Lesson 16: Configuring Domain Controllers

MOAC 70-411: Administering Windows Server 2012

Microsoft Official Academic Course

WILEY

Overview

- Exam Objective 5.2: Configure Domain Controllers
- Understanding Domain Controllers
- Installing and Configuring an RODC
- Cloning a Domain Controller

Understanding Domain Controllers

Lesson 16: Configuring Domain Controllers

Active Directory Logical Components

- Organization Units
- Domains
- Domain Trees
- Forests

Active Directory Physical Components

- Domain Controllers
- Global Catalog Servers
- Operations Masters
- Read-Only Domain Controllers

Domain Controllers

- A ***domain controller*** is a Windows server that stores a replica of the account and security information for the domain and defines the domain boundaries.
- To make a computer running Windows Server 2012 a domain controller, you must install the AD DS and execute `dcpromo` from Server Manager.
- Each domain has its own set of domain controllers.
- For fault tolerance, a site should have two or more domain controllers.

Global Catalogs

- As a domain controller, a ***global catalog*** stores a full copy of all objects in the domain.
- In addition, as a global catalog, it also has a partial copy of all objects for all other domains in the forest.
- The partial copy of all objects is used for logon, object searches, and universal group membership.
- A global catalog is created automatically on the first domain controller in the forest.
- Optionally, other domain controllers can be configured to serve as global catalogs.

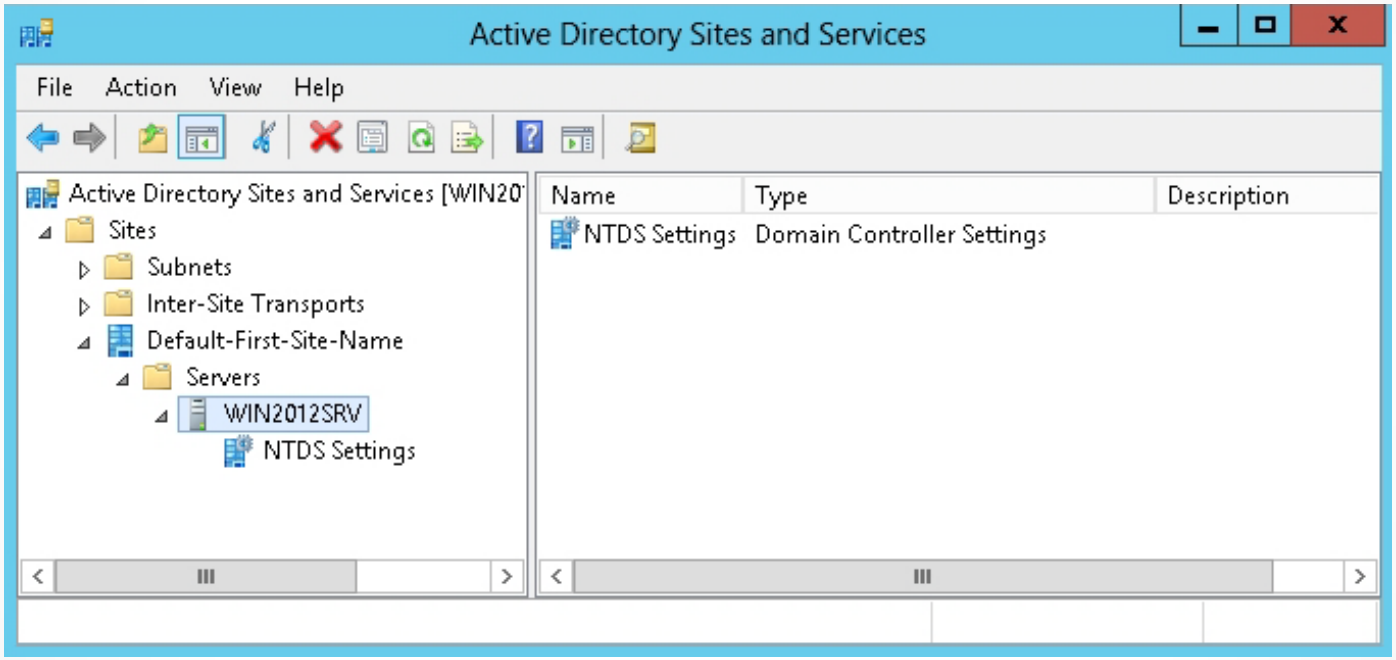
Global Catalogs and Universal Groups

- One of the primary functions of a global catalog is to provide search capability of any object in the forest.
- Another function of global catalog is to resolve User Principal Names (UPNs).
- Membership of universal groups is stored only in the global catalog and is replicated across the forest.
- When a user logs on, the domain controller must be able to view the membership of the universal groups, so that it can be determined whether a user is allowed or denied logon based on the membership of the universal group.

Universal Group Membership Caching

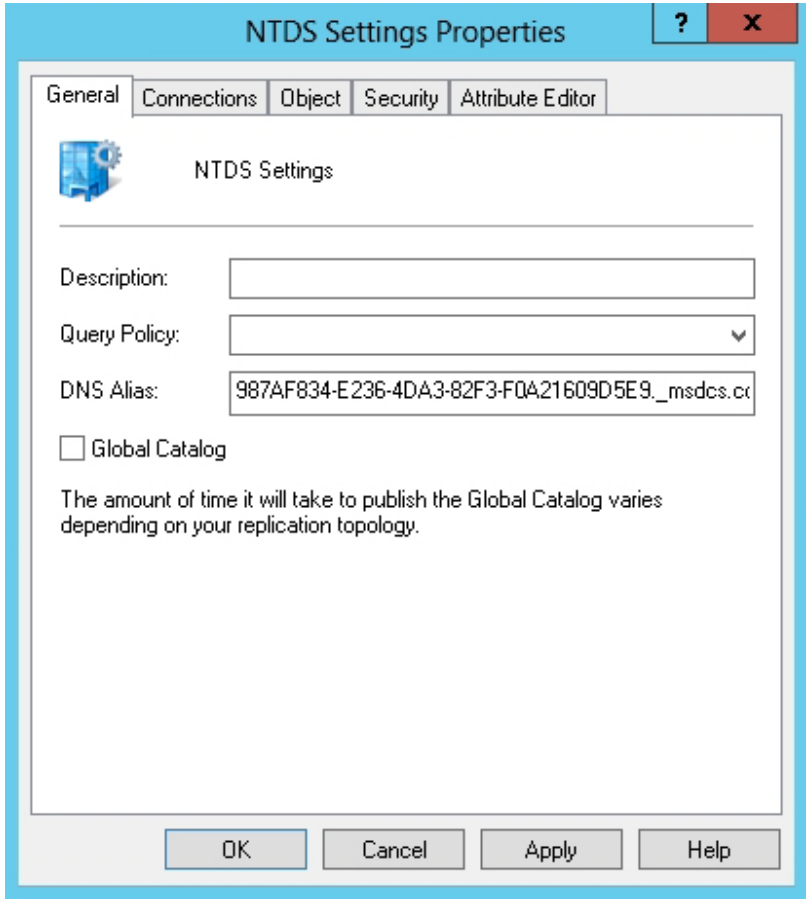
- If the membership of the universal groups cannot be determined, a user's logon request denies the request, and the user cannot log on.
- The only exception to this is that the Administrator account can always log on.
- Therefore, for all other users to log on, there must be at least one domain controller acting as a global catalog available or you need Universal Group Membership Caching enabled.

Enable Global Catalogs



Navigating to domain controllers

Enable Global Catalogs

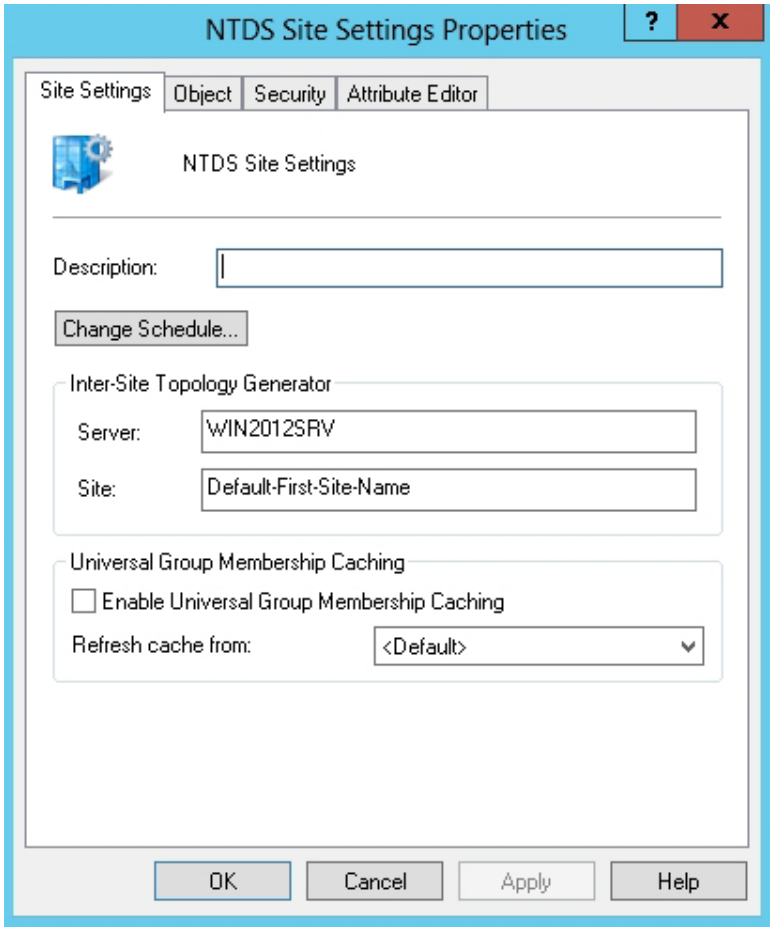


Opening the NTDS Settings Properties dialog box

Universal Group Membership Caching (UGMC)

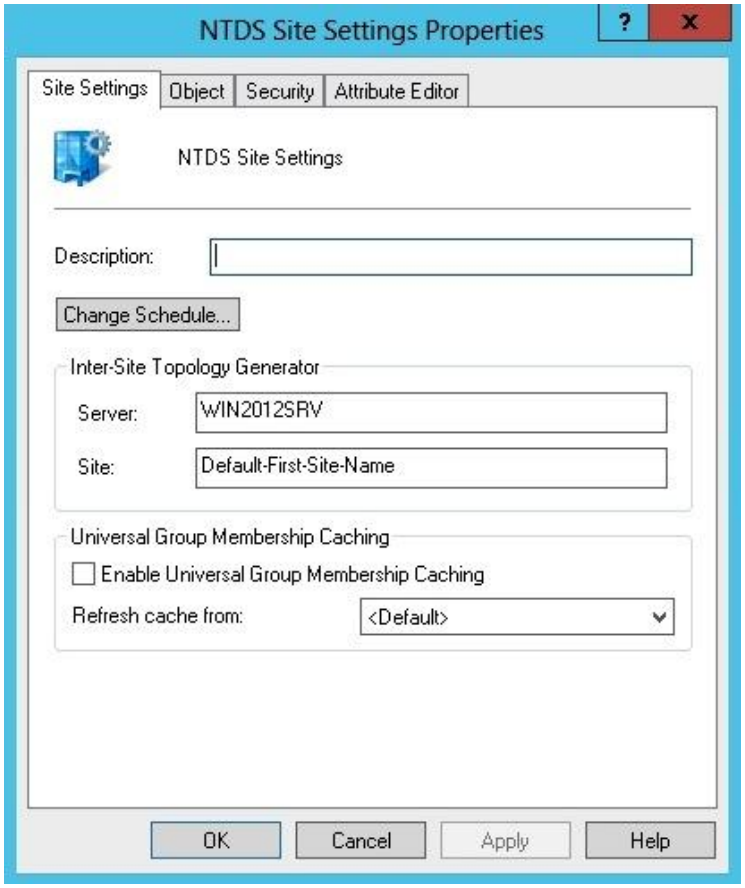
- ***Universal group membership caching (UGMC)*** allows the local domain controller to store the membership of the universal groups in its local cache indefinitely.
- The cache is refreshed by default every eight hours. As a result, domain controllers can process a logon or resource request without the presence of a global catalog server.
- UGMC provides better logon performance and minimizes WAN usage.
- UGMC is enabled on a per-site basis.

Enable Universal Group Membership Caching



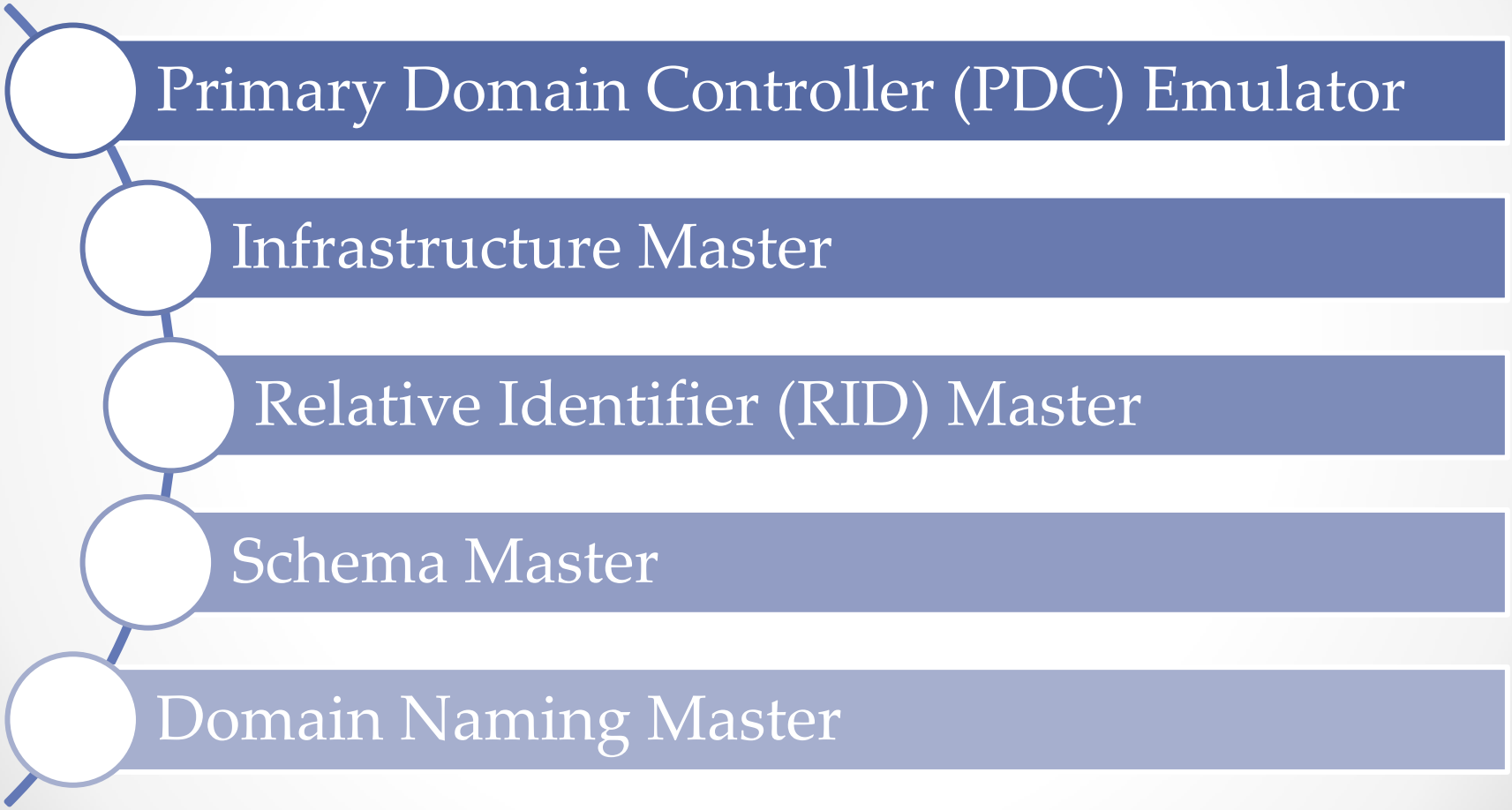
Navigating to a site

Enable Universal Group Membership Caching



Opening the NTDS Site Settings Properties dialog box

Operations Master Roles



Managing Operations Masters

Guidelines for placing the Operations Master roles:

- Place the domain-level roles on high-performance domain controllers.
- Do not place the infrastructure master on a global catalog server unless you have only one domain or all the domain controllers in your forest are also global catalogs.
- The Schema Master and Domain Naming Master should be on domain controllers in the forest-root domain.
- If the Primary Domain Controller (PDC) Emulator becomes overworked, you should offload non-AD DS roles to other servers, upgrade the PDC Emulator, or move the PDC Emulator to a more powerful computer.

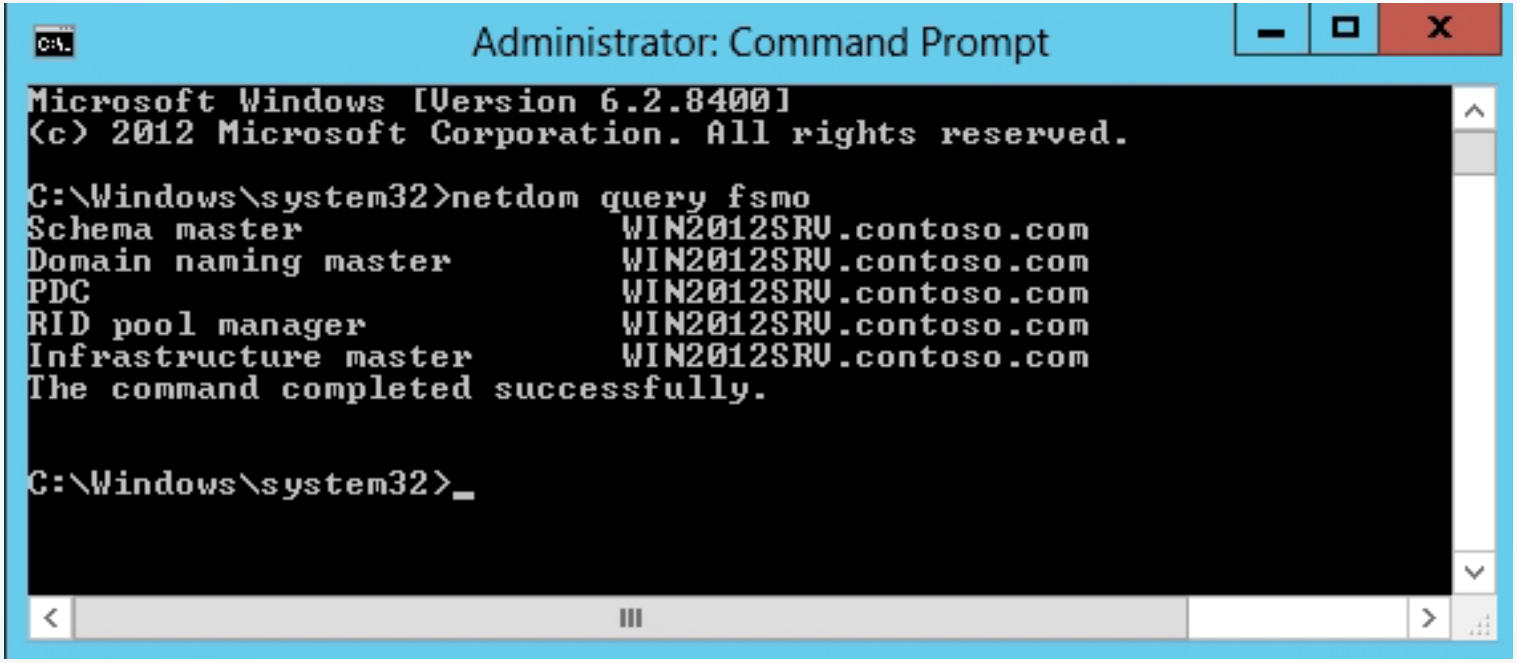
Viewing the Operations Masters Role Holders

- The easiest way to view the holders of all Operations Masters at once:

```
netdom query fsmo
```

- To view the RID Masters, PDC Emulators, or Infrastructure Master, use the Active Directory Users and Computers console.

Viewing Operations Masters

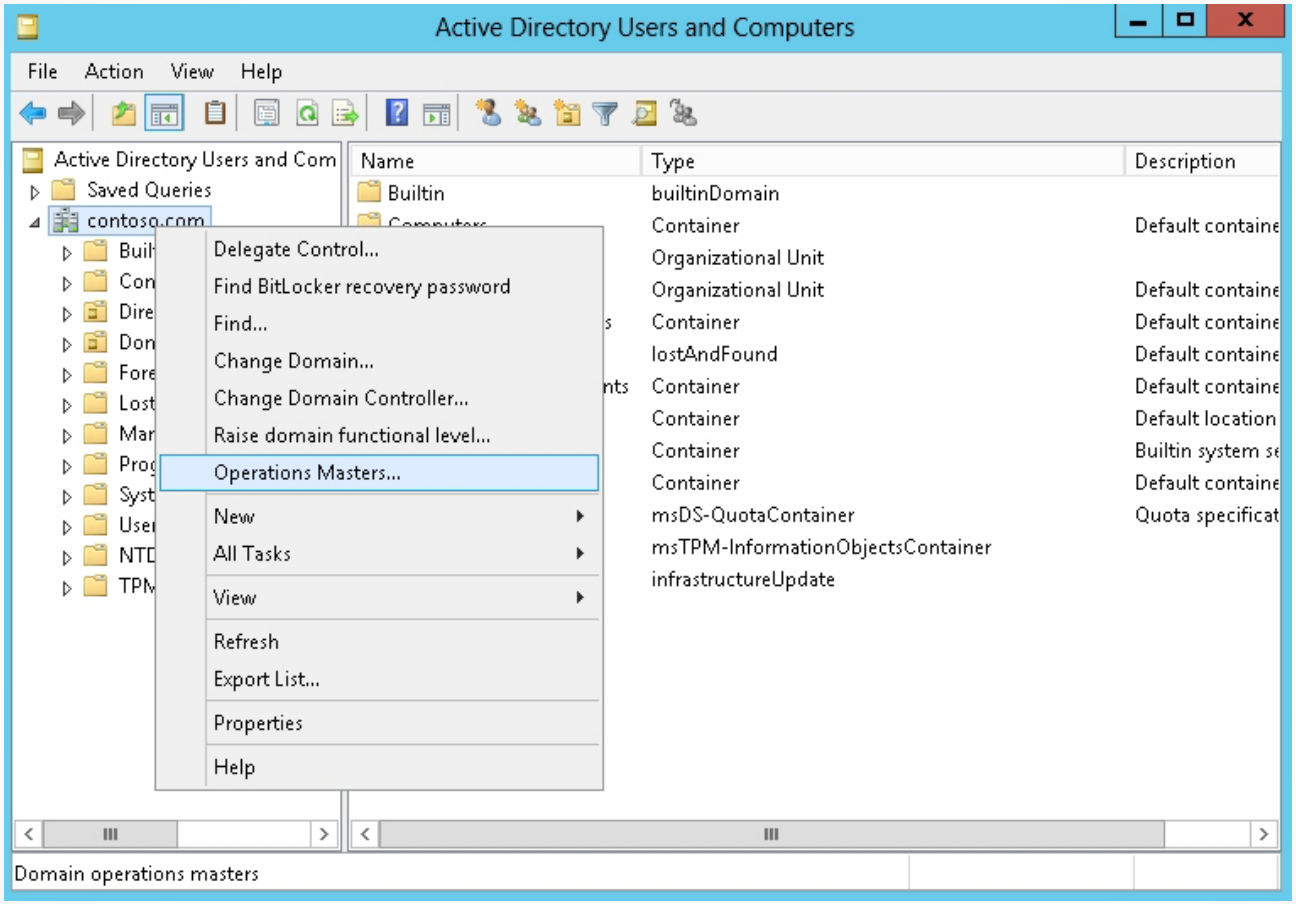


Viewing the holders of the Operations Masters roles at the command prompt

Viewing the Operations Masters Role Holders

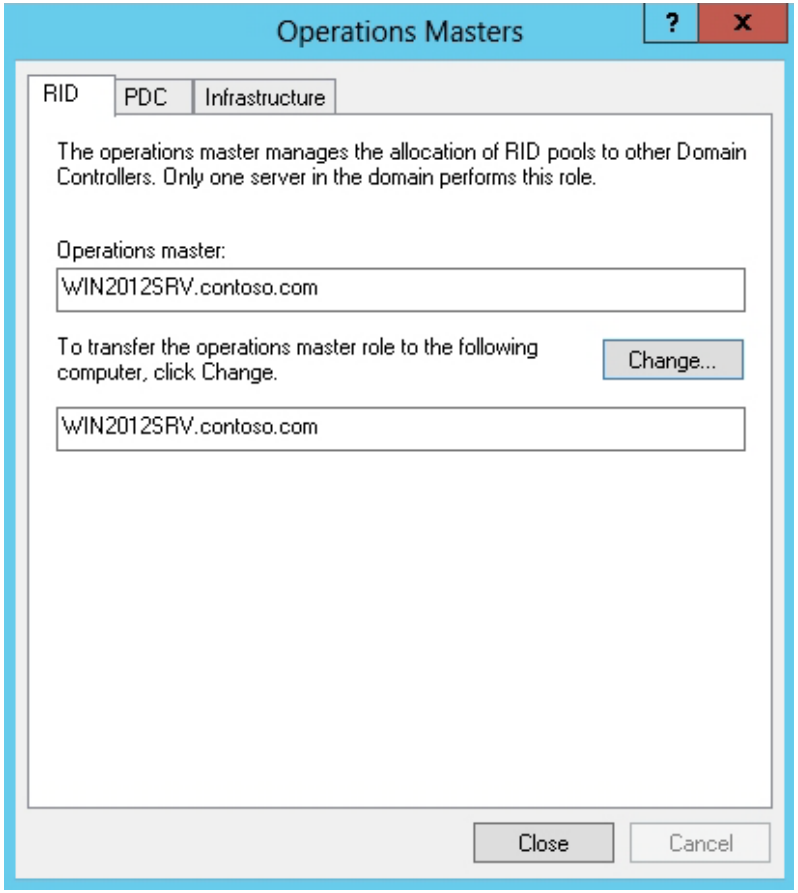
- To view the holder of the Domain Naming Master role, use the Active Directory Domains and Trusts console.
- To view the holder of the Schema Master role, use the Active Directory Schema.

View the Holders of RID Master, PDC Emulator, or Infrastructure Master



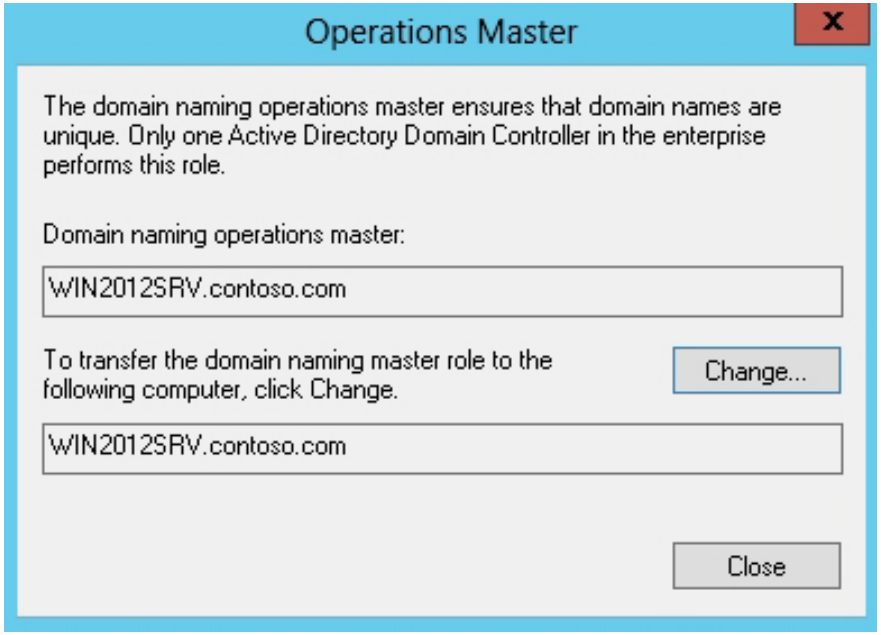
Selecting Operations Masters

View the Holders of RID Master, PDC Emulator, or Infrastructure Master



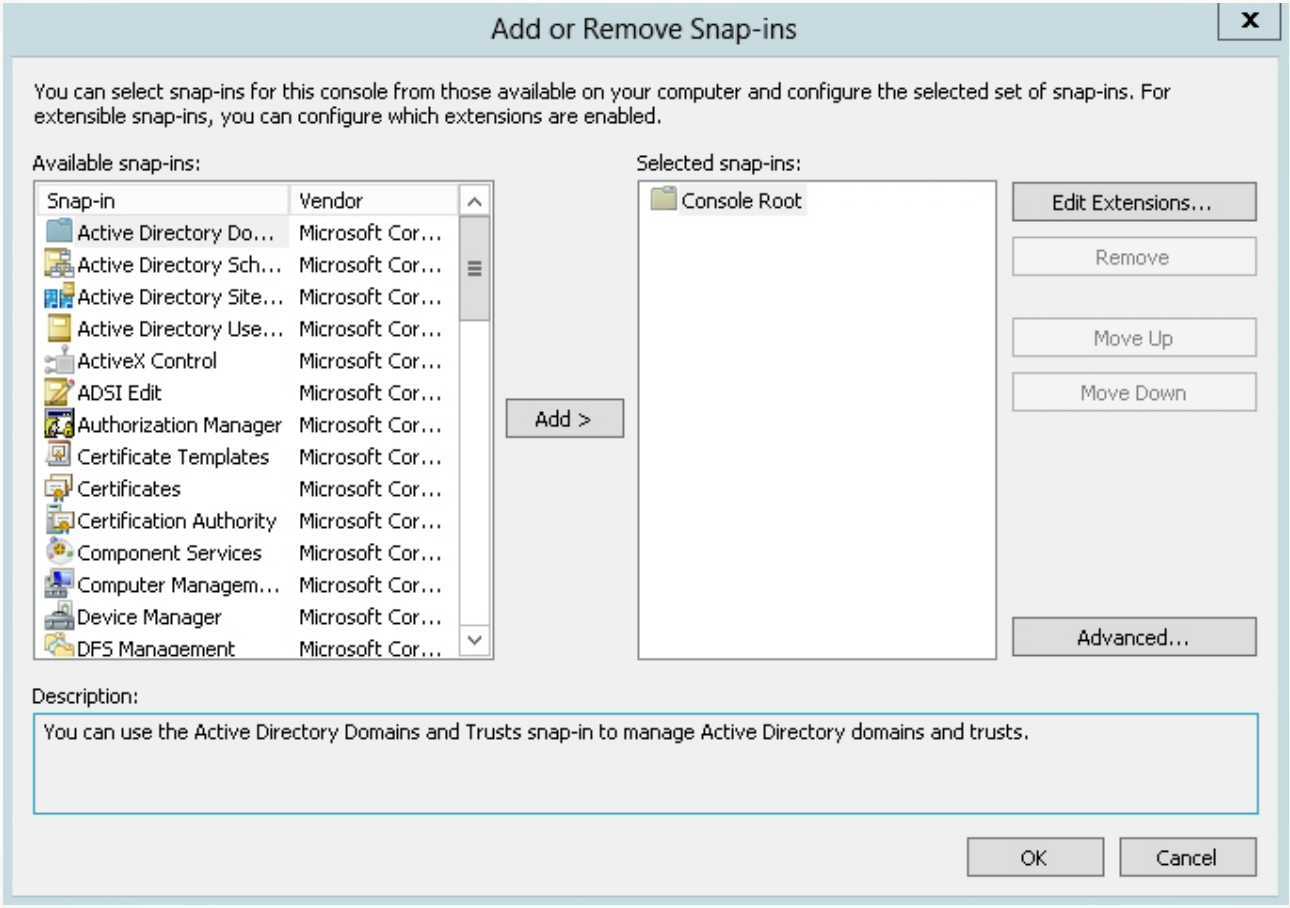
Using the Active Directory Users and Computers console to view the holders of the domain-based Operation Masters roles

View the Domain Naming Operations Master Role Holder



Using the Active Directory Domains and Trusts console to view the holders of the Domain Naming Operations Master

View the Schema Master Operations Master Role Holder



Opening the Add or Remove Snap-in dialog box

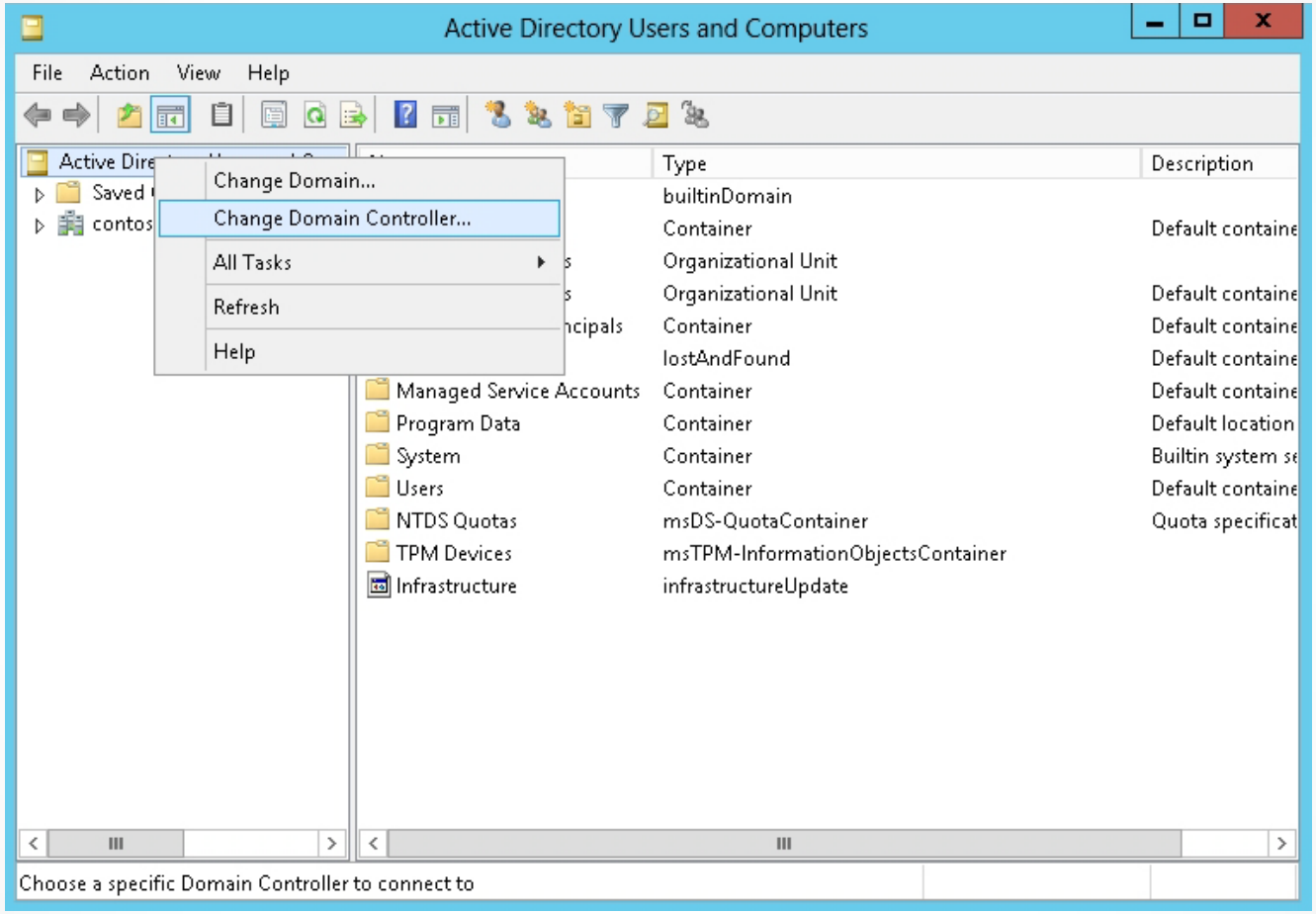
Transferring the Operations Masters Role

Reasons to transfer the Operations Master:

- Planned maintenance
- Retiring a domain controller that holds a role of Operations Master
- Moving a role of Operations Master to a domain controller with more resources

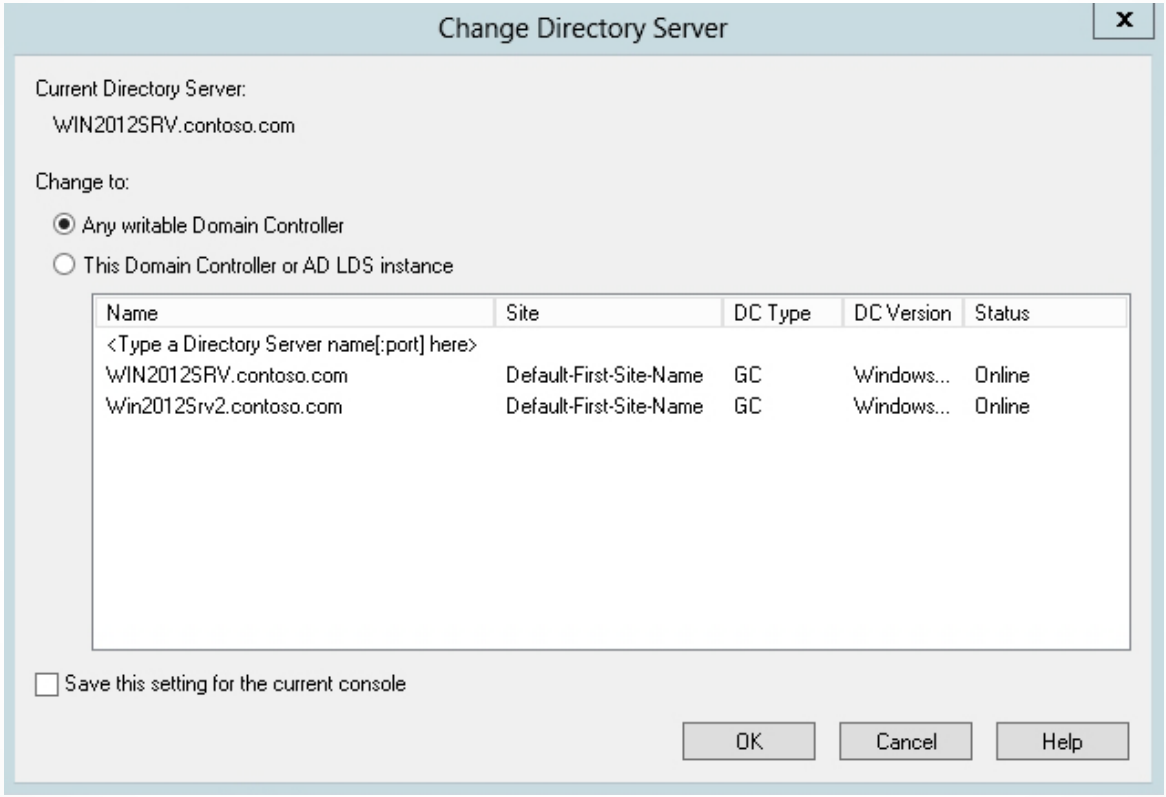
Transferring a FSMO role requires that the source domain controller and the target domain controller be online.

Transfer the Holders of RID Master, PDC Emulator, or Infrastructure Master



Selecting the Change Domain Controller option

Transfer the Holders of RID Master, PDC Emulator, or Infrastructure Master

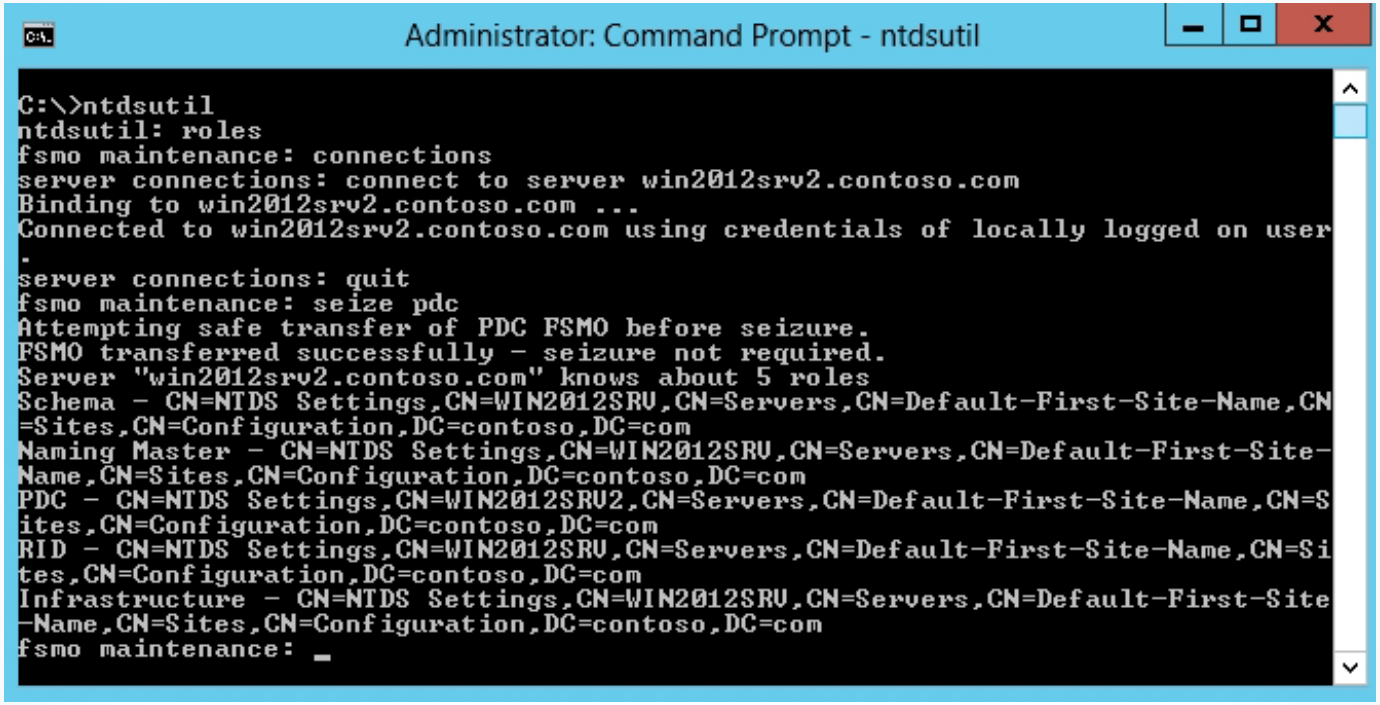


Selecting a domain controller to transfer the role to

Seizing the Operations Masters Role

- If a domain controller that holds an Operations Master role has an unrecoverable failure, you cannot transfer roles because the current domain controller is not online. Therefore, you need to seize the role.
- Seizing a FSMO role is a drastic measure that should be performed only in the event of a permanent role holder failure.
- To seize a role of an Operations Master, you use the `ntdsutil.exe` utility.

Seize the Role of an Operations Master Holder



Seizing the PDC Emulator role

Installing and Configuring an RODC

Lesson 16: Configuring Domain Controllers

Read-Only Domain Controller (RDOC)

The ***Read-Only Domain Controller (RODC)***:

- Contains a full replication of the domain database.
- Was created to be used in places where a domain controller is needed but the physical security of the domain controller could not be guaranteed.

Installing an RDOC

When you install an RODC, you need to define a delegated administrator that has local administrative permission to the RODC, even though the account is not a member of the Domain Admin or domain built-in Administrators group.

Deploying an RDOC

To deploy an RODC:

- Ensure that the forest functional level is Windows Server 2003 or higher.
- Deploy at least one writable domain controller running Windows Server 2008 or higher.

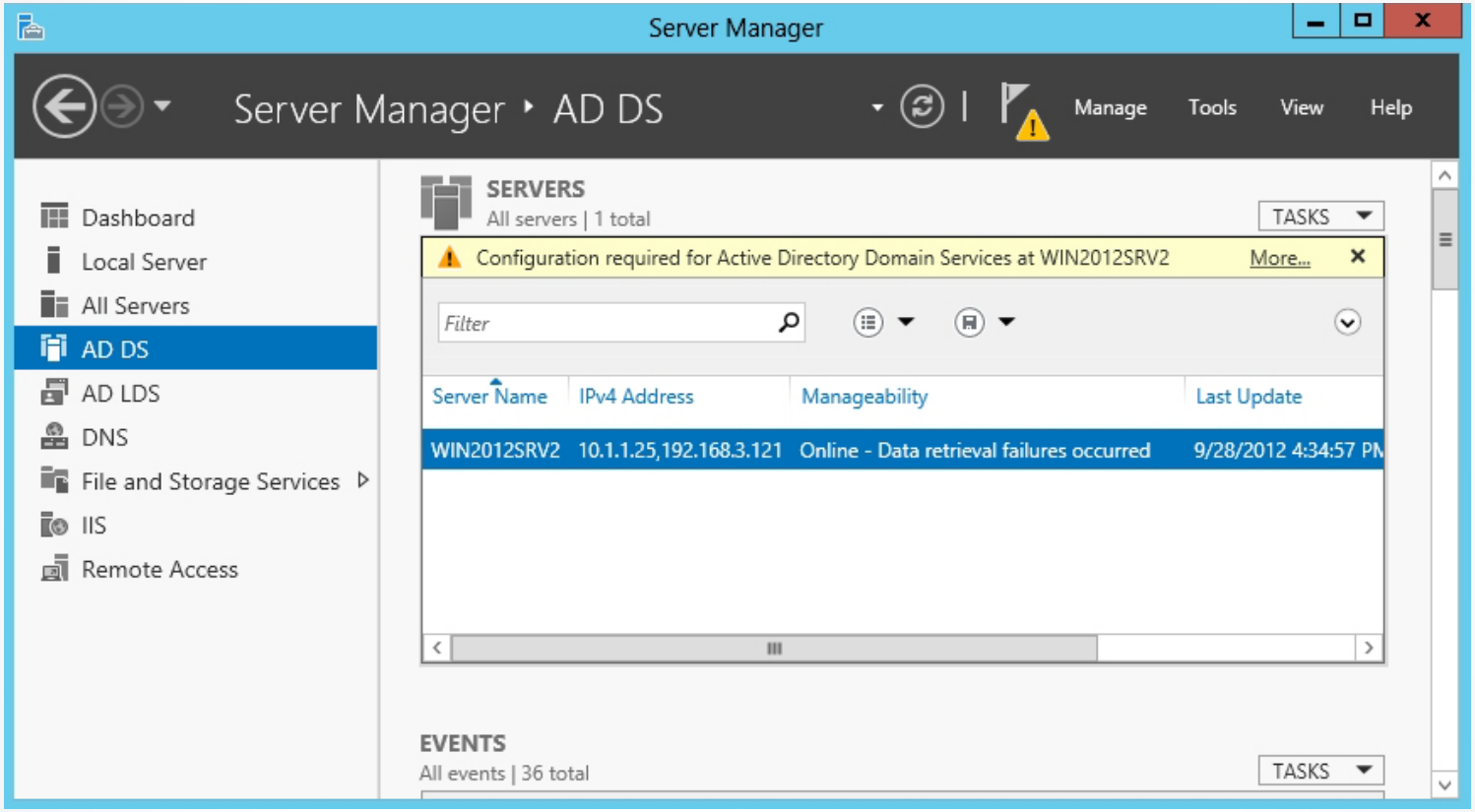
Configuring an RDOC

You can configure each RODC to have its own Password Replication Policy (PRP).

To allow enterprise-wide configuration of the RODC PRP, Windows Server 2008 creates the following security groups:

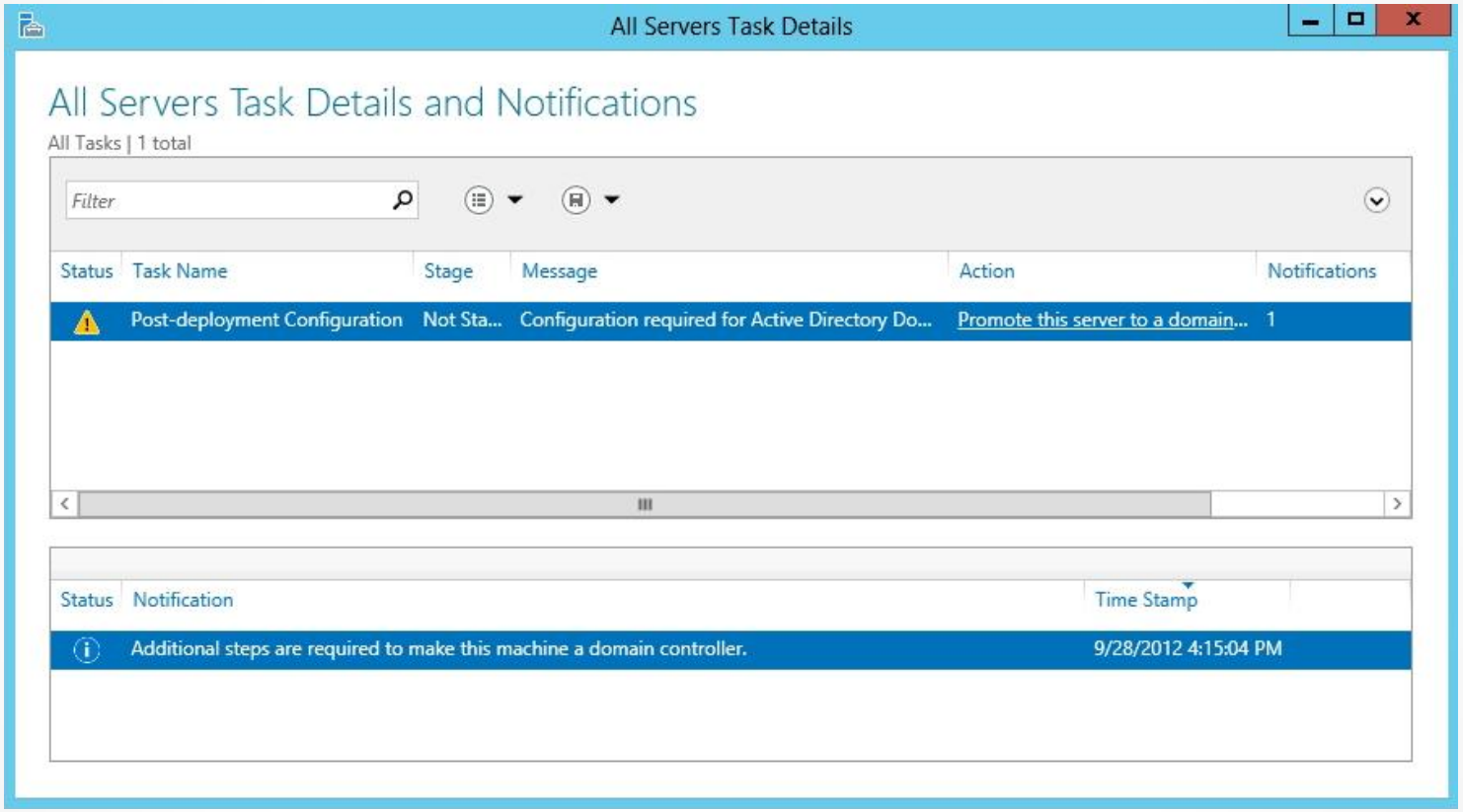
- Denied RODC Password Replication Group
- Allowed RODC Password Replication Group

Install a Read-Only Domain Controller



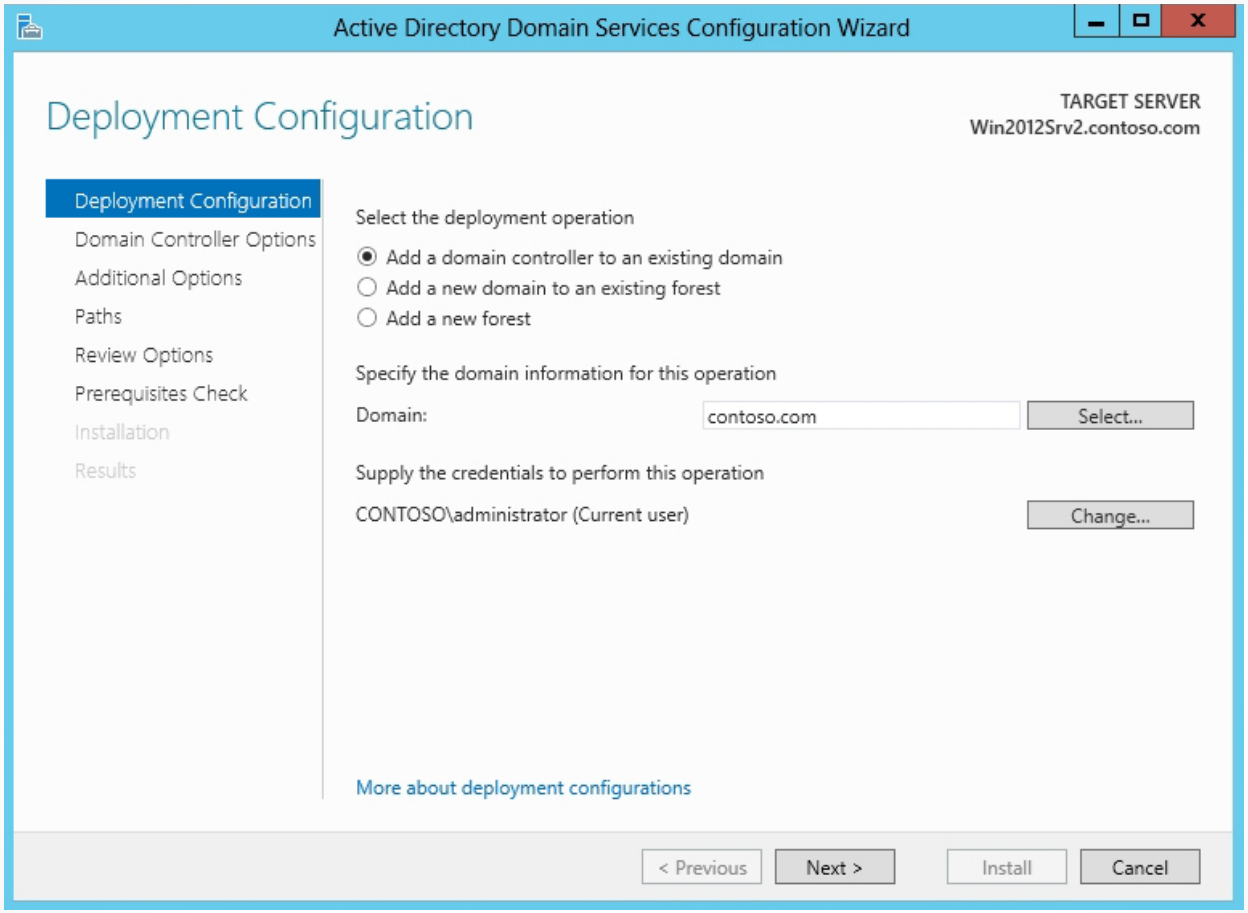
Installing AD DS on a new computer

Install a Read-Only Domain Controller



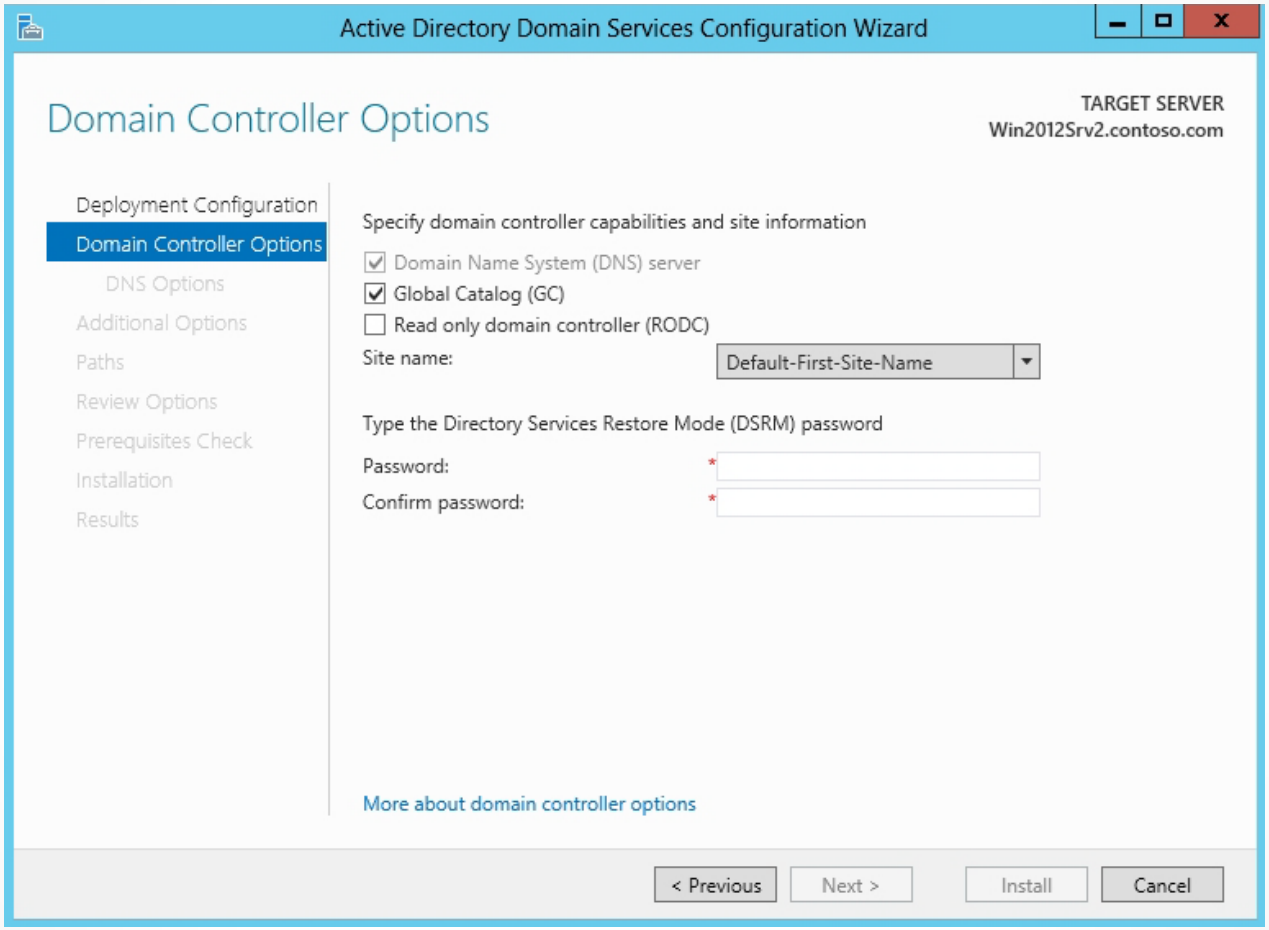
Promoting the server to a domain controller

Install a Read-Only Domain Controller



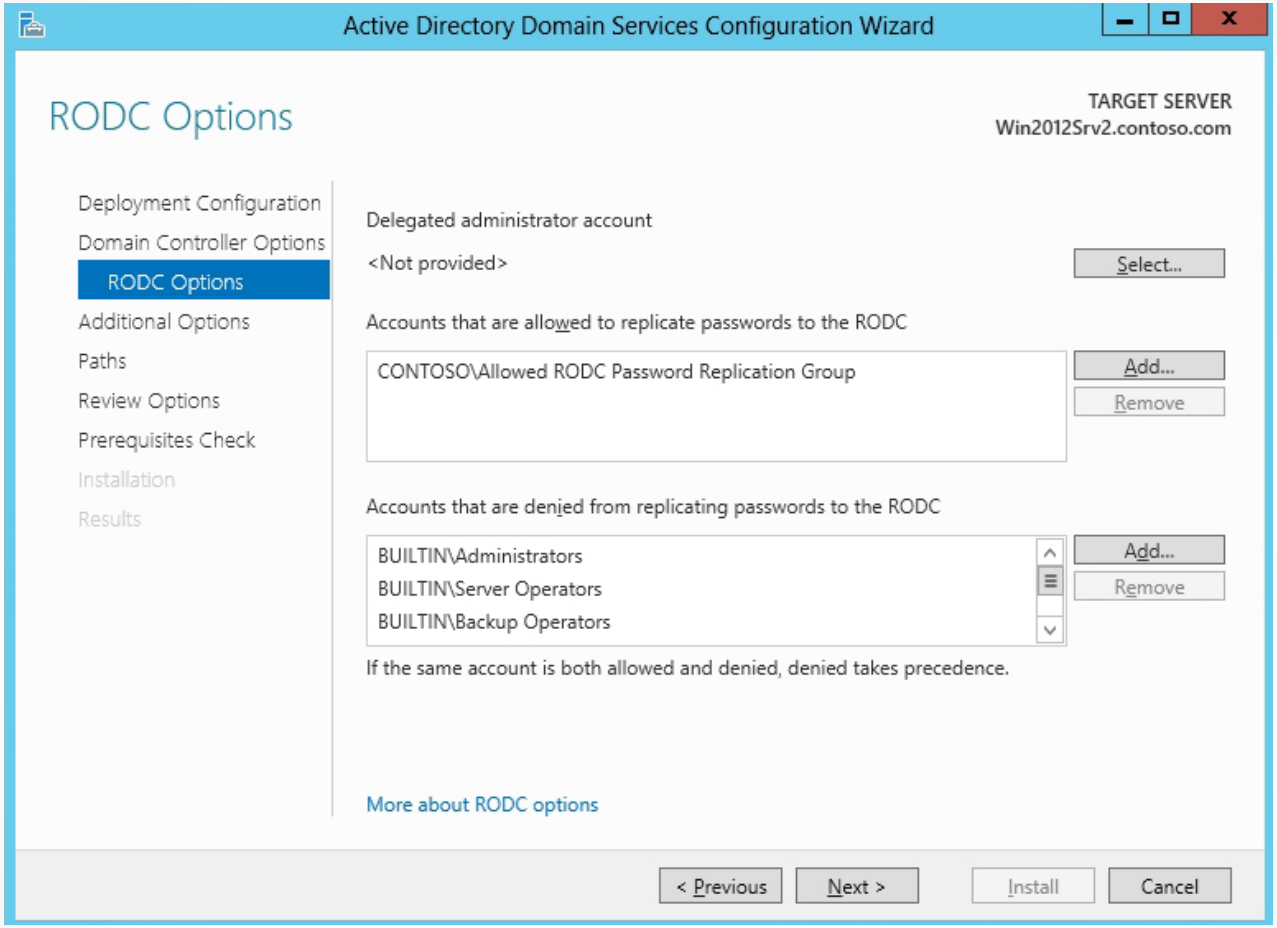
Adding a domain controller to an existing domain

Install a Read-Only Domain Controller



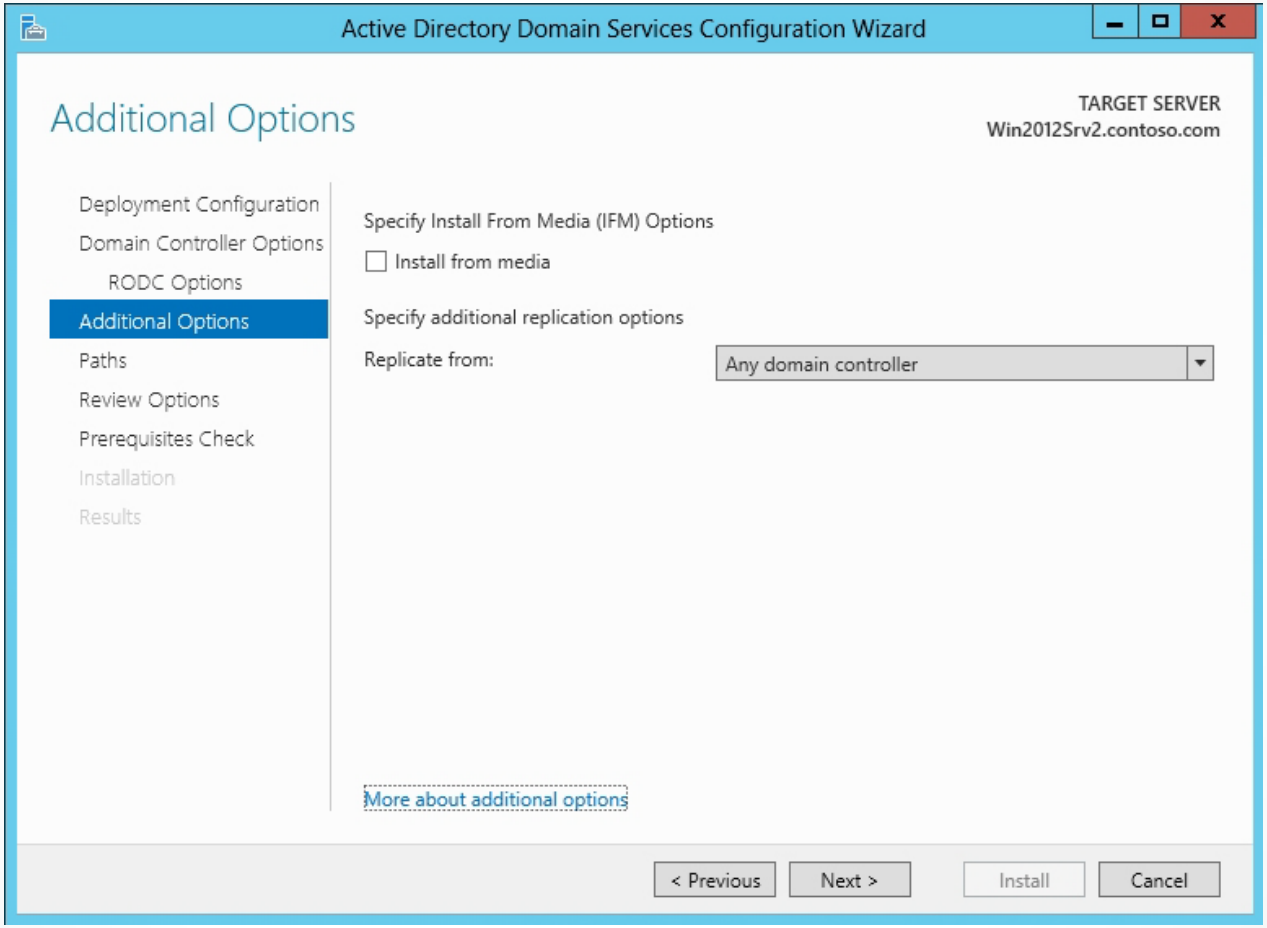
Selecting an RODC

Install a Read-Only Domain Controller



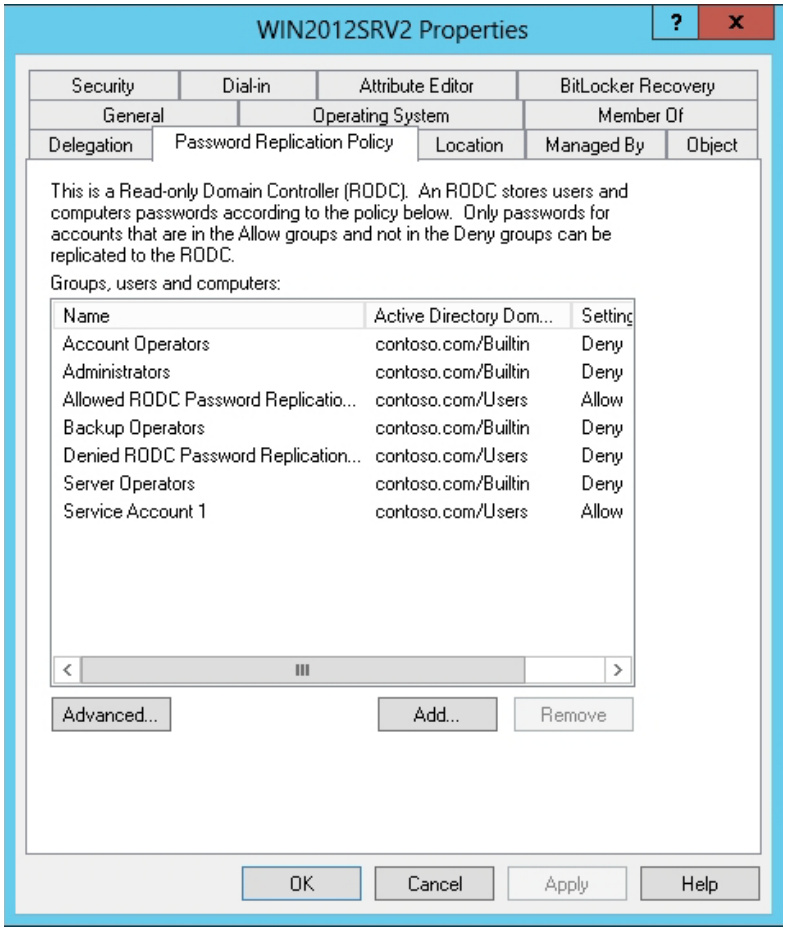
Specifying the delegated administrator

Install a Read-Only Domain Controller



Selecting additional options

Install a Read-Only Domain Controller



Configuring the Password Replication Policy

Cloning a Domain Controller

Lesson 16: Configuring Domain Controllers

Domain Controller Clones

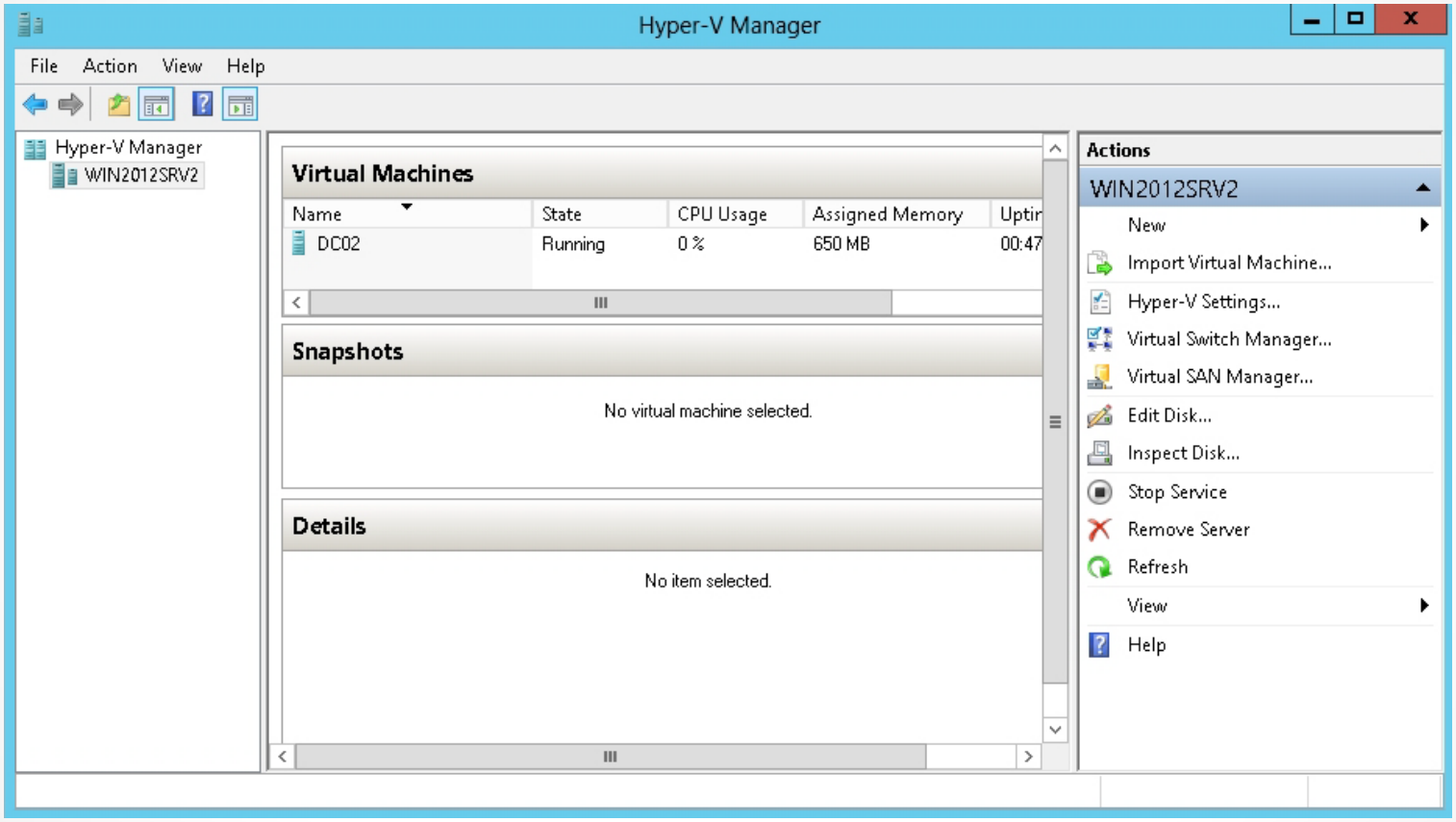
- Starting with Windows Server 2012, you can safely virtualize a domain controller and rapidly deploy virtual domain controllers through cloning.
- It allows you to quickly restore domain controllers when a failure occurs and to rapidly provision a test environment when you need to deploy and test new features or capabilities before you apply the features or capabilities to production.

Deploying a Cloned Domain Controller

Deploying a cloned virtualized domain controller:

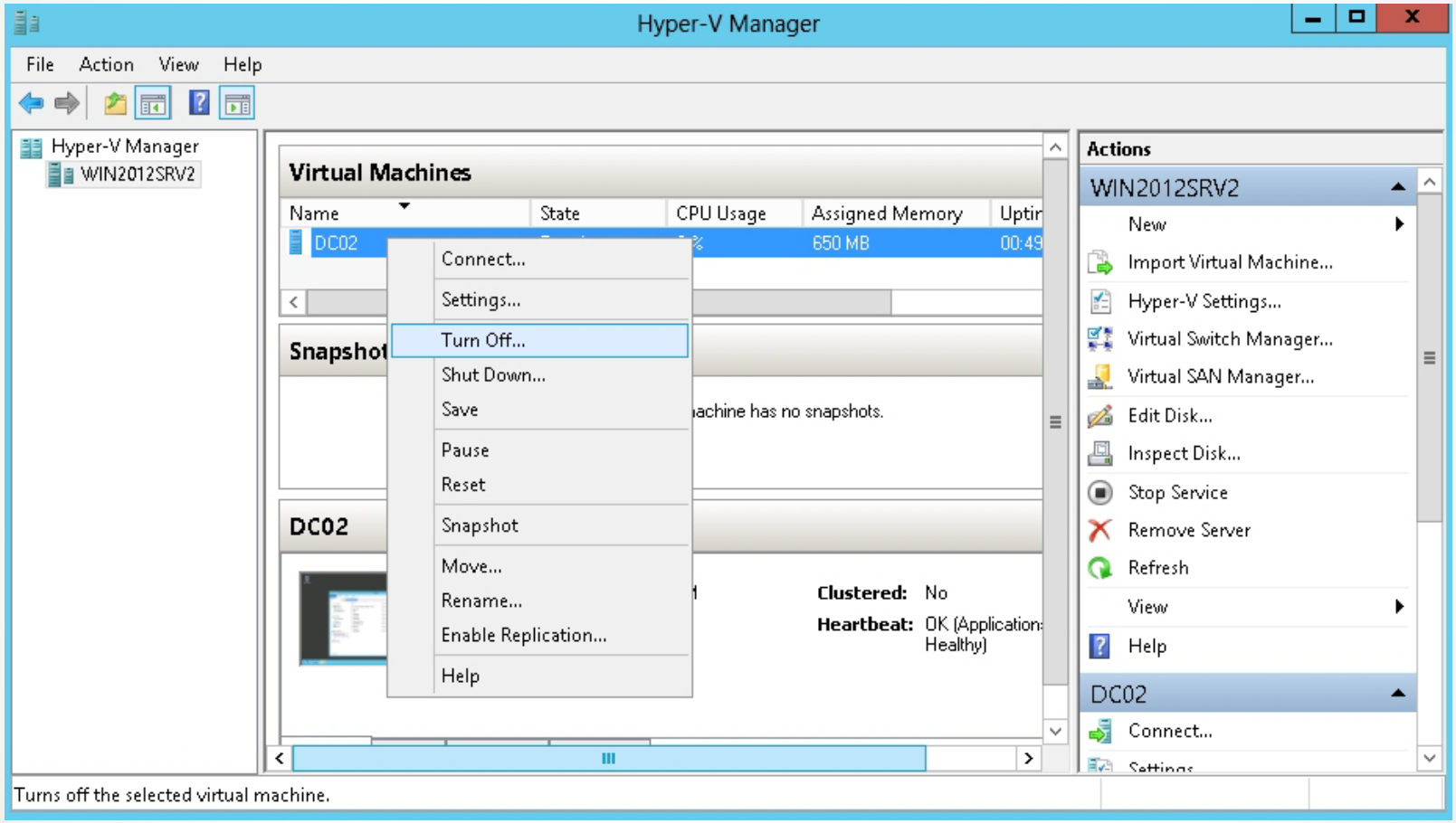
1. Grant the source virtualized domain controller the permission to be cloned by adding the source virtualized domain controller to the Cloneable Domain Controllers group.
2. Run `Get-ADDCCloningExcludedApplicationList` cmdlet in Windows PowerShell to determine which services and applications on the domain controller are not compatible with the cloning.
3. Run `New-ADDCCloneConfigFile` to create the clone configuration file, which is stored in the C:\Windows\NTDS.
4. In Hyper-V, export and then import the virtual machine of the source domain controller.

Deploy a Cloned Virtualized Domain Controller



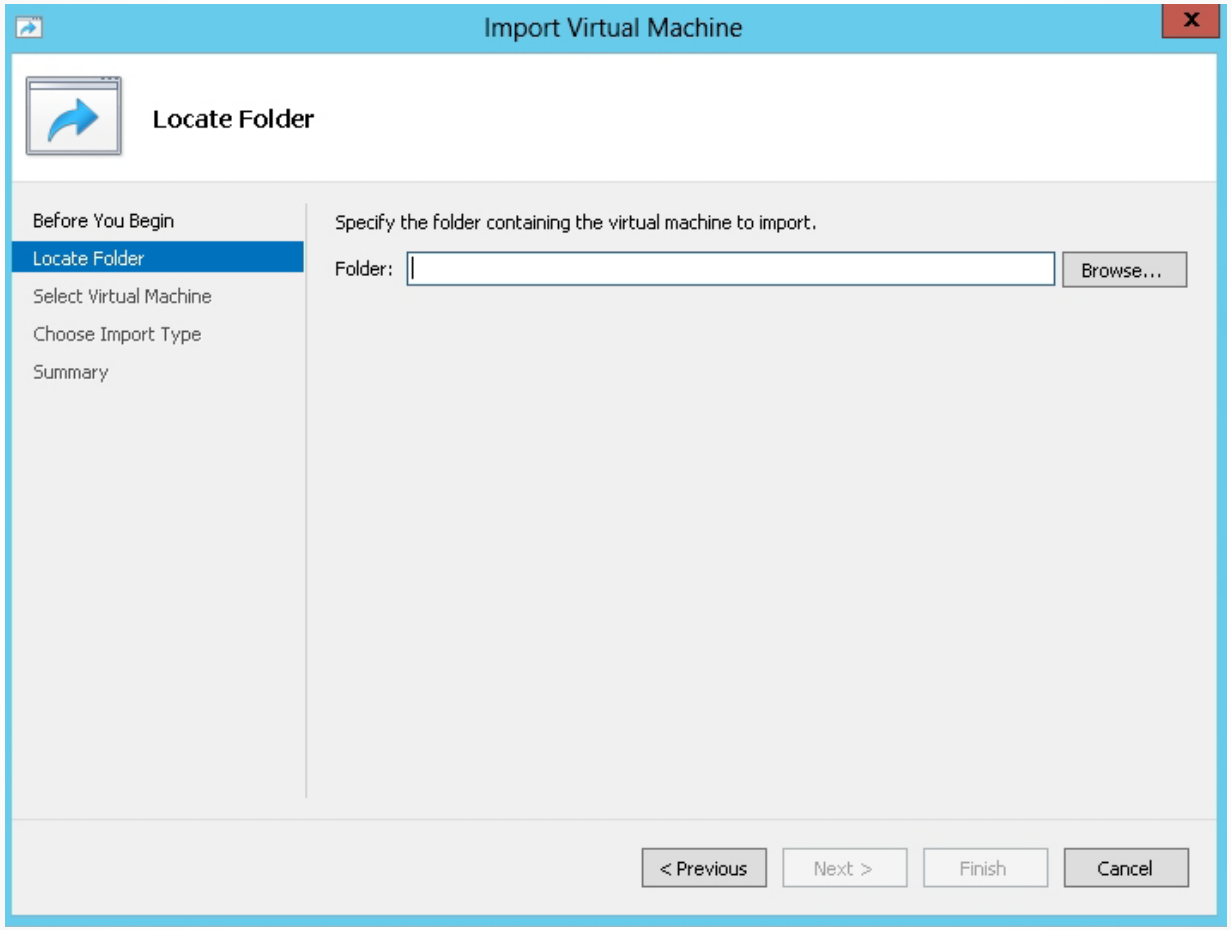
Opening the Hyper-V Manager

Deploy a Cloned Virtualized Domain Controller



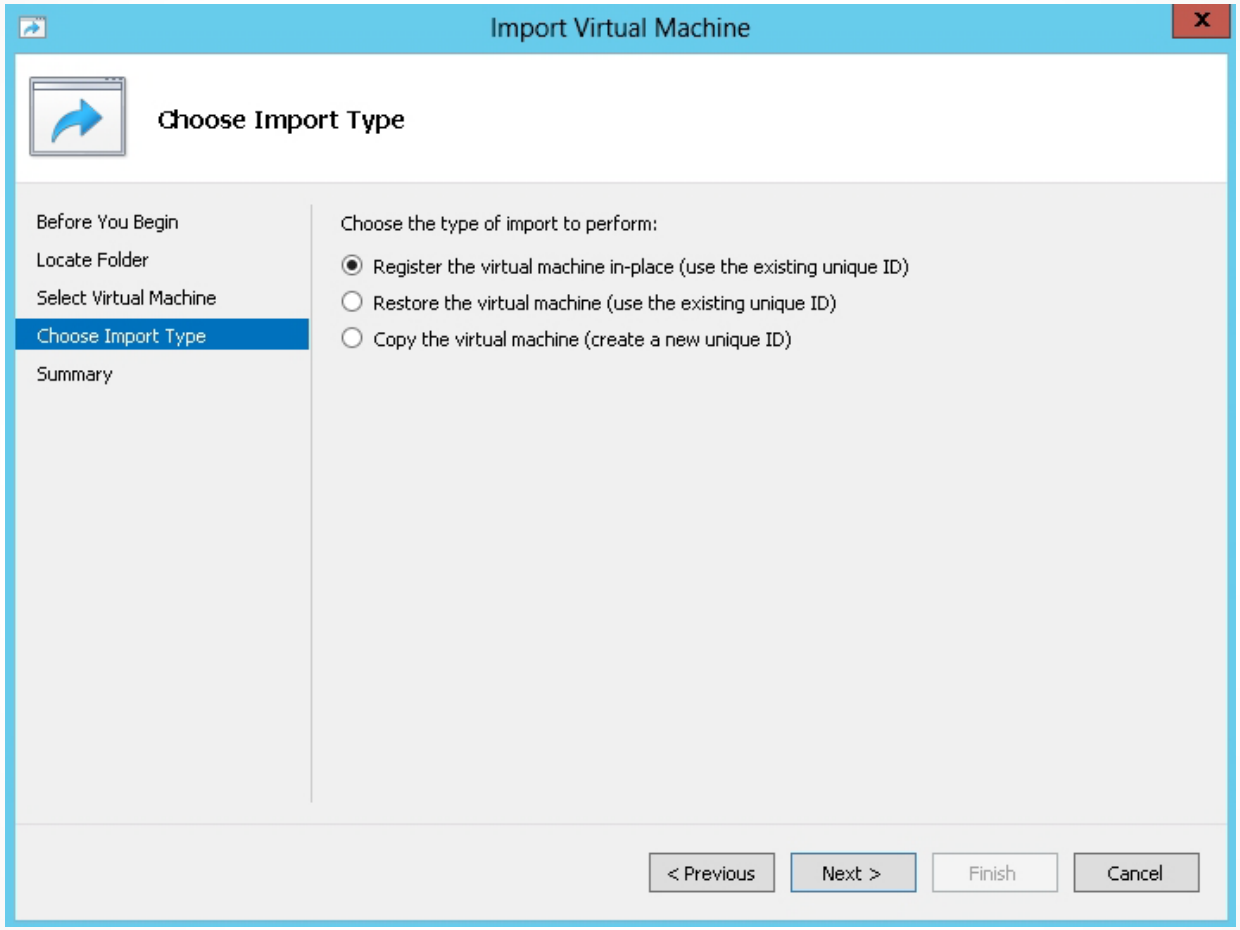
Turning off a virtual machine

Deploy a Cloned Virtualized Domain Controller



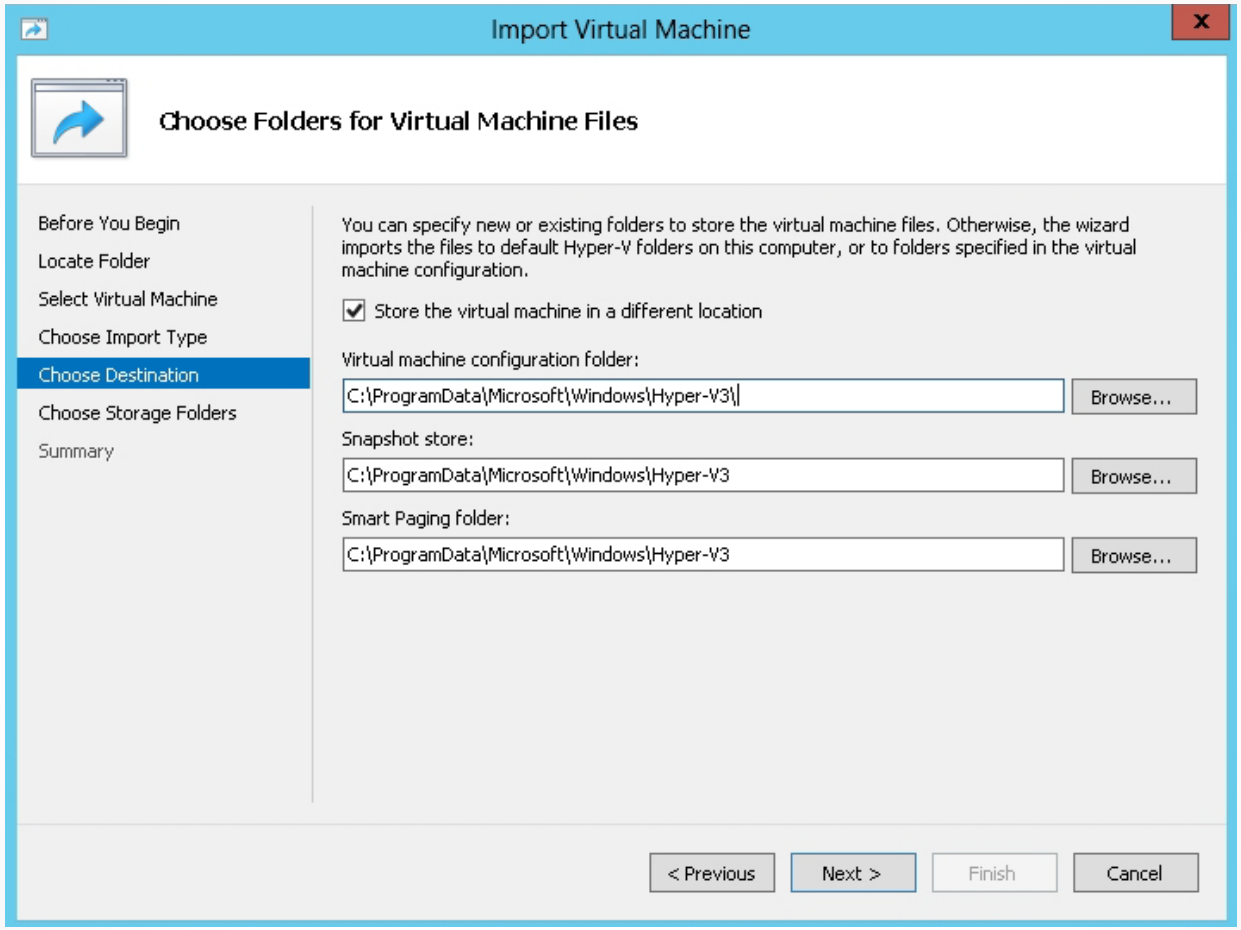
Specifying the virtual machine to import

Deploy a Cloned Virtualized Domain Controller



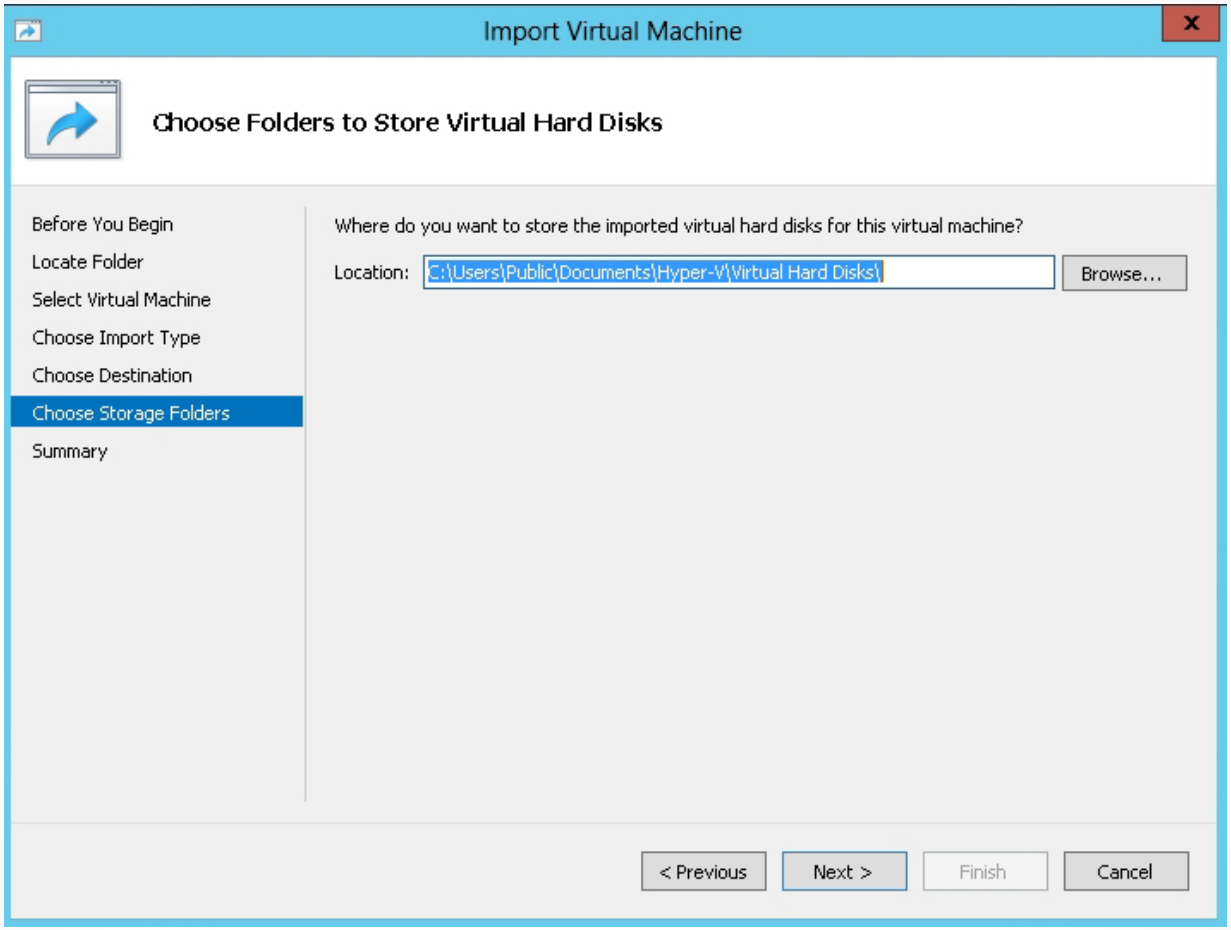
Choosing the import type

Deploy a Cloned Virtualized Domain Controller



Choosing where to store the virtual machine files

Deploy a Cloned Virtualized Domain Controller



Choosing where to store the virtual hard disks

Lesson Summary

- A domain is an administrative boundary for users and computers that are stored in a common directory database. A single domain can span multiple physical locations or sites and can contain millions of objects.
- Domain controllers are servers that contain the Active Directory databases.
- A global catalog stores a full copy of all objects in the domain.
- Universal group membership caching (UGMC) is one method to use to avoid placing a global catalog at every site and to avoid going over a WAN link for login information.
- Operations masters, sometimes referred to as Flexible Single Master Operations (FMSO), are specialized domain controllers that perform certain tasks that can be handled only by a single domain controller in a multi-master environment.

Lesson Summary

- Primary Domain Controller (PDC) Emulator coordinates password changes, account lockouts, and time synchronization; manages edits to Group Policy Objects (GPOs); and acts as a domain master browser (provides a list of workgroups and domains when you browse).
- Infrastructure Master is used to track which objects belong to which domain because it is responsible for reference updates from its domain objects to other domains.
- Relative Identifier (RID) Master is responsible for assigning relative identifiers to domain controllers in the domain.
- Schema Master controls all the updates and modifications to the schema. To update the schema of a forest, you must have access to the schema master.

Lesson Summary

- Domain Naming Master holds the Domain Naming Master role that controls the addition or removal of domains in the forest.
- If you are planning to do maintenance where a domain controller that holds the Operations Master will be down for an extended period of time, you are going to retire a domain controller that holds a role of Operations Master or you need to move the role to a domain controller with more resources, you will need to transfer the Operations Master.
- The Read-Only Domain Controller (RODC) contains a full replication of the domain database and cannot be modified directly.
- Starting with Windows Server 2012, you can safely virtualize a domain controller and rapidly deploy virtual domain controllers through cloning.