Ondřej Ševeček | PM Windows Server | GOPAS a.s. |
MCM: Directory Services | MVP: Enterprise Security |
ondrej@sevecek.com | www.sevecek.com |

FARM SETUP

Installation

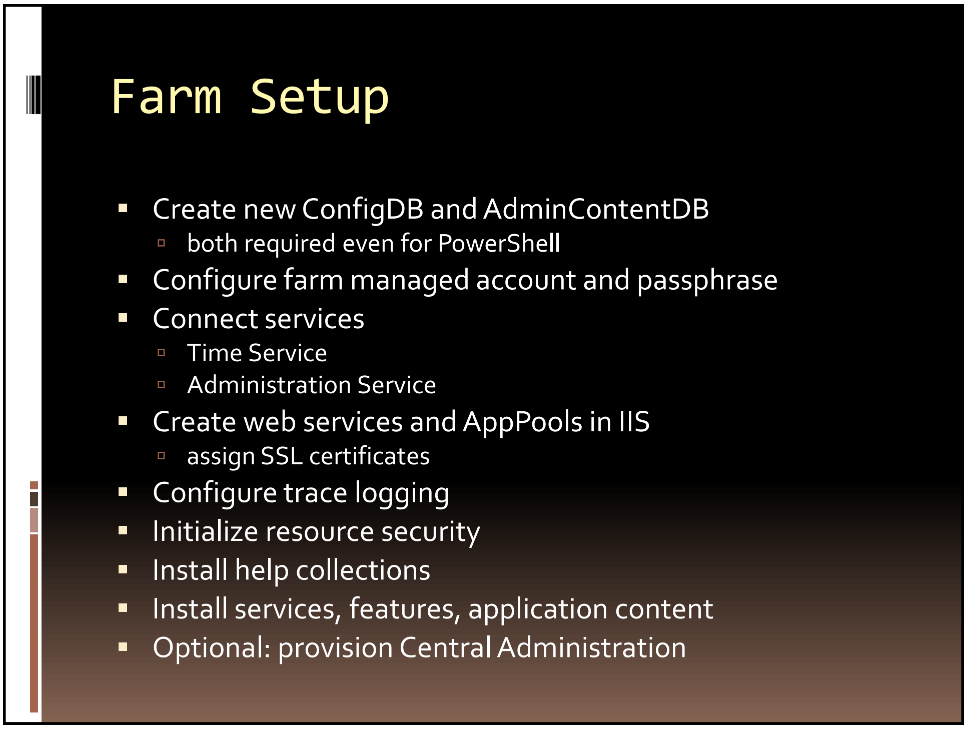
- PrerequisiteInstaller.exe
  - IIS, SQL Native Client, Identity Foundation
  - other tools
- Setup.exe
  - SharePoint binaries
  - Updates
  - Language packs
- Products Configuration Wizard or PowerShell
  - create ConfigDB, enable services, create web services

Installation

- Setup.exe
  - installs binaries
  - %CommonFiles%\Microsoft Shared\Web Server Extensions\14.0
    - SharePoint root
  - %ProgramFiles%\Microsoft Office Server
  - Global Assembly Cache (GAC)
  - HKLM\Software\Microsoft\Shared Tools
  - HKLM\Software\Microsoft\Office Server

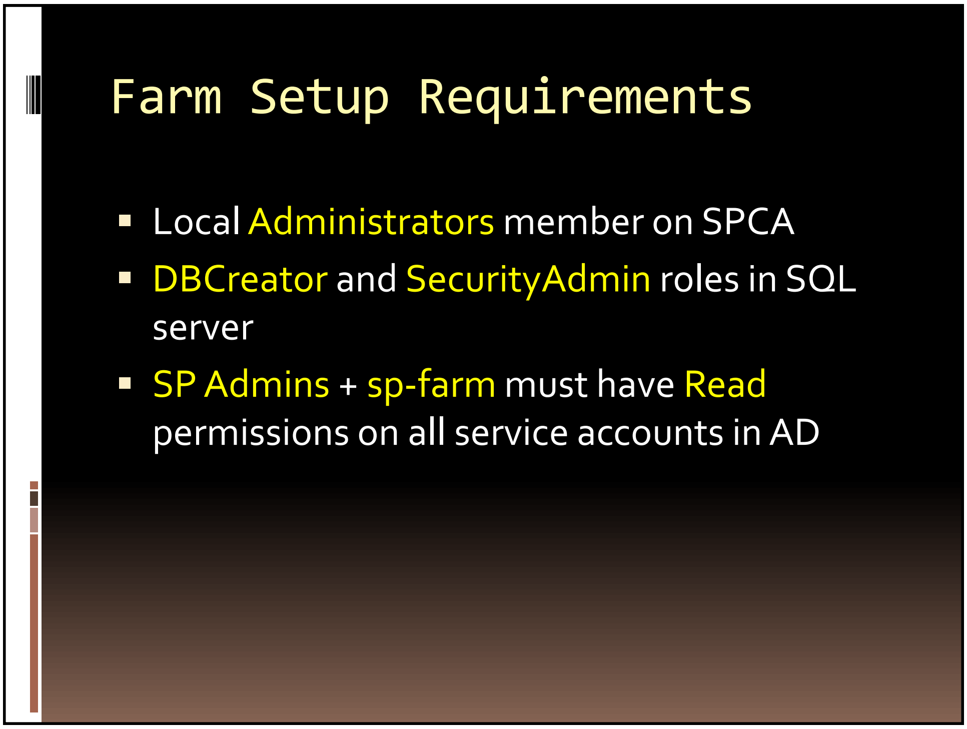
Farm Setup

INITIALIZE CONFIGURATION DATABASE



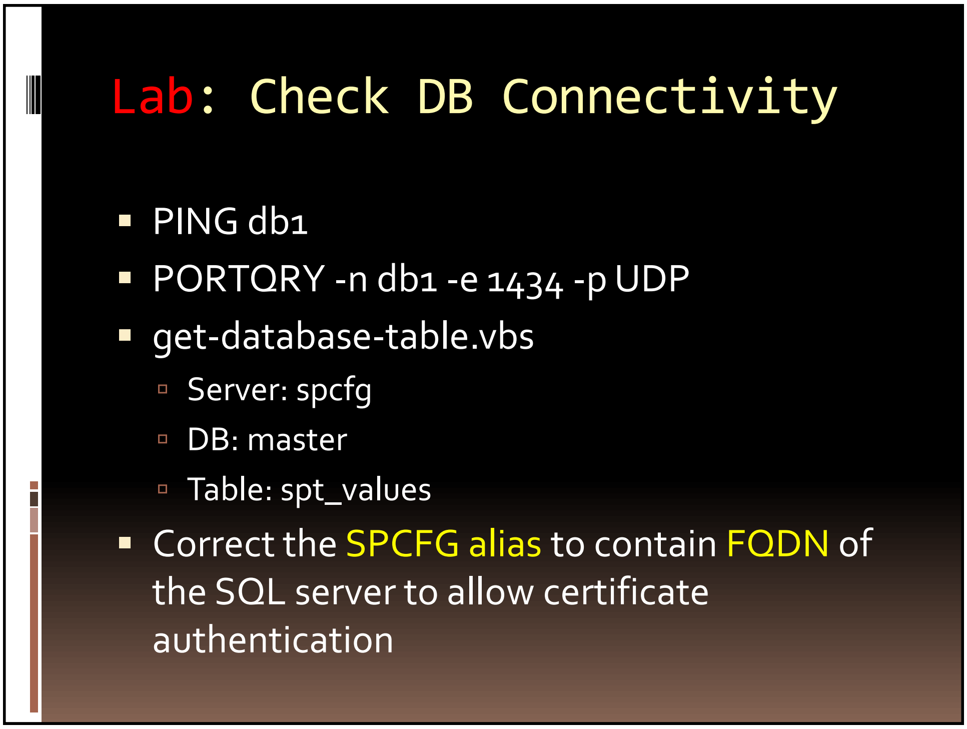
Farm Setup

- Create new ConfigDB and AdminContentDB
  - both required even for PowerShell
- Configure farm managed account and passphrase
- Connect services
  - Time Service
  - Administration Service
- Create web services and AppPools in IIS
  - assign SSL certificates
- Configure trace logging
- Initialize resource security
- Install help collections
- Install services, features, application content
- Optional: provision Central Administration



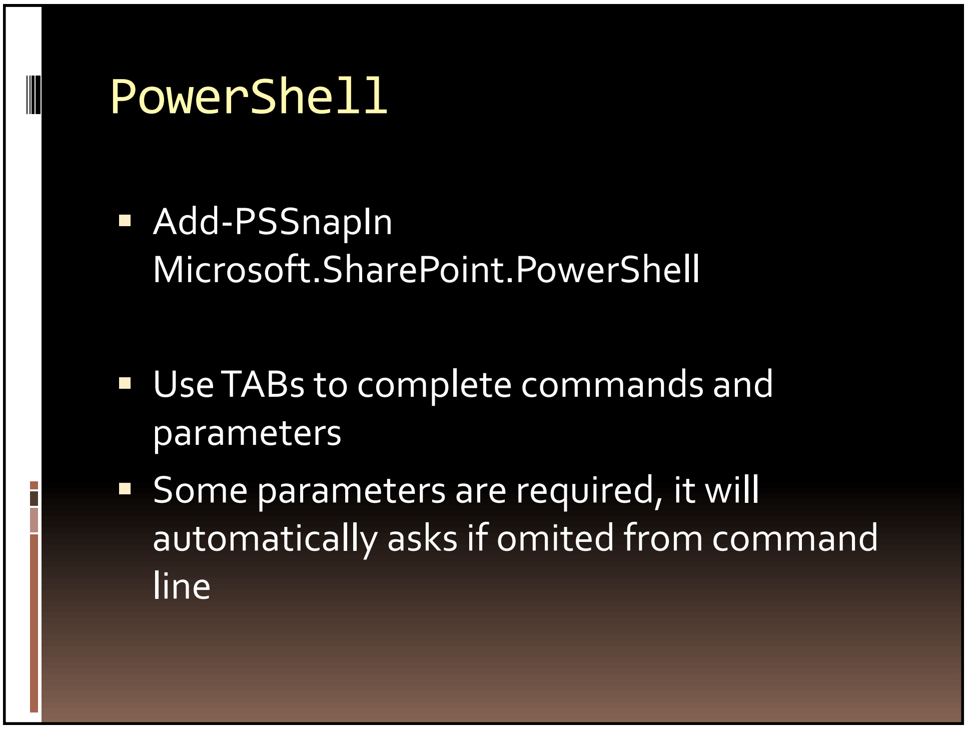
Farm Setup Requirements

- Local Administrators member on SPCA
- DBCreator and SecurityAdmin roles in SQL server
- SP Admins + sp-farm must have Read permissions on all service accounts in AD



Lab: Check DB Connectivity

- PING db1
- PORTQRY -n db1 -e 1434 -p UDP
- get-database-table.vbs
  - Server: spcfg
  - DB: master
  - Table: spt_values
- Correct the SPCFG alias to contain FQDN of the SQL server to allow certificate authentication



PowerShell

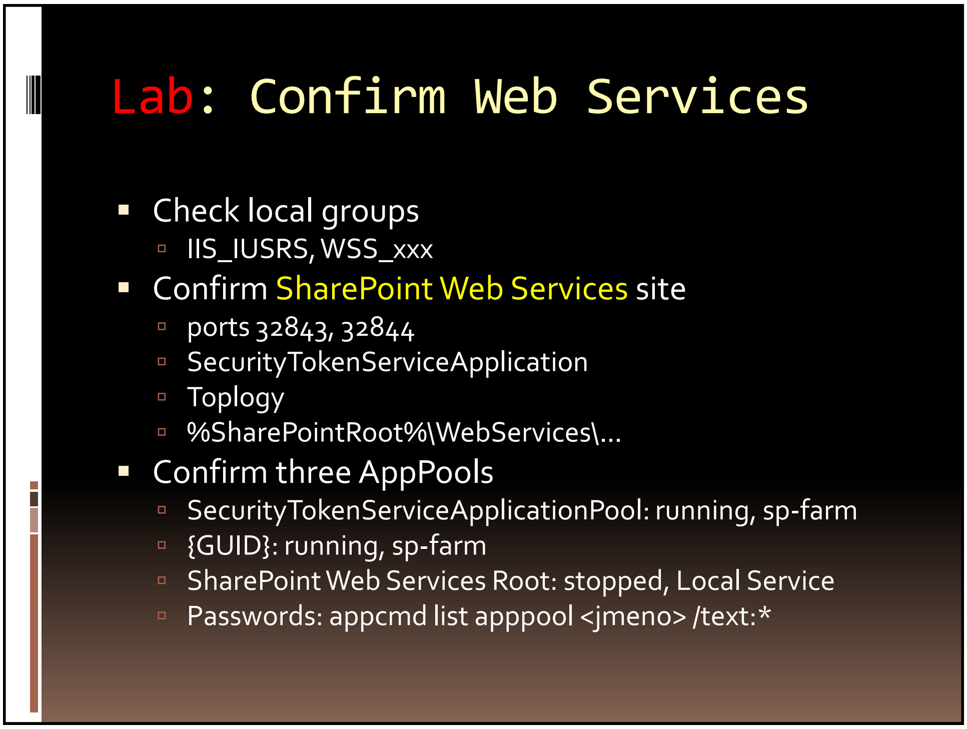
- Add-PSSnapIn Microsoft.SharePoint.PowerShell
- Use TABs to complete commands and parameters
- Some parameters are required, it will automatically asks if omited from command line

Lab: Create New DBs

- New-SPConfigurationDatabase
  - -DatabaseCredentials (Get-Credentials gps\sp-intranet-farm)
  - -Passphrase (ConvertTo-SecureString 'Pa$$wordPa$$word' -AsPlainText -Force)
- Store the passphrase into \\DC1\Support
- always use domain prefix gps\
  - or "user does not exist or is not unique"

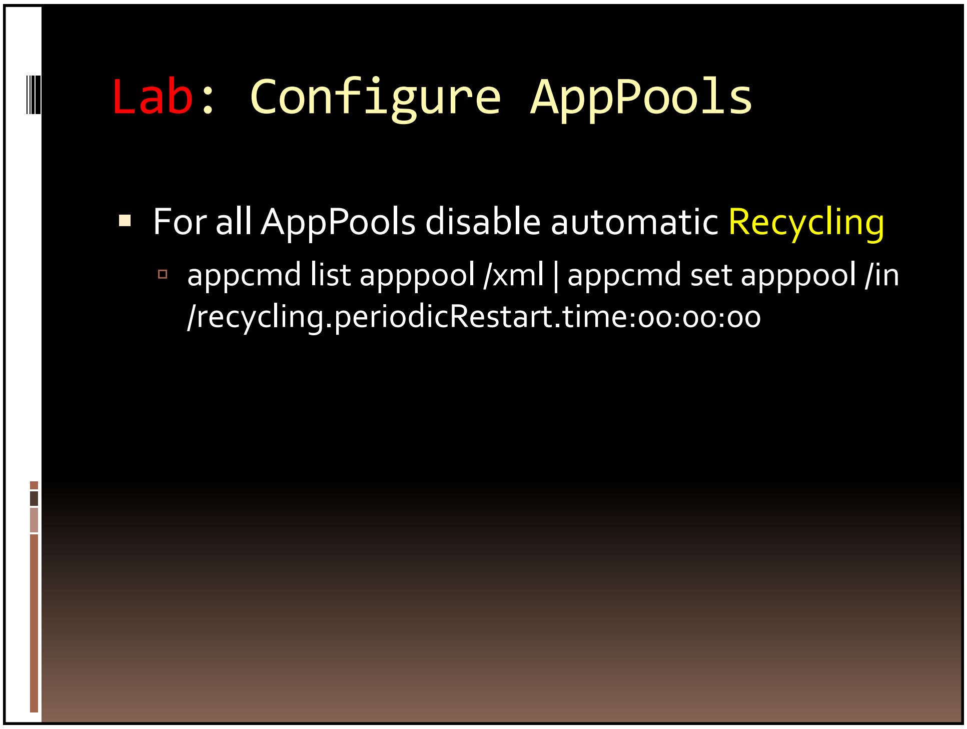
Lab: Confirm the New DBs

- Confirm both DBs created
  - Auto update statistics: false (should be left at that)
- Confirm sp-intranet-farm login created
  - confirm DB roles of the sp-intranet-farm and SP Admins
- Confirm recovery mode of the DBs
- Confirm Time Service configured and running
  - Optional: CAIN to obtain the service password
- Confirm registry settings
  - Secure\ConfigDB
  - Secure\FarmAdmin
- Start SQL Activity Monitor and confirm connections from SPCA



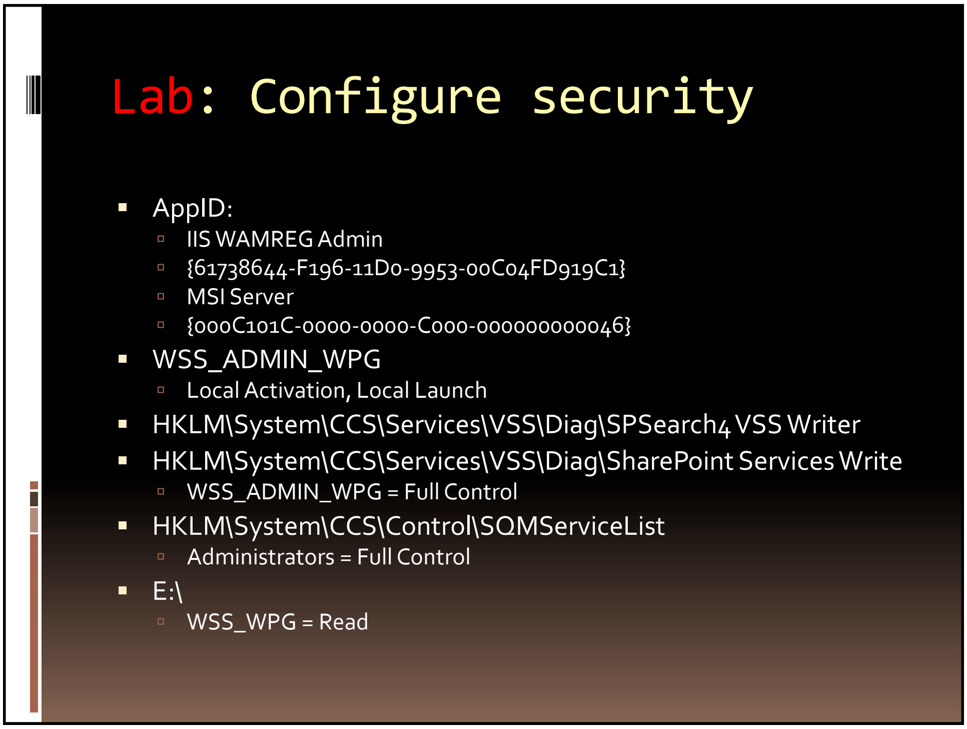
Lab: Confirm Web Services

- Check local groups
  - IIS_IUSRS, WSS_xxx
- Confirm SharePoint Web Services site
  - ports 32843, 32844
  - SecurityTokenServiceApplication
  - Toplogy
  - %SharePointRoot%\WebServices\...
- Confirm three AppPools
  - SecurityTokenServiceApplicationPool: running, sp-farm
  - {GUID}: running, sp-farm
  - SharePoint Web Services Root: stopped, Local Service
  - Passwords: appcmd list apppool <jmeno> /text:*



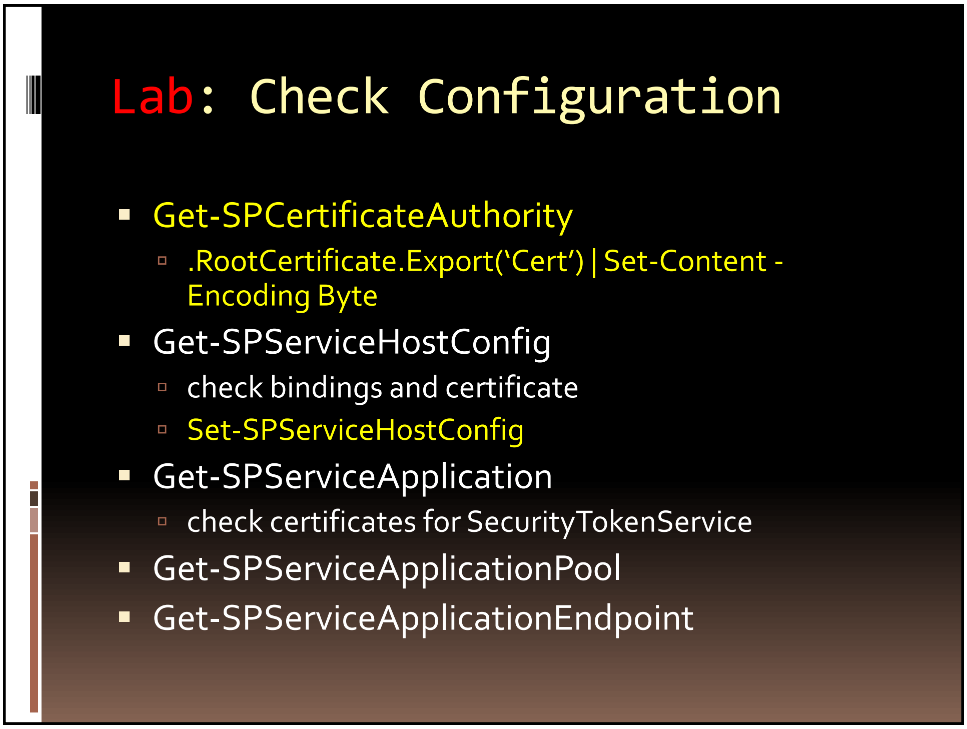
Lab: Configure AppPools

- For all AppPools disable automatic Recycling
  - appcmd list apppool /xml | appcmd set apppool /in /recycling.periodicRestart.time:00:00:00



Lab: Configure security

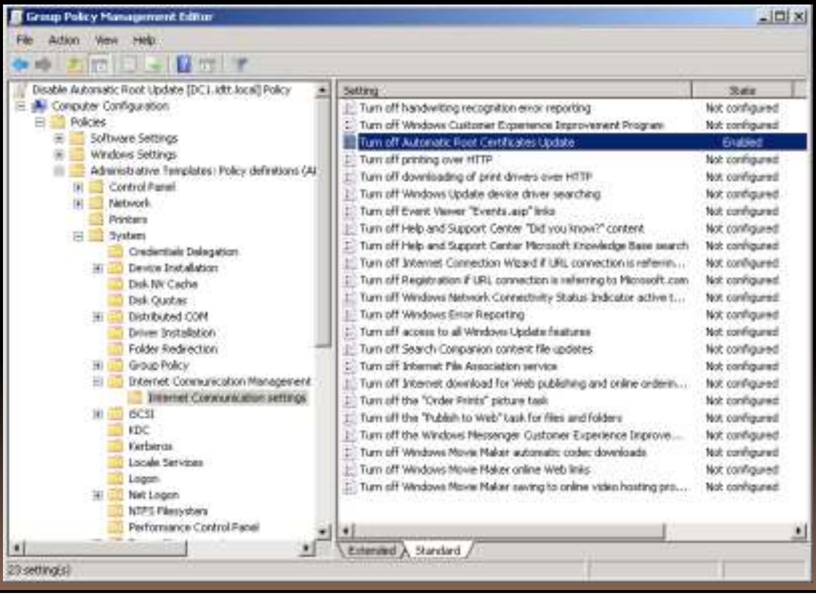
- AppID:
  - IIS WAMREG Admin
  - {61738644-F196-11D0-9953-00C04FD919C1}
  - MSI Server
  - {000C101C-0000-0000-C000-000000000046}
- WSS_ADMIN_WPG
  - Local Activation, Local Launch
- HKLM\System\CCS\Services\VSS\Diag\SPSearch4 VSS Writer
- HKLM\System\CCS\Services\VSS\Diag\SharePoint Services Write
  - WSS_ADMIN_WPG = Full Control
- HKLM\System\CCS\Control\SQMServiceList
  - Administrators = Full Control
- E:\
  - WSS_WPG = Read



Lab: Check Configuration

- Get-SPCertificateAuthority
  - .RootCertificate.Export('Cert') | Set-Content -Encoding Byte
- Get-SPServiceHostConfig
  - check bindings and certificate
  - Set-SPServiceHostConfig
- Get-SPServiceApplication
  - check certificates for SecurityTokenService
- Get-SPServiceApplicationPool
- Get-SPServiceApplicationEndpoint

Disable Root CA download



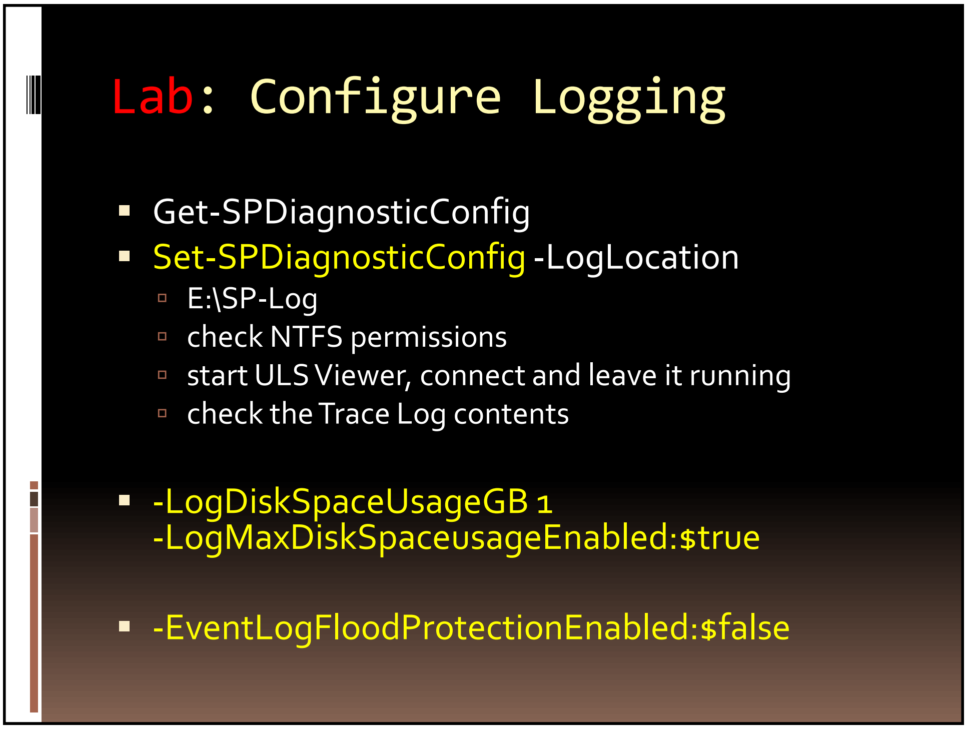
- Disable Automatic Root Update [DC1.idtt.local] Policy
  - Computer Configuration
    - Policies
      - Software Settings
      - Windows Settings
      - Administrative Templates: Policy definitions (AI
        - Control Panel
        - Network
        - Printers
        - System
          - Credentials Delegation
          - Device Installation
          - Disk NV Cache
          - Disk Quotas
          - Distributed COM
          - Driver Installation
          - Folder Redirection
          - Group Policy
          - Internet Communication Management
            - Internet Communication settings
          - iSCSI
          - KDC
          - Kerberos
          - Locale Services
          - Logon
          - Net Logon
          - NTFS Filesystem
          - Performance Control Panel

Setting	State
Turn off handwriting recognition error reporting	Not configured
Turn off Windows Customer Experience Improvement Program	Not configured
Turn off Automatic Root Certificates Update	Enabled
Turn off printing over HTTP	Not configured
Turn off downloading of print drivers over HTTP	Not configured
Turn off Windows Update device driver searching	Not configured
Turn off Event Viewer "Events.asp" links	Not configured
Turn off Help and Support Center "Did you know?" content	Not configured
Turn off Help and Support Center Microsoft Knowledge Base search	Not configured
Turn off Internet Connection Wizard if URL connection is referrin...	Not configured
Turn off Registration if URL connection is referring to Microsoft.com	Not configured
Turn off Windows Network Connectivity Status Indicator active t...	Not configured
Turn off Windows Error Reporting	Not configured
Turn off access to all Windows Update features	Not configured
Turn off Search Companion content file updates	Not configured
Turn off Internet File Association service	Not configured
Turn off Internet download for Web publishing and online orderin...	Not configured
Turn off the "Order Prints" picture task	Not configured
Turn off the "Publish to Web" task for files and folders	Not configured
Turn off the Windows Messenger Customer Experience Improve...	Not configured
Turn off Windows Movie Maker automatic codec downloads	Not configured
Turn off Windows Movie Maker online Web links	Not configured
Turn off Windows Movie Maker saving to online video hosting pro...	Not configured

23 setting(s)

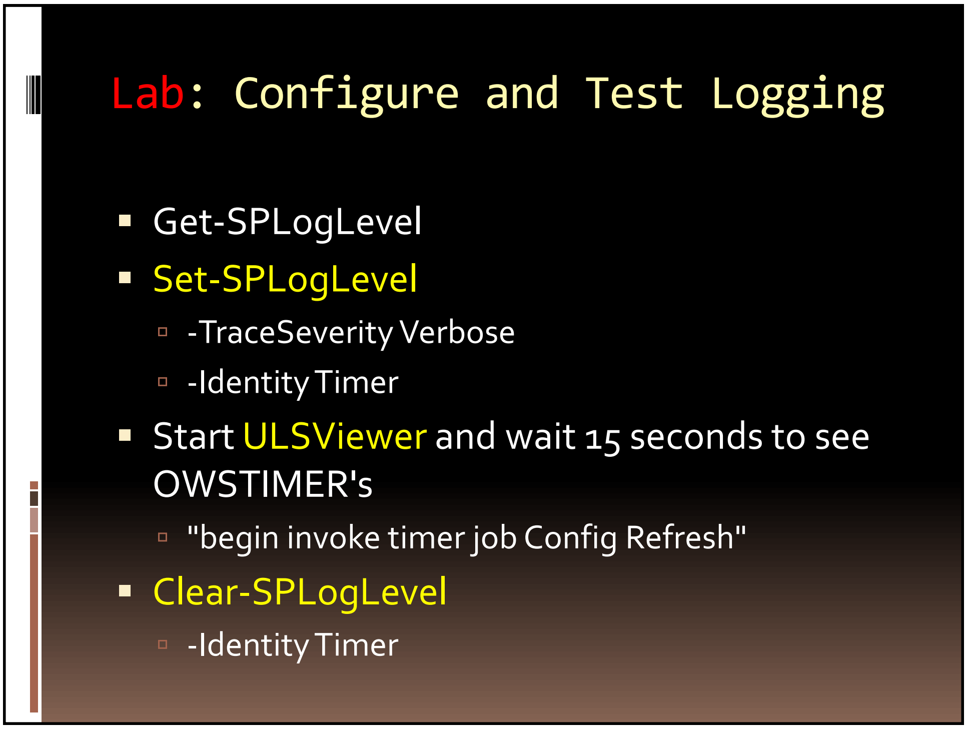
Logging

- SharePoint Tracing Service
  - writes trace logs
  - writes events into event logs
  - manages disk space and number of days of logs
- Runs as local service identity



Lab: Configure Logging

- Get-SPDiagnosticConfig
- Set-SPDiagnosticConfig -LogLocation
  - E:\SP-Log
  - check NTFS permissions
  - start ULS Viewer, connect and leave it running
  - check the Trace Log contents
- -LogDiskSpaceUsageGB 1
  -LogMaxDiskSpaceusageEnabled:$true
- -EventLogFloodProtectionEnabled:$false

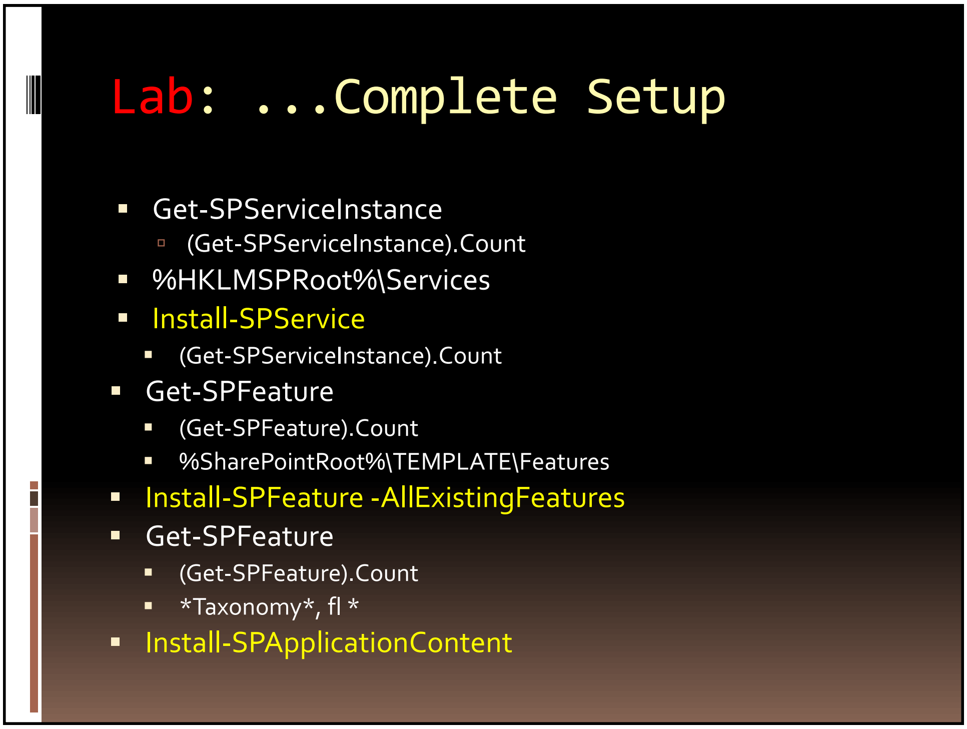


Lab: Configure and Test Logging

- Get-SPLogLevel
- Set-SPLogLevel
  - -TraceSeverity Verbose
  - -Identity Timer
- Start ULSViewer and wait 15 seconds to see OWSTIMER's
  - "begin invoke timer job Config Refresh"
- Clear-SPLogLevel
  - -Identity Timer

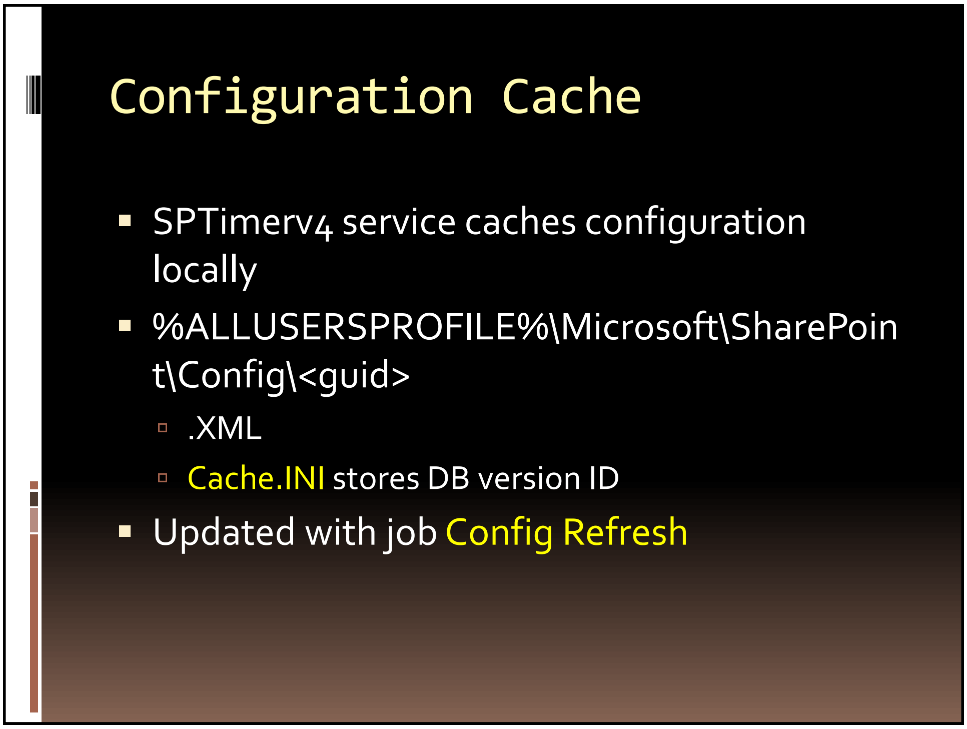
Lab: Complete Setup...

- Start ProcMon
- Initialize-SPResourceSecurity
- Filter out permission related events
- Install-SPHelpCollection -All



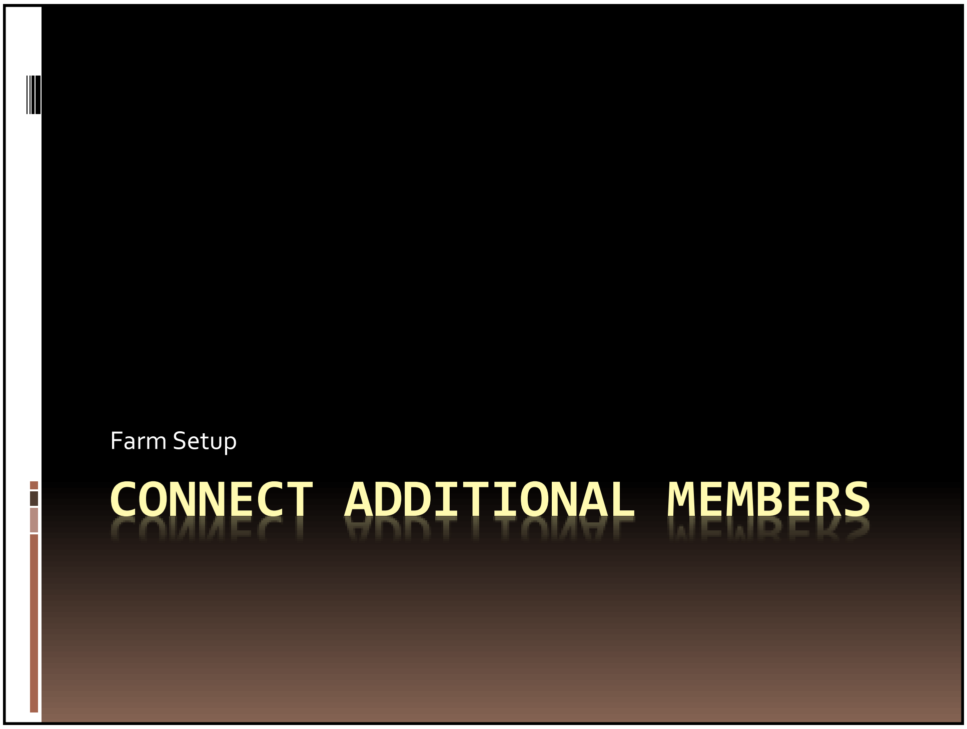
Lab: ...Complete Setup

- Get-SPServiceInstance
  - (Get-SPServiceInstance).Count
- %HKLMSPRoot%\Services
- Install-SPService
  - (Get-SPServiceInstance).Count
- Get-SPFeature
  - (Get-SPFeature).Count
  - %SharePointRoot%\TEMPLATE\Features
- Install-SPFeature -AllExistingFeatures
- Get-SPFeature
  - (Get-SPFeature).Count
  - *Taxonomy*, fl *
- Install-SPApplicationContent



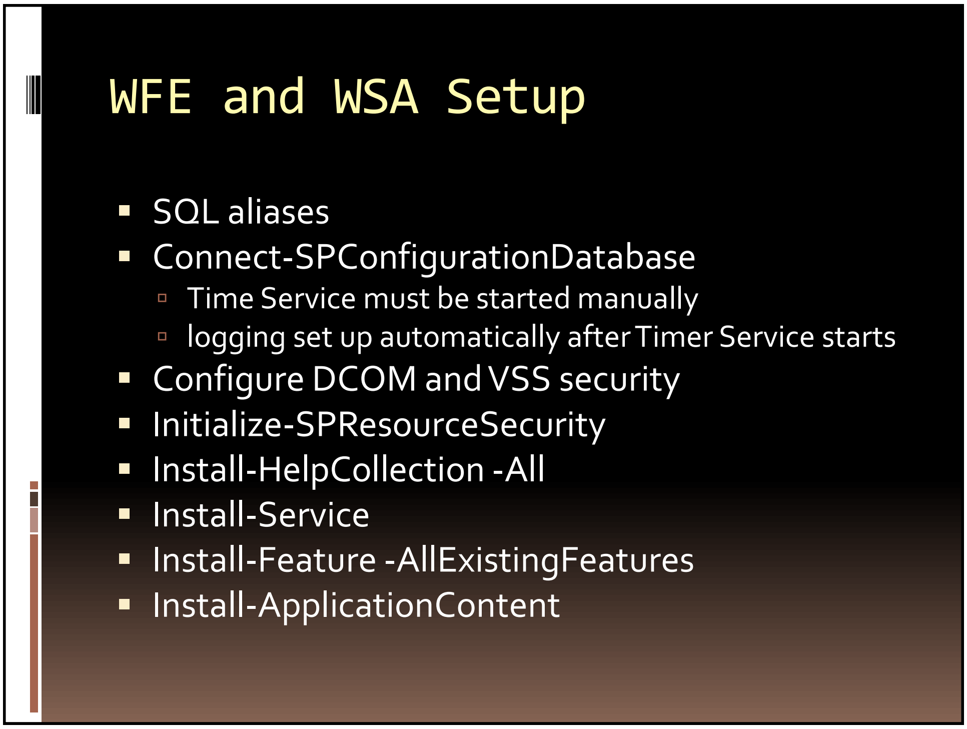
Configuration Cache

- SPTimerv4 service caches configuration locally
- %ALLUSERSPROFILE%\Microsoft\SharePoint\Config\<guid>
  - .XML
  - Cache.INI stores DB version ID
- Updated with job Config Refresh



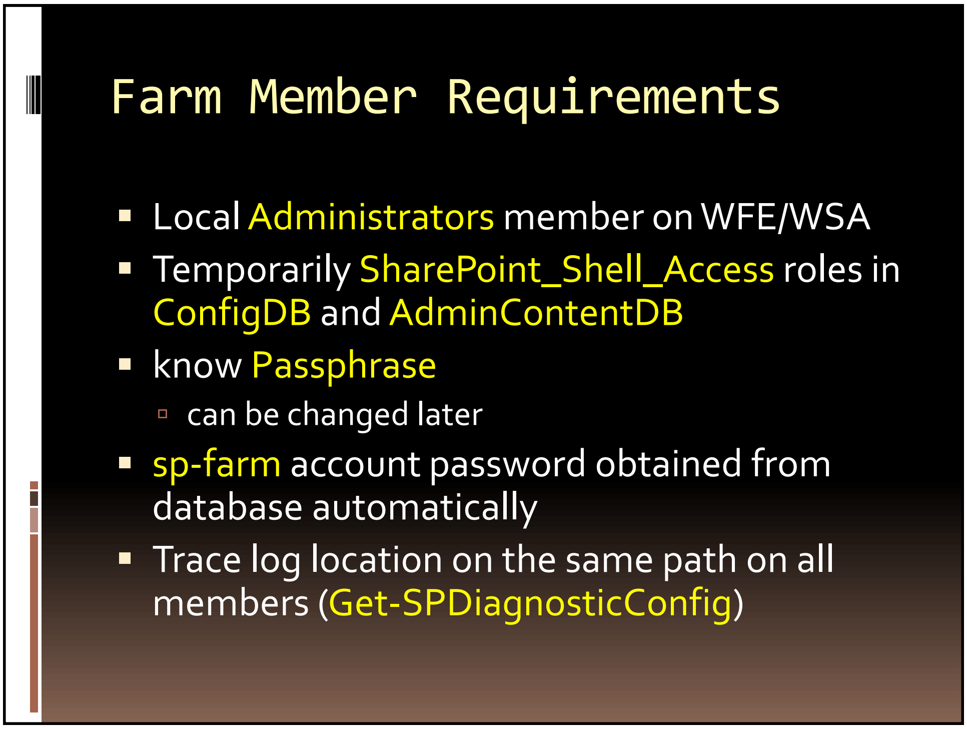
Farm Setup

CONNECT ADDITIONAL MEMBERS



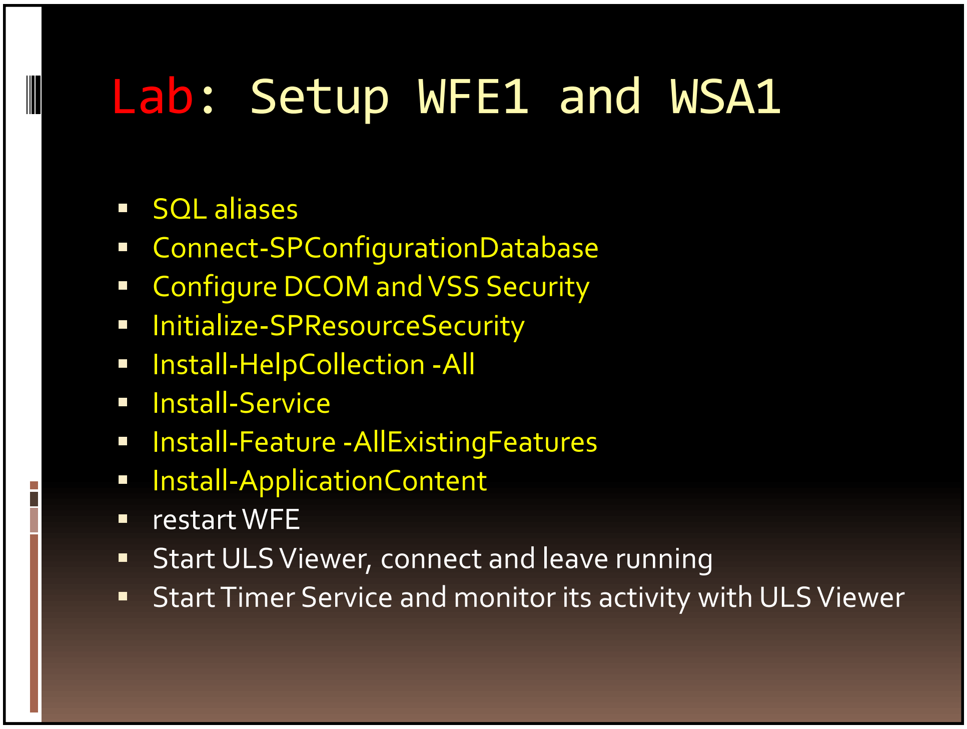
WFE and WSA Setup

- SQL aliases
- Connect-SPConfigurationDatabase
  - Time Service must be started manually
  - logging set up automatically after Timer Service starts
- Configure DCOM and VSS security
- Initialize-SPResourceSecurity
- Install-HelpCollection -All
- Install-Service
- Install-Feature -AllExistingFeatures
- Install-ApplicationContent



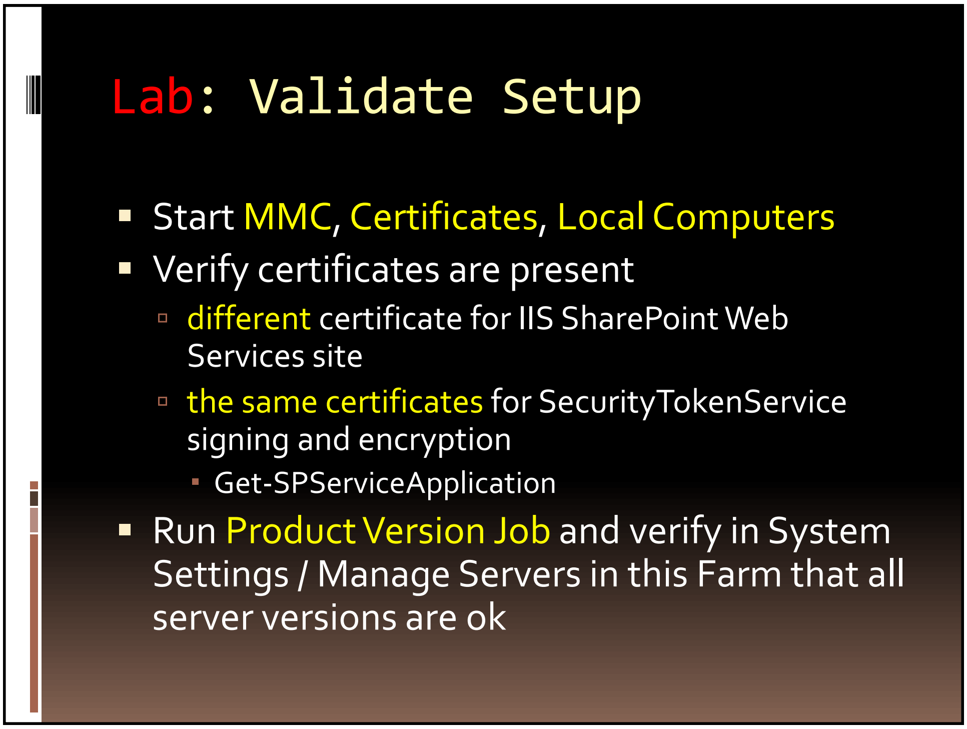
Farm Member Requirements

- Local Administrators member on WFE/WSA
- Temporarily SharePoint_Shell_Access roles in ConfigDB and AdminContentDB
- know Passphrase
  - can be changed later
- sp-farm account password obtained from database automatically
- Trace log location on the same path on all members (Get-SPDiagnosticConfig)



Lab: Setup WFE1 and WSA1

- SQL aliases
- Connect-SPConfigurationDatabase
- Configure DCOM and VSS Security
- Initialize-SPResourceSecurity
- Install-HelpCollection -All
- Install-Service
- Install-Feature -AllExistingFeatures
- Install-ApplicationContent
- restart WFE
- Start ULS Viewer, connect and leave running
- Start Timer Service and monitor its activity with ULS Viewer

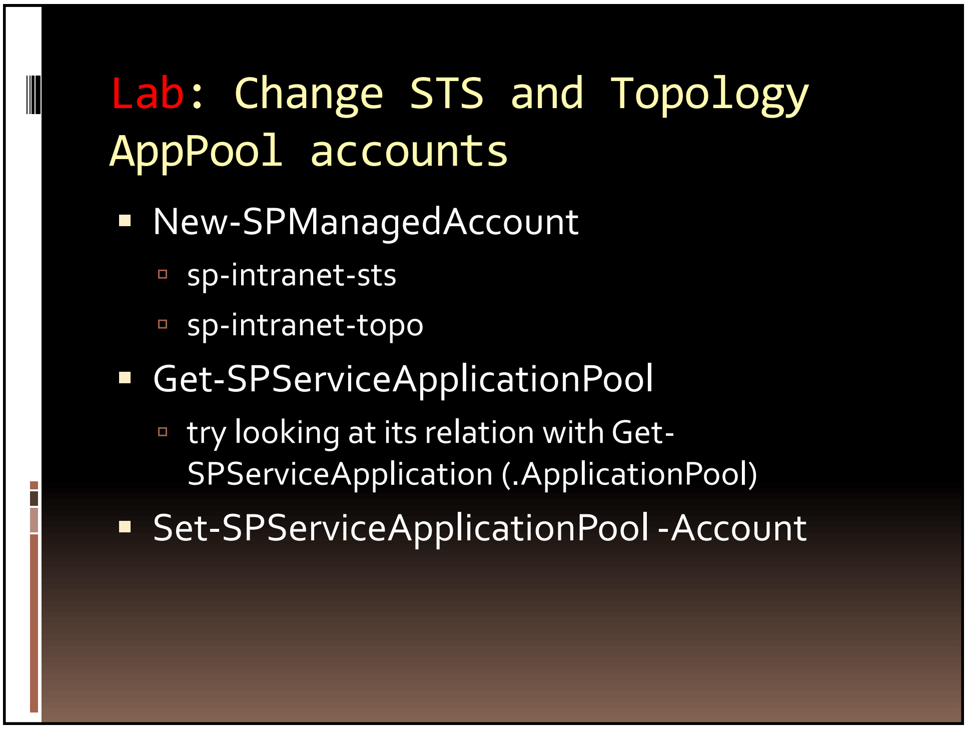


Lab: Validate Setup

- Start MMC, Certificates, Local Computers
- Verify certificates are present
  - different certificate for IIS SharePoint Web Services site
  - the same certificates for SecurityTokenService signing and encryption
    - Get-SPServiceApplication
- Run Product Version Job and verify in System Settings / Manage Servers in this Farm that all server versions are ok

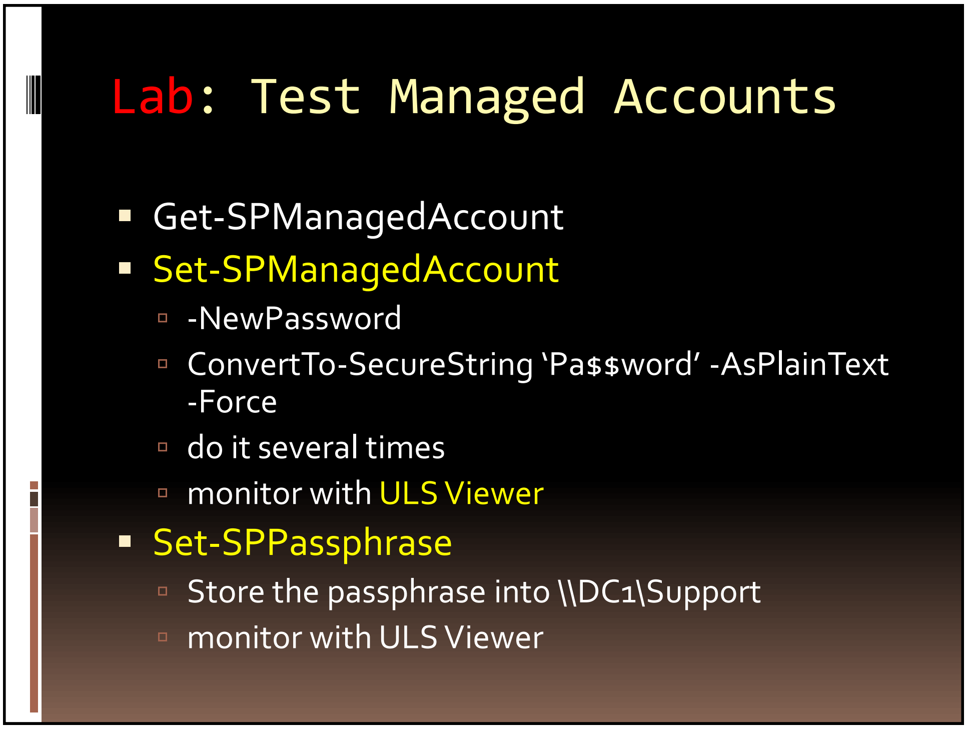
Managed Service Accounts

- Passphrase encrypts passwords in the configuration database
- Farm account stores the passphrase in registry root /Secure



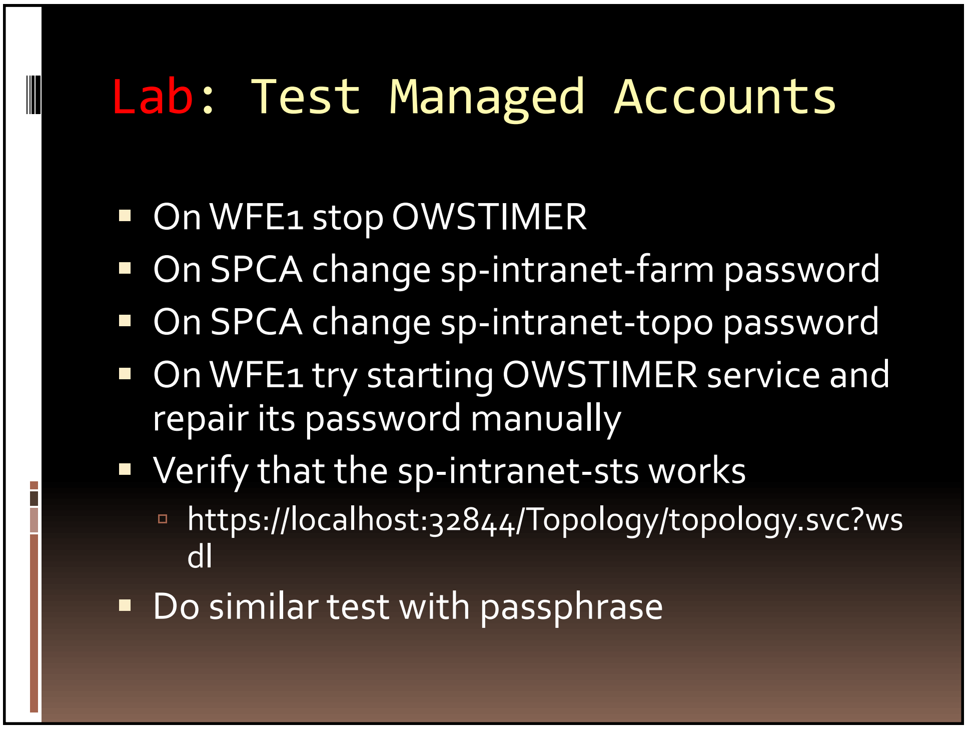
Lab: Change STS and Topology AppPool accounts

- New-SPManagedAccount
  - sp-intranet-sts
  - sp-intranet-topo
- Get-SPServiceApplicationPool
  - try looking at its relation with Get-SPServiceApplication (.ApplicationPool)
- Set-SPServiceApplicationPool -Account



Lab: Test Managed Accounts

- Get-SPManagedAccount
- Set-SPManagedAccount
  - -NewPassword
  - ConvertTo-SecureString ‘Pa$$word’ -AsPlainText -Force
  - do it several times
  - monitor with ULS Viewer
- Set-SPPassphrase
  - Store the passphrase into \\DC1\Support
  - monitor with ULS Viewer



Lab: Test Managed Accounts

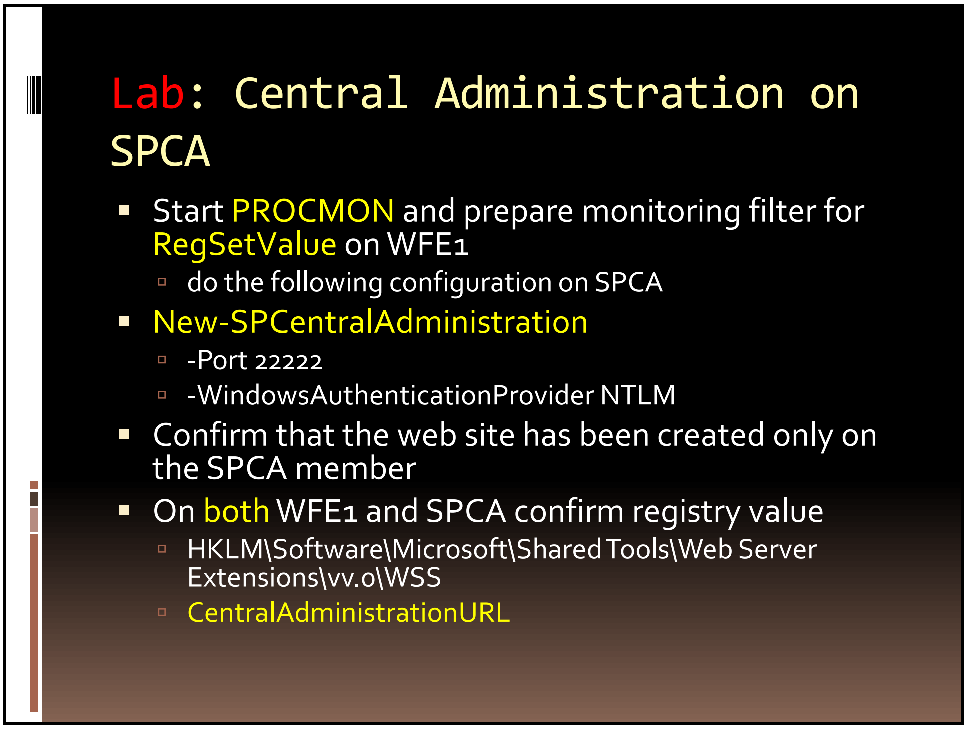
- On WFE1 stop OWSTIMER
- On SPCA change sp-intranet-farm password
- On SPCA change sp-intranet-topo password
- On WFE1 try starting OWSTIMER service and repair its password manually
- Verify that the sp-intranet-sts works
  - https://localhost:32844/Topology/topology.svc?wsdl
- Do similar test with passphrase

Repair-SPManagedAccountDeployment

- Detects and repairs inconsistencies between ConfigDB and local registry and service settings

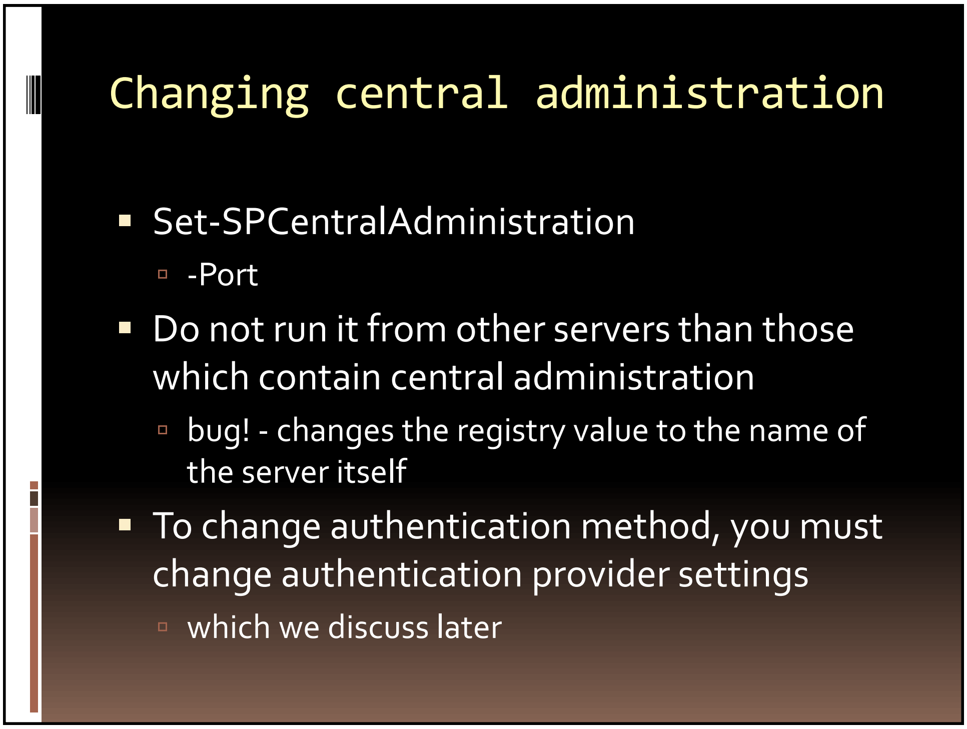
Farm Setup

CENTRAL ADMINISTRATION WEB SITE



Lab: Central Administration on SPCA

- Start PROCMON and prepare monitoring filter for RegSetValue on WFE1
  - do the following configuration on SPCA
- New-SPCentralAdministration
  - -Port 22222
  - -WindowsAuthenticationProvider NTLM
- Confirm that the web site has been created only on the SPCA member
- On both WFE1 and SPCA confirm registry value
  - HKLM\Software\Microsoft\Shared Tools\Web Server Extensions\vv.0\WSS
  - CentralAdministrationURL



Changing central administration

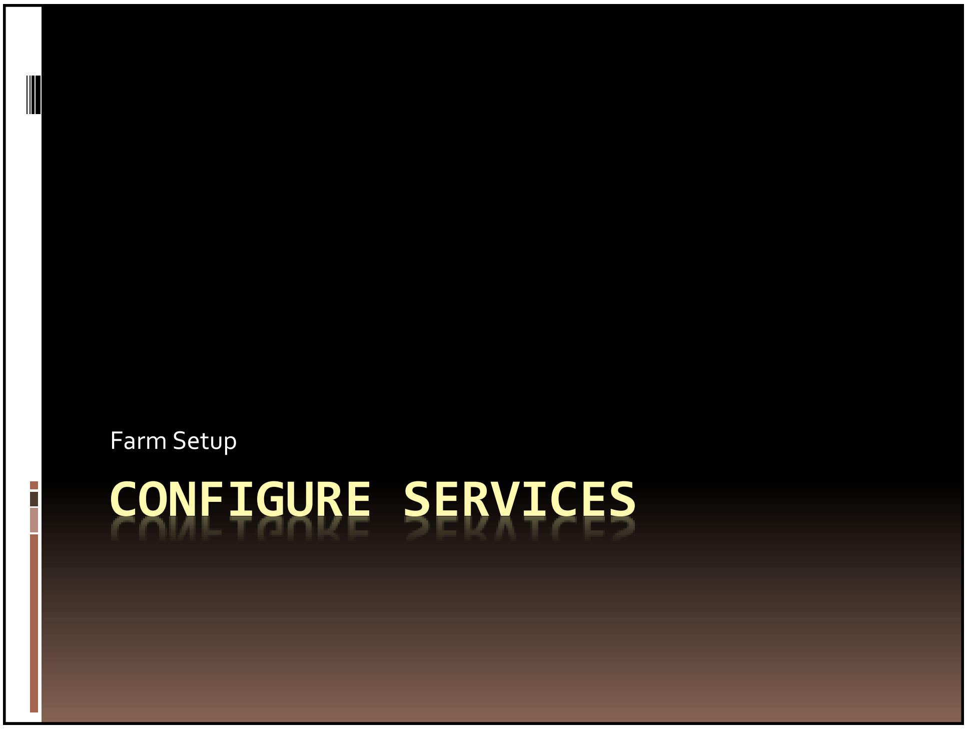
- Set-SPCentralAdministration
  - -Port
- Do not run it from other servers than those which contain central administration
  - bug! - changes the registry value to the name of the server itself
- To change authentication method, you must change authentication provider settings
  - which we discuss later

Lab: Farm Administrators

- Make SP Admins members of Farm Administrators group in Central Administration
- Remove all other user accounts

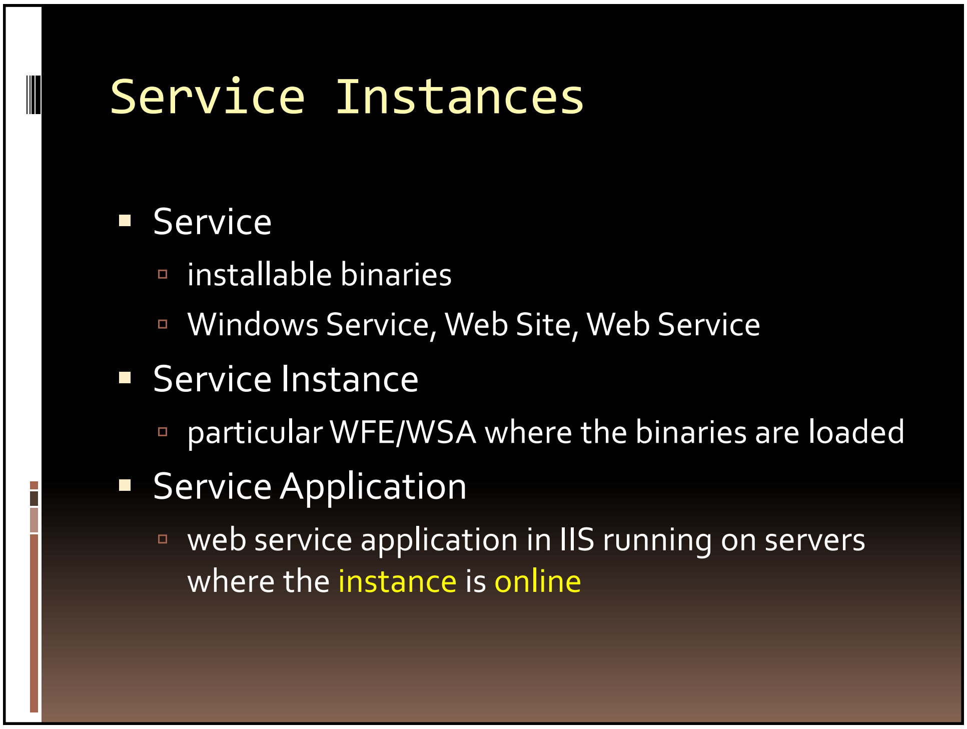
Lab: PowerShell Administrators

- Remove sp-install login from the SQL server
  - verify that he still has full control over the databases. Why?
- Create SP Admins login in the SQL server
- Assign SP Admins the dbcreator and securityadmin server roles
- Assign SP Admins with access as either SharePoint_Shell_Access or SPDataWriter in all relevant databases



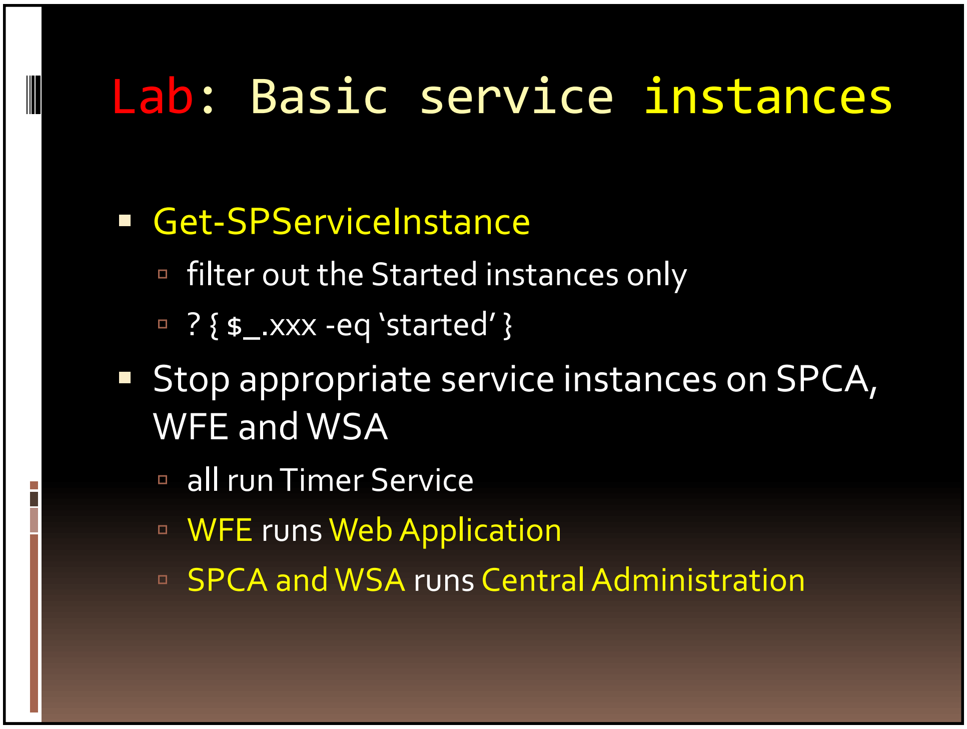
Farm Setup

CONFIGURE SERVICES



Service Instances

- Service
  - installable binaries
  - Windows Service, Web Site, Web Service
- Service Instance
  - particular WFE/WSA where the binaries are loaded
- Service Application
  - web service application in IIS running on servers where the instance is online

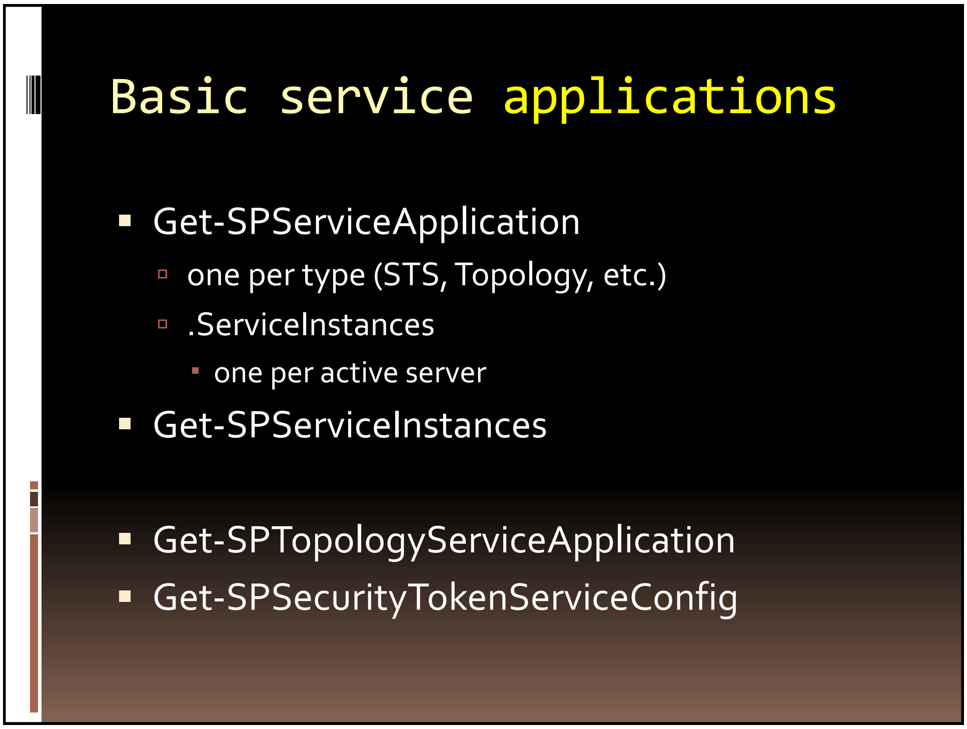


Lab: Basic service instances

- Get-SPServiceInstance
  - filter out the Started instances only
  - ? { $_.xxx -eq 'started' }
- Stop appropriate service instances on SPCA, WFE and WSA
  - all run Timer Service
  - WFE runs Web Application
  - SPCA and WSA runs Central Administration

Basic service applications

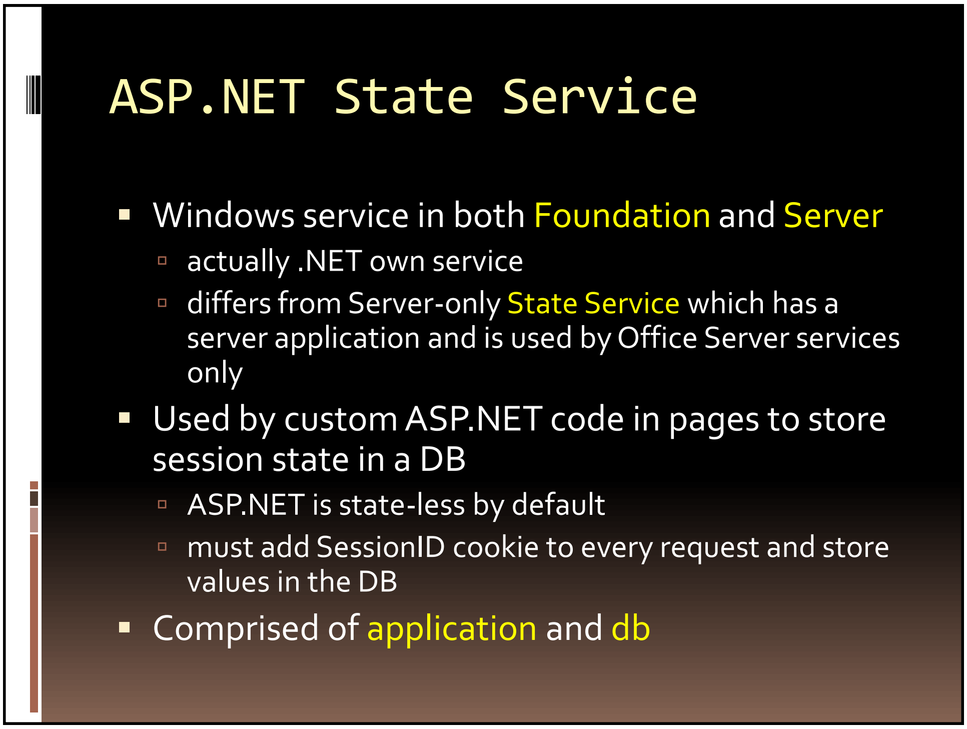
- SecurityTokenService
  - instances on all farm members by default
- Application Discovery and Load Balancer Service
  - instances on all farm members by default



Basic service applications

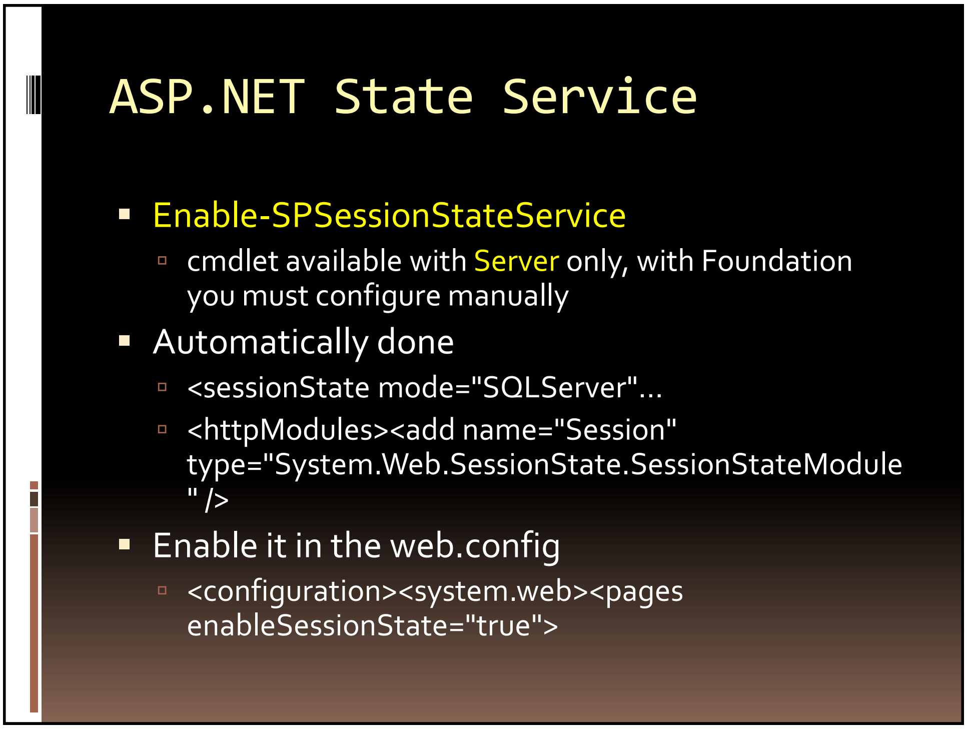
- Get-SPServiceApplication
  - one per type (STS, Topology, etc.)
  - .ServiceInstances
    - one per active server
- Get-SPServiceInstances

- Get-SPTopologyServiceApplication
- Get-SPSecurityTokenServiceConfig



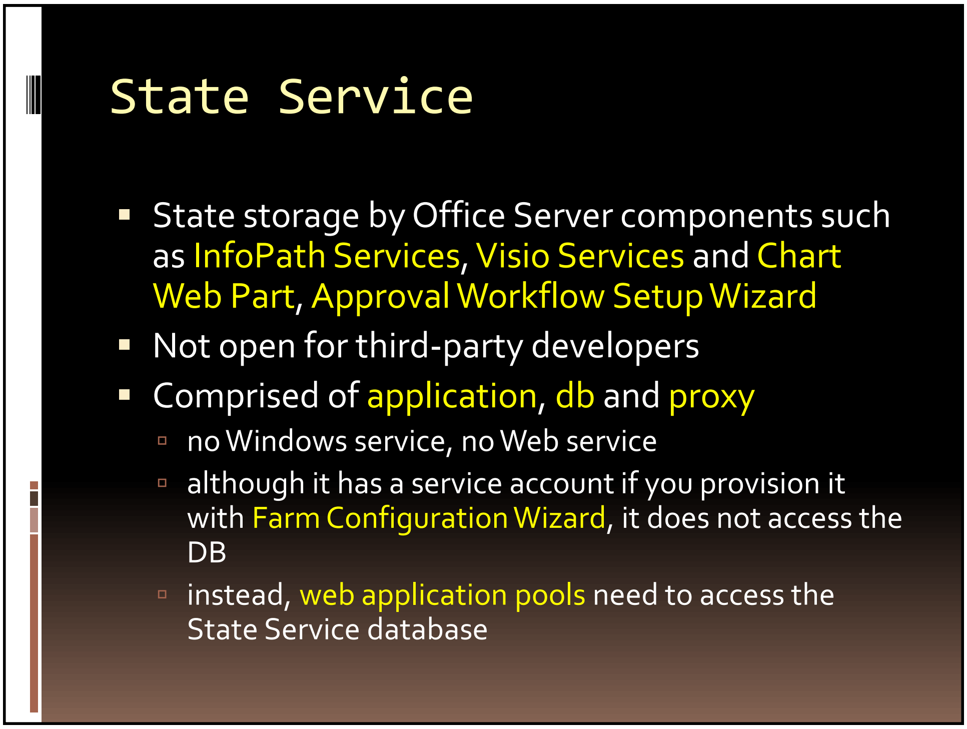
ASP.NET State Service

- Windows service in both Foundation and Server
  - actually .NET own service
  - differs from Server-only State Service which has a server application and is used by Office Server services only
- Used by custom ASP.NET code in pages to store session state in a DB
  - ASP.NET is state-less by default
  - must add SessionID cookie to every request and store values in the DB
- Comprised of application and db



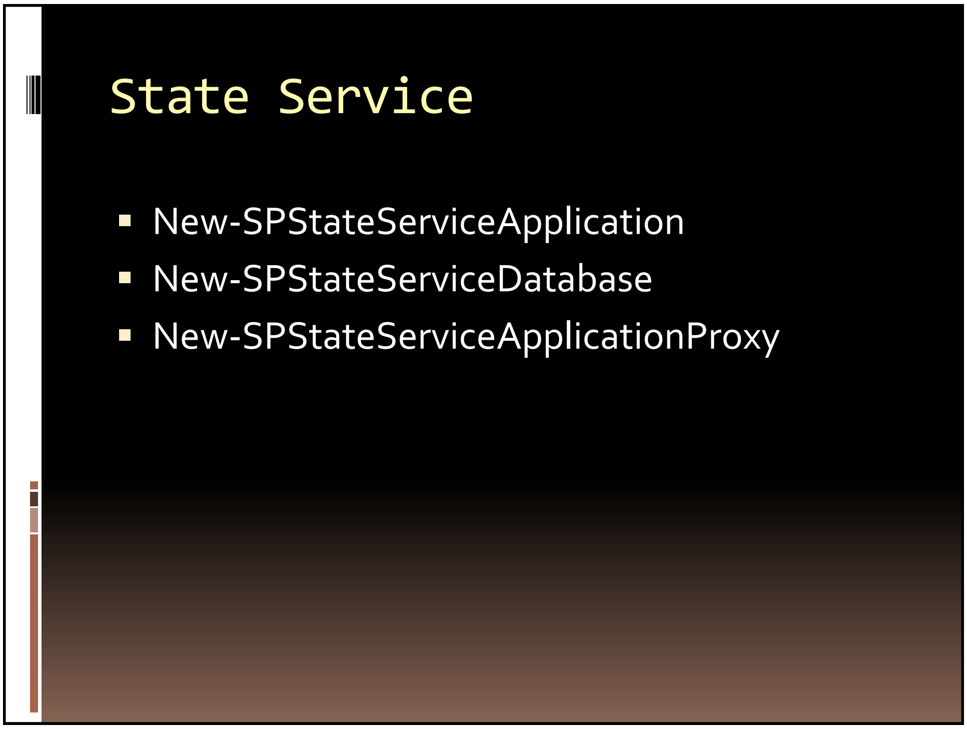
ASP.NET State Service

- Enable-SPSessionStateService
  - cmdlet available with Server only, with Foundation you must configure manually
- Automatically done
  - <sessionState mode="SQLServer"…
  - <httpModules><add name="Session" type="System.Web.SessionState.SessionStateModule " />
- Enable it in the web.config
  - <configuration><system.web><pages enableSessionState="true">



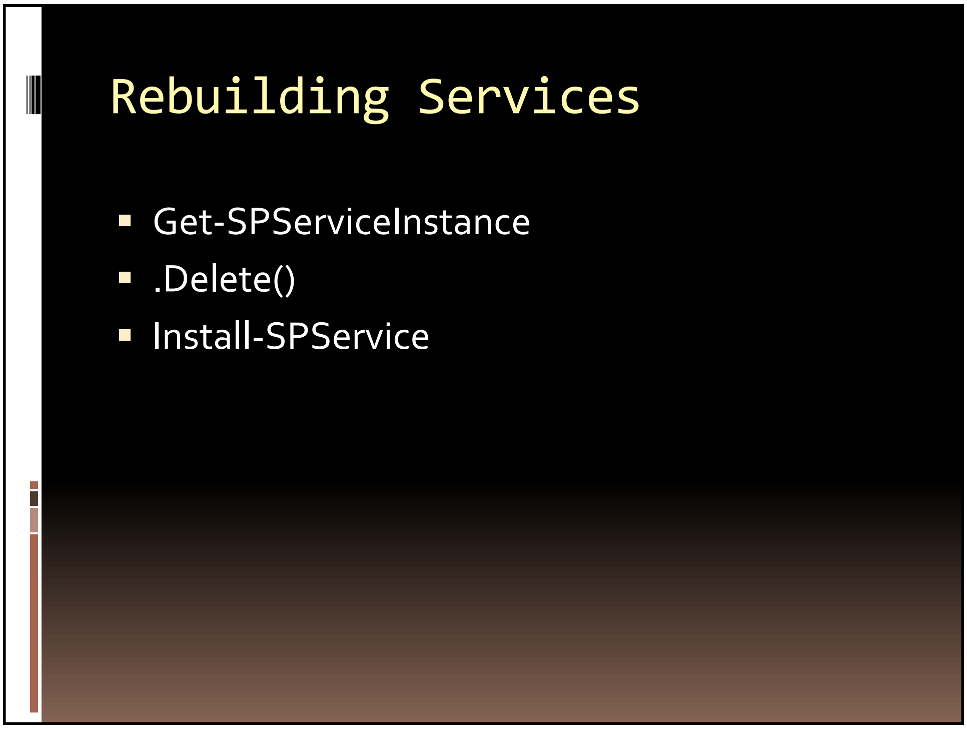
State Service

- State storage by Office Server components such as InfoPath Services, Visio Services and Chart Web Part, Approval Workflow Setup Wizard
- Not open for third-party developers
- Comprised of application, db and proxy
  - no Windows service, no Web service
  - although it has a service account if you provision it with Farm Configuration Wizard, it does not access the DB
  - instead, web application pools need to access the State Service database



State Service

- New-SPStateServiceApplication
- New-SPStateServiceDatabase
- New-SPStateServiceApplicationProxy

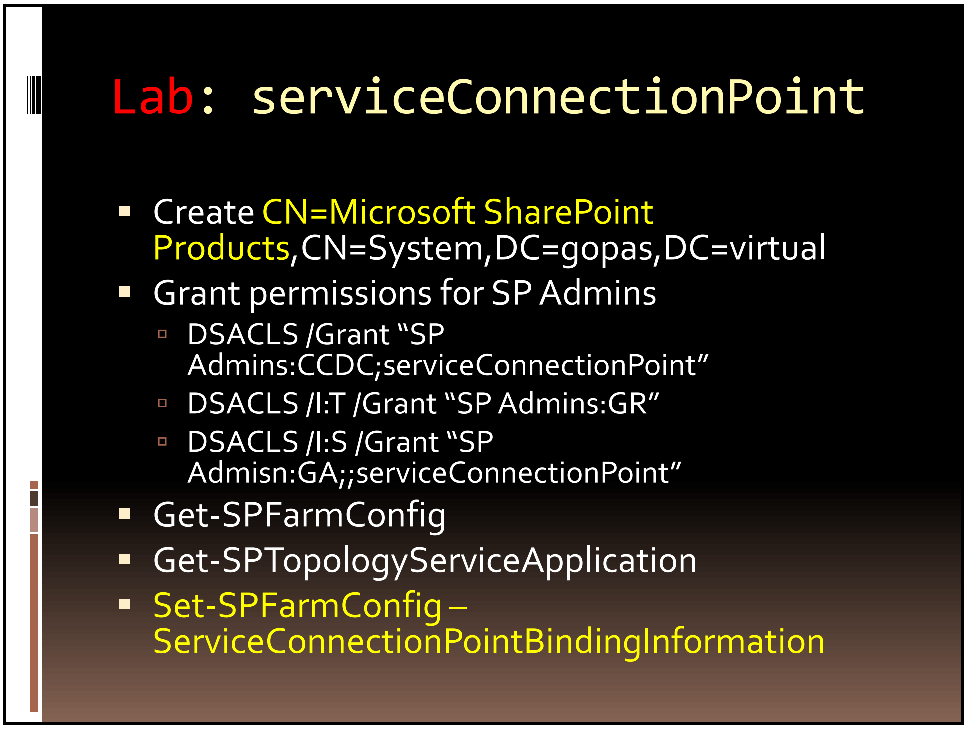


Rebuilding Services

- Get-SPServiceInstance
- .Delete()
- Install-SPService

Farm Setup

DEFINE SERVICECONNECTIONPOINT



Lab: serviceConnectionPoint

- Create CN=Microsoft SharePoint Products,CN=System,DC=gopas,DC=virtual
- Grant permissions for SP Admins
  - DSACLS /Grant “SP Admins:CCDC;serviceConnectionPoint”
  - DSACLS /I:T /Grant “SP Admins:GR”
  - DSACLS /I:S /Grant “SP Admisn:GA;;serviceConnectionPoint”
- Get-SPFarmConfig
- Get-SPTopologyServiceApplication
- Set-SPFarmConfig – ServiceConnectionPointBindingInformation