Presentation Outline:

Pre-work:

DC1 - needs ADDS and no certificate authority

OLRoot - non-domain joined server

EntSub - domain joined member server

Deploy needed modules (demo.ps1)

Each server needs to have its respective config deployed to it

Finish it up manually using pieces in demo.ps1

Intro:

Don’t forget your name. Who are you again?

Today we’re going to talk PKI - but not just any PKI - a Production configuration of PKI.

Repeatable configuration

I thought this was going to be easy! (Smile)

    It wasn’t

    Building brick thingy

This is why you are here:

    My lessons learned in production technology configuration

    The pain, the process, and the things not complete yet.

    And I need your help and involvement

Agenda slide:

* Goals of the config
* Successes
* Problems
* What is missing/incomplete

Goals of the config (Slide)

    Offline root / CRL published in website

    Subordinate CA

    All member servers have root in store

    Autoenrollment policy

    DSC Template for credential encryption

Successes (combine successes and problems)

    PKIDeploy.ps1 - quick walk through

    Show config data and sections

    (Mention the instructions of order you followed)

    Registry settings

* Certutil unfriendliness - need better (or some!) cmdlets to do what certutil does - reverse engineering certutil to figure out what each command does
  + Certutil doesn’t always have get- equivalents (i.e. DSPublish)
* Certutil -dspublish - used a get-ADObject for a get
* PublishCRL - not sure what it does - use GUI to dig around and investigate
* Recycle is not a state
* DNS settings, certutil -dspublish - both needed to be done on the DC itself (double-hop)
* Code to test for imported CRL really tricky because CRL not visible in the Cert:\ provider.
* ACLs - custom resource - squirrel - icacls

What is missing/incomplete

* Setting for a recycle/reboot
* Taking cert request and issuing the certificate for the sub CA/install cert / start CA
* Set CRL/AIA (but can reuse code from root)
* Passing it back (file resources)
* Replace script resources with custom resources

Code complete but not yet located in this config:

* + Autoenrollment GPO\*
  + DSC template\*

Thank-you slide

    Link to repo