Honeywell

EXPERION PKS

RELEASE 516

Windows Domain Implementation Guide for Windows Server 2008 R2

EPDOC-X251-en-516A

August 2020

Disclaimer

This document contains Honeywell proprietary information. Information contained herein is to be used solely for the purpose submitted, and no part of this document or its contents shall be reproduced, published, or disclosed to a third party without the express permission of Honeywell International Sàrl.

While this information is presented in good faith and believed to be accurate, Honeywell disclaims the implied warranties of merchantability and fitness for a purpose and makes no express warranties except as may be stated in its written agreement with and for its customer.

In no event is Honeywell liable to anyone for any direct, special, or consequential damages. The information and specifications in this document are subject to change without notice.

Copyright 2020 - Honeywell International Sàrl

Contents ... 3
Chapter 1 - About this document ... 6
1.1 Intended audience ... 6
1.2 Prerequisite skills ... 6
1.3 Revision history ... 6
1.4 Related documents ... 6
Chapter 2 - Getting started ... 8
2.1 Hardware and software requirements ... 8
2.1.1 Software requirements for a domain controller ... 8
2.1.2 System requirements for a domain controller ... 8
2.2 General guidelines for implementing a domain controller ... 9
Chapter 3 - Installing a Windows domain controller ... 12
3.1 Recording the domain configuration information ... 12
3.1.1 Domain configuration worksheet ... 12
3.2 Preparing a Windows domain controller ... 14
3.2.1 Installing Microsoft Windows Server 2008 R2 Operating System ... 14
3.2.2 Installing Microsoft service packs and Windows updates ... 14
3.2.3 Configuring TCP/IP settings ... 15
3.2.4 Changing the computer name ... 16
3.3 Setting up or installing a domain controller ... 17
3.3.1 Installing the Microsoft Windows Server 2008 R2 server as a domain controller ... 17
3.4 Setting up a peer domain controller ... 20
3.4.1 Adding Microsoft Windows Server 2008 R2 server to the role of a peer domain controller ... 20
3.5 Setting up a Read-only Domain Controller ... 22
3.5.1 Creating user account for staged Read-Only Domain Controller installation ... 23
3.5.2 Adding Microsoft Windows Server 2008 R2 server to the role of a Read-Only Domain Controller ... 24
3.6 Common tasks for setting up a domain controller ... 25
3.6.1 Adding Microsoft Windows Server 2008 R2 to a Windows domain ... 25
3.6.2 Verifying if DNS server role is active ... 26
3.6.3 Verifying if Global Catalog server role is active ... 27
3.6.4 Adding reverse lookup zone ... 28
Chapter 4 - Post installation tasks ... 30
4.1 Configuring Active Directory sites ... 30

4.1.1 Creating a site in Active Directory 30
4.1.2 Moving domain controllers to sites 31
4.1.3 Verifying the availability of Global Catalog server in a site 31
4.1.4 Adjusting replication interval for a site 32
4.2 Creating Active Directory users and groups 33
4.2.1 Creating Honeywell Active Directory users 33
4.2.2 Creating Active Directory groups 33
4.2.3 Changing group membership 34
4.3 Configuring time synchronization in a domain 34
4.3.1 Prerequisites 34
4.4 Adding workstation/server to Windows domain 35
4.4.1 Setting the DNS server IP address 35
4.4.2 Adding a node to a Windows domain 35
4.4.3 Viewing the workstation/server added to a domain 37
4.5 Configuring time synchronization on the workstations/servers added to a Windows domain 37
4.5.1 Prerequisites 37
4.5.2 Tasks to be performed for configuring time synchronization on the workstations/servers added to the Windows domain 38
Chapter 5 - Preparing the domain for migration 39
5.1 Recording the current domain controller configuration information 39
5.1.1 Migration planning worksheet 39
5.2 Inventorying the current domain controller configuration 40
5.2.1 Installing Windows Support Tools on domain controller 41
5.2.2 Identifying the domain controllers holding the FSMO roles 41
5.2.3 Identifying GC servers configured in the domain 41
5.2.4 Identifying DNS servers configured in the domain 42
5.2.5 Identifying the domain operation mode 45
5.3 Verifying domain controller readiness for migration 46
5.3.1 Verifying domain health 46
5.3.2 Ensuring availability of multiple domain controllers 47
5.3.3 Ensuring availability of multiple DNS servers 48
5.4 Preparing the Active Directory 48
5.4.1 Verifying if Service Pack 4 is installed on a Microsoft Windows 2000 Server domain controller 49
5.4.2 Raising the functional level of the domain 50
5.4.3 Expanding the Active Directory schema 51

Chapter 6 - Windows 2000 Server/Windows Server 2003/2008 to migration 53

6.1 Migrating a domain containing multiple domain controllers checklist 53

6.1.1 Prerequisites 53

6.1.2 Migrating a domain containing multiple domain controllers checklist 55

6.2 Configuring the peer domain controller as DNS server 56

6.2.1 Add DNS server role in the peer domain controller 57

6.3 Verifying the domain controller name is listed in the DNS list. 59

6.3.1 Prerequisites 59

6.3.2 To verify the active domain controller in a domain 59

6.3.3 Next steps 59

6.4 Configuring alternate DNS for all the nodes in the domain 59

6.4.1 To configure alternate DNS for all the nodes in the domain 60

6.4.2 Next steps 60

6.5 Transferring FSMO roles to a peer domain controller 60

6.5.1 Transferring/Restoring the schema master role 61

6.5.2 Transferring/Restoring domain naming master role 62

6.5.3 Transferring/Restoring RID Master, PDC Emulator, and Infrastructure Master roles 62

6.5.4 Verifying the transferred FSMO roles 63

6.6 Demoting a domain controller 63

6.6.1 Prerequisites 64

6.6.2 To demote a domain controller on Windows Server 2003, Windows Server 2008 and Windows Server 2008 R2 64

6.6.3 Next steps 65

6.7 Restoring the FSMO roles 65

6.7.1 Verifying the restored FSMO roles 65

6.8 Raising the functional level of the domain 65

6.8.1 Prerequisites 65

6.8.2 To raise the functional level of the domain 65

CHAPTER

1

ABOUT THIS DOCUMENT

This guide describes how to perform the following:

- Implementing Microsoft Windows domain controllers for Experion
- Implementing stand-alone Microsoft Windows domain controllers
- Migrating existing domain controllers to the latest supported Windows operating system for domain controllers
- Demoting domain controllers

1.1 Intended audience

- Customers who want to integrate their process domains into their corporate hierarchy and IT staffs who support them
- Customers with limited networking and IT experience who are using stand-alone domains
- Projects group and Services group

1.2 Prerequisite skills

It is assumed that you are familiar with the operation of Experion system software and the plant processes which Experion controls, Microsoft Windows operating systems, Windows domains and domain controllers, and network administration tasks.

1.3 Revision history

Revision	Publication date	Description
A	August 2020	Initial release of the document.

1.4 Related documents

- *Windows Domain and Workgroup Implementation Guide*
- For planning information, refer to *Windows Domain and Workgroup Planning Guide*
- For operation system migration information, refer the appropriate operating system-specific implementation guide *Windows Domain Implementation Guide for Windows Server 2008 R2*

- *Getting Started with Experion Software Guide*
- *Software Installation User's Guide*
- *Experion migration documentation*
- *Supplementary Installation Tasks Guide*
- *Server and Client Planning Guide*
- *Server and Client Configuration Guide*

CHAPTER

2 GETTING STARTED

- Hardware and software requirements
- General guidelines for implementing a domain controller

2.1 Hardware and software requirements

- Software requirements for a domain controller
- System requirements for a domain controller

2.1.1 Software requirements for a domain controller

To implement a domain controller in Experion R432.1, you need the following media/software.

- Microsoft Windows Server 2008 R2

2.1.2 System requirements for a domain controller

Component	Microsoft Windows Server (2008 through 2016)
Computer and processor	• Minimum - 1.4 GHz (x64) • Recommended - 2GHz or faster
Memory	• Minimum - 512 MB • Recommended - 2GB or greater • Maximum - 32GB
Hard disk	• Minimum - 10GB • Recommended - 40GB or more

ATTENTION

In virtual environments Honeywell recommends that you have at least one DC on each network level serviced by the virtual environment, this would include a domain controller on level 2.5 and each level 2 network. If the entire domain is hosted on virtual machines, you must ensure that the virtual domain is always availability. Refer to the latest version of the following documents on http://www.honeywellprocess.com for the hardware and software requirements of VM.

- HPS Virtualization Specification
- Virtualization Planning and Implementation Guide

Ensure that at least one domain controller is in real environment.

2.2 General guidelines for implementing a domain controller

The following table describes some general guidelines and Honeywell recommendations for implementing a domain controller in a domain.

Guideline	Honeywell recommendation
Number of domain controllers per domain	It is recommended to have a minimum of two domain controllers per domain. In cases where multiple network configuration are used, each network configuration must include at least one domain controller. If you have multiple level 2 with a level 3 network. It is recommend to have at least one domain controller on each network level. Domains with multiple OUs must have at least one domain controller per OU.
Operating system installed on domain controllers	The version of the Windows Server operating system installed on all the domain controllers in a domain should be the same. It is recommended to use different versions of the Windows Server operating system only during a migration scenario. After completing the migration, any servers running an older version of the operating system should be demoted or removed from the domain. After demoting the server, the domain operation level should be set to the native level for that version of the operating system.
Location of Active Directory Database, Log files, and SYSVOL objects	Though Microsoft recommends placing the Database, Log files, and SYSVOL objects on different drives in a system for optimal performance, Honeywell recommends using the following default locations. • Active Directory Database – `C:\Windows\NTDS` • Log Files – `C:\Windows\NTDS` • SYSVOL – `C:\Windows\SYSVOL`
Availability of Domain Name System	When the first domain controller for a domain is configured, DNS and GC server roles are enabled by default. Though Microsoft recommends to disable these roles while creating additional domain controllers in the domain, Honeywell recommendation is to configure these roles on each

Guideline	Honeywell recommendation
(DNS) and Global Catalog (GC) servers	domain controller in the domain. It is recommended to configure minimum of two DNS servers and two GC servers. You can limit the distribution of GC servers based on the network design.
Naming convention for domains	Honeywell recommends the following while configuring domain names. • The length of the domain name should contain 1 to 15 characters. • Domain name should always consist of at least two parts, a name and a designator separated by a period as follows: <Name><Designator> Typical designator values are .com, .org, or .local. Specific suffix values may be required if the domain is part of a multi-domain network. Consult the domain administrators of the domains into which the process domain needs to be integrated, to determine the names to be used as well as the address range for computers in the domain. For local domains which are not integrated into a larger domain forest, the recommendation is to use the designator as 'local'. For example, Customer.local. A domain name without a designator results in a format known as a Single-Label name and could result in various networking problems such as client computers not being able to dynamically register DNS records or encountering problems in resolving DNS name queries. For more information, refer to the following Microsoft website link: http://support.microsoft.com/kb/300684 • The Netbios name must match the DNS name of the domain. For example, pcn.local is the DNS domain name and pcn is the Netbios name.
Reverse Lookup Zones	It is recommended to configure Reverse Lookup Zone for each subnet.
Windows Internet Name Service (WINS)	WINS servers are not required. Do not configure WINS for domain controllers in an Experion network.
Setting Up Standby Operations Master	Honeywell does not recommend configuring Standby Operations Masters for Flexible Single Master Operation (FSMO) roles in a process control network. When the FSMO role holder is unavailable, it does not automatically change the FSMO role to the standby server. A Standby Operations Master is beneficial particularly in large domains with multiple domain controllers hosting millions of objects.

ATTENTION

Fault Tolerant Ethernet (FTE) must be installed on the server before the server is promoted to a domain controller, this ensure that there are no DNS or connections issues.

CHAPTER

3

INSTALLING A WINDOWS DOMAIN CONTROLLER

- Recording the domain configuration information
- Preparing a Windows domain controller
- Setting up or installing a domain controller
- Setting up a peer domain controller
- Setting up a Read-only Domain Controller
- Common tasks for setting up a domain controller

3.1 Recording the domain configuration information

While setting up a domain, as a best practice you must record all the important details about the domain configuration in the following attached Excel worksheet.

The following table provides you an understanding about the information that you need to capture. However, you must use the attached Excel worksheet to record the information mentioned in the table.

3.1.1 Domain configuration worksheet

Table 3.1 Domain configuration worksheet sample

Basic information	
Domain name	
IP address range	
IP Subnet Mask	
Groups for RODC creation(if required)	
Directory Services Restore Mode (DSRM) password	
Starting domain functional level	
Global Catalog (GC) and DNS server roles	
GC server	
DNS servers	
User accounts	*Groups*

Flexible Single Master Operation (FSMO) roles Record the details about the domain controllers which hold each of the FSMO roles in the current domain.	
FSMO role	***Site and owner***
Schema master	
Domain naming master	
Infrastructure master	
Relative ID (RID) master	
PDC emulator	
Site Information	
Site name	***Subnet address***
Domain controller information For each domain controller that is being created, capture the following details which can be used later if required.	
DC type *(One column per domain controller)*	
Domain controller name	
Site	
IP address	
Preferred DNS	
Alternate DNS	
Admin account	
Password	
Group	

3.2 Preparing a Windows domain controller

- Installing Microsoft Windows Server 2008 R2 Operating System
- Installing Microsoft service packs and Windows updates
- Configuring TCP/IP settings
- Changing the computer name

3.2.1 Installing Microsoft Windows Server 2008 R2 Operating System

If you plan to continue to use the server hardware, you must install a fresh Microsoft Windows Server 2008 R2.

It is recommended that you follow the OEM operating system installation document for loading the operating system on Honeywell-qualified or non-qualified platform.

During the initial stages of the operating system installation, a **Select the operating system you want to install** page appears. As Honeywell recommends server installation with a GUI, ensure to select **Microsoft Windows Server 2008 R2 Standard (Server with a GUI)** option.

3.2.2 Installing Microsoft service packs and Windows updates

Install Microsoft service packs and Windows updates as recommended for the Experion system installed on your computer. For more information about the supported versions, refer to the Software Change Notice (SCN) for the release of Experion that is installed on your system. The latest Software Change Notice is available at the following Honeywell Process Solutions website link.

http://www.honeywellprocess.com

> **ATTENTION**
>
> For any Experion release, it is recommended that you install the highest Microsoft service packs for Microsoft Windows Server 2008 R2 operating system.
>
> Clean operating system installation with out Honeywell software is not supported by the ISO disk provided with the SUIT. That is, if you perform a clean operating system installation using the ISO disk provided with the SUIT. Then, Honeywell is not responsible for installing Microsoft service packs and applying Windows updates on such systems. However, Honeywell still supports Domain Controllers set up with clean installation.

3.2.3 Configuring TCP/IP settings

> **ATTENTION**
>
> For any Experion release, it is recommended that you install the highest Microsoft service packs for Microsoft Windows Server 2008 R2 operating system.
>
> If Fault Tolerant Ethernet (FTE) is to be installed on the Domain Controller, you must first configure the NIC adapters for FTE. Refer to the latest version of *Fault Tolerant Ethernet Installation and Service Guide* available on http://www.honeywellprocess.com for the following:
>
> - FTE-qualified NICs.
> - Configure NIC adapters for FTE.

To open Network Connections dialog box

1. Log on to the server using an account with local administrator rights.
2. Click **Start** > **Control Panel**.
   The **Control Panel** window opens.
3. Perform one of the following steps:
   - In the **Control Panel Home** view, under **Network and Internet** area, click **View network status and tasks**.
   - In the **Control Panel Classic** view, click **Network and Sharing Center**.
4. In the **Tasks** area, click **Manage Network Connections**.
   The **Network Connections** dialog box appears.

To configure TCP/IP settings

1. Open the **Network Connections** dialog box.
2. Right-click **Local Area Connection**, and then click **Properties**.
   The **Local Area Connection Properties** dialog box appears.
3. Select **Internet Protocol Version 4 (TCP/IPv4)** and then click **Properties**.
   The **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box appears.
4. Click **Use the following IP address** option button and configure the following:
   - In the **IP address** box, type the IP address to be assigned for this network connection.

     > **ATTENTION**
     >
     > If you are performing migration, you must configure the computer with the IP address of the domain controller that this computer is replacing.

   - In the **Subnet mask** box, type the subnet mask for the network.
   - In the **Default gateway** box, type the IP address of the computer or device on your network that connects your network to another network or to the Internet.
     If you are configuring a stand-alone domain, you need not configure **Default gateway**.

5. Click **Use the following DNS Server addresses** option button and configure the following:
   - In the **Preferred DNS server** box, type the IP address of the DNS server.
   - In the **Alternate DNS server** box, type the IP address of the alternate DNS server.

> ATTENTION
> If you are setting up a domain controller running DNS, the preferred DNS server must be the root domain controller that you are setting up and the alternate DNS server must be the peer domain controller that runs DNS.

6. Click **OK**.
   The **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box closes.
7. In the **Local Area Connection Properties** dialog box, click **OK**.

3.2.4 Changing the computer name

This procedure is normally performed as part of the operating system installation. Perform this procedure if you have not changed the computer name during operating system installation or if you are using a computer preinstalled with the target operating system.

To change the computer name

1. Log on to the computer using a Windows account with local administrator rights.
2. Click **Start** > **Administrative Tools** > **Server Manager**.
   The **Server Manager** window appears.
3. In the **Server Summary** area, under **Computer Information**, click the **Change System Properties** link.
   The **System Properties** dialog box appears.
4. On the **Computer Name** tab, click **Change**.
   The **Computer Name/Domain Changes** dialog box appears.
5. In the **Computer Name** box, type the computer name and click **OK**.
   While performing migration, you must configure the computer with the same name as the domain controller that this computer is replacing.
   A message appears indicating to restart the computer.
6. Click **OK**.
7. In the **System Properties** dialog box, click **OK**.
   The **System Properties** dialog box closes. A message appears prompting to restart the computer.
8. Click **Restart now**.
   The computer restarts.

> ATTENTION
> It is important to restart the server after changing the computer name and before promoting the server to a domain controller.

3.3 Setting up or installing a domain controller

The following table lists the tasks that you must perform for setting up a domain controller.

Task	Refer to
Installing the Microsoft Windows Server 2008 R2 server as a domain controller	Installing the Microsoft Windows Server 2008 R2 server as a domain controller
Verifying if DNS server role is active	Verifying if DNS server role is active
Verifying if Global Catalog server role is active	Verifying if Global Catalog server role is active
Adding reverse lookup zone	Adding reverse lookup zone

If you are setting up a domain controller for adding it to an existing domain or replace an existing domain controller, refer to the section Setting up a peer domain controller. If you are installing the server as a domain controller for the first time or setting up a new domain, perform the steps in this section Installing the Microsoft Windows Server 2008 R2 server as a domain controller.

- **Installing the Microsoft Windows Server 2008 R2 server as a domain controller**

3.3.1 Installing the Microsoft Windows Server 2008 R2 server as a domain controller

This topic describes the steps to set up or install a Microsoft Windows Server 2008 R2 server as a domain controller added to a new domain in a new forest or to a new domain in an existing forest. If this node is the first domain controller that you are setting up in a new domain, to add additional domain controllers in the domain, refer to the sections Setting up a peer domain controller and Setting up a Read-only Domain Controller.

In addition, this section also describes the steps to automatically assign the Microsoft Windows Server 2008 R2 server the role of a primary domain controller.

To install Microsoft Windows Server 2008 R2 server as a domain controller

1. Log on to the computer using a Windows account with administrator privileges.
2. Click **Start** > **Run**.

   The **Run** dialog box appears.
3. Type **dcpromo**, and then press **ENTER**.

   The command validates if the Active Directory Domain Services binaries are available on the system and install them, if not already installed. After completing the installation, the **Active Directory Domain Services Installation Wizard** appears.
4. If the message *If you want to run using advanced mode (Y/N)* appears, press **N**.
5. Click **Next**.

   The **Operating System Compatibility** page appears.
6. Click **Next**.

   The **Choose a Deployment Configuration** page appears.

7. You can set up a primary domain controller in one of the following ways:
   - In a new domain in a new forest
   - In a new domain in an existing forest

   The following table describes the steps that you need to perform for both the configuration options. Perform the steps for one of the options, as desired.

New domain in a new forest	New domain in an existing forest
a. Click the **Create a new domain in a new forest** option button, and then click **Next**. The **Name the Forest Root Domain** page appears. b. On the **FQDN of the forest root domain** box, type the Fully Qualified Domain Name (FQDN) of the new forest domain, and then press **Next**. The system validates the information provided and the **Set Forest Functional Level** page appears. c. In the **Forest functional level** list, click the desired forest functional level, and then click **Next**. The **Additional Domain Controller Options** page appears. **TIP** As the Forest functional level (FFL) can be changed to a higher versions at any point; it is recommended that you set the FFL to the level of the earliest DC in the domain. For example, set the FFL to 2003 if there is still a Windows Server 2003 DC in your domain. This enables the new domain to support the features of Windows Server 2003, in addition to the features provided in higher versions.	a. Click the **Existing forest** and **Create a new domain in an existing forest** option buttons, and then click **Next**. The **Network Credentials** page appears. b. On the **Network Credentials** page, perform the following: i. In the **Type the name of any domain in the forest where you plan to install this domain controller** box, type the name of any existing domain in the forest, and then click **Set**. The **Windows Security** page appears. ii. Type the user name and password for the domain administrator account, and then click **OK**. c. Click **Next**. The **Name the New Domain** page appears. d. On the **Name the New Domain** page, perform the following: i. On the **FQDN of the parent domain** box, type the Fully Qualified Domain Name (FQDN) of the parent domain.

New domain in a new forest	New domain in an existing forest
d. Ensure that the **DNS server** check box is selected, and then click **Next**. A message appears indicating that you should manually create a delegation for this DNS server in the parent zone. e. Click **Yes** to continue.	ii. On the **Single–label DNS name of the child domain** box, type the new domain name. iii. Click **Next**. The **Select a Site** page appears displaying a list of sites which are configured in the domain. e. Select a site for the domain controller, and then click **Next**. The **Additional Domain Controller Options** page appears. f. To enable DNS server and Global Catalog (GC) services, select the **DNS server** and the **Global catalog** check boxes, and then click **Next**.

The **Location for Database, Log Files and SYSVOL** page appears.

By default, the location to store the database files, the log files, and the SYSVOL files is set as the local hard disk. If required, you can change the default location. Honeywell recommends to retain the default locations of the database files, the log files, and the SYSVOL files for domain controllers in a domain where high traffic or space considerations are expected.

8. Click **Next**.

   The **Directory Services Restore Mode Administrator Password** page appears.

9. In the **Password** and **Confirm password** boxes, type the desired password, and then click **Next**.

   The **Summary** page appears.

10. Review the configuration settings that you have selected in the **Active Directory Domain Services Installation Wizard**, and then click **Next**. To change any of the configuration settings, click **Back**.

    The installation of the Active Directory services starts and the progress of installation is displayed. When complete, the **Completing the Active Directory Domain Services Installation Wizard** page appears.

11. Click **Finish**.

    A message appears prompting you to restart the computer.

12. Click **Restart Now**.

    The computer restarts.

3.4 Setting up a peer domain controller

Before performing the tasks described in this section, ensure that you have completed the initial preparation tasks described in the section Preparing a Windows domain controller. The following table lists the task that you must perform for setting up a peer domain controller.

Task	Refer to
Adding Microsoft Windows Server 2008 R2 to a Windows domain	Adding Microsoft Windows Server 2008 R2 to a Windows domain
Adding Microsoft Windows Server 2008 R2 to the role of a peer domain controller	Adding Microsoft Windows Server 2008 R2 server to the role of a peer domain controller
Verifying if DNS server role is active	Verifying if DNS server role is active
Verifying if Global Catalog server role is active	Verifying if Global Catalog server role is active

- Adding Microsoft Windows Server 2008 R2 server to the role of a peer domain controller

3.4.1 Adding Microsoft Windows Server 2008 R2 server to the role of a peer domain controller

This topic describes the steps to add a Microsoft Windows Server 2008 R2 server to the role of a peer domain controller.

Prerequisites

Ensure to add the system to the domain.

To add Microsoft Windows Server 2008 R2 server to the role of a peer domain controller

1. Log on to the computer using a Windows account with Domain administrator rights.
2. Click **Start** > **Run**.

   The **Run** dialog box appears.
3. Type **dcpromo**, and then press **ENTER**.

   The command validates if the Active Directory Domain Services binaries are available on the system and install them, if not already installed. After completing the installation, the **Active Directory Domain Services Installation Wizard** appears.
4. Click **Next**.

   The **Operating System Compatibility** page appears.
5. Click **Next**.

   The **Choose a Deployment Configuration** page appears.
6. On the **Choose a Deployment Configuration** page, perform the following:
   a. Click the **Existing forest** option button.
   b. Click the **Add a domain controller to an existing domain** option button.
   c. Click **Next**.

The **Network Credentials** page appears.

7. On the **Network Credentials** page, perform the following:
   a. In the **Type the name of any domain in the forest where you plan to install this domain controller** box, type the name of the any existing domain in the forest, and then click **Set**.

      The **Windows Security** dialog box appears.
   b. Type the user name and password for the domain administrator account and click **OK**.
   c. Click **Next**.

      The system validates the domain Active Directory information and a dialog box appears displaying the status of the validation. If the validation fails, it indicates that you have entered the incorrect user name or password. Enter the correct user name and password to proceed to the next step.

      The **Select a Domain** page appears displaying a list of available domains.
8. Ensure that the domain to which you want to add the domain controller is selected by default, and then click **Next**.

   The **Select a Site** page appears displaying a list of sites which are configured on the domain.
9. Select a site for the domain controller, and then click **Next**.

   The **Additional Domain Controller Options** page appears.
10. To enable DNS server and Global Catalog (GC) services, select the **DNS server** and the **Global catalog** check boxes, and then click **Next**.

> ATTENTION
>
> It is recommended to enable DNS server and GC services in each domain controller in a domain.

   The system validates the DNS configuration. If the domain does not contain information about an authoritative parent zone, a message appears indicating that you should manually create a delegation for this DNS server in the parent zone.
11. Click **Yes** to continue.

    The **Location for Database, Log Files and SYSVOL** page appears.

    By default, the location to store the database files, the log files, and the SYSVOL files is set as the local hard disk. If required, you can change the default location. Honeywell recommends to retain the default locations of the database files, the log files, and the SYSVOL files for domain controllers in a domain where high traffic or space considerations are expected.
12. Click **Next**.

    The **Directory Services Restore Mode Administrator Password** page appears.
13. In the **Password** and **Confirm password** boxes, type the desired password, and then click **Next**.

    The **Summary** page appears.
14. Review the configuration settings that you have selected in the **Active Directory Domain Services Installation Wizard**, and then click **Next**. To change any of the configuration settings, click **Back**.

    The installation of the Active Directory services starts and the progress of installation is displayed. When complete, the **Completing the Active Directory Domain Services Installation Wizard** page appears.
15. Click **Finish**.

    A message appears prompting you to restart the computer.
16. Click **Restart Now**.

    The computer restarts.

3.5 Setting up a Read-only Domain Controller

You can set up a Read-only Domain Controller (RODC) in one of the following ways:

- Direct installation - Enables you to install an RODC similar to the approach used for installing additional domain controllers in the domain. In this method, RODC installation can performed by a member of the domain administrator group. This method installs an RODC by selecting the **Read-only domain controller (RODC)** option in the **Active Directory Domain Services Installation Wizard**.
- Staged installation - Enables you to install an RODC in two stages. First you create a user account in the domain administrator group. In this method, a member of the domain administrator group creates a special account which is granted the privileges to create an RODC. The delegated RODC administrator can complete the installation by attaching a server to the RODC account. This method also eliminates the need to use the domain administrator credentials to set up an RODC.

> **ATTENTION**
>
> It is not possible to change a domain controller from writable to read-only or from read-only to writable, directly. To change a writable domain controller to an RODC, you must demote the domain controller and then promote it again to an RODC. This requires domain administrator permissions and uses the direct installation method for creating the RODC.

The following table lists the task that you must perform for setting up a read-only domain controller.

Task	Refer to
Creating user account for staged Read-Only Domain Controller installation	Creating user account for staged Read-Only Domain Controller installation
Adding Microsoft Windows Server 2008 R2 to a Windows domain	Adding Microsoft Windows Server 2008 R2 to a Windows domain
Adding Microsoft Windows Server 2008 R2 to the role of a read-only domain controller	Adding Microsoft Windows Server 2008 R2 server to the role of a Read-Only Domain Controller
Verifying if DNS server role is active	Verifying if DNS server role is active
Verifying if Global Catalog server role is active	Verifying if Global Catalog server role is active

- **Creating user account for staged Read-Only Domain Controller installation**
- **Adding Microsoft Windows Server 2008 R2 server to the role of a Read-Only Domain Controller**

3.5.1 Creating user account for staged Read-Only Domain Controller installation

To create a user account for staged Read-Only Domain Controller installation

1. Log on to an active domain controller in the domain.
2. Click **Start** > **All Programs** > **Administrative Tools** > **Active Directory Administrative Center**.

   The **Active Directory Administrative Center** window appears.
3. In the navigation pane on the left side of the **Active Directory Administrative Center** window, click the right arrow against the domain name, and then click **Domain Controllers**.
4. In the tasks pane, click **Pre-create a Read-only domain controller account**.

   The **Active Directory Domain Services Installation Wizard** appears.
5. Click **Next**.

   The **Operating System Compatibility** page appears.
6. Click **Next**.

   The **Network Credentials** page appears.
7. Under **Specify the account credentials to use to perform the installation**, click the **My current logged on credentials**, and then click **Next**.

   The **Specify the Computer Name** page appears.
8. In the **Computer name** field, type the computer name, and then click **Next**.

   The **Select a Site** page appears.
9. Select a site for the domain controller, and then click **Next**.

   The **Additional Domain Controller Options** page appears.
10. On the **Additional Domain Controller Options** page, set the following options.
    - **DNS server**- The **DNS server** check box is selected by default. If you do not want the domain controller to be configured as the DNS server, clear the check box.
    - **Global catalog**- The **Global catalog** check box is selected by default. If you do not want the domain controller to be configured as the GC server, clear the check box.

    > ATTENTION
    > By default, the **Read-only domain controller** option is selected and disabled.

    The system validates the DNS configuration. If the domain does not contain information about an authoritative parent zone, a message appears indicating that you should manually create a delegation for this DNS server in the parent zone. Click **Yes** to continue.

    The **Delegation of RODC Installation and Administration** page appears.
11. In the **Group or user** box, type the name of the user or group to which you can delegate the rights to attach a server to the RODC account, and then click **Next**.

    If you do not know the name of the user or the group, click **Set** to search the directory for the required user or group.

    The **Summary** page appears.
12. Review the configuration options that you have selected in the **Active Directory Domain Services Installation Wizard**, and then click **Next**.

    The installation of the Active Directory services starts and the progress of installation is displayed. When complete, the **Completing the Active Directory Domain Services Installation Wizard** page appears.

13. Click **Finish**.

    The **Active Directory Domain Services Installation Wizard** closes. The newly added user account appears in the **Active Directory Administrative Center** window.

3.5.2 Adding Microsoft Windows Server 2008 R2 server to the role of a Read-Only Domain Controller

This topic describes the steps to add a Microsoft Windows Server 2008 R2 server to the role of an RODC.

Prerequisites

Ensure to add the node to the domain controller before promoting the domain controller as an RODC.

To add Microsoft Windows Server 2008 R2 server to the role of an RODC

1. Log on to the computer using a Windows account with administrator rights.

   While logging on to the computer, you can type the user name either as `UserName` or `Domain\UserName`. If you specify the domain name along with the user name, the domain credentials are used and you need not provide them later while running the **dcpromo** command.

2. Click **Start** > **Run**.

   The **Run** dialog box appears.

3. Type **dcpromo**, and then press **ENTER**.

   The command validates if the Active Directory Domain Services binaries are available on the system and install them, if not already installed. After completing the installation, the **Active Directory Domain Services Installation Wizard** appears.

4. Click **Next**.

   The **Operating System Compatibility** page appears.

5. Click **Next**.

   The **Choose a Deployment Configuration** page appears.

6. On the **Choose a Deployment Configuration** page, perform the following:
   a. Click the **Existing forest** option button.
   b. Click the **Add a domain controller to an existing domain** option button.
   c. Click **Next**.

   The **Network Credentials** page appears.

7. On the **Network Credentials** page, perform the following:
   a. In the **Type the name of any domain in the forest where you plan to install this domain controller** box, type the name of the any existing domain in the forest, and then click **Set**.

      The **Windows Security** dialog box appears.
   b. Type the user name and password for the domain administrator account and click **OK**.
   c. Click **Next**.

      The system validates the domain Active Directory information and a dialog box appears displaying the status of the validation. If the validation fails, it indicates that you have entered the incorrect user name or password. Enter the correct user name and password to proceed to the next step.

      The **Select a Domain** page appears displaying a list of available domains.

8. Select the domain to which you want to add the domain controller, and then click **Next**.

   A warning message appears indicating that a read-only domain controller is created using an existing account in AD DS.

9. Click **OK** to continue.

   The **Location for Database, Log Files and SYSVOL** page appears.

   By default, the location to store the database files, the log files, and the SYSVOL files is set as the local hard disk. If required, you can change the default location. Honeywell recommends to retain the default locations of the database files, the log files, and the SYSVOL files for domain controllers in a domain where high traffic or space considerations are expected.

10. Click **Next**.

    The **Directory Services Restore Mode Administrator Password** page appears.

11. In the **Password** and **Confirm password** boxes, type the desired password, and then click **Next**.

    The **Summary** page appears.

12. Review the configuration settings that you have selected in the **Active Directory Domain Services Installation Wizard**, and then click **Next**. To change any of the configuration settings, click **Back**.

    The installation of the Active Directory services starts and the progress of installation is displayed. When complete, the **Completing the Active Directory Domain Services Installation Wizard** page appears.

13. Click **Finish**.

    A message appears prompting you to restart the computer.

14. Click **Restart Now**.

    The computer restarts.

3.6 Common tasks for setting up a domain controller

This section describes the tasks that are common for setting up a primary or peer or read-only domain controller.

- Adding Microsoft Windows Server 2008 R2 to a Windows domain
- Verifying if DNS server role is active
- Verifying if Global Catalog server role is active
- Adding reverse lookup zone

3.6.1 Adding Microsoft Windows Server 2008 R2 to a Windows domain

To add a Microsoft Windows Server 2008 R2 to a Windows domain

1. Log on to the computer using a Windows account with local administrator rights.
2. Click **Start** > **Administrative Tools** > **Server Manager**.

   The **Server Manager** window appears.

3. In the **Server Summary** area, under **Computer Information**, click the **Change System Properties** link.

   The **System Properties** dialog box appears.

4. On the **Computer Name** tab, click **Change**.

   The **Computer Name/Domain Changes** dialog box appears.

5. Click the **Domain** option button, and then type the name of the domain.

6. If prompted, type the user name and the password of the domain administrator account, and then click **OK**.

   The computer registers with the domain. This may take several seconds.

7. Click **OK** to acknowledge the welcome message.
8. Click **OK**.
9. In the **System Properties** dialog box, click **OK**.

   The **System Properties** dialog box closes. A message appears prompting to restart the computer.

10. Click **Restart Now**.

    The computer restarts.

3.6.2 Verifying if DNS server role is active

To verify if DNS server role is active on the domain controller

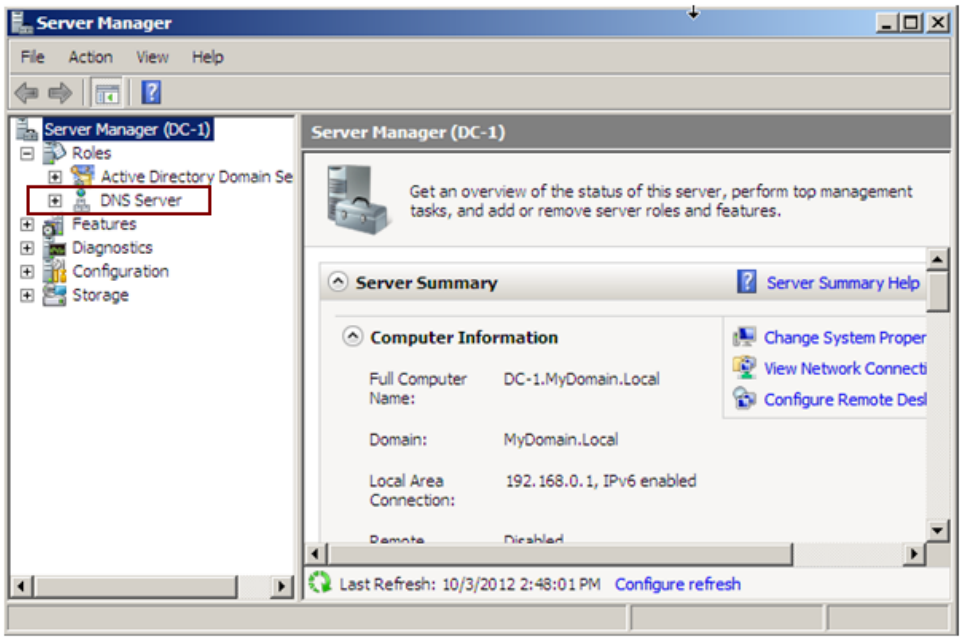
1. Log on to the domain controller.
2. Click **Start** > **Administrative Tools** > **Server Manager**.

   The **Server Manager** window appears.

3. In the left pane, expand **Roles**.

   The roles currently configured for the domain controller are displayed.

4. To determine if a domain controller is configured as DNS server, in **Roles**, check if **DNS Server** item is available.



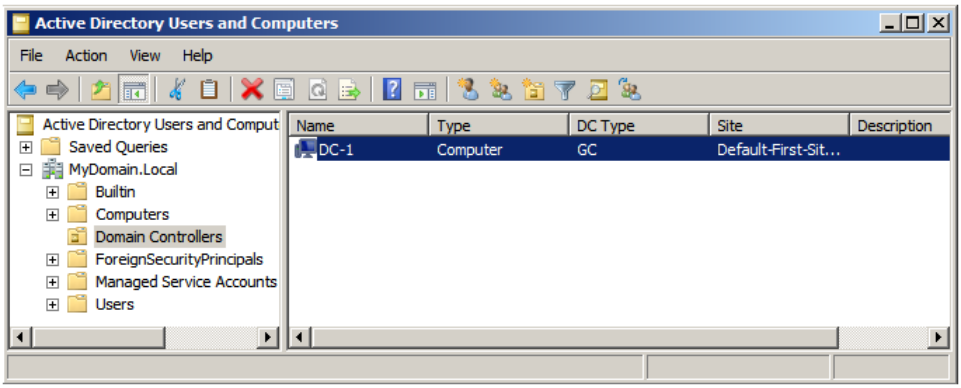
5. Close the **Server Manager** window.

3.6.3 Verifying if Global Catalog server role is active

To verify if Global Catalog server role is active on the domain controller

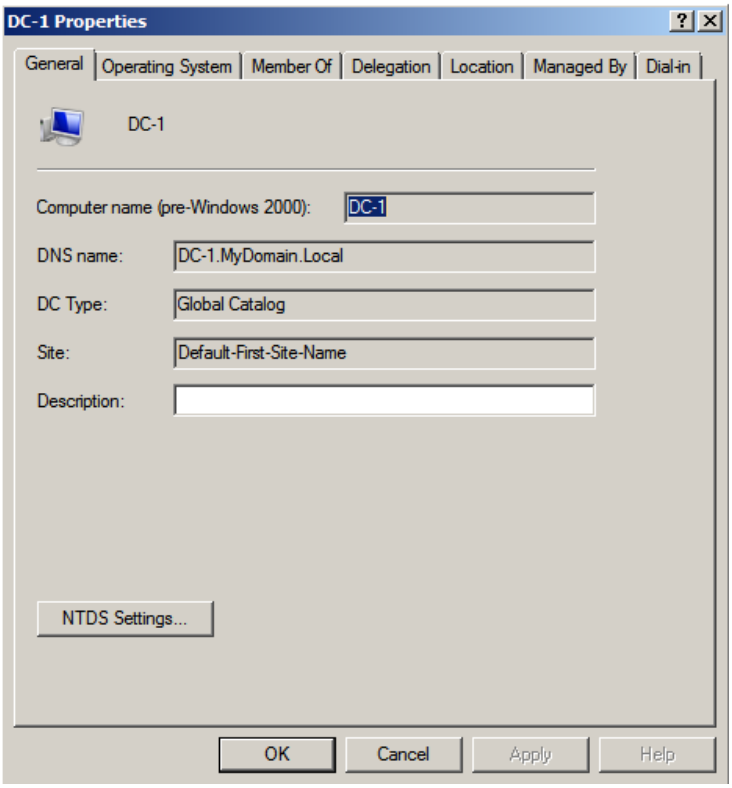
1. Log on to the domain controller.
2. Click **Start** > **Administrative Tools** > **Active Directory Users and Computers**.

   The **Active Directory Users and Computers** window opens.
3. In the console tree on the left pane of the **Active Directory Users and Computers** window, expand <domain name>, and then click **Domain Controllers**.



4. In the details pane that is on the right side of the **Active Directory Users and Computers** window, right-click the domain controller, and then click **Properties**.

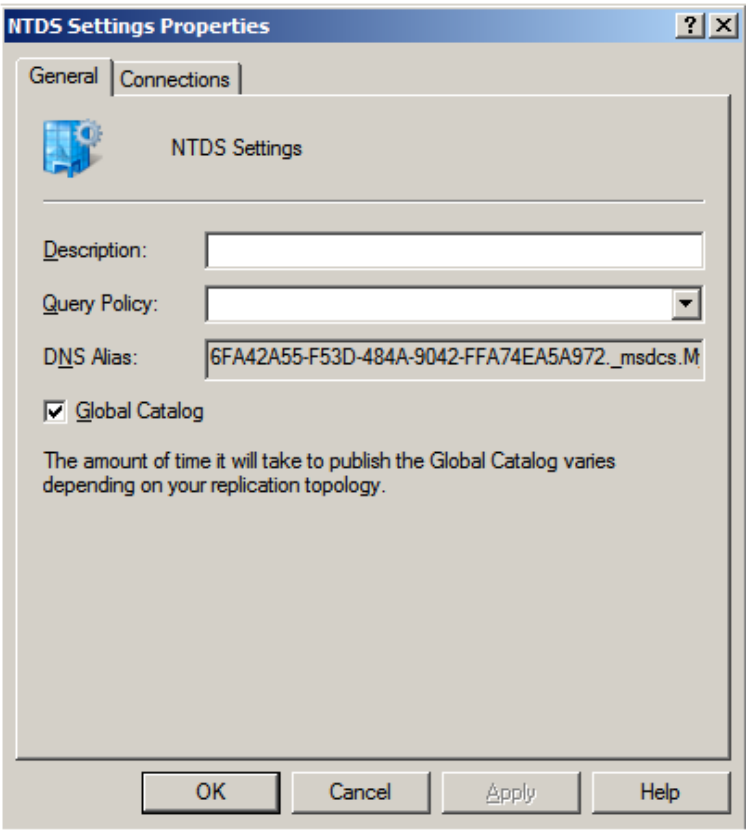
   The domain controller **Properties** dialog box appears.



5. On the **General** tab, ensure that the **DC Type** field displays **Global Catalog**.

6. Click **NDTS Settings**.

   The **NDTS Settings Properties** dialog box appears.



7. On the **General** tab, ensure that the **Global Catalog** check box is selected.

   This indicates that the **Global Catalog** server role is active

8. Close all the open dialog boxes.

3.6.4 Adding reverse lookup zone

Reverse lookup zones that are active directory integrated are replicated to the new DNS server.

To add reverse lookup zone

1. Click **Start** > **All Programs** > **Administrative Tools** > **DNS**.

   The **DNS Manager** window appears.

2. In the console tree, expand items under **DNS** until **Reverse Lookup Zones** item appears.

   If there is an entry for the IP address configured in your domain, do not perform the remaining steps in this procedure. Proceed to the section Configuring alternate DNS for all the nodes in the domain. Note that the order of the IP address octets is reversed in the IP address entry.

3. Right-click DNS server name, and then click **New Zone**.

   The **New Zone Wizard** appears.

4. On the Welcome page of the **New Zone Wizard**, click **Next**.

5. Click **Primary zone**, and then click **Next**.

6. On the **Active Directory Zone Replication Scope** page, click **To all DNS servers in this domain**, and then click **Next**.

7. On the **Forward or Reverse Lookup Zone** page, click **Reverse lookup zone**, and then click **Next**.

8. On the **Reverse Lookup Zone Name** page, click **IPv4 Reverse Lookup Zone**, and then click **Next**.

   The **Reverse Lookup Zone Name** page updates to provide options to configure **Network ID** and **Reverse lookup zone name**.

   The **Dynamic Update** page appears.

9. Select **Allow only secure dynamic updates (recommended for Active Directory)** and then click **Next**.

   The **Completing the New Zone Wizard** page appears.

10. On the **Completing the New Zone Wizard** page, review the settings that you have configured in the wizard, and then click **Finish**.

Results

Ensure that the reverse lookup zone is created under the DNS.

CHAPTER

4

POST INSTALLATION TASKS

- Configuring Active Directory sites
- Creating Active Directory users and groups
- Configuring time synchronization in a domain
- Adding workstation/server to Windows domain
- Configuring time synchronization on the workstations/servers added to a Windows domain

4.1 Configuring Active Directory sites

A default site is always provided. The default site is adequate for simple installations.

- Creating a site in Active Directory
- Moving domain controllers to sites
- Verifying the availability of Global Catalog server in a site
- Adjusting replication interval for a site

4.1.1 Creating a site in Active Directory

To create a site in Active Directory

1. Log on to one of the domain controllers in the domain using an account with administrative privileges.
2. Click **Start** > **All Programs** > **Administrative Tools** > **Active Directory Sites and Services**.
   The **Active Directory Sites and Services** window opens.
3. In the console tree, right-click **Sites**, and then click **New Site**.
   The **New Object – Site** dialog box appears.
4. In the **Name** box, type the name of the new site.
5. In **Link Name** list, select the site link object for this site and then click **OK**.
   A dialog box appears indicating that a new site is created in the Active Directory.

   > **NOTE**
   > This Dialog box does not appears, if the user deletes an old site and tries to add a **New Site**.

6. Click **OK**.
   The new site name appears under **Sites** folder in the console tree.

7. In the console tree, right-click the **Subnets** folder, and then click **New Subnet**.
   The **New Object – Site** dialog box appears.
8. In the **Prefix** box, type the IPv4 or the IPv6 subnet prefix.
9. In the **Select a site object for this prefix** list, click the site to be associated with the subnet prefix.
10. Click **OK**.
    This creates a site in Active directory.

4.1.2 Moving domain controllers to sites

To move domain controllers to sites

1. Log on to one of the domain controllers in the domain using an account with administrative privileges.
2. Click **Start** > **All Programs** > **Administrative Tools** > **Active Directory Sites and Services**.
   The **Active Directory Sites and Services** window opens.
3. In the console tree, expand the **Sites** folder and the site in which the server object resides.
   By default, a domain controller is added to the site named **Default-First-Site-Name**.
4. Expand the site **Default-First-Site-Name**, and then the **Servers** folder.
   The **Servers** folder displays the domain controllers that are currently configured for that site.
5. Right-click the sever object that you want to move, and then click **Move**.
   The **Move Server** dialog box appears.
6. In the **Select the site that should contain this server** list, click the site name to which the server needs to be transferred, and then click **OK**.
   The **Active Directory Sites and Services** window updates indicating that the server is moved to the site.

4.1.3 Verifying the availability of Global Catalog server in a site

It is recommended that at least one of the domain controllers associated with each site is configured as a GC server. This accelerates the authentication requests within the site and also helps to avoid cross site transfers.

To verify the availability of Global Catalog server in a site

1. Log on to one of the domain controllers in the domain using an account with administrative privileges.
2. Click **Start** > **All Programs** > **Administrative Tools** > **Active Directory Sites and Services**.
   The **Active Directory Sites and Services** window opens.
3. In the console tree, expand **Sites** folder, and then expand the site object on which the servers reside.
4. Expand the **Servers** folder, and then expand the server name.
   The **NDTS Settings** items appear under the server name.
5. Right-click **NDTS Settings** item, and then click **Properties**.
   The **NDTS Settings Properties** dialog box appears.
6. Verify if the **Global Catalog** check box is selected. If not, select the **Global Catalog** check box, and then click **OK**.
   The **NDTS Settings Properties** dialog box closes.

4.1.4 Adjusting replication interval for a site

Changes to the Active Directory information in any of the domain controllers replicates to the other servers in the domain on a regular basis. The replication also occurs during a system reboot or when manually initiated. Windows uses a very efficient algorithm to replicate only the information that is changed so that the network load due to replication is minimal. The default time between replications can be configured using the Active Directory Sites and Services snap-in as follows.

> ATTENTION
>
> Honeywell recommends that you to leave the replication interval with the default settings. However, refer to the following procedure if you want to make any adjustment to the replication interval for your site.

To adjust replication interval for a site

1. Log on to one of the domain controllers in the domain using an account with administrative privileges.
2. Click **Start** > **All Programs** > **Administrative Tools** > **Active Directory Sites and Services**.

   The **Active Directory Sites and Services** window opens.
3. In the console tree, expand **Inter-Site Transports** folder, and then click the **IP** folder.
4. In the right-pane of the **Active Directory Sites and Services** window, double-click **DEFAULTIPSITELINK**.

   The **DEFAULTIPSITELINK Properties** dialog box appears. The **Replicate every** box displays the configured replication time.
5. To change the replication time, in the **Replicate every** box, type or select the new time in minutes.

   > ATTENTION
   >
   > The minimum replication time is 15 minutes and the maximum replication time is 10080 minutes (168 hours, or 7 days). When the sites are interconnected over high-speed links, it is recommended to configure the replication interval as 15 minutes. If slow links are used or in cases where the network traffic is heavy, the replication interval can be increased.

   You can also adjust the replication interval as follows:

   a. Click **Change Schedule**.

      The **Schedule for DEFAULTIPSITELINK** dialog box appears. By default, the replication schedule appears as 24 hours a day, 7 days a week.

   b. To change the default replication interval, adjust the day and time settings using the mouse pointer.

   c. Click **Replication Not Available** or **Replication Available**, as appropriate.

   d. Click **OK**.
6. Click **Apply**, and then click **OK**.

   The **DEFAULTIPSITELINK Properties** dialog box closes.

4.2 Creating Active Directory users and groups

- Creating Honeywell Active Directory users
- Creating Active Directory groups
- Changing group membership

4.2.1 Creating Honeywell Active Directory users

To create Honeywell Active Directory users

1. Log on to the domain controller using an account with administrative privileges.
2. Click **Start** > **All Programs** > **Administrative Tools** > **Active Directory Users and Computers**.
   The **Active Directory Users and Computers** window opens.
3. In the console tree, expand <domain name>, right-click **Users**, and then click **New** > **User**.
   The **New Object – User** dialog box appears.
4. In the **First name** box, type the user's first name.
5. In the **Initials** box, type the user's initials.
6. In the **Last name** box, type the user's last name.
7. In the **Full name** box, modify the details to add initials or reverse the order of first and last names.
8. In the **User logon** box, type the user logon name, click the UPN suffix in the drop-down list, and then click **Next**.
9. Type the password in the **Password** and **Confirm Password** boxes.
10. Ensure that the **Password never expires** option is selected. This setting is configured at the site.
11. Click **Next** and then click **Finish**.
    The new user account is created in Active Directory Domain Services.
12. To verify if the new user account is created, perform the following steps.
    a. In the console tree, under <domain name>, click **Users**.
    b. In the right-pane, verify if the new user name is displayed in the list of available users and groups.

4.2.2 Creating Active Directory groups

To create Active Directory groups

1. Log on to the domain controller using an account with administrative privileges.
2. Click **Start** > **All Programs** > **Administrative Tools** > **Active Directory Users and Computers**.
   The **Active Directory Users and Computers** window opens.
3. In the console tree, right-click the folder (*Active Directory Users and Computers/domain node/folder*) in which you want to add a group.
4. Click **New** > **Group**.
   The **New Object – Group** dialog box appears.
5. Type the **Group** name.

6. Select **Group scope** and **Group type** for the group, as desired.
7. Click **OK**.

   A new group is created and appears in the details pane of the **Active Directory Users and Computers** window.

4.2.3 Changing group membership

To change group membership

1. Log on to the domain controller using an account with administrative privileges.
2. Click **Start** > **All Programs** > **Administrative Tools** > **Active Directory Users and Computers**.

   The **Active Directory Users and Computers** window opens.
3. In the console tree, browse to the folder (Active Directory Users and Computers/domain node/folder) containing the group that you want to modify.
4. Select the **Honeywell Group** that you want to modify.
5. In the details pane (right pane), right-click the group, and then click **Properties**.
6. On the **Members** tab, click **Add**.
7. Enter the Honeywell user name and then **Check Names**.

   A valid entry will have an underline.
8. Click **OK**.
9. Repeat steps until the required users are added to the group.
10. Click **OK**.

For further guidance on managing groups, refer to the following Microsoft documentation.

http://technet.microsoft.com/en-us/library/cc738263(WS.10).aspx

4.3 Configuring time synchronization in a domain

After configuring all systems for roles in a domain, any prior time topology becomes invalid due to the configuration changes. Hence, you must configure a new time topology by considering the domain and control system requirements; otherwise, the system uses the local clock for the authoritative time source in the domain.

Refer to the section *Setting up time synchronization* in *Supplementary Installation Tasks Guide*.

You can also use an external time source if desired. You must set the external time source only on the PDC role holder. For more information about configuring an external time source, refer to the following Microsoft documentation.

http://support.microsoft.com/kb/816042

4.3.1 Prerequisites

Before setting up time synchronization, read the section " Time synchronization" in the *Server and Client Planning Guide*.

4.4 Adding workstation/server to Windows domain

- Setting the DNS server IP address
- Adding a node to a Windows domain
- Viewing the workstation/server added to a domain

4.4.1 Setting the DNS server IP address

The steps in this topic are specific to Microsoft Windows 7 operating system.

Setting the DNS server IP address

1. Log on to the stand-alone workstation/Experion server as a local administrator.
2. Open Control Panel.
3. Click **Network and Sharing Center**, and then in the left side of the window, click **Change adapter settings**.

   The **Network Connections** window appears.
4. Right-click **Local Area Connection**, and then click **Properties**.

   The **Local Area Connection Properties** dialog box appears.
5. Click **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.

   The **Internet Protocols (TCP/IP) Properties** dialog box appears.
6. Click **Use the following DNS server addresses**.
7. In **Preferred DNS server** and **Alternate DNS server** box, type the preferred DNS server IP address and the alternate DNS server IP address of the domain controller.
8. Click **OK**.

   The **Local Area Connection Properties** dialog box closes.

4.4.2 Adding a node to a Windows domain

> **CAUTION**
>
> While adding a node to a domain, you must not change the computer name and the domain at the same time.

> **ATTENTION**
>
> To join the domain, the client machine (server or desktop) must have DNS resolution to the domain. This may require editing the network card properties and configuring primary and alternative DNS server addresses. These should be the addresses of the domain controllers on a domain running Active Directory-integrated DNS.

1. Log on to the client node as a local administrator.
2. Perform one of the following:

Operating system	Steps
For Windows 7:	a. Click **Start** > **Control Panel**. b. In **View by** list, click **Small icons**. c. Click **System**. d. Under **Computer name, Domain, and Workgroup Settings** area, click **Change Settings**. e. Click **Continue** in the **User Account Control** dialog box, if prompted. The **System Properties** dialog box appears.
For Windows Server 2008:	a. Click **Start** > **Control Panel**. b. Select **Classic View**, if not selected. c. Double-click **System**. d. Under **Computer name, Domain, and Workgroup Settings** area, click **Change Settings**. e. Click **Continue** in the **User Account Control** dialog box, if prompted. The **System Properties** dialog box appears.
For Microsoft Windows Server 2008 R2:	a. On the taskbar, click **Server Manager** icon. The **Server Manager** dialog box appears. b. In the left pane click **Local Server**. The **Local Server** page appears. c. In **PROPERTIES** field, click the text against **Workgroup**. The **System Properties** dialog box appears.

3. Click **Change**.
4. Under **Member of** area, click the **Domain** option button, and then type the domain name.
5. Click **OK**.
6. Type the user name and password of a domain administrator account, and then click **OK**.
7. In the **Welcome** dialog box, click **OK**.
8. In the **You must restart...** dialog box, click **OK**
9. In the **System Properties** dialog box, click **Close**.
10. Click **Restart Now**.
    The computer restarts.

4.4.3 Viewing the workstation/server added to a domain

To view the workstation/server added to a domain

1. Click **Start** > **All Programs** > **Administrative Tools** > **Active Directory Users and Computers**.

   The **Active Directory Users and Computers** window opens.
2. In the console tree, expand <domain name> and then click **Computers** folder.

   The details pane on the right side of the window displays the computer accounts available in the domain. The computer account uniquely identifies the computer added to the domain. The Windows computer account matches the name of the computer joining the domain.
3. Verify if the name of the workstation/server that you have added appears in the available list of computer accounts.

> **ATTENTION**
> All new computers that are added to the domain will be assigned to the computers container. Once the computer is added to the domain it can be moved to another OU.

4.5 Configuring time synchronization on the workstations/servers added to a Windows domain

If your Experion system is integrated with a Windows domain, it is recommended that you use the domain controller as the time source for all the clients within the domain. The Experion server should be configured as the NTP server which receives time from the domain controller. Though Flex Stations and Console Stations are set up as NTP clients, they receive time from the domain controller rather than the Experion servers.

The Experion servers configured as NTP servers serve time to the control hardware. This is because domain controllers are typically not on a network that is accessible to Experion. The controllers within the process control should be configured to get their time from an Experion server that has been set up as an NTP server acting as a secondary NTP server.

4.5.1 Prerequisites

Before setting up time synchronization, read the section " Time synchronization" in the *Server and Client Planning Guide*.

4.5.2 Tasks to be performed for configuring time synchronization on the workstations/servers added to the Windows domain

Task	Go to
Configure primary Experion server as the secondary NTP server.	“Adjusting NTP servers” in the *Supplementary Installation Tasks Guide*.
Configure secondary Experion server and other Experion clients as the NTP clients.	“Adjusting NTP clients” in the *Supplementary Installation Tasks Guide*.
Configure control hardware to receive time from secondary NTP server.	“Setting up control hardware to receive time from an NTP server in a Windows domain” in the *Supplementary Installation Tasks Guide*.

CHAPTER

5

PREPARING THE DOMAIN FOR MIGRATION

- Recording the current domain controller configuration information
- Inventorying the current domain controller configuration
- Verifying domain controller readiness for migration
- Preparing the Active Directory

5.1 Recording the current domain controller configuration information

The first stage in planning a migration is understanding the current domain controller configuration. Before starting the migration, you must record all the important details about the current domain controller configuration in the following attached Excel worksheet.

The following table provides you an understanding about the information that you need to capture. However, you must use the attached Excel worksheet to record the information mentioned in the table.

5.1.1 Migration planning worksheet

Table 5.1 Migration planning worksheet sample

Basic information	
Domain name	
Domain operation mode	
Authentication objects Record the information about each user account and the groups in which the accounts are added as members. Even though this information automatically migrates to the new server, as a best practice it is recommended to capture this information. After migration, you can use this information to check if the migration completed successfully.	
User accounts	*Groups*
Flexible Single Master Operation (FSMO) roles Record the details about the domain controllers which hold each of the FSMO roles in the current domain.	

FSMO role	*Current site and owner*	*Destination site and owner*
Schema master		
Domain naming master		
Domain Functional level		
Forests Functional level		
Infrastructure master		
Relative ID (RID) master		
PDC emulator		
Domain controller networking information For each domain controller that is being migrated, capture the following details which can be used for setting up the network connections during and after the migration.		
Subnet mask		
Domain controller 1 of type peer or RODC		
Domain controller name		
IP address		
Is a GC server (yes or no)		
Is a DNS server (yes or no)		
Preferred DNS		
Alternate DNS		
Path for AD database		
Path for log files		
Path for SYSVOL		

5.2 Inventorying the current domain controller configuration

- Installing Windows Support Tools on domain controller
- Identifying the domain controllers holding the FSMO roles
- Identifying GC servers configured in the domain
- Identifying DNS servers configured in the domain

- Identifying the domain operation mode

5.2.1 Installing Windows Support Tools on domain controller

The process of inventorying the current domain controller configuration utilizes several command line utilities provided by Microsoft known as Windows Support Tools. For systems installed with operating systems earlier than Windows Server 2008, the Windows Support Tools are not installed along with the operating system. You must install them separately from the Windows operating system CD of the version that is currently installed on the domain controller.

To install Windows Support Tools

1. Log on to the domain controller using a Windows account with local administrator rights.
2. Insert the Windows Server 2003 CD into the CD/DVD drive.
3. Browse the contents of the CD and navigate to the folder `\Support\Tools`.
4. Double-click **SupTools.msi**.
5. Follow the on-screen instructions to install Windows Support Tools.

5.2.2 Identifying the domain controllers holding the FSMO roles

To identify the domain controllers holding the FSMO roles

1. Open Command Prompt or Support Tools Command Prompt.
2. Type the following command and then press **ENTER**.

   ```
   netdom query /domain:%userdnsdomain% fsmo
   ```

   > **ATTENTION**
   > You can also use the domain name in place of `%userdnsdomain%`.

   The Command Prompt lists the FSMO roles available and the name of the domain controller that holds the respective FSMO role.
3. Record the information about the domain controllers and the FSMO roles they hold in the Migration planning table.

5.2.3 Identifying GC servers configured in the domain

If you have configured GC servers in your domain, before starting the migration you must identify the domain controllers that are hosting the GC server role. To identify the GC servers, you must perform this task on one of the domain controllers in the domain.

To identify the GC servers in a domain

1. Log on to the domain controller using an account with administrative privileges.
2. Perform one of the following:

Operating System	Steps
Windows 2000 Server	Click **Start** > **Programs** > **Administrative Tools** > **Active Directory Sites and Services**.
Windows Server 2003/2008	Click **Start** > **All Programs** > **Administrative Tools** > **Active Directory Sites and Services**.

   The **Active Directory Sites and Services** window appears.
3. In the console tree, expand **Sites** folder, and then expand the site object on which the servers reside.
4. Expand the **Servers** folder, and then expand the server name.

   The **NDTS Settings** items appear under the server name.
5. Right-click **NDTS Settings** item, and then click **Properties**.

   The **NDTS Settings Properties** dialog box appears.
6. Verify if the **Global Catalog** check box is selected. If not, select the **Global Catalog** check box, and then click **OK**.

   The **NDTS Settings Properties** dialog box closes.
7. Repeat steps 5 through 6 for each available server under the site object.
8. Record the details about the domain controllers configured as GC servers in the Migration planning table.

5.2.4 Identifying DNS servers configured in the domain

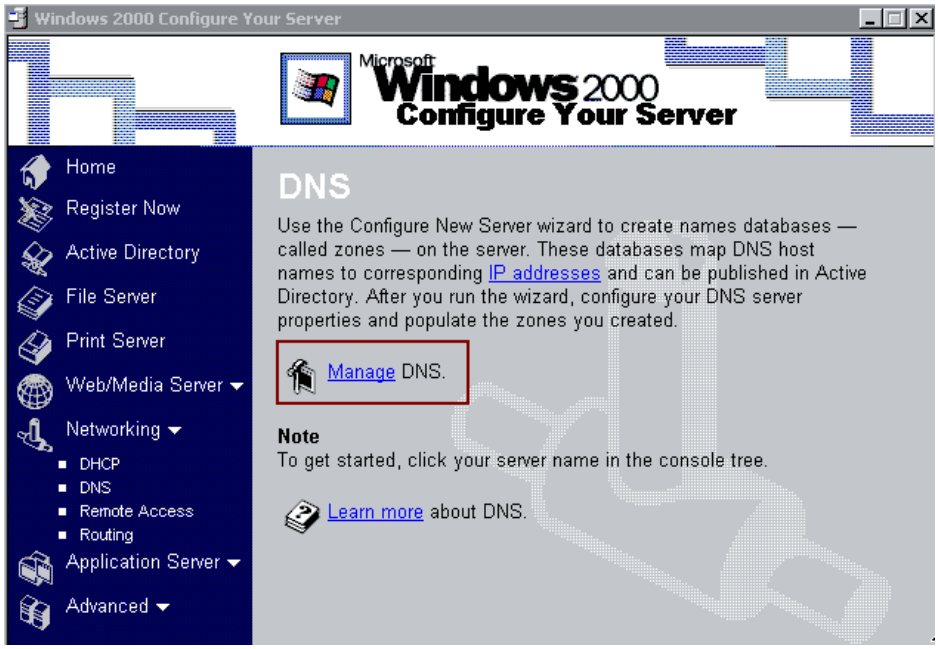
If you have configured DNS servers in your domain, before starting the migration you must identify the domain controllers that are hosting the DNS server role. To identify the DNS servers, you must perform this task on each domain controller in the domain.

To identify DNS servers on Windows 2000 Server domain controllers

1. Click **Start** > **Programs** > **Administrative Tools** > **Configure Your Server**.

   The **Microsoft Windows 2000 Configure Your Server** wizard appears.
2. On the left pane of the wizard, expand **Networking**, and then click **DNS**.

   If the domain controller is configured as a DNS server, the **DNS** page on the wizard displays **Manage DNS** (highlighted in the following image).



If the domain controller is not configured as DNS server, the DNS page displays **Set up DNS**.

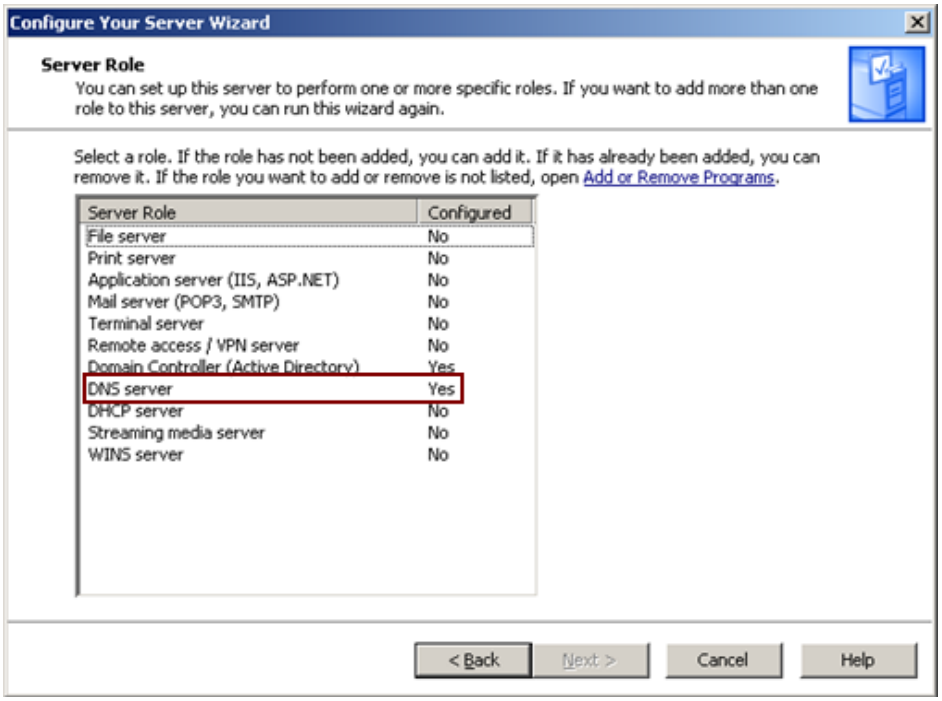
3. If the domain controller is configured as DNS server, record the name of the domain controller in the Migration planning table.
4. Close the **Microsoft Windows 2000 Configure Your Server** wizard.

To identify DNS servers on Windows Server 2003 domain controllers

1. Click **Start** > **All Programs** > **Administrative Tools** > **Configure Your Server**.
   The **Configure Your Server Wizard** appears.
2. On the **Welcome to the Configure Your Server Wizard** page of the wizard, click **Next**.
3. On the **Preliminary Steps** page, click **Next**.

4. On the **Server Role** page, examine the list of server roles to determine if the domain controller is configured as the DNS server.

   If a domain controller is configured as DNS server, **Configured** column entry corresponding to the **DNS server** entry displays **Yes**.



5. If the domain controller is configured as DNS server, record the name of the domain controller in the Migration planning table.
6. Close the **Configure Your Server Wizard**.

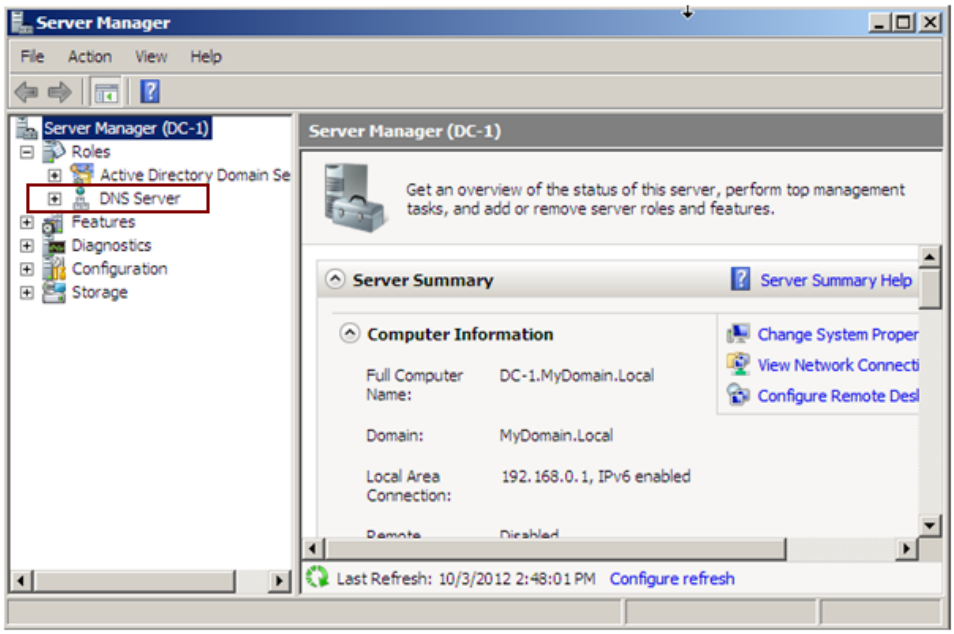
To identify DNS servers on Windows Server 2008 domain controllers

1. Click **Start** > **Administrative Tools** > **Server Manager**.

   The **Server Manager** window appears.
2. In the left pane, expand **Roles**.

   The roles currently configured for the domain controller are displayed.

3. To determine if a domain controller is configured as DNS server, in **Roles**, check if **DNS Server** item is available.



4. If the domain controller is configured as DNS server, record the name of the domain controller in the Migration planning table.
5. Close the **Server Manager** window.

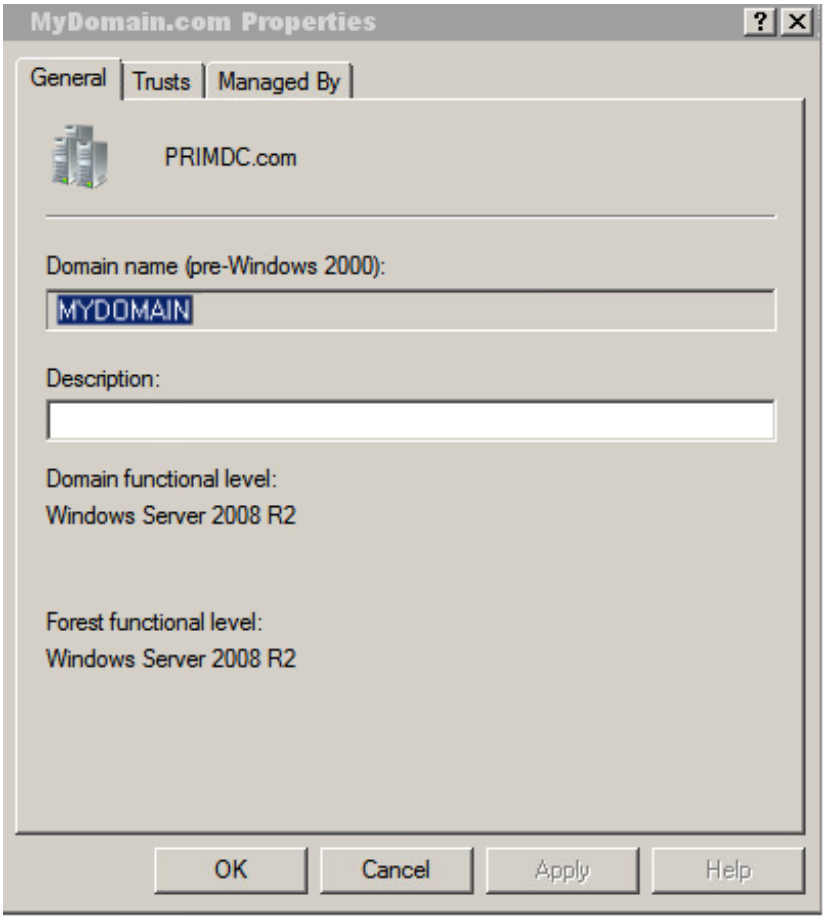
5.2.5 Identifying the domain operation mode

To identify the domain operation mode

1. Perform one of the following:

Operating System	Steps
Windows 2000 Server	Click **Start** > **Programs** > **Administrative Tools** > **Active Directory Domains and Trusts**.
Windows Server 2003/2008	Click **Start** > **All Programs** > **Administrative Tools** > **Active Directory Domains and Trusts**.

   The **Active Directory Domains and Trusts** window appears.
2. In the console tree, right-click the domain name, and then click **Properties**.
   The domain **Properties** dialog box appears.



The **Domain operation mode** box displays the operation mode currently configured for the domain controller.

3. Record the information about the current domain operation mode in the Migration planning worksheet.

5.3 Verifying domain controller readiness for migration

- Verifying domain health
- Ensuring availability of multiple domain controllers
- Ensuring availability of multiple DNS servers

5.3.1 Verifying domain health

Run the Network Diagnostics (NetDiag) utility

NetDiag is a command-line diagnostic utility that is used for diagnosing any network connectivity problems prior to starting the migration. NetDiag utility performs a series of tests to determine the state of the network. Running this utility helps to identify and isolate any network connectivity problems that might occur during migration. NetDiag utility is installed as part of the Windows 2000 Support Tools installation.

Prerequisites

- Adjust the screen buffer size of Command Prompt.

  The NetDiag utility test output displayed in Command Prompt can be enormous and hence it is recommended to adjust the screen buffer size of the Command Prompt. To adjust the screen buffer size,

1. Open Command Prompt, click the upper-left icon on the title bar, and then click **Properties**.
2. Click the **Layout** tab and set the following under **Screen Buffer Size** area.
   - In the **Width** box, type or select `200`.
   - In the **Height** box, type or select `3000`.
3. Click **OK**.

To run the Network Diagnostics (NetDiag) utility

1. At the Command Prompt, type **`NETDIAG`**, and then press **ENTER**.

   The **`NETDIAG`** output displays the details about the system, including the details about the hotfixes that are installed. After the system details, the output also displays the status of the tests that are performed by this utility. The following are the results that are displayed in the output.

   - **Passed** – indicates that the test is completed successfully
   - **Skipped** – indicates that the test is skipped as it is not relevant to the configuration
   - **Failed** – indicates that issues are reported

   Any test that failed or reported any errors should be analyzed before proceeding further.
2. If required, run the command **`DCDiag /fix`**, to resolve the issues which are reported.

Run the Domain Controller Diagnostics (DCDiag) utility

DCDiag is a command-line diagnostic utility that is used for analyzing the performance of one or all of the domain controllers in an Active Directory forest and identifies any problems to assist in troubleshooting. DCDiag consists of many tests that can be run individually or as part of a suite to verify the domain controller health. DCDiag utility is installed as part of the Windows 2000 Support Tools installation.

To run the DCDiag utility

1. Open Command Prompt, type **`DCDIAG`** and then press **ENTER**.

   The **`DCDIAG`** utility displays a summary of the test results, for each domain controller tested. It also reports any issues encountered.
2. If required, run the command **`DCDiag /fix`**, to resolve the issues which are reported.

> **ATTENTION**
>
> For further information about the DCDiag utility or if you have any setup problem while executing the DCDiag utility, contact your nearest Honeywell TAC representative.

5.3.2 Ensuring availability of multiple domain controllers

As a best practice, it is recommended to have at least two domain controllers in a domain, which operate as peers to each other in providing the Active Directory information. An advantage of having multiple domain controllers in a domain is that, the domain controllers can be migrated with minimal impact to the domain members. When migrating one of the domain controllers in a domain, you can transfer the functions that it provides to a peer domain controller to prevent disruption of operations during migration.

In a domain consisting of only a single domain controller, you must add a temporary peer domain controller to enable the migration. The temporary peer should be configured with a unique name and IP address, so that it does not conflict with the name or IP address of the domain controller being migrated. In addition, while setting up a temporary peer, you should also configure it as a GC server and a DNS server.

The server operating system for the temporary peer can either be the same version installed on the current domain controllers in the domain or can be installed with the latest supported operating system.

> ATTENTION
>
> If the temporary peer domain controller is installed with the latest version of the Windows Server operating system, to promote it to a domain controller you must prepare the schema of the temporary peer domain controller by running the **adprep** utility.

After completing the migration of the original domain controller, if you do not want to migrate the temporary peer domain controller and retain it in the domain, demote the temporary peer domain controller and then remove it from the domain. However, since the best practice is to always have a minimum of two domain controllers in a domain, it is recommended to install the temporary peer domain controller with and retain it in the domain even after migrating the original domain controller.

5.3.3 Ensuring availability of multiple DNS servers

> ATTENTION
>
> You can ensure the availability of multiple DNS server only if you have multiple domain controllers.

Before starting the migration of domain controllers, it is important to ensure that there are multiple DNS servers configured in the domain. You can configure one or more of the domain controllers in the domain as the DNS servers. If there is only one domain controller configured as the DNS server, you must configure one of the peer domain controllers in the domain as the alternate DNS server.

For more information about configuring DNS server role in a peer domain controller, refer to the section Configuring the peer domain controller as DNS server.

In addition, ensure that the IP address for the DNS servers, configured on the domain controllers in the domain are accurate.

5.4 Preparing the Active Directory

- Verifying if Service Pack 4 is installed on a Microsoft Windows 2000 Server domain controller
- Raising the functional level of the domain
- Expanding the Active Directory schema

5.4.1 Verifying if Service Pack 4 is installed on a Microsoft Windows 2000 Server domain controller

> **ATTENTION**
>
> Skip this section if your domain controller is not running on Microsoft Windows 2000 Server operating system.

If the domain controller that is being migrated is based on the Microsoft Windows 2000 Server operating system, it must have Service Pack 4 (SP4) installed prior to starting the migration. The following procedure describes the steps to be performed for verifying the service pack version installed on a Microsoft Windows 2000 Server system.

To verify the service pack version installed on a Microsoft Windows 2000 Server domain controller

1. Click **Start** > **Run**.
2. Type **`winver`**, and then press **Enter**.

   The **About Windows** dialog box appears.
3. In the version details, verify the service pack version installed.

   If the version details display SP4, the domain controller is already installed with SP4. If the version details display any other service pack version number, install SP4 using the following procedure.

To install SP4 on a Microsoft Windows 2000 Server domain controller

1. Download Microsoft Windows 2000 Server SP4 from the following Microsoft website link: http://www.microsoft.com/en-us/download/confirmation.aspx?id=4127.

   If the Microsoft download link is unavailable, you can obtain the download file from `Win2k_SP4` folder at the root of the Experion R210 Application Media.

   The **File Download - Security Warning** dialog box appears. Ensure that the file name appears as **W2KSP4_EN.EXE**.
2. To save the executable file on to the local disk drive, click **Save**.
3. Browse to the location where the executable file is saved, double-click **W2KSP4_EN.EXE**, and then click **Run**.

   The files that need to run on the system are extracted and the **Welcome to the Windows 2000 Service Pack 4 Setup Wizard** appears.
4. Click **Next**.

   The **License Agreement** page appears.
5. Review the license agreement, click **I Agree**, and then click **Next**.

   The **Select Options** page appears.
6. Select the desired archiving option.

   If you want to remove the service pack later without restoring the backup image, click **Archive Files**.
7. If you have selected **Archive Files**, under **Uninstall Folder**, click **Browse**.
8. Browse to a location to save the archive files, and then click **Next**.

   The **Updating Your System** page appears. The status and the progress of installation is displayed on the **Updating Your System** page.

9. After the installation is complete, click **Finish**.

   The computer restarts.

10. Repeat the steps on all the Microsoft Windows 2000 Server domain controllers in the domain.

5.4.2 Raising the functional level of the domain

Prior to starting the migration, the domain functional level must be set to the native level or to the highest level supported by the server operating system version installed on the existing domain controllers in the domain. Raising the domain functional level enables the utilization of most of the Active Directory Domain Services (AD DS) features.

Use the following table as a reference to set the domain functional level of the domain.

Current operating system	Recommended domain functional level
Microsoft Windows 2000 Server	Windows 2000 native
Microsoft Windows Server 2003	Windows Server 2003
Microsoft Windows Server 2008	Windows Server 2008
Microsoft Windows Server 2008 R2	Microsoft Windows Server 2008 R2

If the current domain operation mode determined during the domain inventorying task (as described in the section Identifying the domain operation mode) and recorded on the Migration planning table is not at the required level, use the following procedure to raise the domain functional level.

To raise the functional level of the domain

1. Log on to the domain controller.
2. Perform one of the following:

Operating System	Steps
Windows 2000 Server	Click **Start** > **Programs** > **Administrative Tools** > **Active Directory Domains and Trusts**.
Windows Server 2003/2008	Click **Start** > **All Programs** > **Administrative Tools** > **Active Directory Domains and Trusts**.

   The **Active Directory Domains and Trusts** window appears.

3. In the console tree, right-click the domain name, and then click **Raise Domain Functional Level**.

   The **Raise Domain Functional Level** dialog box appears. The dialog box displays the current domain functional level and provides a list of available domain functional levels.

> **ATTENTION**
>
> If the domain functional level is already at the appropriate level, a dialog box appears indicating that it is already set to the highest level. Close the dialog box and then close the **Active Directory Domains and Trusts** window. Skip the rest of the steps in this procedure and proceed to next task in migration Expanding the Active Directory schema.

4. In the **Select an available domain functional level** list, click the required functional level, and then click **Raise**.

   A warning message appears indicating that changing the domain functional level affects the entire domain and that this action cannot be reversed.

5. Click **OK** to close the dialog box.

   When the domain functional level is raised, a confirmation message appears indicating that the level is raised and that the new level replicates to each domain controller in the domain.

6. Click **OK** to close the confirmation dialog box.
7. Close the **Active Directory Domains and Trusts** window.

> **ATTENTION**
>
> While attempting to raise the functional level of the domain, if the Active Directory is busy, there are chances for the raise operation to fail. In such case, you must repeat this procedure till you succeed to raise the functional level of domain.

5.4.3 Expanding the Active Directory schema

To prepare an existing Microsoft Windows 2000 Server,Microsoft Windows Server 2003, Microsoft Windows Server 2003 (64-bit) or Microsoft Windows Server 2008, Microsoft Windows Server 2008 R2 Standard domain controller for a migration, you must run the **Adprep** utility on the domain controllers that are being migrated. The **Adprep** utility is available on the installation disk of each version of Windows server operating system. However, you must use the **Adprep** utility available with the Windows server operating system to which the domain controllers are migrated. On the CD, the utility is available in the `\support\adprep` folder.

Prerequisites

To run the **Adprep** utility on a domain controller running Microsoft Windows 2000 Server, the domain controller must be installed with Microsoft Windows 2000 Server SP4 or later.

To expand the AD schema

1. Log on to the domain controller which is holding the schema master role.

> **ATTENTION**
>
> Refer to the Migration Planning Worksheet in section Recording the current domain controller configuration information.

2. Insert the CD into the CD/DVD drive.

   If a message appears indicating that the installation disk is not compatible with the Windows version installed on your computer, ignore the message and click **OK** to proceed.

3. Open Command Prompt, type the command **<CD/DVD drive letter>:**, and then press **ENTER**.
4. Perform one of the following:If the domain controller is a 64-bit computer, type **adprep.exe /forestprep**, and then press **ENTER**.
   - If the domain controller is a 64-bit computer, type **adprep.exe /forestprep**, and then press **ENTER**.
   - If the domain controller is a 32-bit computer, type **adprep32.exe /forestprep**, and then press **ENTER**.

   A warning message appears prompting you to confirm if all the Microsoft Windows 2000 Server Active Directory domain controllers in the forest are upgraded to Microsoft Windows 2000 Server SP4 or later.

5. Perform one of the following steps.
   - If all the existing Microsoft Windows 2000 Server Active Directory domain controllers meet this requirement, type **C**, and then press **ENTER**.
   - Else, type any other key, and then press **ENTER** to exit. You must upgrade all the Microsoft Windows 2000 Server domain controllers in the domain to Microsoft Windows 2000 Server SP4 or later, and then repeat the steps in this procedure.

   The schema upgrade starts and the Command Prompt console displays the status of the upgrade. When complete, the console displays the message that **Adprep** successfully updated the forest-wide information.

6. Perform one of the following:If the domain controller is a 64-bit computer, type **adprep.exe /domainprep**, and then press **ENTER**.
   - If the domain controller is a 64-bit computer, type **adprep.exe /domainprep**, and then press **ENTER**.
   - If the domain controller is a 32-bit computer, type **adprep32.exe /domainprep**, and then press **ENTER**.

   When the command completes, the console displays the message that **Adprep** successfully updated the domain-wide information.

7. Perform one of the following:If the domain controller is a 64-bit computer, type **adprep.exe /domainprep /gpprep**, and then press **ENTER**.
   - If the domain controller is a 64-bit computer, type **adprep.exe /domainprep /gpprep**, and then press **ENTER**.
   - If the domain controller is a 32-bit computer, type **adprep32.exe /domainprep /gpprep**, and then press **ENTER**.

   When the command completes, the console displays the message that **Adprep** successfully updated the Group Policy Object (GPO) information.

8. If you are planning to add an RODC to the domain, run the following command.
   - If the domain controller is a 64-bit computer, type **adprep /rodcprep**, and then press **ENTER**.
   - If the domain controller is a 32-bit computer, type **adprep32.exe /rodcprep**, and then press **ENTER**.

   When the command completes, the console displays the message that **Adprep** completed without errors and all the partitions are updated.

9. Close the Command Prompt window.

CHAPTER

6

WINDOWS 2000 SERVER/WINDOWS SERVER 2003/2008 TO MIGRATION

- Migrating a domain containing multiple domain controllers checklist
- Configuring the peer domain controller as DNS server
- Verifying the domain controller name is listed in the DNS list.
- Configuring alternate DNS for all the nodes in the domain
- Transferring FSMO roles to a peer domain controller
- Demoting a domain controller
- Restoring the FSMO roles
- Raising the functional level of the domain

6.1 Migrating a domain containing multiple domain controllers checklist

This topic provides a checklist that describes the tasks to be performed for migrating a domain containing multiple domain controllers. The checklist serves as a ready reference to review the progress of migration as you move from one phase of your migration to another. The sections following the checklist provide the details about each task in detail.

Ensure that you perform the migration tasks in the sequence in which the tasks are listed in the checklist.

6.1.1 Prerequisites

- Ensure that you have completed all the required migration preparation tasks mentioned in the Preparing the domain for migration.
- Ensure to install and configure the FTE before setting up a domain controller. For instruction about installing and configuring FTE, refer to the latest *Fault Tolerant Ethernet Installation and Service Guide* on the http://www.honeywellprocess.com website.

You must install a new domain controller domain hosted by a single controller for migrating a domain hosted by a single controller.

Refer to the following table for installing a new server as a domain controller.

Steps	Task	Go to	Done?
1	Prepare a system.	Installing Microsoft Windows Server 2008 R2 Operating System	

Steps	Task	Go to	Done?
2	Install a temporary peer domain controller.	Setting up a peer domain controller	
3	Configure DNS server role in the temporary peer domain controller.	Configuring the peer domain controller as DNS server	
4	Configure the temporary peer domain controller as the alternate DNS for all the nodes in the domain.	Configuring alternate DNS for all the nodes in the domain	
5	Transfer the FSMO roles to the temporary peer domain controller.	Transferring FSMO roles to a peer domain controller	
6	Demote the original domain controller.	Demoting a domain controller	
7	Remove the original domain controller from the domain and shutdown the system.		

Refer to the following table for migrating a domain hosted by a single controller. The following table describes the tasks to recreate a new domain controller using existing hardware (server).

Steps	Task	Go to	Done?
1	Do one of the following: • If you are planning to migrate and use the Windows Server which was used as the domain controller in the domain, install Microsoft Windows Server 2008 R2 operating system on the system. • If you are planning to add a new system as the domain controller, ensure the new system is installed with Microsoft Windows Server 2008 R2 operating system. In both the above scenarios, the IP address and the name of the system must be the same as the name and IP address of the original domain controller.	Preparing a Windows domain controller	
2	Add the Microsoft Windows Server 2008 R2 server to a Windows domain.	Adding Microsoft Windows Server 2008 R2 to a Windows domain	
3	Installing the Microsoft Windows Server 2008 R2 server as a domain controller	Installing the Microsoft Windows Server 2008 R2 server as a domain	

Steps	Task	Go to	Done?
		controller	
4	Configure the Microsoft Windows Server 2008 R2 domain controller as the alternate DNS for all the nodes in the domain.	Setting the DNS server IP address	
5	Restore the FSMO roles.	Restoring the FSMO roles	
6	Demote the temporary peer domain controller.	Demoting a domain controller	
7	Raise the functional level of the domain.	Raising the functional level of the domain	

6.1.2 Migrating a domain containing multiple domain controllers checklist

Steps	Task	Go to	Done?
1	Configure DNS server role in one of the peer domain controllers in the domain.	Configuring the peer domain controller as DNS server	
2	Verify that the nodes on the network that are being serviced by the domain controller that will be upgraded have at least one working DC that is listed in its DNS settings.	Verifying the domain controller name is listed in the DNS list.	
3	Configure the peer domain controller as the alternate DNS for all the nodes in the domain.	Configuring alternate DNS for all the nodes in the domain	
4	As you are migrating an entire domain to Microsoft Windows Server 2008 R2 the FSMO roles will be present on at least one DC. Hence, you must transfer the FSMO roles to the peer domain controller.	Transferring FSMO roles to a peer domain controller	
5	Demote the original domain controller.	Demoting a domain controller	
6	Remove the original domain controller from the domain and shutdown the system.		
7	Perform one of the following steps: • If you are planning to migrate and use the original domain controller in the domain, install	Preparing a Windows domain controller	

Steps	Task	Go to	Done?
	Microsoft Windows Server 2008 R2 operating system on the domain controller. • If you are planning to add a new system as the domain controller, ensure the new system is installed with Microsoft Windows Server 2008 R2 operating system. In both the above scenarios, the IP address and the name of the system must be the same as the name and IP address of the original domain controller.		
8	Add the Microsoft Windows Server 2008 R2 server to a Windows domain.	Adding Microsoft Windows Server 2008 R2 to a Windows domain	
9	Promote the Microsoft Windows Server 2008 R2 server to the role of a domain controller.	Promoting the server to the role of a domain controller	
10	Configure the Microsoft Windows Server 2008 R2 domain controller as the alternate DNS for all the nodes in the domain.	Setting the DNS server IP address	
11	Restore the FSMO roles.	Restoring the FSMO roles	
12	Repeat all the above steps to migrate the other domain controllers in the domain, as required.		
13	Raise the functional level of the domain.	Raising the functional level of the domain	

6.2 Configuring the peer domain controller as DNS server

This section describes the tasks that you must perform to configure an alternate DNS server in a domain. If a domain consist of only a single domain controller and if that domain controller hosts the DNS server service, migrating the domain controller causes disruption to the DNS services in the domain. To prevent any disruption due to the unavailability of a DNS server, you must add a peer domain controller and configure it as the alternate DNS server.

In a domain consisting of multiple domain controllers, you can configure one of the peer domain controllers as the alternate DNS for all the nodes in the domain.

To configure a peer domain controller as the DNS server, you must perform the following tasks on the peer domain controller:

- Add DNS server role
- Add reverse lookup zone

- Add DNS server role in the peer domain controller

6.2.1 Add DNS server role in the peer domain controller

Prerequisites

Ensure that you have inserted the installation CD of the respective operating system in the CD/DVD drives of the domain controller on which you plan to add the DNS server role.

On Microsoft Windows 2000 Server domain controllers

1. Click **Start** > **Programs** > **Administrative Tools** > **Configure Your Server**.

   The **Microsoft Windows 2000 Configure Your Server** wizard appears.
2. On the left pane of the wizard, expand **Networking**, and then click **DNS**.
3. On the right pane of the wizard, click **Set up DNS**

   The **Windows Server Setup - Installing DNS Server** dialog box appears displaying the status of the configuration of DNS server components.

   If a dialog box appears indicating that there would be a delay in starting some of the services, click **OK** to close the dialog box.
4. After the installation is complete, click **Next**.

   The **Windows Server Setup - Installing DNS Server** dialog box closes. The DNS server role is now added in the peer domain controller and the right pane of the **Microsoft Windows 2000 Configure Your Server** wizard displays **Manage DNS**.
5. Close the **Microsoft Windows 2000 Configure Your Server** wizard.

On Microsoft Windows Server 2003 domain controllers

1. Click **Start** > **All Programs** > **Administrative Tools** > **Configure Your Server**.

   The **Configure Your Server Wizard** appears.
2. On the **Welcome to the Configure Your Server Wizard** page of the wizard, click **Next**.
3. On the **Preliminary Steps** page, click **Next**.
4. On the **Server Role** page, click **DNS server**, and click **Next**.
5. On the **Summary of Selections** page, review the configuration options available, and click **Next**.

   The following are the configuration options that must be available while adding the DNS server role.

   - **Install DNS server**
   - **Run the Configure a DNS Server Wizard to configure DNS**

   If the options mentioned are not available, click **Back** to return to the **Server Role** page and repeat step Adding_DNS_Server_roles_to_the_peer_domain_controller.dita#Adding_DNS_Server_roles_to_the_peer_domain_controller/Server_role_click_DNS.

   The files that are required to add the DNS server role are accessed from the Microsoft Windows Server 2003 CD.

> **ATTENTION**
>
> If a dialog box appears reporting that the `dnsmgmt.ms_` file could not be located, click **Browse** and navigate to the **I386** folder on the CD and open the file, and then click **OK**.

The **Configure a DNS Server Wizard** appears.

6. On the **Welcome to the Configure a DNS Server Wizard** page, click **Next**.
7. On the **Select Configuration Action** page, click **Configure root hints only**, and then click **Next**.

   The **Searching for Root Hints** dialog box appears indicating that the system is searching for root hints and the dialog box closes automatically.
8. On the **Completing the Configure a DNS server Wizard** page, click **Finish**.

   A dialog box appears indicating that Root Hints could not be configured. Ignore the message and close the dialog box as no further action is required. Root Hints information is automatically copied from the Active Directory information maintained by the current DNS server on the domain.
9. On the **This Server is Now a DNS Server** page, click **Finish**.

   The DNS server role is added in the peer domain controller.

On Microsoft Windows Server 2008 domain controllers

1. Click **Start** > **Administrative Tools** > **Server Manager**.

   The **Server Manager** window appears.
2. In the right pane, under **Roles Summary**, click **Add Roles**.

   The **Add Roles Wizard** appears.
3. Click **Next**.

   The **Select Server Roles** page appears.
4. Select **DNS Server**, and then click **Next**.

   The **DNS Server** page appears.
5. Read the information available on this page, and then click **Next**.

   The **Confirm Installation Selections** page appears.
6. Read the information available on this page, and then click **Install**.

   The installation begins and the wizard displays the progress of installation. After the installation is complete, the **Installation Results** page appears displaying an installation succeeded message.
7. Click **Close**.

   The **Add Roles Wizard** closes.

On Microsoft Windows Server 2008 R2 domain controllers

Next steps

1. Refer to the section Adding reverse lookup zone and perform the tasks for adding reverse lookup zone.
2. Go to the checklist Migrating a domain containing multiple domain controllers checklist and continue with the next task listed in the checklist.

6.3 Verifying the domain controller name is listed in the DNS list.

Use this procedure to verify that the nodes on the network that are being serviced by the domain controller that will be upgraded have at least one working domain controller listed in their DNS settings. This server lists the DNS servers in a domain.

6.3.1 Prerequisites

6.3.2 To verify the active domain controller in a domain

1. On your DNS, click **Start**, and then click **Run**.

   The **Run** dialog box appears.
2. Type **cmd**.

   The **Command** dialog box appears.
3. Type **nslookup**, and then press **ENTER**.
4. Type **set type=all**, and then press **ENTER**.
5. Type **_ldap._tcp.dc._msdcs.Domain_Name**, where Domain_Name is the name of your domain, and then press **ENTER**.

   A list of domain controllers with accounts in the domain are listed. Ensure that the peer domain controller name is listed.

6.3.3 Next steps

Go to the checklist Migrating a domain containing multiple domain controllers checklist and continue with the next task listed in the checklist.

6.4 Configuring alternate DNS for all the nodes in the domain

After configuring the peer domain controller as the alternate DNS server, you must manually update all the other nodes in the domain to include the address of the new DNS server. This prevents any disruption to the network services in the domain during migration.

6.4.1 To configure alternate DNS for all the nodes in the domain

1. Open Control Panel.
2. Perform one of the following:

Operating System	Steps
Windows 2000 Server	• Open **Network and Dial-up Connections**. The **Network and Dial-up Connections** window appears.
Windows Server 2003	• In the **Control Panel Classic view**, open **Network Connections**. The **Network Connections** window appears.
Windows Server 2008	a. In the **Control Panel Classic view**, open **Network and Sharing Center**. b. In the **Tasks** area, click **Manage Network Connections**. The **Network Connections** window appears.

3. Right-click **Local Area Connection**, and then click **Properties**.
   The **Local Area Connection Properties** dialog box appears.
4. Click **Internet Protocol (TCP/IP)**, and then click **Properties**.
   The **Internet Protocols (TCP/IP) Properties** dialog box appears.
5. Click **Use the following DNS server addresses**.
6. In the **Alternate DNS server** box, type the IP address of the alternate DNS server, and then click **OK**.
   If the system is a Domain Controller hosting DNS, then first DNS must display a different ip address of a DNS server. However, the second DNS ip address must be 127.0.0.1.
7. Click **OK**.
   The **Local Area Connection Properties** dialog box closes.

6.4.2 Next steps

Go to the checklist Migrating a domain containing multiple domain controllers checklist and continue with the next task listed in the checklist.

6.5 Transferring FSMO roles to a peer domain controller

This section describes how to transfer the FSMO roles from a domain controller to a peer domain controller. The steps in this section describes transferring the FSMO roles by logging onto the domain controller which is currently hosting the roles, and then transferring (pushing) them to the domain controller identified to host the roles. However, you can also transfer the roles by logging onto the domain controller which is identified to host the roles, and then transferring (pulling) them from the domain controller that is currently hosting the roles.

You can transfer FSMO roles by using the following Active Directory snap-in tools in Microsoft Management Console (MMC).

- Active Directory Schema snap-in
- Active Directory Domains and Trusts snap-in
- Active Directory Users and Computers snap-in

If the domain controller does not host any of the FSMO roles, skip this section and proceed to the section Demoting a domain controller.

- Transferring/Restoring the schema master role
- Transferring/Restoring domain naming master role
- Transferring/Restoring RID Master, PDC Emulator, and Infrastructure Master roles
- Verifying the transferred FSMO roles

6.5.1 Transferring/Restoring the schema master role

This section describes the tasks that must be performed to transfer/restore the schema master role to the domain controller. The schema master role is transfer/restore using the MMC snap-in tool, **Active Directory Schema Master snap-in**. To use the **Active Directory Schema Master snap-in**, you must register the `Schmmgmt.dll` file.

To register Schmmgmt.dll

1. Click **Start** > **Run**.

   The **Run** dialog box appears.

   Or

   Open **Command Prompt** with **Administrator rights**.
2. Type **`regsvr32 schmmgmt.dll`**, and then click **OK**.

   The command executes and a confirmation message appears indicating that the registration of `Schmmgmt.dll` succeeded.
3. Click **OK**.

   The confirmation dialog box closes.

To transfer/restore the schema master role

1. Click **Start** > **Run**, type **mmc**, and then click **OK**.

   The MMC **Console Root** window appears.
2. On the **File** menu, click **Add/Remove Snap-in**.

   The **Add or Remove Snap-ins** dialog box appears.
3. In the list of available snap-ins, click **Active Directory Schema** and click **Add**.

   The Active Directory Schema snap-in appears in the **Selected snap-ins** box.
4. Click **OK**.

   The **Add or Remove Snap-ins** dialog box closes and the **Active Directory Schema** appears under **Console Root** item in the MMC **Console Root** window.
5. In the left pane of the MMC **Console Root** window, right-click **Active Directory Schema**, and then click **Change Active Directory Domain Controller**.

   The **Change Directory Server** dialog box appears.
6. Under **Change to**, click the **This domain Controller or AD LDS instance** option button.

7. In the list of domain controllers, click the name of the domain controller to which you have to transfer the schema master role, and then click **OK**.
8. If a message appears indicating that the Active Directory Schema snap-in is not connected to the operations master, click **OK** to close the message box.
9. In the left pane of the **Console Root** window, right-click **Active Directory Schema**, and then click **Operations Master**.

   The **Change Schema Master** dialog box appears. The name of the domain controller that currently hosts the schema master role and the name of the target domain controller where the schema role would be transferred are displayed in the dialog box.
10. Click **Change**.

    A confirmation message appears.
11. Click **Yes** to confirm the action.

    A message appears indicating that the Operations Master role is successfully transferred.
12. Click **OK** to close the dialog box.
13. Close the **Change Schema Master** dialog box and the MMC window.

6.5.2 Transferring/Restoring domain naming master role

This section describes the tasks that you must perform to transfer/restore the domain naming master role to the migrated domain controller.

To transfer/restore domain naming master role

1. Click **Start** > **All Programs** > **Administrative Tools** > **Active Directory Domains and Trusts**.

   The **Active Directory Domains and Trusts** window opens.
2. In the console tree, right-click **Active Directory Domains and Trusts** and click **Change Active Directory Domain Controller**.

   The **Change Domain Controller** dialog box appears.
3. In the list of available domain controllers, click the name of the domain controller to which you want to transfer the domain naming master role and click **OK**.
4. In the console tree, right-click **Active Directory Domains and Trusts**, and then click **Operations Master**.

   The **Operations Master** dialog box appears.

   The **Domain naming operations master** box displays the name of the domain controller that currently hosts the domain naming master role. The name of the target domain controller to which the domain naming master role would be transferred is displayed in the second box.
5. Click **Change**.

   A confirmation message appears.
6. Click **Yes** to confirm the action.

   A message appears indicating that the operations master role is successfully transferred.
7. Click **OK**.
8. Close the **Operations Master** dialog box and the **Active Directory Domains and Trusts** window.

6.5.3 Transferring/Restoring RID Master, PDC Emulator, and Infrastructure Master roles

This section describes the tasks that must be performed to transfer/restore the RID Master, PDC Emulator, and Infrastructure Master roles to the migrated domain controller.

To transfer/restore RID Master, PDC Emulator, and Infrastructure Master roles

1. Click **Start** > **Programs** > **Administrative Tools** > **Active Directory Users and Computers**.

   The **Active Directory Users and Computers** window opens.
2. In the left pane of the **Console Root** window, right-click **Active Directory Users and Computers**, and then click **Change Domain Controller**.

   The **Change Domain Controller** dialog box appears.
3. Under **Change to**, click the **This domain Controller or AD LDS instance** option button.
4. In the list of domain controllers, click the name of the domain controller to which you want to transfer/restore the schema master role, and then click **OK**.

   The **Change Domain Controller** dialog box closes.
5. In the console tree, right-click **Active Directory Users and Computers**, and then click **All Tasks** > **Operations Master**.

   The **Operations Masters** dialog box appears.

   The **Operations Masters** dialog box consists of three tabs, where each tab represents a role that the domain controller supports.
6. Click the tab that represents the role that you want to transfer to another domain controller, as required.

   In each of the tabs, the **Operations master** box displays the name of the domain controller that currently hosts the role that you want to change. The name of the target domain controller to which the selected role would be transferred is displayed in the second box.
7. Click **Change**.

   A confirmation dialog box appears.
8. Click **Yes** to confirm the action.

   A message appears indicating that the operations master role is successfully transferred.
9. Click **OK** to acknowledge the message.
10. If required, repeat steps to transfer the other roles available, as appropriate.
11. After transferring all the roles, click **OK**.

    The **Operations Master** dialog box closes.
12. Close all the open dialog boxes.
13. Restart the computer for the changes to appear.

6.5.4 Verifying the transferred FSMO roles

To verify if the mastership changes for the transferred FSMO roles are complete, open **Command Prompt** and run the command **netdom query /domain:%USERDNSDOMAIN% fsmo**. The command queries the domain for the current FSMO role holders and lists the domain controllers that hosts each of the FSMO roles. Ensure that the name of the domain controller to which the FSMO roles are transferred and the roles that it hosts are available in the list.

6.6 Demoting a domain controller

After transferring the FSMO roles from the domain controller, you must demote the domain controller to a stand-alone server. This operation should be performed online so that the Active Directory information on the peer domain controller is accurate.

6.6.1 Prerequisites

Ensure to disable the firewall before demoting a domain controller.

6.6.2 To demote a domain controller on Windows Server 2003, Windows Server 2008 and Windows Server 2008 R2

1. Log on to the domain controller using a Windows account with local administrator rights.
2. Click **Start** > **Run**.

   The **Run** dialog box appears.
3. Type `dcpromo` and press **ENTER**.

   The **Active Directory Installation Wizard** appears.
4. Click **Next**.

   ATTENTION

   a. If the primary domain controller is set up as the GC server, a message appears indicating that the current domain controller is a GC server and that before removing this system from the domain, another domain controller must already be configured as the alternate GC. As this consideration is already addressed in the Preparing the domain for migration section, ignore the message and click **OK** to proceed.

   b. Click **Next** even, If **You want to Delete the Domain** message appears with **if the Server is the last in the domain** Checkbox option.

      i. After **Delete the Domain**, you are prompted for the **Administrator Password**. Enter the **Administrator Password** and click **Next**

      The **Summary Page** appears.

      ii. Click **Next** to **Remove Active Directory Domain Services from this computer**.

   The **Remove Active Directory** page appears.
5. Click **Next** and follow the on-screen instructions to complete the wizard.

   When complete, the wizard displays a message indicating that the Active Directory is removed from the domain.

   ATTENTION

   If the system reports an error indicating that the action did not complete successfully, ensure that the peer domain controller is running on the domain. Wait for several minutes and then repeat the steps.
6. Click **Finish** and then restart the computer.

   If you are not upgrading the demoted computer to the latest operating system, ensure that you turn off the computer and remove it from the network.

6.6.3 Next steps

Go to the checklist Migrating a domain containing multiple domain controllers checklist and continue with the next task listed in the checklist.

6.7 Restoring the FSMO roles

After promoting the server to a domain controller, you need to restore the transferred FSMO roles from the peer or temporary domain controller to the domain controller.

Refer to the section Transferring FSMO roles to a peer domain controller and perform the steps describe in it to restore the FSMO roles to the domain controller. If the original domain controller did not host any of the FSMO roles, no further action is required. You can proceed with the migration of the other domain controllers in the domain, if any.

- Verifying the restored FSMO roles

6.7.1 Verifying the restored FSMO roles

To verify if the mastership changes for the restored FSMO roles are complete, open **Command Prompt** and run the command **netdom query /domain:%USERDNSDOMAIN% fsmo**. The command queries the domain for the current FSMO role holders and lists the domain controllers that hosts each of the FSMO roles. Ensure that the name of the migrated domain controller and the restored roles that it hosts are available in the list.

Go to the checklist Migrating a domain containing multiple domain controllers checklist and continue with the next task listed in the checklist.

6.8 Raising the functional level of the domain

After migrating all the domain controllers to Microsoft Windows Server 2008 R2, you must raise the functional level of the domain to Microsoft Windows Server 2008 R2.

6.8.1 Prerequisites

To raise the domain functional level,

- You must be a member of the Domain Admins group or Enterprise Admins group, or must be delegated with appropriate authority.
- All the domain controllers in the domain must be migrated to Microsoft Windows Server 2008 R2.

6.8.2 To raise the functional level of the domain

1. Click **Start** > **All Programs** > **Administrative Tools**, right-click **Active Directory Domains and Trusts**, and then click **Run as administrator**.
2. In the console tree, right-click the domain name, and then click **Raise Domain Functional Level**.

   The **Raise Domain Functional Level** dialog box appears. The dialog box displays the current domain functional level and provides a list of available domain functional levels.

3. In **Select an available domain functional level** list, select Microsoft Windows Server 2008 R2, and then click **Raise**.

   A warning message appears indicating that changing the domain functional level affects the entire domain and that this action cannot be reversed.

4. Click **OK** to close the dialog box.

   When the domain functional level is raised, a confirmation message appears indicating that the level is raised and that the new level replicates to each domain controller in the domain.

5. Click **OK** to close the confirmation dialog box.
6. Close the **Active Directory Domains and Trusts** window.

> **ATTENTION**
>
> While attempting to raise the functional level of the domain, if the Active Directory is busy, there are chances for the raise operation to fail. In such case, you must repeat this procedure till you succeed to raise the functional level of domain.

Notices

Trademarks

Experion®, PlantScape®, SafeBrowse®, TotalPlant®, and TDC 3000® are registered trademarks of Honeywell International, Inc.

ControlEdge™ is a trademark of Honeywell International, Inc.

OneWireless™ is a trademark of Honeywell International, Inc.

Matrikon® and MatrikonOPC™ are trademarks of Matrikon International. Matrikon International is a business unit of Honeywell International, Inc.

Movilizer® is a registered trademark of Movilizer GmbH. Movilizer GmbH is a business unit of Honeywell International, Inc.

Other trademarks

Microsoft and SQL Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Trademarks that appear in this document are used only to the benefit of the trademark owner, with no intention of trademark infringement.

Third-party licenses

This product may contain or be derived from materials, including software, of third parties. The third party materials may be subject to licenses, notices, restrictions and obligations imposed by the licensor. The licenses, notices, restrictions and obligations, if any, may be found in the materials accompanying the product, in the documents or files accompanying such third party materials, in a file named third_party_licenses on the media containing the product, or at http://www.honeywell.com/ps/thirdpartylicenses.

Documentation feedback

You can find the most up-to-date documents on the Honeywell Process Solutions support website at: http://www.honeywellprocess.com/support

If you have comments about Honeywell Process Solutions documentation, send your feedback to: hpsdocs@honeywell.com

Use this email address to provide feedback, or to report errors and omissions in the documentation. For immediate help with a technical problem, contact your local Honeywell Process Solutions Customer Contact Center (CCC) or Honeywell Technical Assistance Center (TAC).

How to report a security vulnerability

For the purpose of submission, a security vulnerability is defined as a software defect or weakness that can be exploited to reduce the operational or security capabilities of the software.

Honeywell investigates all reports of security vulnerabilities affecting Honeywell products and services.

To report a potential security vulnerability against any Honeywell product, please follow the instructions at:

https://www.honeywell.com/product-security

Support

For support, contact your local Honeywell Process Solutions Customer Contact Center (CCC). To find your local CCC visit the website, https://www.honeywellprocess.com/en-US/contact-us/customer-support-contacts/Pages/default.aspx.

Training classes

Honeywell holds technical training classes that are taught by process control systems experts. For more information about these classes, contact your Honeywell representative, or see http://www.automationcollege.com.