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

Eli Chang

MSSA Cohort #2

Diagram Exercise 8,9

3/15/2020

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

There are three types of CA hierarchies in AD CS in Windows Server 2016: Policy CA, Cross-certification trust, and Two-tier hierarchy. The lab has chosen the two-tier hierarchy, which should contain a root CA and at least one subordinate CAs. For the root CA, a standalone CA is configured because the standalone CA is not joined to the AD DS domain and typically used for offline CAs. The subordinate CAs are the enterprise CAs to issue certificates to users, computers, and services.

Below the subordinate CAs, there are two more CAs for load balancing. Since it is a large company, the admins should manage a large number of certificates so that they can divide the network load between CAs. Also, backup and fault tolerance would be provided in this diagram so that when one or more goes down, the other could provide the certificates. The users should have the smart cards to sign in to the computers. Each user will have their limited resources and storage in their smart cards and authenticate their identities.

Root CA

Subordinate CA   Subordinate CA