

Module 4 – Network Controller

Estimated Time: 90 minutes

A. Datum Corporation intends to deploy and use Network Controller to manage network services and devices. You need to test a deployment of Network Controller in a lab environment.

Objectives

After completing this lab, students will be able to:

- Prepare for Network Controller deployment.
- Deploy Network Controller.

Lab environment

The lab consists of the following computers:

- LON-DC1 (172.16.0.10) – a Windows Server 2016 domain controller in the adatum.com single-domain forest. You will use it to host a Certification Authority.

In general, you should avoid using AD domain controllers to host PKI roles. We are not following this approach in the lab strictly in order to optimize use of lab VMs. The process of deploying and configuring a Certification Authority server would be identical when using a domain member server.

- LON-SVR1 (172.16.0.11) – a Windows Server 2016 domain member server with Remote Server Administrative tools installed. This server will host the Network Controller server role.

All computers have Windows PowerShell Remoting enabled

Exercise 1: Prepare for a deployment of Network Controller

In this exercise, you will step through preparing a Windows Server 2016 environment for Network Controller deployment. The main tasks for this exercise are as follows:

1. Prepare Active Directory Domain Services on LON-DC1
2. Install and configure an Enterprise CA on LON-DC1
3. Enroll LON-SVR1 for a certificate issued by Enterprise CA

► Task 1: Prepare Active Directory Domain Services and DNS on LON-DC1

1. Sign in to the LON-DC1 Windows Server 2016 lab virtual machine with the following credentials:
 - USERNAME: ADATUM\Administrator
 - PASSWORD: Pa55w.rd
2. Click **Start**, in the Start menu, expand the **Windows Administrative Tools** menu, and then click **Active Directory Administrative Center**.
3. In Active Directory Administrative Center, double-click **adatum.com (local)**, and then click **IT**.
4. In the Tasks pane, in the **IT** section, click **New**, and then click **Group**.
5. In the **Create Group** window, specify the following settings and then click **OK**:
 - Group name: **Network Controller Admins**

- Group (SamAccountName): **Network Controller Admins**
 - Group type: **Security**
 - Group scope: **Global**
 - Members: **ADATUM\Administrator**
6. In the Tasks pane, in the **IT** section, click **New**, and then click **Group**.
 7. In the **Create Group** window, specify the following settings and then click **OK**:
 - Group name: **Network Controller Operators**
 - Group (SamAccountName): **Network Controller Operators**
 - Group type: **Security**
 - Group scope: **Global**
 - Members: **ADATUM\Administrator**
 8. In the Tasks pane, in the **IT** section, click **New**, and then click **User**.
 9. In the **Create User** window, specify the following settings and then click **OK**:
 - Full name: **NCAdmin**
 - User UPN logon: **NCAdmin@adatum.com**
 - User SamAccountName: **ADATUM\NCAdmin**
 - Password: **Pa55w.rd**
 - Confirm password: **Pa55w.rd**
 - Password options: **Password never expires**

You will reference the ADATUM\NCAdmin account when testing installation of Network Controller in the second exercise of this lab.

10. Click **Start**, in the Start menu, expand the **Windows Administrative Tools** menu, and then click **DNS**.
11. In the DNS Manager console, navigate to the **Adatum.com** zone.
12. Right-click **Adatum.com** and, in the right-click menu, click **New Host (A or AAAA)**.
13. In the **New Host** dialog box, type the following and click **Add Host**:
 - Name: **lon-ncrest**
 - IP address: **172.16.0.211**
14. In the **DNS** dialog box, click **OK**.
15. In the **New Host** dialog box, click **Done**.

► Task 2: Install and configure an Enterprise CA on LON-DC1

1. From the LON-DC1 Windows Server 2016 lab virtual machine where you are signed on as USERNAME: ADATUM\Administrator, click **Start** and then click **Server Manager**.

2. In Server Manager, in the **Manage** menu, click **Add Roles and Features**. This will start the **Add Roles and Features Wizard**.
3. On the Select installation type page, ensure that the **Role-based or feature-based installation** option is selected and click **Next**.
4. On the Server destination server page, ensure that **LON-DC1** is selected and click **Next**.
5. On the Select server roles page, select the **Active Directory Certificate Services** check box. When prompted whether to add features that are required for Active Directory Certificate Services, click **Add Features**, and then click **Next**.
6. On the **Select features** page, click **Next**.
7. On the Active Directory Certificate Services page, click **Next**.
8. On the Select role services page, ensure that the **Certification Authority** check box is selected and then click **Next**.
9. On the **Confirm installation selections** page, click **Install**. Wait for the installation to complete.
10. Once the installation completes, click **Configure Active Directory Certificate Services on the destination server**.
11. On the Specify credentials to configure role services, click **Next**.
12. On the Select Role Services to configure page, select the **Certification Authority** checkbox and click **Next**.
13. On the Specify the setup type of the CA page, click **Enterprise CA**, and then click **Next**.
14. On the Specify the type of the CA page, ensure that **Root CA** is selected, and then click **Next**.
15. On the Specify the type of the private key page, ensure that the **Create a new private key** option is selected and then click **Next**.
16. On the Specify the cryptographic options page, set the key length to **4096**, accept the remaining settings with their default values and click **Next**.
17. On the Specify the name of the CA page, specify the following settings and click **Next**:
 - Common name for this CA: **adatum-root-CA**
 - Distinguished name suffix: **DC=adatum,DC=com**
 - Preview of distinguished name: **CN=adatum-root-CA,DC=adatum,DC=com**
18. On the Specify the validity period page, accept the default validity period and click **Next**.
19. On the Specify the database locations page, accept the default location of the certificate database and its log and click **Next**.
20. On the Confirmation page, click **Configure**.
21. Wait until the configuration completes and click **Close**.
22. Back on the Installation progress of the Add Roles and Features Wizard, click **Close**.

► **Task 3: Enroll LON-SVR1 for a certificate issued by Enterprise CA**

1. Sign in to the LON-SVR1 Windows Server 2016 lab virtual machine with the following credentials:

- USERNAME: ADATUM\Administrator
 - PASSWORD: Pa55w.rd
2. While signed in to LON-SVR1 as ADATUM\Administrator, click **Start** and then run **Windows PowerShell** as an administrator.
 3. From the **Administrator: Windows PowerShell** window, type the following and press Enter:

```
gpupdate /target:computer /force  
certlm
```

This will open the Microsoft Management Console (MMC) with the **Certificates - Local Computer** snap-in loaded.

4. Expand the **Certificates - Local Computer** top level node, right-click the **Personal** folder, click **All Tasks**, and click **Request New Certificate**. This will start the **Certificate Enrollment** wizard.
5. On the **Before You Begin** page, click **Next**.
6. On the **Select Certificate Enrollment Policy** page, ensure that **Active Directory Enrollment Policy** is selected and click **Next**.
7. On the **Request Certificates** page, select the checkbox next to the **Computer** certificate and click **Enroll**.
8. On the Certificate Installation Results page, click **Finish**.

Results: After completing this exercise, you will have prepared Active Directory domain for deployment of Network Controller, installed Enterprise CA, and enrolled LON-SVR1, which will be hosting the Network Controller server role, for a Computer certificate issued by the Enterprise CA.

Exercise 2: Deploy Network Controller

Now that you have prepared for Network Controller deployment, it is time to implement it and validate its functionality. The main tasks for this exercise are as follows:

1. Install the Network Controller server role on LON-SVR1
2. Configure the Network Controller cluster on LON-SVR1
3. Test the deployment of Network Controller on LON-SVR1

► Task 1: Install the Network Controller server role on LON-SVR1

1. While signed in to LON-SVR1 as ADATUM\Administrator, click **Start** and then click **Server Manager**.
2. From the **Manage** menu in **Server Manager**, select **Add Roles and Features**. This will launch **Add Roles and Features Wizard**.
3. On the **Before you begin** page, click **Next**.
4. On the **Select installation type** page, ensure that **Role-based or feature-based installation** option is selected and click **Next**.
5. On the **Select destination server** page, ensure that the local server is selected and click **Next**.
6. On the **Server Roles** page, select the **Network Controller** checkbox and click **Next**.

7. In the **Add features that are required for Network Controller** window, click **Add Features** and click **Next**.
8. On the **Select features** page, click **Next**.
9. On the **Network Controller** page, click **Next**.
10. On the **Confirm installation selections** page, select the **Restart the destination server automatically if required** checkbox, click **Yes** when prompted for confirmation, and click **Install**. Wait for the installation to complete.
11. Wait until the configuration completes, review the detailed operation results, and click **Close**.
12. Back on the Installation progress of the Add Roles and Features Wizard, click **Close**.
13. Restart LON-SVR1.

► Task 2: Configure the Network Controller cluster on LON-SVR1

1. Sign back in to the LON-SVR1 Windows Server 2016 lab virtual machine with the following credentials:
 - USERNAME: ADATUM\Administrator
 - PASSWORD: Pa55w.rd
2. While signed in to LON-SVR1 as ADATUM\Administrator, click **Start**, right-click **Windows PowerShell**, in the right-click menu click **More** and then click **Run as administrator**.
3. From the **Administrator: Windows PowerShell** window, type the following and press Enter:

```
$node = New-NetworkControllerNodeObject -Name "Node1" -Server "LON-SVR1.adatum.com" -FaultDomain "fd://londc1/rack1/host1" -RestInterface "Ethernet"
```

This creates a Network Controller node object, which will be subsequently used to create a Network Controller cluster. The value of fault domain designates physical location of the server hosting the node, to allow the clustering services to increase resiliency by distributing Network Controller nodes across separate fault domains. Since you are deploying a single node, its value is not relevant here, but it would be important in multi-node deployments.

4. From the **Administrator: Windows PowerShell** window, type the following and press Enter:

```
$cert = Get-Item Cert:\LocalMachine\My | Get-ChildItem | where {$_.Subject -imatch 'LON-SVR1' }
```

This identifies the Computer certificate that will be used to facilitate encryption of Network Controller cluster communication.

5. From the **Administrator: Windows PowerShell** window, type the following and press Enter:

```
Install-NetworkControllerCluster -Node $node -ClusterAuthentication Kerberos -ManagementSecurityGroup "Adatum\Network Controller Admins" -CredentialEncryptionCertificate $cert
```

This installs a Network Controller cluster, which, in our case, consists of a single node only.

- From the **Administrator: Windows PowerShell** window, type the following and press Enter:

```
Install-NetworkController -Node $node -ClientAuthentication Kerberos -
ClientSecurityGroup "Adatum\Network Controller Operators" -RestIpAddress
"172.16.0.211/24" -ServerCertificate $cert
```

This adds the node into the newly installed cluster and assigns the IP address you designate to its REST endpoint on the interface you specified when creating the node object.

► Task 3: Test deployment of Network Controller on LON-SVR1

You will start the test by creating a Network Controller Credential resource. You can use credential resources to provide security context during operations that require authentication, such as, for example, backups of Network Controller database.

- While logged on to LON-SVR1 as ADATUM\Administrator, right-click **Start** and then click **Windows PowerShell (Admin)**.

- From the **Administrator: Windows PowerShell** window, type the following and press Enter:

```
$cred = New-Object Microsoft.Windows.NetworkController.CredentialProperties
```

- From the **Administrator: Windows PowerShell** window, type the following and press Enter:

```
$cred.Type = 'usernamePassword'
```

- From the **Administrator: Windows PowerShell** window, type the following and press Enter:

```
$cred.UserName = 'ADATUM\NCAdmin'
```

- From the **Administrator: Windows PowerShell** window, type the following and press Enter:

```
$cred.Value = 'Pa55w.rd'
```

- From the **Administrator: Windows PowerShell** window, type the following and press Enter:

```
New-NetworkControllerCredential -ConnectionUri https://LON-SVR1.adatum.com -
Properties $cred -ResourceId AdminUser
```

- Press **Y**, and then press Enter when prompted

- From the **Administrator: Windows PowerShell** window, type the following and press Enter:

```
Get-NetworkControllerCredential -ConnectionUri https://LON-SVR1.adatum.com -
ResourceId AdminUser
```

- Verify that you have received an output similar to the following:

```
Tags          :
ResourceRef   : /credentials/AdminUser
InstanceId    : e16ffe62-a701-4d31-915e-7234d4bc5a18
Etag         : W/"1ec59631-607f-4d3e-ac78-94b0822f3a9d"
ResourceMetadata :
ResourceId    : AdminUser
Properties    : Microsoft.Windows.NetworkController.CredentialProperties
```

Next, you will validate the status of the Network Controller deployment by running the **Debug-NetworkControllerConfigurationState** cmdlet.

10. From the **Administrator: Windows PowerShell** window, type the following and press Enter:

```
$cred = Get-Credential
```

11. When prompted, in the **Windows PowerShell credential request** dialog box, in the **User name** text box, type **ADATUM\Administrator**, in the **Password** text box, type **Pa55w.rd**, and click **OK**.
12. From the **Administrator: Windows PowerShell** window, type the following and press Enter:

```
Debug-NetworkControllerConfigurationState -NetworkController "LON-SVR1.adatum.com" -RestURI "https://lon-ncrest.adatum.com" -Credential $cred
```

13. Verify that you have received an output like the following (with no configuration state messages that would indicate an issue):

```
Fetching ResourceType: accessControlLists
Fetching ResourceType: servers
Fetching ResourceType: virtualNetworks
Fetching ResourceType: networkInterfaces
Fetching ResourceType: virtualGateways
Fetching ResourceType: loadbalancerMuxes
Fetching ResourceType: Gateways
```

Results: After completing this exercise, you will have deployed Network Controller and tested its functionality.