3/29/2021

Hands On Exercise

Chapter 6

Domain Controller and Active Directory Management

(Part1)

El Adel, Taoufik
IT 416 - SPRING 2021 - OLD DOMINION UNIVERSITY

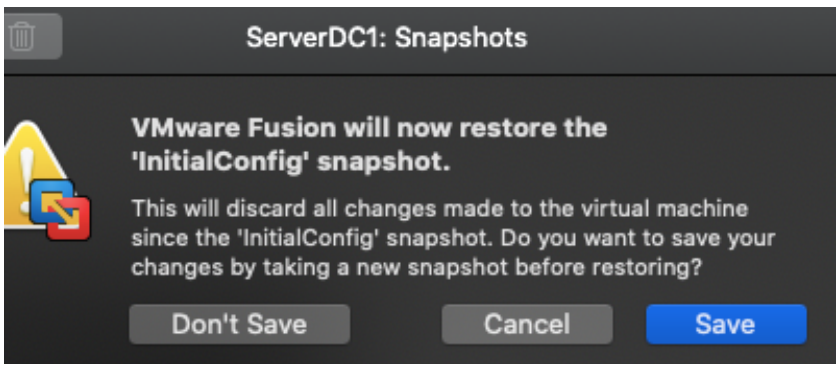
Table 6-1 Activity requirements

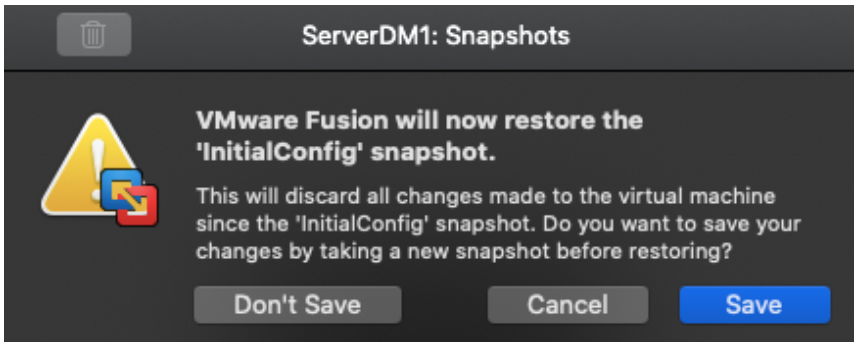
Activity	Requirements	Notes
Activity 6-1: Resetting Your Virtual Environment	ServerDC1, ServerDM1, ServerSA1	
Activity 6-2: Installing an RODC with Staging	ServerDC1, ServerSA1	
Activity 6-3: Configuring the Password Replication Policy	ServerDC1, ServerSA1	
Activity 6-4: Creating a Subnet in Active Directory Sites and Services	ServerDC1	
Activity 6-5: Viewing Site Properties	ServerDC1	
Activity 6-6: Changing an RODC to a Standard DC	ServerDC1, ServerSA1	
Activity 6-7: Transferring FSMO Roles	ServerDC1, ServerSA1	
Activity 6-8: Creating a System State Backup	ServerDC1, ServerSA1	
Activity 6-9: Restoring Active Directory from a System State Backup	ServerDC1, ServerSA1	
Activity 6-10: Restoring Deleted Objects from the Active Directory Recycle Bin	ServerDC1, ServerSA1	
Activity 6-11: Compacting the Active Directory Database	ServerDC1, ServerSA1	

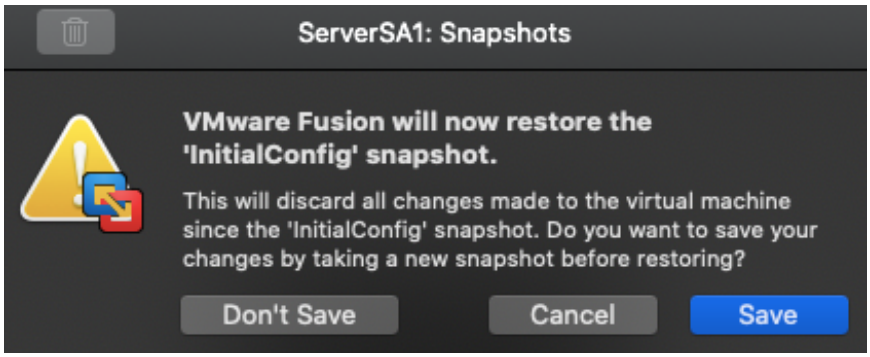
Activity 6-1: Resetting Your Virtual Environment

Time Required: 5 minutes
Objective: Reset your virtual environment by applying the InitialConfig checkpoint or snapshot.
Required Tools and Equipment: ServerDC1, ServerDM1, ServerSA1
Description: Apply the InitialConfig checkpoint or snapshot to ServerDC1, ServerDM1, and ServerSA1.

1. Be sure all servers are shut down. In your virtualization program, apply the InitialConfig checkpoint or snapshot to ServerDC1, ServerDM1, and ServerSA1.
2. When the snapshot or checkpoint has finished being applied, continue to the next activity.







Activity 6-2: Installing an RODC with Staging

Time Required: 20 minutes
Objective: Install a RODC with staging.
Required Tools and Equipment: ServerDC1, ServerSA1
Description: In this activity, you use RODC staging using PowerShell, so first you create a group and an account you delegate administration to. ServerSA1 will be the RODC.

1. Start ServerDC1 and ServerSA1, and sign in to both as **Administrator.**
2. On ServerDC1, open Active Directory Users and Computers. Create a new OU under the domain node named **BranchOffice**. In the BranchOffice OU, create a global group named **BranchOff-G** and a user named **BranchUser1** with **Password01**. Make sure to set the password to never expire. Make BranchUser1 a member of the BranchOff-G group.
3. Right-click the **Domain Controllers** OU. Notice the option to "Pre-create" an RODC account. You can use this wizard to stage the RODC account, but you're using PowerShell.
4. On ServerDC1, open a PowerShell window. Type **Add-ADDSReadOnlyDomainControllerAccount -DomainControllerAccountName ServerSA1 -DomainName mcsa2016.local -SiteName Default-First-Site-Name -DelegatedAdministratorAccountName BranchOff-G** and press **Enter**. You might see a warning message about default security settings, which you can ignore. The last part of the output should say "Operation completed successfully."
5. In Active Directory Users and Computers, make sure the **Domain Controllers** OU is selected and click the **Refresh** button. You should see ServerSA1 in the middle pane with the DC Type showing Unoccupied DC Account (see Figure 6-7).
6. On ServerSA1, open a PowerShell prompt. First you need to install the Active Directory server role. Type **Install-WindowsFeature AD-Domain-Services -IncludeManagementTools** and press **Enter**. This installation takes some time.
7. At the PowerShell prompt, type **Install-ADDSDomainController -DomainName mcsa2016.local -UseExistingAccount -credential (get-credential)** and press **Enter**.

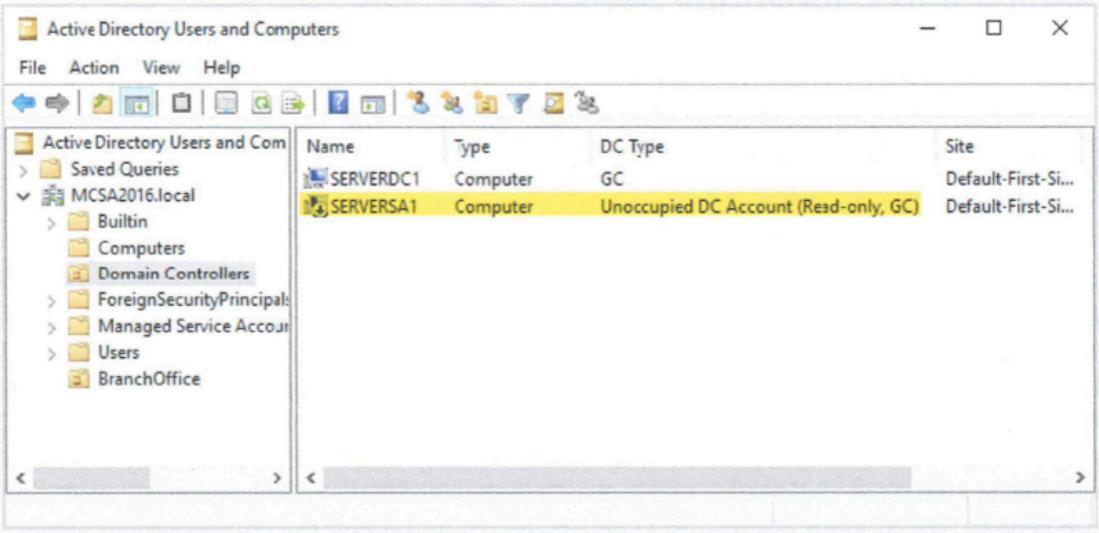
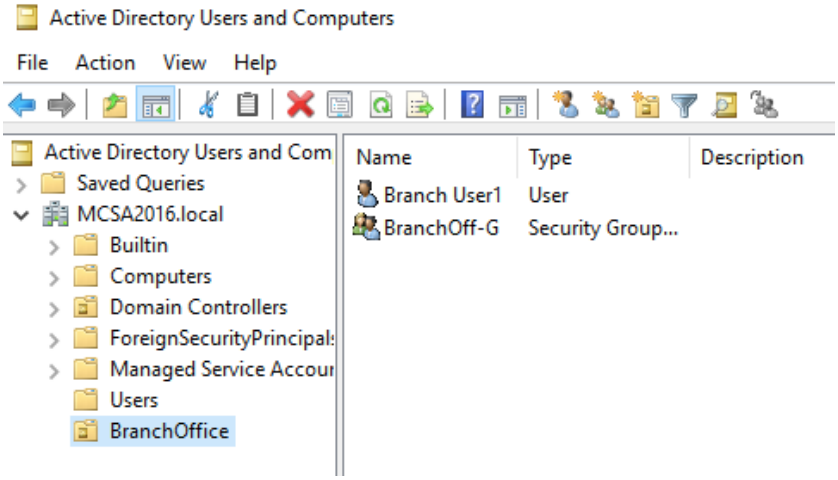
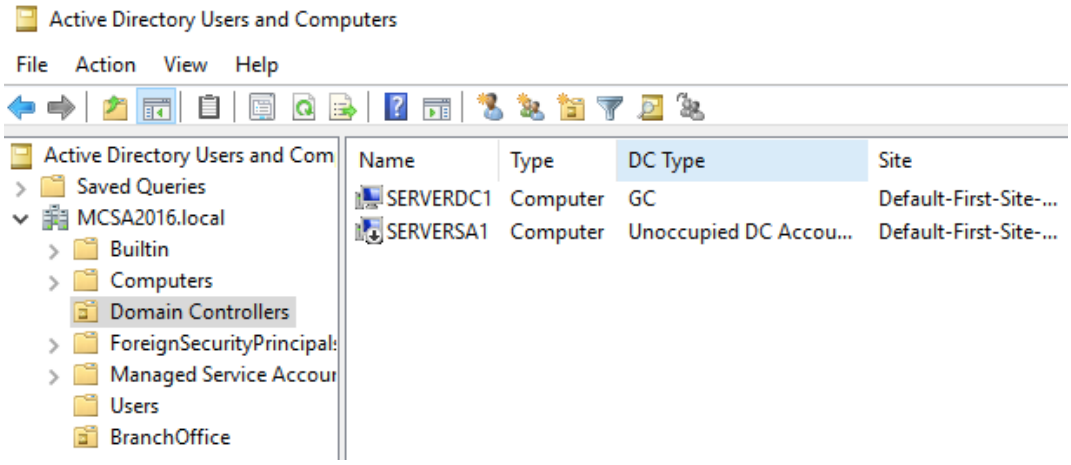


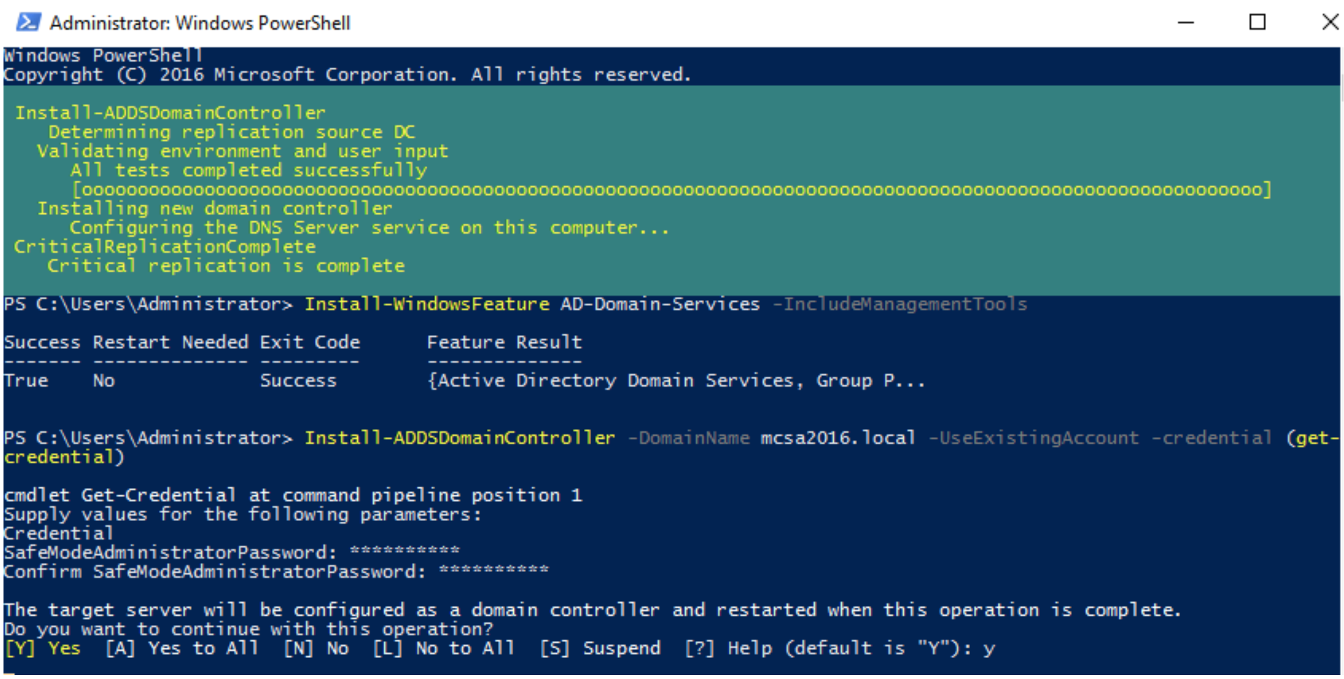
Figure 6-7 The staged RODC account in Active Directory Users and Computers

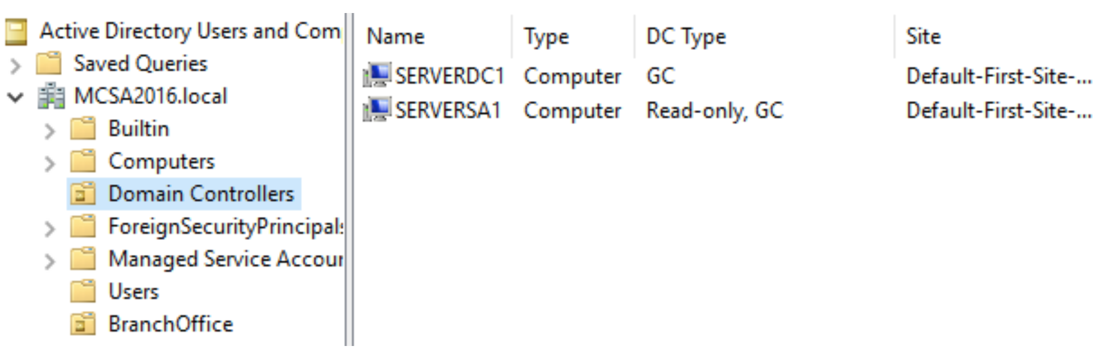
8. In the credentials dialog box, type **mcsa2016\BranchUser1** in the User name text box and **Password01** in the Password text box, and then click **OK**.
9. When you're prompted for the SafeModeAdministratorPassword (which is the DSRM password), type **Password01**, press **Enter**, type it again, and press **Enter**.
10. When you're prompted to continue with the operation, press **Enter**.
11. The installation takes a while. When it's finished, you see a message stating that you'll be signed out. Click **Close** or just wait for Windows to restart.
12. While ServerSA1 is restarting, refresh the screen in Active Directory Users and Computers on ServerDC1 to see that ServerSA1 is now listed as a read-only, global catalog domain controller.
13. Continue to the next activity.



```
PS C:\Users\Administrator> Add-ADDSReadOnlyDomainControllerAccount -DomainControllerAccountName Se
WARNING: Windows Server 2016 domain controllers have a default for the security setti
ng named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents
 weaker cryptography algorithms when establishing security channel sessions.

For more information about this setting, see Knowledge Base article 942564 (http://go
.microsoft.com/fwlink/?LinkId=104751).


WARNING: Windows Server 2016 domain controllers have a default for the security setti
ng named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents
 weaker cryptography algorithms when establishing security channel sessions.

For more information about this setting, see Knowledge Base article 942564 (http://go
.microsoft.com/fwlink/?LinkId=104751).



Message                      Context           RebootRequired  Status
-------                      -------           --------------  ------
Operation completed successfully DCPromo.General.1          False Success
```



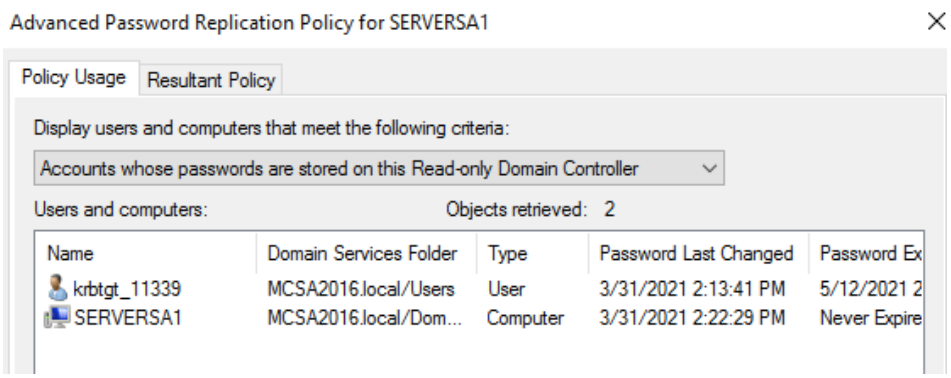




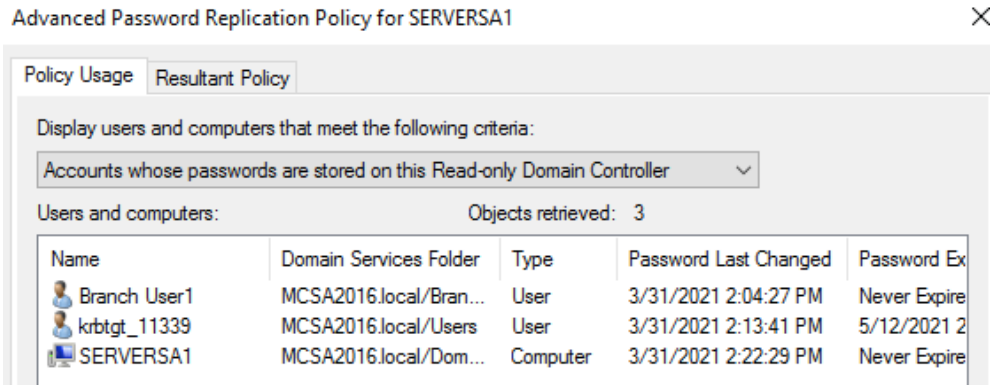
Activity 6-3: Configuring the Password Replication Policy

Time Required: 15 minutes
Objective: Add a group to the PRP of the ServerSA1 computer account.
Required Tools and Equipment: ServerDC1, ServerSA1
Description: In this activity, you create a group and add it to the Allowed RODC Password Replication group.

1. On ServerDC1, open Active Directory Users and Computers, click **Domain Controllers** in the left pane, and in the middle pane, double-click **ServerSA1** to open its Properties dialog box. Click the **Password Replication Policy** tab.
2. Click the **Advanced** button. The Advanced Password Replication Policy for ServerSA1 dialog box shows you which account passwords are stored on the RODC. By default, the RODC computer account is replicated as is a special account used by the Kerberos authentication process. Click **Close** and then **Cancel**.
3. Open a PowerShell prompt. Add the BranchOff-G group to the Allowed RODC Password Replication Group by typing **Add-ADGroupMember "Allowed RODC Password Replication Group" BranchOff-G** and pressing **Enter**.
4. Sign in to ServerSA1 as **BranchUser1**.
5. On ServerDC1, open the Properties dialog box for the ServerSA1 account again, and click the **Password Replication Policy** tab. Click **Advanced** to see that BranchUser1 is now among the accounts whose passwords are stored on the RODC. Click **Close** and then **Cancel**.
6. Sign out of ServerSA1. Continue to the next activity.



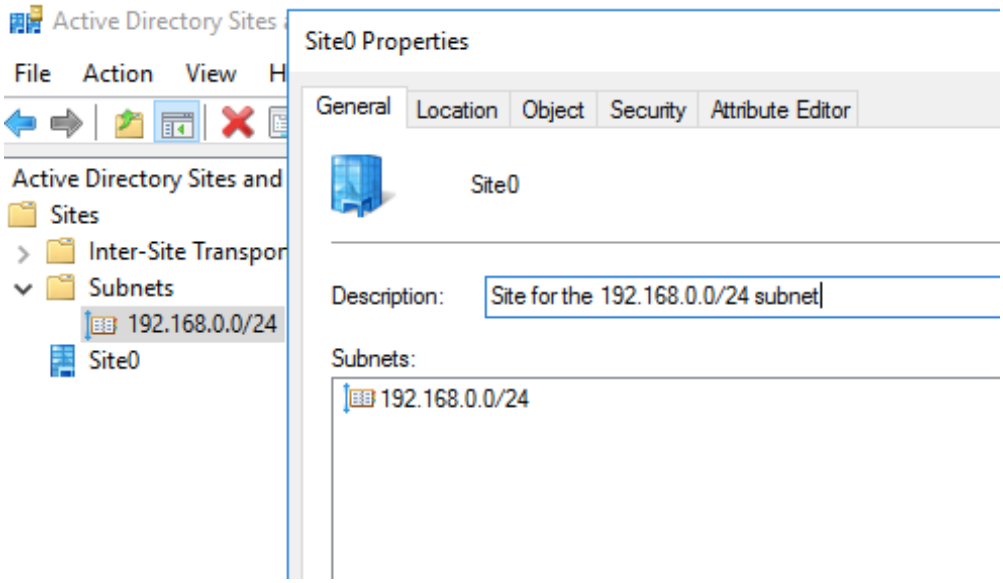

```
PS C:\Users\Administrator> Add-ADGroupMember "Allowed RODC Password Replication Group" BranchOff-G
PS C:\Users\Administrator>
```



Activity 6-4: Creating a Subnet in Active Directory Sites and Services

Time Required: 5 minutes
Objective: Create a subnet in Active Directory Sites and Services and associate it with a site.
Required Tools and Equipment: ServerDC1
Description: In this activity, you configure the default site to use the subnet already in use in your network. In addition, you rename the default site.

1. On ServerDC1, in Server Manager, click **Tools, Active Directory Sites and Services** from the menu.
2. Double-click to expand **Sites**, if necessary. Right-click **Subnets**, point to **New**, and click **Subnet**.
3. In the Prefix text box, type **192.168.0.0/24** (assuming that you're following the IP address scheme used in this book; otherwise, ask your instructor what to enter).
4. In the Select a site object for this prefix list box, click **Default-First-Site-Name**, and then click **OK**.
5. In the left pane, click **Subnets**. Right-click **192.168.0.0/24** and click **Properties**. In the General tab, you can give the subnet a description and change the site with which the subnet is associated. For now, leave it as is. Click **Cancel**.
6. In the left pane, right-click **Default-First-Site-Name** and click **Rename**. Type **Site0** and press **Enter**. You're using the third octet of the IP address as part of the site name.
7. In the left pane, right-click **Site0** and click **Properties**. In the Description text box, type **Site for the 192.168.0.0/24 subnet**, and then click **OK**.
8. Continue to the next activity.



Activity 6-5: Viewing Sites Properties

Time Required: 10 minutes
Objective: View site properties.
Required Tools and Equipment: ServerDC1
Description: In this activity, you explore the properties of NTDS site settings, server NTDS settings, and connection objects.

1. On ServerDC1, open Active Directory Sites and Services, if necessary. Click to expand **Sites**, **Site0**, **Servers**, and **ServerDC1**. Under ServerDC1 in the left pane, right-click **NTDS Settings** and click **Properties**.
2. In the General tab, you can select or clear the Global Catalog option to configure whether the server is a global catalog server. Click the **Connections** tab. You see ServerSA1 in the Replicate To list box (see Figure 6-13). Click **Cancel**.

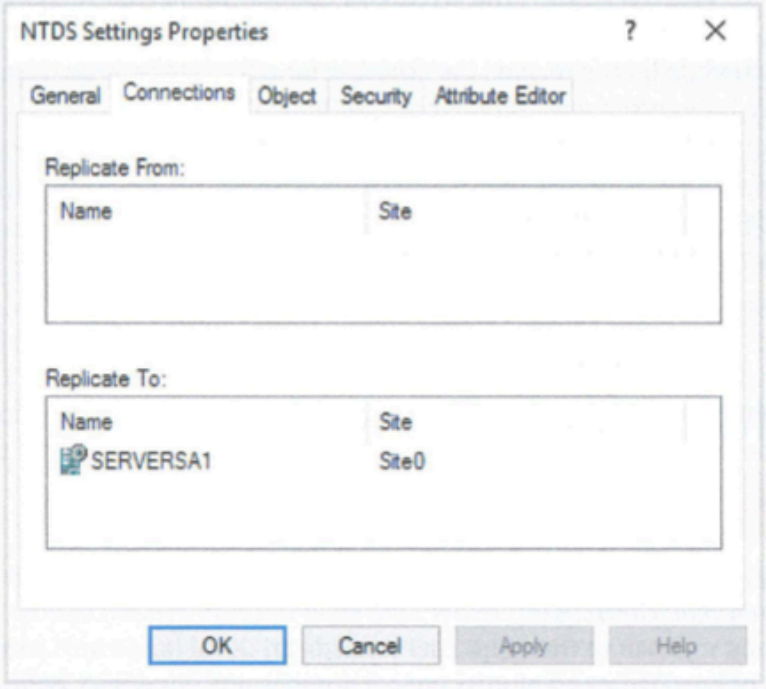


Figure 6-13 NTDS settings for ServerDC1

3. In the left pane, click **Site0**. In the right pane, right-click **NTDS Site Settings** and click **Properties** to open the dialog box shown in Figure 6-14. There are NTDS settings associated with server objects and NTDS site settings associated with site objects.

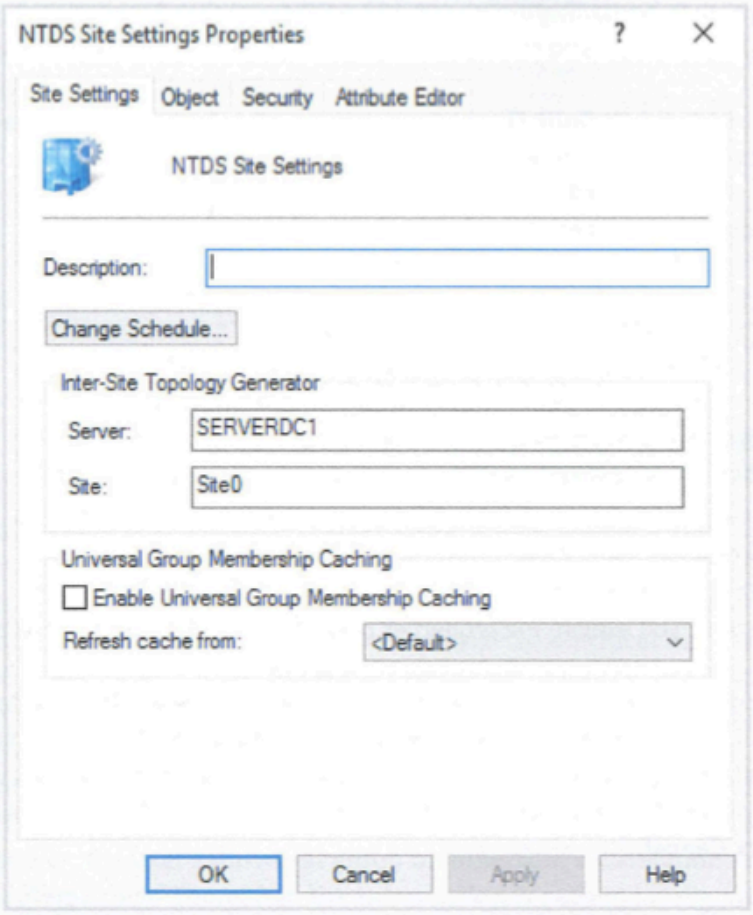
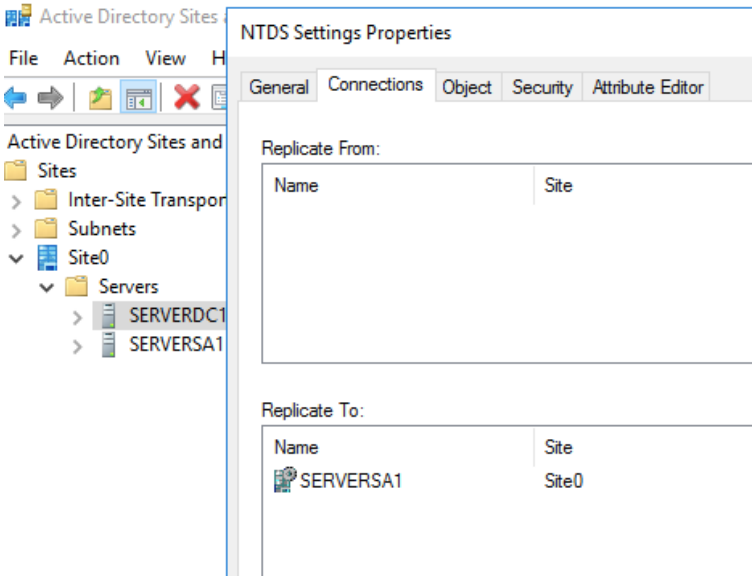
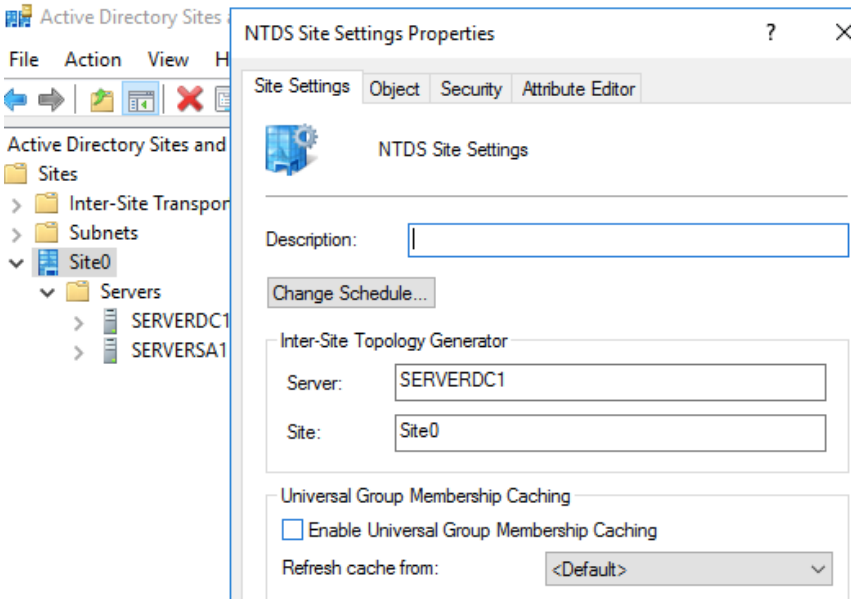
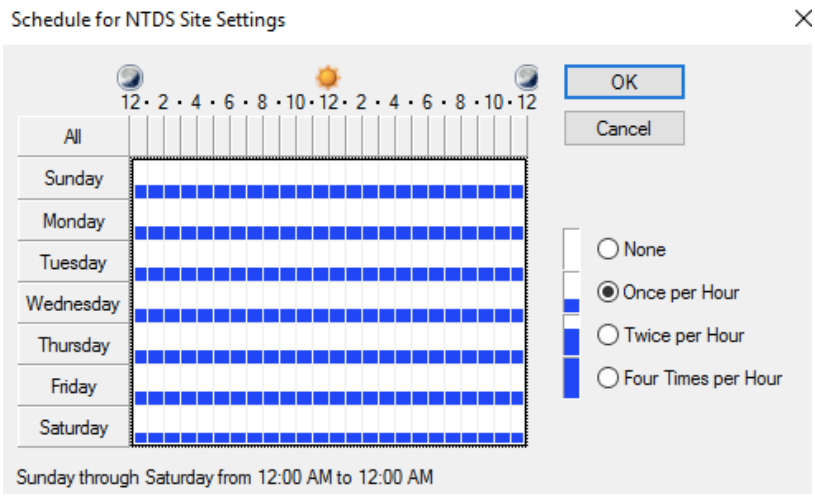


Figure 6-14 The NTDS Site Settings Properties dialog box

4. Click the **Change Schedule** button to open the Schedule for NTDS Site Settings dialog box. As you can see, the regular schedule for intersite replication is once per hour. Click **Cancel**.
5. Notice the Enable Universal Group Membership Caching check box, which is where you enable this feature if the DC isn't a global catalog server. Because it is, enabling this feature has no effect. In the *Refresh cache from* list box, you can select a site for refreshing the cache. Click **Cancel**.
6. Close Active Directory Sites and Services, and continue to the next activity.


Active Directory Sites
File Action View H
Active Directory Sites and
Sites
Inter-Site Transpor
Subnets
Site0
Servers
SERVERDC1
SERVERSA1
NTDS Settings Properties
General Connections Object Security Attribute Editor
Replicate From:
Name Site
Replicate To:
Name Site
SERVERSA1 Site0

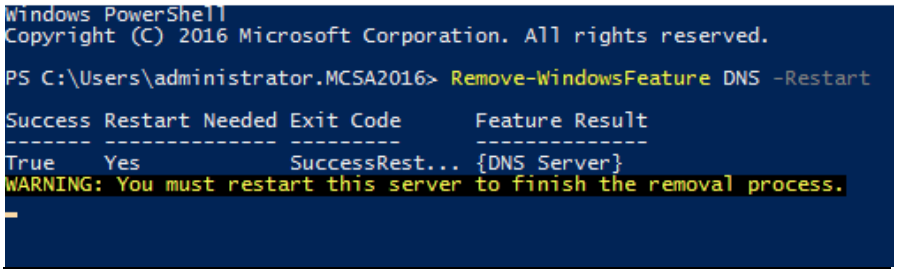

Active Directory Sites
File Action View H
Active Directory Sites and
Sites
Inter-Site Transpor
Subnets
Site0
Servers
SERVERDC1
SERVERSA1
NTDS Site Settings Properties
Site Settings Object Security Attribute Editor
NTDS Site Settings
Description:
Change Schedule...
Inter-Site Topology Generator
Server: SERVERDC1
Site: Site0
Universal Group Membership Caching
Enable Universal Group Membership Caching
Refresh cache from: <Default>

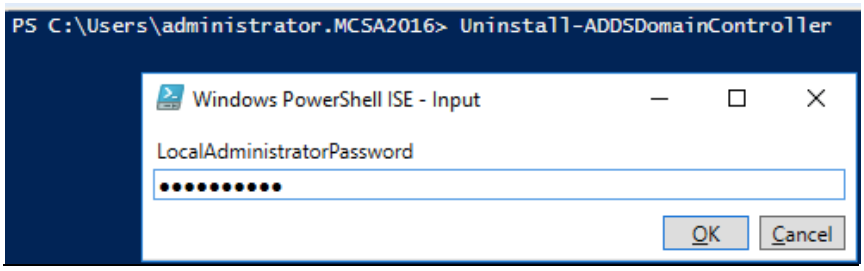


Activity 6-6: Changing a RODC to a standard DC

Time Required: 20 minutes
Objective: Change an RODC to a standard writeable DC.
Required Tools and Equipment: ServerDC1, ServerSA1
Description: You want to transfer some FSMO roles from ServerDC1 to ServerSA1, but first you must change ServerSA1 from an RODC to a standard DC. You use PowerShell for this task.

1. Sign in to ServerSA1 as **Administrator**. On ServerSA1, open a PowerShell prompt. First, uninstall DNS because it's also read only. Type **Remove-WindowsFeature DNS -Restart** and press **Enter**. DNS is removed, and the server restarts.
2. Next, uninstall the domain controller function. This command doesn't remove the role; it just demotes ServerSA1 to being a member server. From a PowerShell window, type **Uninstall-ADDSDomainController** and press **Enter**.
3. When you're prompted for the local administrator password (which you need to sign in to the server when it's no longer a DC), type **Password01**, press **Enter**, type **Password01** to confirm, and press **Enter**.
4. A message states that the server restarts automatically. When you're prompted to continue, press **Enter**. When the operation is finished, ServerSA1 restarts.
5. Sign in to ServerSA1 as **Administrator**. When you installed Active Directory and DNS, the DNS server address in the IP address configuration was set to 127.0.0.1 because this server was a DNS server. You need to set it back to the address of ServerDC1. Open a PowerShell window and type **Set-DnsClientServerAddress -InterfaceAlias Ethernet -ServerAddresses 192.168.0.1** and press **Enter**.
6. Sign in to ServerSA1 as **mcsa2016\Administrator**, and open a PowerShell prompt. Type **Install-ADDSDomainController -DomainName mcsa2016.local -credential (get-credential)** and press **Enter**. When you're prompted for credentials, type **mcsa2016\administrator** and **Password01**.
7. When you're prompted for the safe mode administrator password, type **Password01**, press **Enter**, type **Password01** to confirm, and press **Enter**. Press **Enter** to confirm. The rest of the settings are the defaults for new DCs, which include installing DNS and configuring the paths to C:\Windows. The site is chosen based on the server's IP address, or if no subnets are defined, the default site is used.
8. You see warning messages about default security settings, dynamic IP addresses, and DNS delegation, which you can ignore. When the configuration is finished, the server restarts. Continue to the next activity.





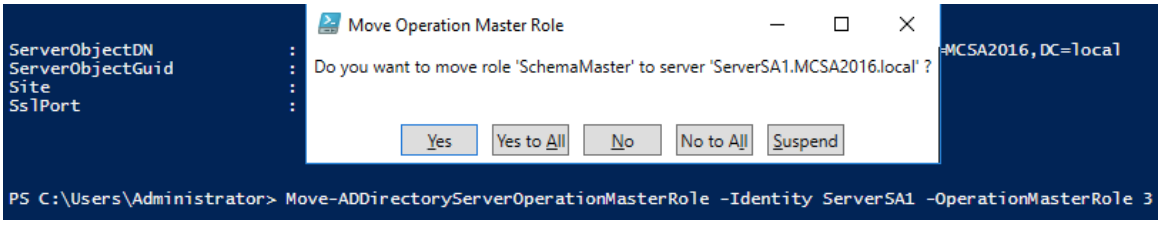

```
 Install-ADDSDomainController
    Determining replication source DC
   Validating environment and user input
      All tests completed successfully
      [oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo]
   Installing new domain controller
      Configuring the DNS Server service on this computer...
 CriticalReplicationComplete
    Critical replication is complete

PS C:\Users\administrator.MCSA2016> Install-ADDSDomainController -DomainName mcsa2016.local -credential (get-credential)


cmdlet Get-Credential at command pipeline position 1
Supply values for the following parameters:
Credential
SafeModeAdministratorPassword: **********
Confirm SafeModeAdministratorPassword: **********

The target server will be configured as a domain controller and restarted when this operation is complete.
Do you want to continue with this operation?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): y
WARNING: Windows Server 2016 domain controllers have a default for the security setting named "Allow cryptography
algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security
channel sessions.

For more information about this setting, see Knowledge Base article 942564
(http://go.microsoft.com/fwlink/?LinkId=104751).

WARNING: A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it
 does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually
create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain
"MCSA2016.local". Otherwise, no action is required.
```

Activity 6-7: Transferring FSMO Roles

Time Required: 15 minutes
Objective: Transfer the schema master and infrastructure master roles.
Required Tools and Equipment: ServerDC1, ServerSA1
Description: In this activity, you transfer the schema master and infrastructure master roles to ServerSA1 using PowerShell.

1. On ServerDC1, open a PowerShell prompt. Type **Get-ADForest** and press **Enter**. Find the output lines listing DomainNamingMaster and SchemaMaster. Both indicate that ServerDC1 is the FSMO role holder for the two forest-wide roles.
2. Type **Get-ADDomain** and press **Enter**. Find the FSMO roles and verify that ServerDC1 is shown as the FSMO role holder for all three domain-wide roles.
3. To see what roles, if any, a server holds, type **Get-ADDomainController** and press **Enter**. Look for the output line OperationMasterRoles, which lists the roles held by the current DC.
4. Now move the schema master role to ServerSA1 by typing **Move-ADDirectoryServerOperationMasterRole -Identity ServerSA1 -OperationMasterRole 3** and pressing **Enter**. The number 3 is the role number for the schema master.
5. When prompted to confirm, press **Enter**. When the operation is finished (no confirmation message, but the PowerShell prompt returns), type **Get-ADForest** and press **Enter**. Verify that the schema master role is now held by ServerSA1. Another way to confirm is to type **Get-ADDomainController -Server ServerSA1** and press **Enter**. It might take a while to display the results.
6. Next, transfer the infrastructure master role by typing **Move-ADDirectoryServerOperationMasterRole -Identity ServerSA1 -OperationMasterRole 2** and pressing **Enter**.
7. Press **Enter** to confirm. To view the domainwide FSMO role holders in an easier-to-read format, type **Get-ADDomain | Format-Table PDCEmulator, RIDMaster, InfrastructureMaster** and press **Enter**. This command displays information about only these three items.
8. You'll need the schema master back on ServerDC1 to enable the Active Directory Recycle Bin in a future activity, so transfer it back by typing **Move-ADDirectoryServerOperationMasterRole -Identity ServerDC1 -OperationMasterRole 3** and pressing **Enter**. Press **Enter** to confirm.
9. Continue to the next activity.

```
PS C:\Users\Administrator> Get-ADDomainController


ComputerObjectDN           : CN=SERVERDC1,OU=Domain Controllers,DC=MCSA2016,DC=local
DefaultPartition           : DC=MCSA2016,DC=local
Domain                     : MCSA2016.local
Enabled                    : True
Forest                     : MCSA2016.local
HostName                   : ServerDC1.MCSA2016.local
InvocationId               : aa6fd034-6f94-4520-83ea-474f04f1413c
IPv4Address                : 192.168.1.1
IPv6Address                : ::1
IsGlobalCatalog            : True
IsReadOnly                 : False
LdapPort                   : 389
Name                       : SERVERDC1
NTDSSettingsObjectDN       : CN=NTDS Settings,CN=SERVERDC1,CN=Servers,CN=Site0,CN=Sites,CN=Configuration,DC=M
                             CSA2016,DC=local
OperatingSystem            : Windows Server 2016 Datacenter Evaluation
OperatingSystemHotfix      :
OperatingSystemServicePack :
OperatingSystemVersion     : 10.0 (14393)
OperationMasterRoles       : {SchemaMaster, DomainNamingMaster, PDCEmulator, RIDMaster...}
Partitions                 : {DC=ForestDnsZones,DC=MCSA2016,DC=local,
                             DC=DomainDnsZones,DC=MCSA2016,DC=local,
                             CN=Schema,CN=Configuration,DC=MCSA2016,DC=local,
                             CN=Configuration,DC=MCSA2016,DC=local...}
ServerObjectDN             : CN=SERVERDC1,CN=Servers,CN=Site0,CN=Sites,CN=Configuration,DC=MCSA2016,DC=local
ServerObjectGuid           : 3b518303-e8c5-4766-842f-78f5b726c932
Site                       : Site0
SslPort                    : 636
```




```
PS C:\Users\Administrator> Get-ADForest


ApplicationPartitions : {DC=DomainDnsZones,DC=MCSA2016,DC=local, DC=ForestDnsZones,DC=MCSA2016,DC=local}
CrossForestReferences : {}
DomainNamingMaster    : ServerDC1.MCSA2016.local
Domains               : {MCSA2016.local}
ForestMode            : Windows2016Forest
GlobalCatalogs        : {ServerDC1.MCSA2016.local, ServerSA1.MCSA2016.local}
Name                  : MCSA2016.local
PartitionsContainer   : CN=Partitions,CN=Configuration,DC=MCSA2016,DC=local
RootDomain            : MCSA2016.local
SchemaMaster          : ServerSA1.MCSA2016.local
Sites                 : {Site0}
SPNSuffixes           : {}
UPNSuffixes           : {}
```