# Microsoft Windows: Extending Active Directory to Oracle Cloud Infrastructure

## Quick Start White Paper

ORACLE WHITE PAPER | JUNE 2017 | VERSION 1.1

## Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

## Table of Contents

## Assumptions

Consumers of this document should:

- Be familiar with the fundamentals of the Oracle Cloud Infrastructure:
  - https://docs.us-phoenix-1.oraclecloud.com/

  The Oracle Cloud Infrastructure walkthrough is highly recommended if this is the first time you have used the platform:

  - https://docs.us-phoenix-1.oraclecloud.com/Content/GSG/Reference/overviewworkflow.htm
- Have an existing Virtual Cloud Network (VCN) already created and configured:
  - https://docs.us-phoenix-1.oraclecloud.com/Content/Network/Tasks/managingVCNs.htm
- Have a VPN or FastConnect connection fully configured between the on-premises environment and your VCN:
  - 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
- Have a basic understanding of Active Directory:
  - Active Directory key concepts

## Target Audience

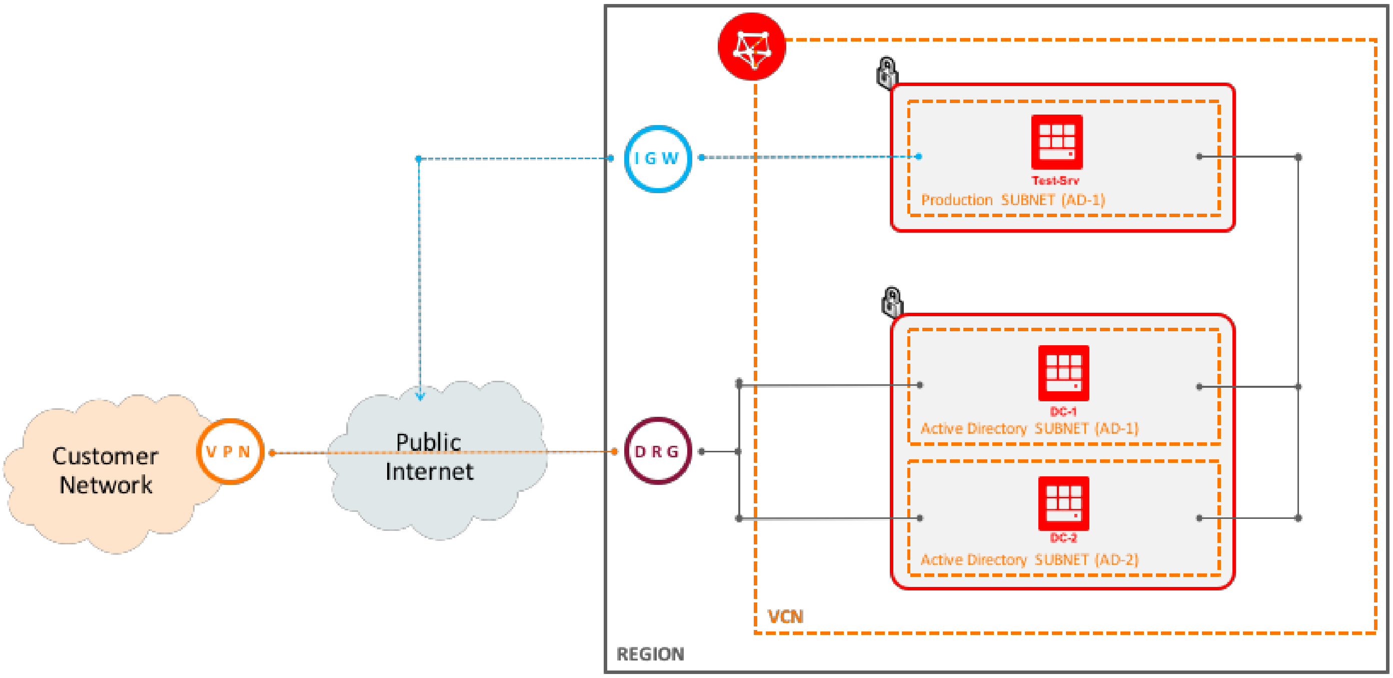
This whitepaper is targeted at customers who would like to understand how to extend their on-premises Active Directory environment to Oracle Cloud Infrastructure.

## Introduction

This whitepaper walks you through the process of extending your Windows Active Directory infrastructure in Oracle Cloud Infrastructure. Two read-only domain controllers will be installed, each in different Availability Domains (ADs) (for redundancy). A third system will be used as a test server to ensure that you can both join to and log in to the domain controllers running in Oracle Cloud Infrastructure.

In order for you to accomplish this, several assumptions are made:

- A secure (nonpublic) connection exists between your on-premises environment and Oracle Cloud Infrastructure (this can either be a FastConnnect or IPSec VPN connection, as shown in the diagram below).
- You have a domain admin account in the on-premises Active Directory environment (or an account that has permission to both join the domain and install a domain controller).



***Best Practice***

*The domain controllers should not be accessible externally from the internet. Allowed access should only be from specific IP addresses from the on-premises network. These IP addresses should include the current on-premises Active Directory controllers and any Administrative desktops that will be used to create/manage the domain controllers*

## Setting up the network environment

This whitepaper assumes that a VCN has already been configured and there is sufficient IP address space to create at least 2 new subnets. These subnets (as illustrated in the diagram above) will be used to host the 2 read-only domain controllers created in the steps below. Because subnets are associated with Availability Domains (ADs), this ensures that each of the domain controllers reside in different ADs, thereby removing a single point of failure in the Active Directory environment.  In the examples that follow, an IP space of 10.x.x.x is assumed.

Each of the subnets will require a route table and at least one security list. The route table for the domain controller subnets should already exist since your VCN is already connected to your on-premises environment using this route table. If you don’t already have a route table that can be used for the test server (assuming it requires internet access), you can create one as outlined below.

### Creating the Security Lists

You need at least two security lists: one for the Active Directory domain controllers and one for the test server. This section will only create the security lists themselves and not the security list rules (those are outlined later in this whitepaper).

Create two security lists:

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

***Best Practice***

*Always be as prescriptive in your naming of Oracle Cloud Infrastructure components as you can. This will make it easier in the future when you have to revisit an environment.*

### Create the Route Table

Next, create a route table that can be used for the test. This route table will be used to allow the test server to route to the Internet. The route table used for the domain controllers should route traffic to your on-premises network.

Create the following route table:

- Production - Application (Private)

### Create Security List Rules

Active Directory uses a number of protocols to communicate, including RPC, NetBIOS, SMB, LDAP, Kerberos, WINS and DNS. While your configuration may only use some of these, all are listed here. For example, if WINS is not used in your environment, you can remove those from the list.

As stated in the best practice section, all the domain controllers should be in a subnet that either has no external IP addresses or has no access from the Internet. Due to this, you may want to just enable all ports to communicate between your subnets and the Active Directory subnets. If you choose to do this, however, be aware that this still opens potential paths of attack from those subnets. Therefore, it is a best practice to only open the ports listed below between the subnets:

| Name | Protocol | Port |
|---|---|---|
| DNS | TCP, UDP | 53 |
| LDAP | TCP, UDP | 389 |
| LDAP over SSL | TCP | 636 |
| Global catalog LDAP | TCP | 3268 |
| Global catalog LDAP over SSL | TCP | 3269 |
| Kerberos | TCP, UDP | 88 |
| RPC endpoint mapper | TCP, UDP | 135 |
| NetBIOS name service | TCP, UDP | 137 |
| NetBIOS datagram service | UDP | 138 |
| NetBIOS session service | TCP | 139 |
| SMB over IP (Microsoft-DS) | TCP, UDP | 445 |
| WINS resolution | TCP, UDP | 1512 |
| WINS replication | TCP, UDP | 42 |

Create new ingress rules on the **Production Active Directory** security list to allow the required port communication into the new Active Directory subnets (make sure these rules exist to allow traffic between the two domain controller subnets). Also make sure that you enable TCP port 3389 (RDP) from the internal on-premises network to all three subnets.

### Creating the Subnets

As mentioned previously, you will need at least 2 subnets (a third subnet in the third Availability Domain can be used for extra availability of the Active Directory environment). The subnets for this whitepaper are:

| Name | Availability Domain | CIDR Block | Route Table | Security Lists |
|---|---|---|---|---|
| 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) |

## Instances

Our environment requires three instances. Two will be used for the Active Directory domain controllers and the third will be used as a test server.

Use the following properties to create the instances (the instance shape we used for this white paper (VM.Standard1.4) is a recommendation, you can scale it up or down as you deem fit):

| Name | Image | Shape | Availability Domain | Subnet |
|---|---|---|---|---|
| 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 | (Dependent on your network configuration) | (Dependant on your network configuration) |

For each instance, record the RFC1918 IP addresses:

| Instance | RFC1918 IP |
|---|---|
| **DC-1** | |
| **DC-2** | |
| **Test-SRV** | |

## Configuring the Domain Controllers

You are now ready to install the appropriate roles and features on the servers and promote them to Read Only Domain Controllers. To do that, you will need to complete the following steps:

1. Install Active Directory Domain Services and DNS Server roles.
2. Configure the DNS server.
3. Join the domain.
4. Promote the server to a read-only domain controller.

### Installing the server roles

For this server to be promoted to a domain controller, you need to install the **Active Directory Domain Services** role. You can also install the **DNS Server** role if you want to replicate some of the DNS entries from your on-premises DNS servers. This role is optional, but is covered in the instructions below.

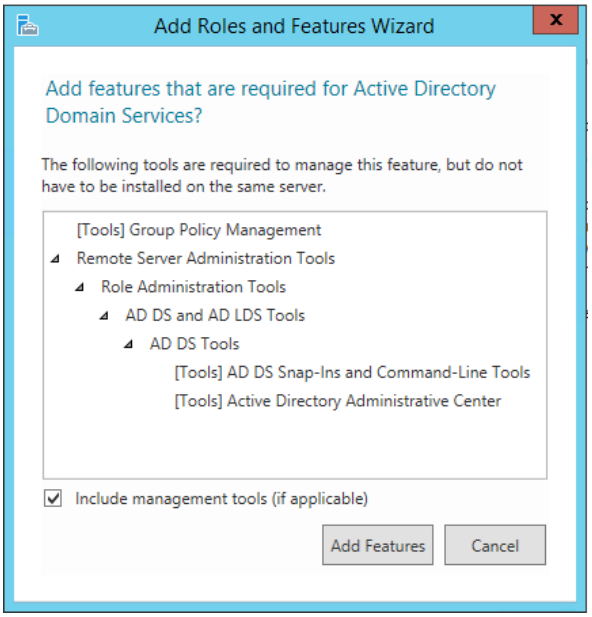
Information needed:

1. Credentials for Windows OPC account.

Install the **Active Directory Domain Services** Role:

1. Log in to the first instance that is to be promoted to a domain controller, using the OPC user credentials (administrator user).
2. Run **Server Manager.**
3. Click **Add Roles and Features.**
4. Click **Next** until you get to the **Server Role** dialog.
5. Select the **Active Directory Domain Services** checkbox.

6. In the dialog box that appears, click the **Add Features** button.



Add features that are required for Active Directory Domain Services?

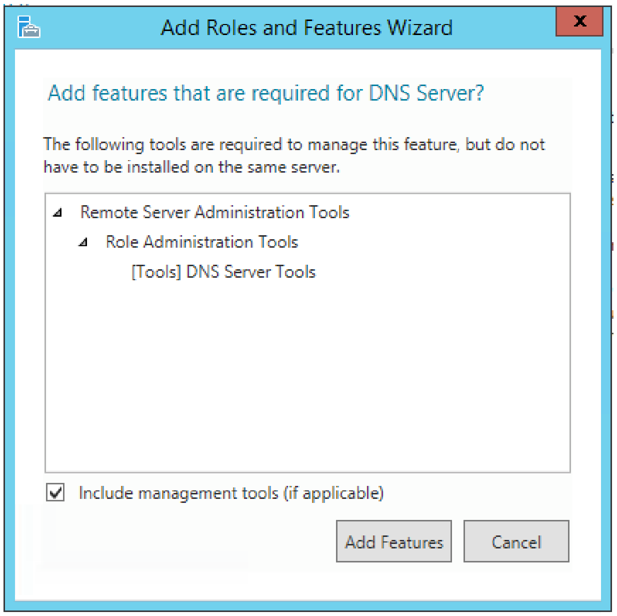
The following tools are required to manage this feature, but do not have to be installed on the same server.

[Tools] Group Policy Management
- Remote Server Administration Tools
  - Role Administration Tools
    - AD DS and AD LDS Tools
      - AD DS Tools
        - [Tools] AD DS Snap-Ins and Command-Line Tools
        - [Tools] Active Directory Administrative Center

☑ Include management tools (if applicable)

7. (Optional) Select the **DNS Server** checkbox.

8. In the dialog box that appears, click the **Add Features** button.



Add features that are required for DNS Server?

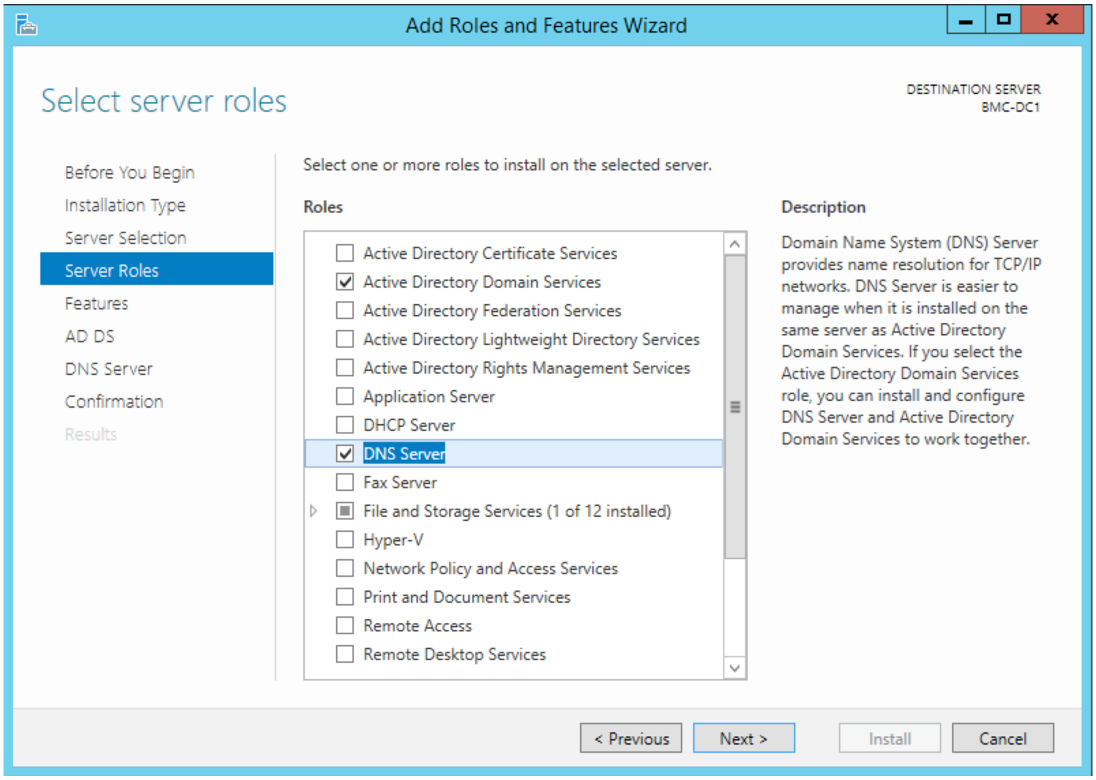
The following tools are required to manage this feature, but do not have to be installed on the same server.

- Remote Server Administration Tools
  - Role Administration Tools
    - [Tools] DNS Server Tools

☑ Include management tools (if applicable)

**Note:** If you selected to install the DNS Server role, you will get a warning dialog box informing you that no static IP addresses were found on the computer. Because the IP address associated with this instance will be associated with it for the life of the instance, you can click the **Continue** button.

9. Once these 2 options have been selected, click **Next** to continue:



Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
BMC-DC1

Select one or more roles to install on the selected server.

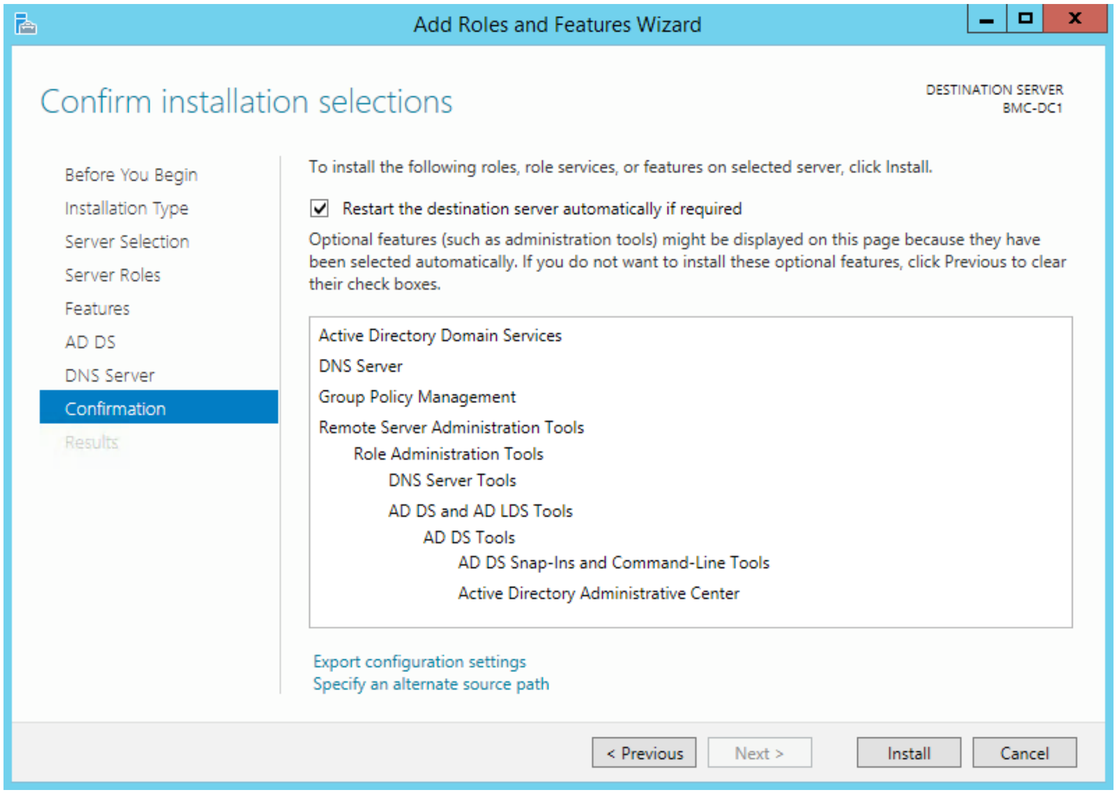
**Roles**

- ☐ Active Directory Certificate Services
- ☑ Active Directory Domain Services
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Application Server
- ☐ DHCP Server
- ☑ DNS Server
- ☐ Fax Server
- ▣ File and Storage Services (1 of 12 installed)
- ☐ Hyper-V
- ☐ Network Policy and Access Services
- ☐ Print and Document Services
- ☐ Remote Access
- ☐ Remote Desktop Services

**Description**

Domain Name System (DNS) Server provides name resolution for TCP/IP networks. DNS Server is easier to manage when it is installed on the same server as Active Directory Domain Services. If you select the Active Directory Domain Services role, you can install and configure DNS Server and Active Directory Domain Services to work together.

10. Click **Next** until you get to the Confirmation dialog. Check **Restart the destination server automatically if required** (accept the pop up dialog box) and click **Install**:



Add Roles and Features Wizard

Confirm installation selections

DESTINATION SERVER
BMC-DC1

To install the following roles, role services, or features on selected server, click Install.

☑ Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

Active Directory Domain Services
DNS Server
Group Policy Management
Remote Server Administration Tools
- Role Administration Tools
  - DNS Server Tools
  - AD DS and AD LDS Tools
    - AD DS Tools
      - AD DS Snap-Ins and Command-Line Tools
      - Active Directory Administrative Center

Export configuration settings
Specify an alternate source path
< Previous
Next >
Install
Cancel

11. The installation of the new roles will begin. Once the installation is complete, you can click **Close** to complete the **Add roles and features** wizard.

Repeat the steps above for the second domain controller.

## Configure DNS

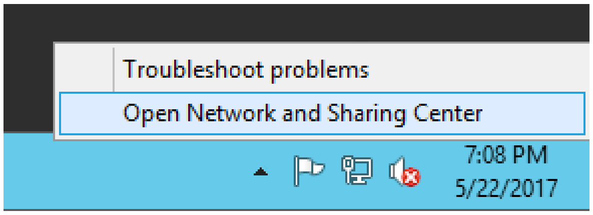
Before you can join the domain and promote the domain controller, you need to reconfigure the DNS server to point to the on-premises Active Directory DNS server. (Another option is to create a DNS server in the Oracle Cloud Infrastructure environment that can receive a Zone transfer from the on-premises DNS servers. This will allow you to use the Oracle Cloud Infrastructure DNS server to join the domain.) Having the DNS server on the soon-to-be domain controller map to the on-premises DNS server will allow the server to resolve the domain information and join the domain.

Information needed:

1. Credentials for Windows OPC account.
2. IP address(es) of the on-premises DNS server(s).

Configure the on-premises DNS server:

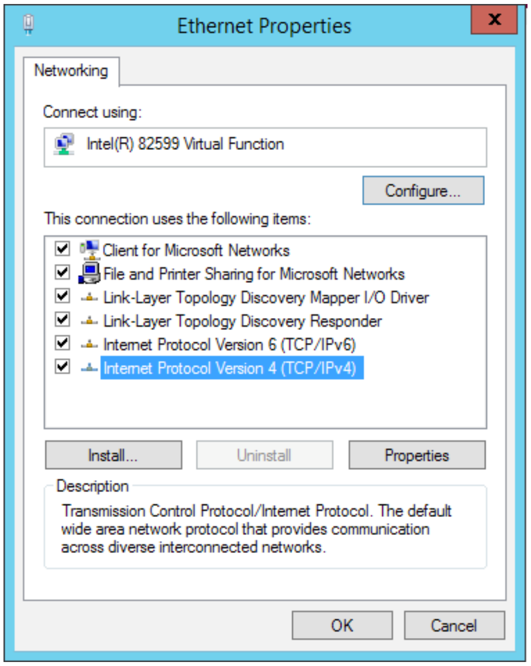
1. Log in to the first system as the OPC user.
2. Right-click the Network icon in the right corner of the screen and choose **Open Network and Sharing Center**.



3. Click **Change adapter settings** in the left pane.

   **Note:** The options appearing in the **Network Connections** window discussed here are for instances launched as Virtual Machine instances. If you launched the Windows servers as Bare Metal instances, the name of the adapter will be different, however, the steps are the same regardless of instance type.

4. Right-click the **Ethernet** network adapter (it should be labeled "Intel(R) 82599 Virtual function") and choose **Properties**. (For Bare Metal instances, it should be labeled "Intel(R) Ethernet Server Adapter X520-2" or similar.)
5. Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties.**



Connect using:

Intel(R) 82599 Virtual Function

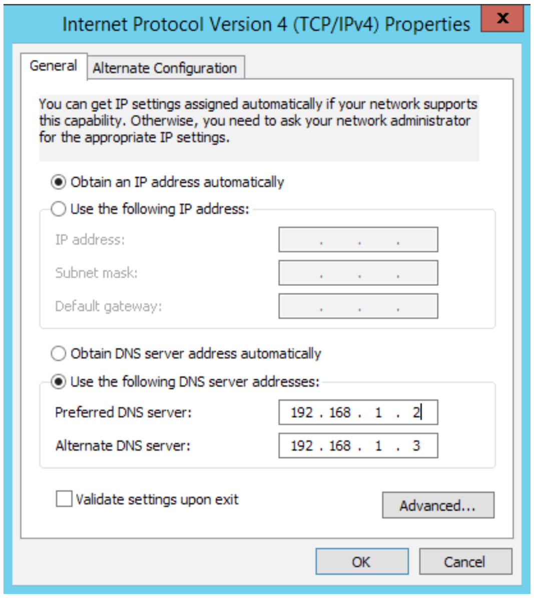
This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ Link-Layer Topology Discovery Mapper I/O Driver
☑ Link-Layer Topology Discovery Responder
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

6. Choose **Use the following DNS server addresses**.
7. Enter the IP address(s) of the on-premises DNS server(s) and click **OK**.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 1 . 2

Alternate DNS server: 192 . 168 . 1 . 3

□ Validate settings upon exit

8. Click **Close**.
9. You can test that the DNS server is working by either navigating to a public website (assuming that your instance(s) have Internet access) or by running the **nslookup** command from a command prompt.

Repeat the steps above for the second domain controller.

## Join the domain

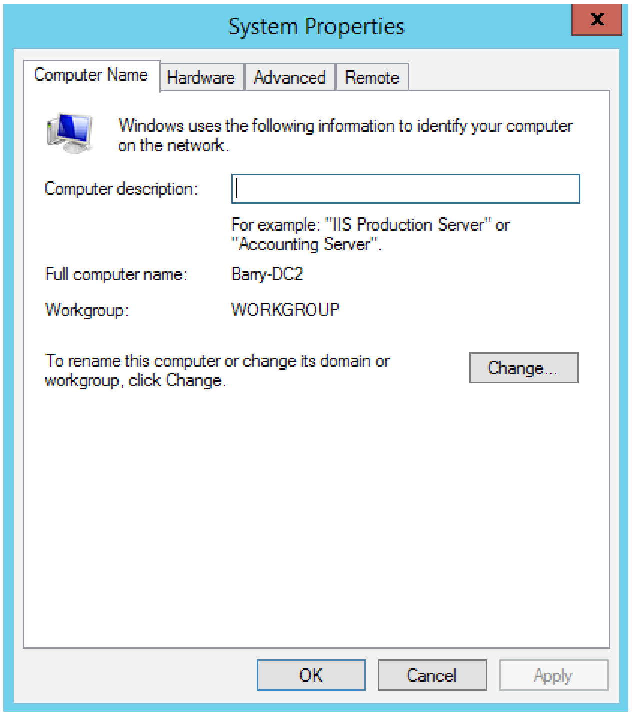
Now that the DNS server is configured on your instance, you can join the domain.

Information needed:

1. Credentials for Windows OPC account.
2. Domain credentials for an account that has permission to join the domain.
3. The Fully Qualified Domain Name (FQDN) of the domain to be joined.

Join the domain:

1. Log in to the first system as the OPC user.
2. Run **Windows Explorer.**
3. Right-click **This PC** and choose **Properties**.
4. In the *Computer name, domain, and workgroup settings* section, click **Change settings**.
5. Click **Change**.



Windows uses the following information to identify your computer on the network.

Computer description:

For example: "IIS Production Server" or "Accounting Server".

Full computer name: Barry-DC2

Workgroup: WORKGROUP

To rename this computer or change its domain or workgroup, click Change.

6. Select the **Domain** radio button.

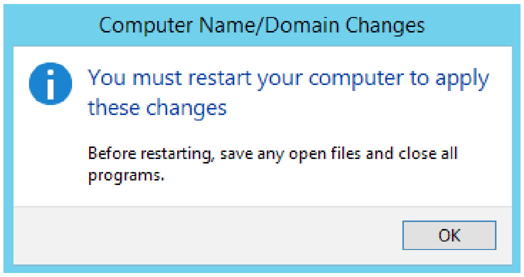
7. Enter the FQDN name of the domain that you are joining and click **OK**.

8. If the DNS server is configured correctly, you should be prompted with a dialog box to enter the domain administrator credentials. Enter the credentials and click **OK**.

9. If the credentials are correct and have the appropriate permissions, you should receive a *Welcome to the … domain* message.

10. Click **OK** to close the dialog.

11. Another dialog box notifying you that you need to reboot the server will be displayed, click **OK.**



You must restart your computer to apply these changes

Before restarting, save any open files and close all programs.

12. Click **Close** to close the *System Properties* control panel.

13. Click **Restart Now** to restart the server

Repeat the steps above for the second domain controller.

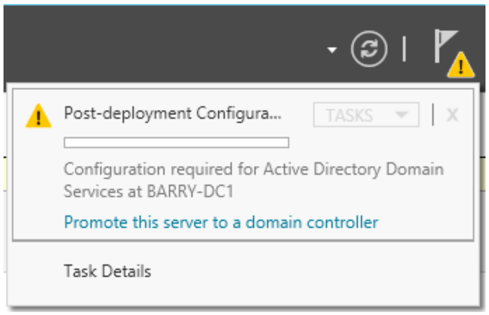
## Promote the domain controller

Information needed:

1. Domain credentials for an account that has domain administrator permission to promote a server as a domain controller.

Promote the server to a read-only domain controller:

1. Log in to the first system as a domain administrator (or account that has equivalent permissions). You will need to change the username from “.\opc” to “*your_domain\your_domain_admin”*
2. Run **Server Manager.**
3. You should notice a yellow warning notification icon. Click it and you should see a message stating that configuration is required for Active Directory Services. Click **Promote this server to a domain controller**.



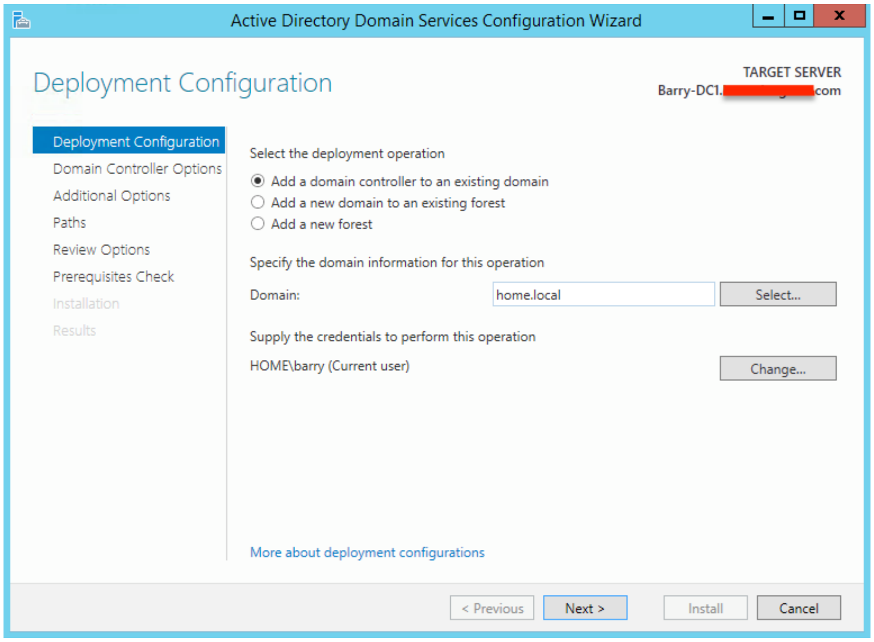
Post-deployment Configura...

Configuration required for Active Directory Domain Services at BARRY-DC1

Promote this server to a domain controller

Task Details

4. In the *Active Directory Domain Services Configuration Wizard*, make sure that **Add a domain controller to an existing domain** is selected, the correct domain is listed in the *Domain* field, and the credentials displayed are correct, and click **Next**.



Active Directory Domain Services Configuration Wizard

Deployment Configuration

TARGET SERVER
Barry-DC1.[redacted].com

Select the deployment operation

● Add a domain controller to an existing domain
○ Add a new domain to an existing forest
○ Add a new forest

Specify the domain information for this operation

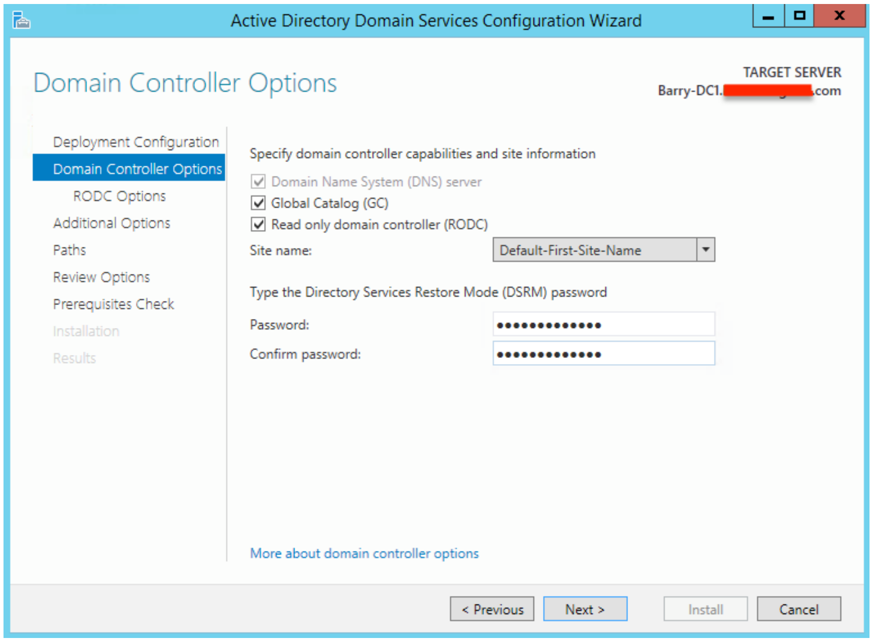
Domain: home.local

Supply the credentials to perform this operation

HOME\barry (Current user)

5. If this domain controller is to become a read-only domain controller, make sure you check the **Read only domain controller (RODC)** checkbox, otherwise, leave the checkbox unchecked.

6. Enter and confirm a password for **Directory Services Restore Mode (DSRM)** and click **Next**.



Active Directory Domain Services Configuration Wizard

Domain Controller Options

TARGET SERVER
Barry-DC1.[redacted].com

Specify domain controller capabilities and site information

☑ Domain Name System (DNS) server
☑ Global Catalog (GC)
☑ Read only domain controller (RODC)

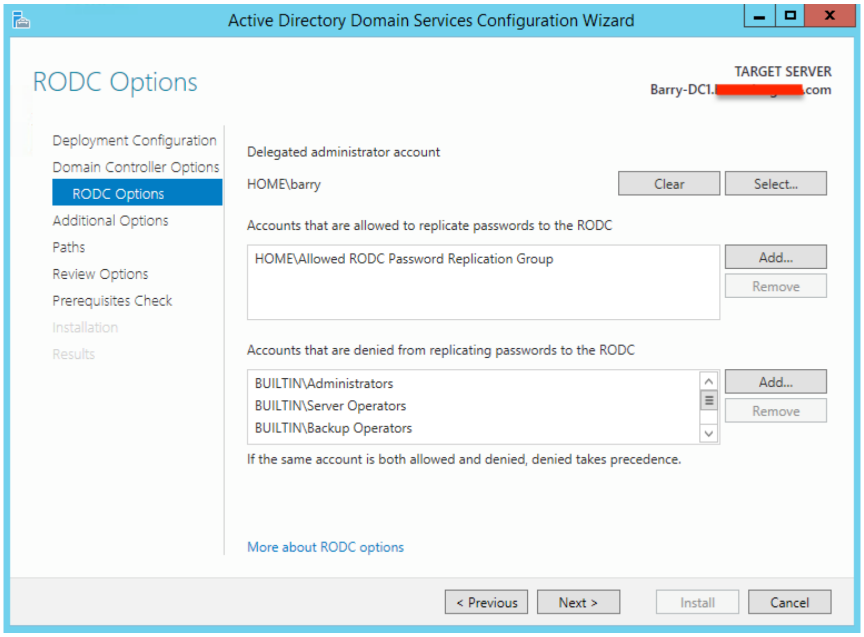
Site name: Default-First-Site-Name

Type the Directory Services Restore Mode (DSRM) password

Password: ●●●●●●●●●●●●●
Confirm password: ●●●●●●●●●●●●●

More about domain controller options

7. If you chose to install a read-only domain controller, select **Delegated administrator account** and list the account(s) that are allowed or denied from replicating passwords to this domain controller and click **Next.**



Active Directory Domain Services Configuration Wizard

RODC Options

TARGET SERVER
Barry-DC1.[redacted].com

Delegated administrator account

HOME\barry

Accounts that are allowed to replicate passwords to the RODC

HOME\Allowed RODC Password Replication Group

Accounts that are denied from replicating passwords to the RODC

BUILTIN\Administrators
BUILTIN\Server Operators
BUILTIN\Backup Operators

If the same account is both allowed and denied, denied takes precedence.

More about RODC options

8. Click **Next** until you get to the **Prerequisites Check** step. You may be presented with some warnings on this screen, review the warnings and click **Install**.

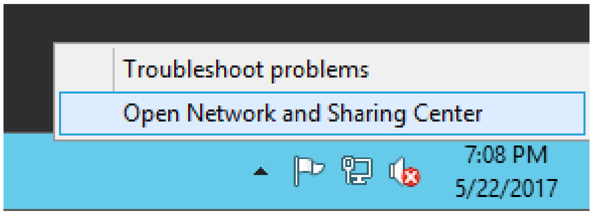
9. The server will reboot at the end of the installation process.

## Testing Active Directory

Your Oracle Cloud Infrastructure tenancy should now have two read-only domain controllers and you can now test if these domain controllers can be used to both join the domain from the tenancy, and log in to your servers using the domain credentials.

Configure the test instance to use the newly created domain controllers as the DNS server:

1. Log in to the test system as the OPC user.
2. Right-click the Network icon in the right corner of the screen and choose **Open Network and Sharing Center**.



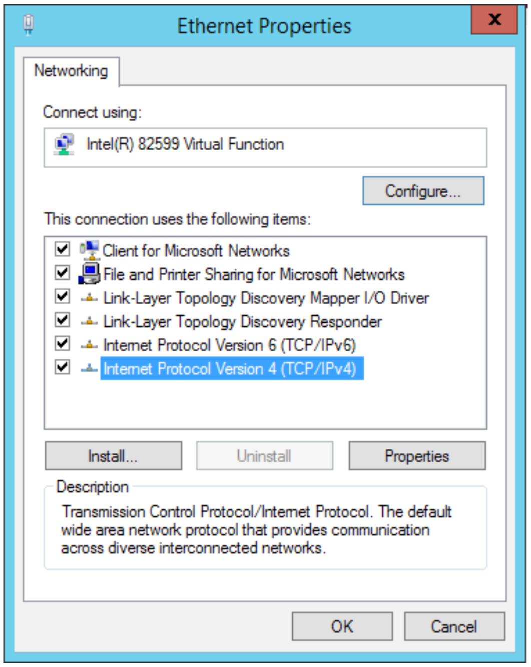
Troubleshoot problems

Open Network and Sharing Center

3. Click **Change adapter settings** in the left pane

   **Note:** The options appearing in the **Network Connections** window discussed here are for instances launched as Virtual Machine instances. If you launched the Windows servers as Bare Metal instances, the name of the adapter will be different, however, the steps are the same regardless of instance type.

4. Right-click the **Ethernet** network adapter (it should be labeled “Intel(R) 82599 Virtual function”) and choose **Properties**. (For Bare Metal instances, it should be labeled “Intel(R) Ethernet Server Adapter X520-2”, or similar.)
5. Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties.**



Connect using:

Intel(R) 82599 Virtual Function

This connection uses the following items:

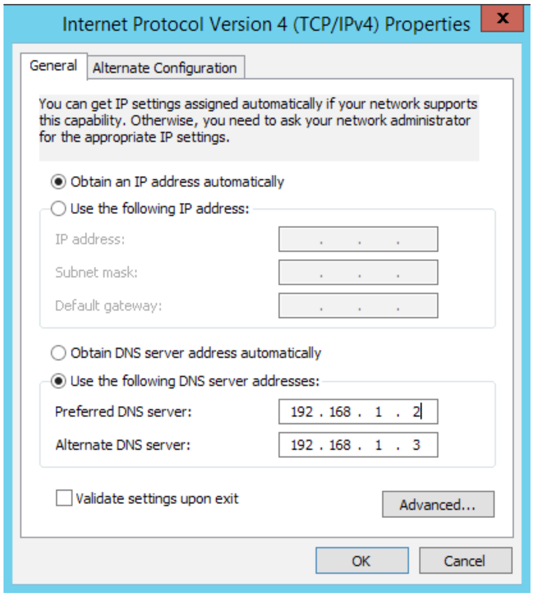
- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

6. Choose **Use the following DNS server addresses**.

7. Enter the IP address(s) of the newly created domain controllers (these are the RFC1918 IP addresses you recorded earlier and click **OK**.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 1 . 2

Alternate DNS server: 192 . 168 . 1 . 3

□ Validate settings upon exit

8. Click **Close**.

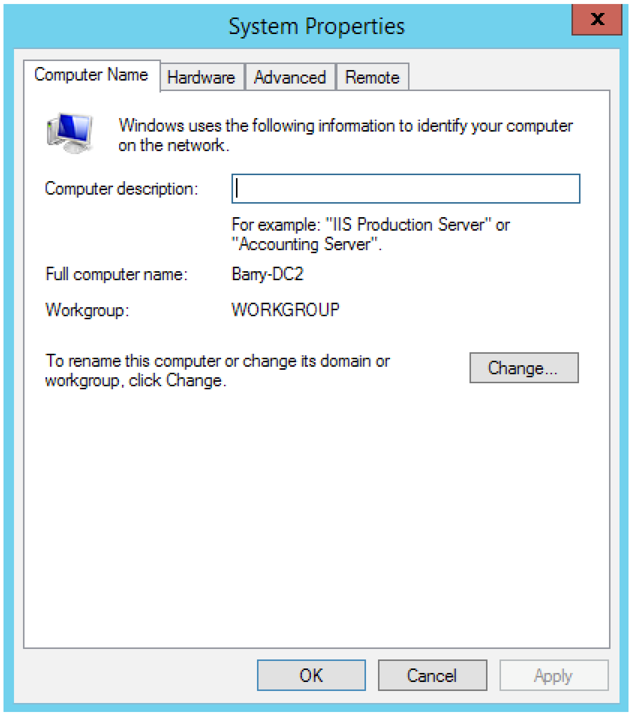
Next, you can join the test server to the domain:

1. Run **Windows Explorer.**

2. Right-click **This PC** and choose **Properties.**

3. In the *Computer name, domain, and workgroup settings* section, click **Change settings**.

4. Click **Change**.



Windows uses the following information to identify your computer on the network.

Computer description:

For example: "IIS Production Server" or "Accounting Server".

Full computer name: Barry-DC2

Workgroup: WORKGROUP

To rename this computer or change its domain or workgroup, click Change.

5. Select the **Domain** radio button.

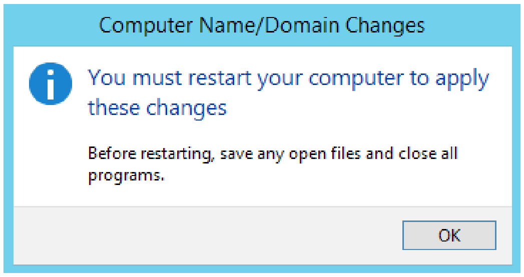
6. Enter the FQDN name of the domain that you are joining and click **OK**.

7. If the DNS server is configured correctly, you should be prompted with a dialog box to enter the domain administrator credentials. Enter the credentials and click **OK**.

8. If the credentials are correct and have the appropriate permissions, you should receive a *Welcome to the … domain* message.

9. Click **OK** to close the dialog.

10. Another dialog box notifying you that you need to reboot the server will be displayed. Click **OK**.



You must restart your computer to apply these changes

Before restarting, save any open files and close all programs.

11. Click **Close** to close the *System Properties* control panel.

12. Click **Restart Now** to restart the server.

Once the server has restarted, you can test that it is now part of the domain by using remote desktop to connect to the server and log in using your domain account rather than the local OPC account.

**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: Extending Active Directory to Oracle Cloud Infrastructure
June 2017
Author: Barry Shilmover (barry.shilmover@oracle.com)