<Date>

CyberApprentice

Deploy Active Directory with VCSA

By CyberApprentice

Table of Contents

[**Introduction** 2](#_Toc55429559)

[**Materials and References** 2](#_Toc55429560)

[**Installing Active Directory Domain Controller** 2](#_Toc55429561)

[**Configuring AD DC** 7](#_Toc55429562)

[**Installing ESXi** 8](#_Toc55429563)

[**Installing VCSA** 9](#_Toc55429564)

[**Securing** 10](#_Toc55429565)

[**Troubleshooting** 10](#_Toc55429566)

# **Introduction**

For so long, I believed that Active Directory was a system administrator’s focus and rarely bothered to learn more. The signs were all around, but it took me way too long to realize its importance. My first internship interview consisted of one of the interviewers asking about my Active Directory knowledge. It was for a information assurance consulting department. I shadowed my superiors as they worked on a daily basis and there were many occurrences that were relative to the domain controllers. I was a part of many conversations but was left as the least knowledgeable because I didn’t understand the policy structure, the capabilities, the architecture, and as a result, I lacked a sector of solutions to offer or provide by just knowing that there was a policy available. Today was the final straw when a previous superior/mentor viewed an environment and pointed out flaws relative to Active Directory’s security groups. Prior to this writing, I’ve set up a domain controller once and watched one, maybe two videos on an introduction to Active Directory. I’m also familiar with its open-source, Linux counterpart, LDAP, but never learned much of any about it. This writing will conduct a hands-on lab experience of setting up an Active Directory domain with security capabilities implemented. The goal is to have a better understanding of the capabilities and potential issues with Active Directory as I will also take the initiative to attack the experimental domain using FireEye’s Commando, a Window’s pentesting appliance.

# **Materials and References**

\* = This parameter is unique to my environment and be different for yours. Adjust accordingly.

# **Installing Active Directory Domain Controller**

Resources:

1. Install a Windows 2016 Server\*
   1. Give the Administrator account a password
   2. [OPTIONAL] tweaks
      1. Power settings to not sleep
2. Update and create snapshot/template
3. Statically set the IPv4 address = 192.168.2.97\*
   1. DNS servers = 127.0.0.1, 192.168.2.1\*
4. Change hostname
   1. Control Panel > System > Change Settings
5. Set the Administrator account’s password
   1. CTRL + ALT + DELETE
6. Open Server Manager
   1. Add Roles and features
      1. Active Directory Wizard
         1. Before you begin
            1. Next
         2. Installation type
            1. Next
         3. Server selection
            1. Next
         4. Server roles
            1. Select “Active Directory Domain Services”

Add Features

Next

* + - 1. Features
         1. Next
      2. AD DS
         1. Next
      3. Confirmation
         1. Install
         2. Takes ~ 1 minute\*
      4. Results
         1. Select “Promote this server to a domain controller”
         2. Active Directory Domain Services Configuration Wizard

Deployment Configuration

Select “Add a new forest”

Domain name = apprentice.net\*

Next

Domain Controller Options

Password = <password>\*

DSRM = domain controller’s safe mode boot option for repair, recover, or restore options[[1]](#endnote-1)

DNS Options

Next

Additional Options

Next

Paths

Important files: Log files = C:\Windows\NTDS

Next

Review Options

Next

Prerequisites Check

Two warning received:

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>).

See **Securing**

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 "apprentice.net". Otherwise, no action is required.

Safely ignored since we do not need public connections to resolve the domain.[[2]](#endnote-2)\*

Install

Takes ~5 minutes including the reboot\*

* + 1. Add your domain account to the Enterprise Admins domain group.
       1. This is necessary to setup the Certificate Authority
       2. Open Active Directory Users and Accounts
       3. Find your domain account and select
          1. Apprentice.net > Users
       4. Select the Member Of tab > Add
          1. Add “Enterprise Admins” and “Domain Admins”
       5. Signing out and sign in to enact the privileges
    2. Create a Service Account (SA) to run the AD Certificate Services site
       1. Open AD Users and Computer > Create a user > name it svc\_certauth
    3. Add the SA to the IIS\_IUSRS group
       1. Open dsa.msc (Active Directory Users and Computers)
       2. Apprentice.net > built-in > IIS\_IUSRS
       3. Members tab > Add > svc\_certauth > OK
    4. AD Root Certificate Authority Wizard
       1. Before you begin
          1. Next
       2. Installation type
          1. Next
       3. Server selection
          1. Next
       4. Server roles
          1. Select “Active Directory Certificate Services”

Add Features

Next

* + - 1. Features
         1. Next
      2. AD CS
         1. Check Certificate Authority, Certificate Enrollment Policy Web Service, Certificate Enrollment Web Service, and Certification Authority Web Enrollment
         2. Next
      3. Web Server Role (IIS)
         1. Next
         2. Next
      4. Confirmation
         1. Install
         2. Takes ~5 minutes\*
      5. AD CS Configurations
         1. On the left, go to AD CS
         2. Select the warning, **More…**
         3. Select **Configure Active Directory Certificate Services on the destination server** “under the **Action** column
         4. AD CS Configuration Wizard
         5. Credentials

Next

* + - * 1. Role Services

Select **Certificate Authority** and **Certificate Authority Web Enrollment**

Next

* + - * 1. Setup Type

Select **Enterprise CA**

* + - * 1. CA type

Select **Root CA**

* + - * 1. Private Key

**Create a new private key**

Next

* + - * 1. Cryptography

Next

* + - * 1. CA Name

Next

* + - * 1. Validity Period

Next

* + - * 1. Certification Database

Next

* + - * 1. Confirmation

Configure

Takes ~10 seconds\*

* + - * 1. Results

Close

* + - * 1. After competition, a popup stating, “Do you want to configure additional role services?” will display, select **Yes**
        2. Credentials

Next

* + - * 1. Role Services

Select **Certificate Enrollment Web Service** and **Certificate Enrollment Policy Web Service**

Next

* + - * 1. CA for CES

Next

* + - * 1. Authentication types for CED

Windows Integrated authentication\*

Next

* + - * 1. Service Account for CES

**Use the built-in application pool identity**

**~~Use a service account (recommended)~~**

Next

* + - * 1. Authentication Type for CEP

Windows Integrated authentication\*

Next

* + - * 1. Server Certificate

Next

* + - * 1. Confirmation

Configure

Takes ~5 seconds\*

* + - * 1. Results

Close

* + 1. AD Intermediate CA
       1. Everything is the same as the Root CA until “AD CS Configurations”
       2. As a note, assure in the Credentials tab you’re using an account to configure the service has Enterprise Admin privileges.
       3. AD CS Configurations
          1. On the left, go to AD CS
          2. Select the warning, **More…**
          3. Select **Configure Active Directory Certificate Services on the destination server** “under the **Action** column
          4. AD CS Configuration Wizard
          5. Credentials

Next

* + - * 1. Role Services

Select **Certificate Authority** and **Certificate Authority Web Enrollment**

Next

* + - * 1. Setup Type

Select **Enterprise CA**

* + - * 1. CA type

Select **Subordinate**

* + - * 1. Private Key

**Create a new private key**

Next

* + - * 1. Cryptography

Next

* + - * 1. CA Name

Next

* + - * 1. Certificate Request

Send a certificate request to a parent CA

CA name

Parent CA – select the Root CA

Next

* + - * 1. Certification Database

Next

* + - * 1. Confirmation (~30s)

Configure

* + - * 1. Results

Close

* + - * 1. After competition, a popup stating, “Do you want to configure additional role services?” will display, select **Yes**
        2. Credentials

Next

* + - * 1. Role Services

Select **Certificate Enrollment Web Service** and **Certificate Enrollment Policy Web Service**

Next

* + - * 1. CA for CES

Next

* + - * 1. Authentication types for CED

Windows Integrated authentication\*

Next

* + - * 1. Service Account for CES

**Use the built-in application pool identity**

**~~Use a service account (recommended)~~**

Next

* + - * 1. Authentication Type for CEP

Windows Integrated authentication\*

Next

* + - * 1. Server Certificate

Next

* + - * 1. Confirmation

Configure

Takes ~5 seconds\*

* + - * 1. Results

Close

* + - 1. Server Manager > Tools > Certificate Authority
         1. Right-click Certificate Templates > Manage

For the commonly issued certificate templates listed (e.g. web server), right-click it > properties

Go to the Security tab

Adjust the groups and users you wish to have permissions to request certificates

For that role (e.g. Domain Admins), select it, and check the Allow checkbox for Enroll to enable it

* + 1. RADIUS wizard
       1. Before you begin
          1. Next
       2. Installation type
          1. Next
       3. Server selection
          1. Next
       4. Server roles
          1. Select **Network Policy and Access Services**

Add Features

Next

* + - 1. Features
         1. Next
      2. Network Policy and Access Services
         1. Next
      3. Confirmation
         1. Install
         2. Takes ~30 seconds\*
      4. Results
         1. Close
  1. RADIUS Configurations
     1. In Server Manager, Select **Tools** > **Network Policy Server**
     2. On the left pane, **NPS (Local)** > **RADIUS Clients and Servers** > right click **RADIUS Clients** > **New**

# **Configuring AD DC**

1. Create organizational unit (OU) structure
   1. Open Server Manager > Tools > AD Users and Computers
      1. Right click the domain name, “apprentice.net” > New > Organizational Unit
         1. The first OU will be by geography. Name it, “Range”
            1. Create two sub-OUs under “Range”

Management

Create two sub-OUs under “Management”

Computers

Users

Business

Create two sub-OUs under “Management”

Computers

Users

1. Create users
   1. Create Domain admin account
      1. Active Directory Users and Computers > apprentice.net > Users
         1. Right click “Administrator” > Copy
            1. First name = Cyber
            2. Last name = Apprentice
            3. Initials = CA
            4. User logon name = apprentice.admin
            5. Next
            6. Password = <password>
            7. Next
            8. Finish
         2. Drag the created user to the appropriate OU (apprentice.net > Range > Management > Users)
   2. Create standard account
      1. Apprentice.net > Range > Business > Users
         1. Right click the OU > New > User
            1. First name = Customer
            2. Last name = 1
            3. Initials = 1
            4. Next
            5. Password = <password>
            6. Deselect “user must change password at next logon”
            7. Next
            8. Finish

# **Installing ESXi**

Resources:

* Memory = 11GB
* Processors = 2
* Storage = 100GB
* Dd

1. Welcome to the VMware ESXi 6.7.0 Installation
   1. (Enter) Continue
2. EULA
   1. (F11) Accept and Continue
3. Select a Disk to Install or Upgrade
   1. (Enter) Continue
      1. Only had one drive so I left the default
4. Keyboard Layout
   1. (Enter) Contiue
      1. Default is “US Default”
5. Enter a root password
   1. <password>
6. Confirm install
   1. (F11) Install
      1. Takes 1 minute
7. Installation Complete
   1. Go to the VM settings and delete the CD drive or deselect the radio box, “Connect at power on”.
   2. (Enter) Reboot
8. [OPTIONAL] Statically set IPv4 address
   1. Select F2 key to change the settings
      1. Enter password
         1. Configure Management Network
            1. IPv4 Configuration

Set static IPv4 address and network configuration

192.168.2.99\*

255.255.255.0\*

192.168.2.1\*

Save, exit, and restart services

# **Installing VCSA**

Version: vCenter Server Appliance 6.7 Installer

Resources: 11GB

1. Log onto a host machine (I’m using a Windows VM)
2. Mount the VCSA ISO (I’m using VCSA 6.7)
3. Install
   1. Stage 1 – Deploy appliance
      1. Introduction
         1. Next
      2. End user license agreement
         1. Accept
         2. Next
      3. Select Deployment Type
         1. Embedded Platform Services Controller – vCenter Server with an embedded platform services controller
      4. Appliance Deployment Target
         1. ESXi host or vCenter Server name = 192.168.2.99\*
            1. IPv4 address is may be different for you
         2. HTTPS port = 443
         3. Username = <username of ESXi>\*
         4. Password = <password of ESXi>\*
         5. Next
            1. Certificate Warning

Yes

* + 1. Set up appliance VM
       1. VM Name = VMware vCenter Server Appliance\*
       2. Root pass = <pass>\*
       3. Next
    2. Select Deployment size
       1. Deployment size = tiny\*
       2. Storage size = default\*
    3. Select datastore
       1. Select thin provisioning\*
       2. Next
    4. Configure network settings
       1. IP address = 192.168.2.98\*
       2. Subnet mask = 255.255.255.0\*
       3. Default Gateway = 192.168.2.1\*
       4. DNS servers = 192.168.2.97\*
          1. This is the Active Directory server
       5. The rest are defaults. Select Next.
    5. Finish
       1. Takes ~10 minutes\*
  1. Stage 2: Setup VCSA with an embedded platform services controller
     1. Introduction
        1. Next
     2. Appliance Configuration
        1. Next
     3. SSO Configuration
        1. Create a new SSO domain
           1. Domain name = apprentice.net\*
           2. Password = <password>\*
           3. Next
     4. Configure CEIP
        1. Deselect\*
           1. I think engaging in these programs are useful because ultimately it makes a better product. However, when not connected to the Internet, it’s useless and just causes unnecessary traffic.
        2. Next
     5. Ready to Complete
        1. Finish
           1. Warning

Ok

* + - 1. Takes ~30 minutes\*

# **Securing**

# Group Policy

* https://www.aventistech.com/kb/fixes-for-vulnerabilities-detected-by-nessus/

# **Troubleshooting**

* SSL
  + Google
    - NET::ERR\_CERT\_COMMON\_NAME\_INVALID
    - CA Invalid
      * Download the CA to your local machine
        + Add san:dns=dns.name[&dns=dns.name]under “Additional Attributes”
        + san:dns=192.168.88.5
        + **certutil -setreg policy\EditFlags +EDITF\_ATTRIBUTESUBJECTALTNAME2**

**net stop certsvc  
net start certsvc**

* + - * Place in appropriate directory
        + Centos 7:

/etc/pki/ca-trust/source/anchors/CAcert.crt

update-ca-trust

**Bibliography (16th Edition Chicago Style)**

1. https://searchwindowsserver.techtarget.com/definition/Directory-Services-Restore-Mode-DSRM [↑](#endnote-ref-1)
2. https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc754463(v=ws.10)?redirectedfrom=MSDN [↑](#endnote-ref-2)