Upgrading and Deploying
Windows Server 2012
In the Legal Environment
# Table of Contents

Purpose of This Lab ........................................................................................................................... 3  
Lab Environment ............................................................................................................................... 3  
Presenter .......................................................................................................................................... 3  
Exercise 1 – Add Roles and Features ............................................................................................ 4  
Exercise 2 – Promote the Server to a Domain Controller .............................................................. 5  
Exercise 3 – Verify Domain Controller Promotion .......................................................................... 9  
Exercise 4 – Update Servers (and clients) to Support Domain Controller Migration .................. 12  
Exercise 5 – Move Operations Master (FSMO) Roles .................................................................. 16  
Exercise 6 – Demote Windows Server 2008 R2 Domain Controller ............................................ 20  
Exercise 7 – Verify Domain Controller Demotion and Finish Clean up ........................................ 21  
Exercise 8 – Raise the Domain and Forest Functional Levels to Windows 2012 ......................... 22  
Exercise 9 – Use Security Configuration Wizard .......................................................................... 23
Purpose of This Lab
This lab is designed to provide IT staff and management experience deploying Windows Server 2012, including upgrading Active Directory Domain Services and using Windows Security Configuration Wizard to secure servers. The exercises will walk you through a full Active Directory upgrade including moving operations master (FSMO) roles and decommissioning a Windows 2008 R2 domain controller. A general familiarity with Windows Server 2012 and completion of HAND6A: Implementing and Using Windows Server 2012 in the Legal Environment is assumed.

Lab Environment
This lab consists of two Windows Server 2012 virtual machines installed on a Windows Server 2008 R2 Hyper-V environment.

**IMPORTANT**
DO NOT USE THE CTRL-ALT-DEL KEY SEQUENCE, AS IT WILL DISRUPT YOUR VIRTUAL SERVER SESSION. You should use the CTRL-ALT-END key sequence instead.

You may use the CTRL – ALT – DEL button in the Hyper-V session console as well.

Server Information
The virtual machines for this lab all begin with HAND6, not all HAND6 virtual machines will be used for this lab.

<table>
<thead>
<tr>
<th>Virtual Machine</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>hand6a-win08dc</td>
<td>Windows Server 2008 R2 Domain Controller</td>
</tr>
<tr>
<td>hand6awin2012dc</td>
<td>Windows Server 2012 R2 Member Server</td>
</tr>
</tbody>
</table>

User Accounts
The following user accounts will be needed for this lab

<table>
<thead>
<tr>
<th>User</th>
<th>Domain</th>
<th>Password</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>ILTAadmin</td>
<td>ILTA2013.local</td>
<td>P@SSw0rd (0 = zero)</td>
<td>Primary Test Account</td>
</tr>
<tr>
<td>Administrator</td>
<td>N/A</td>
<td>P@SSw0rd (0 = zero)</td>
<td>Local Test Account</td>
</tr>
</tbody>
</table>

Presenter
Patrick Sklodowski
Sklodowski Consulting LLC
Independent Consultant

Pat@Sklodowski.com
856-425-0029
Exercise 1 – Add Roles and Features

Install the Roles and Features required to support Active Directory Domain Services.

1. Logon to hand6awin2012dc
2. Add a new role using one of the following methods

   - In Server Manager, use the Manage Drop Down and select Add Roles and Features
   - Or in Server Manager, All Servers, use the Tasks drop down in the Add Roles and Features section
   - Follow the Add Roles and Features Wizard as follows:
     - Next on the Before You Begin screen
     - Next on the Installation Type screen
     - Verify hand6awin2012dc is selected on the Server Selection Screen and click Next
     - On the Select Server Roles screen, select the following roles. If a dialog opens asking to add related features, select Add Features
       - Active Directory Domain Services
       - DNS Server
       - Click Next
     - On the Features screen, select Group Policy Management
     - Next on the Active Directory Domain Services screen
     - Next on the DNS Server screen
On the Confirmation screen, check the box to Restart if required

Confirm the restart
Click Install
Close the installation window

Status may be viewed by selecting the Notification Area

Click the Notification icon to see the status

Select Task Detail to see additional information
Wait for installation to complete
Check Notification area to determine when the installation is complete. The notification will state configuration is required. Ignore this for now
The server may reboot, if it does, installation is complete

Exercise 2 – Promote the Server to a Domain Controller

Use the Active Directory Domain Services Configuration Wizard to promote the server to a domain controller. This lab will allow the wizard to upgrade the Active Directory Schema to support Windows Server 2012 domain controllers. In a small environment, a single physical site with one domain in the forest and few domain controllers, using the wizard to upgrade the schema is an acceptable process. For a large environment, multiple physical sites or multiple domains within a forest, the schema should be upgraded and validated before running through the domain controller promotion process.

1. Logon to hand6awin2012dc
2. Open Server Manager and select AD DS (Active Directory Domain Services)
3. Select More in the status message

4. In Task Details, Select **Promote this server to a domain controller**

5. Follow the Active Directory Domain Services Configuration Wizard to promote the server to a domain controller.
   - On the Deployment Configuration screen
     - Ensure **Add a domain controller to an existing domain** is selected
     - Verify the domain name is ILTA2013.local
     - Verify the user performing the operation has the correct permissions
   - On the Domain Controller Options screen, verify the following options are selected
     - Domain Name System (DNS) server
     - Global Catalog (GC)
     - In a multi-site environment, verify the Site Name is correct
☐ Type “P@SSw0rd” (without quotes) into the Directory Services Restore Mode (DSRM) Password fields

☐ Ignore the warning that appears on the DNS Options screen

☐ Select Next on the Additional Options screen
☐ Use the default file paths on the Paths screen

☐ Select Next to prepare the schema
☐ Review the selections to confirm the correct options were chosen
Select View Script to see the PowerShell command that will be executed to perform this installation

- This command could be run directly from PowerShell

```powershell
# Windows PowerShell script for AD DS Deployment

Import-Module ADDSDeployment
Install-ADSDomainController -NoGlobalCatalog:$false
-CreateDnsDelegation:$false -CriticalReplicationOnly:$false
-DatabasePath "C:\Windows\NTDS"
-DomainName "ilta2013.local"
-InstallDns:$true
-LogPath "C:\Windows\NTDS"
-NoRebootOnCompletion:$false
-SiteName "Default-First-Site-Name"
-SysvolPath "C:\Windows\SYSVOL"
-Force:$true
```

- Select Next to scan for all required prerequisites
- Review the results of the prerequisite check and verify no issues will prevent the domain controller promotion.

It is possible some warning will occur in a production environment; however, these warnings may not prevent the upgrade. It is important to understand all warnings and errors, rectify those issues that may prevent the upgrade from completing.

- Click Install to start the process
Exercise 3 – Verify Domain Controller Promotion

Verify the domain controller promotion was successful.

1. Logon to hand6awin2012dc
2. Wait for Server Manager to launch
3. Go to AD DS node in Server Manager
4. Review events to ensure server was properly promoted
   - Under AD DS, go to the Events section

- Watch the status
- The server should reboot upon completion. If the server prompts to reboot, please follow steps to reboot

- Change the event filtering
  - In the Tasks menu select Configure Event Data
Check the box to include Informational events and click OK

Review the events

- Warnings are generally expected and provide notification of tasks that have not yet completed
- It may take a few minutes for the entire AD promotion to complete
- Scan for the following successful events.
  - Note: The full Event Viewer tool can be used to look for these events. The screen shots below include those from the full Event Viewer tool.

Events that show a successful domain controller promotion

- Active Directory Domain Services started successfully
All problems that were preventing Active Directory from starting have been cleared. These “problems” are normal for the first few minutes after a server has been promoted.

DFS replication has successfully started.
5. **Confirm DNS Entries**

- Open DNS Manager under the Tools, or as shown

- Look through the _msdcs.ila2013.local zone and verify records have been created for hand6awin1012dc. Look through each of the sub-domains

---

**Exercise 4 – Update Servers (and clients) to Support Domain Controller Migration**

Member servers; clients; network devices; and in some cases, other domain controllers must be modified in support of the domain controller migration. These updates may include, but are not limited to, changing DHCP scopes, certificate services, manually updating client and member server TCP/IP settings, moving DFS roots; or updating LDAP authentication settings on network devices.

1. Logon to hand6awin2012dc
2. Update the TCP/IP properties on hand6awin2012dc
   - Open the network configuration using one of the following methods:
     - Method 1 – Right click on the network icon in the task bar and select **Open Network and Sharing Center**
Method 2 – Open the Windows Charm and select Settings
  - Under Settings, choose Control Panel

Select Network and Internet

Click Network and Sharing Center

In the Network and Sharing Center window, select Change Adapter Settings
- Right click on the network adapter – **Ethernet X** (there should only be one adapter) and select **Properties**

- **Highlight Internet Protocol Version 4** and select **Properties**

- **Change the DNS server setting to 127.0.0.1 (localhost)**

- **Click OK twice and close any remaining windows**
3. Logon to hand6a-win08dc
4. Update the TCP/IP properties on hand6a-win08dc

- Right click on the network icon in the task bar and select **Open Network and Sharing Center**

- In the Network and Sharing Center window, select **Change Adapter Settings**

- Right click on the network adapter – **Ethernet X** (there should only be one adapter) and select **Properties**

- Highlight **Internet Protocol Version 4** and select **Properties**
- Change the DNS server setting to 192.168.11.4

![Image of DNS configuration]

- Click OK twice and close any remaining windows

Exercise 5 – Move Operations Master (FSMO) Roles

The operations masters (Flexible Single Master Operations) are five functions which only run on one server per forest or domain. These roles must be moved from the old domain controller before it is decommissioned.

1. Logon to hand6a-win08dc
   - Note: These steps may be performed on the Windows Server 2012 domain controller as well
2. Prepare management console
   - Click `Start` and type the following into the search bar: `Regsvr32 C:\Windows\System32\schmmgmt.dll`
   - Press Enter key and confirm success
   - This step makes the Active Directory Schema management console available for use

- Click `Start` and type “MMC” (without quotes) and press Enter key to open a new management console
- Go to `File` – `Add/Remove Snap-in`
Add the following Snap-ins

- Active Directory Domains and Trusts
- Active Directory Schema
- Active Directory Sites and Services
- Active Directory Users and Computers

Click OK

3. Move Operations Master roles
   - Move Forest Level Operations Master Roles
   - Move Domain Naming Master (forest level role)
     - Select and right click on Active Directory Domains and Trusts and select Change Active Directory Domain Controller
Select hand6awin2012dc and click OK

Right click on Active Directory Domains and Trusts and select Operations Master

Verify hand6awin2012dc is listed in the second field as the server the role will be transferred to

Click Change and confirm the operations
Select OK to close the notification

![Image of Operations Master successfully transferred]

Note: For the remaining roles, screenshots will only be shown where steps differ from the Domain Naming Master

- Move Schema Master (forest level role)
  - Select and right click on Active Directory Schema and select Change Active Directory Domain Controller
  - Select hand6awin2012dc and click OK
  - Right click on Active Directory Schema and select Operations Master
  - Verify hand6awin2012dc is listed in the second field as the server the role will be transferred to
  - Click Change and confirm the operations
  - Select OK to close the notification

- Move Domain Level Operations Master Roles
  - Expand Active Directory Users and Computer and select the ILTA2013.local domain
  - Right click on ILTA2013.local and select Change Active Directory Domain Controller
  - Select hand6awin2012dc and click OK
  - Right click on ILTA2013.local and select Operations Master
For each of the three roles (tabs) move the operations master role

When complete, select Close

Exercise 6 – Demote Windows Server 2008 R2 Domain Controller

The Windows 2008 R2 Domain controller must have Active Directory Services cleanly removed.

1. Logon to hand6a-win08dc
2. Click start and type the following into the search bar and press Enter

3. Demote the domain controller
   - Walk through the Active Directory Domain Services Installation Wizard to remove Active Directory from this server
   - Select Next on the welcome screen
   - Select Next on the Delete the Domain screen
   - Do NOT select the box stating this is the last domain controller in the domain.
   - Enter a new password for the local administrator for after the server has been demoted.
     - Enter “P@SSw0rd” (without quotes)
   - Select Next on the Summary screen
Exercise 7 – Verify Domain Controller Demotion and Finish Clean up

Verify the domain controller has been cleanly uninstalled.

1. Logon to hand6a-win08dc as domain administrator. If it is not possible to logon as domain administrator, use the local administrator account
2. Check Event Viewer for errors
3. Logon to hand6awin2012dc
4. Open Active Directory Users and Computers and verify the computer account for hand6a-win08dc was moved from the Domain Controllers OU into the Computers container
5. Open Active Directory Sites and Services and validate hand6awin2012dc is no longer a domain controller

- Open AD sites and services
- Expand the top level, Sites and Default-First-Site-Name
- hand6a-win08dc will be listed but there should be nothing under this node

- Right click on hand6a-win08dc and delete it
6. Open DNS console

- Check the _msdcs zone and make sure all references to hand6a-win08dc are removed

Exercise 8 – Raise the Domain and Forest Functional Levels to Windows 2012

Raising the functional levels will enable all features of Windows Server 2012 Active Directory. This process cannot be completed if older domain controllers still exist in the domain. Once this task has been performed, older servers cannot be promoted to be a domain controller.

1. Logon to hand6awin2012dc
2. Open Active Directory Forests and Trusts
3. Raise the domain functional level

- Drill down to and right click on ILTA2013.local and select Raise Domain Functional Level

- In the drop down, select Windows Server 2012. Because this domain was already at Windows 2008 R2 level, there are no other options
4. Raise the forest functional level

- In Active Directory Domains and Trusts, right click on **Active Directory Domains and Trusts** and select **Raise Forest Functional Level**

- In the drop down, select Windows Server 2012. Because this domain was already at Windows 2008 R2 level, there are no other options

- Select OK to confirm the action
- Select Ok to complete.

**Exercise 9 – Use Security Configuration Wizard**

Security Configuration Wizard can be used to create security policy templates for deployment to one or many machines. The wizard can read the security settings from an existing machine to build a template. Templates can be converted to Group Policy for centralized management and deployment.

1. Logon to hand6awin2012dc
2. Open Security Configuration Wizard
3. Create a new security policy

- Walk through the wizard to create a new policy
Select hand6awin2012dc as the server to use as the baseline for the policy.

When the baseline processing is complete, select Next.

Keep the default selected client features. These are the features found on the baseline server.

Continue to step through the wizard, review each screen, and make changes as you desire.

Take a minute to understand how each of the settings affect the servers they are applied to.

When prompted to save the security policy, save using the following settings.

Select Apply Later.
4. Apply policy the Security Policy to a single machine

- Open Security Configuration Wizard
- Step through the wizard and when prompted for the **Configuration Action**, select **Apply an existing policy**

5. Apply policy the Security Policy to multiple machines using Group Policy
Open Group Policy Management console
Browse to Group Policy Objects (as shown)

Notice there are two group policies
Open PowerShell and type the following command on a single line and press Enter. This will convert the security policy template to a group policy

```
scwcmd transform /p:C:\Windows\security\msscw\Policies\ilta-DC-security-policy.xml /g:ILTA-DomainController-Security-Policy
```

Switch back to Group Policy Management Console
Right click on Group Policy Objects and select Refresh

Note the new policy has been created
Explorer the new policy and apply as appropriate.