Deploying and Configuring a Two-Tier CA Hierarchy/ Deploying and Using Certificates

Eli Chang

MSSA Cohort #2

Lab Summary 8,9

3/15/2020

Deploying and Configuring a Two-Tier CA Hierarchy/ Deploying and Using Certificates

The company has increased the security level and now wants to enable secure access to critical websites with additional security for some features, such as EFS, digital signatures, smart cards, and DA features. The administrators decided to implement a PKI with the AD CS role in Windows Server 2016 so that the AD CS should be deployed. In the next lab, the company decided to use certificates issued by the AD CS role in Windows Server 2016. The admins should implement certificate enrollment and develop the procedures and processes for managing certificate templates.

AD CS in Windows Server 2016

Active Directory Certificate Services (AD CS) allows the admins to implement a Public Key Infrastructure (PKI), which means it issues and manages certificates. There are several options for AD CS, but only certification authority and certificate enrollment web service is used for this lab. Since the primary purpose of AD CS is to issue, revoke, and publish certificates, the certification authority is an essential option for the company. The root CA should be created as the highest point in the hierarchy. Certification authority web enrollment is the component to provide a method to issue and renew certs.

Implementing CA hierarchies

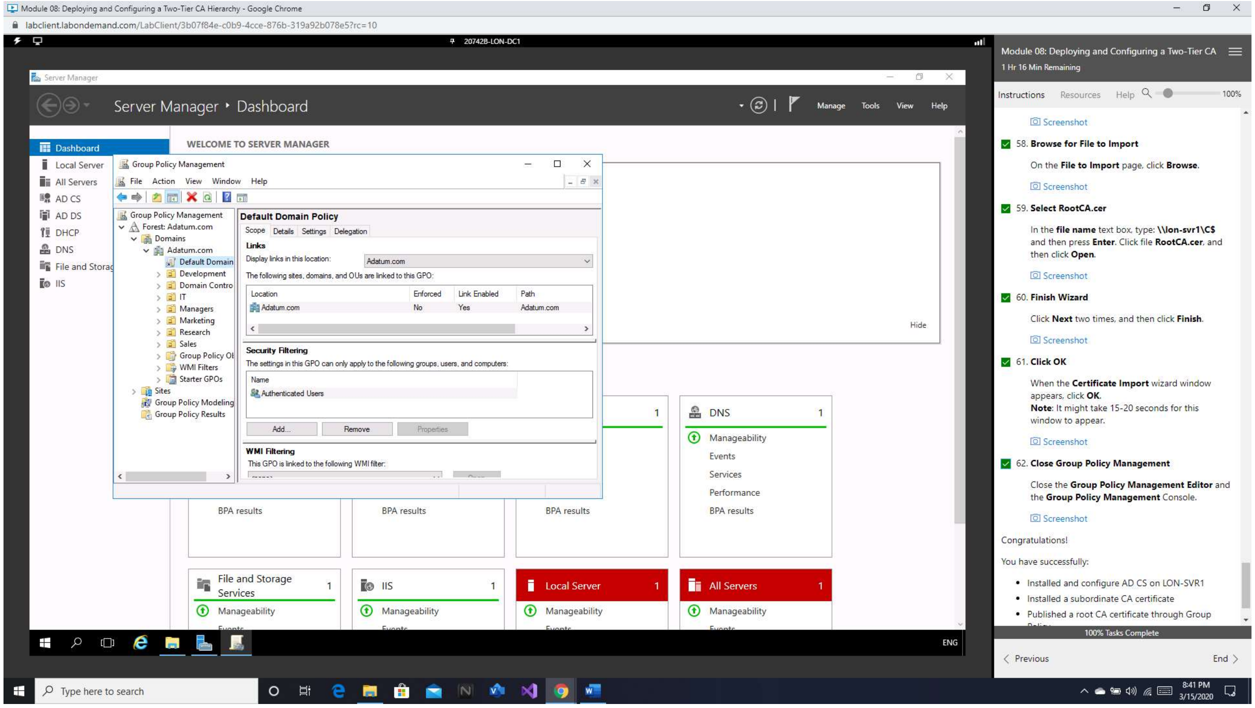
There are three categories in CA hierarchies: CA hierarchies with a policy CA, a cross-certification trust, and a two-tier hierarchy. The first hierarchy is the policy CA is a subordinate CA that is directly below the root CA. This hierarchy is useful when describing policies and procedures to secure its PKI. The second hierarchy is cross-certification trust. Two independent CA hierarchies interoperate with one another so that they can establish mutual trust between two different CA hierarchies. Lastly, CA, with a two-tier hierarchy, is the type used in the lab. There is one root CA and at least one or more subordinate CAs. The subordinate CA should have responsibilities of policies and issuing certificates.

Enrollment Agent

An enrollment agent is a user account to request certificates on behalf of another user account. There are two other types of enrollment agents: enrollment agent (computer) and exchange enrollment agent (offline request). The enrollment agent is used to request certificates on behalf of another subject, while the enrollment agent (computer) is doing it on behalf of another computer subject. The exchange enrollment agent (offline request) is used to request certificates on behalf of another subject and supply the name of the subject.

Standalone CA vs. Enterprise CA

There are two types of Cas in Windows Server 2016 AD CS: standalone and enterprise CAs. In typical usage, the standalone CA is used for offline CAs and CA on the network. The enterprise CA issue certificates for users, services, and computers but cannot be used as an offline CA. The standalone CA does not depend on the AD DS, but the enterprise CA depends on the AD DS and provides a publication point for certificates. The certificate issuance method in the standalone CA must be approved by the admins manually, whereas the enterprise CA could be automatic, based on issuance requirement settings.



Module 08: Deploying and Configuring a Two-Tier CA Hierarchy - Google Chrome

labclient.labondemand.com/LabClient/3b07f84e-c0b9-4cce-876b-319a92b078e5?rc=10

Group Policy Management — Default Domain Policy

Links

Display links in this location: Adatum.com

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled	Path
Adatum.com	No	Yes	Adatum.com

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

Name
Authenticated Users

WMI Filtering

This GPO is linked to the following WMI filter:

Module 08: Deploying and Configuring a Two-Tier CA

1 Hr 16 Min Remaining

58. **Browse for File to Import**

On the **File to Import** page, click **Browse**.

59. **Select RootCA.cer**

In the **file name** text box, type: **\\lon-svr1\C$** and then press **Enter**. Click file **RootCA.cer**, and then click **Open**.

60. **Finish Wizard**

Click **Next** two times, and then click **Finish**.

61. **Click OK**

When the **Certificate Import** wizard window appears, click **OK**.
Note: It might take 15-20 seconds for this window to appear.

62. **Close Group Policy Management**

Close the **Group Policy Management Editor** and the **Group Policy Management** Console.

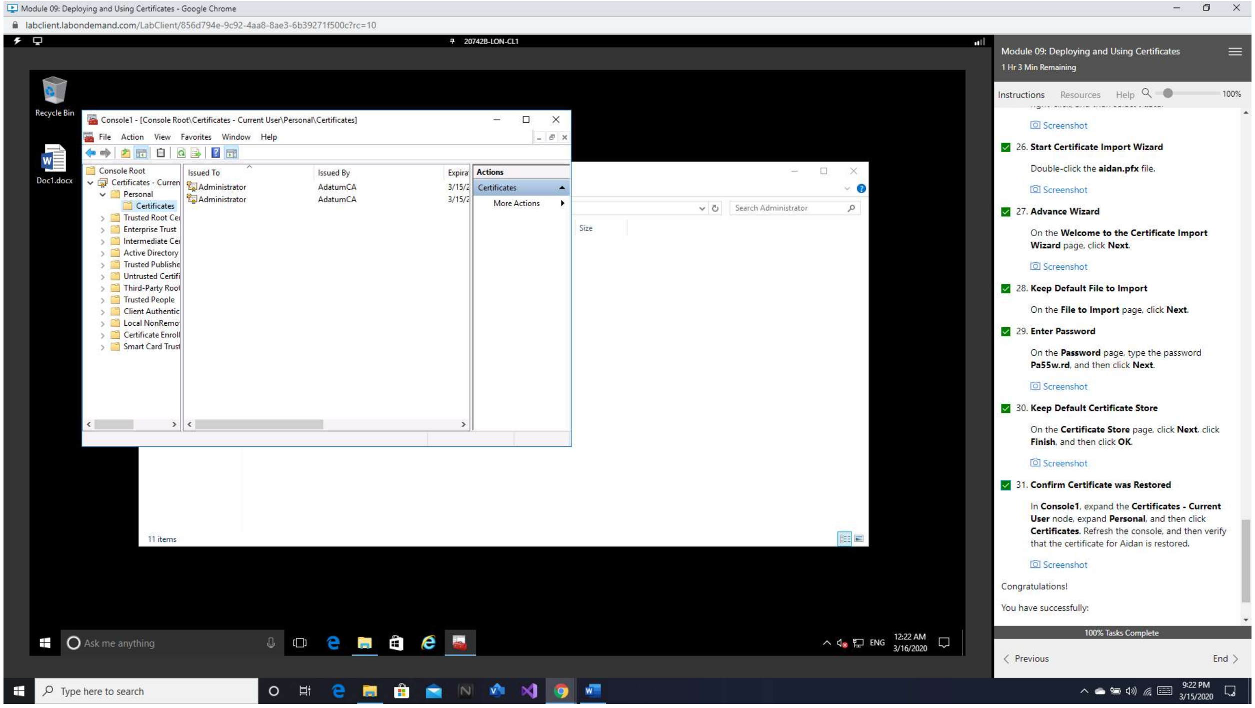
Congratulations!

You have successfully:

- Installed and configure AD CS on LON-SVR1
- Installed a subordinate CA certificate
- Published a root CA certificate through Group Policy

100% Tasks Complete

8:41 PM 3/15/2020



Module 09: Deploying and Using Certificates - Google Chrome

labclient.labondemand.com/LabClient/856d794e-9c92-4aa8-8ae3-6b39271f500c?rc=10

Console1 - [Console Root\Certificates - Current User\Personal\Certificates]

Issued To	Issued By	Expira
Administrator	AdatumCA	3/15/2
Administrator	AdatumCA	3/15/2

11 items

Module 09: Deploying and Using Certificates

1 Hr 3 Min Remaining

26. **Start Certificate Import Wizard**

Double-click the **aidan.pfx** file.

27. **Advance Wizard**

On the **Welcome to the Certificate Import Wizard** page, click **Next**.

28. **Keep Default File to Import**

On the **File to Import** page, click **Next**.

29. **Enter Password**

On the **Password** page, type the password **Pa55w.rd**, and then click **Next**.

30. **Keep Default Certificate Store**

On the **Certificate Store** page, click **Next**, click **Finish**, and then click **OK**.

31. **Confirm Certificate was Restored**

In **Console1**, expand the **Certificates - Current User** node, expand **Personal**, and then click **Certificates**. Refresh the console, and then verify that the certificate for Aidan is restored.

Congratulations!

You have successfully:

100% Tasks Complete

12:22 AM 3/16/2020

9:22 PM 3/15/2020