Identity with Windows Server 2016

Course Outline – (70-742)

Please note that the questions may test on, but will not be limited to, the topics described in the bulleted text

Install and configure Active Directory Domain Services (AD DS) (20–25%)

- Install and configure domain controllers
  - Install a new forest, add or remove a domain controller from a domain, upgrade a domain controller, install AD DS on a Server Core installation, install a domain controller from Install from Media (IFM), resolve DNS SRV record registration issues, configure a global catalog server, transfer and seize operations master roles, install and configure a read-only domain controller (RODC), configure domain controller cloning
- Create and manage Active Directory users and computers
  - Automate the creation of Active Directory accounts; create, copy, configure, and delete users and computers; configure templates; perform bulk Active Directory operations; configure user rights; implement offline domain join; manage inactive and disabled accounts; automate unlocking of disabled accounts using Windows PowerShell; automate password resets using Windows PowerShell
- Create and manage Active Directory groups and organizational units (OUs)
  - Configure group nesting; convert groups, including security, distribution, universal, domain local, and domain global; manage group membership using Group Policy; enumerate group membership; automate group membership management using Windows PowerShell; delegate the creation and management of Active Directory groups and OUs; manage default Active Directory containers; create, copy, configure, and delete groups and OUs

Manage and maintain AD DS (15–20%)

- Configure service authentication and account policies
  - Create and configure Service Accounts, create and configure Group Managed Service Accounts (gMSAs), configure Kerberos Constrained Delegation (KCD), manage Service Principal Names (SPNs), configure virtual accounts, configure domain and local user password policy settings, configure and apply Password Settings Objects (PSOs), delegate password settings management, configure account lockout policy settings, configure Kerberos policy settings within Group Policy
- Maintain Active Directory
  - Back up Active Directory and SYSVOL, manage Active Directory offline, perform offline defragmentation of an Active Directory database, clean up metadata, configure Active Directory snapshots, perform object- and

container-level recovery, perform Active Directory restore, configure and restore objects by using the Active Directory Recycle Bin, configure replication to Read-Only Domain Controllers (RODCs), configure Password Replication Policy (PRP) for RODC, monitor and manage replication, upgrade SYSVOL replication to Distributed File System Replication (DFSR)

- Configure Active Directory in a complex enterprise environment
  - Configure a multi-domain and multi-forest Active Directory infrastructure; deploy Windows Server 2016 domain controllers within a pre-existing Active Directory environment; upgrade existing domains and forests; configure domain and forest functional levels; configure multiple user principal name (UPN) suffixes; configure external, forest, shortcut, and realm trusts; configure trust authentication; configure SID filtering; configure name suffix routing; configure sites and subnets; create and configure site links; manage site coverage; manage registration of SRV records; move domain controllers between sites

Create and manage Group Policy (25–30%)

- Create and manage Group Policy Objects (GPOs)
  - Configure a central store; manage starter GPOs; configure GPO links; configure multiple local Group Policies; back up, import, copy, and restore GPOs; create and configure a migration table; reset default GPOs; delegate Group Policy management; detect health issues using the Group Policy Infrastructure Status dashboard
- Configure Group Policy processing
  - Configure processing order and precedence, configure blocking of inheritance, configure enforced policies, configure security filtering and Windows Management Instrumentation (WMI) filtering, configure loopback processing, configure and manage slow-link processing and Group Policy caching, configure client-side extension (CSE) behaviour, force a Group Policy update
- Configure Group Policy settings
  - Configure software installation, configure folder redirection, configure scripts, configure administrative templates, import security templates, import a custom administrative template file, configure property filters for administrative templates
- Configure Group Policy preferences
  - Configure printer preferences, define network drive mappings, configure power options, configure custom registry settings, configure Control Panel settings, configure Internet Explorer settings, configure file and folder deployment, configure shortcut deployment, configure item-level targeting

Implement Active Directory Certificate Services (AD CS) (10–15%)

- Install and configure AD CS

    - Install Active Directory Integrated Enterprise Certificate Authority (CA), install offline root and subordinate CAs, install standalone CAs, configure Certificate Revocation List (CRL) distribution points, install and configure Online Responder, implement administrative role separation, configure CA backup and recovery
- Manage certificates
    - Manage certificate templates; implement and manage certificate deployment, validation, and revocation; manage certificate renewal; manage certificate enrollment and renewal for computers and users using Group Policies; configure and manage key archival and recovery

Implement identity federation and access solutions (15–20%)

- Install and configure Active Directory Federation Services (AD FS)
    - Upgrade and migrate previous AD FS workloads to Windows Server 2016; implement claims-based authentication, including Relying Party Trusts; configure authentication policies; configure multi-factor authentication; implement and configure device registration; integrate AD FS with Microsoft Passport; configure for use with Microsoft Azure and Office 365; configure AD FS to enable authentication of users stored in LDAP directories
- Implement Web Application Proxy (WAP)
    - Install and configure WAP, implement WAP in pass-through mode, implement WAP as AD FS proxy, integrate WAP with AD FS, configure AD FS requirements, publish web apps via WAP, publish Remote Desktop Gateway applications, configure HTTP to HTTPS redirects, configure internal and external Fully Qualified Domain Names (FQDNs)
- Install and configure Active Directory Rights Management Services (AD RMS)
    - Install a licensor certificate AD RMS server, manage AD RMS Service Connection Point (SCP), manage AD RMS templates, configure Exclusion Policies, back up and restore AD RMS