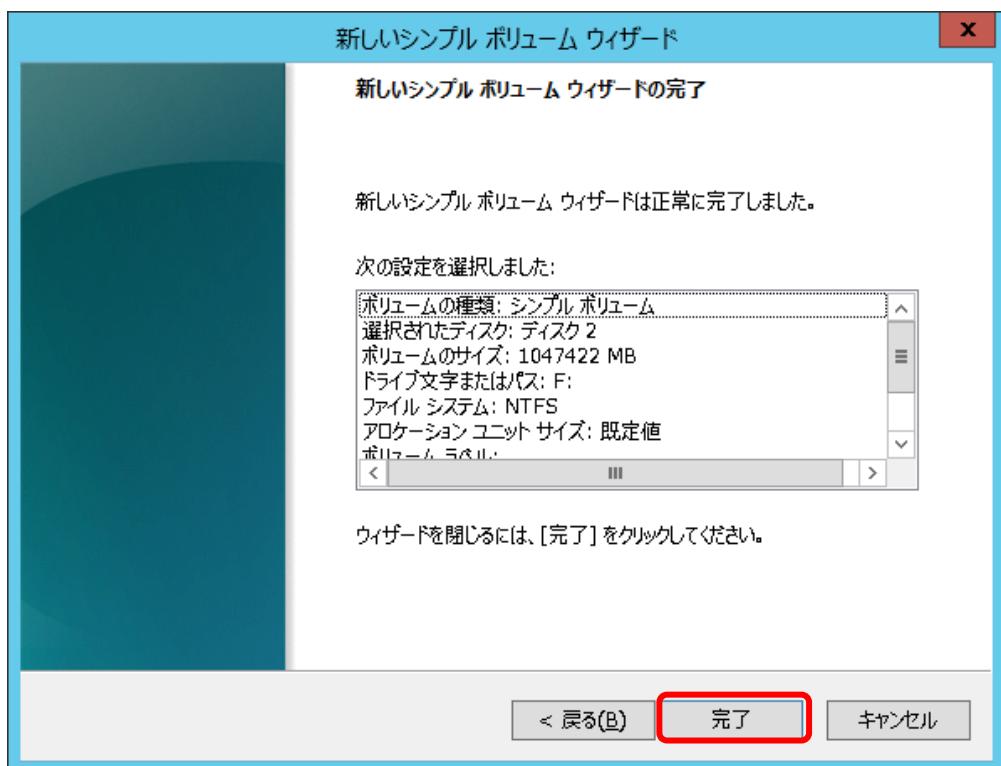
企業内システムと Microsoft Azure の VPN 接続、ファイルサーバー連携

8. [このボリュームを次の設定でフォーマットする]と[クイックフォーマットする]にチェックが入っているのを確認し[次へ]ボタンをクリックします。

今回は[ボリュームラベル]に何も入れません。

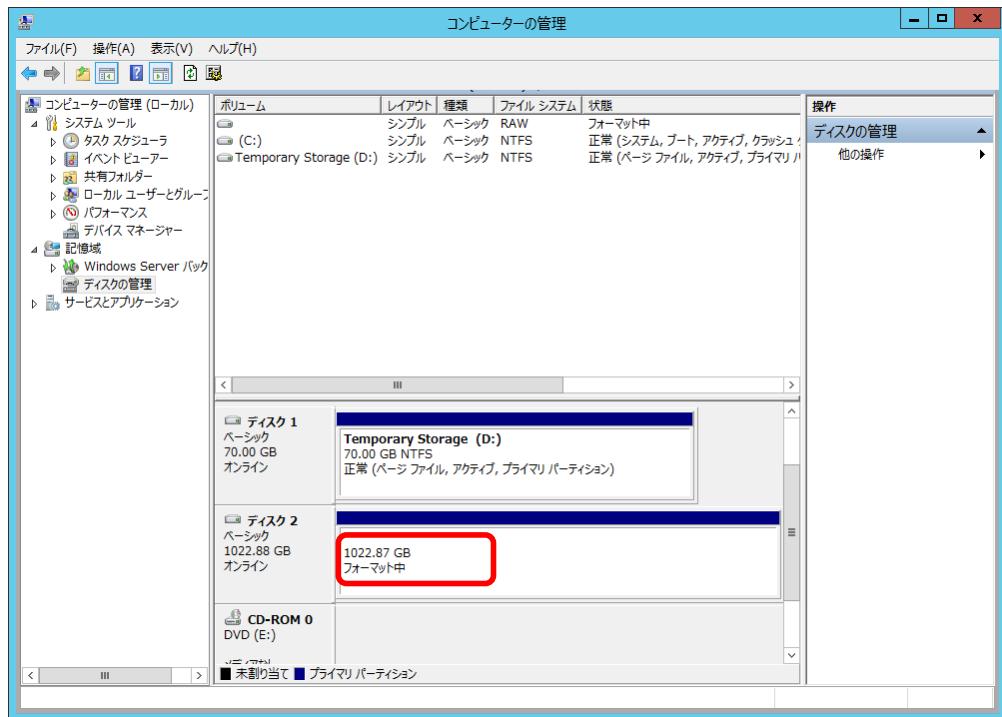


9. [新しいシンプルボリュームウィザード]を[完了]します。

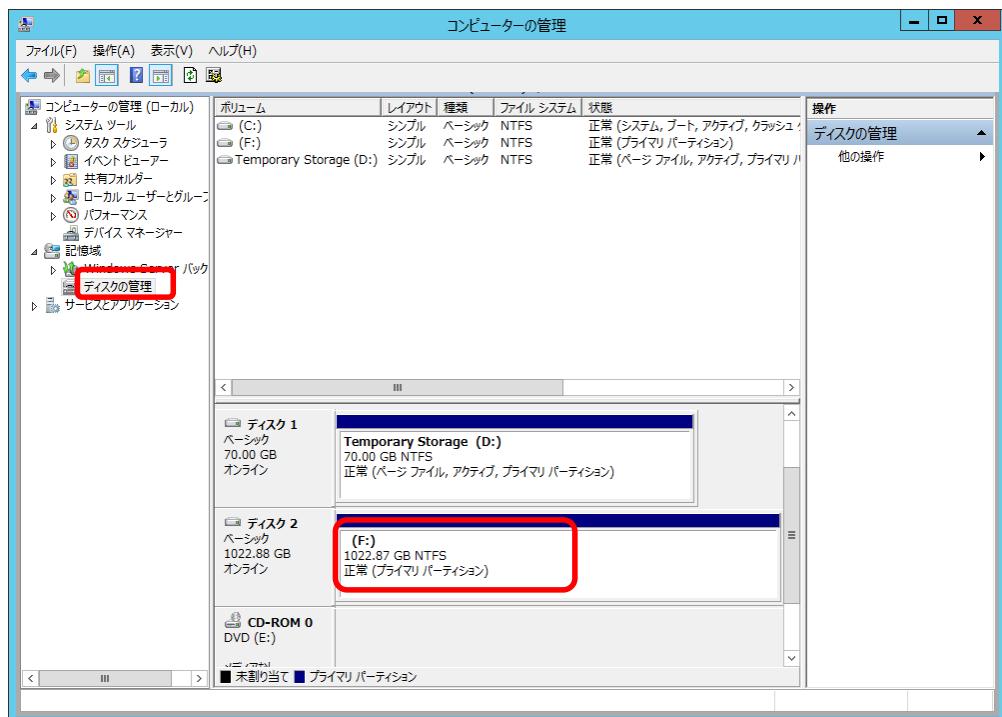


企業内システムと Microsoft Azure の VPN 接続、ファイルサーバー連携

10. ディスクの管理画面で[フォーマット中]の表示になります。フォーマットが完了するまでしばらく待ちます。



11. フォーマットが完了すると[正常]と表示されドライブとして認識されます。[コンピューターの管理]画面を閉じて完了します。



5.7 ユーザーとグループを作成する

5.7.1 ユーザーの作成

→ ユーザーの追加

Azure 上のファイルサーバーにユーザーを追加します。

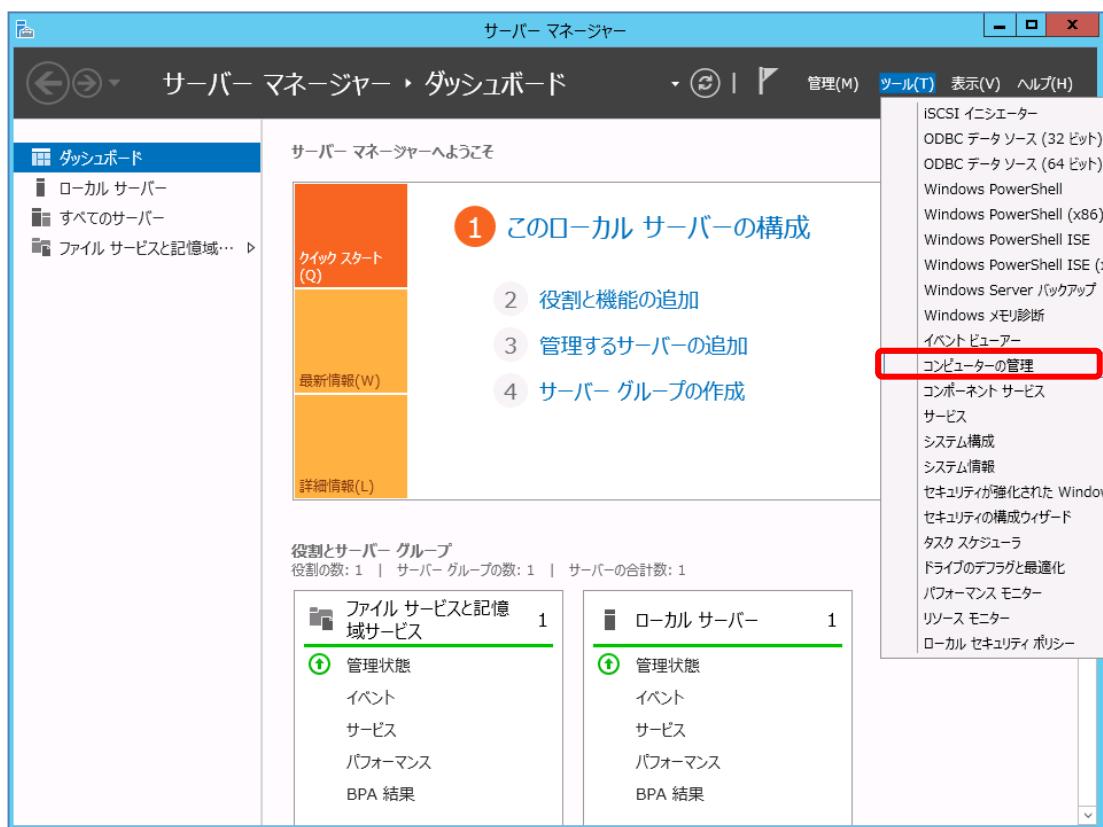
本自習書では以下のユーザーを作成します。

ユーザー名
localuser01
localuser02

1. デスクトップ画面左下の[サーバー マネージャー]をクリックします。

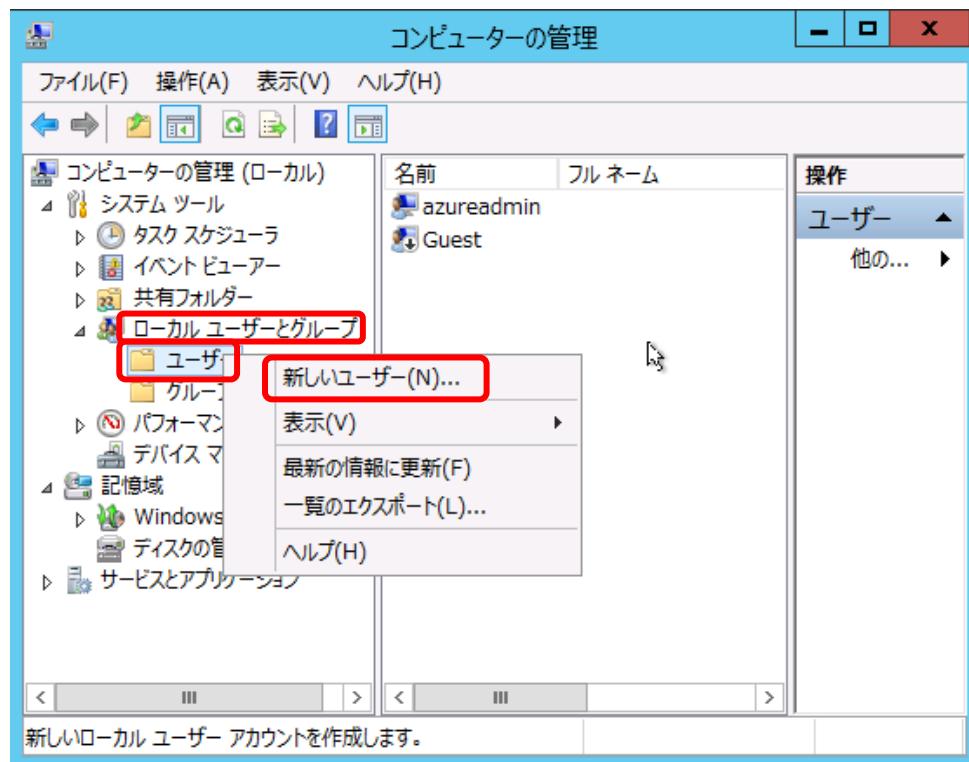


2. [ツール]→[コンピューターの管理]を選択します。



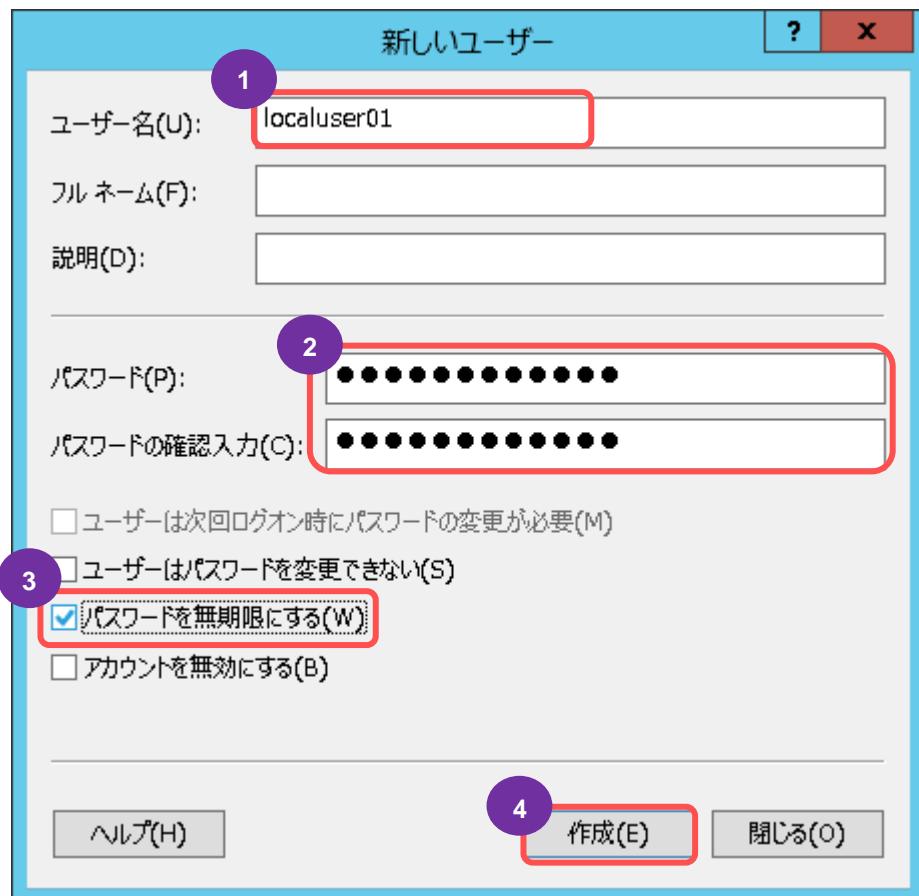
企業内システムと Microsoft Azure の VPN 接続、ファイルサーバー連携

3. [ローカルユーザーとグループ]→[ユーザー]右クリックのメニューで[新しいユーザー]をクリックします。



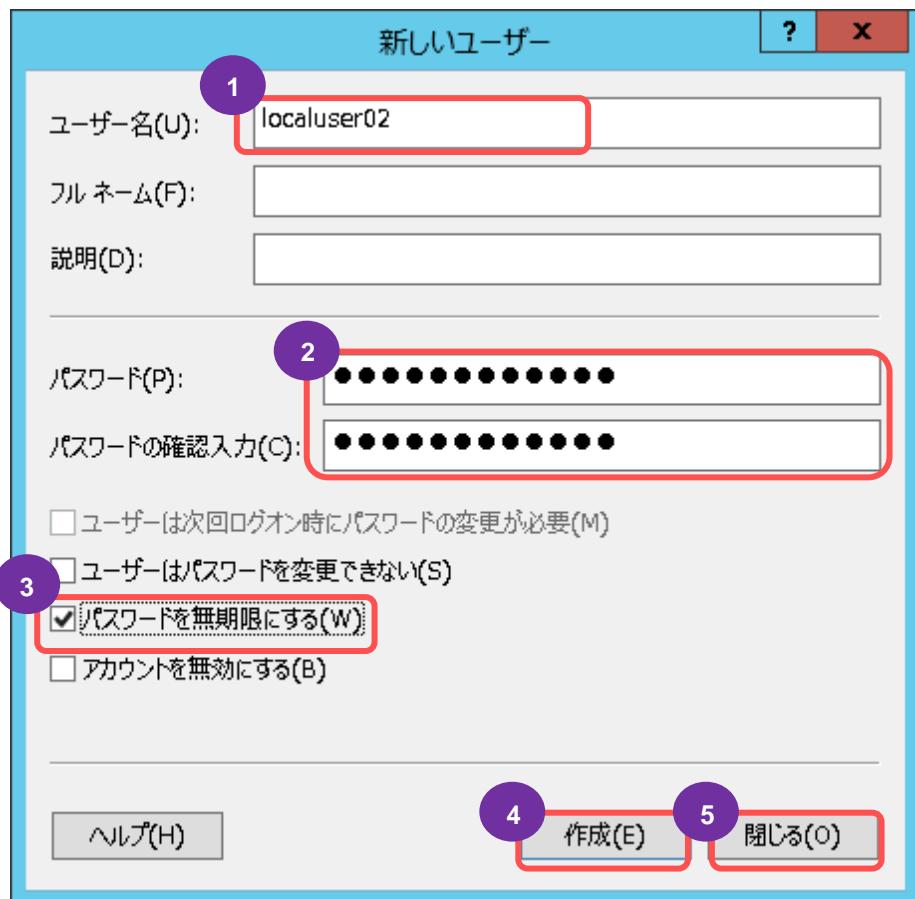
企業内システムと Microsoft Azure の VPN 接続、ファイルサーバー連携

4. [新しいユーザー]ボックスに「localuser01」とパスワードを入力し、[作成]をクリックします。本自習書では[パスワードを無期限にする]に団を入れます。

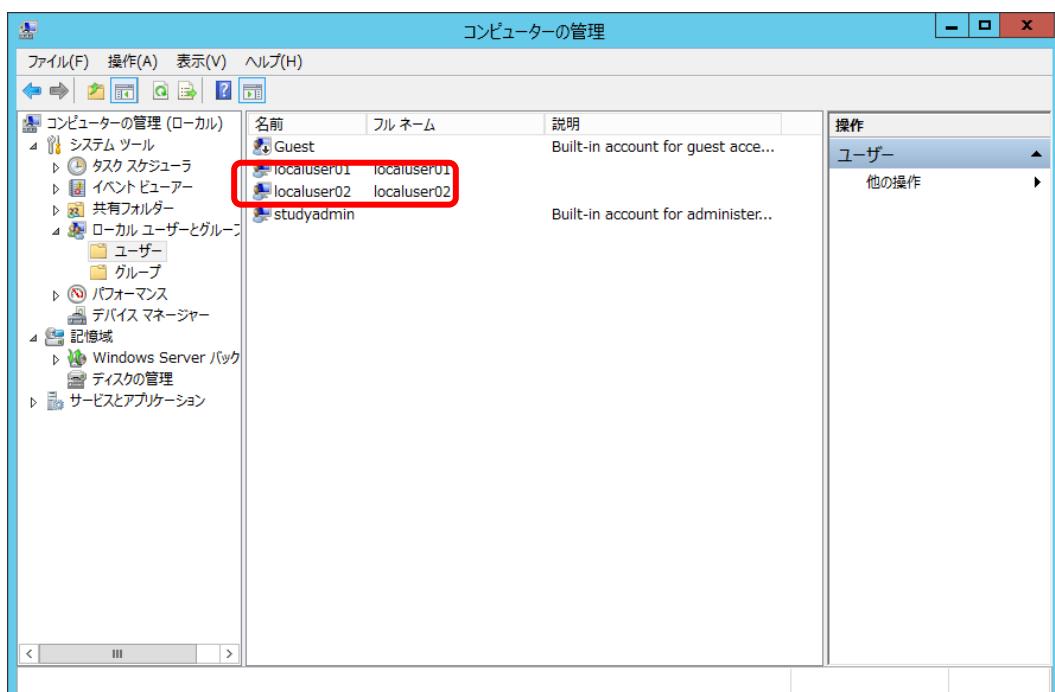


企業内システムと Microsoft Azure の VPN 接続、ファイルサーバー連携

5. 引き続き、ユーザー名「localuser02」とパスワードを入力し、[作成]、[閉じる]順にクリックします。本自習書では[パスワードを無期限にする]に☑を入れます。



6. 新しい作成したユーザーが存在することを確認します。



5.8.2 グループの作成

→ グループの追加

Azure 上のファイルサーバーにグループを追加します。

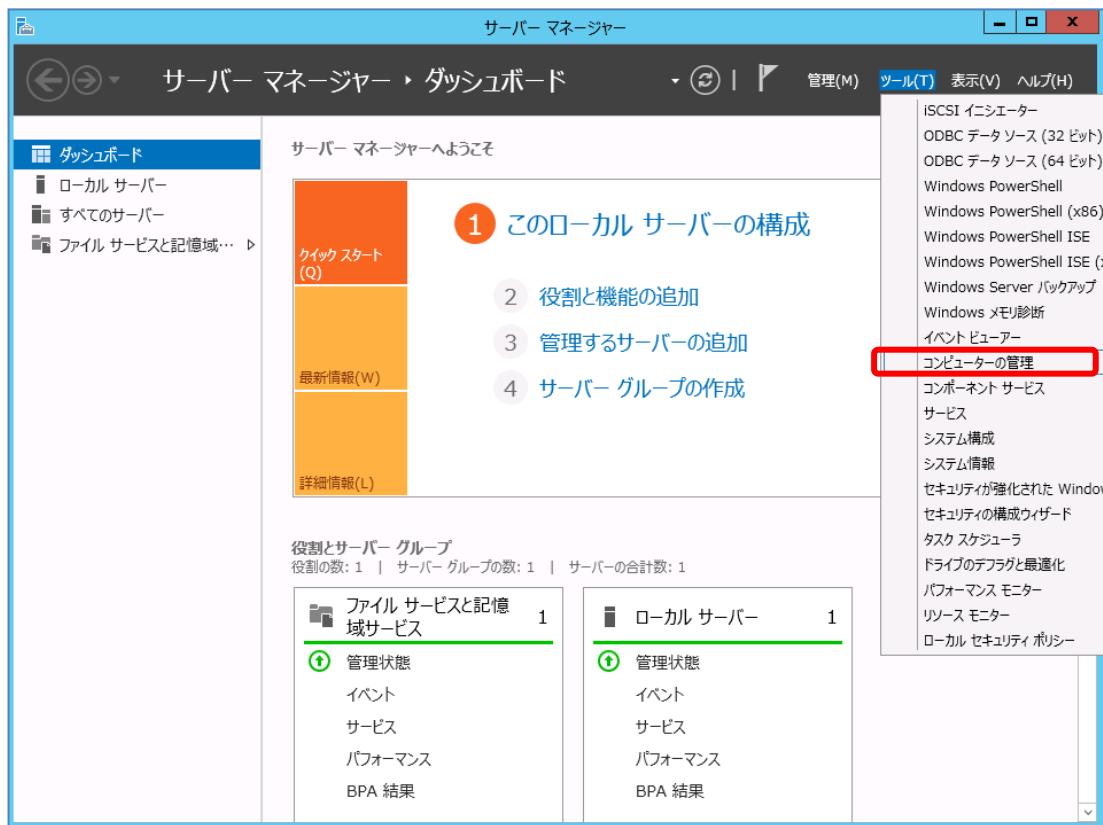
本自習書では以下のユーザーを作成します。

グループ名
localgroup01

1. デスクトップ画面左下の[サーバー マネージャー]をクリックします。

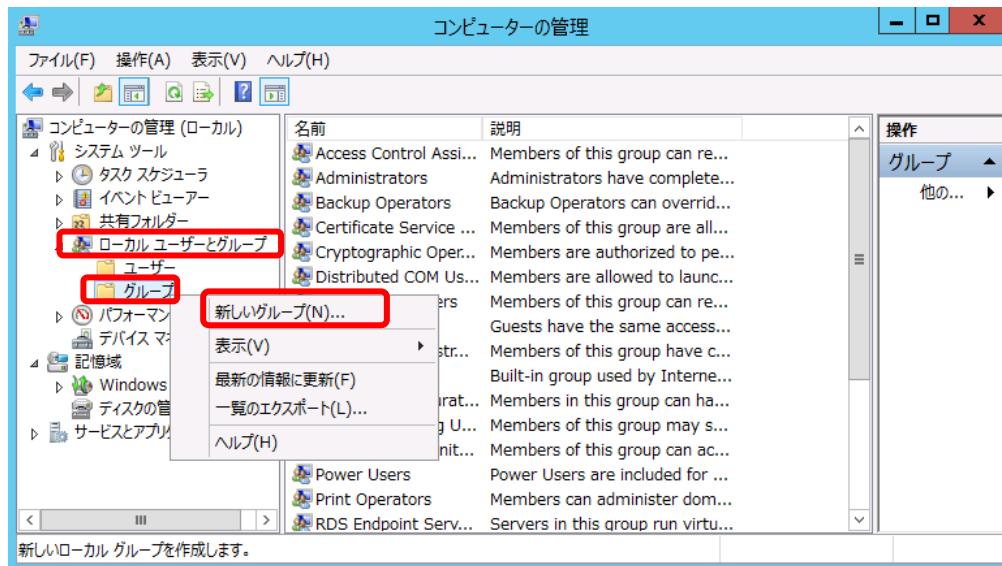


2. [ツール]→[コンピューターの管理]を選択します。

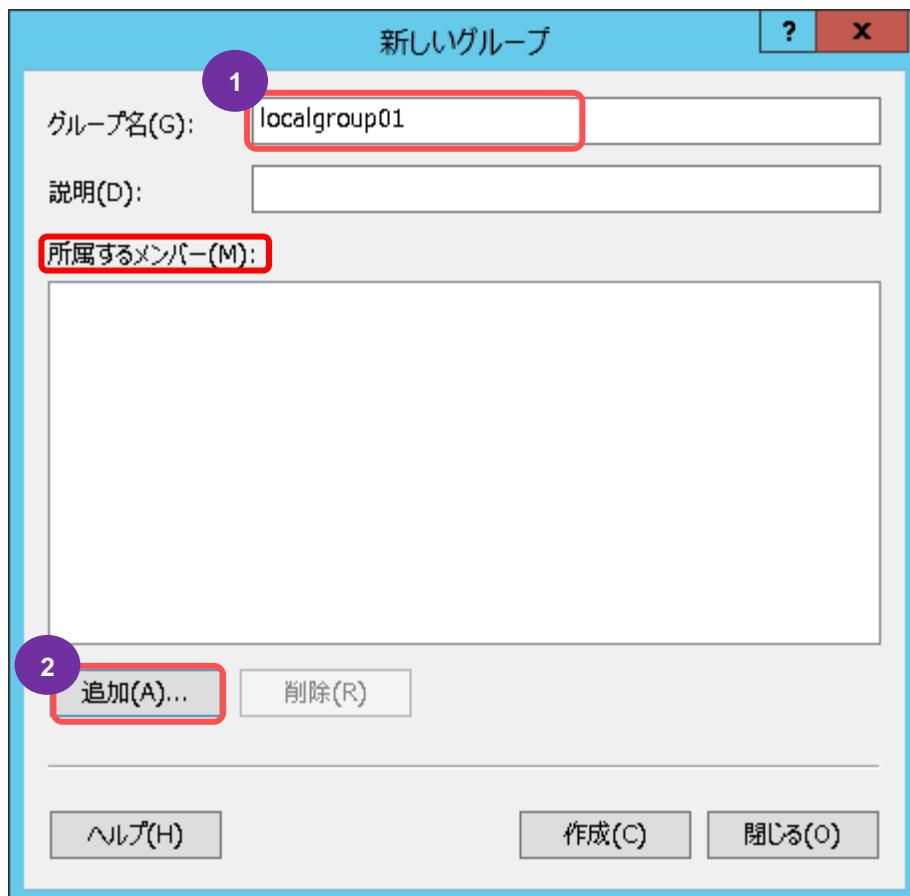


企業内システムと Microsoft Azure の VPN 接続、ファイルサーバー連携

3. [ローカルユーザーとグループ]→[グループ]右クリックメニューで[新しいグループ]を選択します。

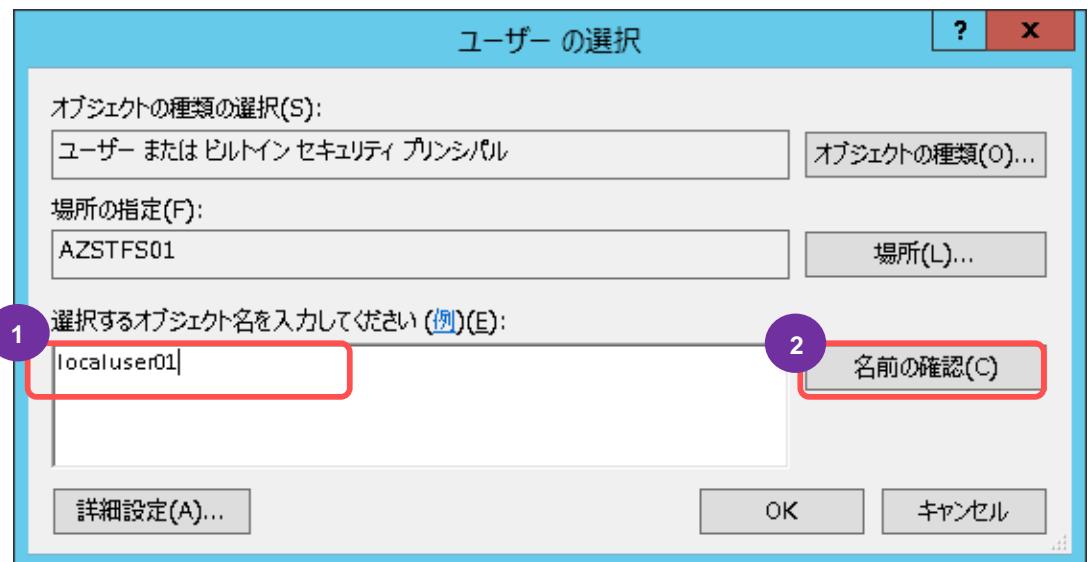


4. [新しいグループ]ボックスに「localgroup01」を入力します。[所属するメンバー]で[追加]をクリックします。

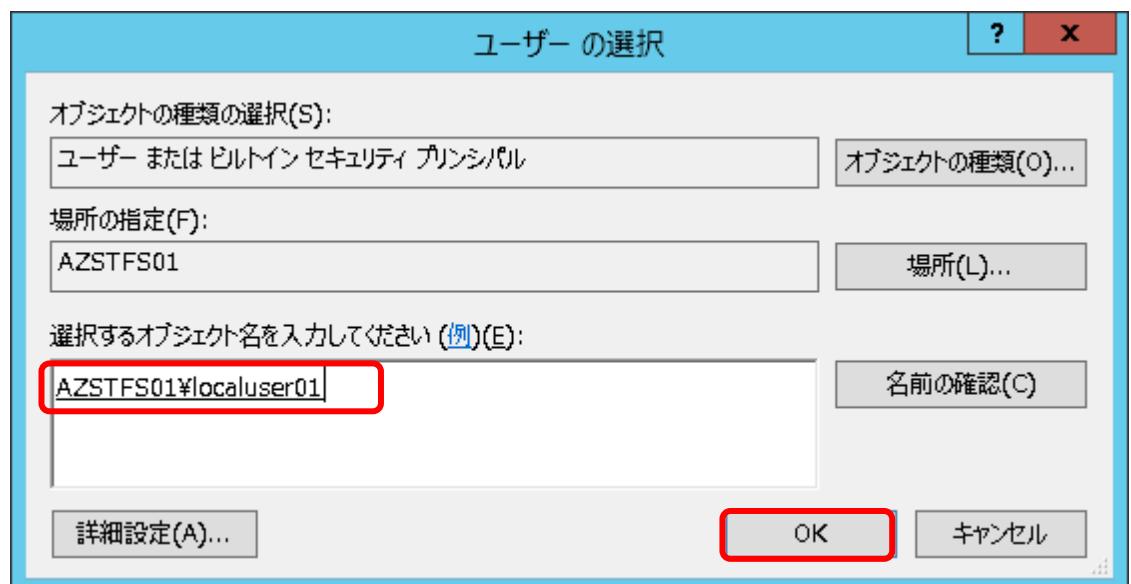


企業内システムと Microsoft Azure の VPN 接続、ファイルサーバー連携

5. [選択するオブジェクト名を入力してください]画面で「localuser01」を入力し、[名前の確認]をクリックします。



6. [選択するオブジェクト名を入力してください]画面に「AZSTFS01¥localuser01」に表示されたら、[OK]をクリックします。



企業内システムと Microsoft Azure の VPN 接続、ファイルサーバー連携

7. ユーザー名、「localuser02」も上記 5~6 と同じように「localgroup01」に所属させます。

8. グループ名、「localgroup01」に所属するメンバー画面に以下ユーザーが追加されていることを確認し、[作成]、[閉じる]順にクリックします。



STEP 6. Microsoft Azure 上にファイルサーバーを導入する

この STEP では、Azure 上にファイルサーバーを導入するための手順について説明します。

この STEP では、次のことを学習します。

- ✓ ファイルサーバーの構成
- ✓ 共有フォルダーの作成
- ✓ アクセス権の設定
- ✓ ネットワーク共有

6.1 ファイルサーバーの構成

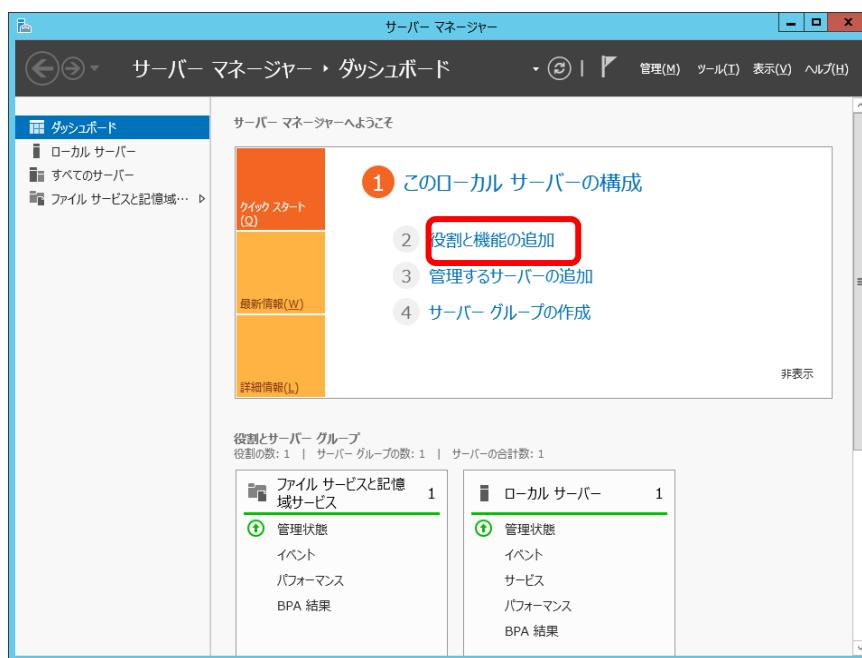
◆ 役割と機能の追加

役割および機能の追加ウィザードを使用して役割、役割サービス、および機能をインストールします。

1. デスクトップ画面左下の[サーバー マネージャー]をクリックします。

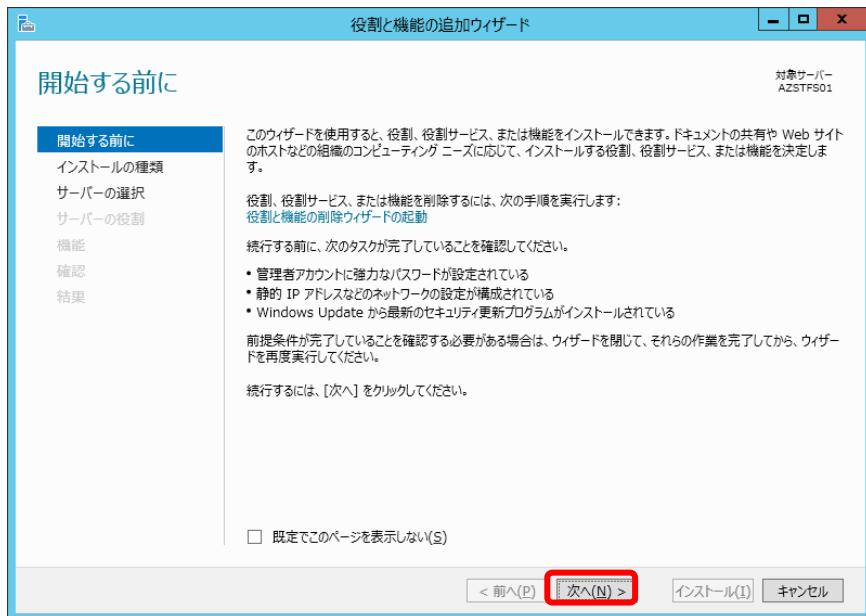


2. ダッシュボードの[②役割と機能の追加]をクリックします。

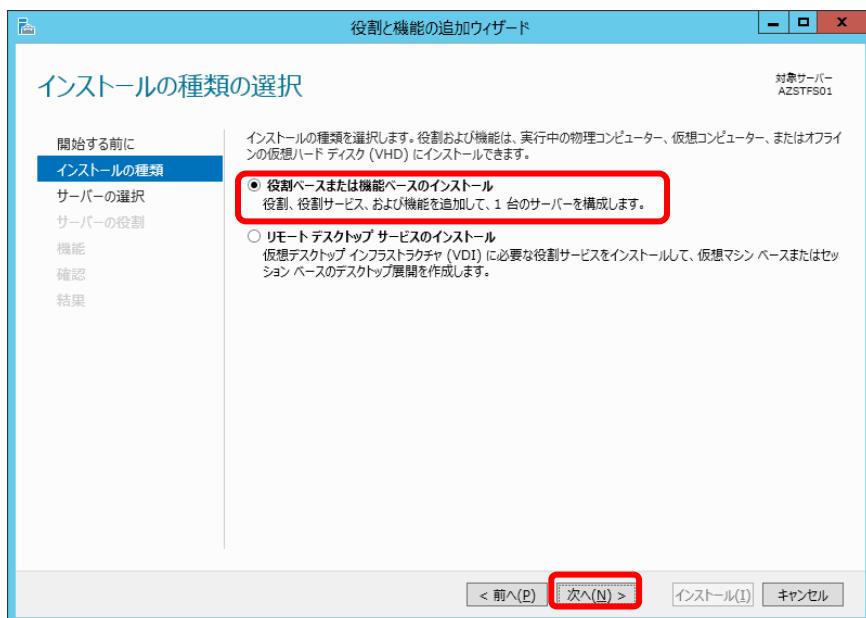


企業内システムと Microsoft Azure の VPN 接続、ファイルサーバー連携

3. [開始する前に] ページで、インストールする役割と機能のために、対象サーバーとネットワーク環境の準備が整っていることを確認してください。[次へ] をクリックします。

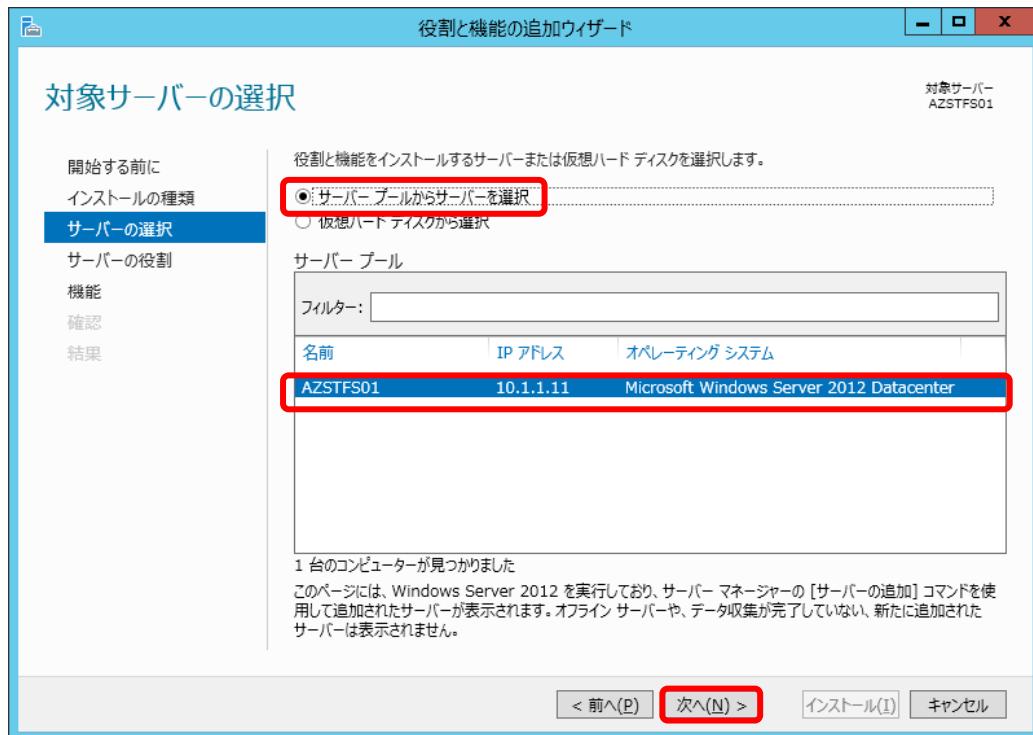


4. [インストールの種類の選択] ページで、[役割ベースまたは機能ベースのインストール] を選択して[次へ] をクリックします。

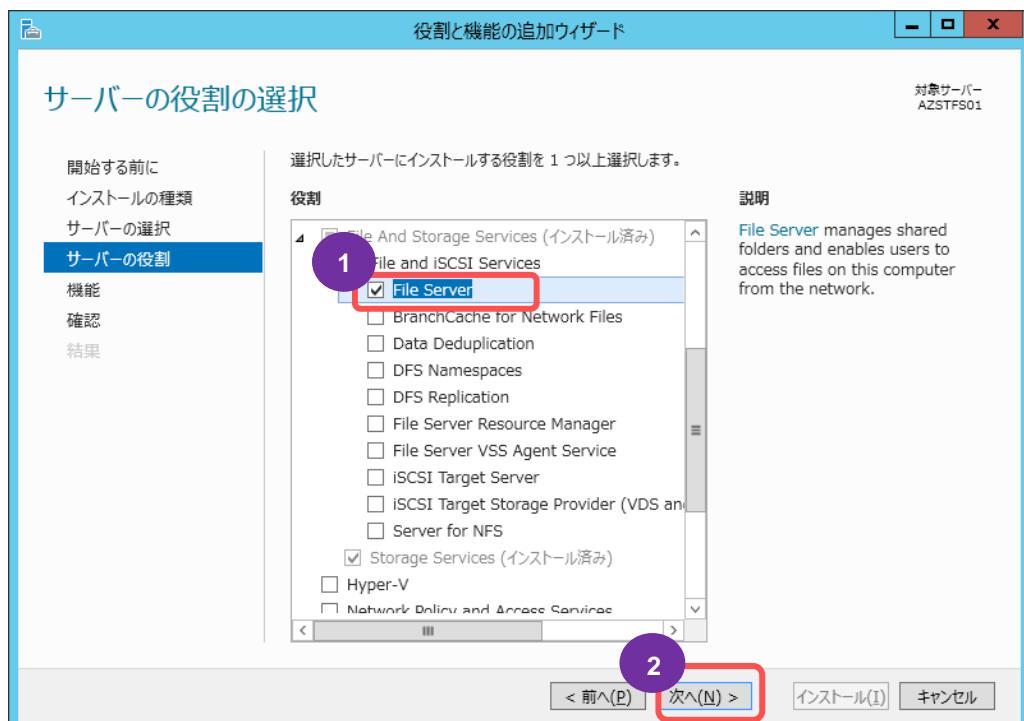


企業内システムと Microsoft Azure の VPN 接続、ファイルサーバー連携

5. [対象サーバーの選択] ページで適切なサーバーを選択し、[次へ] をクリックします。既定ではローカル サーバーが選ばれます。

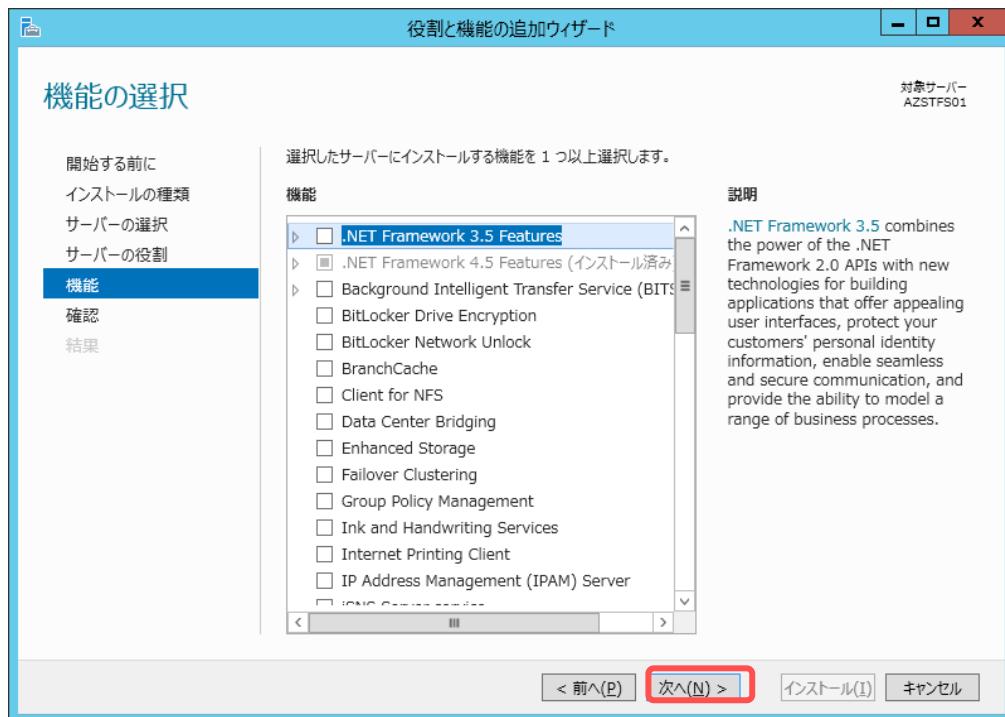


6. [サーバーの役割の選択] ページで、[ファイル サービスおよび記憶域サービス] と [ファイル サービス] を展開し、[ファイル サーバー] のチェック ボックスをオンにします。[次へ] をクリックします。

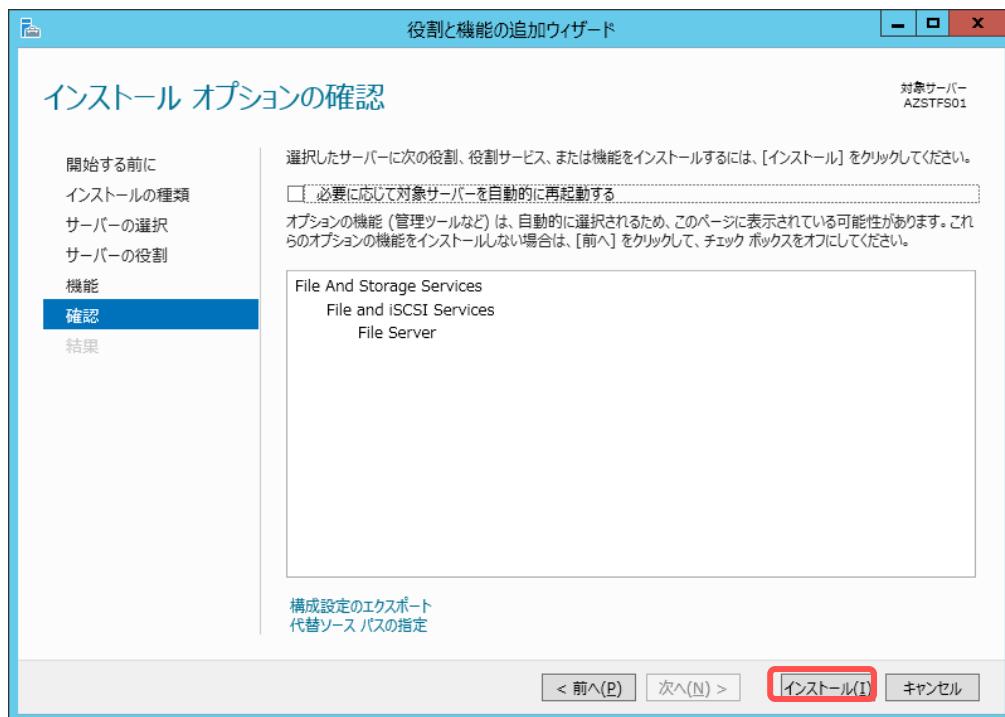


企業内システムと Microsoft Azure の VPN 接続、ファイルサーバー連携

7. [機能の選択] ページで、何も選択せずに、[次へ] をクリックします。

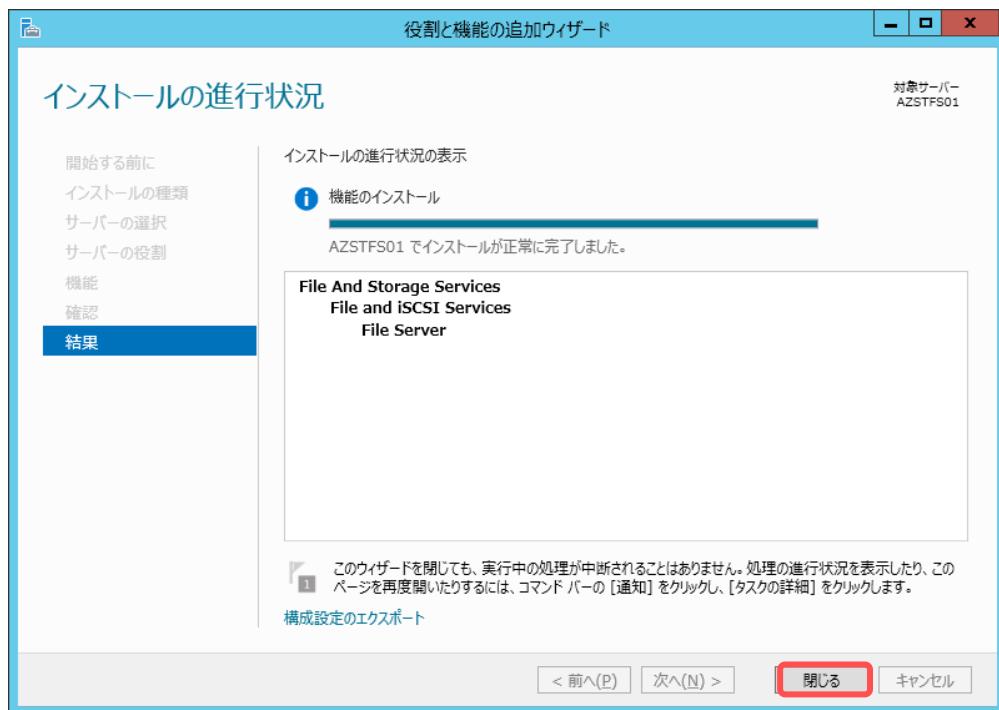


8. [インストール オプションの確認] ページで、[インストール] をクリックします。



企業内システムと Microsoft Azure の VPN 接続、ファイルサーバー連携

9. [インストール進行状況] ページで、機能のインストールが正常に完了したら、[閉じる]をクリックします。



6.2 共有フォルダーの作成

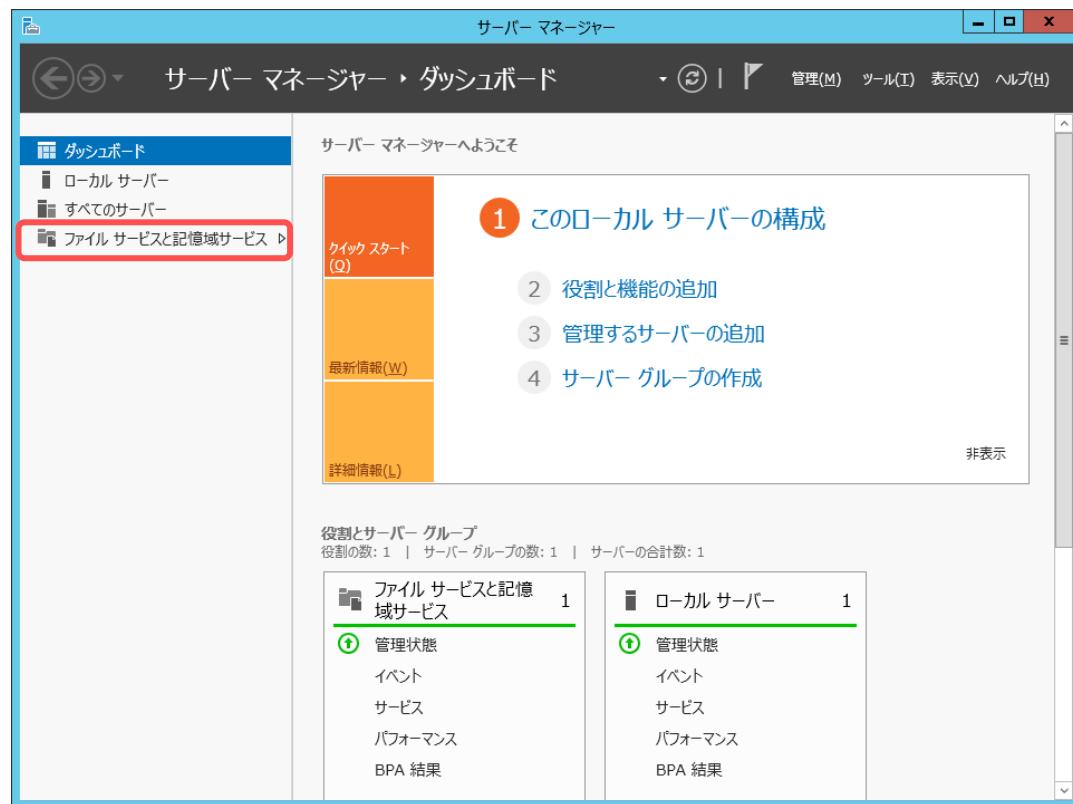
◆ 共有フォルダーの作成

ファイルサーバー上に共有フォルダーを作成します。

1. デスクトップ画面左下の[サーバー マネージャー]をクリックします。

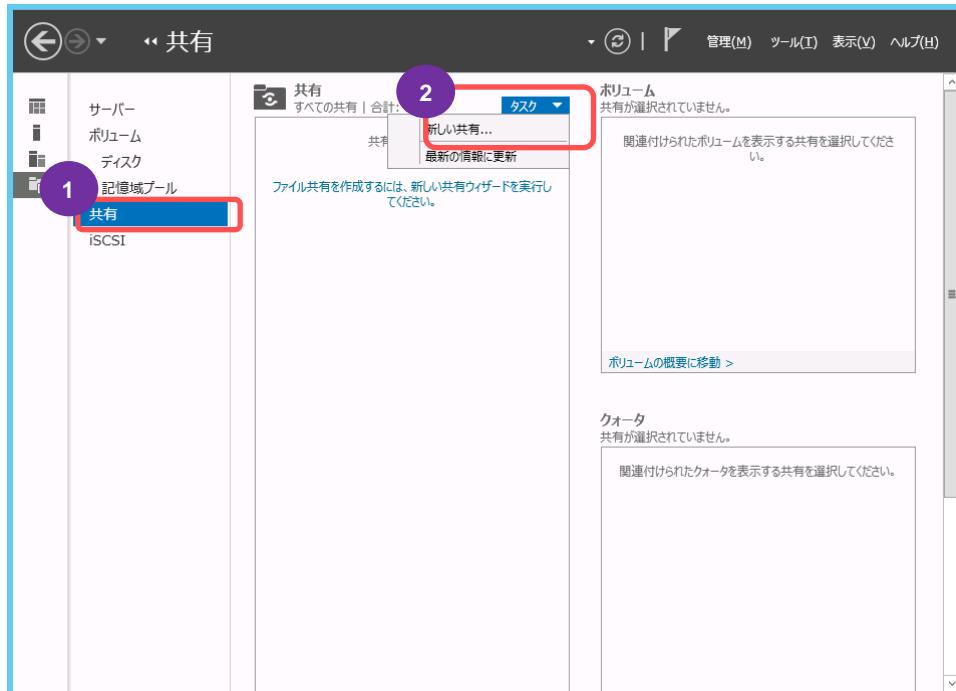


2. [ファイルサービスと記憶域サービス] をクリックします。



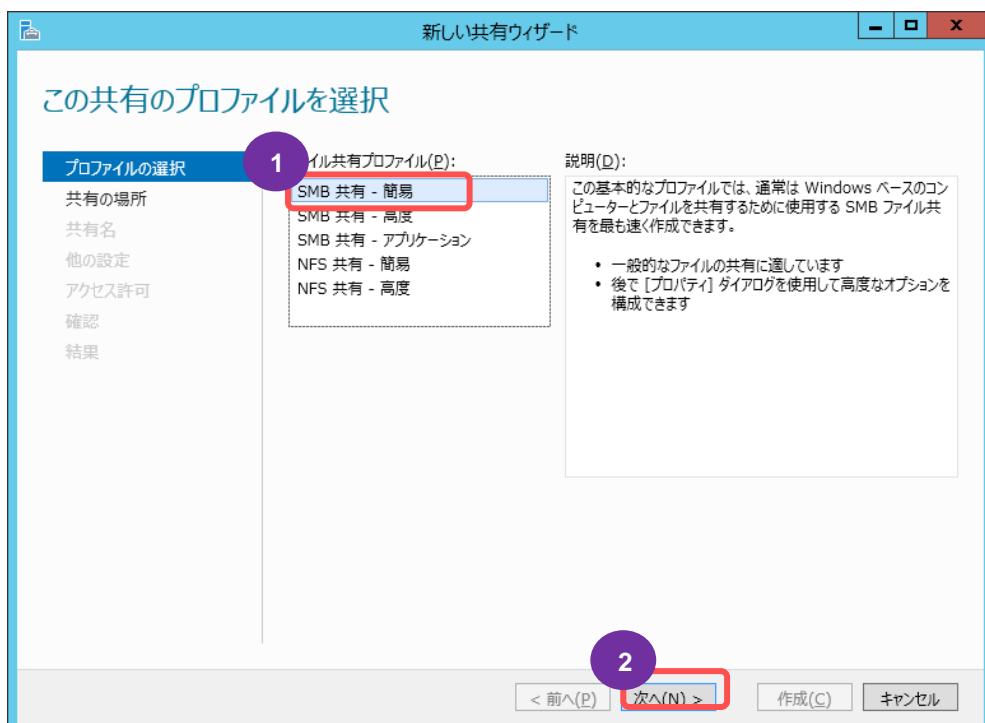
企業内システムと Microsoft Azure の VPN 接続、ファイルサーバー連携

3. [共有]を選択します。[共有]にある[タスク▼]メニューから[新しい共有...]をクリックします。



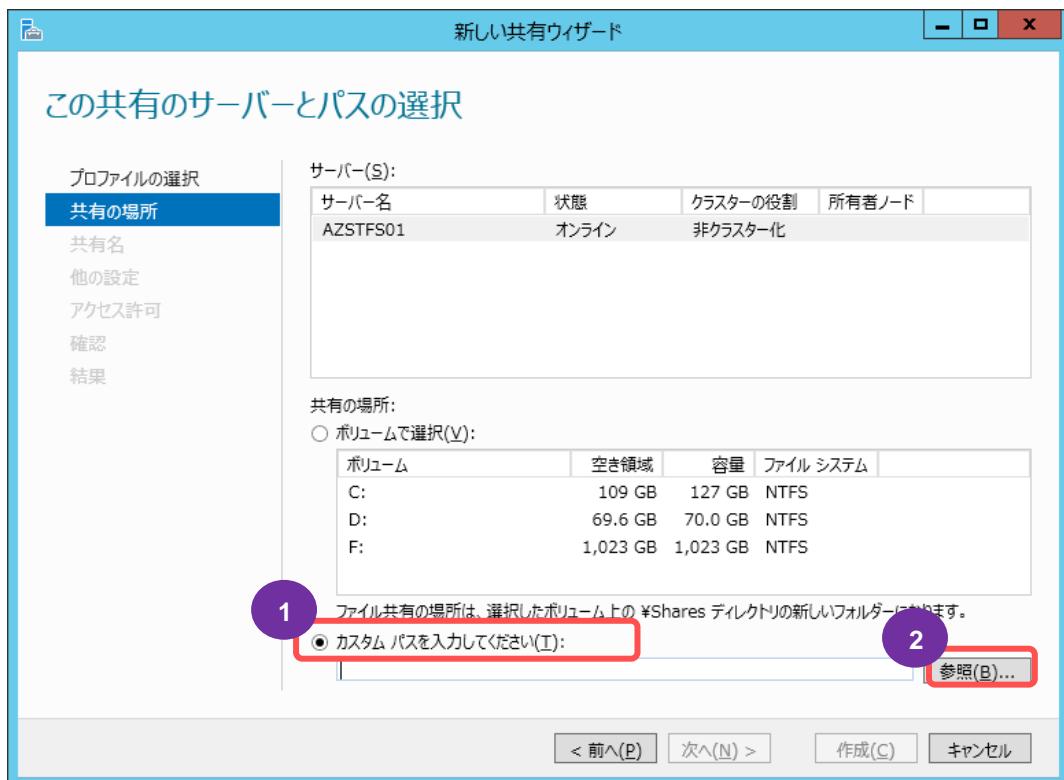
4. [新しい共有ウィザード] が開始されます。

[この共有のプロファイルを選択] ページで[SMB 共有 - 簡易]を選択し、[次へ]をクリックします。

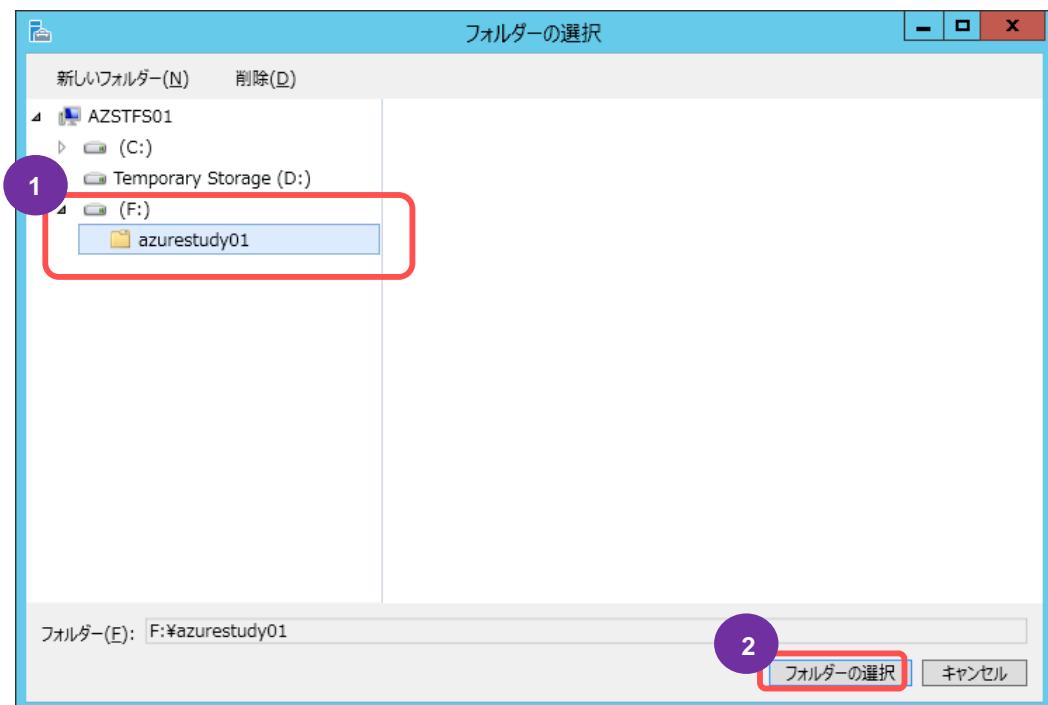


企業内システムと Microsoft Azure の VPN 接続、ファイルサーバー連携

5. [この共有のサーバーとパスの選択]ページでサーバー名確認します。共有の場所で[カスタムパスを入力してください]を選択し、[参照]をクリックします。



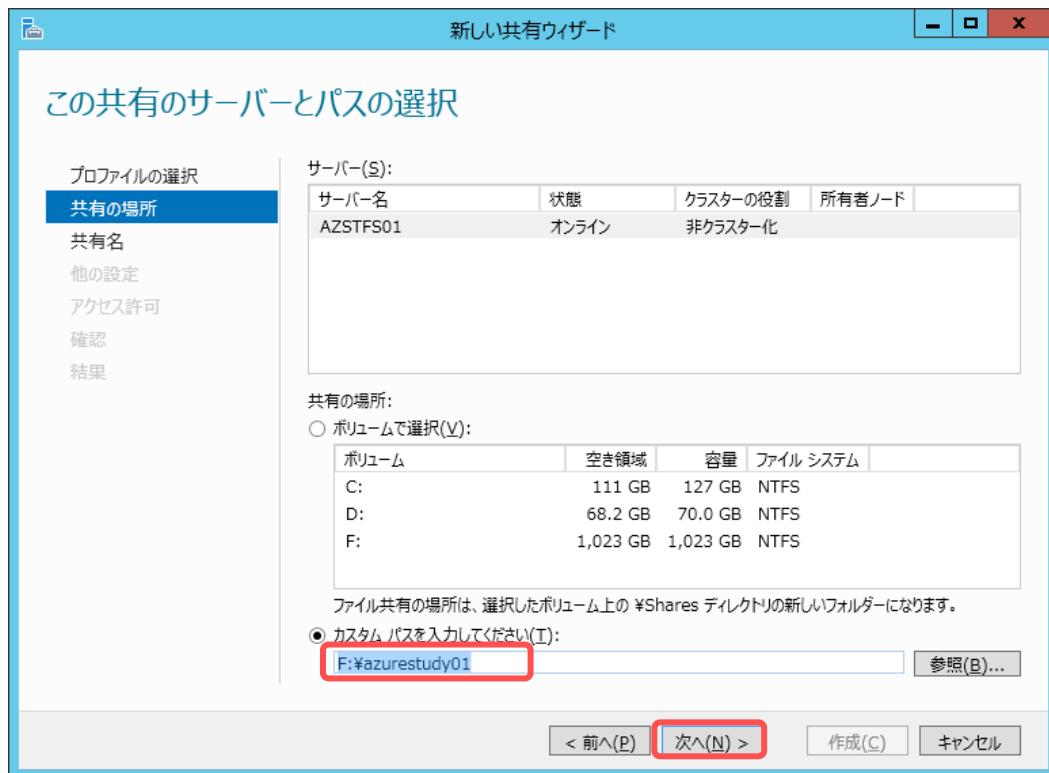
6. 共有するフォルダーを選択し、[フォルダーの選択]をクリックします。



※事前に F ボリュームに「azurestudy01」(本自習書例)というフォルダーを作成しておきます。

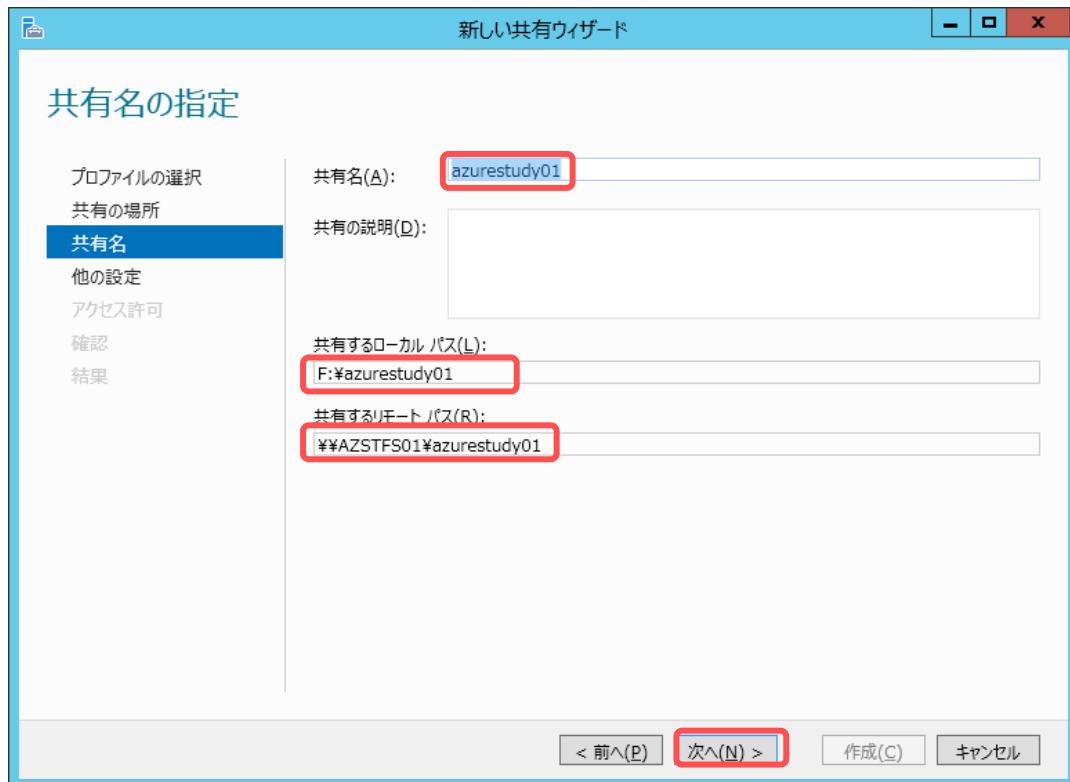
企業内システムと Microsoft Azure の VPN 接続、ファイルサーバー連携

7. [共有の場所]が選択されたことを確認し、[次へ]をクリックします。

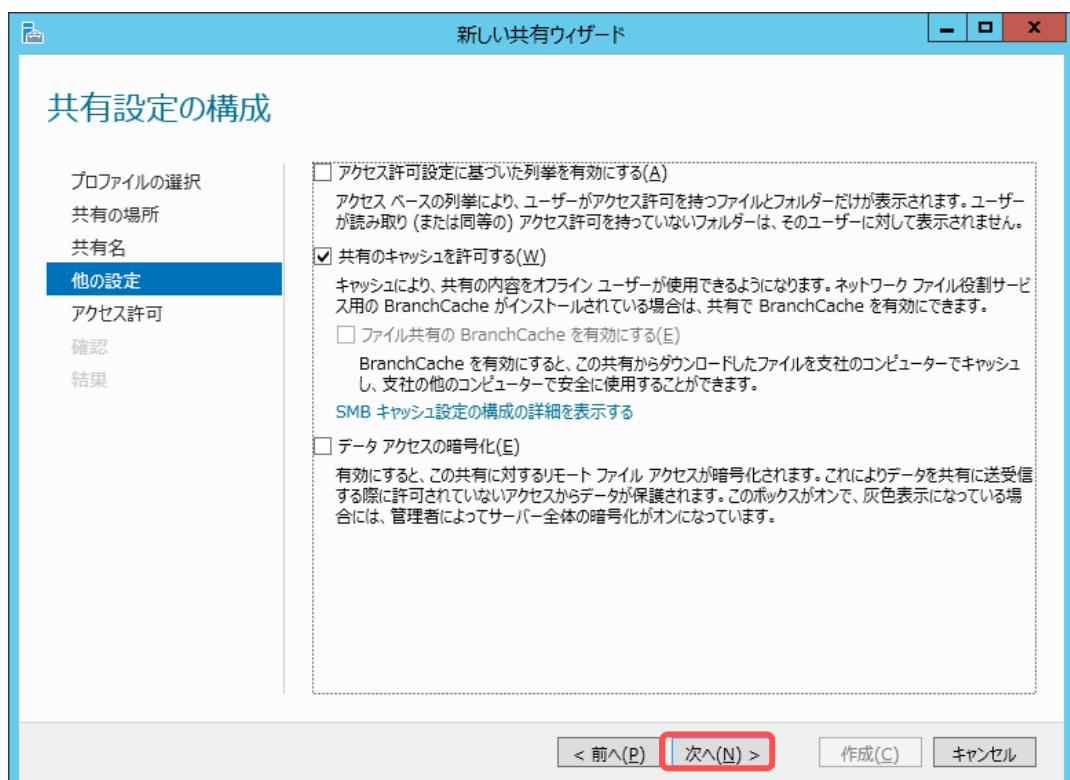


企業内システムと Microsoft Azure の VPN 接続、ファイルサーバー連携

8. [共有名の指定]ページで**共有名、共有するローカルパス、共有するリモートパス**を確認し、[次へ]をクリックします。



9. 他の設定を確認し、[次へ]をクリックします。

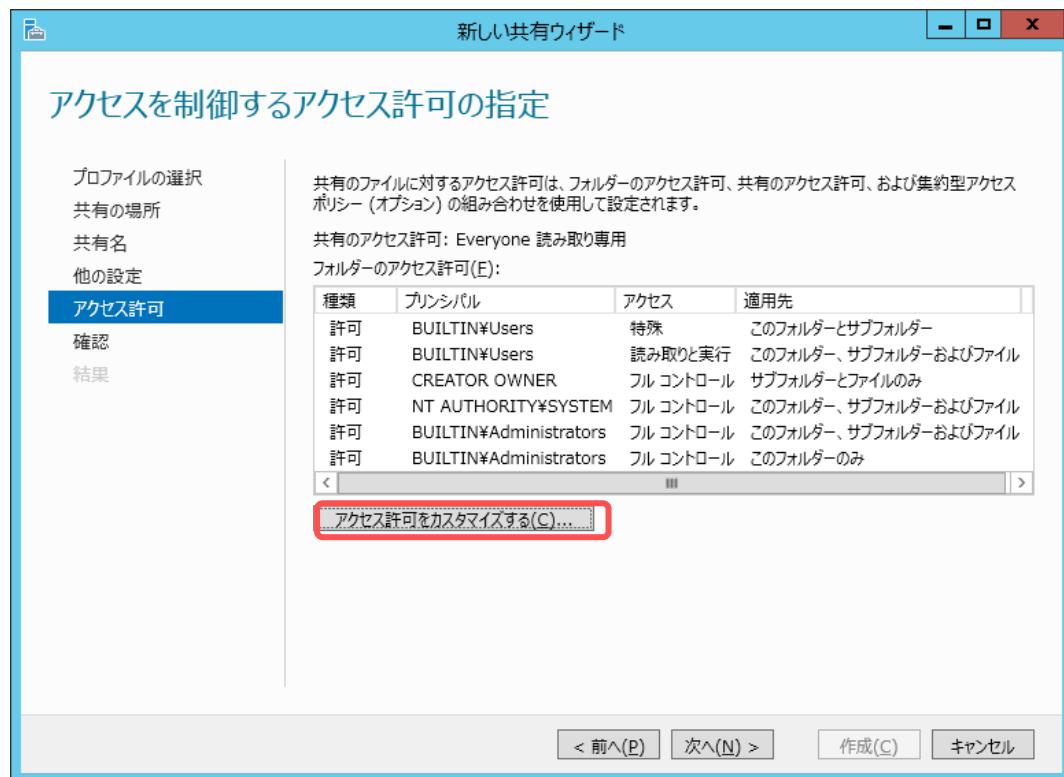


6.3 アクセス権の設定

◆ アクセス権の許可

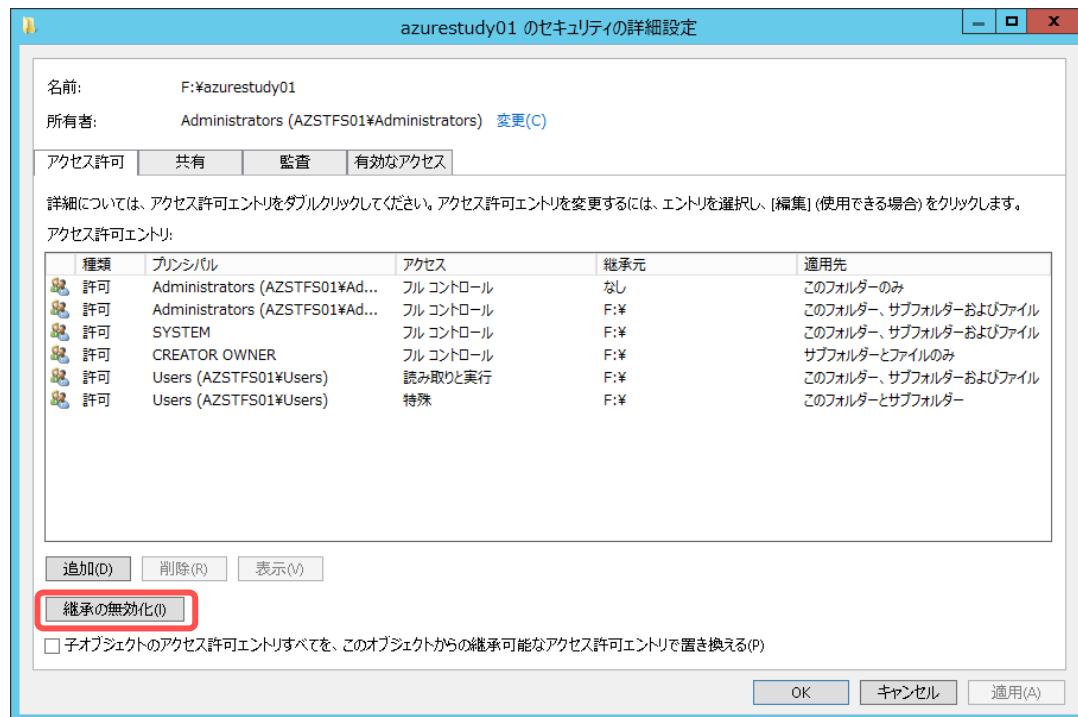
新しい共有ウィザードページでアクセスを制御するアクセス許可の指定を行います。

- 【新しい共有ウィザード】が続きます。【アクセスを制御するアクセス許可の指定】ページで【アクセス許可をカスタマイズする】をクリックします。

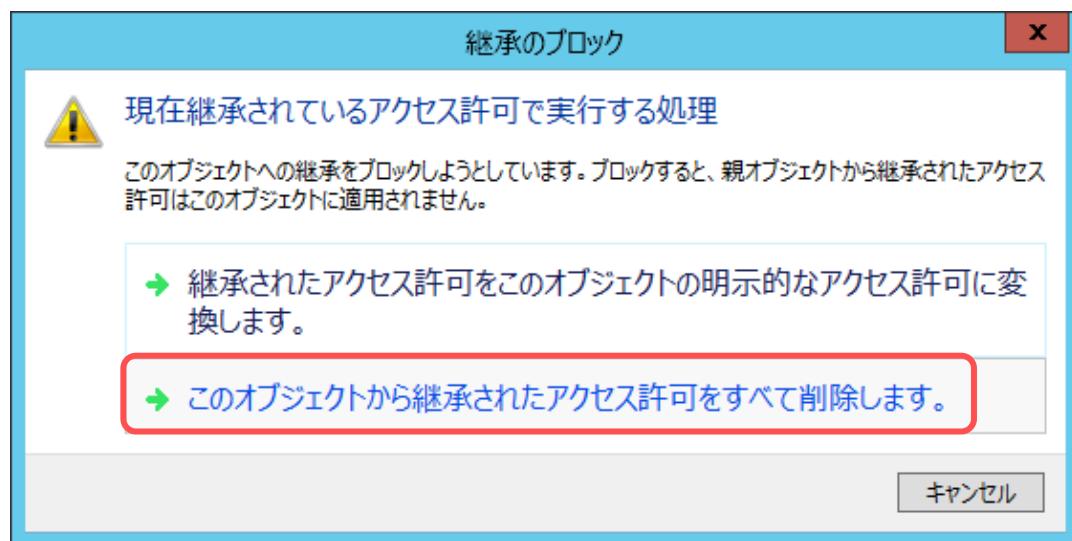


企業内システムと Microsoft Azure の VPN 接続、ファイルサーバー連携

2. 共有フォルダーのセキュリティの詳細設定ページで、[継承の無効化]をクリックします。

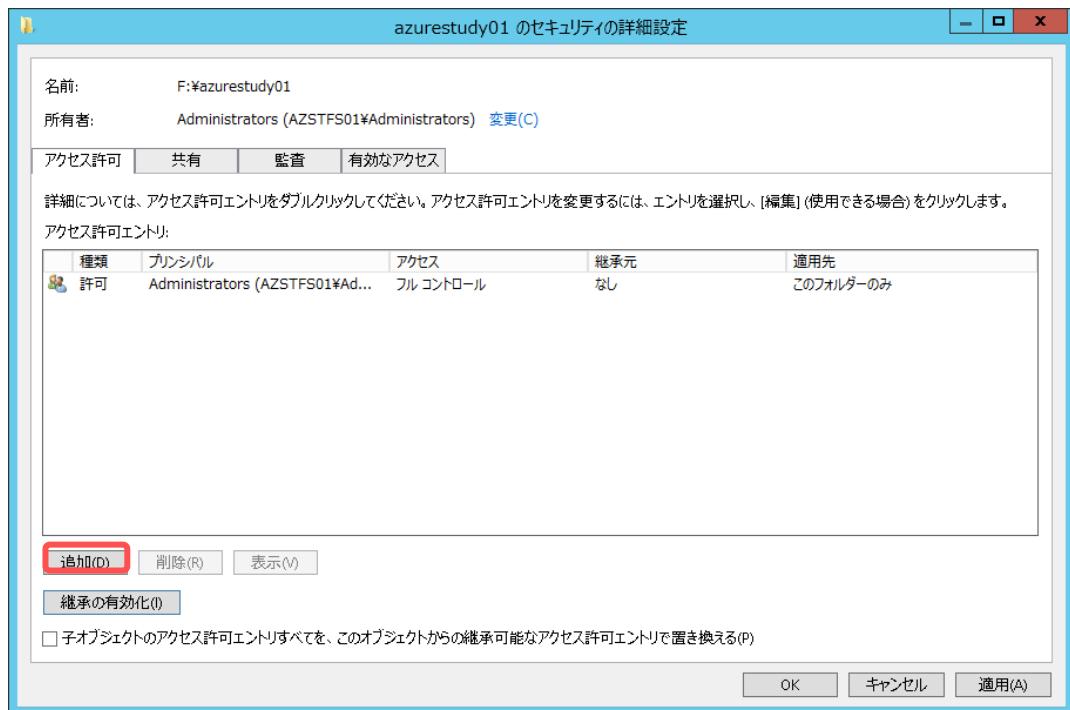


3. [継承のブロック]画面で[このオブジェクトから継承されたアクセス許可をすべて削除します]をクリックします。

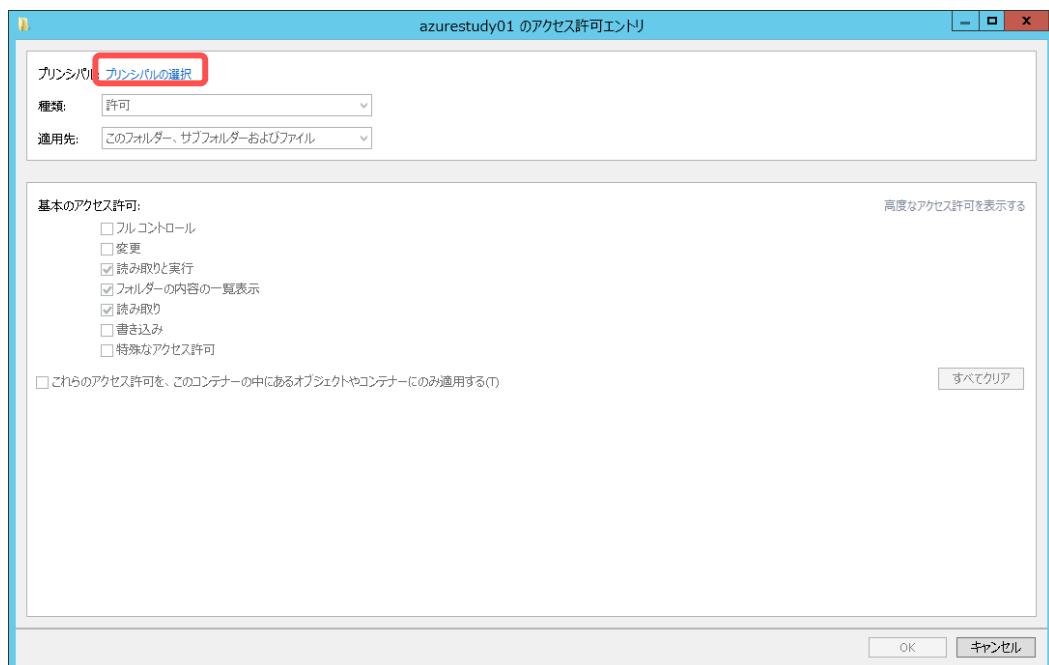


企業内システムと Microsoft Azure の VPN 接続、ファイルサーバー連携

4. [アクセスを制御するアクセス許可の指定]ページで[追加]をクリックします。

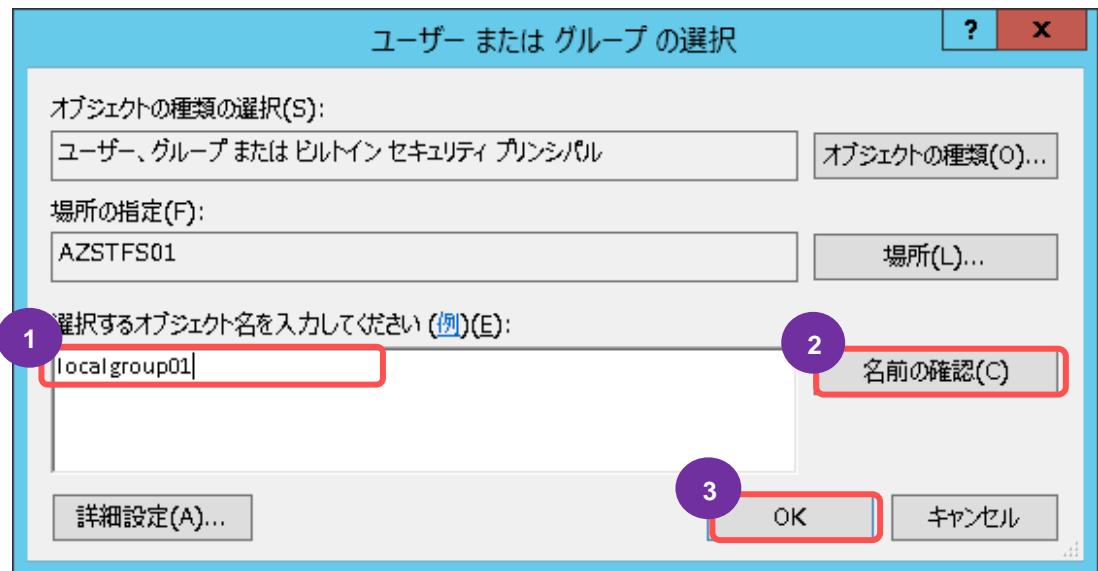


5. [プリンシパルの選択]をクリックします。

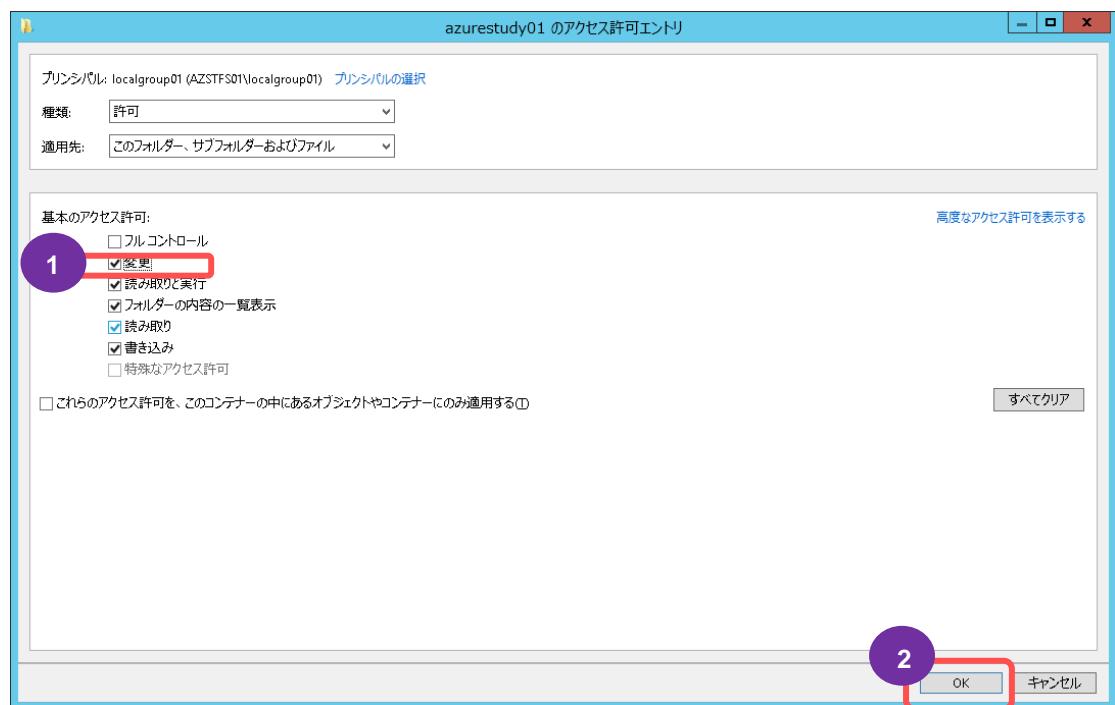


企業内システムと Microsoft Azure の VPN 接続、ファイルサーバー連携

6. 選択するオブジェクト名を入力し、[名前の確認]をクリックし、[OK]をクリックします。

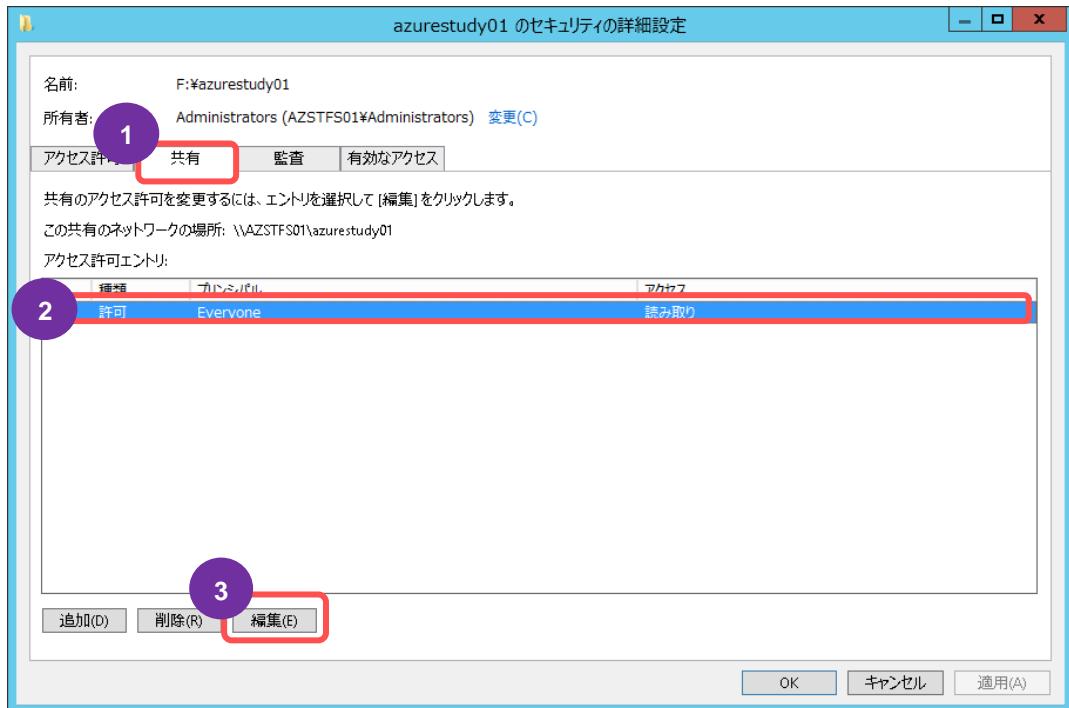


7. [基本のアクセス許可]で[変更]に□を入れ、[OK]をクリックします。

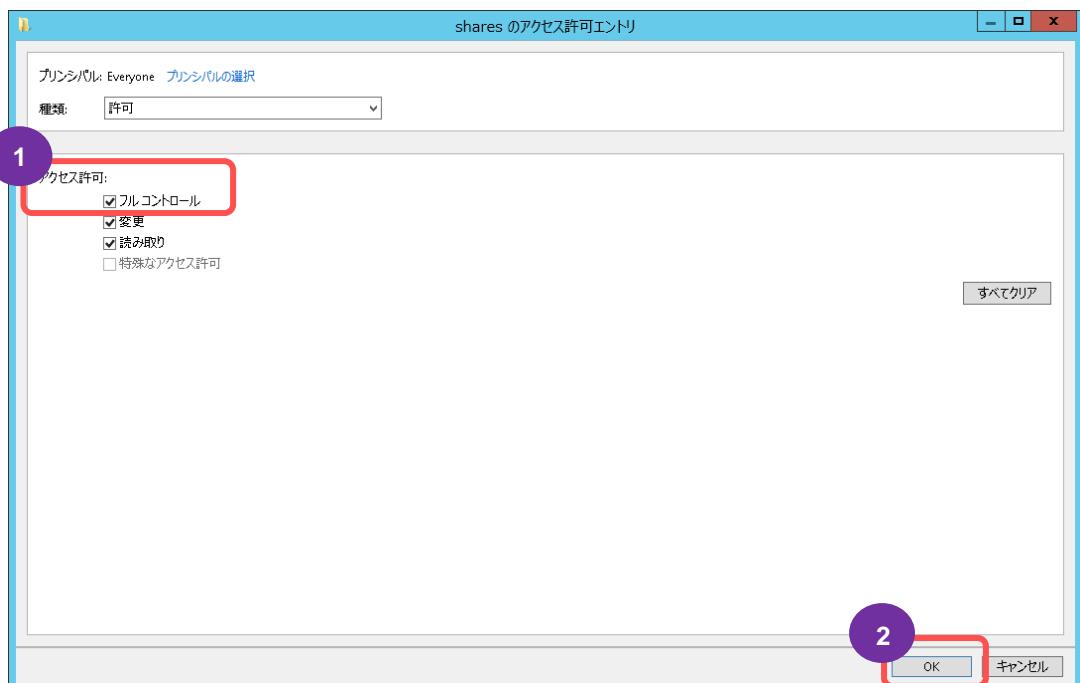


企業内システムと Microsoft Azure の VPN 接続、ファイルサーバー連携

8. [共有]タブをクリックします。アクセス許可エントリを選択し、[編集]をクリックします。

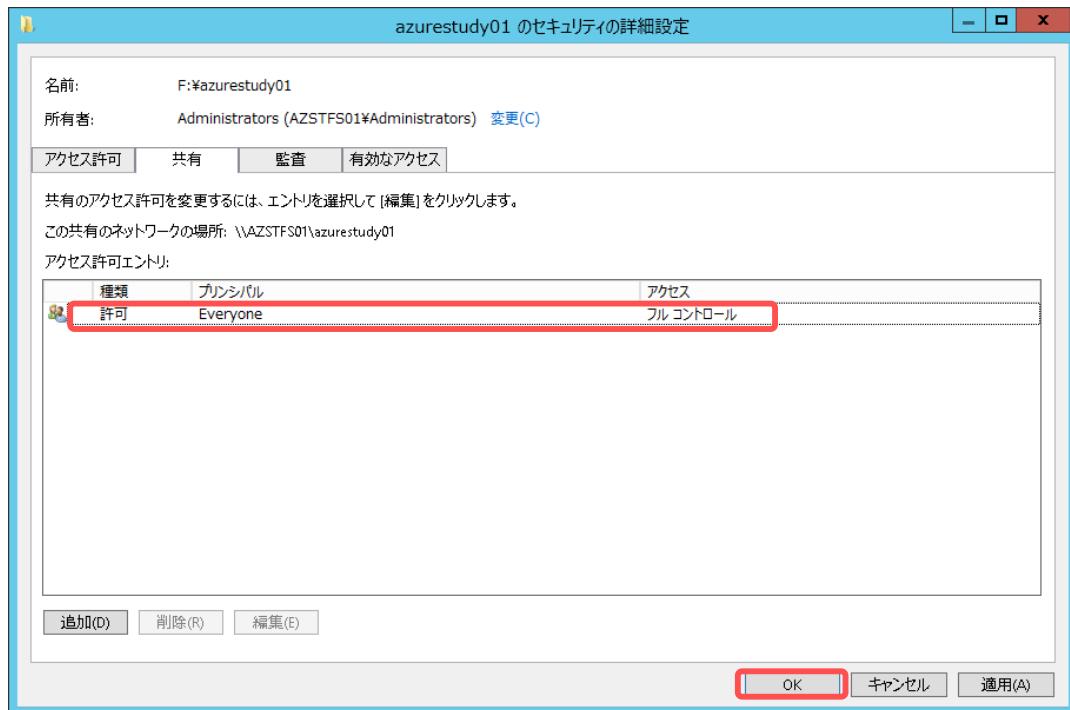


9. [アクセス許可]で[フルコントロール]をクリックし、[OK]をクリックします。

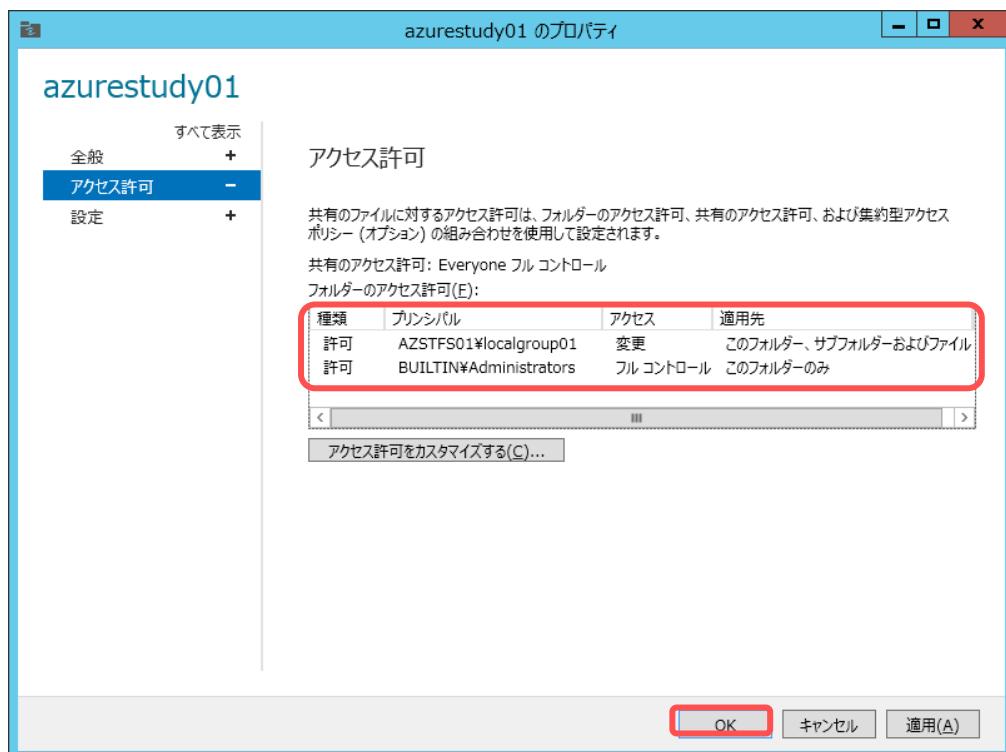


企業内システムと Microsoft Azure の VPN 接続、ファイルサーバー連携

10. 「Everyone」に対して「フルコントロール」が付与されていることを確認し、[OK]をクリックします。

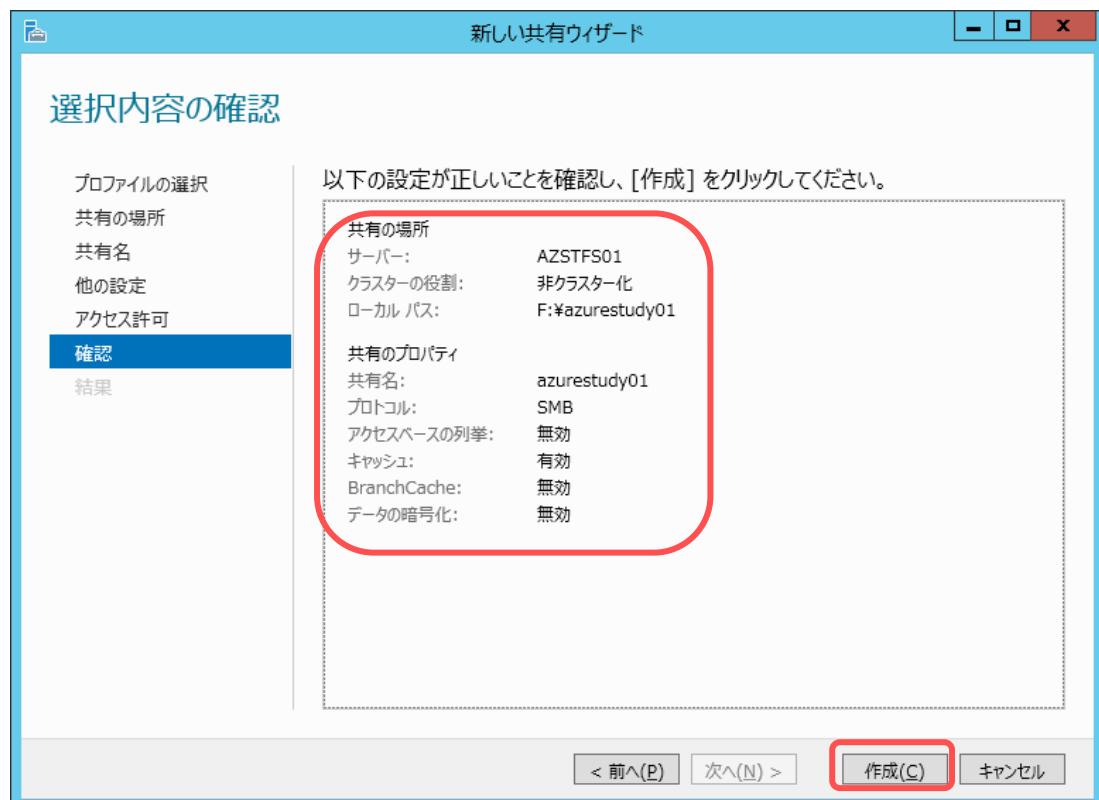


11. フォルダーのアクセス許可を確認し、[OK]をクリックします。

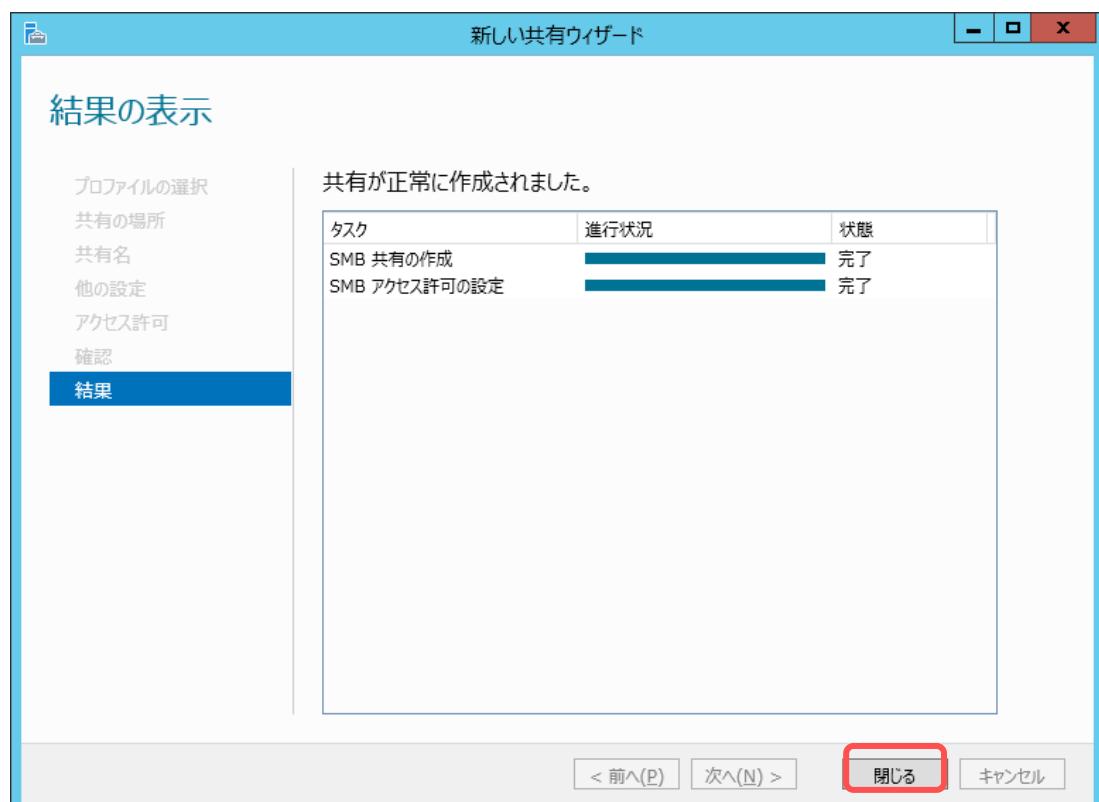


企業内システムと Microsoft Azure の VPN 接続、ファイルサーバー連携

12. 選択内容の確認ページで以下の設定が正しいことを確認し、[作成]をクリックします。

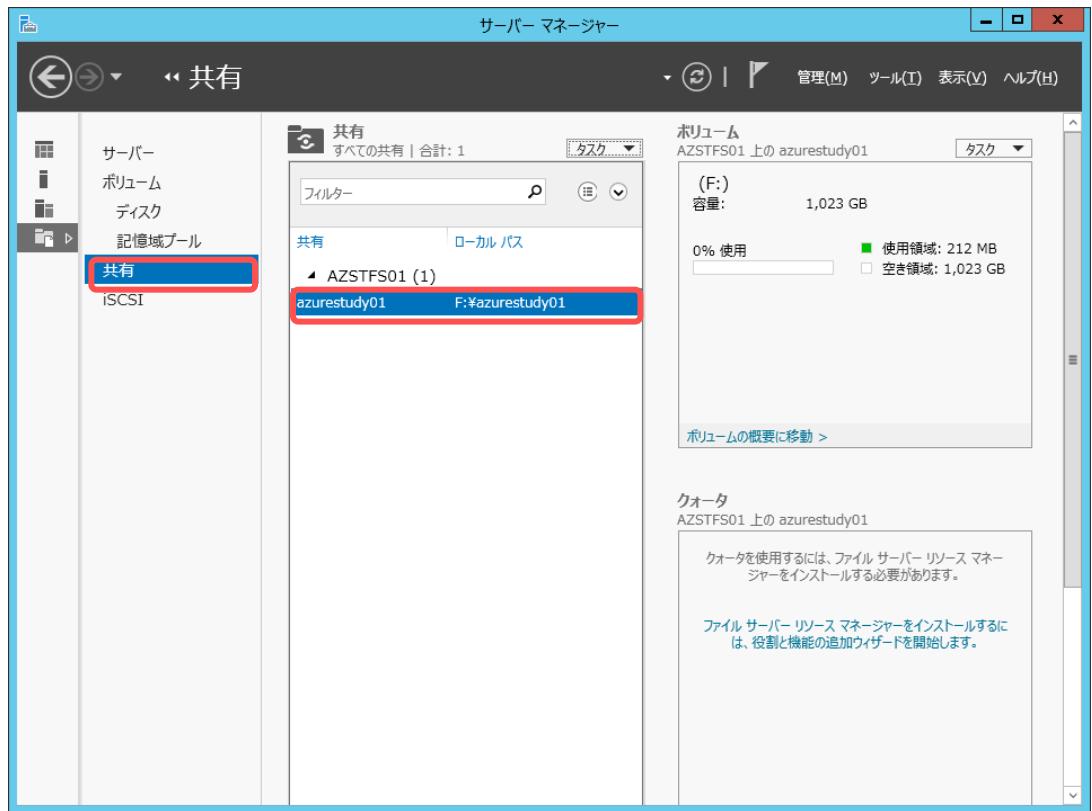


13. [結果の表示]ページで[共有が正常に作成されました]を確認し、[閉じる]をクリックします。



企業内システムと Microsoft Azure の VPN 接続、ファイルサーバー連携

14. [サーバー マネージャー]→[ファイルサービスと記憶域サービス￥共有]画面で上記 6.2 で作成したフォルダーが共有されていることを確認し、[サーバー マネージャー]を閉じます。



6.4 ネットワーク共有

◆ 共有フォルダーへのアクセス

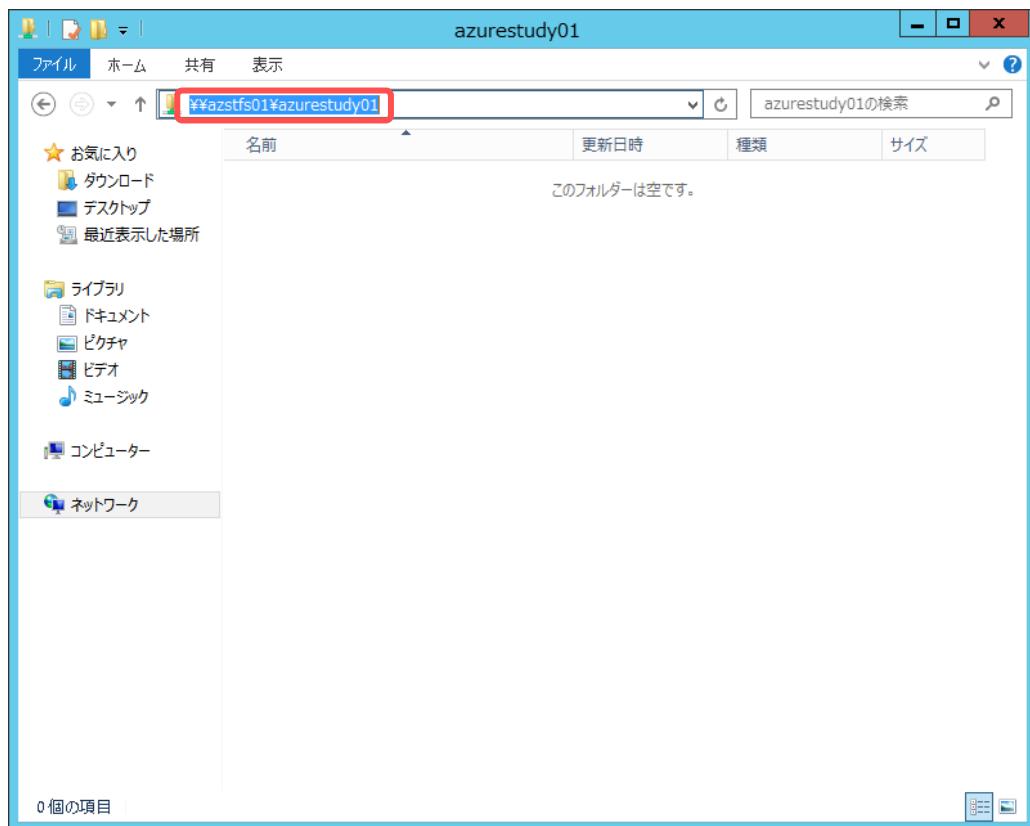
上記 6.2 で作成した共有フォルダーへアクセスします。

Note : 名前解決

オンプレミス環境から NetBIOS 名による名前解決はできません。

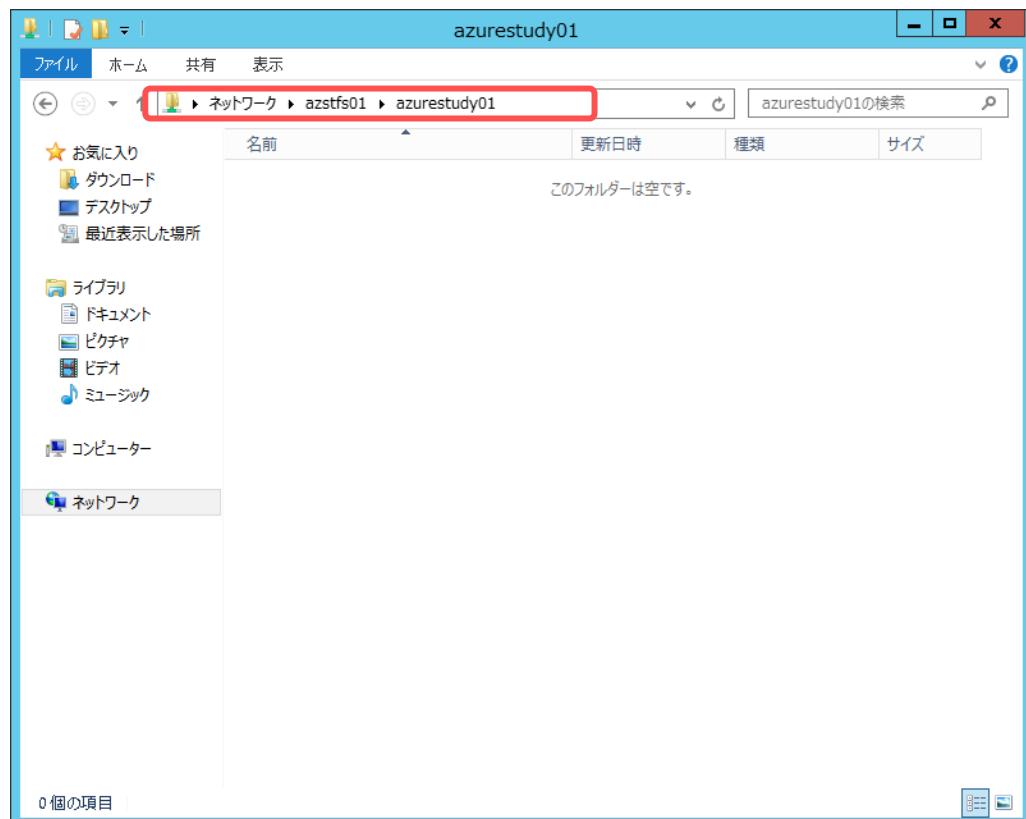
1. オンプレミス側のクライアント PC にてエクスプローラを開き、次の画面のように、直接にアドレスを入力します。入力形式は [¥¥<コンピュータ名>¥<共有フォルダ名>]です。

本自習書例) ¥¥azstfs01¥azurestudy01



Note : オンプレミス側のクライアント PC から共有フォルダーへのアクセスができない場合

1. クライアント PC のネットワーク設定にてデフォルトゲートウェイ(オンプレミス側の VPN 装置のローカル側の IP アドレス)を設定してみてください。
2. 名前解決ができない場合は Azure 上のファイルサーバーの IP を確認して[¥¥IPアドレス¥共有フォルダ名]に接続してみてください。

2. 共有フォルダーが開けることを確認します。

◆ おわりに

この自習書では、Microsoft Azure 仮想マシンにファイルサーバーを導入する手順について学習しました。

Azure 上のファイルサーバーは AD とセキュアに連携することによって社内と変わらないセキュアなファイルサーバーが手に入れることができます。

このあとも、Azure 上に Active Directory を構築し、仮想サーバーをドメインに参加させてファイルサーバー導入する自習書を用意していますので、ぜひチャレンジしてみてください。

なお、この自習書で取り扱った環境を構築あるいは活用するために、以下の自習書についてもご参考ください。

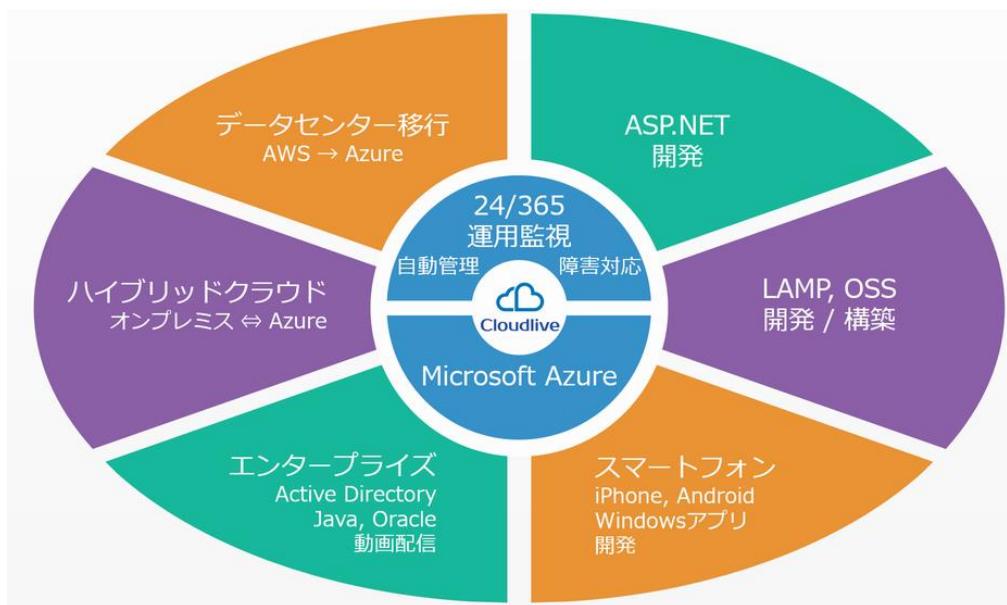
- **Microsoft Azure 自習書シリーズ「企業内システムと Microsoft Azure の VPN 接続」**
Azure 上に初めて仮想ネットワークを構築することができる自習書となっています。
- **Microsoft Azure 自習書シリーズ「企業内システムと Microsoft Azure の VPN 接続、Active Directory 連携」**
Azure 上に初めて Active Directory Domain Controller を導入することができる自習書となっています。
- **Microsoft Azure 自習書シリーズ「企業内システムと Microsoft Azure の VPN 接続、Active Directory、ファイルサーバー連携」**
Azure 上の AD DS にドメイン参加し、ファイルサーバーを導入することができる自習書となっています。

執筆者プロフィール

Cloudlive 株式会社 (<http://www.cloudlive.jp/>)

皆様が Microsoft Azure の恩恵を受け、最大限に活用できるよう、支援することをミッションとした企業です。24/365 の運用監視や、各種コンサルティング、開発支援を行っています。

Azure の 2008 年レビュー時から、Azure 事業に取り組んでおり、Windows, Linux ともに日本 TOP のノウハウと実績を持ちます。Microsoft Azure MVP 経験者が 4 名在籍しており、Microsoft 本社へフィードバックや情報交換も頻繁に行うとともに、変化の速いクラウド業界において最新のノウハウを提供します。お困りの点がありましたら、ぜひご相談ください。本書に対する感想や、ご意見もお待ちしています。



安心、安全の運用監視
24時間365日 Microsoft Azure を監視



ノウハウに基づく、最適なプラン、構成を提案
Microsoftテクノロジに限らず、Linux/OSSの実績も豊富



Microsoft Azureスペシャリストによるサービス提供
Microsoft Azure MVP経験者4名 + 経験豊富なメンバー



初回アセスメント無料
ちょっとしたわからないことも、まずはご相談ください