



Microsoft Azure

Microsoft Azure 自習書シリーズ No.5

企業内システムと Microsoft Azure の VPN 接続、Active Directory 連携

Published: 2014 年 5 月 30 日

Updated: 2015 年 1 月 31 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。

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 | 2015/1/31 | ・2015年1月現在の情報に更新 |

目次

| | |
|---|-----|
| STEP 1. Active Directory Domain Service の概要と本書の目的について | 5 |
| 1.1 Active Directory Domain Service の概要 | 6 |
| 1.2 シナリオ | 7 |
| 1.3 ゴール | 8 |
| STEP 2. 自習書の前提について | 9 |
| 2.1 対象 | 10 |
| 2.2 前提条件 | 11 |
| STEP 3. VPN 接続を設定する際に 参照すべき資料について | 12 |
| 3.1 VPN 接続を設定する際に参考すべき資料について | 13 |
| STEP 4. ストレージアカウントを作成する | 14 |
| 4.1 ストレージアカウントの作成 | 15 |
| STEP 5. 仮想マシンを作成する | 18 |
| 5.1 環境情報一覧 | 19 |
| 5.2 仮想ネットワークへの DNS サーバーの設定 | 21 |
| 5.3 仮想マシンの作成 | 25 |
| 5.4 仮想マシンへのリモートデスクトップ接続 | 33 |
| 5.5 日本語化 | 36 |
| 5.6 タイムゾーン | 46 |
| 5.7 Windows Update の設定 | 48 |
| 5.8 ディスクの追加 | 51 |
| STEP 6. 仮想マシン上に AD DS を構築する | 61 |
| 6.1 ドメインへの参加 | 62 |
| 6.2 AD DS のインストール | 67 |
| 6.3 ドメインコントローラーへの昇格 | 76 |
| 6.4 初期レプリケートの完了 | 84 |
| 6.5 NTP に関する注意点 (PDC エミュレーターとは同期しない) | 87 |
| 6.6 サイトとサブネットの作成 | 88 |
| STEP 7. Azure 上に 2 台目以降の AD DS を 構築する際のポイント | 99 |
| 7.1 AD DS のレプリケート元の選択 | 100 |
| 7.2 複数台の AD DS とのレプリケート確認 | 101 |
| 7.3 サイトの移動 | 102 |
| STEP 8. 追加構築した AD DS を DNS サーバーとして登録する | 103 |
| 8.1 仮想ネットワークへの DNS サーバーの追加設定 | 104 |

STEP 1. Active Directory Domain Service の概要と本書の目的について

この STEP では、仮想ネットワーク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。

- ✓ Active Directory Domain Service の概要
- ✓ シナリオ
- ✓ ゴール

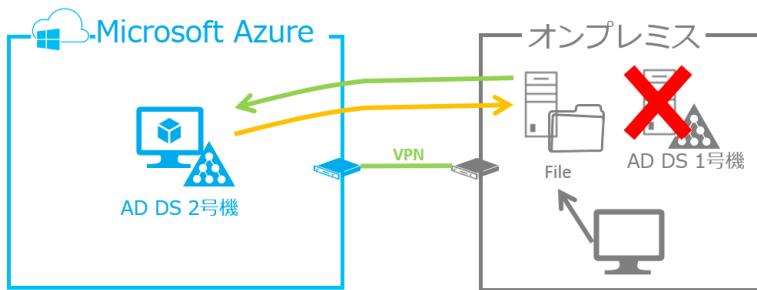
1.1 Active Directory Domain Service の概要

Active Directory Domain Service (以降 AD DS と呼称) は、ディレクトリ データを格納し、ユーザーのログオン プロセス、認証、およびディレクトリ検索など、ユーザーとドメイン間の通信を管理します。Active Directory ドメイン コントローラーは、AD DS を実行するサーバーです。

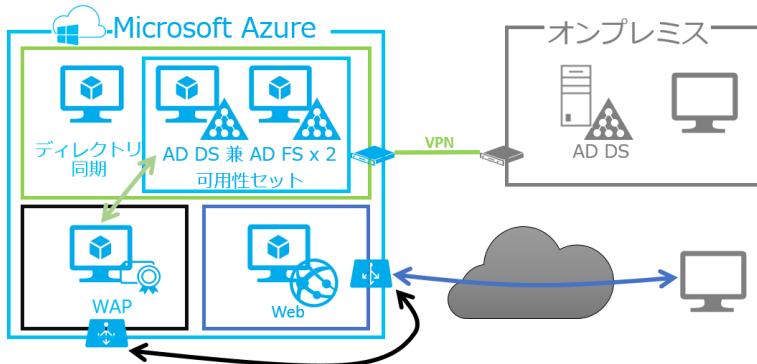
1.2 シナリオ

Microsoft Azure (以降 Azure と呼称) 上に AD DS を構築する際の目的を明確にします。その目的に応じて Azure 上に構築する AD DS の構成について検討を行う必要があります。

- オンプレミス環境の災害対策サイトとして利用するのか？

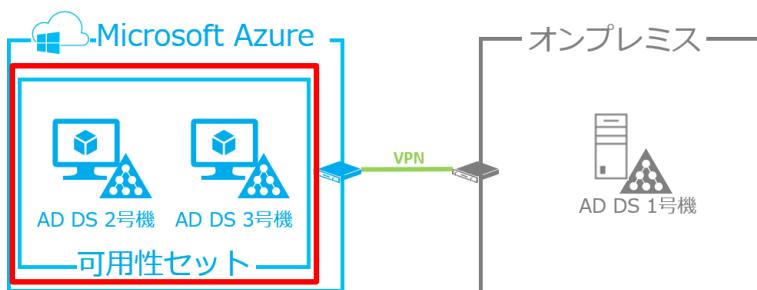


- Azure 上に展開したサービスの認証用に利用するのか？



災害対策サイトとして利用するのみであれば AD DS を Azure 上に 1 台構築する想定でも構いませんが、インターネット経由でのサービス提供などの利用であれば 2 台構成とし「可用性セット」などを行うことも想定する必要があります。

この自習書では、サービスの認証用に利用することを前提とした、可用性セットを用いた AD DS の構築を行います。



1.3 ゴール

サービスの認証用に利用することを前提に、Azure 上に 2 台の AD DS を構築します。
これにより、Azure 上に AD DS を構築するための手順やそれに伴う注意点を学びます。

STEP 2. 自習書の前提について

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。

- ✓ 対象
- ✓ 前提条件

2.1 対象

この自習書では、物理環境に於ける AD DS の構築経験・知識があり、初めて Azure 上に AD DS を構築しようとしている方を対象としております。

2.2 前提条件

- Azure 管理ポータルへサインインできるアカウントを持っていることを前提としています。
- VPN 接続用のインターネット回線があることを前提としています。 加えて、固定グローバル IP アドレスが必要となります。
- 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ります。
また、VPN の設定については別途自習書「企業内システムと Microsoft Azure の VPN 接続」をご参照ください。
- Azure 管理ポータルへのサインインの手順は省略しています。
- 既にオンプレミス環境に Active Directory Domain Service が存在していることを前提とします。

STEP 3. VPN 接続を設定する際に 参考すべき資料について

VPN 接続の設定については本書では触れません。本 STEP では VPN 接続設定で参考にすべき自習書を記載するのみとなります。

3.1 VPN 接続を設定する際に参照すべき資料について

VPN の設定については別紙「企業内システムと Microsoft Azure の VPN 接続」をご参照ください。

STEP 4. ストレージアカウントを作成する

この STEP では、ストレージアカウントの作成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。

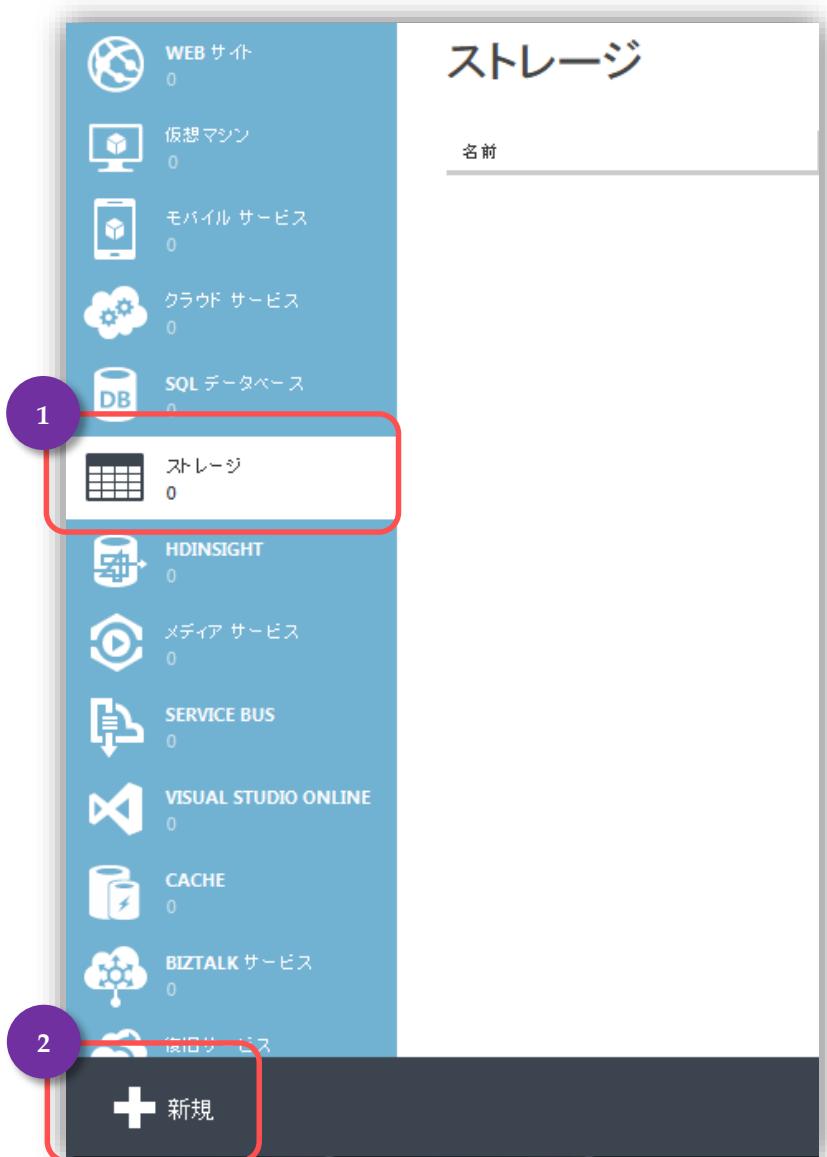
- ✓ ストレージアカウントの作成

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この自習書では、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。

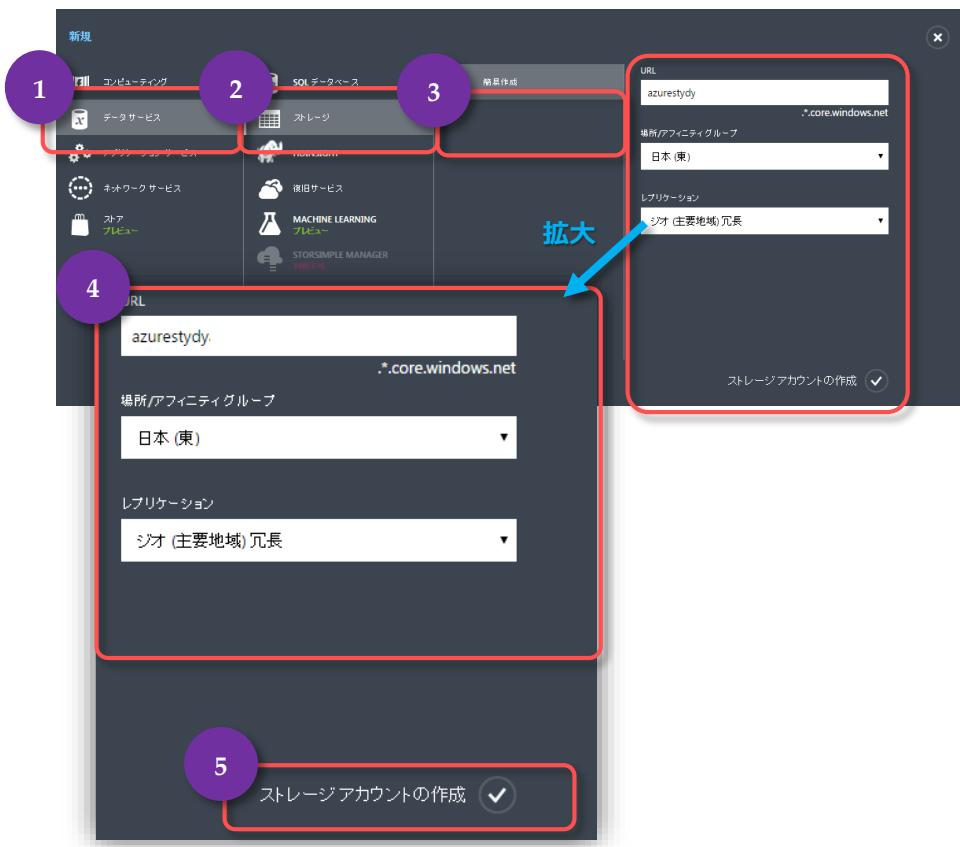
1. Azure 管理ポータルにサインインし、左のメニューから[ストレージ]をクリックします。画面左下に表示される[+新規]をクリックします。



企業内システムと Microsoft Azure の VPN 接続、Active Directory 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 3 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。 尚、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。 ブロック 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。 尚、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。 ブロック 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。 尚、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。 ブロック 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。



以上でストレージアカウントの作成が完了となります。

STEP 5. 仮想マシンを作成する

この STEP では、仮想マシン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。

- ✓ 環境情報一覧
- ✓ 仮想ネットワークへの DNS サーバーの設定
- ✓ 仮想マシンの作成
- ✓ 仮想マシンへのリモートデスクトップ接続
- ✓ 日本語化
- ✓ タイムゾーン
- ✓ Windows Update の設定
- ✓ ディスクの追加

5.1 環境情報一覧

この自習書では Azure 上に AD DS を 2 台構築しますが、構築手順については 1 台目のみの記載となります。2 台目以降を構築する際には下記情報を元に 1 台目と同じ手順で作成します。

◆ オンプレミス上の AD DS

| 項目 | 説明 |
|-----------|---------------------------|
| マシン名 | OPSTADDS01 |
| IP アドレス | 192.168.118.160 |
| ドメイン名 | azurestudy.local |
| ドメイン管理者権限 | administrator / studyP@ss |
| サイト | on-premise |

◆ Azure 上の AD DS 1 号機

| 項目 | 説明 |
|----------------|---------------------------|
| マシン名 | AZSTADDS01 |
| インスタンス | 標準 |
| サイズ | A1 (S) |
| クラウドサービス DNS 名 | AZSTADDS |
| 可用性セット | AZSTADDS-AS |
| 内部 IP アドレス | 10.1.1.4 |
| ローカル管理者 | studyadmin / studyP@ss |
| ドメイン名 | azurestudy.local |
| ドメイン管理者権限 | administrator / studyP@ss |
| サイト | on-azure |

◆ Azure 上の AD DS 2号機

| 項目 | 説明 |
|----------------|---------------------------|
| マシン名 | AZSTADDS02 |
| インスタンス | 標準 |
| サイズ | A1 (S) |
| クラウドサービス DNS 名 | AZSTADDS |
| 可用性セット | AZSTADDS-AS |
| 内部 IP アドレス | 10.1.1.5 |
| ローカル管理者 | studyadmin / studyP@ss |
| ドメイン名 | azurestudy.local |
| ドメイン管理者権限 | administrator / studyP@ss |
| サイト | on-azure |

5.2 仮想ネットワークへの DNS サーバーの設定

Azure 上に構築した仮想マシンへの IP の払い出しと DNS サーバーの払い出しも DHCP によって行われます。DNS サーバーの IP 設定は手動でも設定することは可能ですが、特別な理由がない限り DHCP で DNS サーバー(AD DS)の IP を払い出せるようにしておくことが推奨されます。

ここではまず、オンプレミス上の AD DS の IP アドレスを DNS サーバーとして登録します。

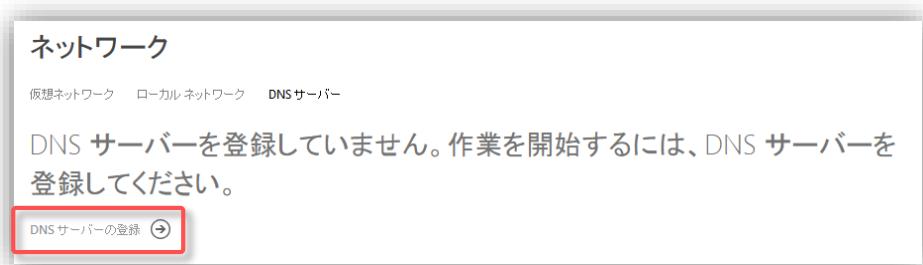
1. Azure 管理ポータルにサインインし、左のメニューから[ネットワーク]をクリックします。



2. [DNS サーバー]をクリックします。

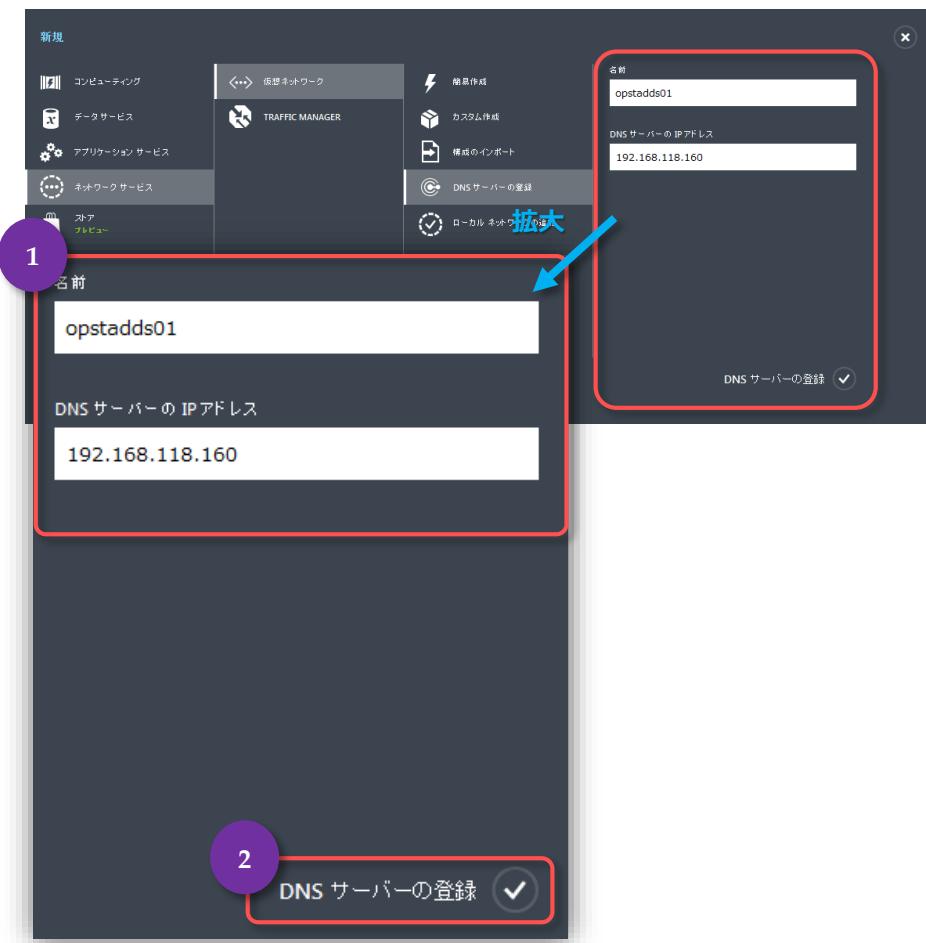


3. [DNS サーバーの登録]をクリックします。



企業内システムと Microsoft Azure の VPN 接続、Active Directory 連携

4. [名前]に「opstadds01」と入力し[DNS サーバーの IP アドレス]に「192.168.118.160」と入力します。
[DNS サーバーの登録]をクリックします。



5. DNS サーバーが登録されます。
[仮想ネットワーク]をクリックします。



6. [tokyo-nw]をクリックします。

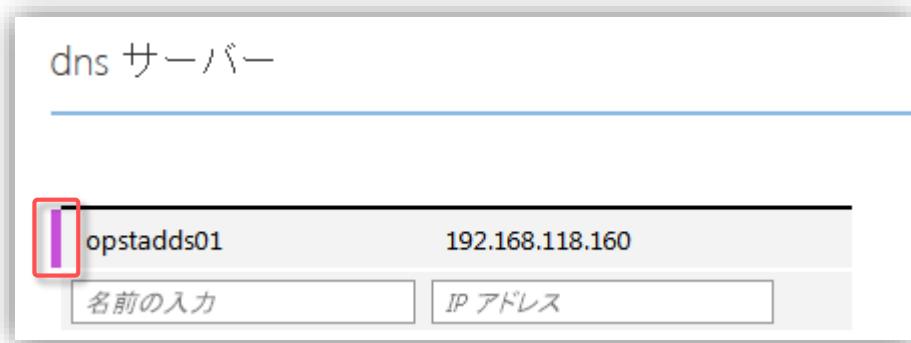


7. [構成]をクリックします。

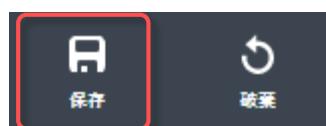


8. 先ほど登録した DNS サーバーをプルダウンから選択して行きます。

変更等が入った箇所の DNS サーバー(AD DS)名の左に紫のバーが表示されます。今回は 1 つ新規に追加したため下記のように表示されています。

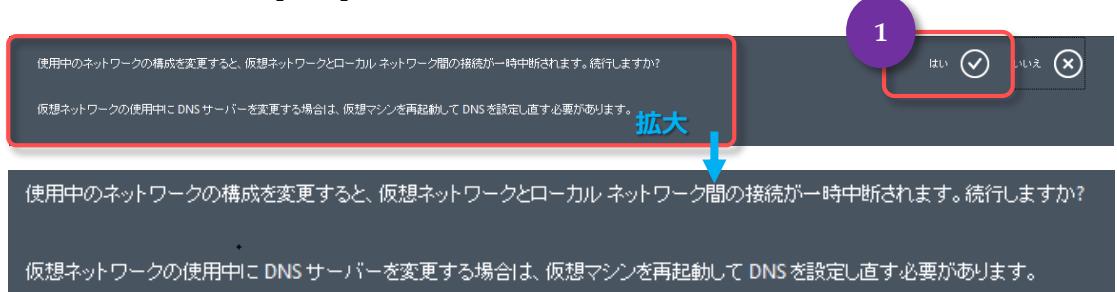


9. 画面下の[保存]をクリックします。



企業内システムと Microsoft Azure の VPN 接続、Active Directory 連携

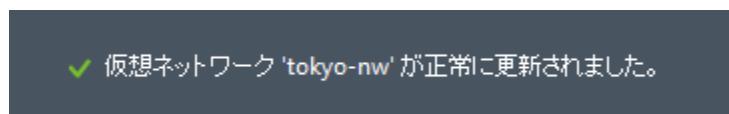
10. DNS サーバーの設定を変更する際、一時的にネットワークが切断されることがあるため、その警告が表示されます。[はい]をクリックします。



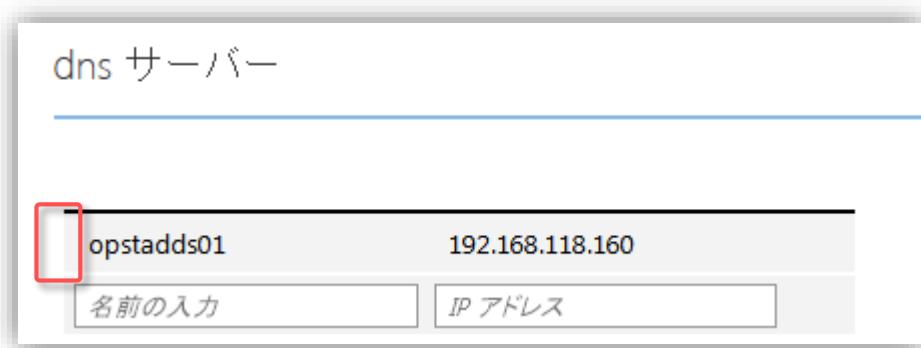
11. 更新中です。



12. 更新完了です。



13. 設定が確定すると、各 DNS サーバー(AD DS)名の左に表示されていた紫のバーが消えます。



以上で仮想ネットワーク上の DNS サーバーの作成及び DHCP による DNS サーバーの IP 払い出しの設定が完了となります。

5.3 仮想マシンの作成

Azure 上の 1 台目の AD DS 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、左のメニューから[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。



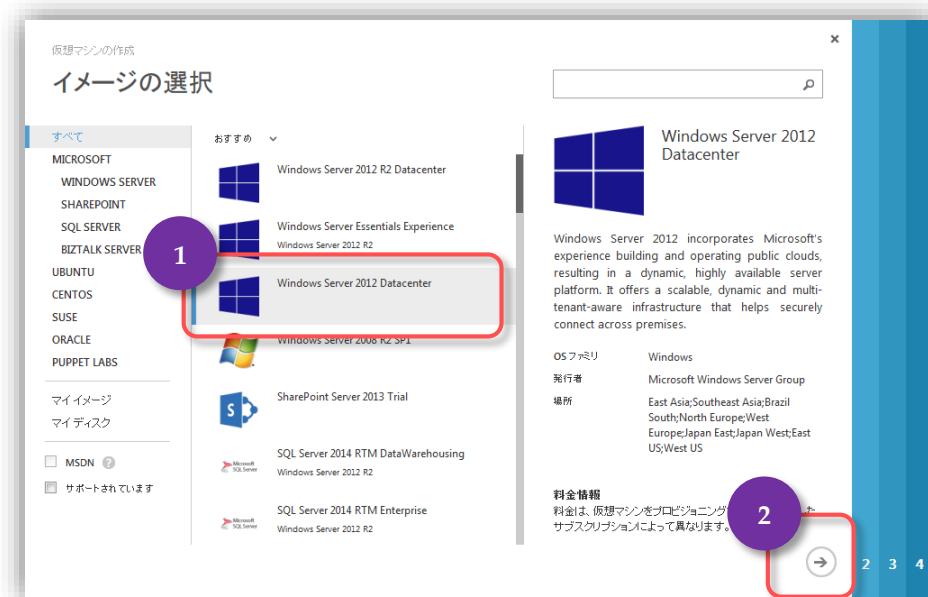
企業内システムと Microsoft Azure の VPN 接続、Active Directory 連携

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。



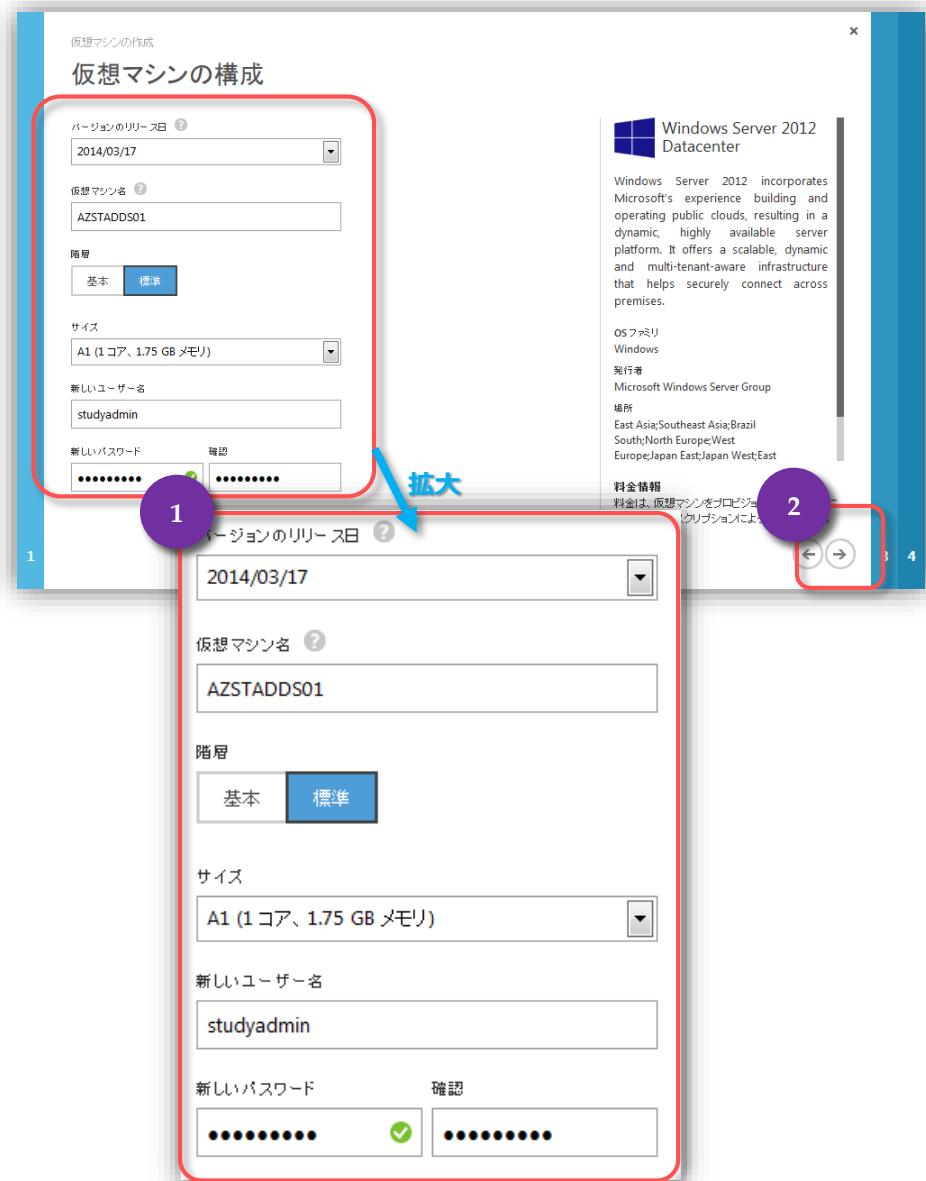
3. インストールする OS[Windows Server 2012 Datacenter]を選択し[+]をクリックします。



企業内システムと Microsoft Azure の VPN 接続、Active Directory 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ため、作成時点の最新の日付を選択します)、[仮想マシン名]に「**AZSTADD501**」(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、[**⊕**]をクリックします。



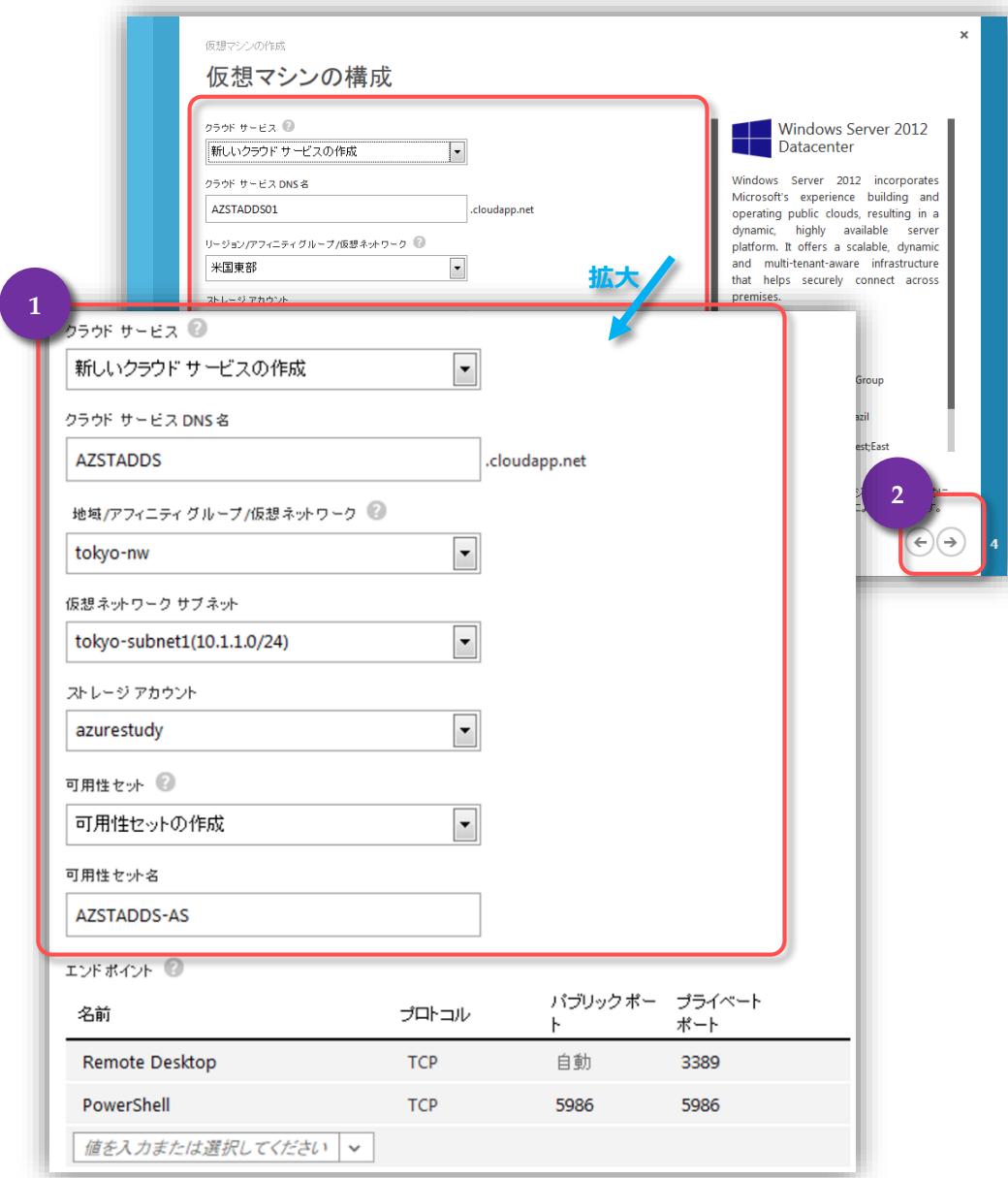
企業内システムと Microsoft Azure の VPN 接続、Active Directory 連携

| 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、単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。 |
| 標準(標準コンピューティング レベル) | <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。 |
| 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。 尚、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、Active Directory 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「AZSTADDS」(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「tokyo-nw」(事前に作成した仮想ネットワーク名)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「可用性セットの作成」を選択、[可用性セット名]に「AZSTADDS-AS」(任意の文字列)を入力し、[④] をクリックします。

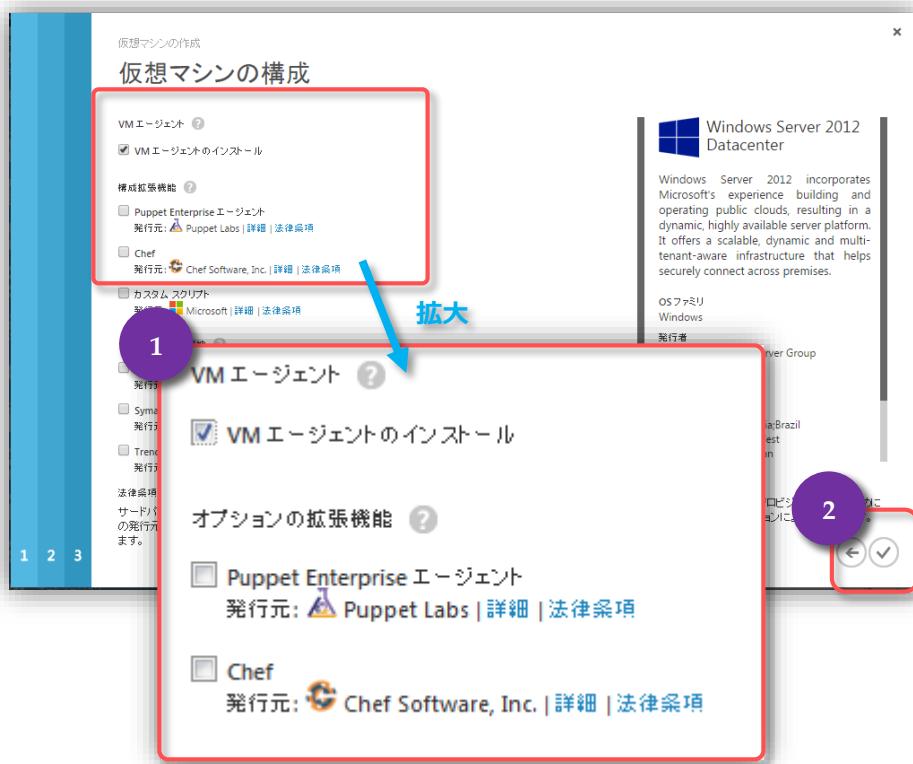


| 項目 | 説明 |
|-------------------------------|--|
| クラウドサービス | <ul style="list-style-type: none"> ・ クラウドサービスを選択します。 <p>クラウドサービスとは、1つまたは複数の仮想マシンを配置する箱を意味します。同じクラウド サービス内に複数の仮想マシンを作成すると、仮想マシンの相互通信、仮想マシン間での負荷分散、仮想マシンの高可用性を実現できます。</p> <p>先にクラウドサービスを作成している場合に選択できます。また、既存のクラウドサービスが存在しない、もしくは選択しなかった(「新しいクラウドサービスの作成」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>「地域/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 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出来ます。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、Active Directory 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、[?]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 Enterprise エージェント | <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。 |
| 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 Endpoint Protection | <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。 |
| Trend Micro Deep Security Agent | <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。 |

7. 仮想マシンが作成されると[状態]が[実行中]になります。



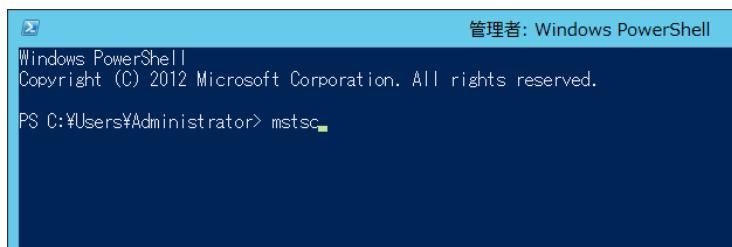
以上で仮想マシンの作成が完了となります。

5.4 仮想マシンへのリモートデスクトップ接続

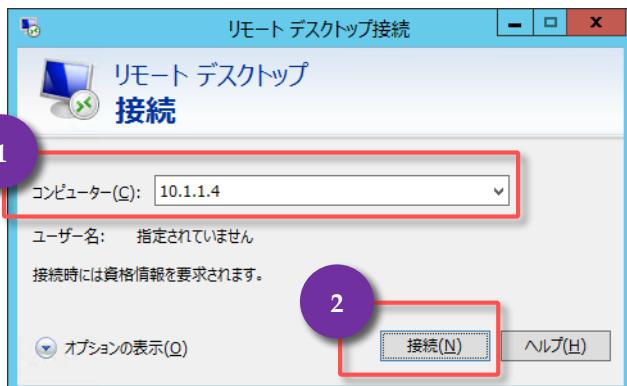
オンプレミス上の端末から作成した仮想マシンにリモートデスクトップを使って接続します。Azure で作成した仮想マシンはデフォルトでリモートデスクトップ接続が有効になっています。

- PowerShell もしくはコマンドプロンプトを起動し、以下のコマンドを入力し、「Enter」キーを入力します。

```
mstsc
```



- [コンピューター]に「10.1.1.4」(仮想マシンの内部 IP アドレス)と入力し[接続]をクリックします。



Note : 仮想マシンの IP アドレスは DHCP で払い出される

Azure 上の仮想マシンには基本的に DHCP で払い出されます。

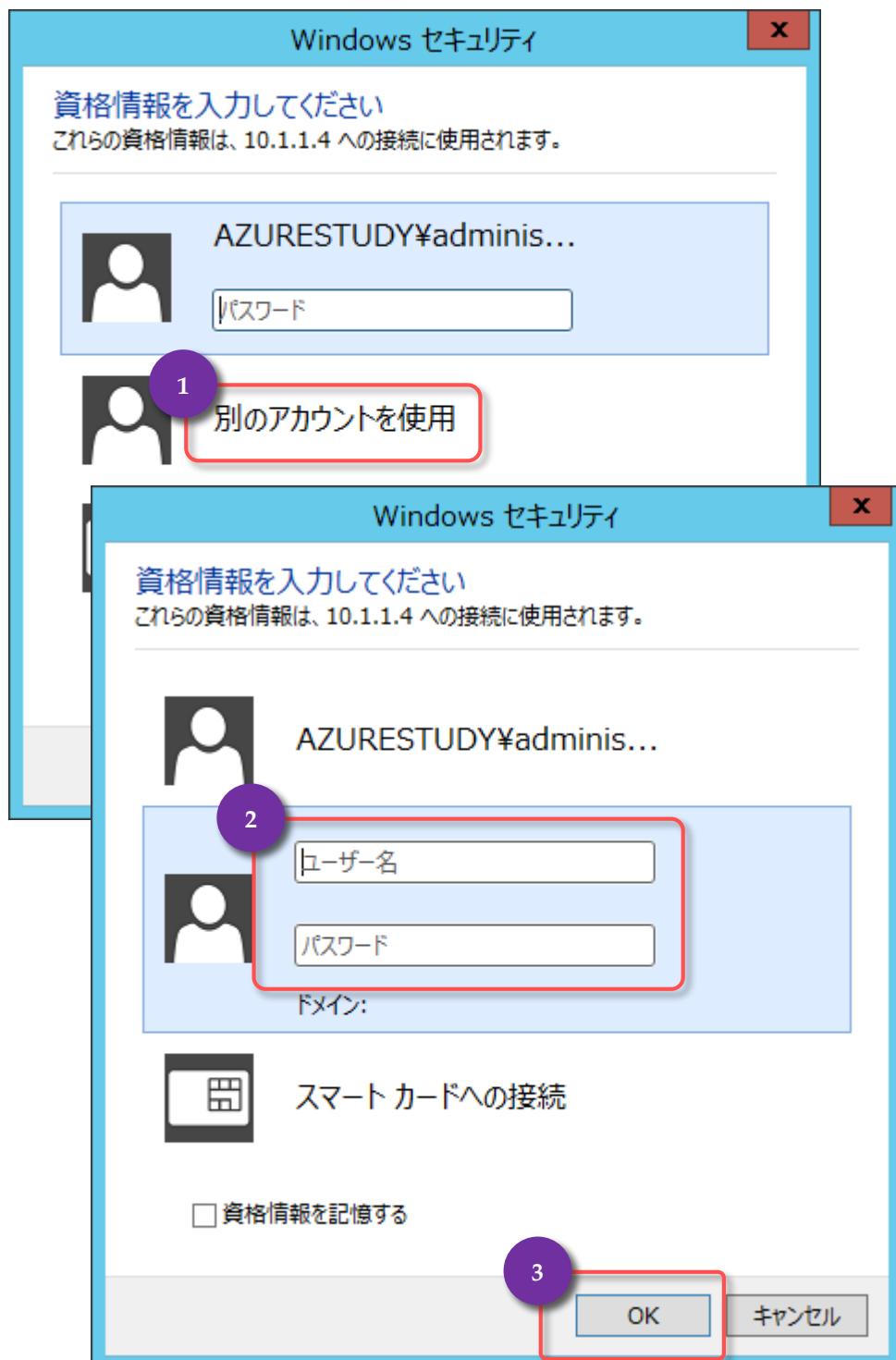
| | | |
|------------------------------|---|---|
| IPv4 Address | : | 10.1.1.4 (Preferred) |
| Subnet Mask | : | 255.255.255.0 |
| Lease Obtained | : | 2014/04/22 10:56:05 |
| Lease Expires | : | 215005/29 17:34:03 |
| Default Gateway | : | 10.1.1.1 |
| DHCP Server | : | 168.63.129.16 |
| DHCPv6 IAID | : | 251663709 |
| DHCPv6 Client DUID | : | 00-01-00-01-1A-E6-85-B8-00-15-5D-90-40-C8 |
| DNS Servers | : | 10.1.1.4 |

また、IP アドレスが分からなくなったら場合には、Azure の管理ポータルから[仮想マシン]→「対象の仮想マシン名」をクリックし[ダッシュボード]をクリックします。切り替わった画面右側の[概要]でも確認できます。

内部 IP アドレス

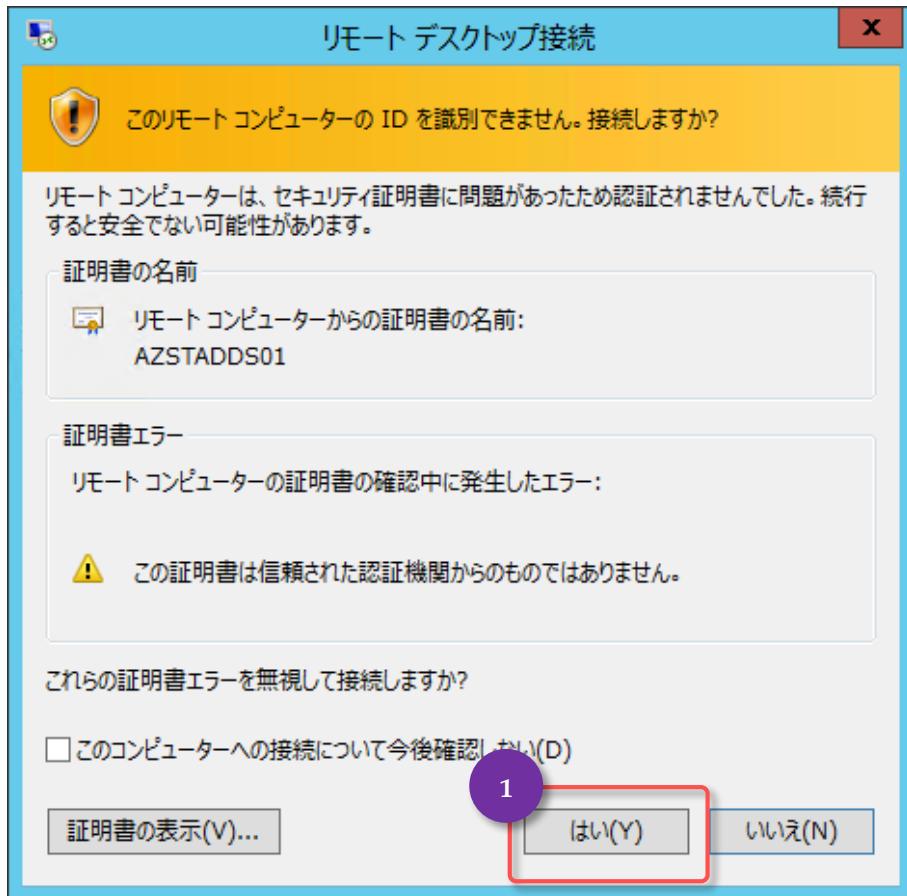
10.1.1.4

3. [別のアカウントを使用]をクリックし、[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。

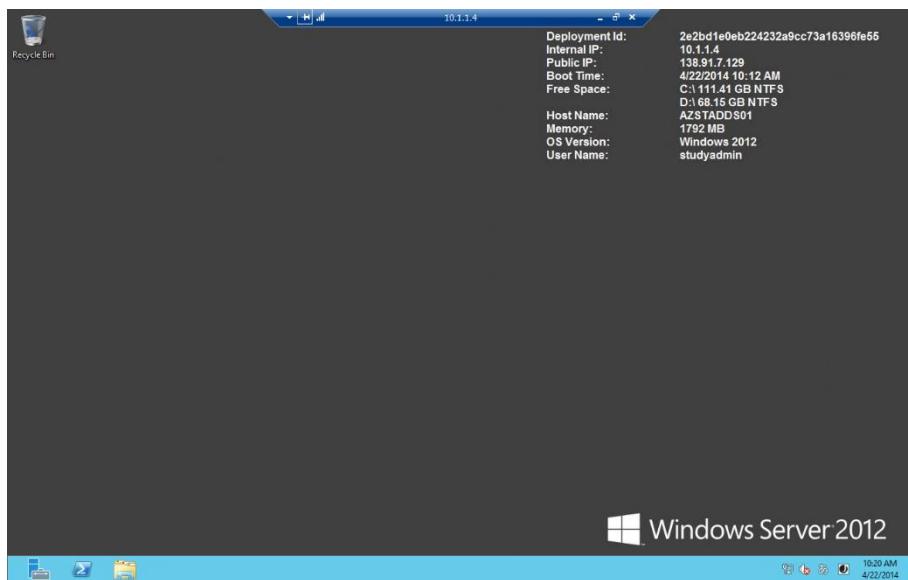


企業内システムと Microsoft Azure の VPN 接続、Active Directory 連携

4. 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] ボタンをクリックします。



5. 仮想マシンに接続されます。

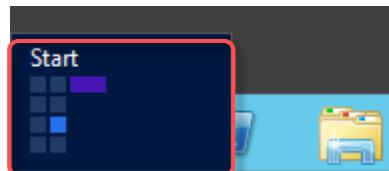


以上でリモートデスクトップを使った仮想マシンへの接続が完了となります。

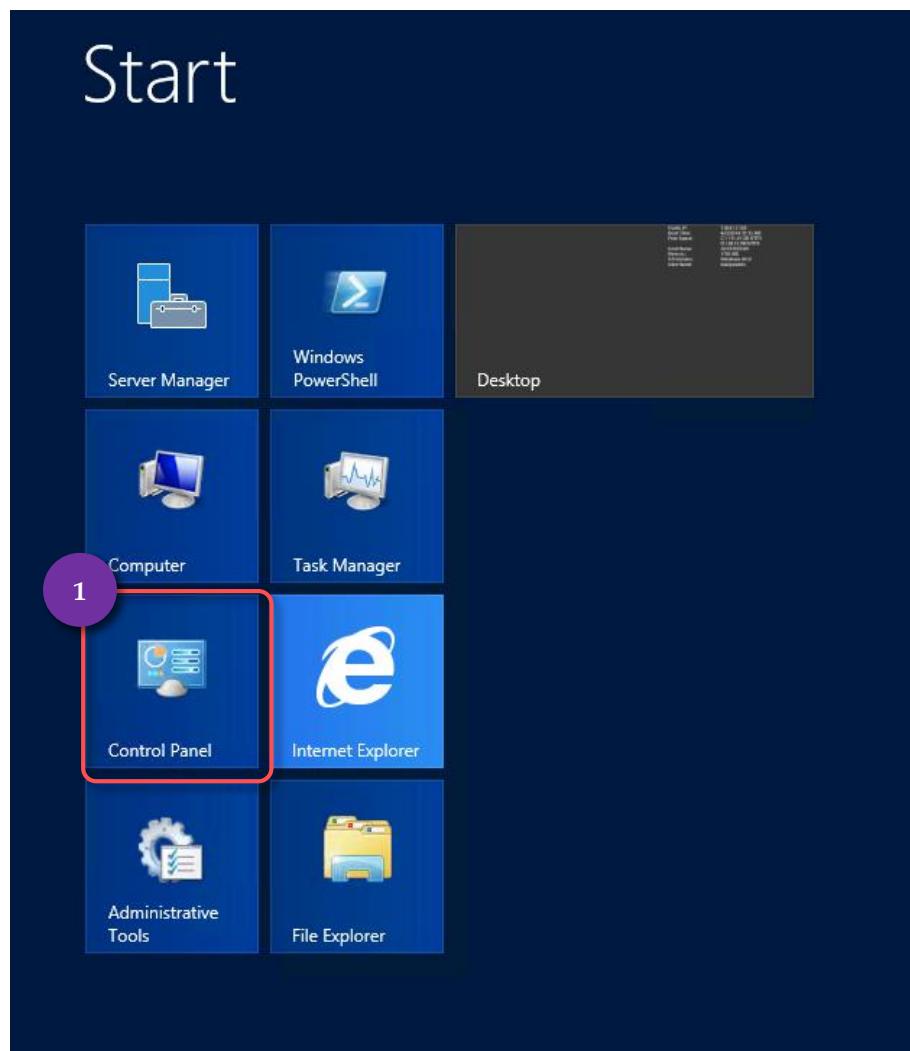
5.5 日本語化

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。

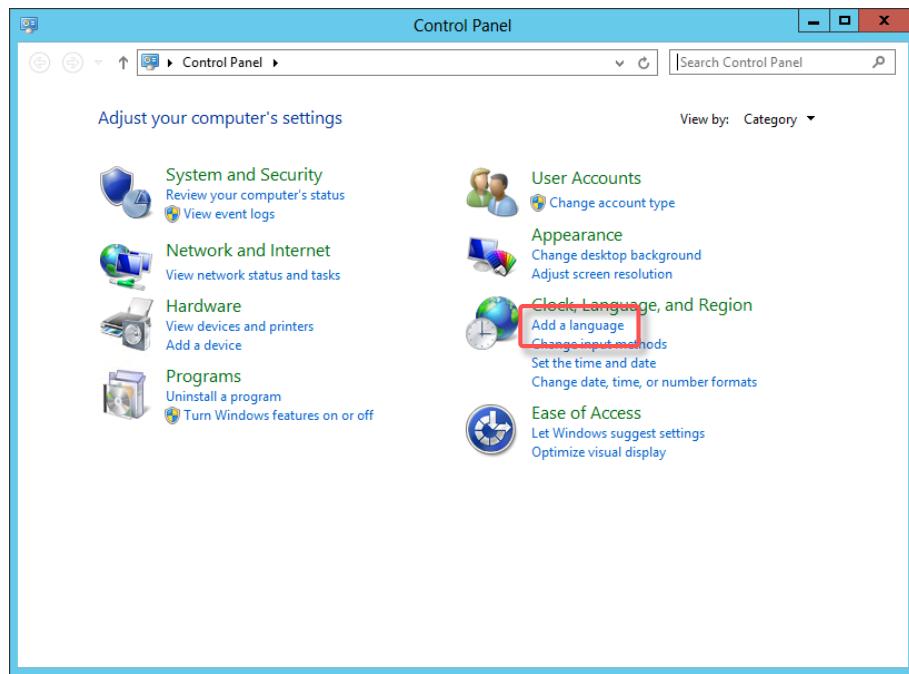


2. [Control Panel]をクリックします。

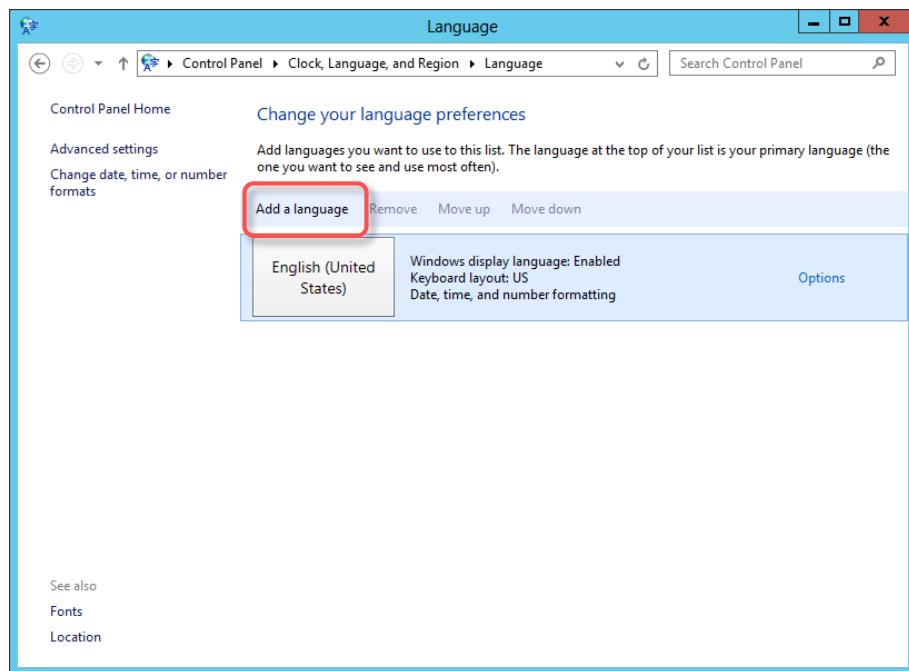


企業内システムと Microsoft Azure の VPN 接続、Active Directory 連携

3. [Add a language]をクリックします。

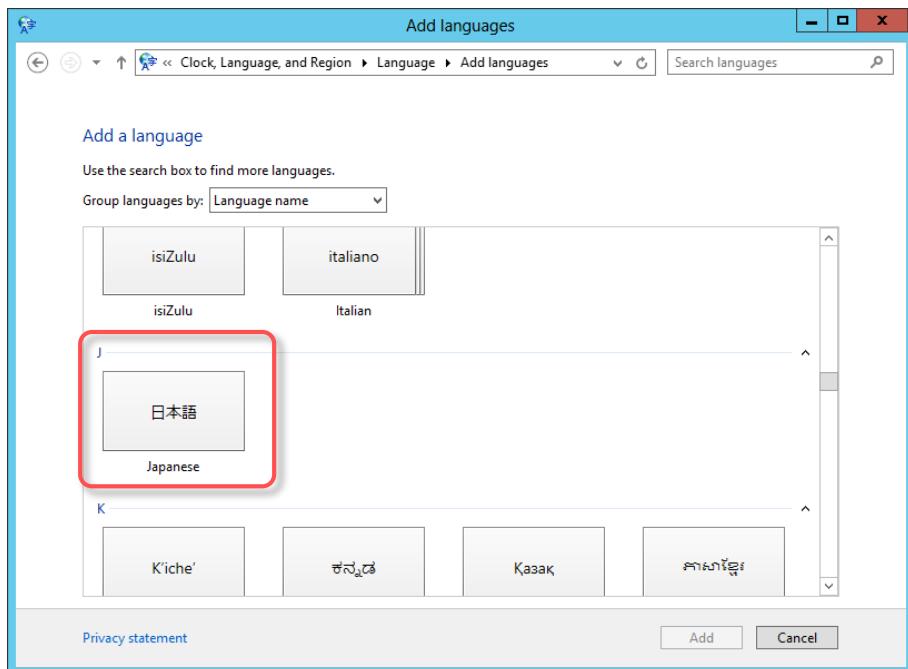


4. [Add a language]をクリックします。

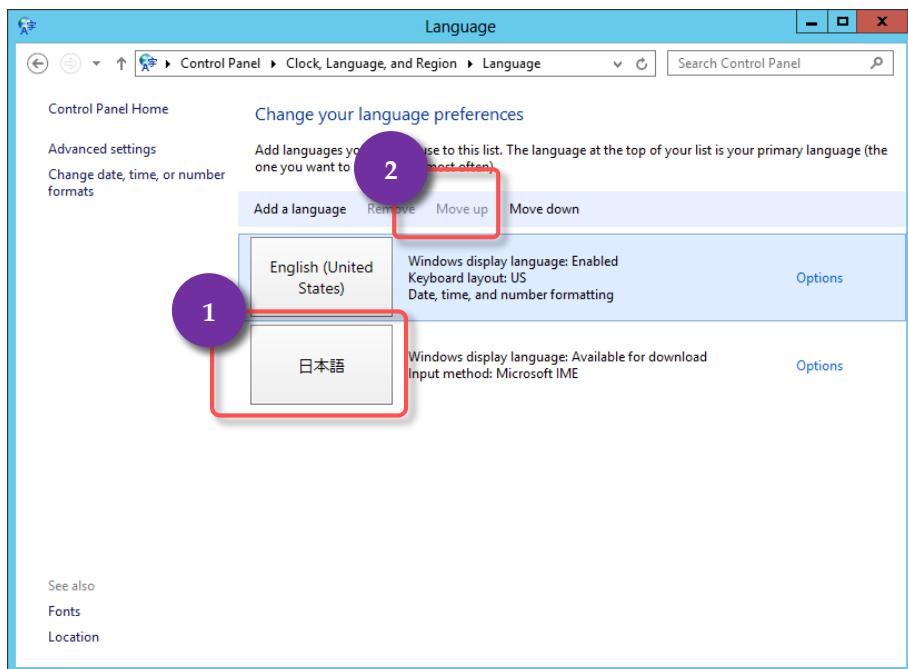


企業内システムと Microsoft Azure の VPN 接続、Active Directory 連携

5. [日本語]をクリックします。

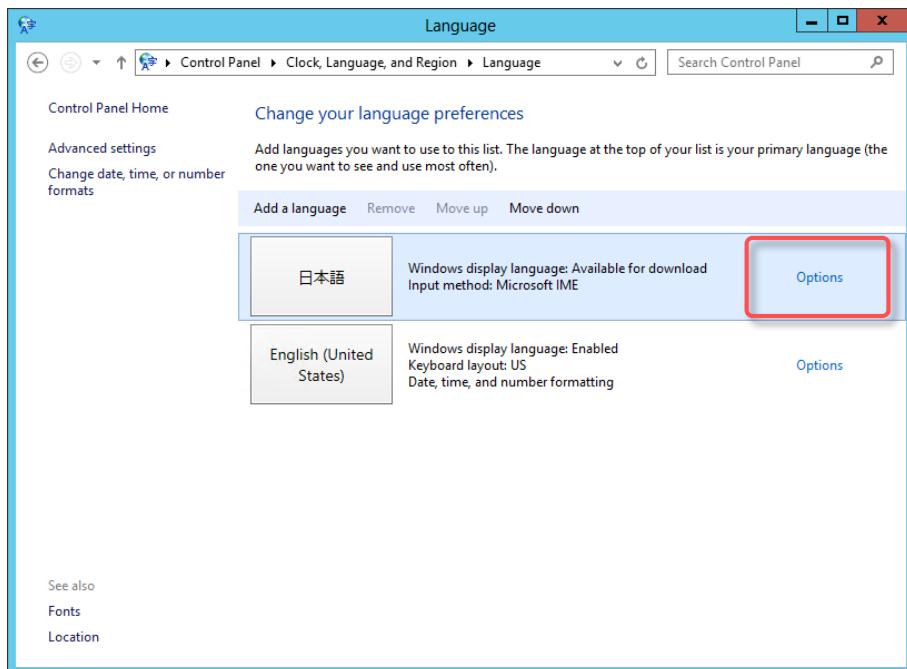


6. [日本語]を選択し[Move up]をクリックします。

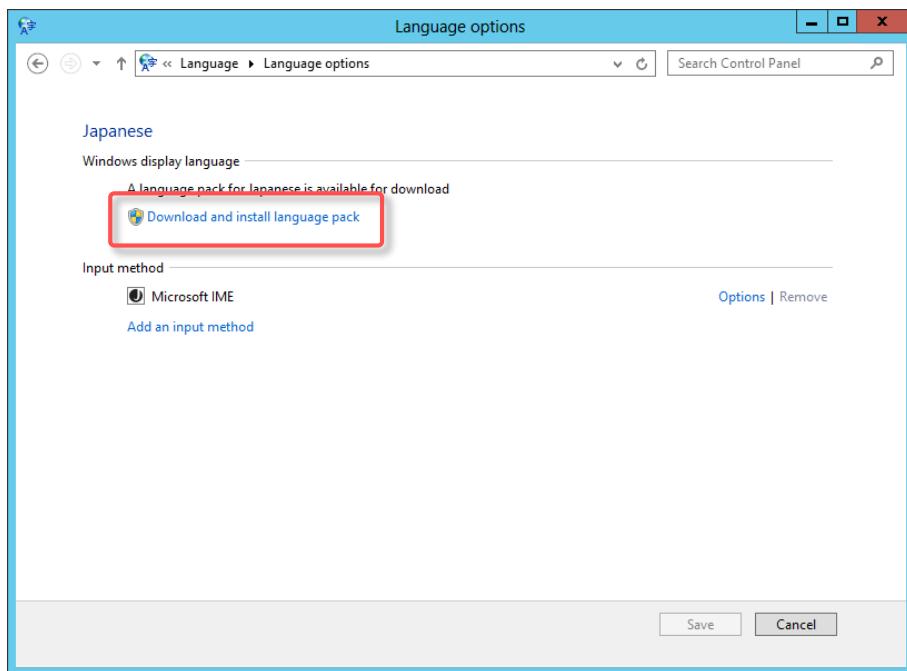


企業内システムと Microsoft Azure の VPN 接続、Active Directory 連携

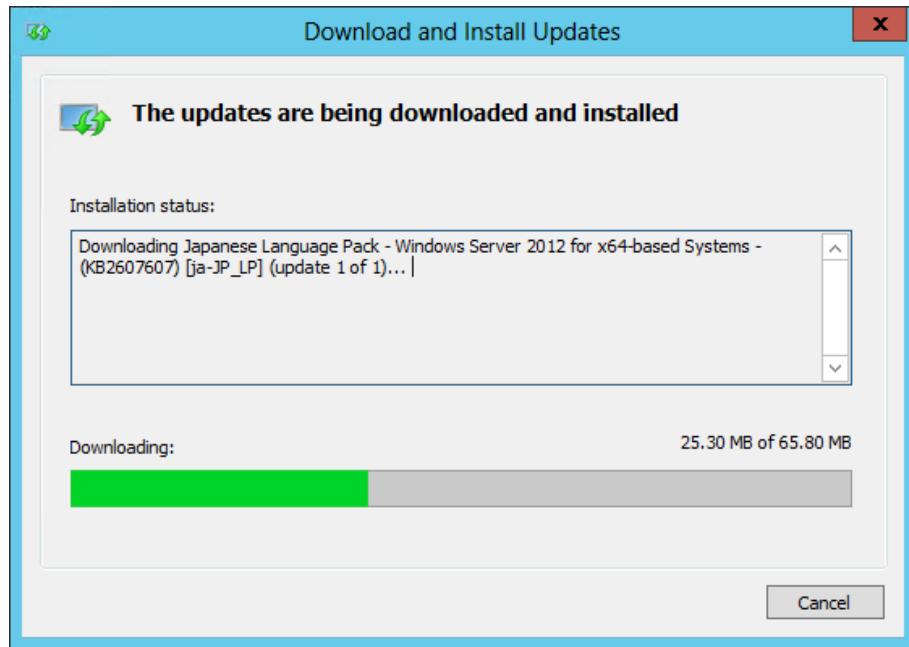
7. [Options]をクリックします。



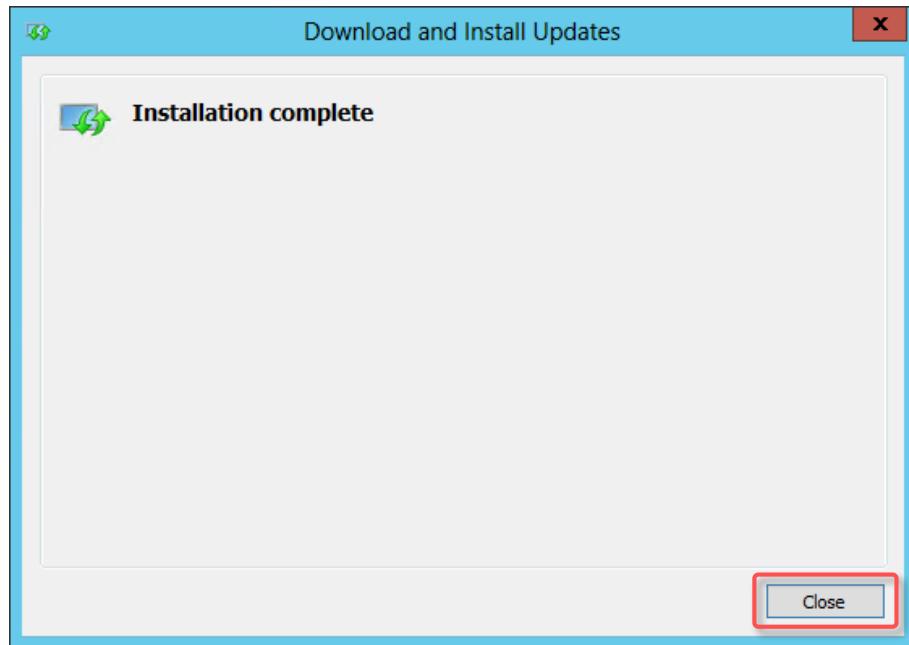
8. [Download and install language pack]をクリックします。



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. [Close]をクリックします。



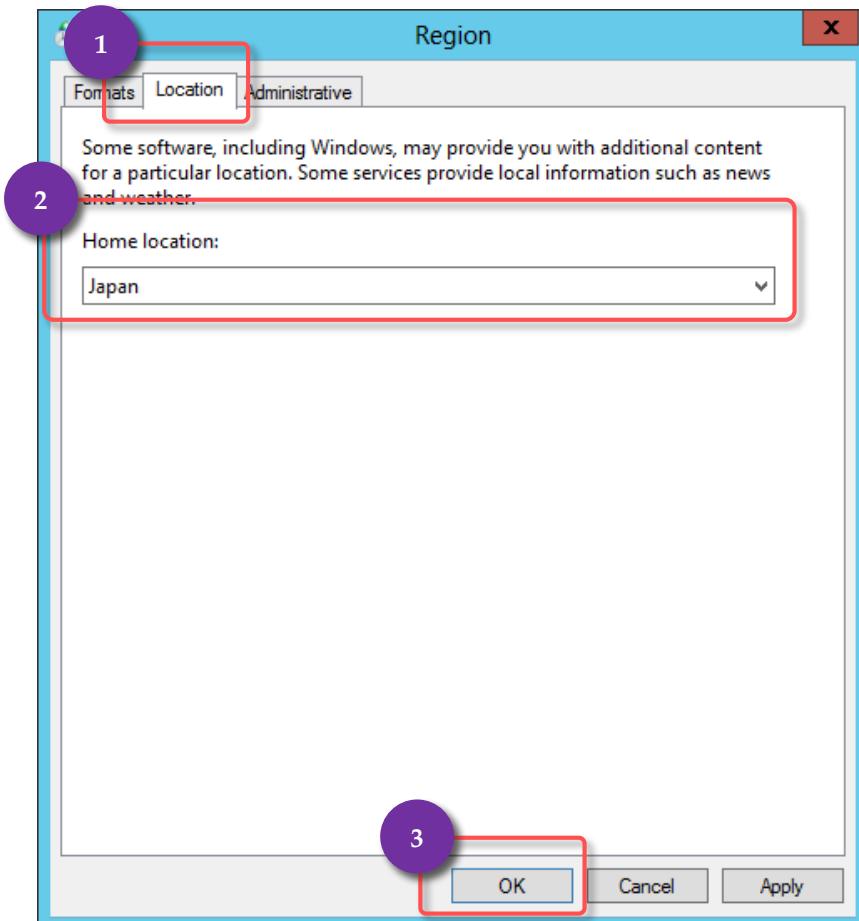
企業内システムと Microsoft Azure の VPN 接続、Active Directory 連携

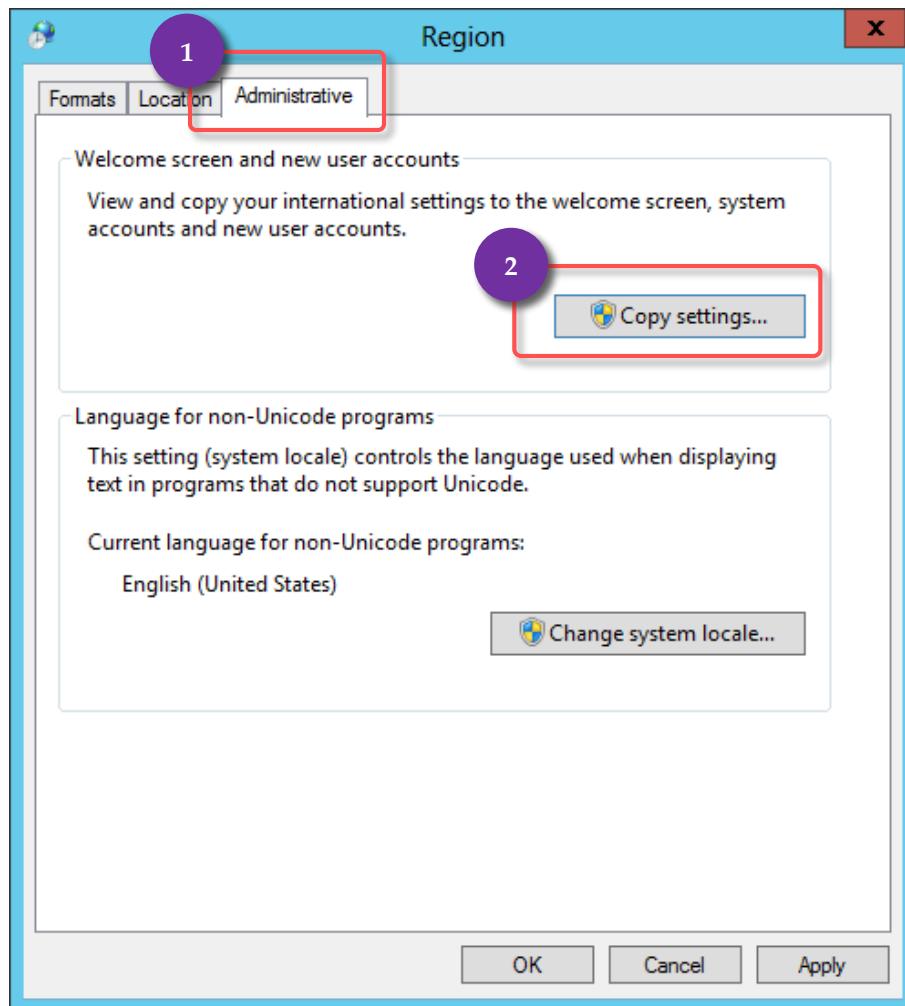
11. 場所(Location)を変更し、サインイン画面の日本語化や PowerShell やコマンドプロンプトで日本語が使えるように設定を変更します。

[Language] ウィンドウの[Location]をクリックします。

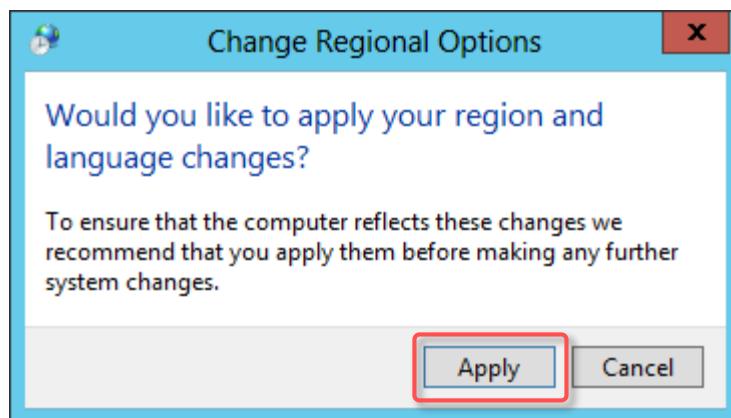


12. [Location]を開き[Home location]のプルダウンメニューから[Japan]を選択し[OK]をクリックします。



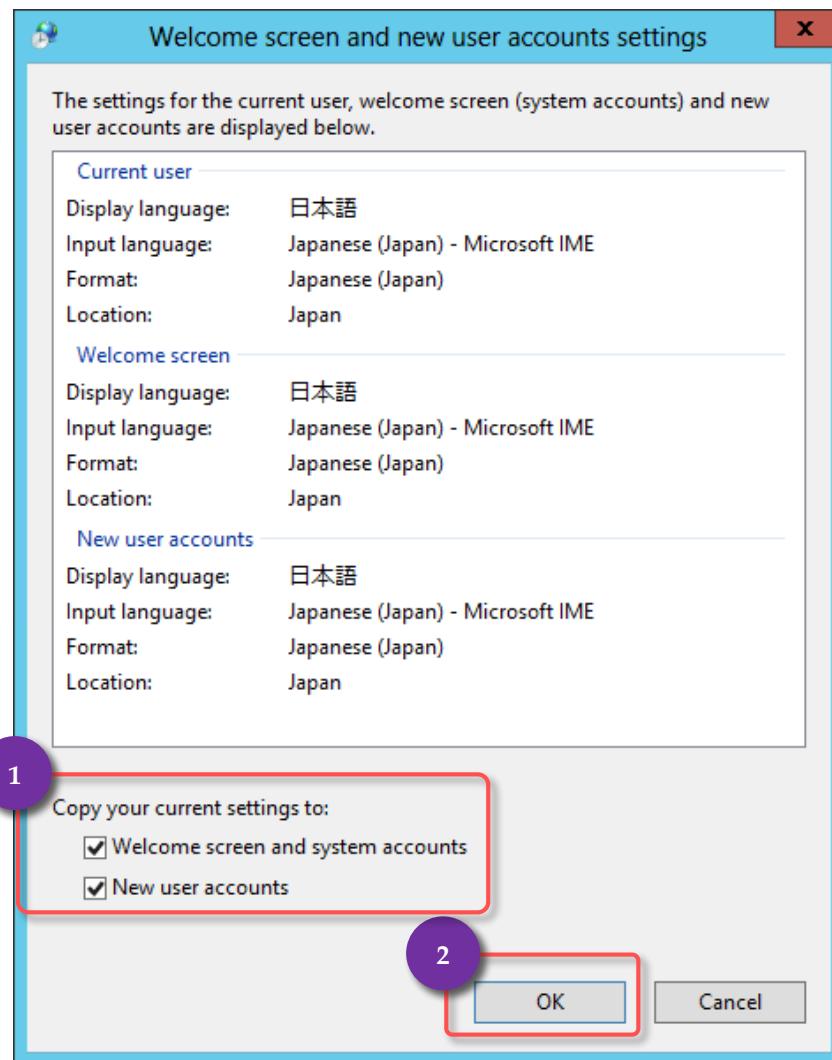
13. [Administrative]を開き、[Copy settings]をクリックします。**14. 場所と言語の変更を適用するか確認のウィンドウが開きます。**

[Apply]をクリックします。

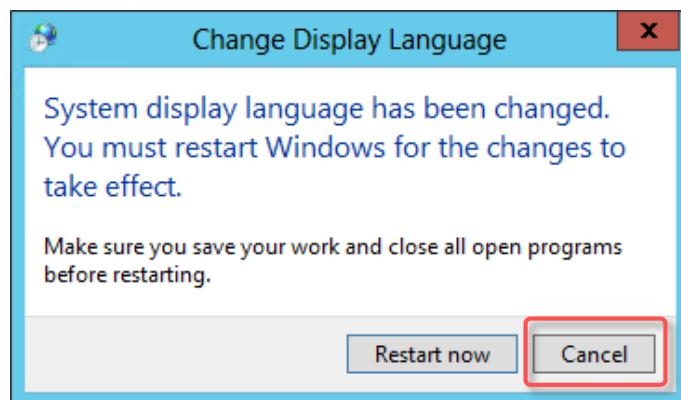


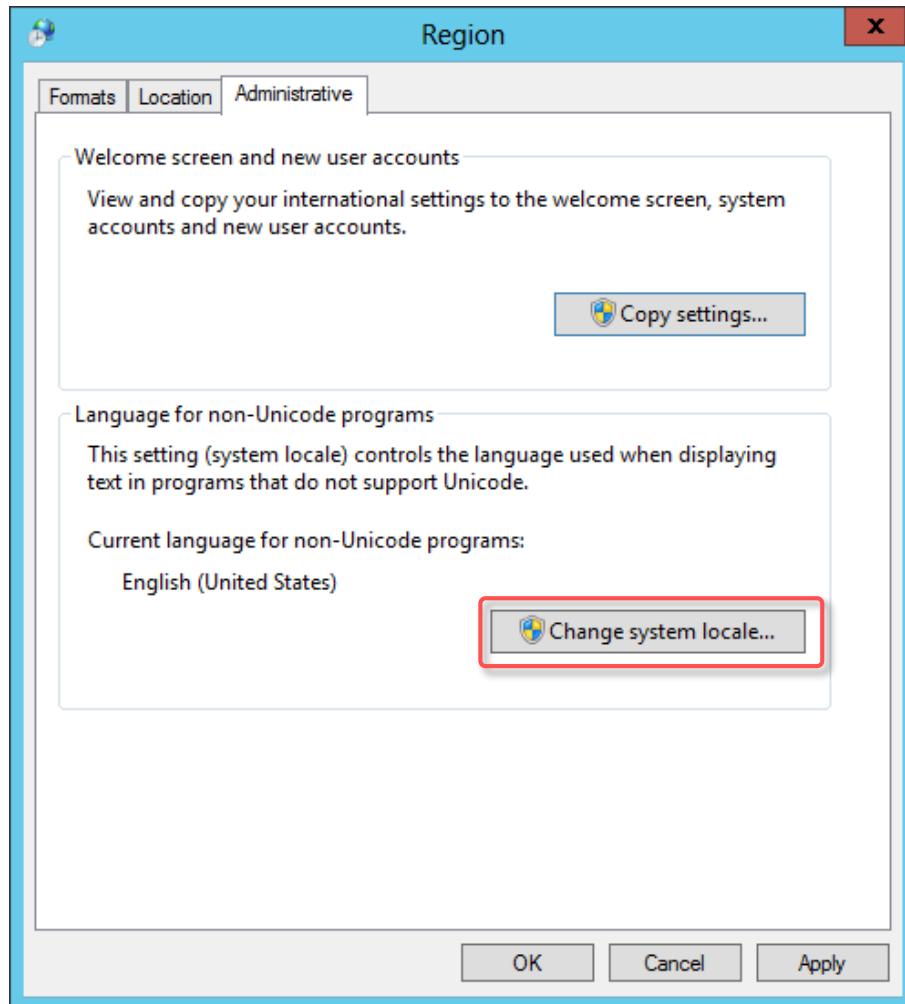
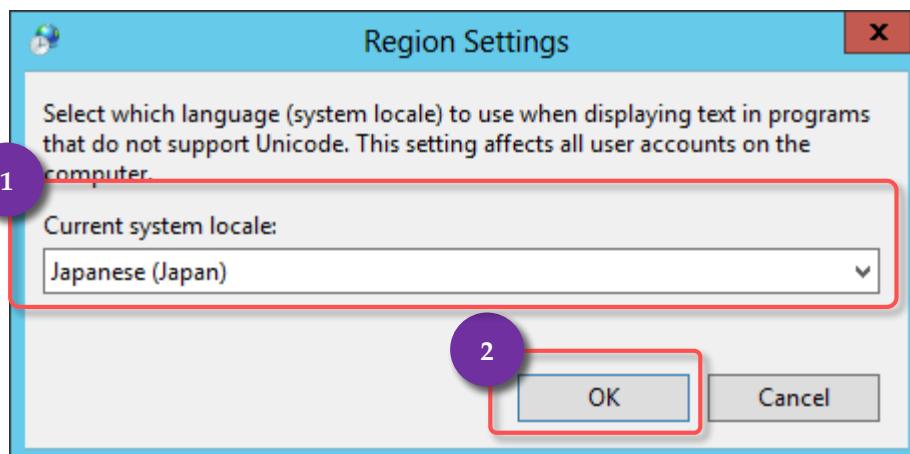
企業内システムと Microsoft Azure の VPN 接続、Active Directory 連携

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。



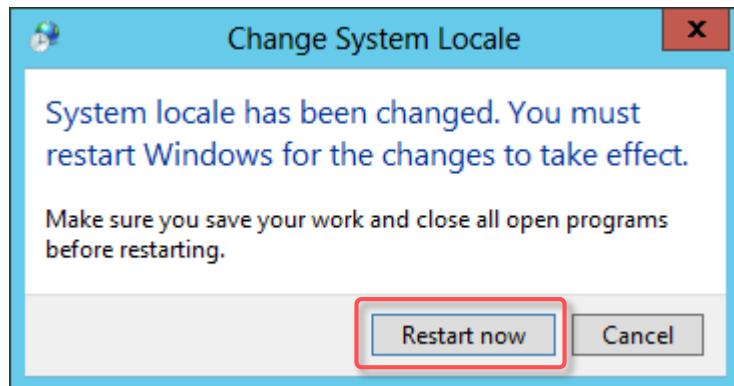
16. 再起動を薦めるウィンドウが表示されますが、続けて作業を行うため[Cancel]をクリックします。



17. [Change system locale]をクリックします。**18. [Current system local:]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。



以上で仮想マシンの日本語化が完了となります。

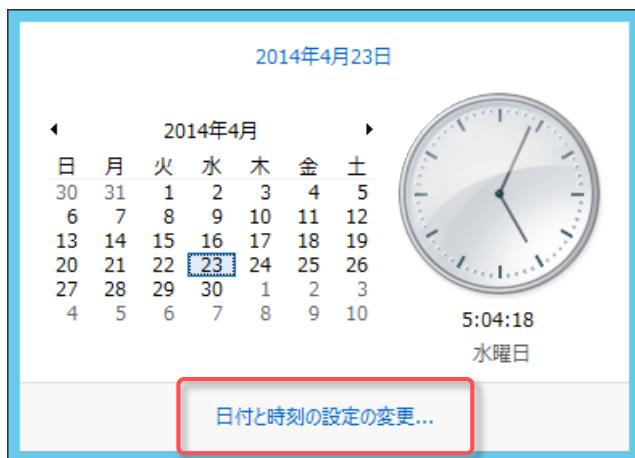
5.6 タイムゾーン

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。

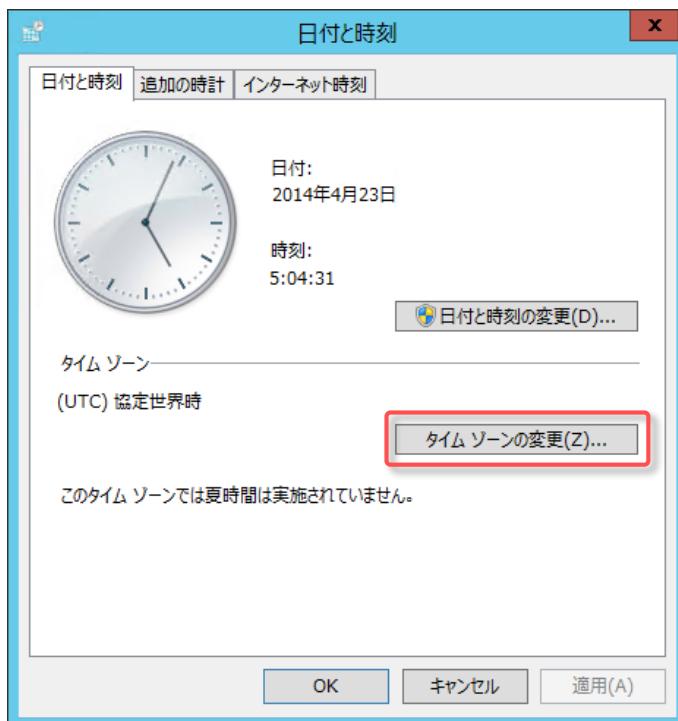
1. デスクトップ画面右下の時計をクリックします。



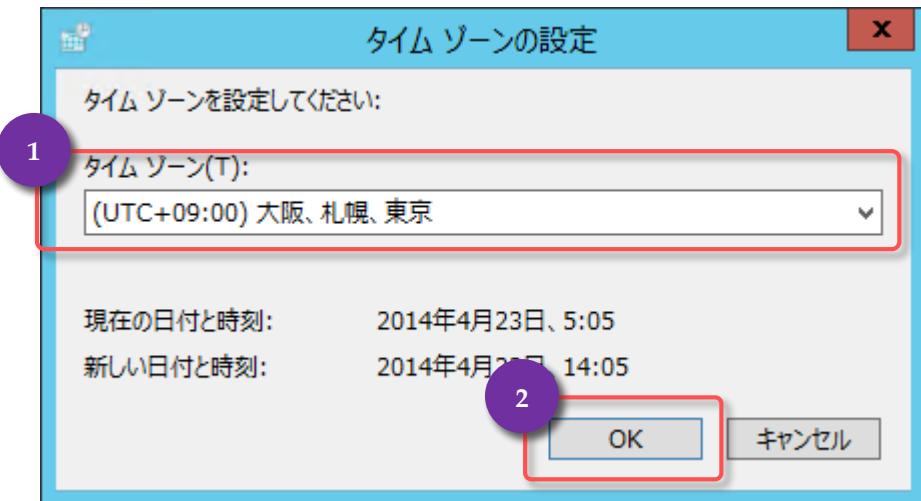
2. [日付と時刻の設定の変更]をクリックします。



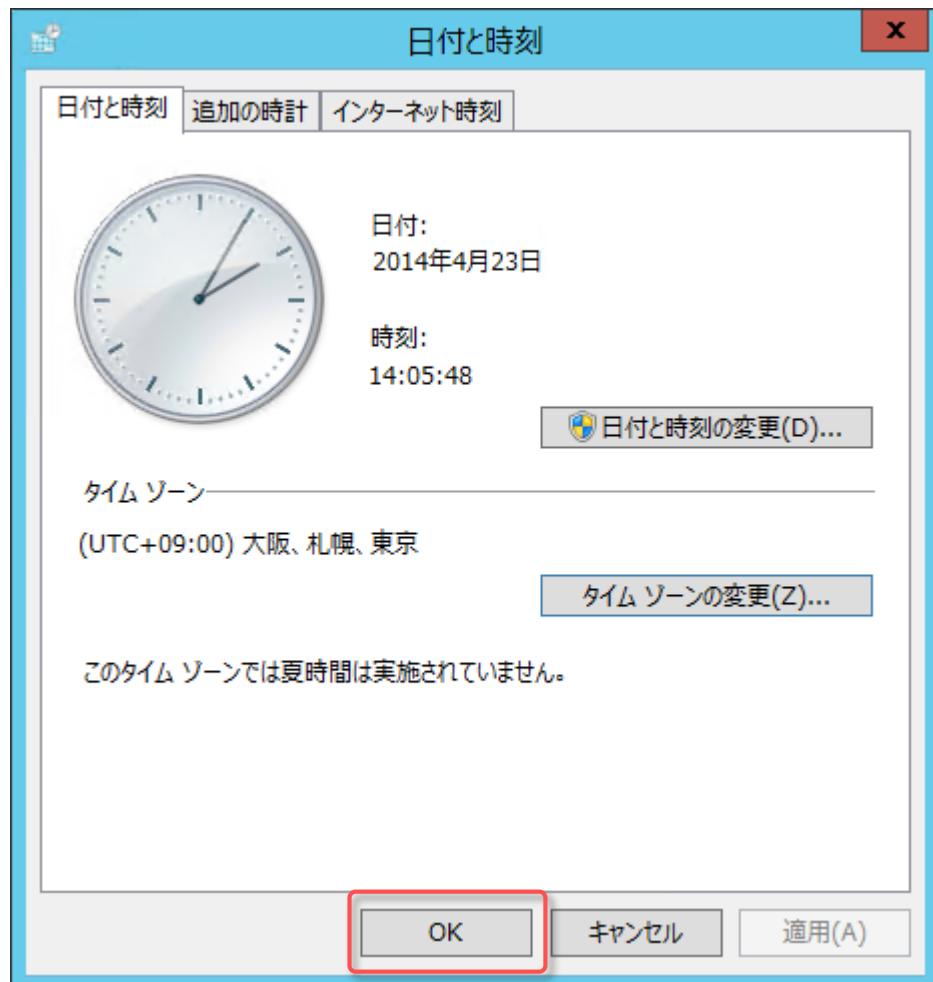
3. [タイムゾーンの変更]をクリックします。



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。



以上でタイムゾーンの変更が完了となります。

5.7 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、Windows Update が自動で実行されないように設定します。これにより、Windows Update 後の自動再起動を抑止させます。ただし、セキュリティの観点から定期的にアップデートを行うことは重要です。必ず運用での対応を考慮してください。

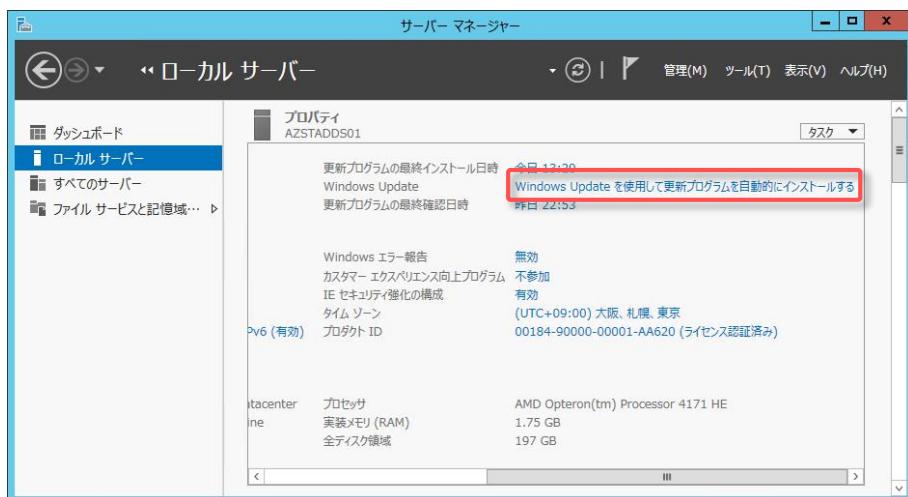
1. デスクトップ画面左下の[サーバー マネージャー]をクリックします。



2. [ローカル サーバー]をクリックします。

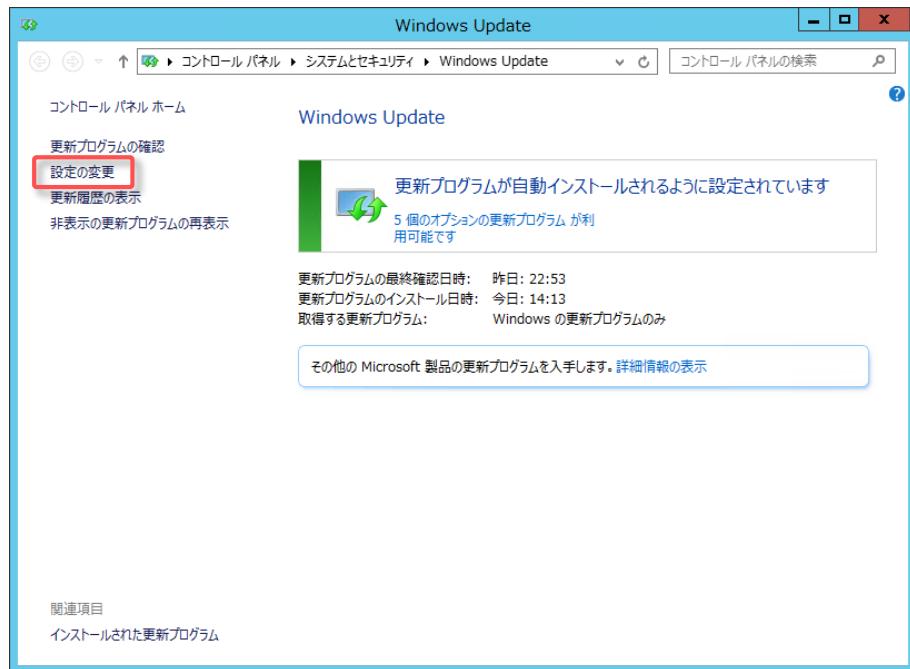


3. 画面をスクロールし[Windows Update を使用して更新プログラムを自動的にインストールする]をクリックします。

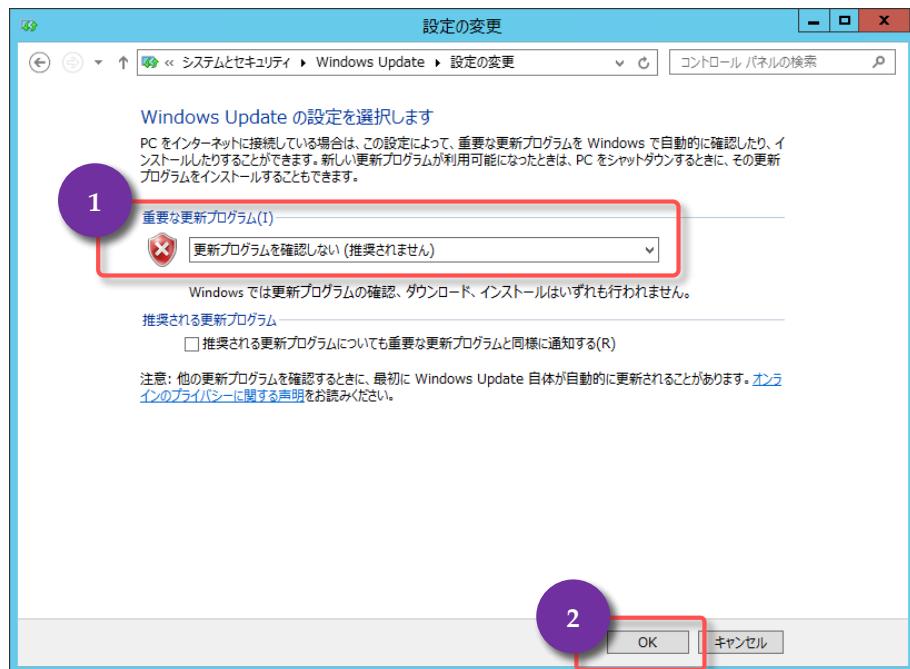


企業内システムと Microsoft Azure の VPN 接続、Active Directory 連携

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、更新プログラムが特にならない場合には[設定の変更]をクリックします。

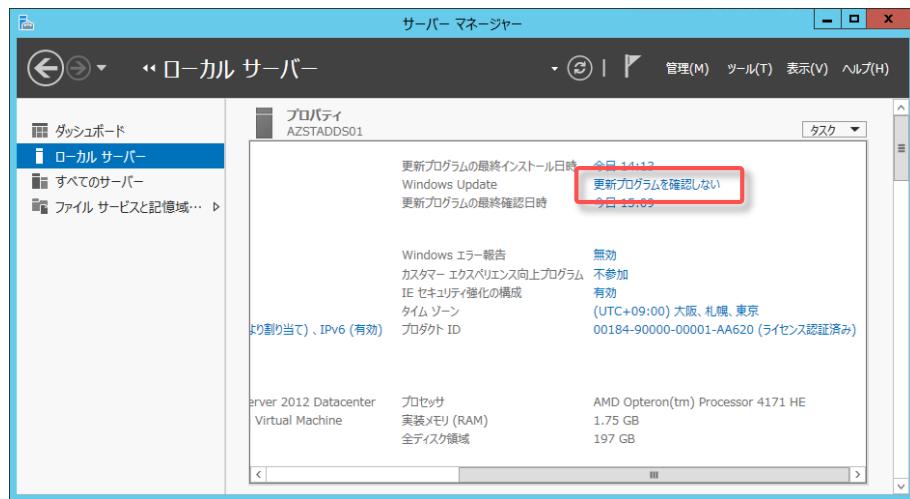


5. [重要な更新プログラム]のプルダウンから[更新プログラムを確認しない(推奨されません)]を選択し、[OK]をクリックします。



企業内システムと Microsoft Azure の VPN 接続、Active Directory 連携

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。



以上で Windows Update の設定が完了となります。

Note : Windows Update について

尚、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。

5.8 ディスクの追加

◆ Azure 管理ポータルの作成と追加

Azure 管理ポータルにて BLOB ストレージの作成と追加を行います。

AD DS のデータベース、ログファイル、SYSVOL を格納するために使用します。

これは既定で作成される OS 用の C ドライブはディスクキャッシュ機能が有効になっており、AD DS のデータベース、ログファイル、SYSVOL を格納するには適していないためです。

1. ポータルサイトの[仮想マシン]をクリックし対象の仮想マシン([AZSTADDS01])を選択します。



2. ポータルサイト下の[ディスクの接続]をクリックし[空のディスクの接続]をクリックします。



3. [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。 尚、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が推奨されます。 |
| 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が、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。 |

4. 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。
追加が完了すると[実行中]になります。



以上でディスクの作成と仮想マシンへの追加が完了となります。

◆ 仮想マシンで追加したディスクのフォーマット

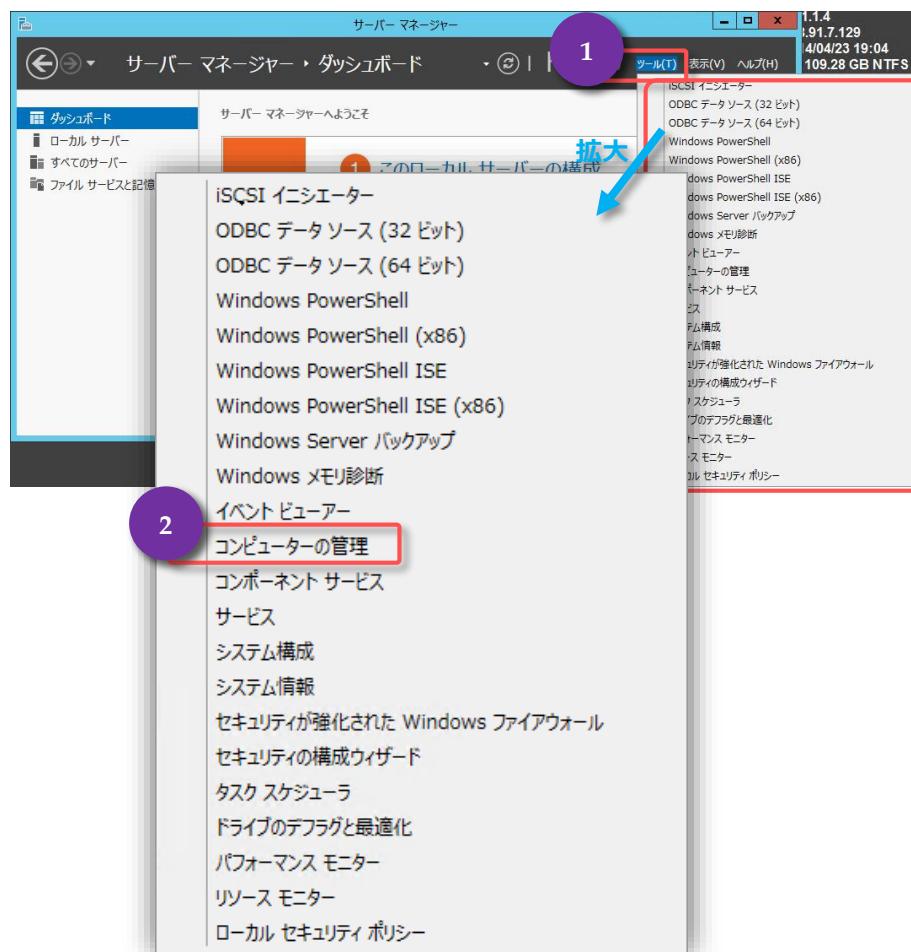
ディスクは Azure のポータルで追加しただけでは使用できません。追加したディスクを仮想マシン上でフォーマットし、仮想マシンで利用できるようにします。

- リモートデスクトップで仮想マシン(AZSTADDS01)に接続(「[仮想マシンへのリモートデスクトップ接続](#)」参照)します。

- 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。

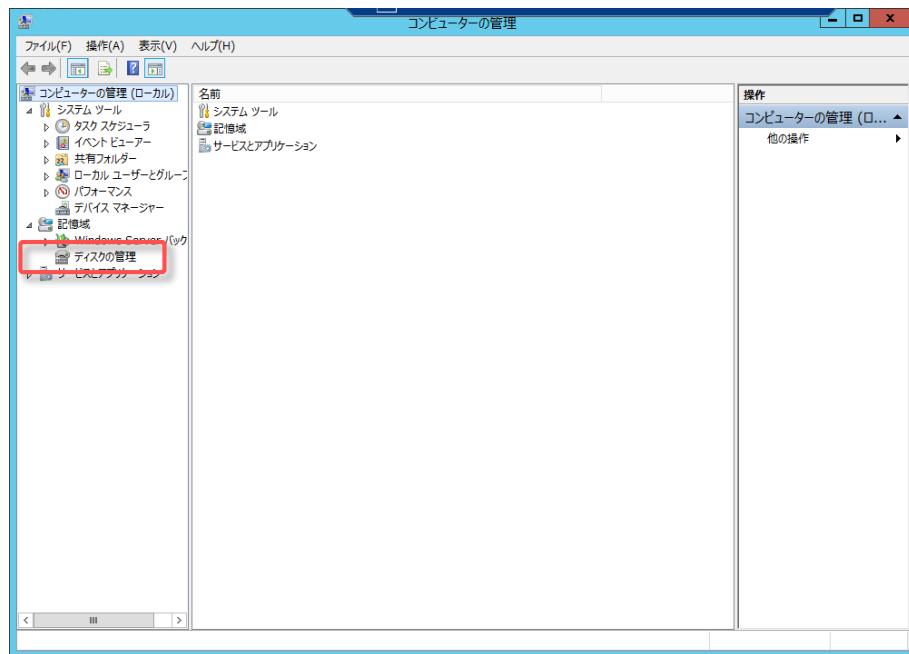


- [ツール]をクリックし[コンピューターの管理]をクリックします。



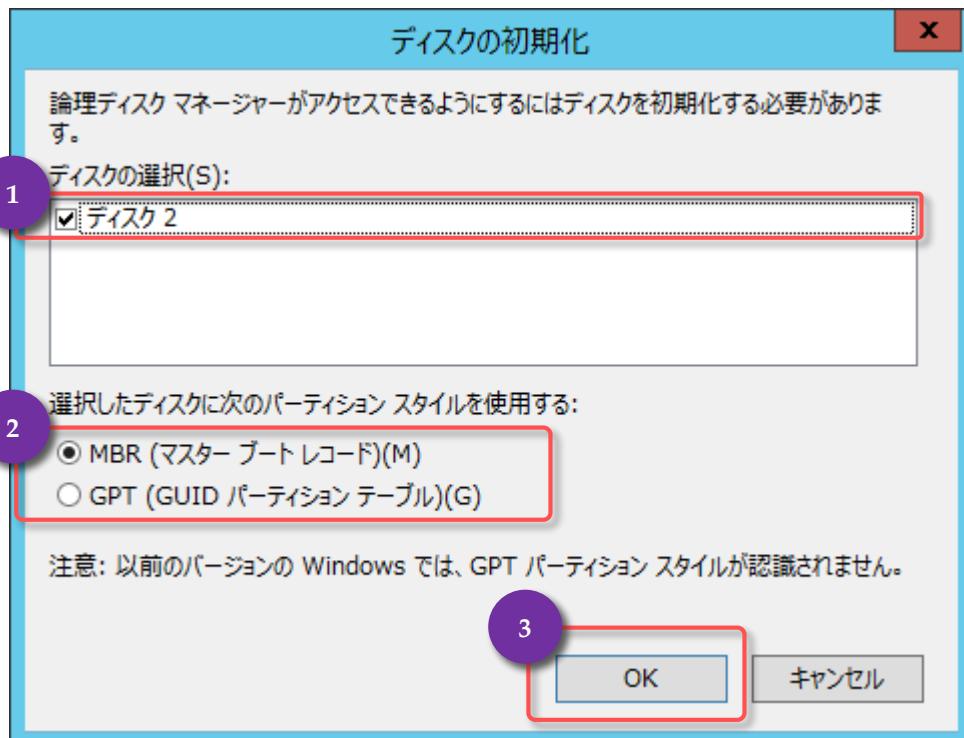
企業内システムと Microsoft Azure の VPN 接続、Active Directory 連携

4. [ディスクの管理]をクリックします。



5. [ディスク 2]にチェックが付いていることを確認します。

[MBR](任意のスタイル)を選択し[OK]をクリックします。

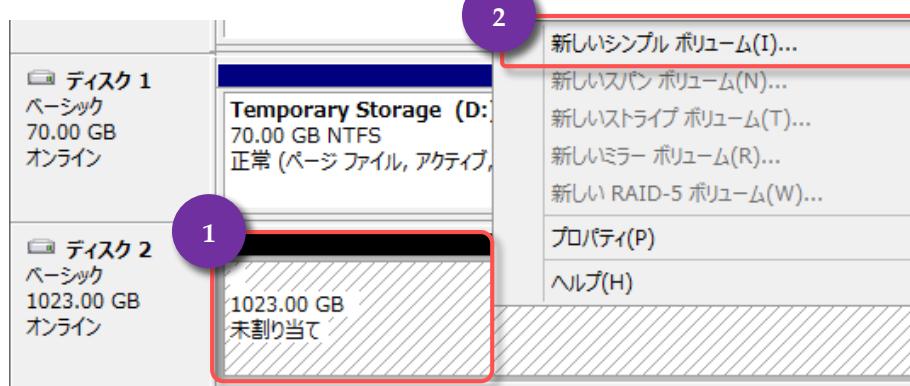


企業内システムと Microsoft Azure の VPN 接続、Active Directory 連携

6. 追加したディスクが認識されていることを確認します。

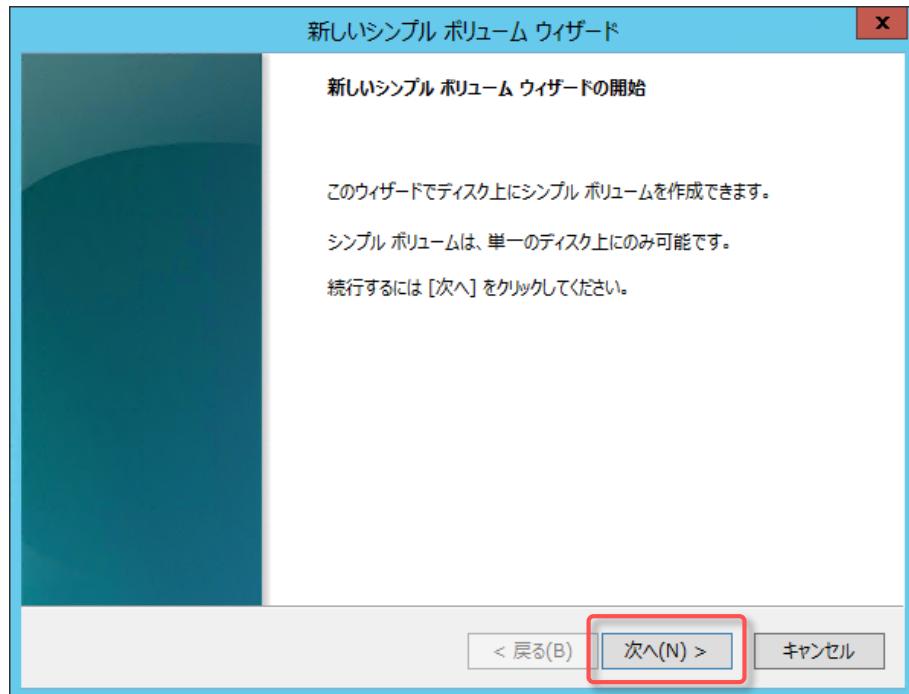


7. [未割り当て]を右クリックし[新しいシンプル ポリューム]をクリックします。

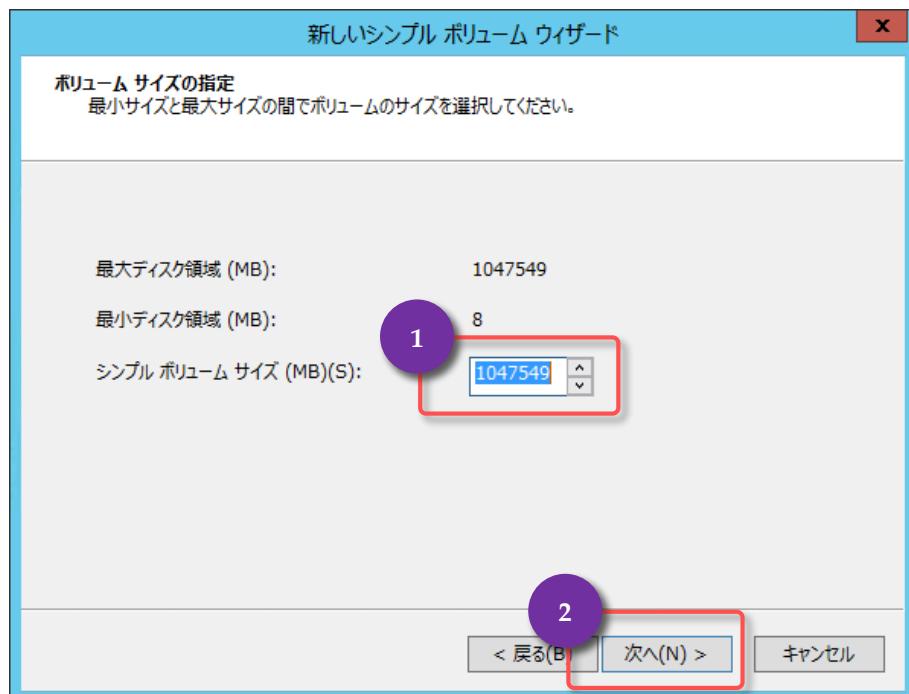


企業内システムと Microsoft Azure の VPN 接続、Active Directory 連携

8. [次へ]をクリックします。



9. [シンプル ポリューム サイズ(MB)]に最大値を入力し[次へ]をクリックします。



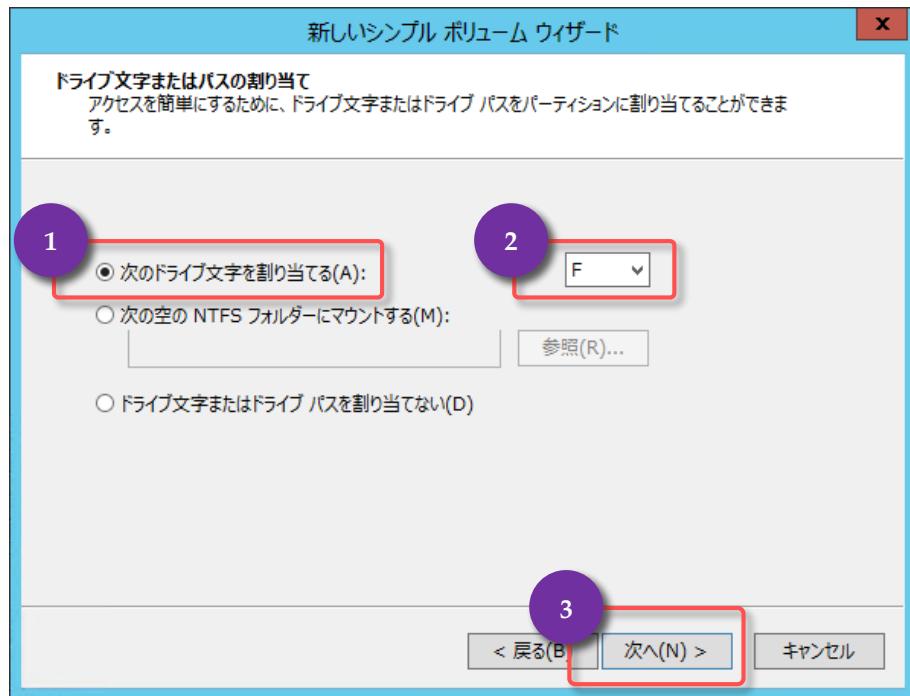
Note : ディスクのサイジング

今回は自習書ということですべての容量を割り当てています。

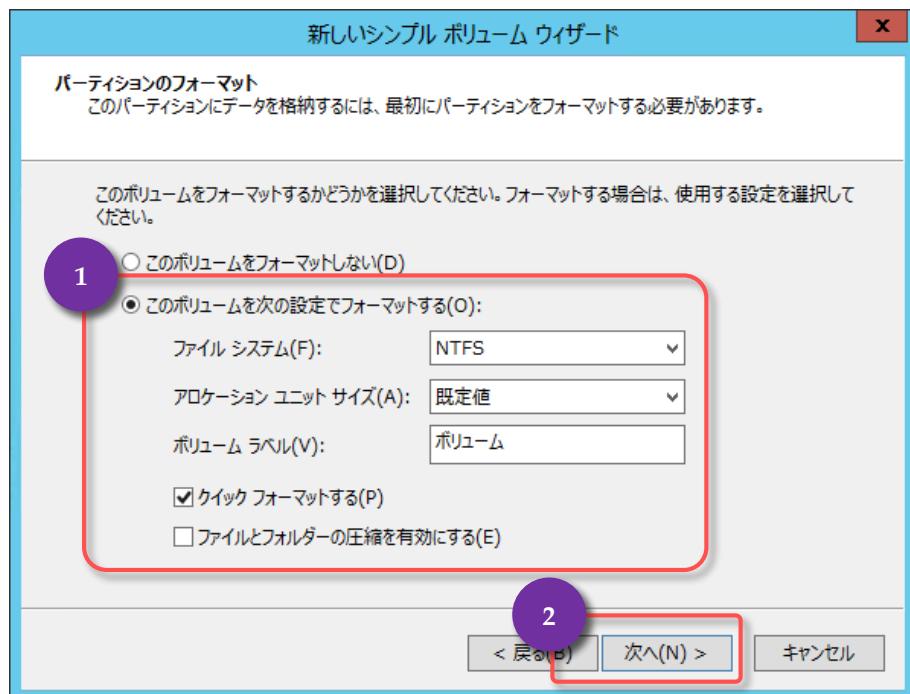
実際には AD DS のオブジェクト数などから環境に合わせた適切なサイズを割り当てます。

企業内システムと Microsoft Azure の VPN 接続、Active Directory 連携

10. [次のドライブ文字を割り当てる]にチェックを付け、プルダウンで[F](任意のドライブ文字)を選択し[次へ]をクリックします。



11. [このボリュームを次の設定でフォーマットする]にチェックを付け、[ファイル システム]に[NTFS]を選択、[アロケーション ユニット サイズ]に[既定値]を選択、[ボリューム ラベル]に「ボリューム」(任意の文字列)を入力、[クイック フォーマットする]にチェックを付け、[次へ]をクリックします。

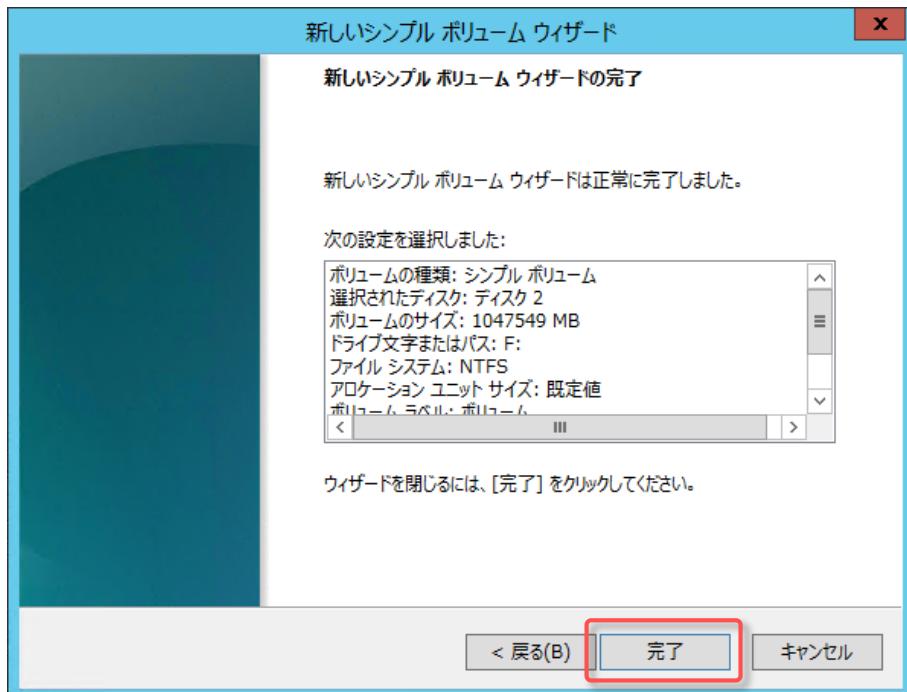


Note : クイックフォーマットする

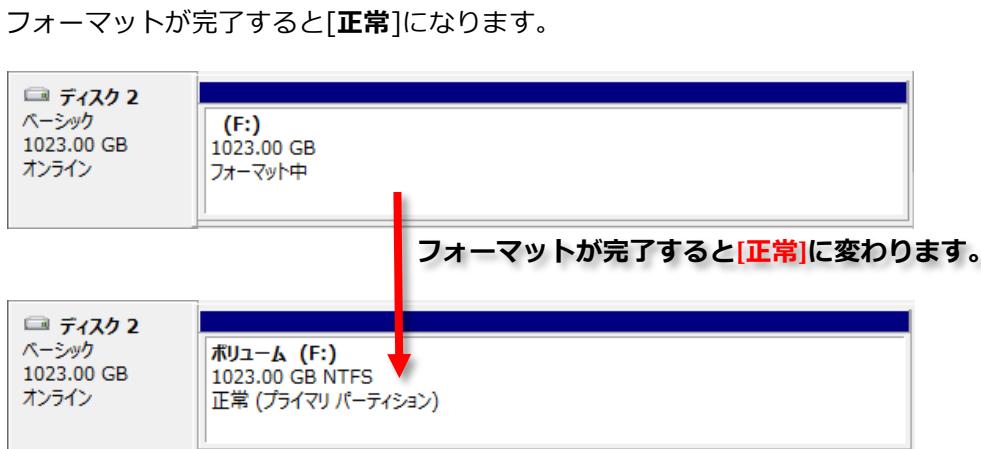
Azure のストレージは使用容量に応じて課金されます。

ディスクを通常フォーマットしてしまうと、ディスクのすべての領域を使用しているとされ、全容量(この自習書では約 1TB)分が課金対象となってしまいます。しかしながらクイックフォーマットでフォーマットした場合は、実際のデータ量に比例した容量分のみが課金対象となります。

12. [完了]をクリックします。

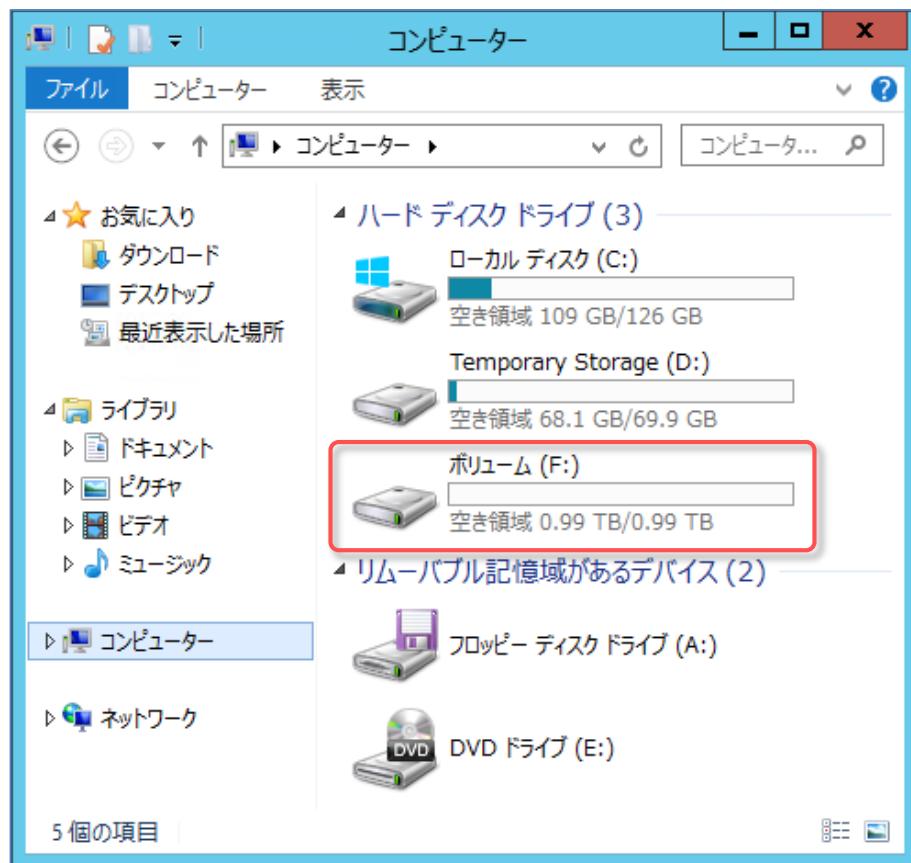


13. ディスクのフォーマットが始まると対象のディスクの状態が[フォーマット中]になります。



以上で仮想マシン上でのディスクの追加とフォーマットは完了となります。

14. [コンピューター]で確認するとディスクが追加されているのが分かります。



以上で仮想マシンへのディスクの追加が完了となります。

STEP 6. 仮想マシン上に AD DS を構築する

この STEP では、仮想マシン上に AD DS を構築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。

- ✓ ドメインへの参加
- ✓ AD DS のインストール
- ✓ ドメインコントローラーへの昇格
- ✓ 初期レプリケートの完了
- ✓ NTP に関する注意点 (PDC エミュレーターとは同期しない)
- ✓ サイトとサブネットの作成

6.1 ドメインへの参加

AD DS のインストールを行う前に、仮想サーバーをドメインに参加させます。

- 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。



- [ローカル サーバー]をクリックします。

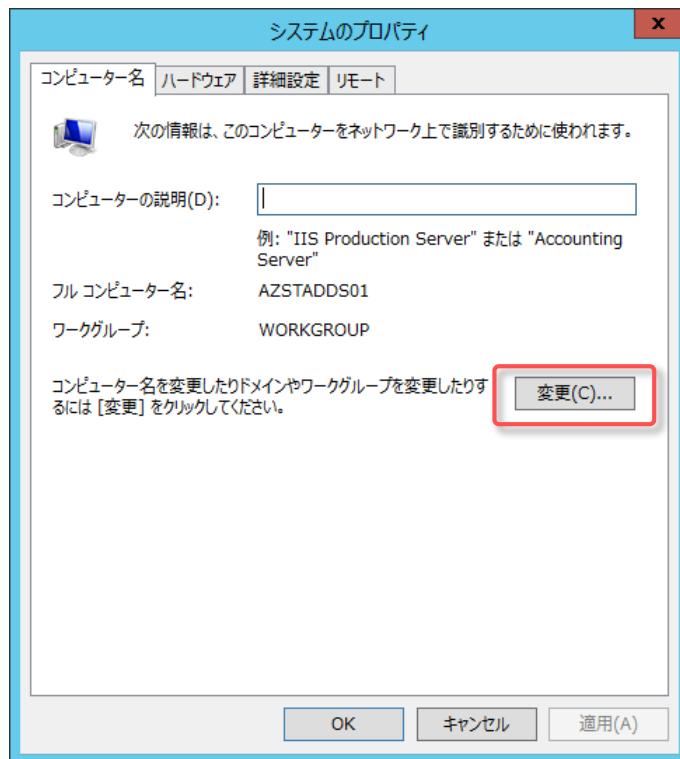


- [AZSTADDS01]をクリックします。

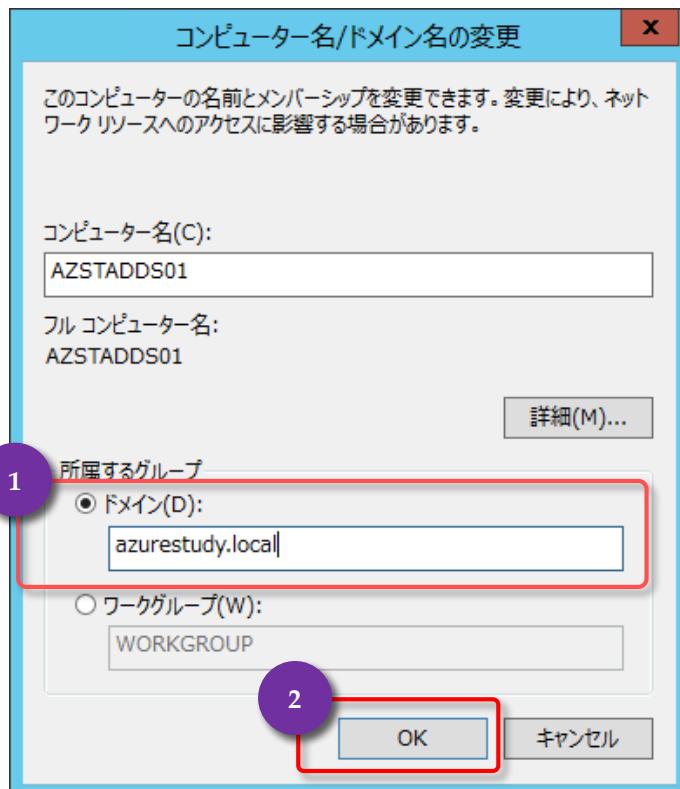


企業内システムと Microsoft Azure の VPN 接続、Active Directory 連携

4. [変更]をクリックします。

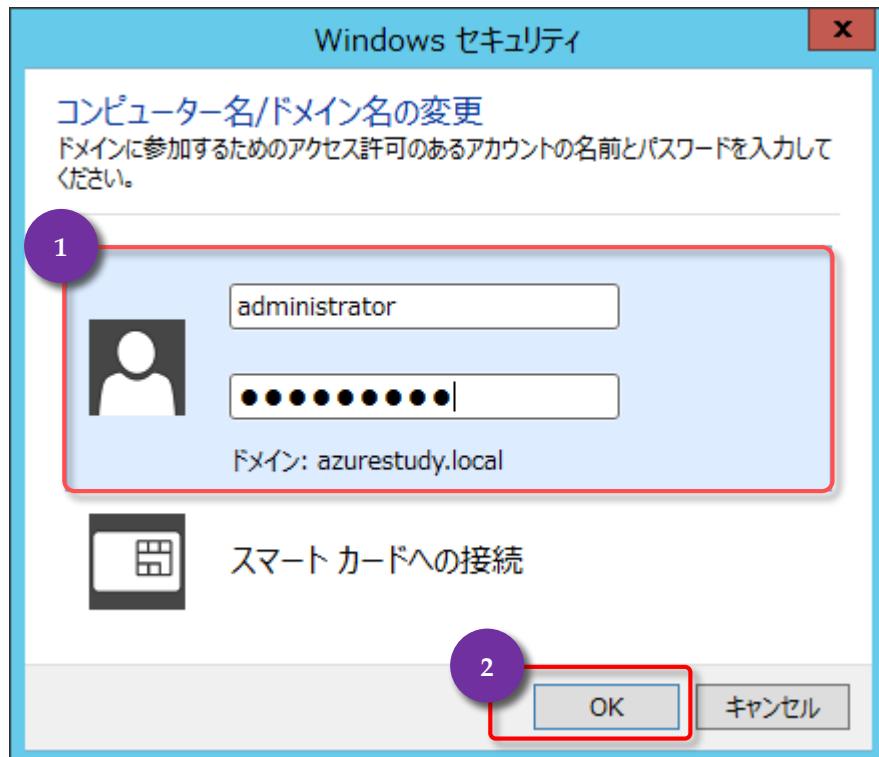


5. [ドメイン]にチェックを付け「azurestudy.local」(今回の自習書で参加するドメイン名)と入力し[OK]をクリックします。

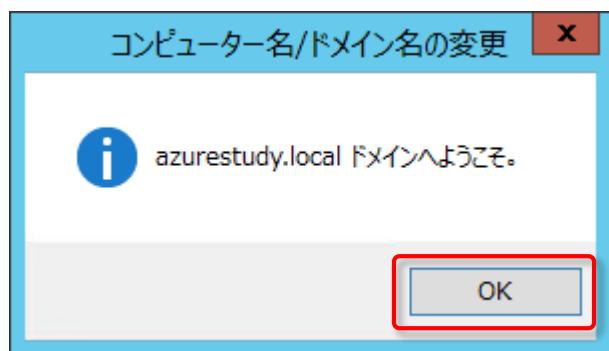


企業内システムと Microsoft Azure の VPN 接続、Active Directory 連携

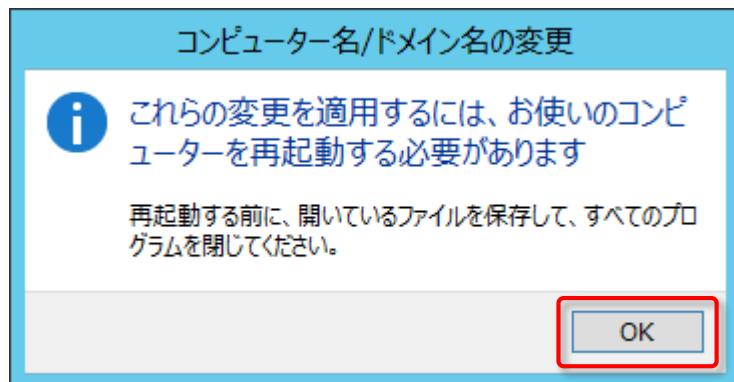
6. [ユーザー]に「**administrator**」(オンプレミス環境の AD DS の Domain Admin 権限のあるユーザーアカウント名)と入力、[パスワード]に「**studyP@ss**」(オンプレミス環境の AD DS の Domain Admin 権限のあるユーザーアカウントのパスワード)と入力し[OK]をクリックします。



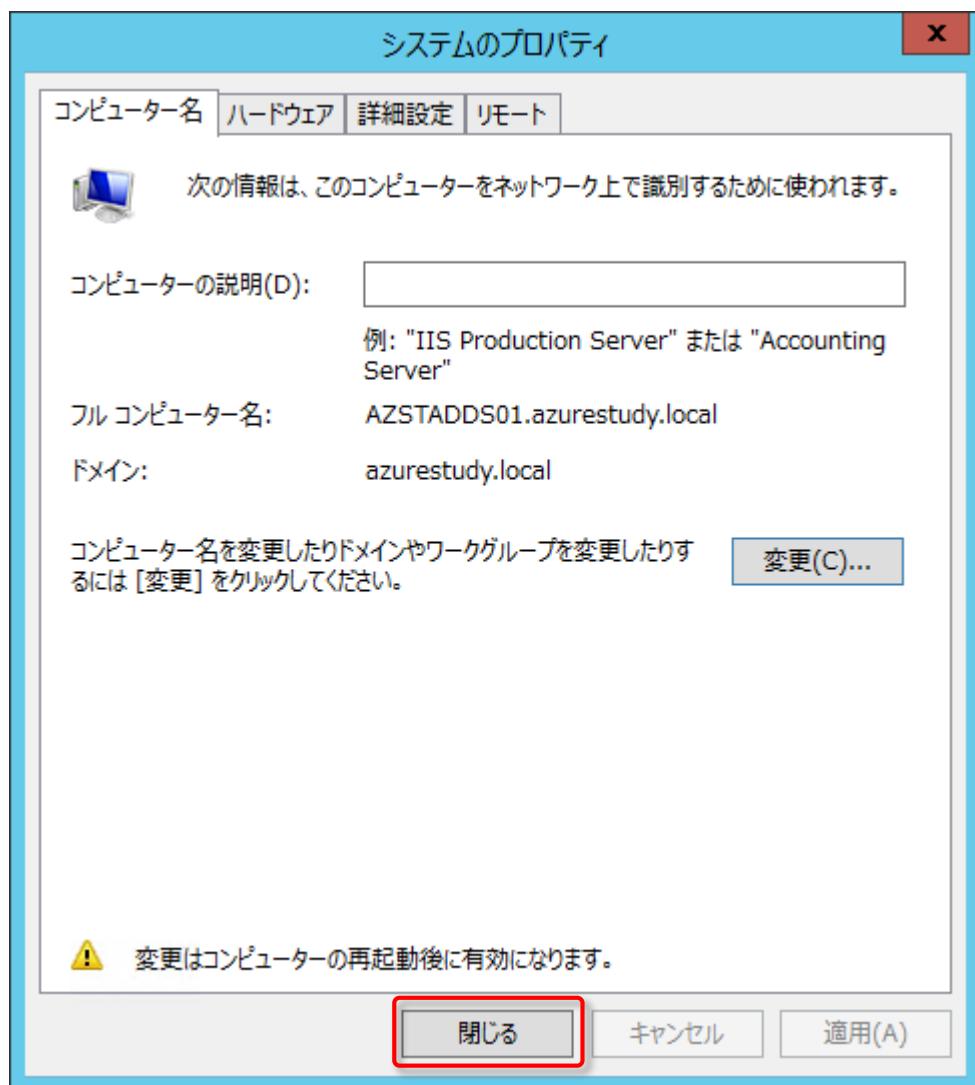
7. [OK]をクリックします。



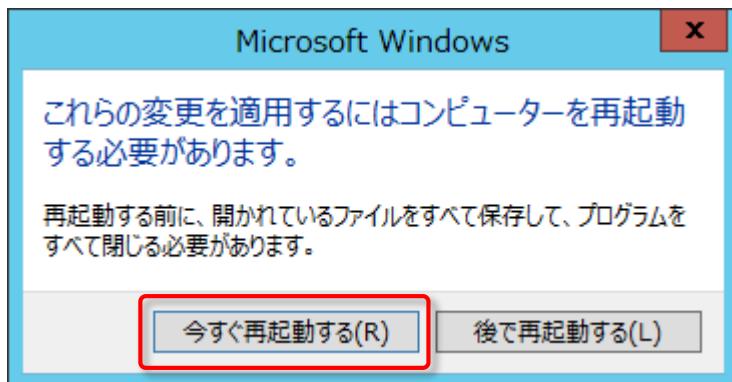
8. [OK]をクリックします。



9. [閉じる]をクリックします。



10. [今すぐ再起動する]をクリックします。



以上で仮想マシンのドメイン参加設定が完了となります。

6.2 AD DS のインストール

AD DS のインストールを行います。

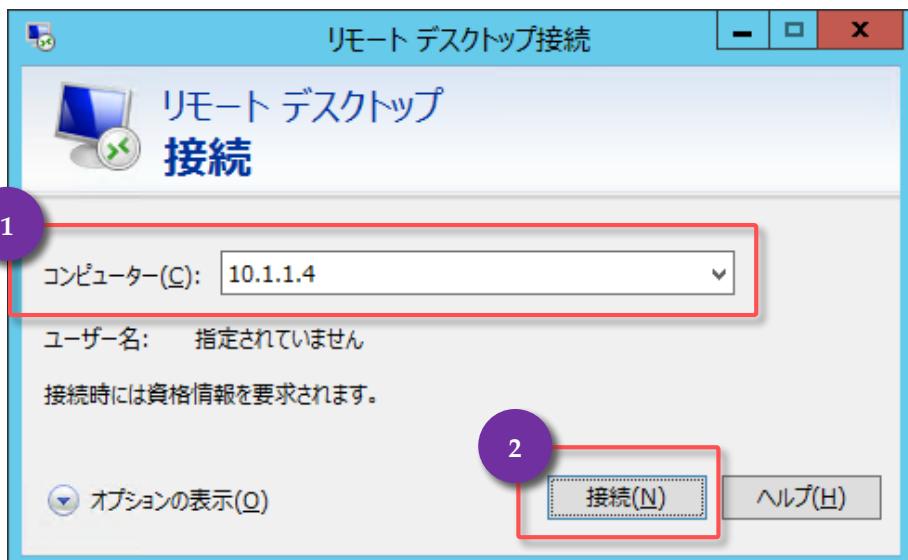
➔ Domain Admin 権限でのログイン

- PowerShell もしくはコマンドプロンプトを起動し、以下のコマンドを入力し、[Enter]キーを入力します。

```
mstsc
```

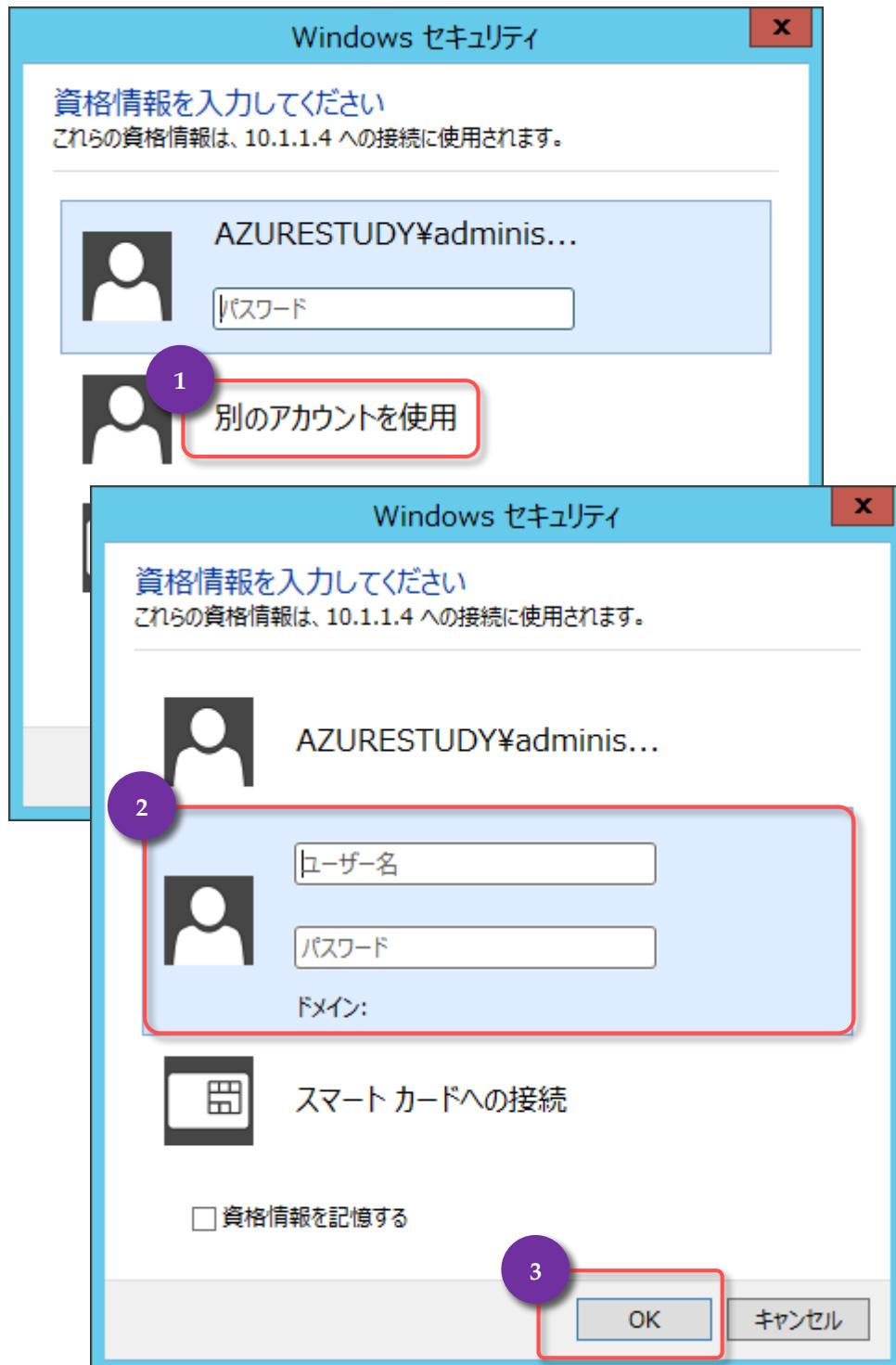


- [コンピューター]に「10.1.1.4」(仮想マシンの内部 IP アドレス)と入力し[接続]をクリックします。



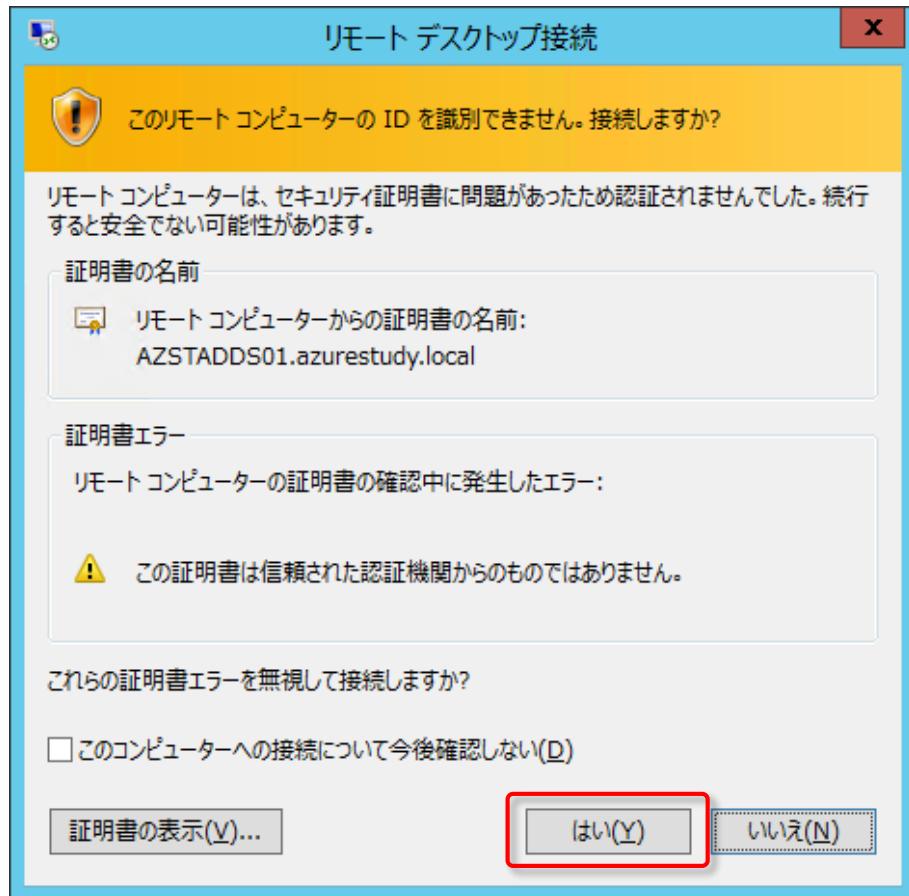
企業内システムと Microsoft Azure の VPN 接続、Active Directory 連携

3. [別のアカウントを使用]をクリックし、[ユーザー]に「**azurestudy.local\\$administrator**」(オンプレミス環境の AD DS の Domain Admin 権限のあるユーザーアカウント名)と入力、[パスワード]に「**studyP@ss**」(オンプレミス環境の AD DS の Domain Admin 権限のあるユーザーアカウントのパスワード)と入力し[OK]をクリックします。

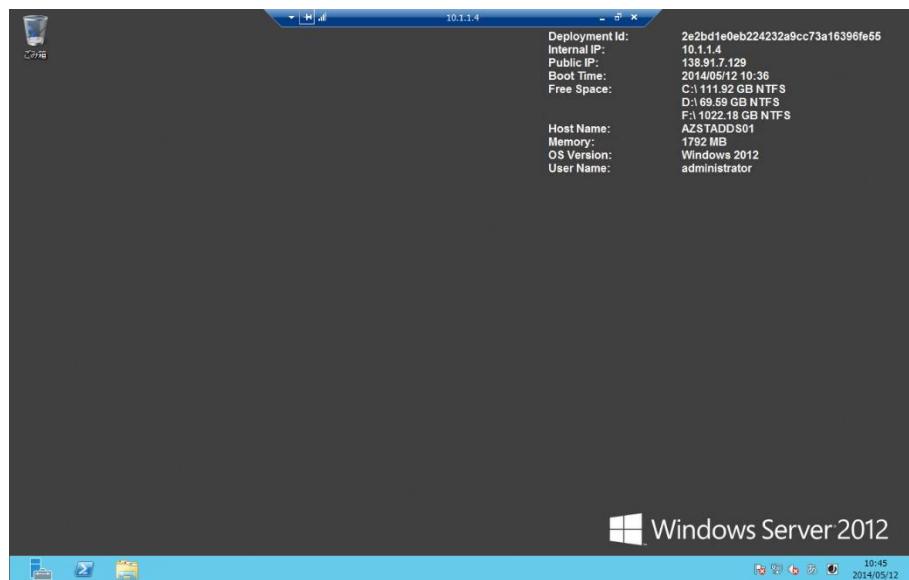


企業内システムと Microsoft Azure の VPN 接続、Active Directory 連携

4. 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] ボタンをクリックします。



5. 仮想マシンに接続されます。



➔ AD DS のインストール

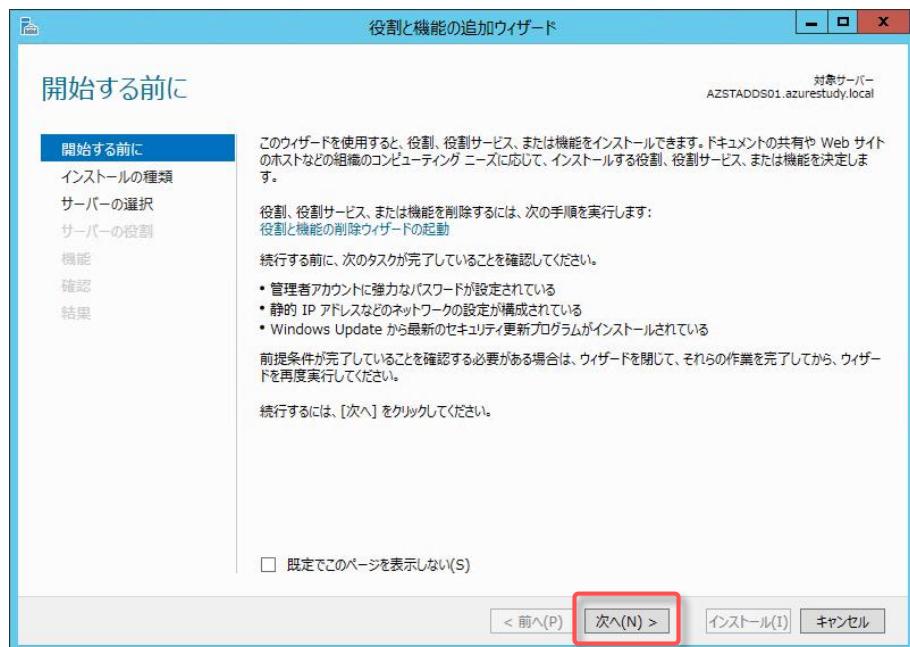
1. デスクトップ画面左下の[サーバー マネージャー]をクリックします。



2. [役割と機能の追加]をクリックします。

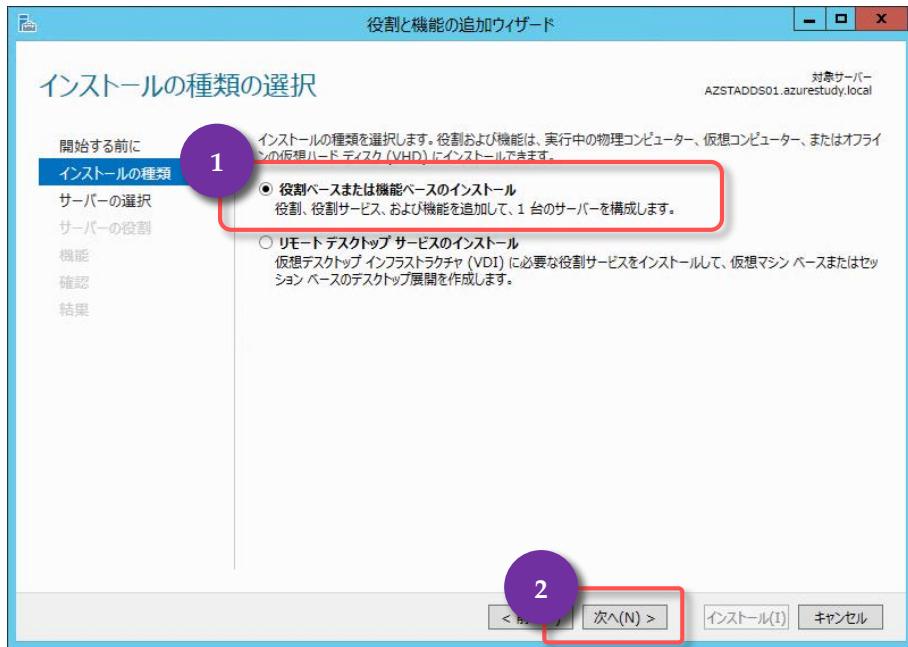


3. [次へ]をクリックします。

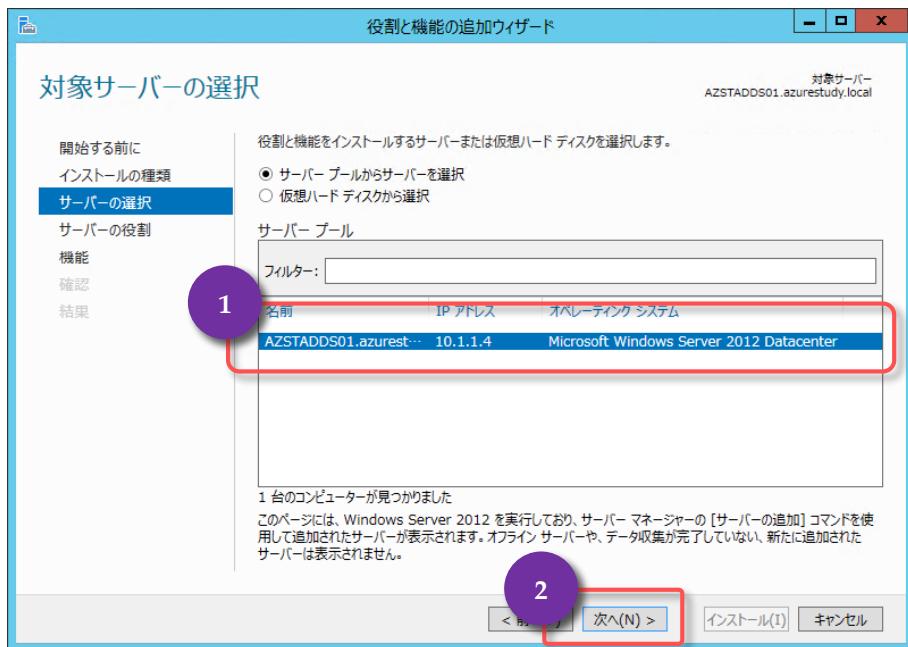


企業内システムと Microsoft Azure の VPN 接続、Active Directory 連携

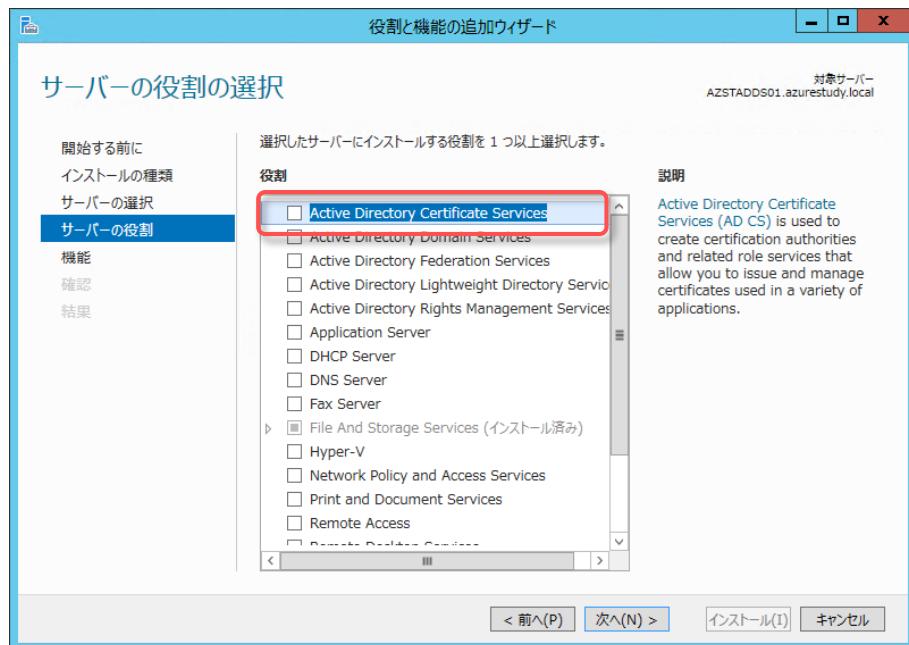
4. [役割ベースまたは機能ベースのインストール]を選択し[次へ]をクリックします。



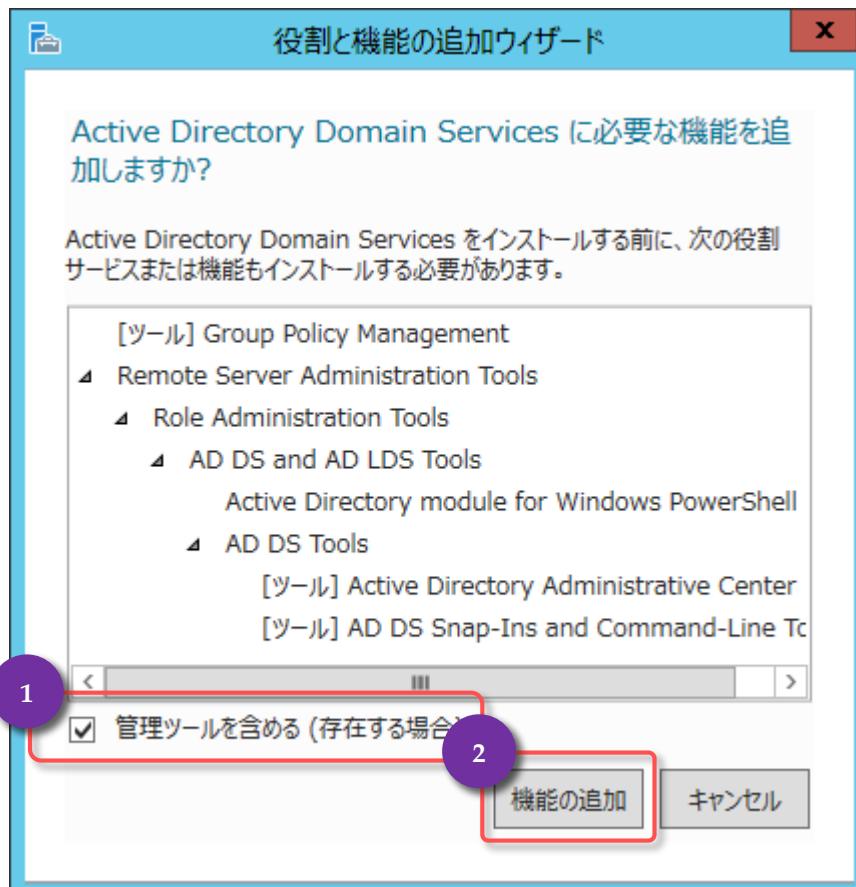
5. [サーバーブールからサーバーを選択]を選択し[サーバーブール]内から「AZSTADDS01.azurestudy.local」を選択し[次へ]をクリックします。



6. [Active Directory Domain Service]にチェックを付けます。

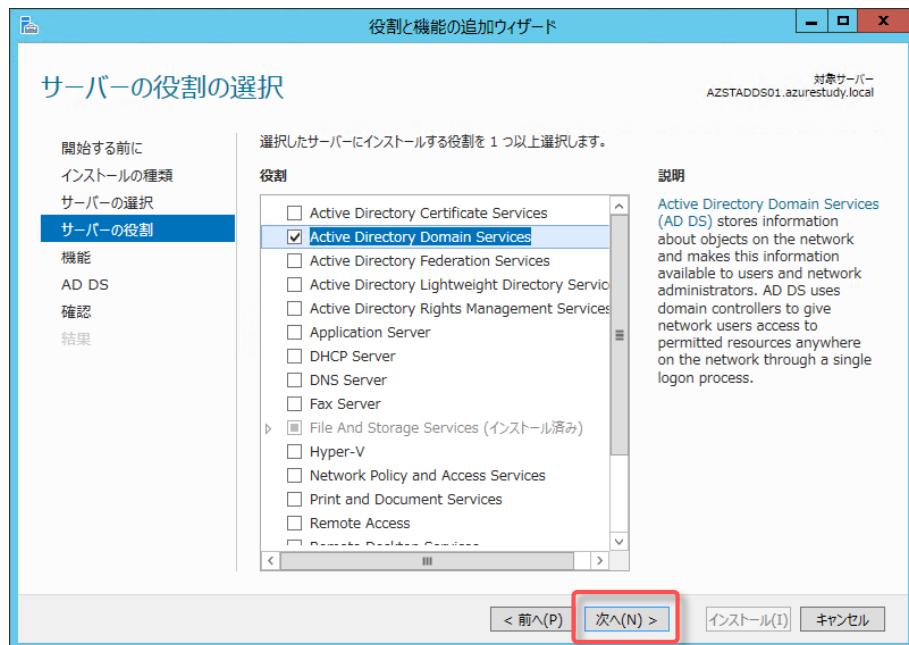


7. [管理ツールを含める(存在する場合)]にチェックを付け[機能の追加]をクリックします。

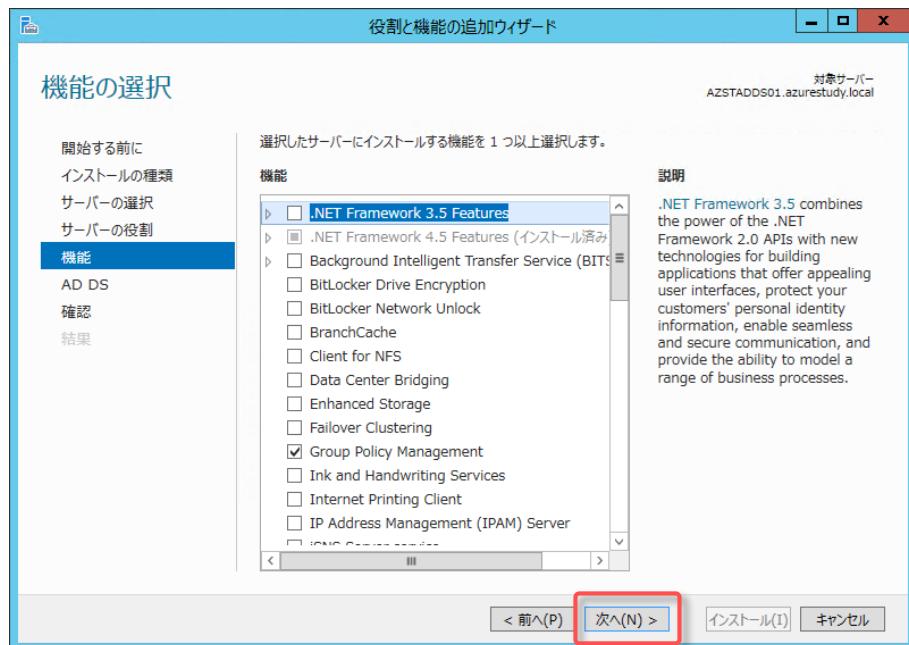


企業内システムと Microsoft Azure の VPN 接続、Active Directory 連携

8. [次へ]をクリックします。

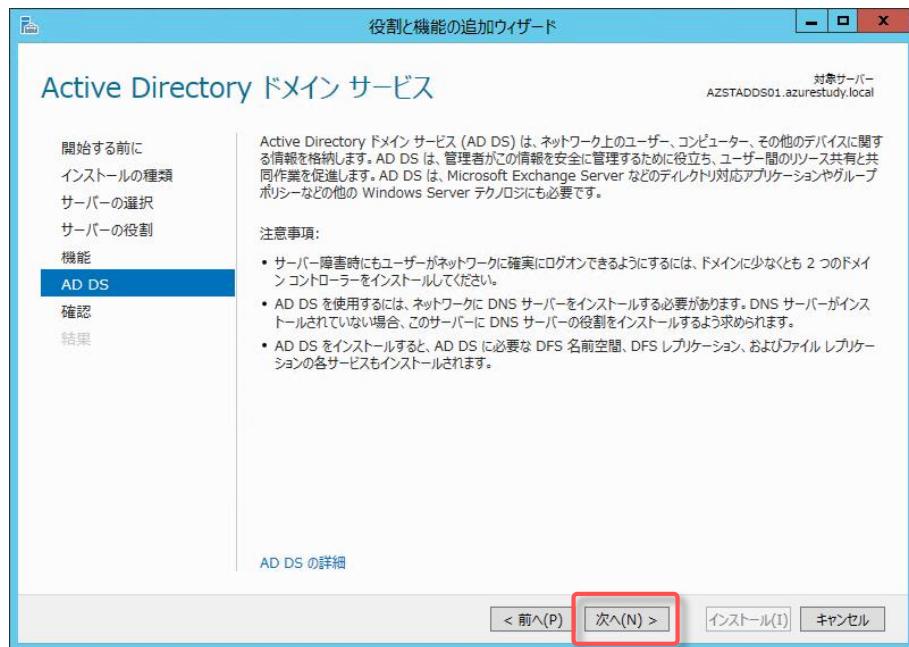


9. [次へ]をクリックします。

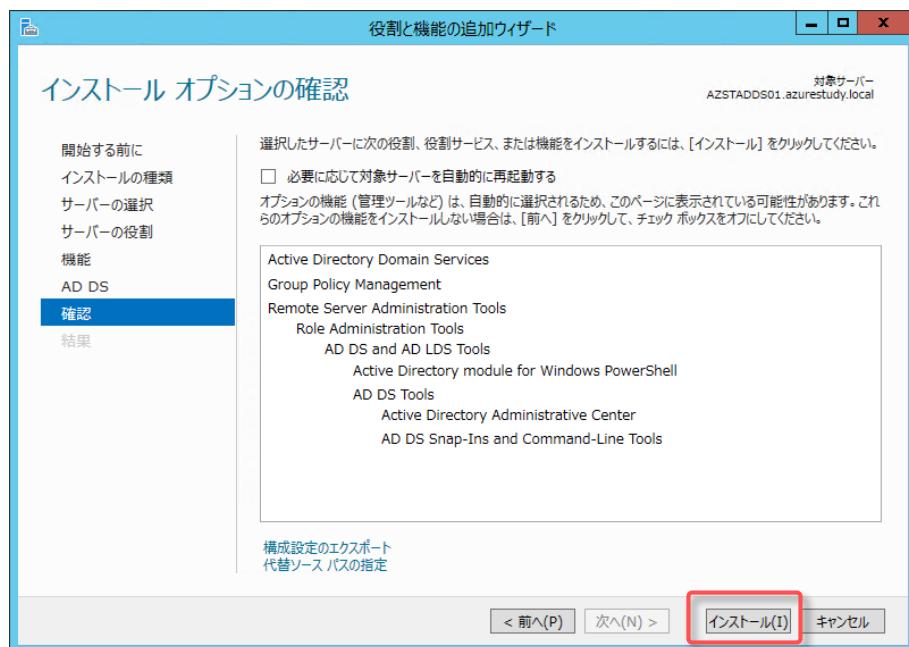


企業内システムと Microsoft Azure の VPN 接続、Active Directory 連携

10. [次へ]をクリックします。

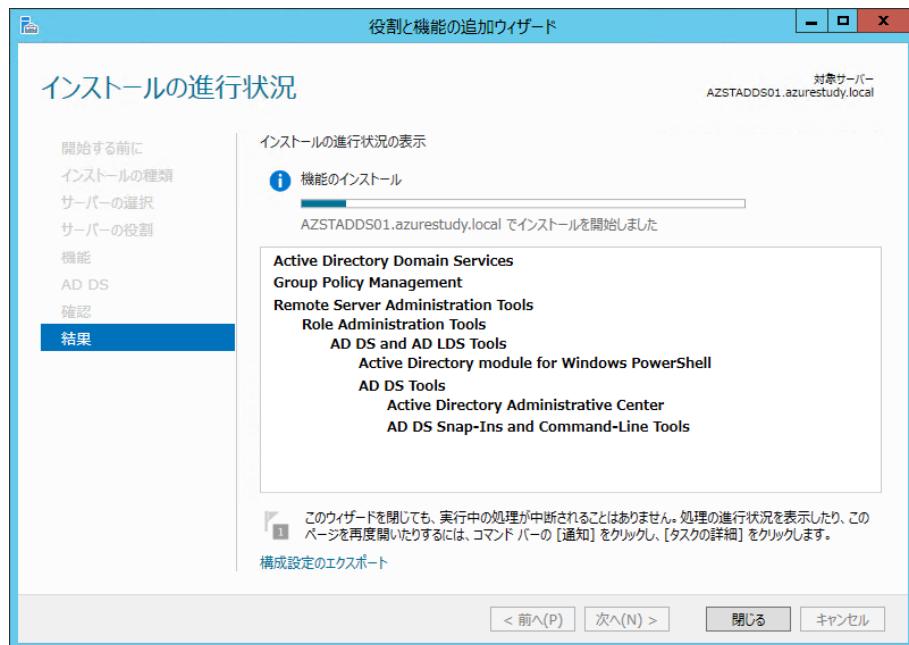


11. [インストール]をクリックします。

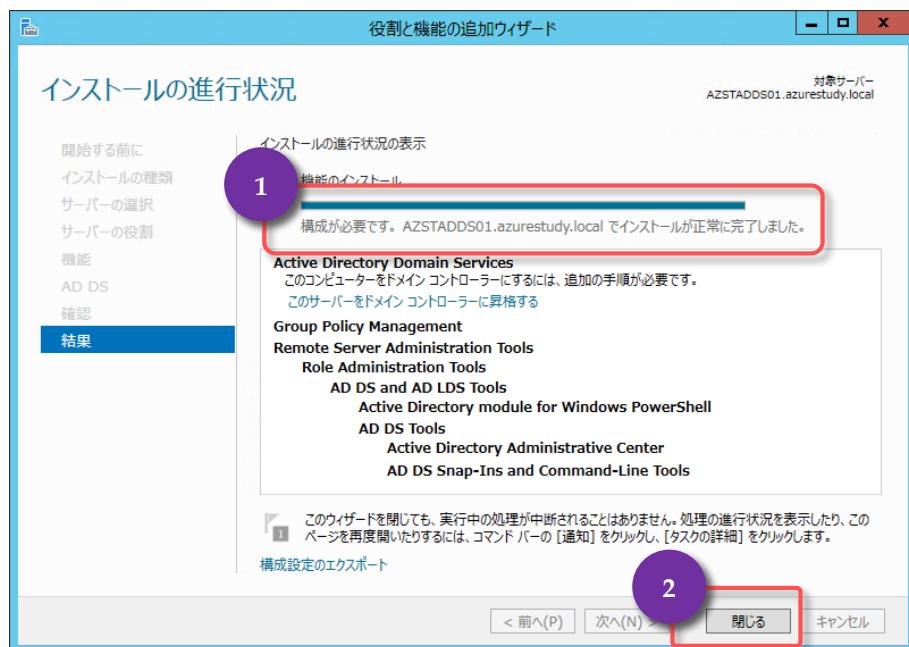


企業内システムと Microsoft Azure の VPN 接続、Active Directory 連携

12. インストールが終了するのを待ちます。



13. [構成が必要です。AZSTADDS01.azurestudy.local でインストールが正常に完了しました。]と表示されたことを確認し、[閉じる]をクリックします。



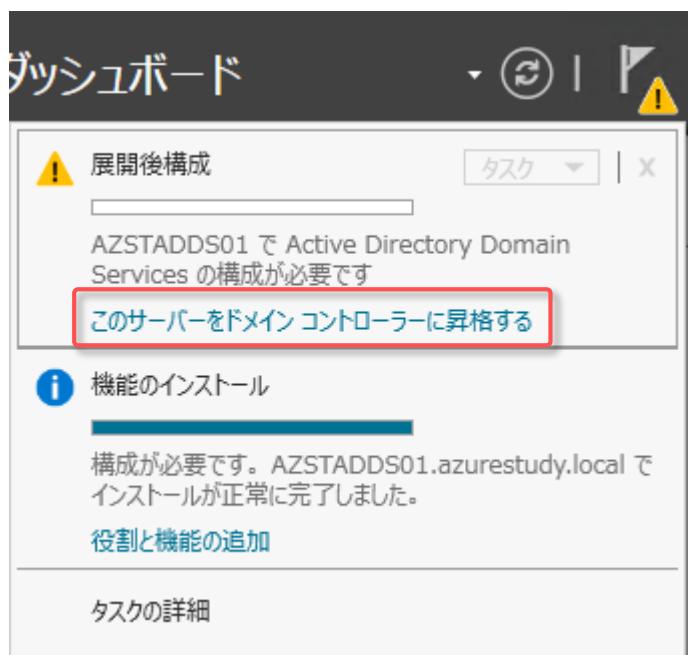
以上で AD DS のインストールが完了となります。

6.3 ドメインコントローラーへの昇格

- [サーバーマネージャー]の「！」(通知)をクリックします。

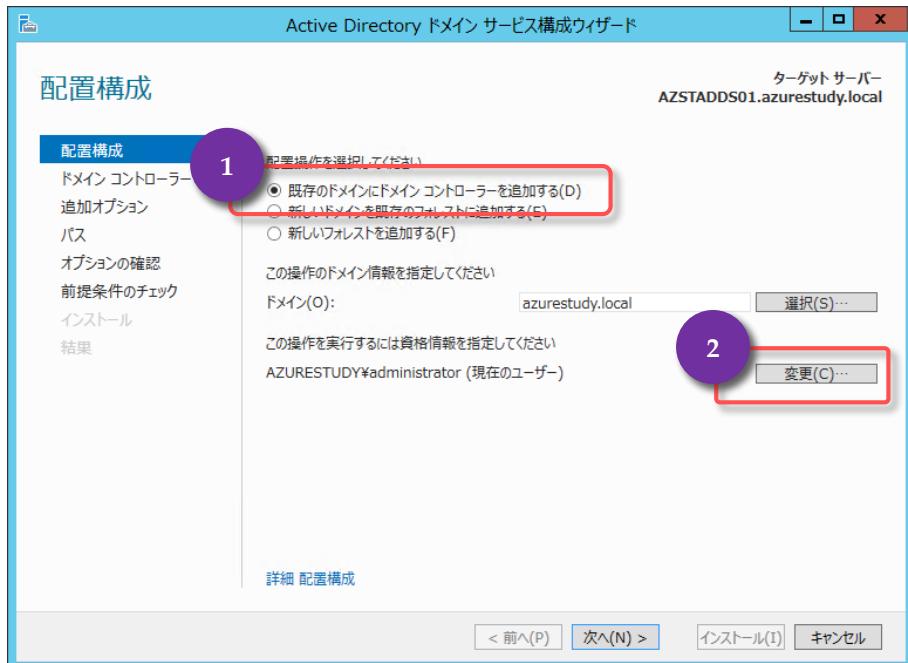


- [このサーバーをドメインコントローラーに昇格する]をクリックします。



企業内システムと Microsoft Azure の VPN 接続、Active Directory 連携

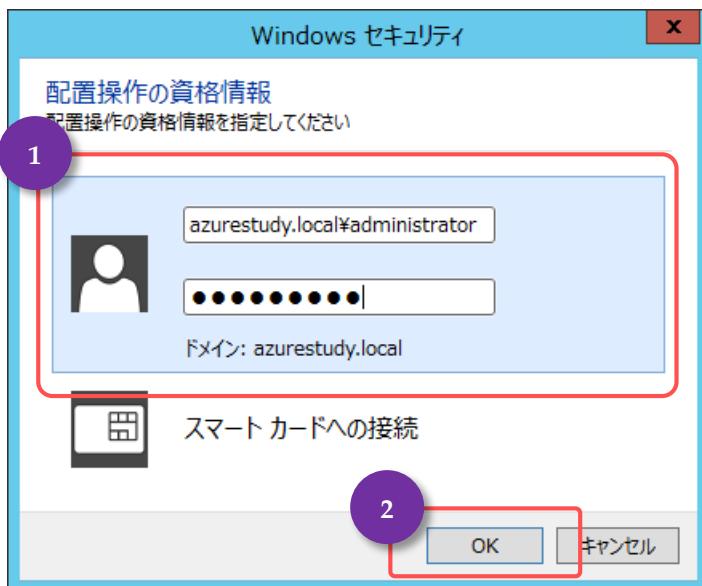
3. [既存のドメインコントローラに追加する]を選択し[変更]をクリックします。

**Note : 資格情報の入力**

「技術情報の文書番号 2737935」の問題により、ローカル管理者とドメイン管理者のパスワードが同じ場合、昇格に失敗することがあります。そのため、自動で入力された資格情報のまま進めず手動で入力し直す必要があります。

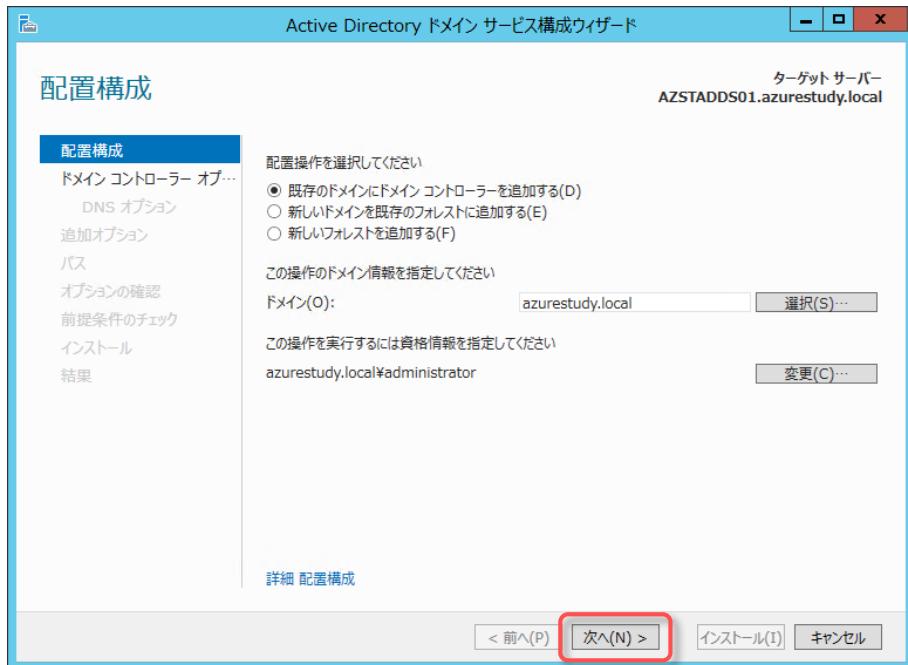
「Active Directory installation stalls at the "Creating the NTDS settings object" stage
(<http://support.microsoft.com/kb/2737935/ja>)」

4. [ユーザー名]に「azurestudy.local\\$administrator」と入力し[パスワード]に「studyP@ss」と入力し[OK]をクリックします。



企業内システムと Microsoft Azure の VPN 接続、Active Directory 連携

5. [次へ]をクリックします。

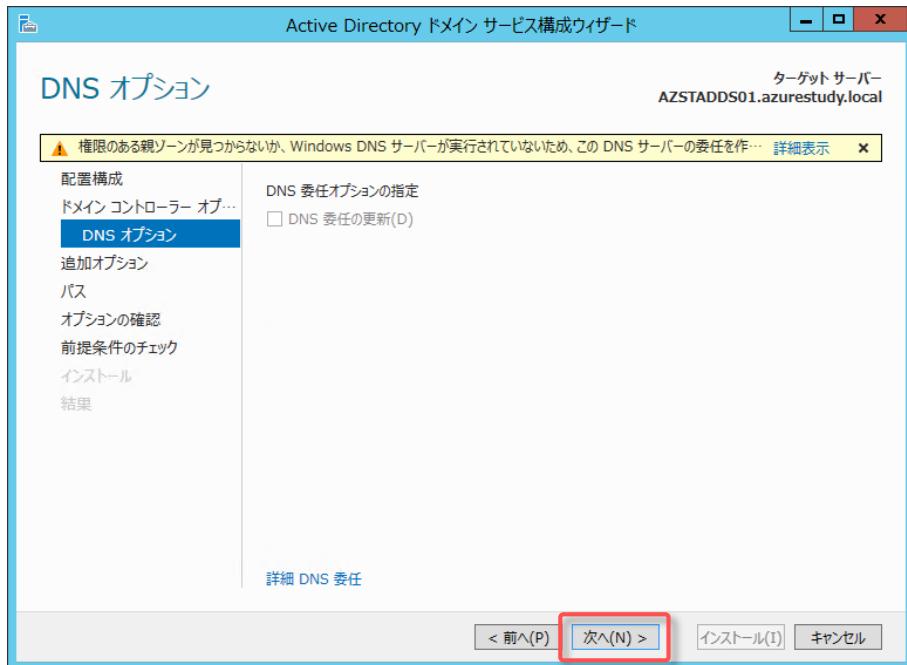


6. [ドメイン ネーム システム (DNS) サーバー]と[グローバル カタログ (GC)]にチェックを付け[サイト名]に[Default-First-Site-Name]が選択されていることを確認し、[パスワード]及び[パスワードの確認入力]に「studyP@ss」と入力し[次へ]をクリックします。

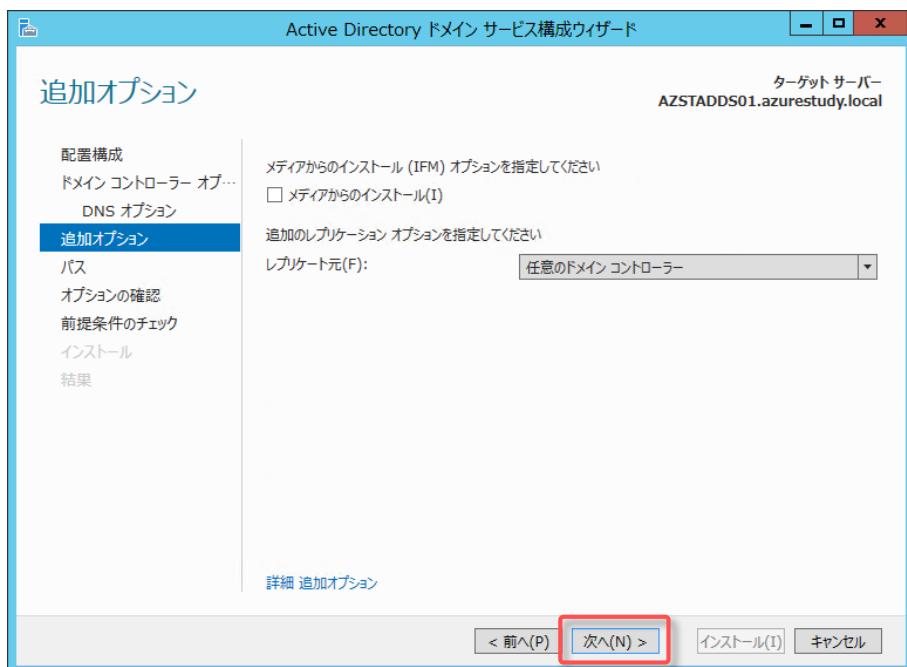


企業内システムと Microsoft Azure の VPN 接続、Active Directory 連携

7. [次へ]をクリックします。

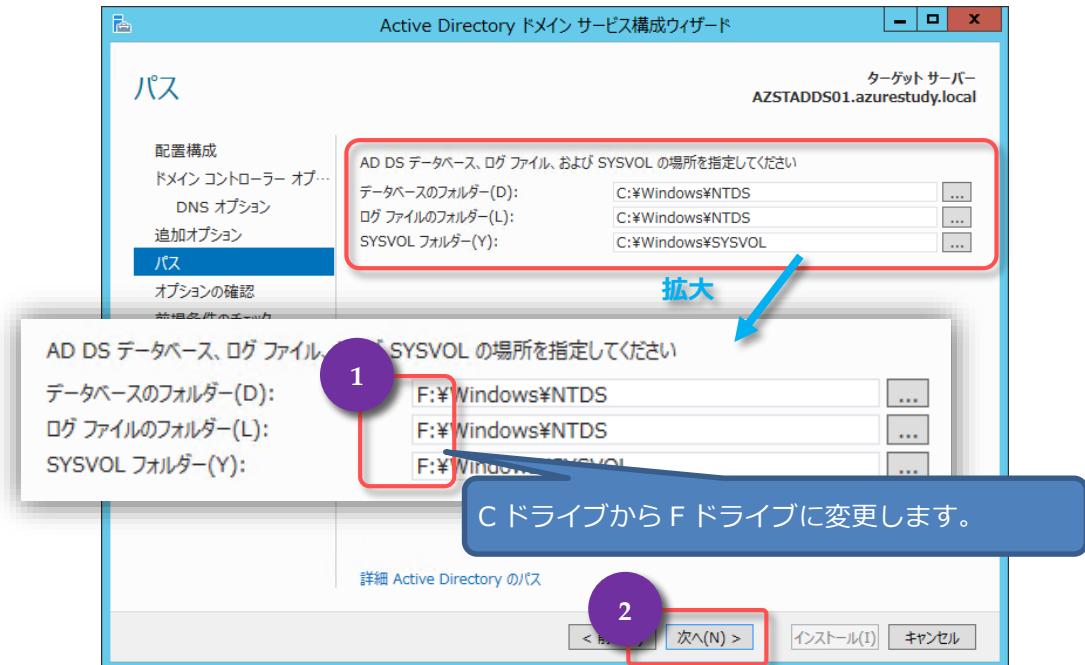


8. [次へ]をクリックします。

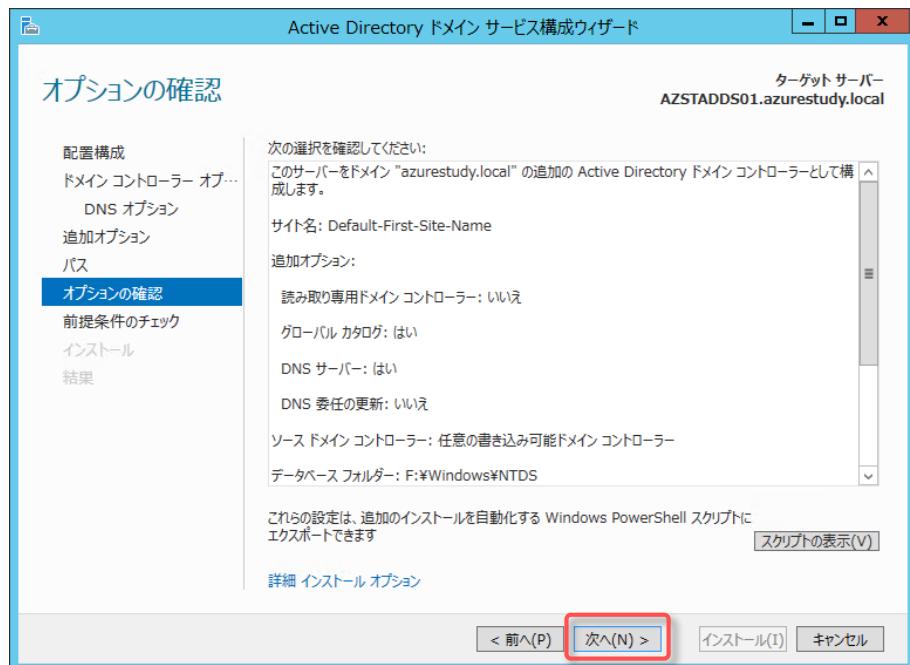


企業内システムと Microsoft Azure の VPN 接続、Active Directory 連携

9. 各情報の格納場所を、追加したディスク(F ドライブ)に変更し[次へ]をクリックします。

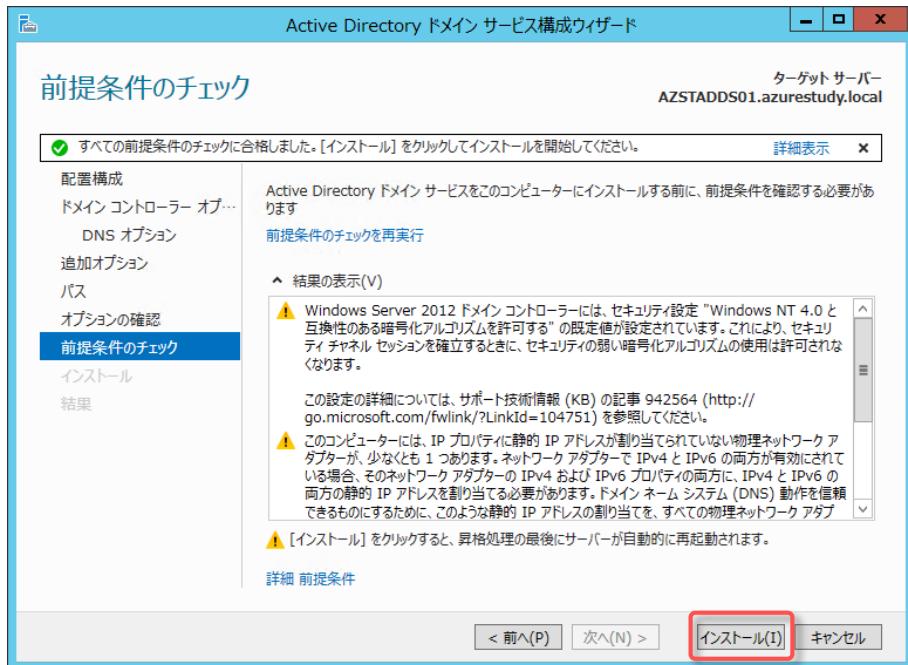


10. [次へ]をクリックします。



企業内システムと Microsoft Azure の VPN 接続、Active Directory 連携

11. 警告が 3 件表示されますが、そのまま[インストール]をクリックします。



Note : 警告について

これら 3 つの警告は基本的に無視して構いません。

Windows NT 4.0 で使用されている暗号化アルゴリズムとの互換性がないために表示されるメッセージとなります。今回の環境では Windows Server 2012 のみの環境であるため、無視します。

! Windows Server 2012 ドメインコントローラーには、セキュリティ設定 "Windows NT 4.0 と互換性のある暗号化アルゴリズムを許可する" の既定値が設定されています。これにより、セキュリティチャネルセッションを確立するときに、セキュリティの弱い暗号化アルゴリズムの使用は許可されなくなります。

この設定の詳細については、サポート技術情報 (KB) の記事 942564 (<http://go.microsoft.com/fwlink/?LinkId=104751>) を参照してください。

動的 IP(DHCP)が設定されているために表示されるメッセージとなります。

AD DS で動的 IP を用いることは不可ですが、Azure の制限として静的 IP が指定できないため、無視します。

! このコンピューターには、IP プロパティに静的 IP アドレスが割り当てられていない物理ネットワークアダプターが、少なくとも 1 つあります。ネットワークアダプターで IPv4 と IPv6 の両方が有効にされている場合、そのネットワークアダプターの IPv4 および IPv6 プロパティの両方に、IPv4 と IPv6 の両方の静的 IP アドレスを割り当てる必要があります。ドメインネームシステム (DNS) 動作を信頼できるものにするために、このような静的 IP アドレスの割り当てを、すべての物理ネットワークアダプターに対して行う必要があります。

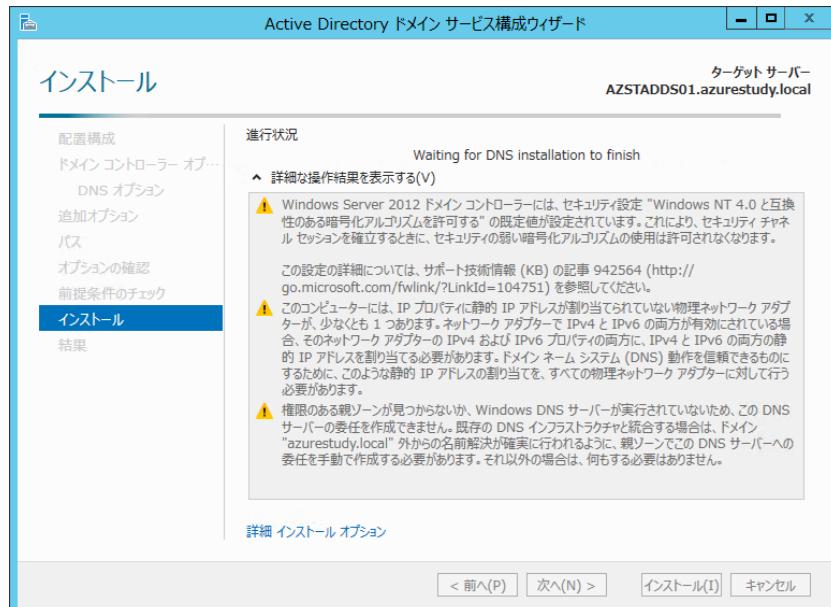
DNS サーバーが存在していないために表示されるメッセージとなります。

AD DS インストール時に合わせてインストールされるため、無視します。

! 権限のある親ゾーンが見つからないか、Windows DNS サーバーが実行されていないため、この DNS サーバーの委任を作成できません。既存の DNS インフラストラクチャと統合する場合は、ドメイン "azurestudy.local" 外からの名前解決が確実に行われるよう、親ゾーンでこの DNS サーバーへの委任を手動で作成する必要があります。それ以外の場合は、何もする必要はありません。

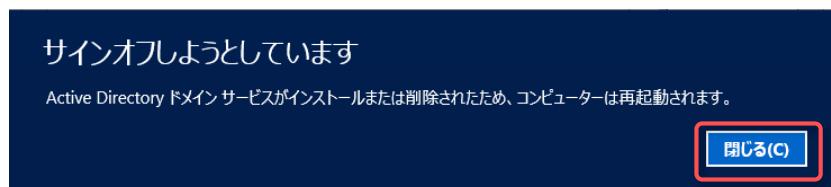
企業内システムと Microsoft Azure の VPN 接続、Active Directory 連携

12. インストールが完了するのを待ちます。

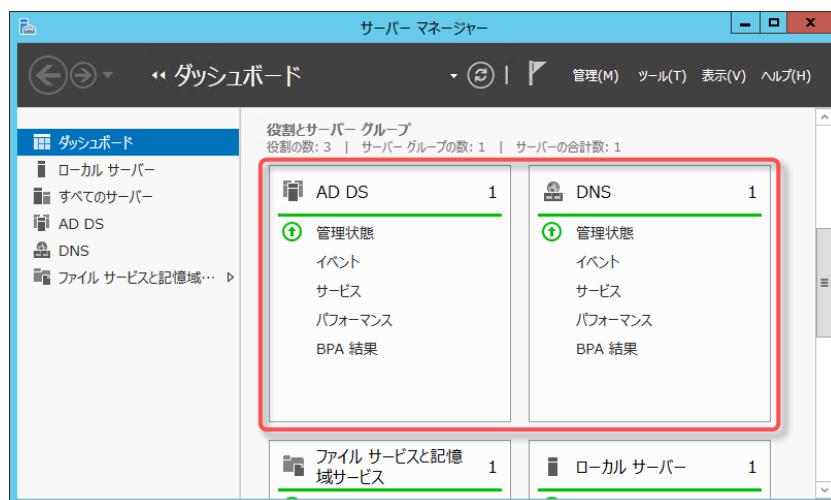


13. インストールが完了すると自動的に再起動が開始されます。

[閉じる]をクリックします。



14. 再起動後、[サーバー マネージャー]を起動すると[AD DS]と[DNS]が追加されています。



以上でドメインコントローラへの昇格が完了となります。

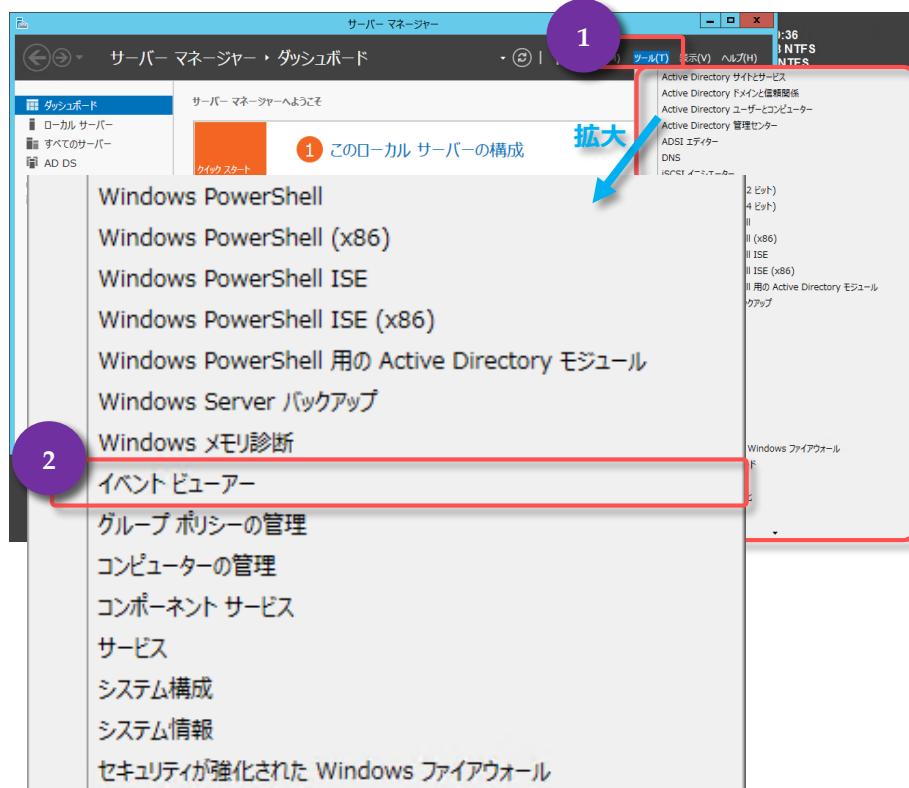
6.4 初期レプリケートの完了

AD DS の初期レプリケートが正常に完了したことを確認します。

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。

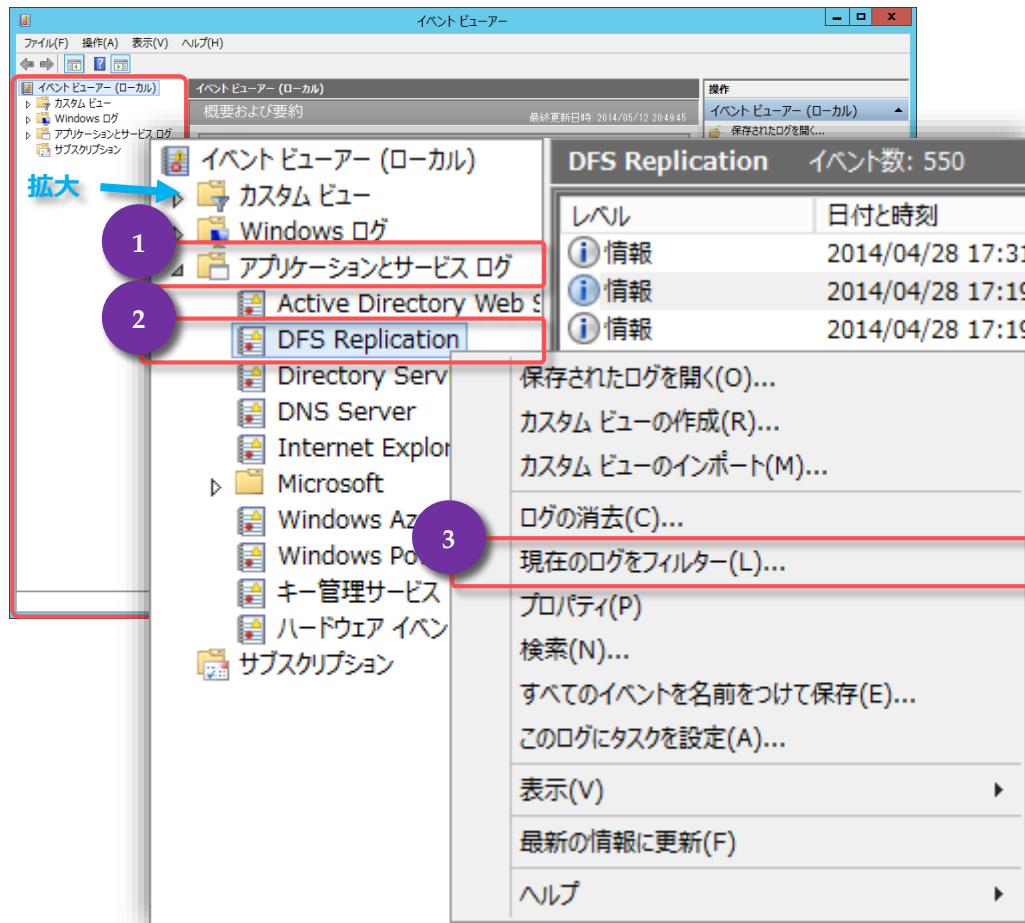


2. [ツール]をクリックし[イベント ビューアー]をクリックします。

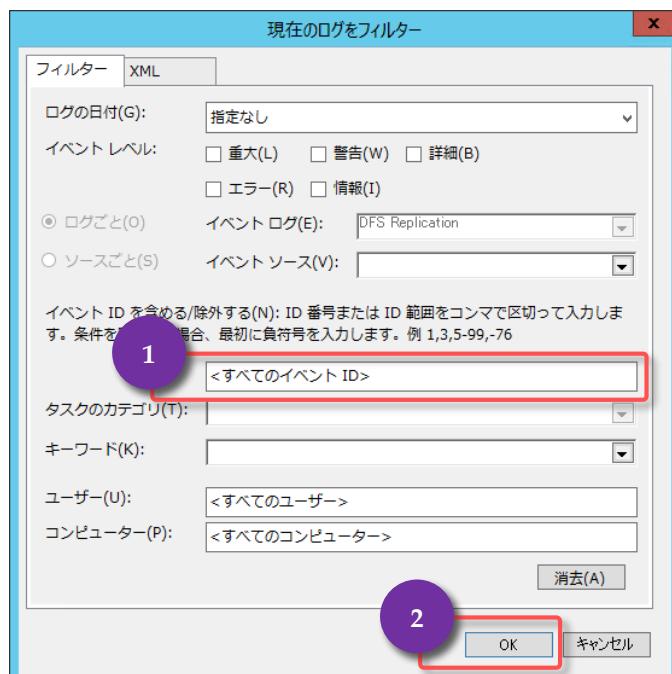


企業内システムと Microsoft Azure の VPN 接続、Active Directory 連携

3. [アプリケーションとサービス ログ]を展開し[DFS Replication]を右クリックし[現在のログをフィルター]をクリックします。

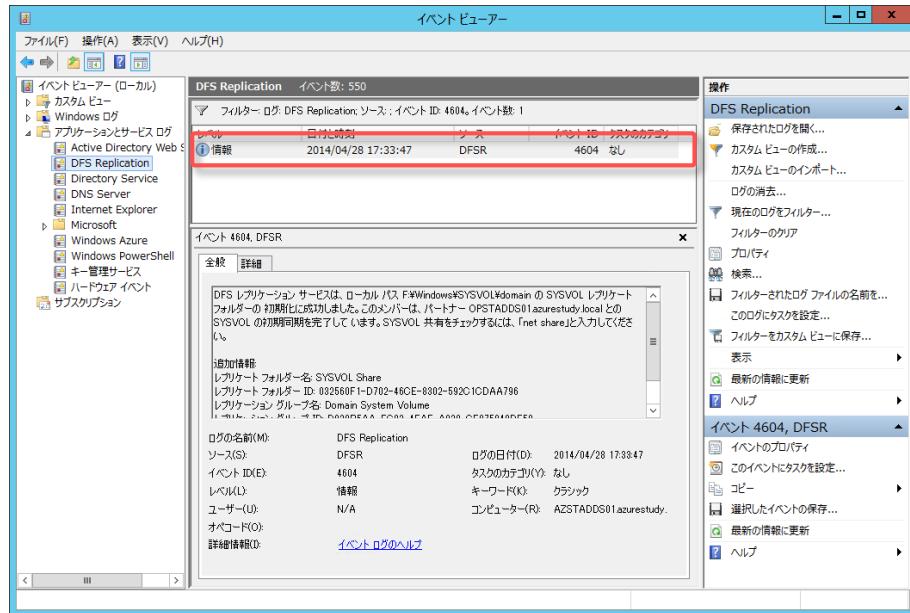


4. [<すべてのイベント ID>]に「4604」と入力して[OK]をクリックします。



企業内システムと Microsoft Azure の VPN 接続、Active Directory 連携

5. フィルターの結果「4604」のイベントが出力されていれば初期レプリケートが完了したことを示します。尚、ネットワーク環境によっては初期レプリケートの完了までに時間がかかることがあります。



以上で初期レプリケートの確認が完了となります。

6.5 NTP に関する注意点 (PDC エミュレーターとは同期しない)

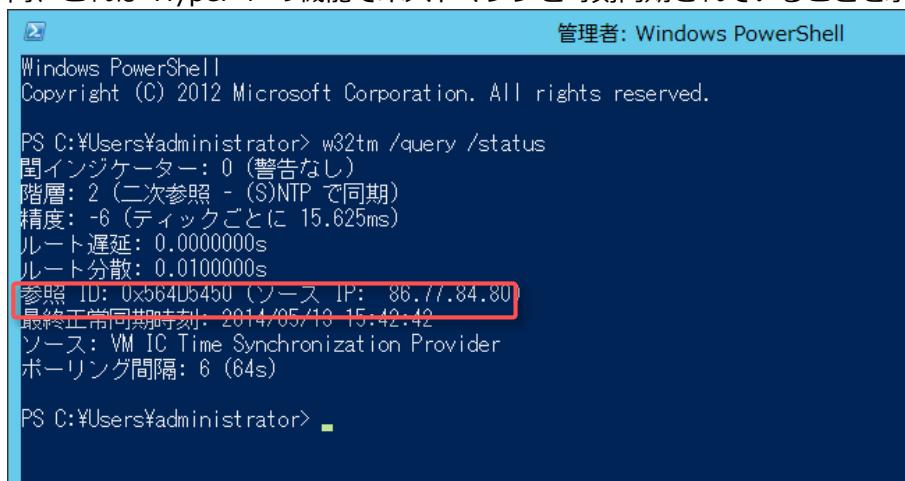
通常ドメインコントローラーに昇格すると、PDC エミュレーターの役割を持ったドメインコントローラーと時刻同期を行います。

しかしながら、Azure 上に構築した AD DS は Hyper-v の仕様により PDC エミュレーターと同期を行いません。(イベントログ上には PDC エミュレーターとも同期を試みているログが出力される。)

以下は「**w32tm /query /status**」を実行した結果となります。

ソースには[**VM IC Time Synchronization Provider**]と表示されています。

尚、これは Hyper-v の機能でホストマシンと時刻同期されていることを示します。



```
管理者: Windows PowerShell
Windows PowerShell
Copyright (C) 2012 Microsoft Corporation. All rights reserved.

PS C:\$Users\$administrator> w32tm /query /status
閲インジケーター: 0 (警告なし)
階層: 2 (二次参照 - (S)NTP で同期)
精度: -6 (ティックごとに 15.625ms)
ルート遅延: 0.0000000s
ルート分散: 0.0100000s
参照 ID: 0x564D5430 (ソース IP: 86.77.84.80)
最終正常同期時刻: 2014/05/13 15:42:42
ソース: VM IC Time Synchronization Provider
ポーリング間隔: 6 (64s)

PS C:\$Users\$administrator>
```

6.6 サイトとサブネットの作成

サイトとサブネットを適正に設定することにより Azure 側に AD DS の認証を必要とするサーバーを構築した際に適切な AD DS (Azure 上に構築した AD DS)にて認証が行われるようになります。通信コストが低減できます。

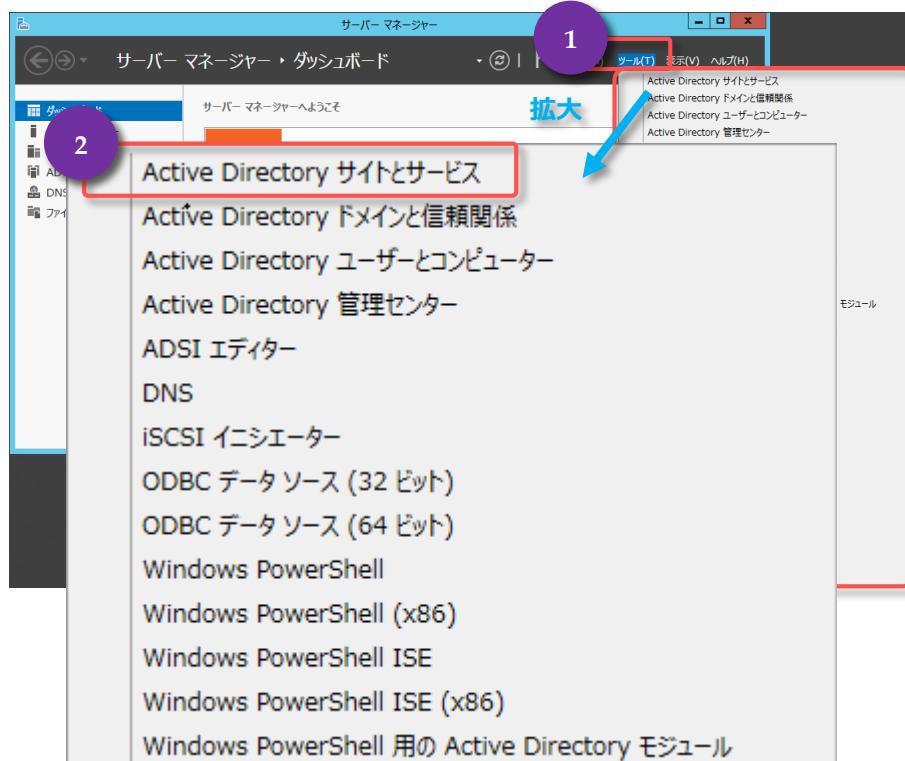
▼ サイトの作成

サイトの作成はオンプレミス側にて実施します。(尚、Azure 上で行っても構いませんがこの自習書ではオンプレミス側で作成し、Azure 側でレプリケートの確認を行います。)

1. オンプレミス側 AD DS(OPSTADDS01)の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。

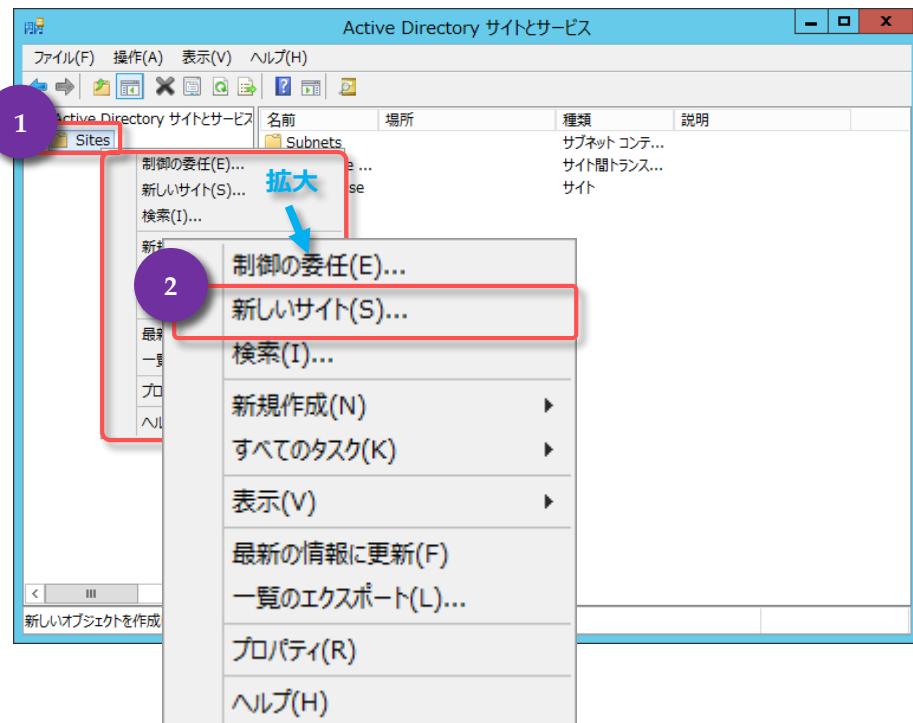


2. [ツール]をクリックし[Active Directory サイトとサービス]をクリックします。

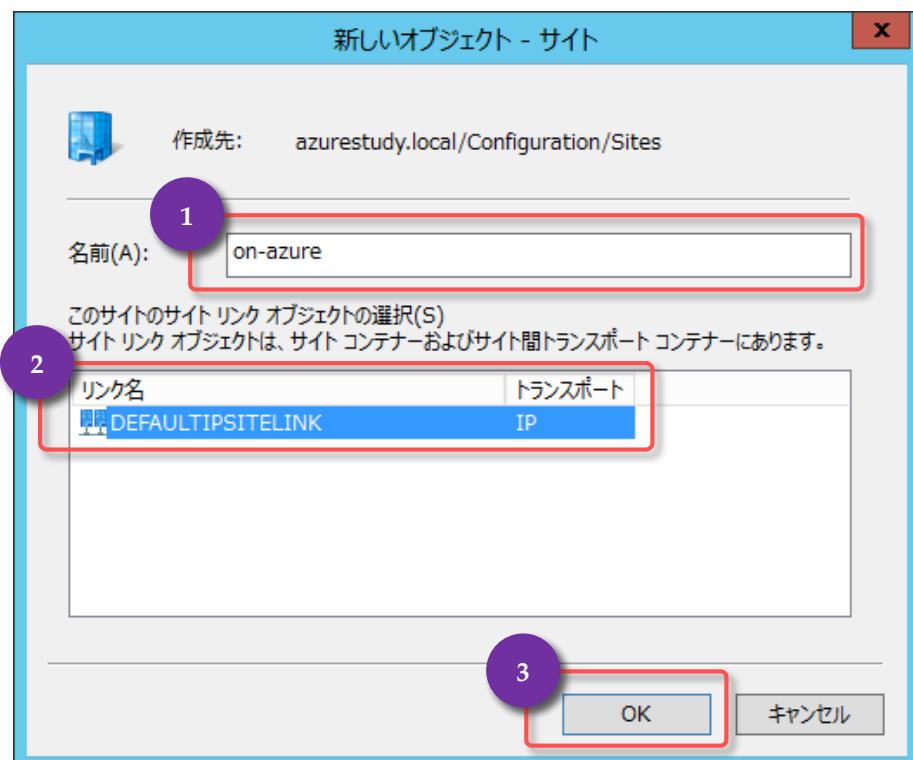


企業内システムと Microsoft Azure の VPN 接続、Active Directory 連携

3. [Site]を右クリックし [新しいサイト]をクリックします。

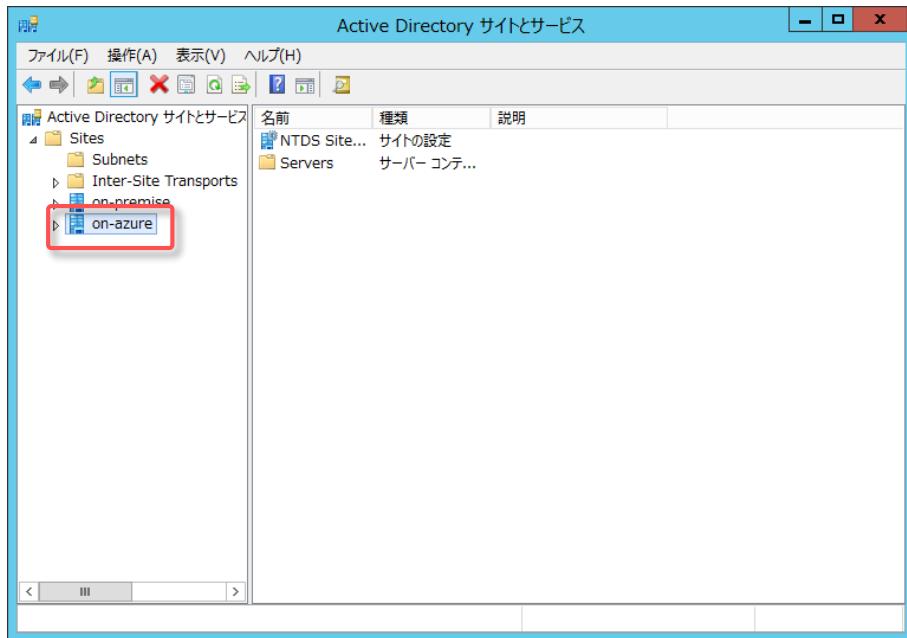


4. [名前]に「on-azure」と入力し[DEFAULTIPSITELINK]を選択し[OK]をクリックします。



企業内システムと Microsoft Azure の VPN 接続、Active Directory 連携

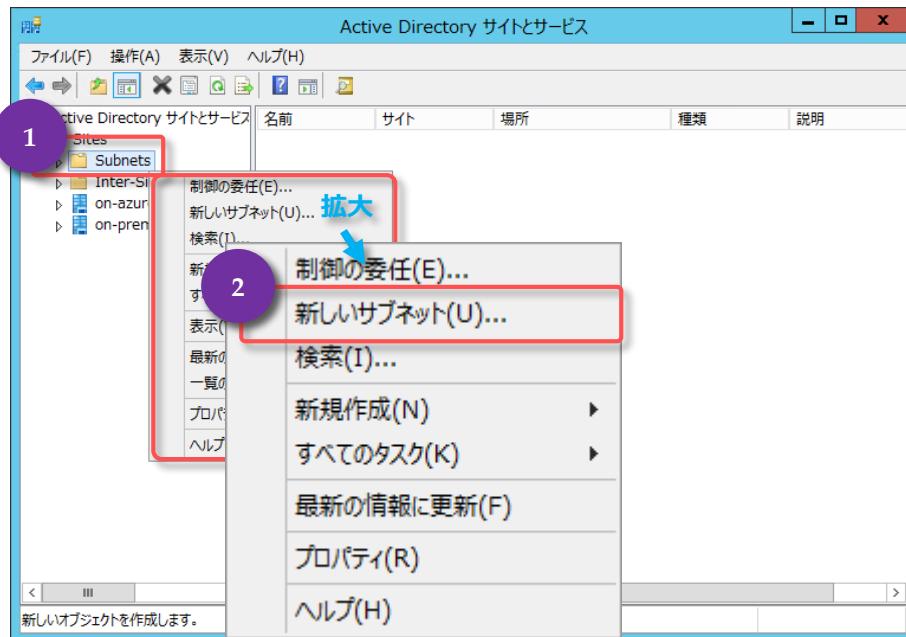
5. [on-azure]が作成されます。



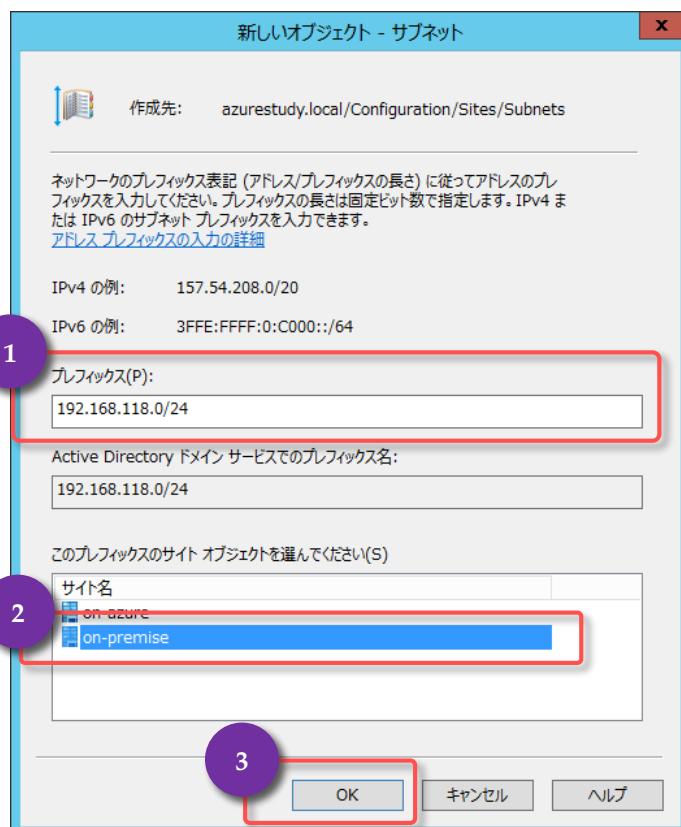
以上でサイトの作成が完了となります。

▼ サブネットの作成(オンプレミス環境用)

- [Subnets]を右クリックし[新しいサブネット]をクリックします。

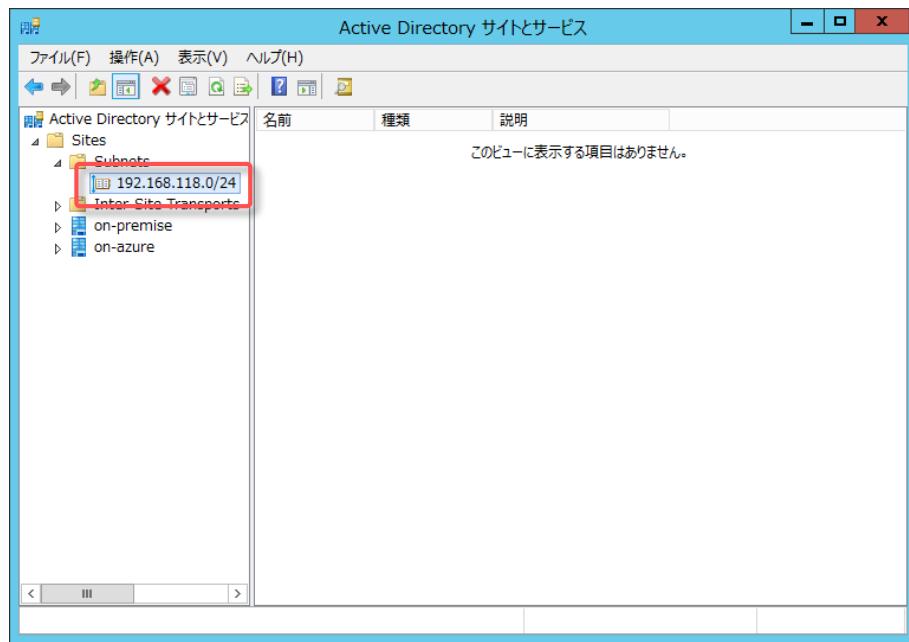


- [プレフィックス]にオンプレミス側のサブネットである[192.168.118.0/24]を入力し[on-premise]を選択し[OK]をクリックします。



企業内システムと Microsoft Azure の VPN 接続、Active Directory 連携

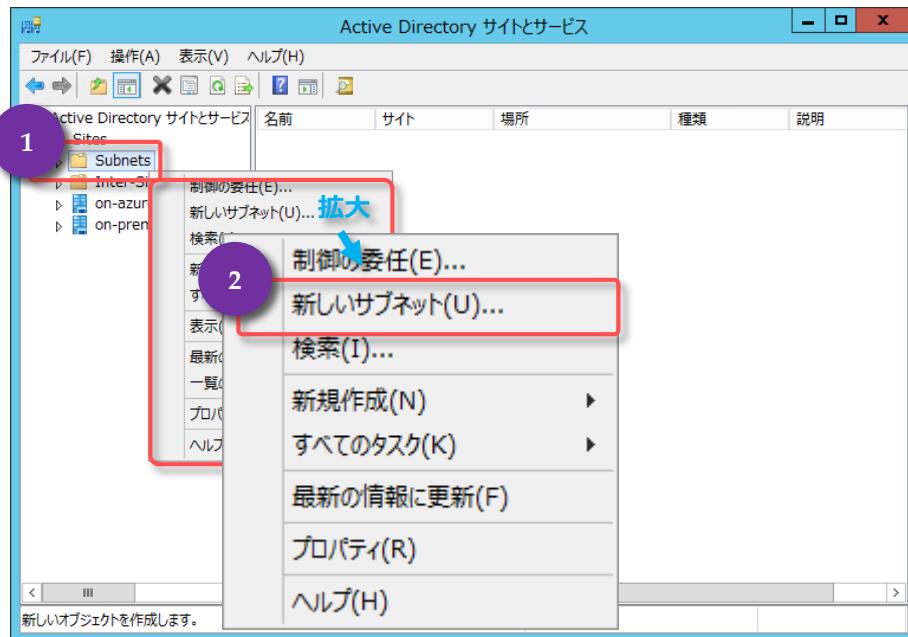
3. オンプレミス用のサブネットが作成されます。



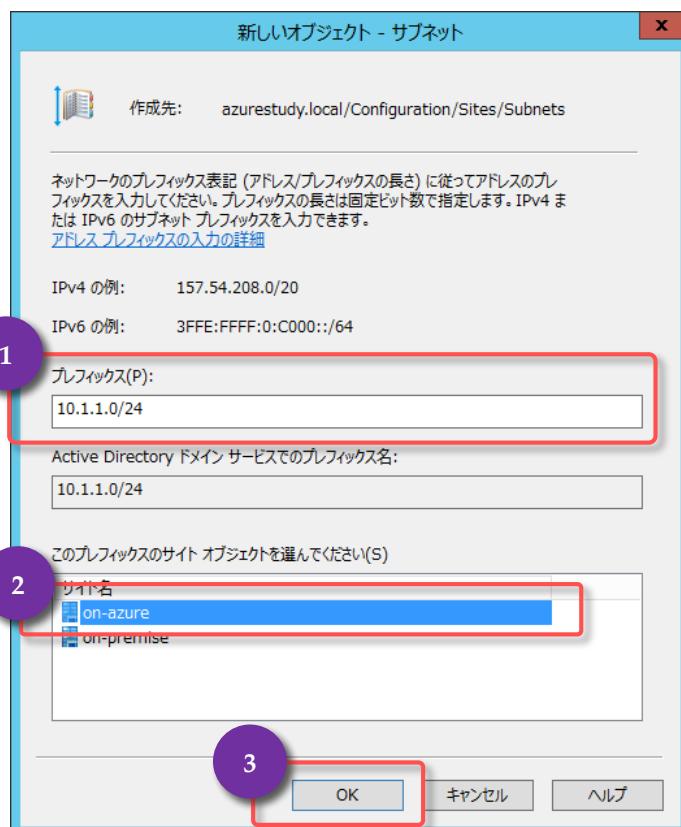
以上でオンプレミス用のサブネットの作成とサイトへの割り当てが完了となります。

▼ サブネットの作成(Azure 環境用)

- [Subnets]を右クリックし[新しいサブネット]をクリックします。

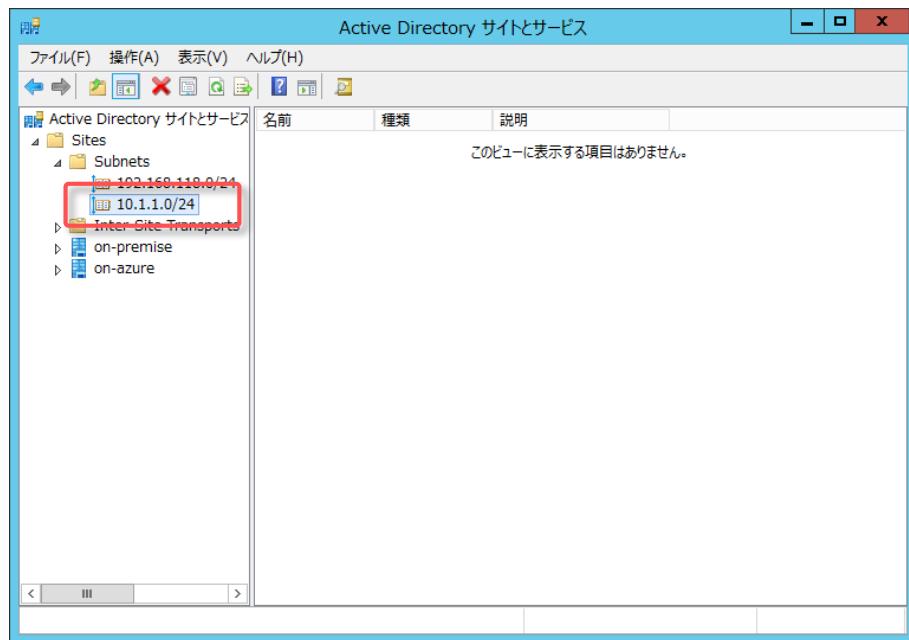


- [プレフィックス]に Azure 側のサブネットである「10.1.1.0/24」を入力し[on-azure]を選択し[OK]をクリックします。



企業内システムと Microsoft Azure の VPN 接続、Active Directory 連携

3. Azure 用のサブネットが作成されます。

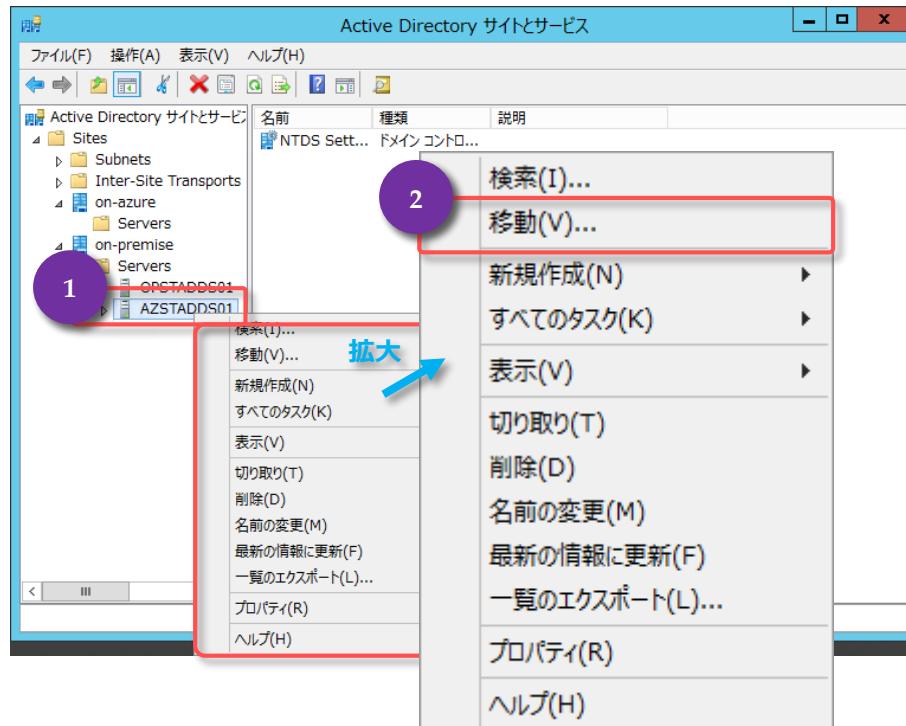


以上で Azure 用のサブネットの作成とサイトへの割り当てが完了となります。

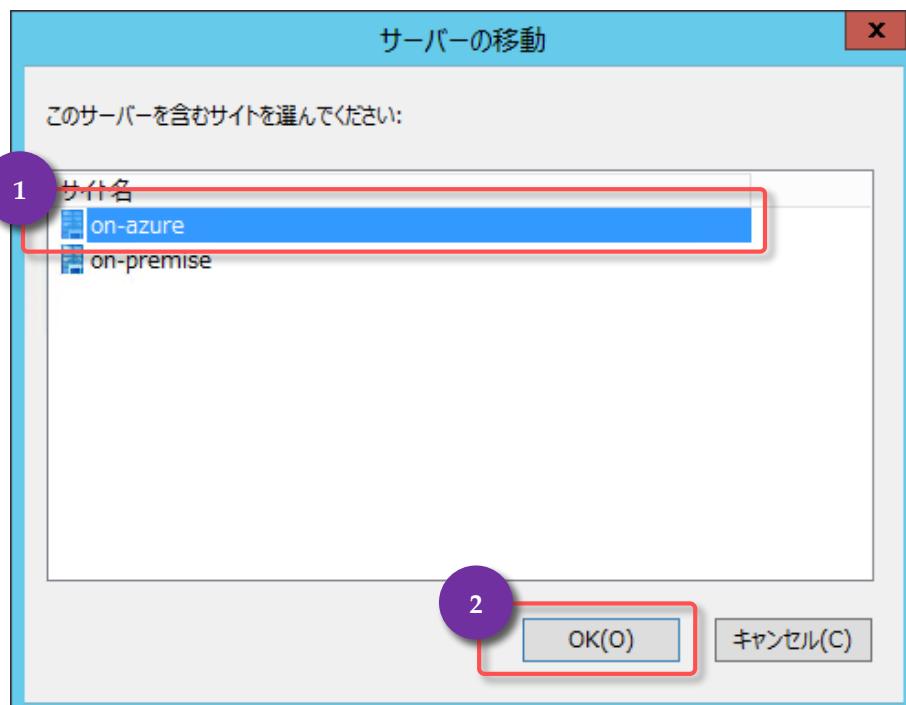
▼ オブジェクトの移動

Azure 上の AD DS を作成したサイトに移動します。

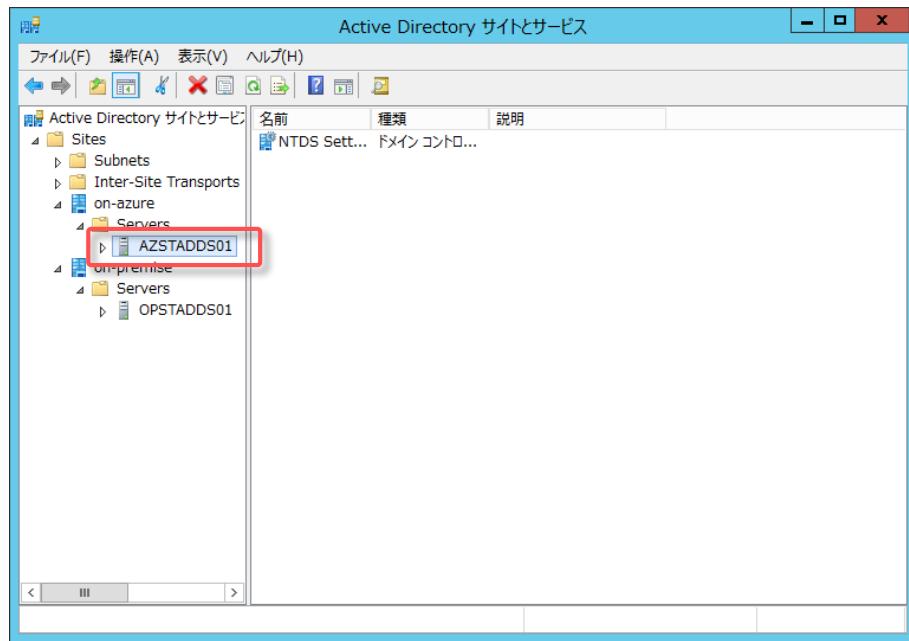
- [AZSTADDS01]を右クリックし[移動]をクリックします。



- [on-azure]を選択し[OK]をクリックします。



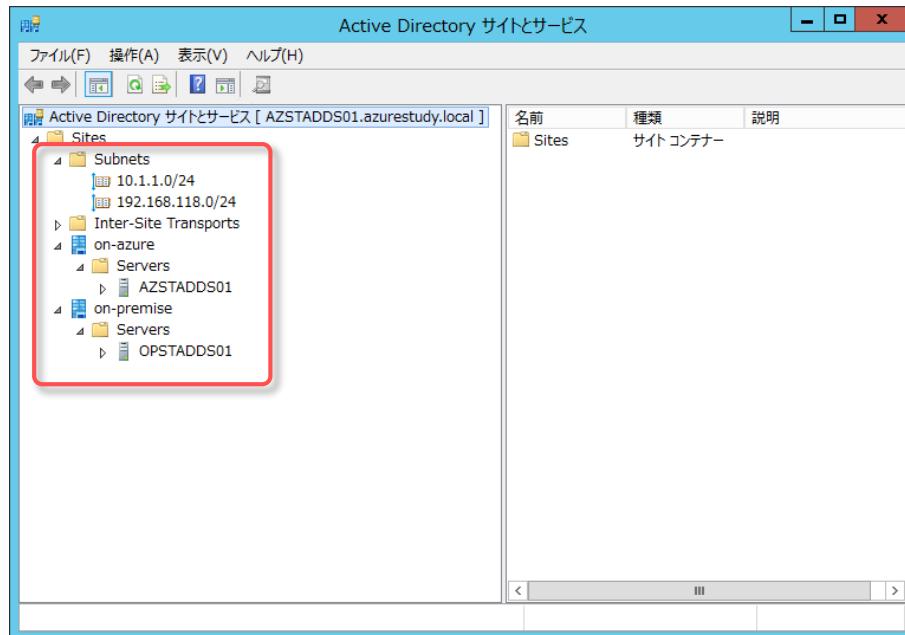
3. [AZSTADDS01]が[on-azure]配下の[Servers]に追加されます。



以上でオブジェクトの移動が完了となります。

➡ Azure 上での確認

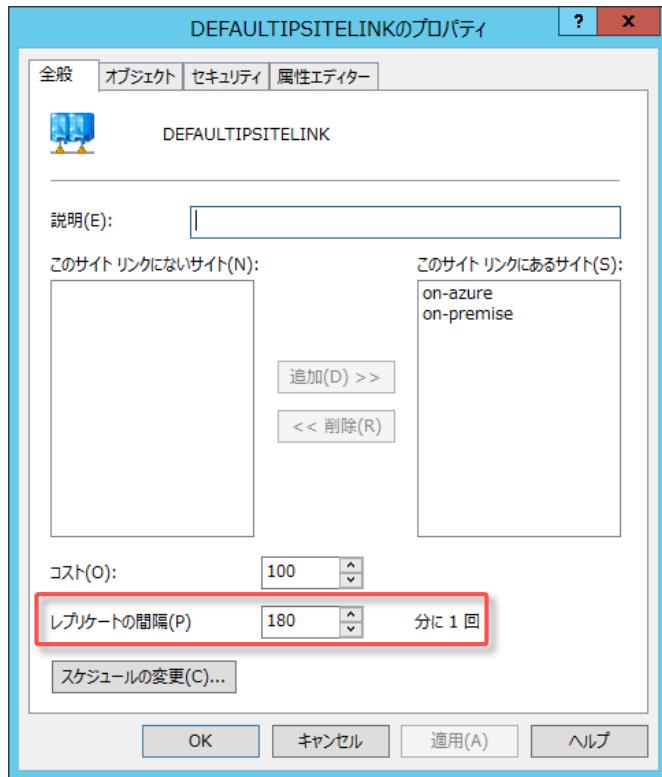
1. Azure 上に構築した AZSTADDS01 にログインしサイトとサブネットが作成されていることを確認します。



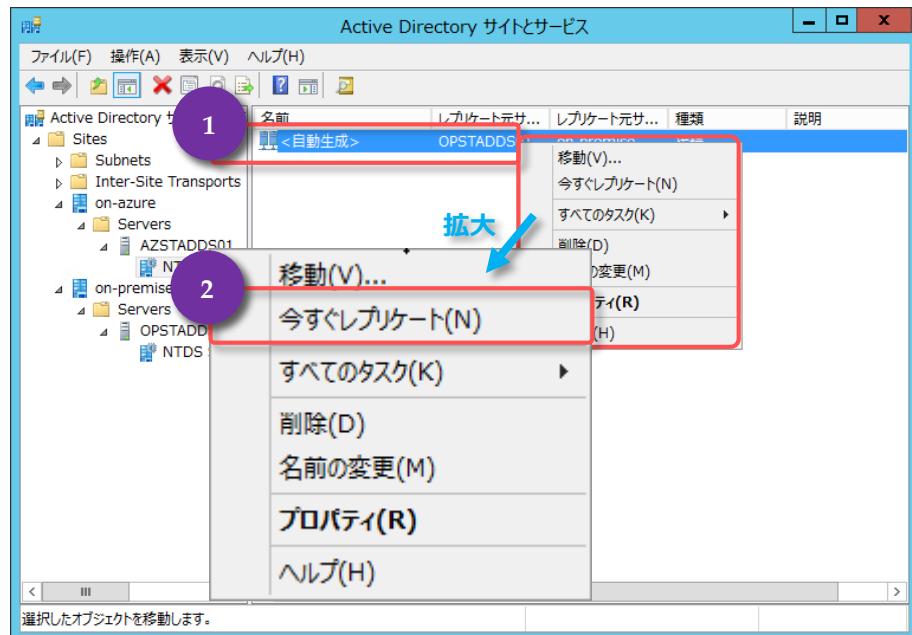
企業内システムと Microsoft Azure の VPN 接続、Active Directory 連携

Note : サイト間 AD DS のレプリケートについて

同じサイトに配置されている場合にはリアルタイムでレプリケートされますが、サイトを分けている場合、既定では180分となっています。



すぐにレプリケートをさせたい場合には[NTDS Settings]を選択し[<自動生成>]を右クリックし[今すぐレプリケート]をクリックします。



以上で Azure 上からのレプリケート確認が完了となります。

STEP 7. Azure 上に 2 台目以降の AD DS を構築する際のポイント

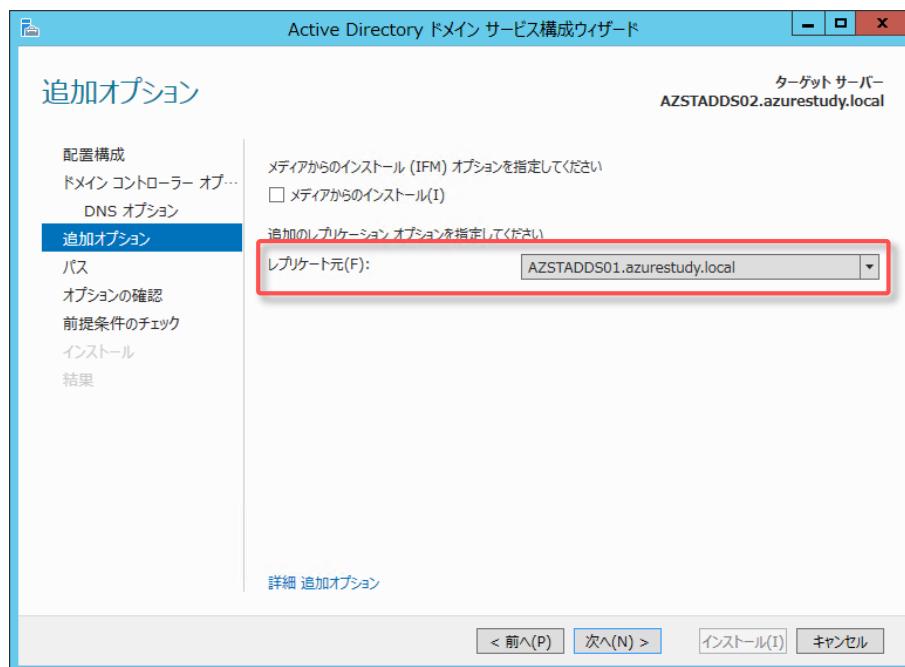
この STEP では、仮想マシン上に 2 台目以降の AD DS を構築するためのポイントについて説明します。

この STEP では、次のことを学習します。

- ✓ AD DS のレプリケート元の選択
- ✓ 複数台の AD DS とのレプリケート確認
- ✓ サイトの移動

7.1 AD DS のレプリケート元の選択

- ドメインに昇格させる際のレプリケート元を Azure 上に構築した AD DS にする。
レプリケーションの効率化から先に構築した AD DS(azstadds01.azurestudy.local)を明示的に選択します。

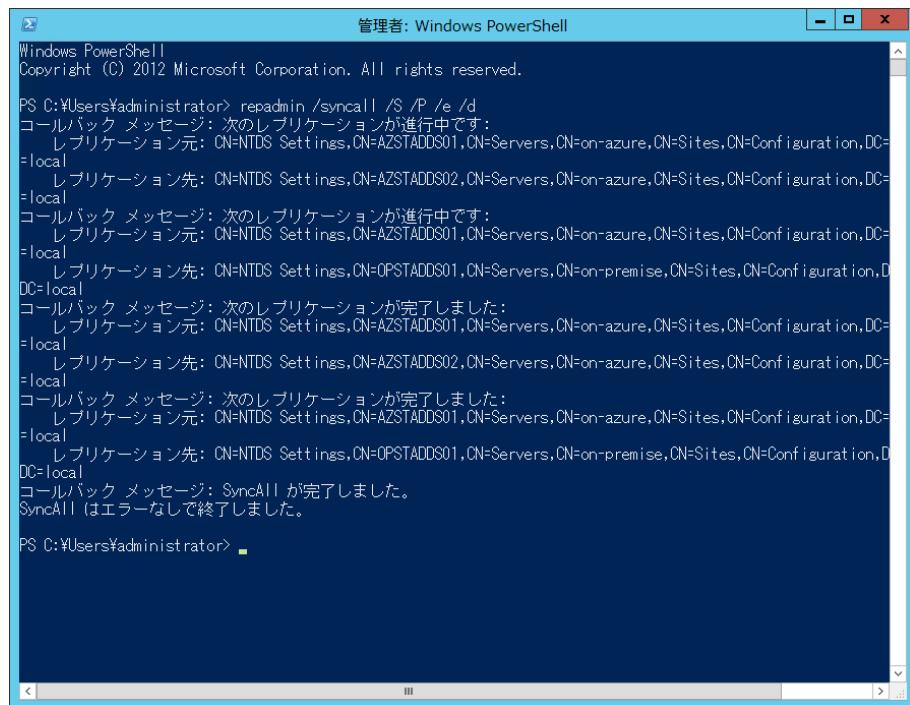


7.2 複数台の AD DS とのレプリケート確認

Azure 上に 2 台以上の AD DS を構築した際には、インストール時に選択したレプリケート元とのレプリケートを確認するだけでなく、他の AD DS(オンプレミスなど)とのレプリケートが可能かも確認します。

- PowerShell もしくはコマンドプロンプトを起動し、以下のコマンドを入力し、[Enter]キーを入力し、失敗が無いことを確認します。尚、オプションの「/S」はテストであるため、実際のレプリケーションは行われませんが、各 AD DS とレプリケーションが可能であるかの確認は可能です。

```
repadmin /syncall /S /P /e /d
```



The screenshot shows a Windows PowerShell window titled "管理者: Windows PowerShell". The command entered is "repadmin /syncall /S /P /e /d". The output displays multiple replication log entries for various servers and configurations, indicating successful synchronization between them.

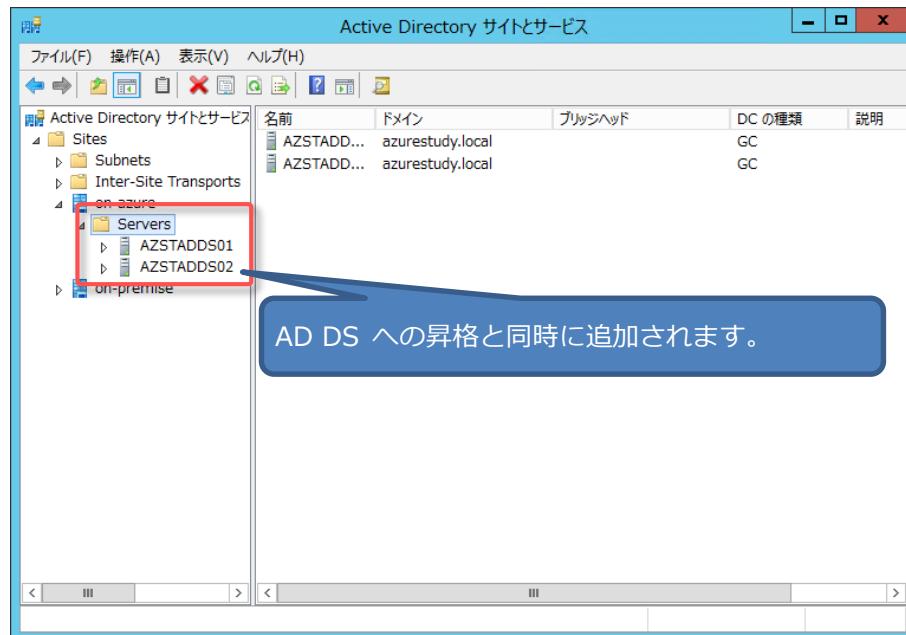
```
Windows PowerShell
Copyright (C) 2012 Microsoft Corporation. All rights reserved.

PS C:\Users\administrator> repadmin /syncall /S /P /e /d
コールバック メッセージ: 次のレプリケーションが進行中です:
    レプリケーション元: CN=NTDS Settings,CN=AZSTADDS01,CN=Servers,CN=on-azure,CN=Sites,CN=Configuration,DC=local
    レプリケーション先: CN=NTDS Settings,CN=AZSTADDS02,CN=Servers,CN=on-azure,CN=Sites,CN=Configuration,DC=local
コールバック メッセージ: 次のレプリケーションが進行中です:
    レプリケーション元: CN=NTDS Settings,CN=AZSTADDS01,CN=Servers,CN=on-azure,CN=Sites,CN=Configuration,DC=local
    レプリケーション先: CN=NTDS Settings,CN=OPSTADDS01,CN=Servers,CN=on-premise,CN=Sites,CN=Configuration,DC=local
コールバック メッセージ: 次のレプリケーションが完了しました:
    レプリケーション元: CN=NTDS Settings,CN=AZSTADDS01,CN=Servers,CN=on-azure,CN=Sites,CN=Configuration,DC=local
    レプリケーション先: CN=NTDS Settings,CN=AZSTADDS02,CN=Servers,CN=on-azure,CN=Sites,CN=Configuration,DC=local
コールバック メッセージ: 次のレプリケーションが完了しました:
    レプリケーション元: CN=NTDS Settings,CN=AZSTADDS01,CN=Servers,CN=on-azure,CN=Sites,CN=Configuration,DC=local
    レプリケーション先: CN=NTDS Settings,CN=OPSTADDS01,CN=Servers,CN=on-premise,CN=Sites,CN=Configuration,DC=local
コールバック メッセージ: SyncAll が完了しました。
SyncAll はエラーなしで終了しました。

PS C:\Users\administrator>
```

7.3 サイトの移動

- 2 台目以降はサブネットを作成しているため自動的に適切なサイトに移動されます。



STEP 8. 追加構築した AD DS を DNS サーバーとして登録する

この STEP では、Azure 上に構築した AD DS 2 台を仮想ネットワークに DNS サーバーとして登録する方法について説明します。

この STEP では、次のことを学習します。

- ✓ 仮想ネットワークへの DNS サーバーの追加設定

8.1 仮想ネットワークへの DNS サーバーの追加設定

Azure 上に構築した AD DS も DNS として登録します。また、優先順位を変更し、Azure 上のサービスは優先的に Azure 上の AD DS に名前解決の問合せを行うよう、設定を行います。

1. Azure 管理ポータルにサインインし、左のメニューから[ネットワーク]をクリックします。



2. [DNS サーバー]をクリックします。

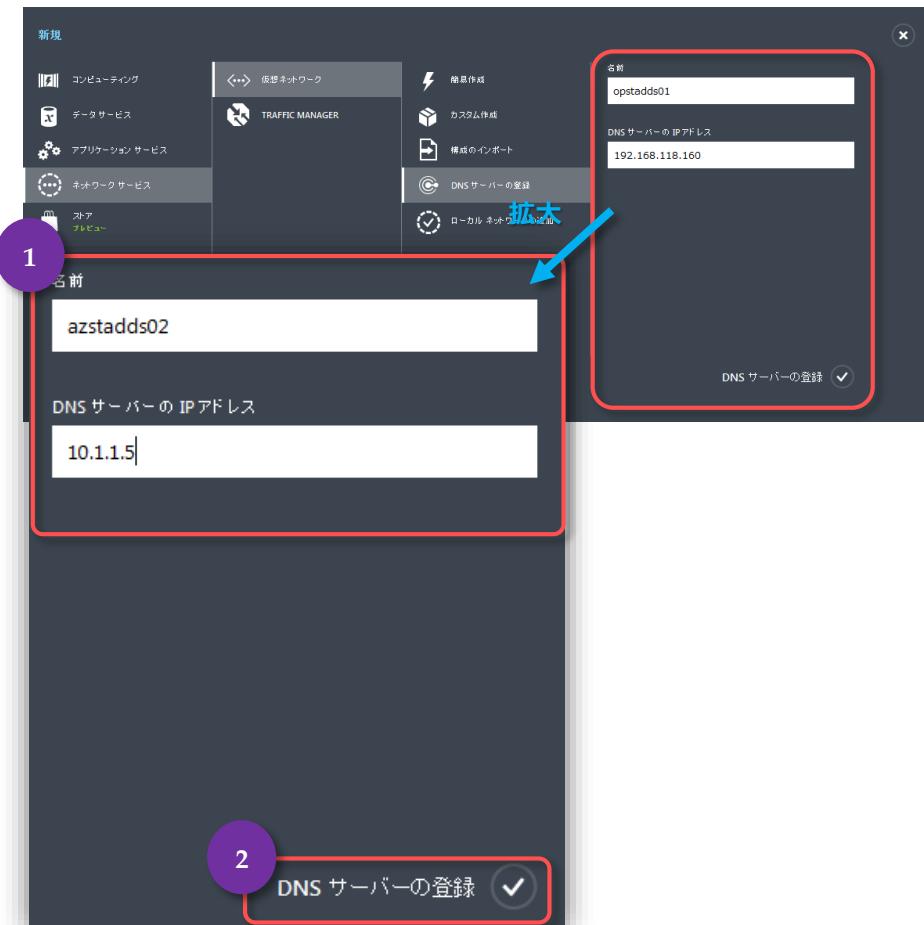


3. 2台目以降の DNS サーバーを登録する場合には、画面したの [+新規] をクリックします。

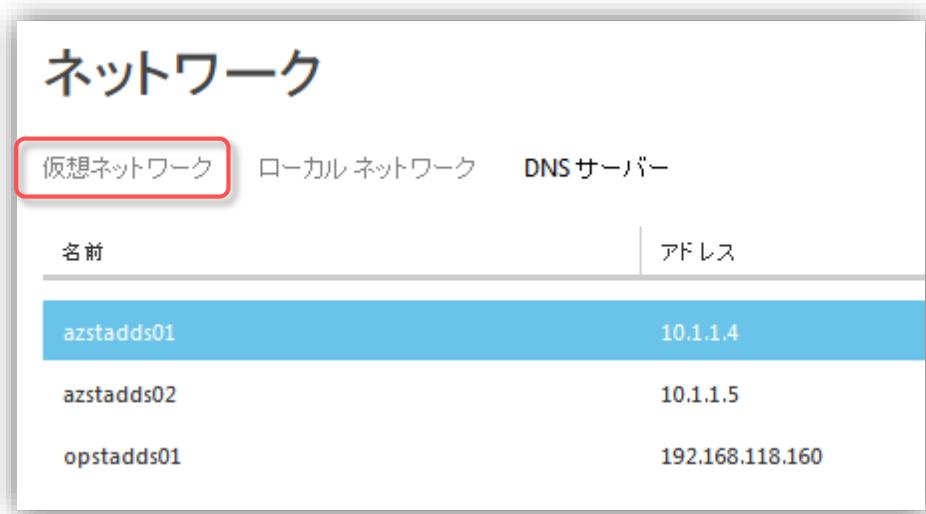


企業内システムと Microsoft Azure の VPN 接続、Active Directory 連携

4. 「DNS サーバーの登録」を選択し、[名前]に「azstadds01」と入力し[DNS サーバーの IP アドレス]に「10.1.1.4」と入力します。
[DNS サーバーの登録]をクリックします。



5. 同様に Azure 側の 2 台目の AD DS を登録した後、[仮想ネットワーク]をクリックします。



6. [tokyo-nw]をクリックします。

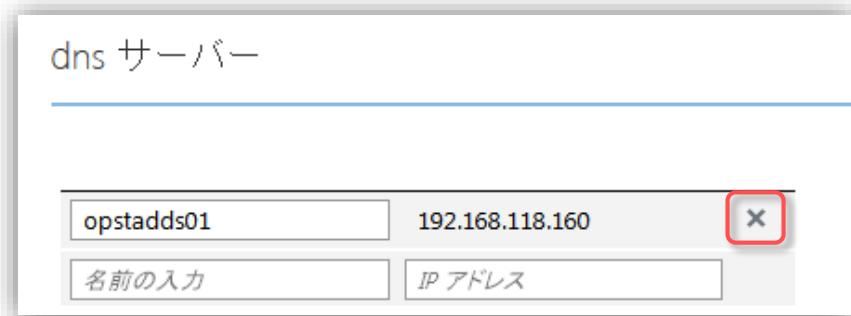


7. [構成]をクリックします。



8. [x]をクリックし、オンプレミスの AD DS を一旦削除します。

dns サーバーは上位ほど優先順位が高くなります。そのため、このまま Azure 上の AD DS を登録してしまうとオンプレミスの AD DS が最優先となってしまうため、これを削除したのちに追加しなおします。

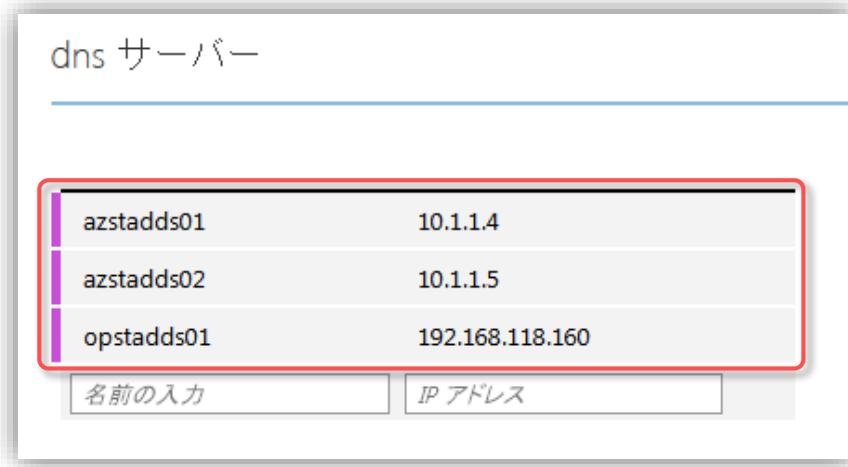


9. 再度以下の順に追加していきます。

azstadds01

azstadds02

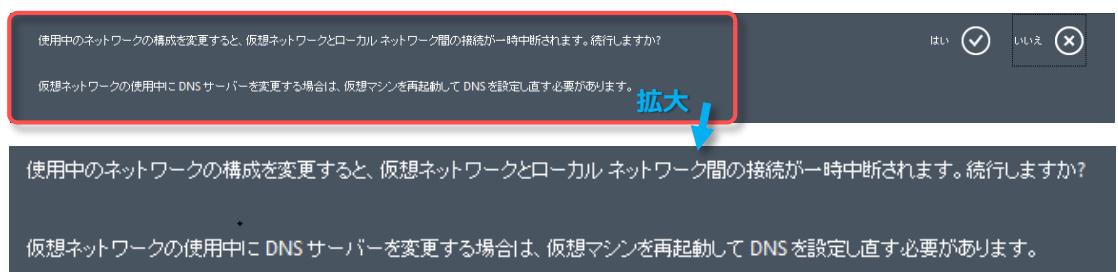
opstadds01



10. 画面下の[保存]をクリックします。



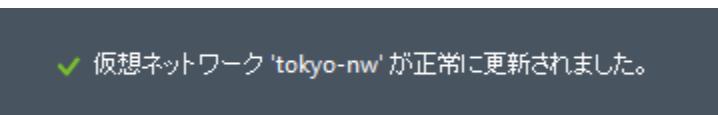
11. D S サーバーの設定を変更する際、一時的にネットワークが切断されることがあるため、その警告が表示されます。[はい]をクリックします。



12. 更新中です。



13. 更新完了です。



14. 設定が確定すると、各 DNS サーバー(AD DS)名の左に表示されていた紫のバーが消えます。

The screenshot shows a list of DNS servers with their names and IP addresses. The first two entries, "azstadds01" and "azstadds02", are highlighted with a red rectangle. Below the list are two input fields: "名前の入力" (Name input) and "IP アドレス" (IP Address).

| 名前 | IP アドレス |
|------------|-----------------|
| azstadds01 | 10.1.1.4 |
| azstadds02 | 10.1.1.5 |
| opstadds01 | 192.168.118.160 |

以上で DNS サーバーの追加設定が完了となります。

尚、仮想マシンの DNS を更新するためには、各仮想マシンを再起動します。

おわりに

この自習書では、Azure 上に AD DS を構築する手順について学習しました。

AD DS を Azure 上に構築できるようになることは、より幅広く AD DS の機能を活用できるようになるだけではなく、コスト削減、迅速な展開、ビジネス継続性の向上、災害対策、社内ネットワークに対する依存の低減などのメリットを得ることができます。

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」
- Microsoft Azure 自習書シリーズ「企業内システムと Microsoft Azure の VPN 接続、ADFS、Office365 との連携」
- Microsoft Azure 自習書シリーズ「企業内システムと Microsoft Azure の VPN 接続、ファイルサーバー連携」
- 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」

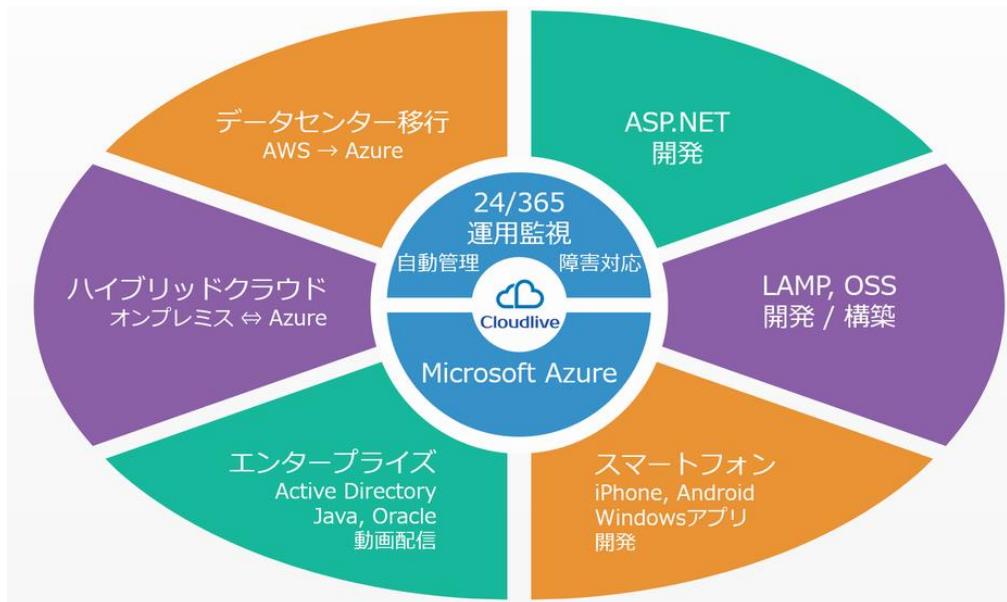
この自習書が仮想マシン上に Active Directory Domain Service を構築する手助けになれば幸いです。

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