Troubleshooting Active Directory

Course outline

Module 1: Installing and configuring domain controllers

- DCPROMO Different Scenarios (NewDC / Additional DC / ChildDC / TreeDC).
- Schema related issue
- Validating the Health of Domain Controllers.
- Unable to make a Domain Controller as a Global Catalog issue
- How to Verify DNS record registration and DNS
- FSMO transfer and Seize scenario.

Tools Usage : DCPromo Log, Netsetup.log, File System, Net share, DCIDAG, Services, Event Logs, Ntdsutil

Module 2: Managing objects in AD DS

- Understand Objects, Attributes and Classes.
- Connecting to different Types of Partitions and their Scope of Replication.
- How Extending Schema, Functional Levels impact from Application Standpoint.
- Domain join issues
- Secure channel issues

Tools Usage : Adsiedit, MMC, Services, Event Logs, Nltest, Netdom, ADUC, ADAC

Module 3: Advanced AD DS infrastructure management

- Pre-Req of Creation of Trusts and management of Trusts by the PDC
- Issues while creating Trust
- Issues while accessing a Resource from one domain to another domain
- Trusted Domain Object and the Domain$$$ object
- Advantages and Dis-advantages of Each type of Trusts
- Domain join issues.
- Netlogon DC Discovery and Netlogon Debug levels
- Generic Records and the Site-Specific Records for DC Discovery.
- DynamicSiteName Vs SiteName under registry
- Netlogon Service creates the Netlogon.dns file

Tools Usage : Domain.msc, Adsiedit, MMC, Services, Event Logs, Network Monitor, ADUC, ADAC, Netsetup.log, Netlogon.log, DNS.

Module 4: Implementing and administering AD DS sites and replication

- Understanding Static and Dynamic Ports.
- RPC Based Application and End Point Mapper service (EPM).
- RPC Client and RPC Service negotiation.
- AD Replication between 2 DC's using Netmon.
- Using PortQueryUI and RPCDump to identify the Open ports.
- What is the difference between Version Number and USN?
- What is Highest Committed USN and where is that stored (RootDSE) ?
- How Replication Engine Replicates an Object from one DC to another DC?
- What is the difference between Upto-Dateness Vector and high Water Mark (Direct Upto-Dateness Vector) ?
- How to enable Replication events to view replication Summary?
- How to use Replication status tool to verify Enterprise Replication?
- How to use repadmin commands to view replication summary?
- Lingering objects events 1988.
- Troubleshooting most common AD replication errors:
    - Replication Access was denied.
    - Access is denied.
    - Target Principal name is incorrect.
    - Target account name is incorrect.
    - DNS lookup failure
    - There are no more endpoint available from the endpoint mapper

Tools Usage : Repadmin, Adsiedit, Services, Event Logs, Network Monitor, PortQueryUI, RPCDump.

Module 5: Implementing Group Policy

- Reviewing various components of a New Group Policy in GPC / GPT
- Reviewing GPCUserExtensions or GPTComputerExtensions
- Reviewing GPLINK and GPOPTIONS Attribute and where is this Attribute Stored?
- Various type of Filtering that we could use to apply / Deny Applying of Group Policy Objects?
- Group Policy is not reaching the client machine.
- Group Policy is not getting applied.
- Reading Gpsvc.log

- Common GPO Troubleshooting Scenarios

Tools Usage : Group Policy Events, Network Monitor, Gpsvc.log, Winlogon.log, RSOP, GPRESULT, Registry.

Module 6: Managing user settings with Group Policy

- Different Types of Profiles and where do we Load from 1st Time and then Subsequent Times.
- Roaming Profile Path not reachable : Temp Profile
- Users SID Removed from Registry and file system : New Folder Username.DomainName
- Users Folder Deleted but Registry Intact : Temp Profile
- Changed the ProfileImage Path in registry : Temp Profile
- Enabling Group Policy Preferences Debug Logging using the RSAT

Tools Usage : Group Policy Events, Winlogon.log, RSOP, GPRESULT, Registry, RSAT

Module 7: Securing Active Directory Domain Services

- How to Prepare Windows Server for the installation of a Read Only Domain Controller?
- How to Test the Password Replication Policy?
- Administrator Role Separation?
- What is difference between Password Policy Vs Account Lockout Policy?
- User rights assignments for Default domain controller policy.
- How Bad Passwords are chained to the PDC by Other DC's?
- What events we found in the Security Logs of the DC / Member Server and the client machine?
- Difference between c000006a vs c0000234?
- How to troubleshoot Account Lockout issues and determine the Client machine?
- What are the 5 Reasons where you get "APP_ERR_Modified"?
- What are the 5 Reasons when Kerberos would fall back to NTLM ?
- Common Authentication errors
    - KDC_ERR_S_PRINCIPAL_UNKNOWN [Service Principal Unknown]
    - KDC_ERR_C_PRINCIPAL_UNKNOWN [Client Principal Unknown]
    - KRB_AP_ERR_MODIFIED [Service is unable to decrypt the ticket]
    - KDC_ERR_BADOPTION [Typically associated with Kerberos delegation issues]
    - KRB_AP_ERR_SKEW
    - KDC_ERR_ETYPE_NOTSUPP
    - KRB_AP_ERR_REPEAT

Tools Usage : Network Monitor, Netlogon.log, Security Events, Account Lockout Tools, GPRESULT, Registry, RSAT, Gpmc.msc.

Module 8: Deploying and managing AD CS

- Difference between Encryption (Symmetric and Asymmetric), Hashing & Digital Signature
- Different Algorithm used for Encryption (Symmetric and Asymmetric) and Hashing
- What is CNG (CAPI2)
- How to use PKIView to monitor all your enterprise CAs and their current health state?
- Enabling certificate Auditing using Certificate Authrority console.
- CA is not configured to include CDP locations in the extensions of issued certificates.
- Clients might not be able to locate a CRL to check the revocation status of a certificate.
- Certificate validation failing
- Certificate template is not published on a CA.
- AIA URL is configured incorrectly on the extensions tab of the CA.

Tools Usage : Adsiedit, MMC, Services, Event Logs, Network Monitor, ADUC, ADAC, Pkiview.msc, Certutil, Capi2.

Module 9: Deploying and managing certificates

- Different Components about Microsoft Implementation of PKI Infrastructure.
- What is the difference Self Signed Cert to an Cert issued by a Public CA or Enterprise CA
- How did we view the Public Key and Private key association of a Certificate at MMC perspective
- Certificate template versions and required permissions.
- Performing revocation check of an issued certificate.
- LDAP over SSL not working
- Auto enrollment is not working
- Smart Card Authentication is not working
- How to troubleshoot Certificate Enrollment in the MMC Certificate Snap-in.
- How did we generate a Self Signed Certificate
- Certificate Validation using CAPI2, Network Monitor and Certutil -verify -urlfetch

Tools Usage : Adsiedit, MMC, Services, Event Logs, Network Monitor, ADUC, ADAC, Pkiview.msc, Certutil, Capi2.

Module 12: Implementing AD DS synchronization with Microsoft Azure AD

- Using fiddler to troubleshoot Azure AD authentication issue.
- Password hash synchronization issues with Azure AD Connect sync
- Azure Active Directory Pass-through Authentication issues
- How to Troubleshoot object synchronization with Azure AD Connect sync.
- Troubleshooting common errors during synchronization
    - Data Mismatch Errors – InvalidSoftMatch
    - Data Mismatch Errors – ObjectTypeMismatch
    - Duplicate Attributes – AttributeValueMustBeUnique
    - Data Validation Failures - IdentityDataValidationFailed

Tools Usage : Azure AD portal, AD sync server, Services, Event Logs, Fiddler.

Module 13: Monitoring, managing, and recovering AD DS

- Slow logon vs Slow boot
- "Verbose vs normal status messages" group policy setting
- Performing Active Directory database maintenance
- LSASS Memory Leak
- LSASS CPU Spike
- LSASS Crash
- Understanding ATQ performance counters to handle requests from Kerberos and LDAP.
- LDAP considerations
- Proper placement of domain controllers and site considerations
- Capacity Planning for Active Directory Domain Services

Tools Usage : Adsiedit, MMC, Services, Event Logs, Network Monitor, Perfmon, Userenv.log.