Microsoft Windows: Active DirectoryをOracle Cloud Infrastructureに拡張

クイック・スタート・ホワイト・ペーパー

ORACLE WHITEPAPER | 2017年6月 | バージョン1.1

免責事項

下記事項は、弊社の一般的な製品の方向性に関する概要を説明するものです。また、情報提供を唯一の目的とするものであり、いかなる契約にも組み込むことはできません。マテリアルやコード、機能の提供をコミットメント（確約）するものではなく、購買を決定する際の判断材料になさらないで下さい。オラクルの製品に関して記載されている機能の開発、リリース、および時期については、弊社の裁量により決定されます。

目次

前提

このドキュメントの利用者に必要な条件を次に示します。

- Oracle Cloud Infrastructureの基本に精通していること
  - https://docs.us-phoenix-1.oraclecloud.com/

    Oracle Cloud Infrastructureのプラットフォームを使用するのが今回が初めての場合、Oracle Cloud Infrastructureのウォークスルーを強くお薦めします。
    - https://docs.us-phoenix-1.oraclecloud.com/Content/GSG/Reference/overviewworkflow.htm
- 既存のVirtual Cloud Network (VCN)がすでに作成済および構成済であること
  - https://docs.us-phoenix-1.oraclecloud.com/Content/Network/Tasks/managingVCNs.htm
- オンプレミス環境とVCNの間でVPNまたはFastConnect接続が完全に構成済であること
  - FastConnect: https://docs.us-phoenix-1.oraclecloud.com/Content/Network/Concepts/fastconnect.htm
  - VPN: https://docs.us-phoenix-1.oraclecloud.com/Content/Network/Tasks/managingIPsec.htm
- Active Directoryの基本を理解していること
  - Active Directoryのキー・コンセプト

対象読者

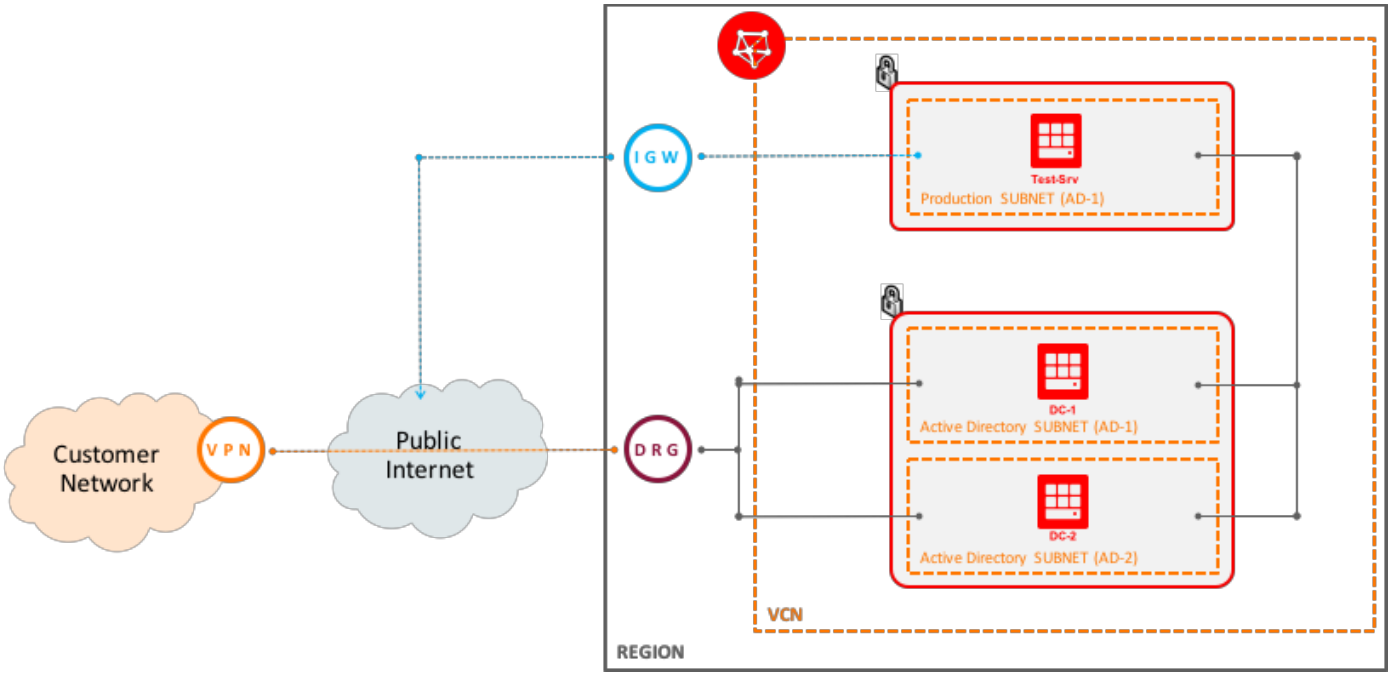
このホワイト・ペーパーは、オンプレミスのActive Directory環境をOracle Cloud Infrastructureに拡張する方法を理解したいお客様を対象としています。

はじめに

このホワイト・ペーパーでは、Oracle Cloud InfrastructureでWindows Active Directoryインフラストラクチャを拡張するプロセスを段階的に説明します。2つの読取り専用ドメイン・コントローラが、それぞれ異なる可用性ドメイン(AD)にインストールされます(冗長化のため)。3つ目のシステムは、Oracle Cloud Infrastructureで実行されているドメイン・コントローラに対して参加とログインの両方が行えることを確認するためのテスト・サーバーとして使用されます。

これを遂行するには、いくつかの前提条件があります。

- オンプレミス環境とOracle Cloud Infrastructure間に安全な(非パブリック)接続が存在すること(次の図に示すように、これは、FastConnectまたはIPSec VPN接続のいずれかになります)。
- オンプレミスのActive Directory環境でドメイン管理アカウント(またはドメインへの参加とドメイン・コントローラのインストールの両方の権限を持つアカウント)を所有していること。



ベスト・プラクティス

ドメイン・コントローラは、インターネットからの外部的なアクセスが不可である必要があります。許可されるアクセスは、オンプレミス・ネットワークからの特定のIPアドレスからのみである必要があります。これらのIPアドレスは、現在のオンプレミスActive Directoryコントローラおよびドメイン・コントローラの作成/管理に使用される管理デスクトップを含む必要があります。

ネットワーク環境の設定

このホワイト・ペーパーでは、VCNがすでに構成済であり、少なくとも2つの新しいサブネットを作成するのに十分なIPアドレス空間があることを前提としています。これらのサブネットは(前述の図に示すように)、次のステップで作成する2つの読取り専用ドメイン・コントローラのホスティングに使用されます。サブネットが可用性ドメイン(AD)に関連付けられていることにより、各ドメイン・コントローラが異なるADに存在するようにでき、Active Directory環境内の単一障害点が取り除かれます。この後の例では、10.x.x.xのIP空間が前提となっています。

各サブネットには、1つのルート表および1つ以上のセキュリティ・リストが必要です。VCNは、ドメイン・コントローラのサブネットのルート表を使用してオンプレミス環境にすでに接続されているため、このルート表はすでに存在している必要があります。テスト・サーバー(インターネット・アクセスが必要と仮定)に使用できるルート表がまだない場合、次の説明に従いルート表を作成できます。

セキュリティ・リストの作成

Active Directoryドメイン・コントローラ用とテスト・サーバー用の少なくとも2つのセキュリティ・リストが必要です。この項では、セキュリティ・リストそのもののみを作成し、セキュリティ・リスト・ルール(このホワイト・ペーパーの後半で説明します)は作成しません。

2つのセキュリティ・リストを作成します。

- Production - Admin (Public)
- Production - Applications (Private)

ベスト・プラクティス

Oracle Cloud Infrastructureコンポーネントのネーミングは可能な限り常に規範に従ったものにする必要があります。将来、環境に再度アクセスする必要がある場合、アクセスが簡単になります。

ルート表の作成

次に、テストに使用できるルート表を作成します。このルート表は、テスト・サーバーがインターネットにルーティングできるようにするために使用されます。ドメイン・コントローラに使用されるルート表は、オンプレミス・ネットワークにトラフィックをルーティングする必要があります。

次のルート表を作成します。

- Production - Application (Private)

セキュリティ・リスト・ルールの作成

Active Directoryは、RPC、NetBIOS、SMB、LDAP、Kerberos、WINSおよびDNSなど、多くの通信プロトコルを使用します。これらの一部のみが構成で使用される場合がありますが、ここではすべてをリストします。たとえば、WINSが自分の環境で使用されていない場合、これらをリストから除外できます。

ベスト・プラクティスの項で述べたように、すべてのドメイン・コントローラは、外部IPアドレスを持たないか、インターネットからアクセスされないサブネット内に存在する必要があります。このため、サブネットとActive Directoryサブネット間で通信するすべてのポートのみを有効化する場合があります。しかし、このように選択した場合、これらのサブネットからの潜在的な攻撃パスが依然として開いていることに注意してください。したがって、次に示すサブネット間のポートのみを開くことがベスト・プラクティスとなります。

名前	プロトコル	ポート
DNS	TCP、UDP	53
LDAP	TCP、UDP	389
LDAP over SSL	TCP	636
グローバル・カタログLDAP	TCP	3268
グローバル・カタログLDAP over SSL	TCP	3269
Kerberos	TCP、UDP	88
RPCエンドポイント・マッパー	TCP、UDP	135
NetBIOS名前サービス	TCP、UDP	137
NetBIOSデータグラム・サービス	UDP	138
NetBIOSセッション・サービス	TCP	139
SMB over IP (Microsoft-DS)	TCP、UDP	445
WINS解決	TCP、UDP	1512
WINSレプリケーション	TCP、UDP	42

新しいActive Directoryサブネットへの必須のポート通信を許可する新しいイングレス・ルールを**Production Active Directory**セキュリティ・リストに作成します(このルールで2つのドメイン・コントローラ・サブネット間のトラフィックが許可されていることを確認します)。また、内部のオンプレミス・ネットワークからすべての3つのサブネットへのTCPポート3389 (RDP)を有効にしていることも確認します。

サブネットの作成

前述したように、少なくとも2つのサブネットが必要です(3つ目の可用性ドメイン内の3つ目のサブネットは、Active Directory環境の追加の可用性のために使用できます)。このホワイト・ペーパーのサブネットは次のとおりです。

名前	可用性ドメイン	CIDRブロック	ルート表	セキュリティ・リスト
Production - Admin - PHX-AD-1	PHX-AD-1	10.0.1.0/24	Production - Admin (Private)	Production - Admin (Private)
Production - Admin - PHX-AD-2	PHX-AD-2	10.0.2.0/24	Production - Admin (Private)	Production - Admin (Private)
Production - Application - PHX-AD-1	PHX-AD-1	10.0.10.0/24	Production - Application (Private)	Production - Application (Private)

インスタンス

この環境は、3つのインスタンスを必要とします。2つはActive Directoryドメイン・コントローラに使用され、3つ目はテスト・サーバーとして使用されます。

次のプロパティを使用して、インスタンス・シェイプを作成します(このホワイト・ペーパーに使用したインスタンス・シェイプ(VM.Standard1.4)は推奨なので、適合するようにスケール・アップ/ダウンできます)。

名前	イメージ	シェイプ	可用性ドメイン	サブネット
DC-1	Windows-Server-2012-R2-Standard-Edition-VM	VM.Standard1.4	PHX-AD-1	Production Active Directory - PHX-AD-1
DC-2	Windows-Server-2012-R2-Standard-Edition-VM	VM.Standard1.4	PHX-AD-2	Production Active Directory - PHX-AD-2
Test-Srv	Windows-Server-2012-R2-Standard-Edition-VM	VM.Standard1.4	(ネットワーク構成に依存)	(ネットワーク構成に依存)

各インスタンスについて、RFC1918 IPアドレスを記録します。

インスタンス	RFC1918 IP
DC-1	
DC-2	
Test-SRV	

ドメイン・コントローラの構成

適切な役割および機能をサーバーにインストールし、読取り専用のドメイン・コントローラに昇格する準備ができました。これを行うには、次のステップを完了する必要があります。

1. Active Directoryドメイン・サービス役割とDNSサーバー役割をインストールします。
2. DNSサーバーを構成します。
3. ドメインに参加します。
4. サーバーを読取り専用ドメイン・コントローラに昇格します。

サーバーの役割のインストール

このサーバーがドメイン・コントローラに昇格されるようにするには、**Active Directoryドメイン・サービス**役割をインストールする必要があります。また、DNSエントリの一部をオンプレミスのDNSサーバーからレプリケートする場合、**DNSサーバー**役割もインストールできます。この役割はオプションですが、次の説明に含められています。

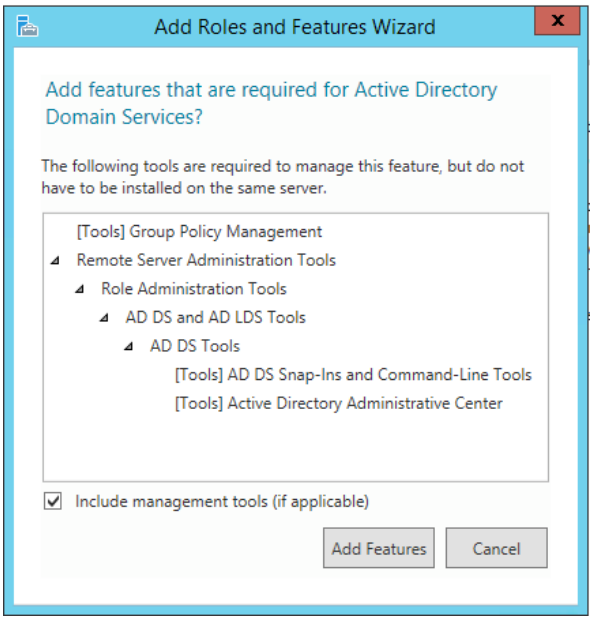
必要な情報:

1. Windows OPCアカウントの資格証明。

Active Directoryドメイン・サービス役割のインストール:

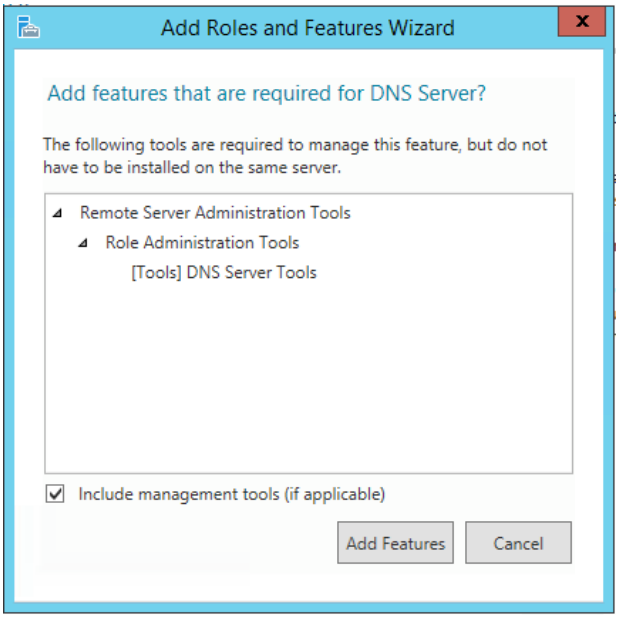
1. OPCユーザー資格証明(管理者ユーザー)を使用して、ドメイン・コントローラに昇格される最初のインスタンスにログインします。
2. **サーバー マネージャー**を実行します。
3. 「**役割と機能の追加**」をクリックします。
4. 「**サーバーの役割**」ダイアログが表示されるまで、「**次へ**」をクリックします。
5. 「**Active Directoryドメイン サービス**」チェックボックスを選択します。

6. 表示されたダイアログ・ボックスで、「**機能の追加**」ボタンをクリックします。



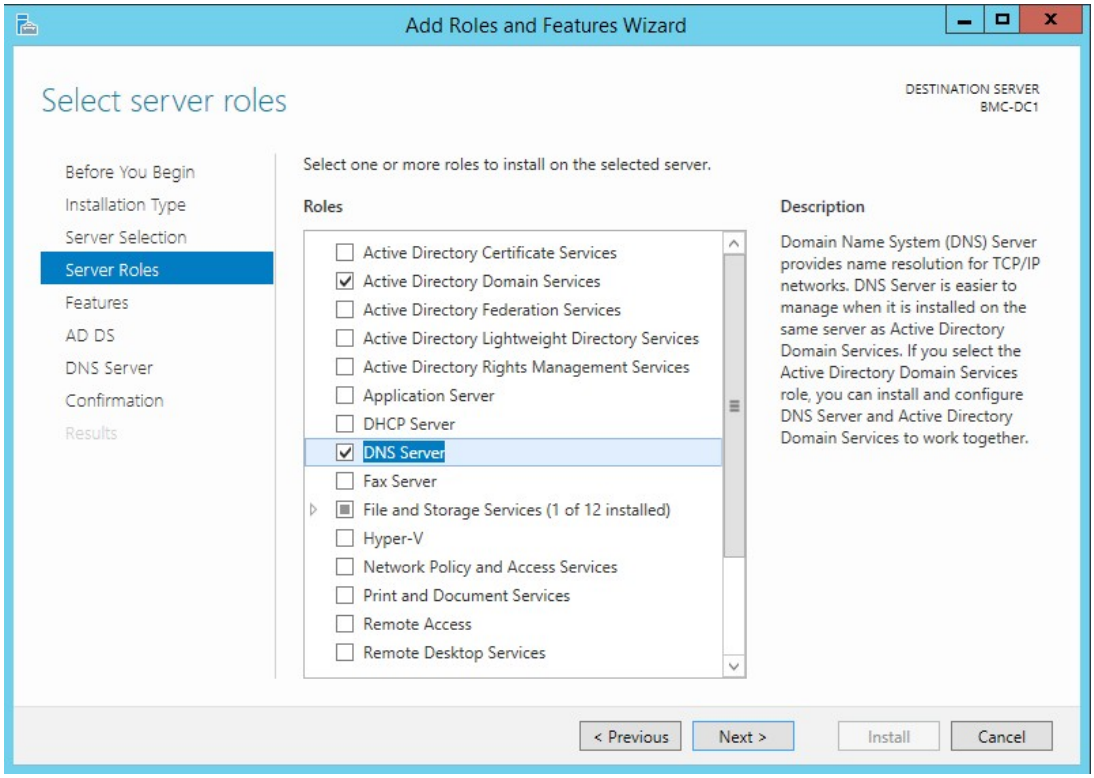
7. (オプション)「**DNSサーバー**」チェックボックスを選択します。

8. 表示されたダイアログ・ボックスで、「**機能の追加**」ボタンをクリックします。

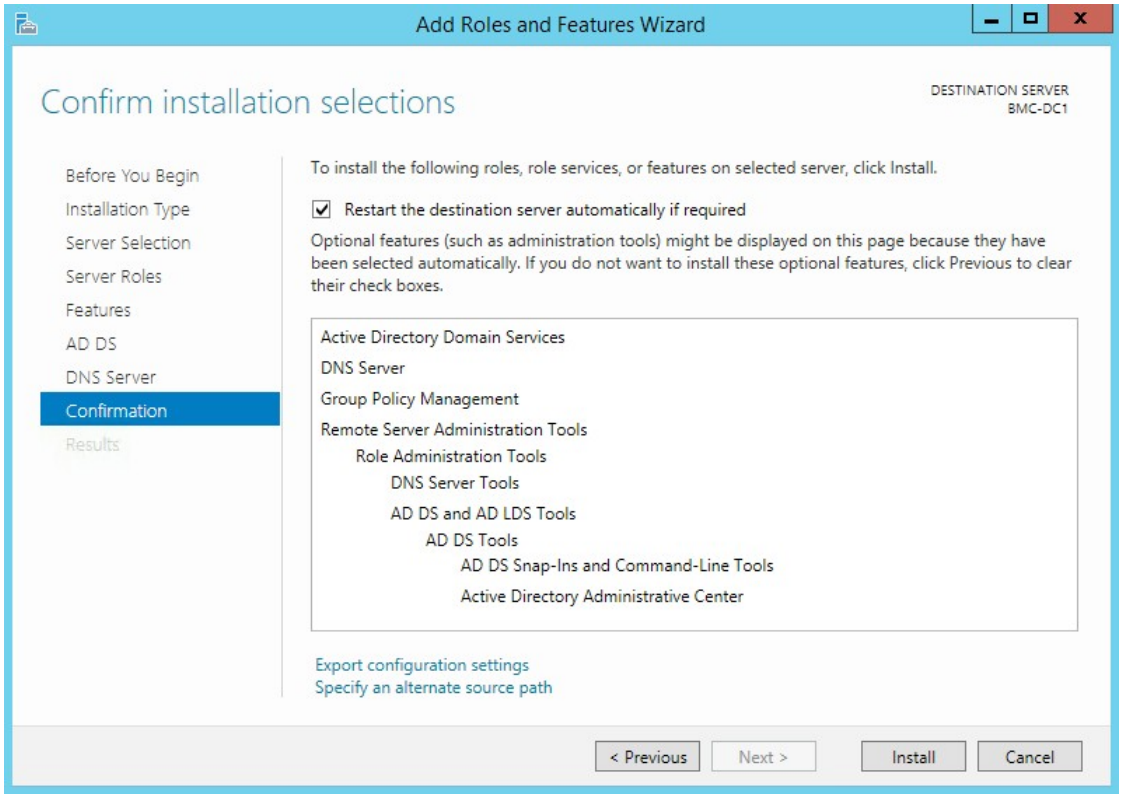


注意: DNSサーバー役割のインストールを選択した場合、静的IPアドレスがコンピュータに見つからなかったことを知らせる警告ダイアログ・ボックスが表示されます。このインスタンスに関連付けられるIPアドレスは、インスタンスの有効期間に関連付けられるため、「**続行**」ボタンをクリックできます。

9. これらの2つのオプションを選択したら、「**次へ**」をクリックして続行します。



10. 「確認」ダイアログが表示されるまで、「**次へ**」をクリックします。「**必要に応じて対象サーバーを自動的に再起動する**」をチェックして(ポップ・アップ・ダイアログ・ボックスを受け入れる)、「**インストール**」をクリックします。



11. 新規役割のインストールが開始されます。インストールが完了したら、「**閉じる**」をクリックして、「**機能と役割の追加**」ウィザードを完了します。

2つ目のドメイン・コントローラについて前述のステップを繰り返します。

DNSの構成

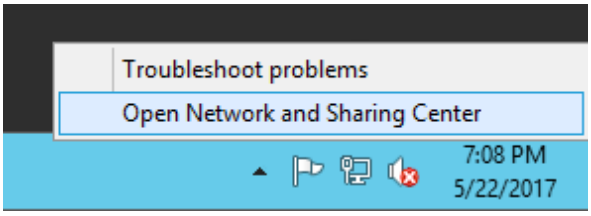
ドメインに参加し、ドメイン・コントローラを昇格するには、オンプレミスのActive Directory DNSサーバーを指すようにDNSサーバーを再構成する必要があります。(別のオプションとして、オンプレミスのDNSサーバーからZone転送を受信できるOracle Cloud Infrastructure環境にDNSサーバーを作成することもできます。この場合、Oracle Cloud InfrastructureのDNSサーバーを使用してドメインに参加できます。)設定予定のドメイン・コントローラ上のDNSサーバーをオンプレミスDNSサーバーにマップすると、サーバーでドメイン情報を解決し、ドメインに参加できるようになります。

必要な情報:

1. Windows OPCアカウントの資格証明。
2. オンプレミスのDNSサーバーのIPアドレス。

オンプレスDNSサーバーの構成:

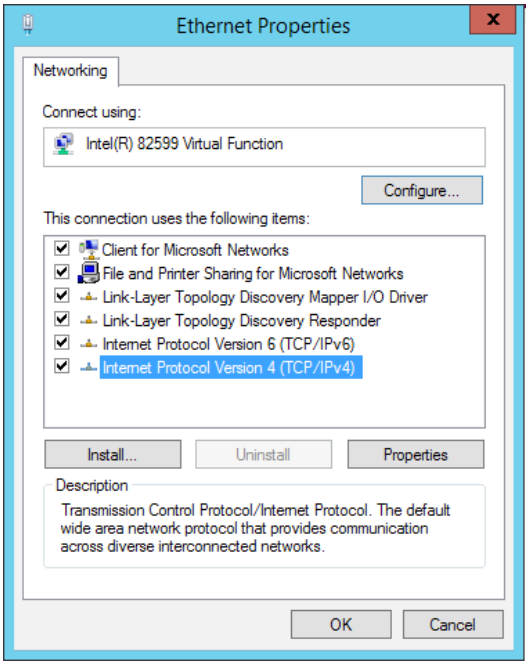
1. 1つ目のシステムにOPCユーザーとしてログインします。
2. 画面の右隅のネットワーク・アイコンを右クリックして、「**ネットワークと共有センターを開く**」を選択します。



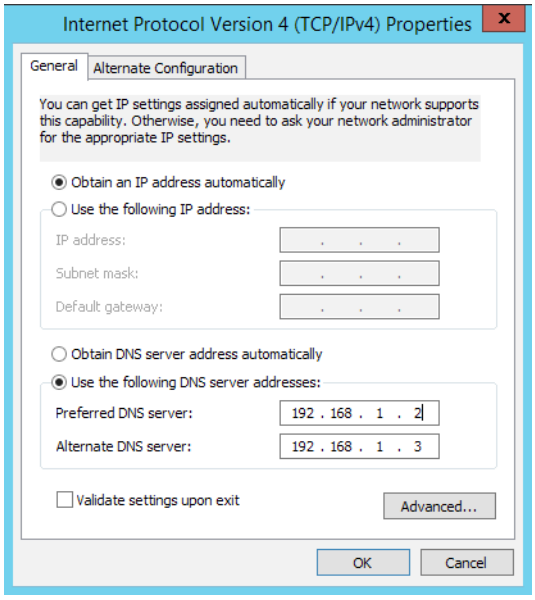
3. 左ペインで「**アダプターの設定の変更**」をクリックします。

   注意: ここで説明する「**ネットワーク接続**」ウィンドウに表示されるオプションは、仮想マシン・インスタンスとして起動されるインスタンス用です。Windowsサーバーをベア・メタル・インスタンスとして起動した場合、アダプタの名前は異なりますが、ステップはインスタンス・タイプにかかわらず同じです。

4. **イーサネット**・ネットワーク・アダプタを右クリックし(ラベルは"Intel(R) 82599 Virtual function"となっています)、「**プロパティ**」を選択します。(ベア・メタル・インスタンスの場合、ラベルは"Intel(R) Ethernet Server Adapter X520-2"またはそれに類似したものになります。)
5. 「**インターネット プロトコル バージョン4 (TCP/IPv4)**」を選択し、「**プロパティ**」をクリックします。



6. 「**次のDNSサーバーのアドレスを使う**」を選択します。
7. オンプレミスのDNSサーバーのIPアドレスを入力し、「**OK**」をクリックします。



8. 「**閉じる**」をクリックします。
9. パブリックWebサイトに移動するか(インスタンスにインターネット・アクセスがあることが前提)、コマンド・プロンプトで**nslookup**コマンドを実行して、DNSサーバーが作動していることをテストします。

2つ目のドメイン・コントローラについて前述のステップを繰り返します。

ドメインへの参加

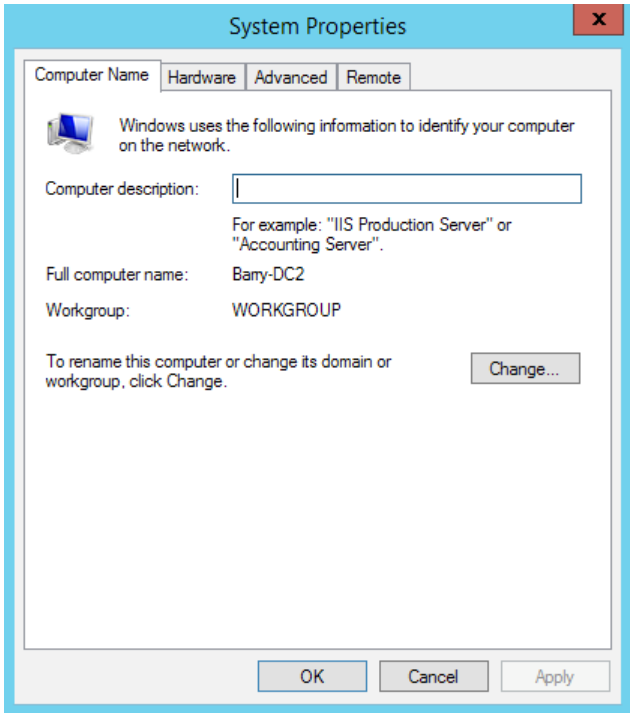
DNSサーバーがインスタンスで構成されたので、ドメインに参加できます。

必要な情報:

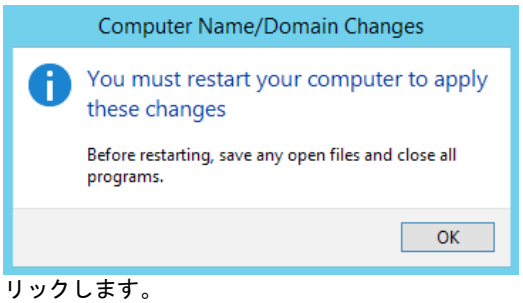
1. Windows OPCアカウントの資格証明。
2. ドメインへの参加権限を持つアカウントのドメイン資格証明。
3. 参加するドメインの完全修飾ドメイン名(FQDN)。

ドメインへの参加:

1. 1つ目のシステムにOPCユーザーとしてログインします。
2. **Windowsエクスプローラー**を実行します。
3. 「**PC**」を右クリックして、「**プロパティ**」を選択します。
4. 「*コンピューター名、ドメインおよびワークグループの設定*」セクションで、「**設定の変更**」をクリックします。
5. 「**変更**」をクリックします。



6. 「**ドメイン**」ラジオ・ボタンを選択します。
7. 参加するドメインのFQDN名を入力し、「**OK**」をクリックします。
8. DNSサーバーが正しく構成されている場合、ドメインの管理者資格証明を入力するためのダイアログ・ボックスが表示されます。資格証明を入力して、「**OK**」をクリックします。
9. 資格証明が正しく、かつ適切な権限がある場合、「*... ドメインへようこそ*」というメッセージが表示されます。
10. 「**OK**」をクリックして、ダイアログを閉じます。
11. サーバーを再起動する必要があることを通知するダイアログ・ボックスが表示されたら、「**OK**」をク



リックします。

12. 「**閉じる**」をクリックして、「*システムのプロパティ*」コントロール・パネルを閉じます。
13. 「**今すぐ再起動する**」をクリックしてサーバーを再起動します。

2つ目のドメイン・コントローラについて前述のステップを繰り返します。

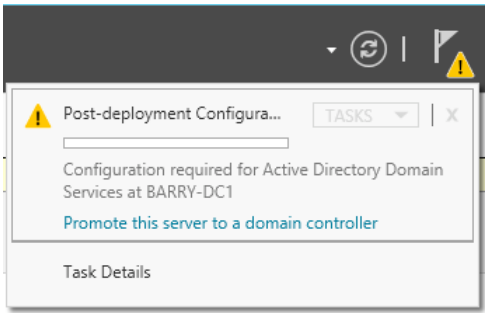
ドメイン・コントローラの昇格

必要な情報:

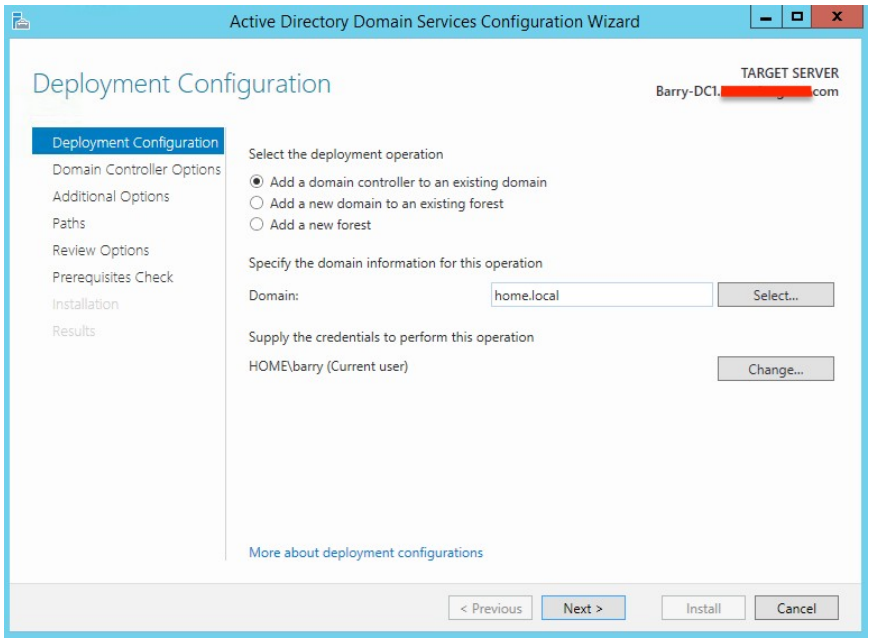
1. サーバーをドメイン・コントローラとして昇格するドメイン管理者権限を持つアカウントのドメイン資格証明。

サーバーの読取り専用ドメイン・コントローラへの昇格:

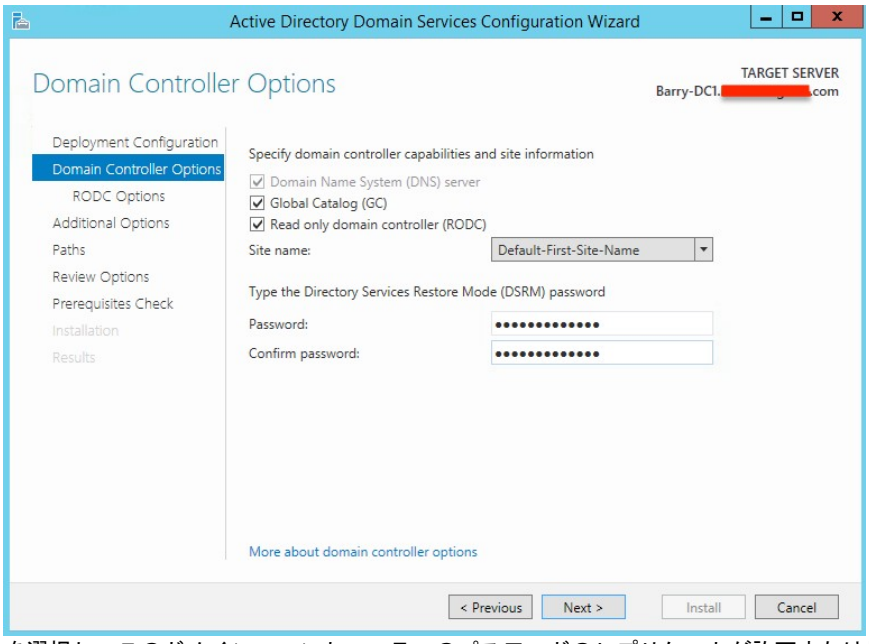
1. 1つ目のシステムにドメイン管理者(または同等の権限を持つアカウント)としてログインします。ユーザー名を".\opc"から"*your_domain\your_domain_admin*"に変更する必要があります。
2. **サーバー マネージャー**を実行します。
3. 黄色の警告通知アイコンが表示されます。クリックすると、Active Directoryサービスを構成する必要があることを示すメッセージが表示されます。「**このサーバーをドメイン コントローラーに昇格する**」をクリックします。



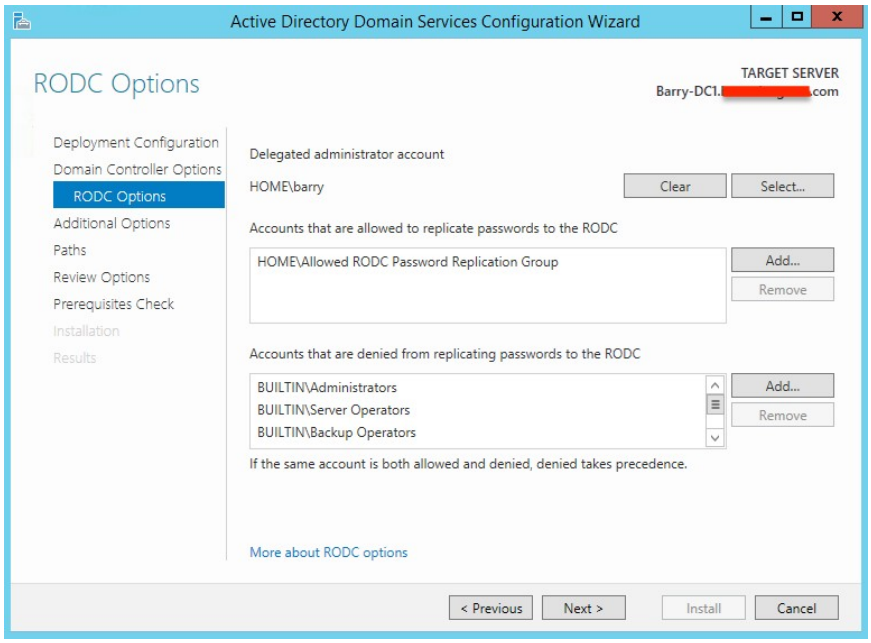
4. *Active Directory ドメイン サービス構成ウィザード*で、「**既存のドメインにドメイン コントローラーを追加する**」が選択されていること、正しいドメインが「*ドメイン*」フィールドにリストされていること、および表示されている資格証明が正しいことを確認し、「**次へ**」をクリックします。



5. このドメイン・コントローラが読取り専用ドメイン・コントローラになる場合は、必ず「**読み取り専用ドメイン コントローラー(RODC)**」チェックボックスを選択します。それ以外の場合は未選択のままにします。
6. **ディレクトリ サービス復元モード(DSRM)**のパスワードを入力し確認したら、「**次へ**」をクリックします。
7. 読取り専用ドメイン・コントローラのインストールを選択した場合、「**委任された管理者アカウント**」



を選択し、このドメイン・コントローラへのパスワードのレプリケートが許可または拒否されるアカウントをリストし、「**次へ**」をクリックします。



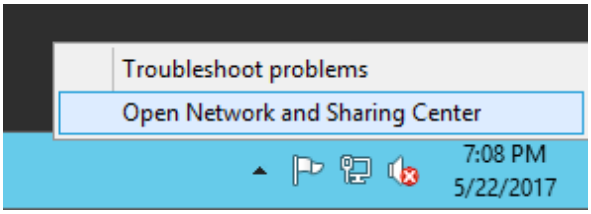
8. 「**前提条件のチェック**」ステップが表示されるまで、「**次へ**」をクリックします。この画面に警告がいくつか表示される場合は、警告を確認して、「**インストール**」をクリックします。
9. インストール・プロセスの最後にサーバーが再起動されます。

Active Directoryのテスト

Oracle Cloud Infrastructureテナンシに2つの読取り専用ドメイン・コントローラが構成されたため、これらのドメイン・コントローラを使用して、テナンシからドメインへの参加、およびドメイン資格証明を使用したサーバーへのログインの両方を行えるかどうかをテストできます。

新たに作成したドメイン・コントローラをDNSサーバーとして使用したテスト・インスタンスの構成

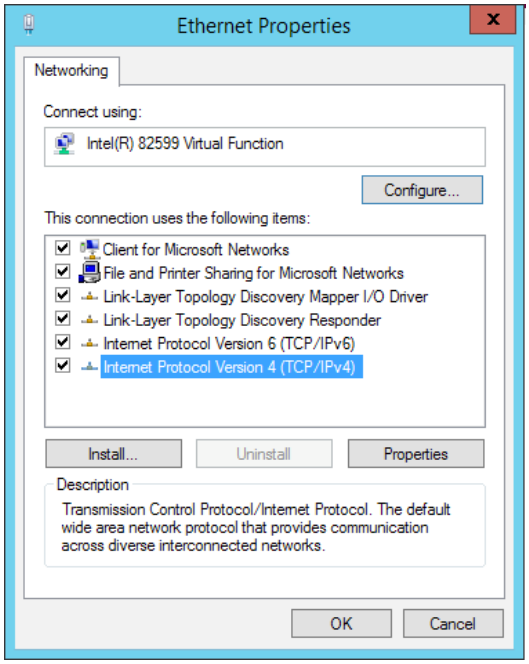
1. テスト・システムにOPCユーザーとしてログインします。
2. 画面の右隅のネットワーク・アイコンを右クリックして、「**ネットワークと共有センターを開く**」を選択します。



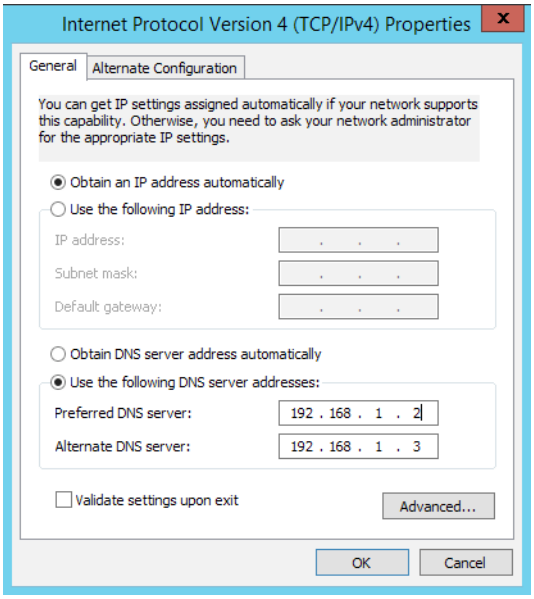
3. 左ペインで「**アダプターの設定の変更**」をクリックします。

   注意: ここで説明する「**ネットワーク接続**」ウィンドウに表示されるオプションは、仮想マシン・インスタンスとして起動されるインスタンス用です。Windowsサーバーをベア・メタル・インスタンスとして起動した場合、アダプタの名前は異なりますが、ステップはインスタンス・タイプにかかわらず同じです。

4. **イーサネット**・ネットワーク・アダプタを右クリックし(ラベルは"Intel(R) 82599 Virtual function"となっています)、「**プロパティ**」を選択します。(ベア・メタル・インスタンスの場合、ラベルは"Intel(R) Ethernet Server Adapter X520-2"またはそれに類似したものになります。)
5. 「**インターネット プロトコル バージョン4 (TCP/IPv4)**」を選択し、「**プロパティ**」をクリックします。



6. 「**次のDNSサーバーのアドレスを使う**」を選択します。
7. 新たに作成したドメイン・コントローラのIPアドレス(これは前に記録したRFC1918 IPアドレスです)を入力し、「**OK**」をクリックします。

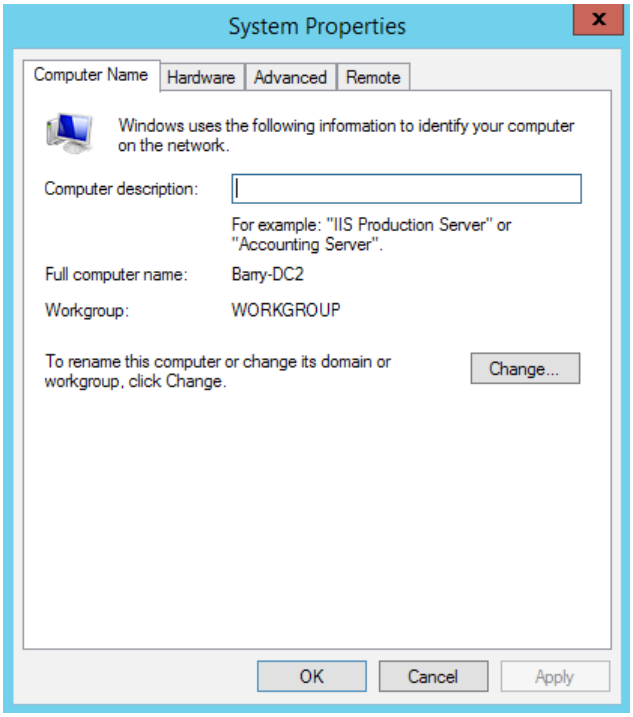


8. 「**閉じる**」をクリックします。

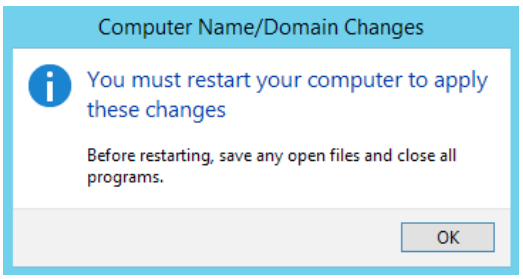
次に、テスト・サーバーをドメインに参加できます。

1. **Windowsエクスプローラー**を実行します。

2. 「**PC**」を右クリックして、「**プロパティ**」を選択します。
3. 「*コンピューター名、ドメインおよびワークグループの設定*」セクションで、「**設定の変更**」をクリックします。
4. 「**変更**」をクリックします。



5. 「**ドメイン**」ラジオ・ボタンを選択します。
6. 参加するドメインのFQDN名を入力し、「**OK**」をクリックします。
7. DNSサーバーが正しく構成されている場合、ドメインの管理者資格証明を入力するためのダイアログ・ボックスが表示されます。資格証明を入力して、「**OK**」をクリックします。
8. 資格証明が正しく、かつ適切な権限がある場合、「*... ドメインへようこそ*」というメッセージが表示されます。
9. 「**OK**」をクリックして、ダイアログを閉じます。
10. サーバーを再起動する必要があることを通知するダイアログ・ボックスが表示されます。「**OK**」をクリックします。



11. 「**閉じる**」をクリックして、「*システムのプロパティ*」コントロール・パネルを閉じます。
12. 「**今すぐ再起動する**」をクリックしてサーバーを再起動します。

サーバーが再起動されたら、リモート・デスクトップを使用してサーバーに接続することで、これがドメインに含まれていることをテストでき、ローカルOPCアカウントではなくドメイン・アカウントを使用してログインできます。

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US

blogs.oracle.com/oracle

facebook.com/oracle

twitter.com/oracle

oracle.com

Integrated Cloud Applications & Platform Services

Microsoft Windows: Active DirectoryをOracle Cloud Infrastructureに拡張
2017年6月
著者: Barry Shilmover (barry.shilmover@oracle.com)

Oracle is committed to developing practices and products that help protect the environment