Domain Setup

DNS, Domain Controller, User Management, and Security

Table of Contents

Overview

This module will discuss domain setup in Windows Server environment. Below are the specification of the environment used by this module:

Specification	
Operating System	Windows Server 2012 R2
RAM	36GB
Hard Disk	1TB

The server that will be used is Valencia server (10.22.64.131). This server is used as a DNS Server where we insert a new domain. This server is also the domain controller for slc.net domain, where it's used for authenticate users in SLC domain. Do note that computer at 724 is also in this domain which means users in SLC domain can log in there.

DNS

DNS is a system for naming computers and network services. This naming locates computers and services in a user friendly name. DNS can resolve name to other information, such as IP address.

There are two type of DNS zone, forward lookup zone and reverse lookup zone. Forward lookup zone is used for obtaining information such as IP address from domain name (host to IP), and reverse lookup zone provides mapping to domain name from an IP address (IP to host).

Add Zone and Domain

To add a new zone to forward lookup zone, follow the steps below:

1. Open DNS Manager
2. Choose **New Zone…** from the context menu of forward lookup zone
3. Select the zone type

   Primary zone is a zone maintained in this server.

   Secondary zone is a copy of zone that is maintained on other DNS server.

   Stub zone is for information about the authoritative name server for this zone
4. Set the zone name which will also be the domain name

Add Subdomain

To add a subdomain to a domain, follow the steps below:

1. Open DNS Manager
2. Choose **New Domain…** from the context menu of the domain
3. Set the subdomain name

Add Host to Forward Lookup Zone

To add a host to a domain or subdomain, follow the steps below:

1. Open DNS Manager
2. Choose **New Host…** from the context menu of the domain or subdomain
3. Set the host name and its IP address
4. If you want to add this host to the reverse lookup zone, then enable the **Create associate pointer (PTR) record**

If there are more than one host to add, then it's more convenient to use this command line:

```
DnsCmd <ServerName> /RecordAdd <Zone> <NodeName> [/Aging] [/OpenAcl] [/CreatePTR]
[<Ttl>] <RRType> <RRData>
```

For example if you want to add the hostname **module** to **binus** zone on this DNS server, with the IP address of **10.22.64.70** and also wants to add a reverse lookup to it, then the command is:

```
DnsCmd localhost /RecordAdd binus module /CreatePTR A 10.22.64.70
```

Add Pointer to Reverse Lookup Zone

To add a pointer to a domain name from an IP address, follow the steps below:

1. Open DNS Manager
2. Choose **New Pointer (PTR)…** from the context menu of a reverse lookup zone
3. Set the IP address

   Note that the IP address is not the complete address, but just the rest of address after the zone name, and the order is reversed in group. For example 10.22.64.130 in zone 22.10 becomes 130.64.
4. Set the host name for this IP address

Do note that you don't have to manually add a pointer to reverse lookup zone if the host is managed by this DNS server, you just need to check the **Create associate pointer (PTR) record** when creating the host.

Domain Controller

Domain controller is a server that responds to security authentication requests within a Windows domain. Each user in a Windows domain is assigned access to resources within the domain.

Setup New Domain Controller

We'll configure domain controller using UI through Server Manager, the steps are:

1. Open Server Manager
2. Click **Mange**, and select **Add roles and features**
3. On the step **Installation Type**, choose **Role-based or feature-based installation**
4. Select the server to be the domain controller
5. On the step **Server Roles**, choose **Active Directory Domain Services**
6. Follow the wizard and do the installation
7. After the installation is complete, open the notification in Server Manager, and click **Promote this server to a domain controller**
8. On the step **Deployment Configuration**:
    a. Select **Add a domain controller to an existing domain** to install an additional domain controller in an existing domain.
    b. Select **Add a new domain to an existing forest** and **Child Domain** as thee domain type to install a new child domain.
    c. Select **Add a new domain to an existing forest** and **Tree Domain** as the domain type to install a new domain tree.
    d. Select **Add a new forest** to install a new forest.
9. On the step **Domain Controller Options**:
    a. If creating a new domain or forest, then determine the **Forest Functional Level** and **Domain Functional Level**, whether or not this should be DNS Server, and DSRM username and password.
    b. If adding a domain controller to an existing domain, then determine the configuration of DNS Server, Global Catalog, and Read Only Domain Controller, determine the site name, and type the DSRM password.

Forest Functional Level and **Domain Functional Level** will affect the features available to forest and domain, where higher operating systems have more functionality considering the operating systems available.

Global Catalog is enabled by default as this is the first domain controller in the forest, which will makes the domain controller stores a copy of all Active Directory objects in the forest in order to improve the performance of querying object.

It's recommended to enable **DNS Server** and **Global Catalog** for high availability in a distributed environments.

Read Only Domain Controller is a domain controller that host complete, read-only copies of Active Directory database partitions and a read only copy of the SYSVOL folder contents.

10. Follow the wizard and install.

Remove Domain Controller

To remove domain controller, follow the steps below:

1. Open Server Manager
2. Click **Manage**, and select **Remove Roles and Features**
3. Select the server to remove
4. On the step **Remove server roles**, clear the checkbox for **Active Directory Domain Services**
5. Follow the wizard, and then there should be a validation error as the domain controller is currently active. To proceed, click **Demote this domain controller**
6. Follow the wizard to demote domain controller
7. After the demotion finished, redo the steps to remove **Active Directory Domain Services**

User Management

The Active Directory user that we manage can be used for doing network authentication or accessing other domain services.

Add New Domain User

To add new user to Active Directory, follow the steps below:

1. Open Active Directory Users and Computer
2. Select the domain e.g. slc.net
3. Choose **New > User** from the context menu
4. Fill in the form

If there are more than one user to add, then it's more convenient to use this command line:

```
dsadd user <UserDN>
```

For example if you want to add a user named **module** in domain **slc.net**, then the command will look like:

```
dsadd user CN=module,CN=Users,DC=slc,DC=net
```

For more information about the command, run the command **dsadd user /?**

Add New Domain Group

To add new group to Active Directory, follow the steps below:

1. Open Active Directory Users and Computer
2. Select the domain e.g. slc.net
3. Choose **New > Group** from the context menu
4. Fill in the form

   Universal scope can contains accounts and groups from any domain in the forest.

   Global scope can contains accounts and groups in the same parent group.

   Domain local scope can contains groups in its own domain, and accounts from any domain in the forest, but only domain local group in the same parent group.

   Distribution group can be used only with e-mail applications such as Exchange.

   Security group can be listed in discretionary access control lists, e.g. remote desktop.

Add New Domain Computer

To add new computer to Active Directory, follow the steps below:

1. Open Active Directory Users and Computer
2. Select the domain e.g. slc.net
3. Choose **New > Computer** from the context menu
4. Fill in the form

If there are more than one computer to add, then it's more convenient to use this command line:

```
dsadd computer <ComputerDN>
```

For example if you want to add a computer named **module** in domain **slc.net**, then the command will look like:

```
dsadd computer CN=module,CN=Computers,DC=slc,DC=net
```

For more information about the command, run the command **dsadd computer /?**

Assign Domain User to Group

There are several built in roles that a user can be assigned to, such as **Remote Desktop Users**. By default, a user will be assigned to **Domain User** group. To assign a domain user in to a group, follow the steps below:

1. Open Active Directory Users and Computer
2. Select the domain e.g. slc.net
3. Select **Users**
4. Double click on the user
5. Go to tab **Member Of**
6. Click **Add** and find the group

Security

Managing Access Control Permission

Access control limits what a user can or cannot do to an object, for example operations on file are read, write, and execute. To manage the permission on a file, follow the steps below:

1. Open the properties of the file
2. On the **Security** tab, click **Edit…**
3. Add or remove user or group to control the permission of this file
4. Allow or deny the related permission for this file and user

Managing Object Ownership

Owner of an object controls how permission are set on the object. The default owner is the user who creates the object. Owner will always be able to change the permission of the object, even if the owner is denied all access to it. Administrator needs to take ownership of the object before changing permission.

To change the owner of a file, follow the steps below:

1. Open the properties of the file
2. On the **Security** tab, click **Advanced**
3. Click **Change** and select the new owner

Windows Logon via Domain Authentication

To enable Windows logon with domain user, the Windows desktop should be added as a domain computer first, and set the computer to join that domain. To join a domain, follow the steps below:

1. Open **System Properties** via **Control Panel\System and Security\System**
2. Click **Change settings** at **Computer name, domain, and workgroup settings**
3. Click **Change…**
4. Type in the domain name e.g. slc.net