SP1 Server Administration

INHALTLICHE RICHTZIELE DER MODULPRÜFUNG

- eine bestehende Serverinfrastruktur überwachen und gängige Wartungsarbeiten durchführen
- grundlegende Dienste eines Server-Betriebssystems erläutern, konfigurieren, betreiben und warten
- Sicherheitseinstellungen gemäss Vorgaben vornehmen und Sicherheitsmassnahmen ausführen
- Server-Abnahmeprotokolle und Server-Dokumentation erstellen und nachführen
- Serverumgebung virtualisieren und virtualisiert betreiben
- Home-Office User/Remote-Worker und Geschäftsaussenstellen/Filialen sicher mit Hauptsitz verbinden
- IT-Infrastrukturen in On-Premise-, Cloud- und hybriden Umgebungen planen, konfigurieren und betreiben

HANDLUNGSZIELE/LERNZIELE DER MODULPRÜFUNG

1 Betrieb und Unterhalt eines Servers (On-Prem & Cloud)

1.1 kann grundlegenden Dienste eines Server-Betriebssystems erläutern, konfigurieren und überwachen

1.1.1 Funktionen grundlegender Serverdienste (Rollen & Features, Dienste, Verwaltung via Windows-Admin Center) in eigenen Worten erläutern und Zusammenspiel aufzeigen

1.1.2 Systemprotokolle und Logdateien interpretieren und konfigurieren (Ereignisanzeige, Performance Monitor)

1.1.3 Gängige Authentifizierungsverfahren im Windows-/Linux-/Hybrid-Umfeld (Kennwort, Kerberos, NTLMv2, Zertifikat/Smartcard, FIDO2/WebAuthn, MFA via Entra ID/Azure AD, Conditional Access) voneinander abgrenzen und einem Szenario zuordnen

1.2 kann einfache Konfigurations- und Wartungsarbeiten mittels PowerShell durchführen

1.2.1 einfaches Skript (PowerShell) strukturiert aufbauen und dokumentieren

1.2.2 Mit PowerShell Änderungen an Registry, Diensten oder Gruppenrichtlinien lokal oder remote vornehmen

1.2.3 Konfigurations- und Wartungsarbeiten per PowerShell oder Windows Admin Center automatisieren

2 Server-Dienste (DNS, DHCP, Deployment, Cloud)

2.1 kann DNS-Dienst konfigurieren

2.1.1 DNS-Server in den Varianten (primär, sekundär, caching-only, Forwarder) installieren und Zonentransfer konfigurieren

2.1.2 Einträge (SOA, NS, A, PTR, CNAME, SRV) einrichten, anpassen und löschen

2.1.3 DNS-Einträge für Cloud-/M365-/Hybrid-Szenarien (SRV, TXT, Autodiscover, SPF, DKIM, DMARC-Grundprinzip, Exchange Online) einrichten und testen

2.1.4 Split-Brain-DNS / Private DNS-Zonen im Hybrid-Kontext erklären

2.1.5 DNS absichern (Zonenübertragung einschränken, DNSSEC, Logging aktivieren)

2.2 kann DHCP-Dienst installieren und konfigurieren

2.2.1 DHCP-Dienst auf Windows Server ausfallsicher installieren und konfigurieren

2.2.2 DHCP-Optionen für VoIP, VPN, M365, PXE definieren

2.3 kann Cloud-Dienste integrieren

2.3.1 Unterschiede von IaaS, PaaS, SaaS benennen

2.3.2 Eine einfache VM in Azure oder AWS beschreiben (Region, VNet/VPC, Security Group/NSG) und in ein bestehendes Netz-Schema einordnen

3 Virtualisierung, Container & Plattformvielfalt

3.1 kann die Grundlagen der Virtualisierung erläutern

3.1.1 Verschiedene Formen der Virtualisierung (Server, Desktop, Storage, Netzwerk) erläutern

3.1.2 Begriffe wie Software Defined Network (SDN) im Rahmen der Virtualisierung erläutern

3.1.3 Vor- und Nachteile verschiedener Containerformen (Docker, Windows-Container, Hyper-V-Container) aufzeigen

3.1.4 Vergleich Service als Container vs. Service als VM bezüglich Patchen, Backup, Security

3.1.5 Lizenzproblematik in einer virtualisierten Umgebung erläutern

3.1.6 Unterschied „klassische Hyper-V-/VMware-VM“ vs. „Workload in Azure/AWS/GCP“ einordnen

3.1.7 Grundidee von Kubernetes bzw. Container-Orchestrierung erklären

3.2 kann Virtualisierungshost und VMs bereitstellen

3.2.1 Hyper-V-Rolle installieren

3.2.2 Virtuelle Maschinen über GUI, PowerShell oder erstellen

3.2.3 Virtuelle Maschinen über GUI, PowerShell oder Windows Admin Center erstellen

3.2.4 Virtuelle Switches erstellen und VLAN konfigurieren

3.2.5 NIC-Teaming / vSwitch-Anbindung umsetzen

3.2.6 Container-Host installieren und einen einfachen Containerdienst (z.B. Webserver) starten

SP1 Server Administration

4 Remote Access / Homeoffice / VPN

4.1 kann zwei Standorte sicher verbinden

4.1.1 Aussenstelle über VPN mit Hauptsitz verbinden (IKEv2, L2TP/IPsec, Site-to-Site, Always On VPN)

4.1.2 Replizierte bzw. gecachte Dienste (RODC,) in einer Aussenstelle nach Vorgaben bereitstellen

4.1.3 Sicherheitsanforderungen für Remotezugriffe (MFA, Gerätecompliance, Einschränkung auf definierte Ports/Protokolle, Protokollierung) beurteilen

4.2 kann Remote Desktop / Applikationen bereitstellen

4.2.1 RDP-/Remote-Dienste über moderne Schutzmechanismen absichern (RDP over TLS, NLA, RD-Gateway, Reverse Proxy, Azure App Proxy)

4.2.2 Anwenderszenario „Remote-Arbeit in die Cloud veröffentlichen“ erläutern (VDI / AVD / AWS Workspaces – Überblick)

5 Web-, Datei- und Mail-/Collaboration-Server

5.1 kann die Funktionsweise eines Web- und Mail-Servers erläutern

5.1.1 Einsatzgebiete eines Web- und sicheren Dateiservers (FTPS, SFTP, HTTPS) in den Varianten OnPrem, Cloud und Hybrid unter den Aspekten Wartung, Sicherheit und Kosten erklären

5.1.2 Grundlegende Konfigurationseinstellungen für einen sicheren Web-/FTPS-/HTTPS-/SFTP-Betrieb (TLS 1.2/1.3, Zertifikate, Härtung von IIS/Apache/Nginx, Logging) erläutern

5.1.3 Inhalt und Aufbau eines Zertifikats erläutern können

5.1.4 Anforderungen an Mailflow und DNS für Exchange Online / Hybrid (Autodiscover, SPF, DKIM, M365-Endpunkte) benennen

5.1.5 Einfaches Reverse-Proxy-/Publishing-Szenario (z.B. RDP/OWA) erläutern

5.2 kann Web- und Datei-/Publishing-Dienste konfigurieren und betreiben

5.2.1 Web-Server (inkl. Komponenten) installieren und konfigurieren

5.2.2 SSL und Server-Authentifizierungsmethoden (inkl. Web-Server-Zertifikat) einrichten

5.2.3 Exchange-Online-/Hybrid-Anbindung im Überblick konfigurieren (kein vollständiger On-Prem-Aufbau)

6 Verzeichnisdienste / Identität / Hybrid-ID

6.1 kann wichtige Kategorien von Verzeichnisdienstinformationen erläutern

6.1.1 Aufgaben und Funktionsweise verschiedener Verzeichnisdienste (AD DS,LDAP, FreeIPA, Cloud-ID) erläutern

6.1.2 AD OnPrem zu Entra ID / Azure AD / Cloud-ID (AAD Connect / Cloud Sync /nur-Cloud-Identität) unterscheiden

6.1.3 Grundidee rollenbasierte Zugriffssteuerung (RBAC) erklären

6.2 kann den Aufbau einer einfachen Domänenstruktur erläutern

6.2.1 Active-Directory-Konzept lesen und nachführen

6.3 kann eine Server-Installation mit AD-Struktur erweitern und pflegen

6.3.1 Benutzer, Gruppen, Organisationseinheiten usw. mittels PowerShell automatisiert erstellen

6.3.2 Gelöschte AD-Objekte wiederherstellen

6.4 kann serverbasierte Benutzerprofile einsetzen

6.4.1 GPOs im Zusammenhang mit Anmeldeprozessen einsetzen

6.4.2 Einfache Anmeldeskripte schreiben

7 Datenträgerverwaltung / Storage / DFS / HA

7.1 kann Möglichkeiten zur Hochverfügbarkeit im Storagebereich aufzeigen

7.1.1 Möglichkeiten zur Verbesserung der Verfügbarkeit von Storage erläutern

7.1.2 Hardware- und Software-RAID-Levels mit Vor-/Nachteilen erläutern

7.1.3 SMB 3.x/3.1.1-Features (Multichannel, Encryption, Signing, Directory Leasing) im Überblick erläutern

7.2 kann die Verfügbarkeit von Storage sicherstellen

7.2.1 Hochverfügbaren Speicher im LAN bereitstellen

7.2.2 Storage Replica / Storage Migration Service im Windows-Server-Umfeld beschreiben und nach Vorgaben einrichten

7.2.3 Hybride Backup-/DR-Konzepte (on-prem + Cloud-Backup) gegenüber lokal-only-Backups bewerten

7.3 kann ein Distributed File System (DFS) einrichten, testen und verwalten

7.3.1 Replikation nach Vorgaben konfigurieren

7.3.2 DFS-Namespace-/Replikations-Härtung (SMB-Signing, Verschlüsselung, Quotas) umsetzen

8 Sicherheit einer Serverinfrastruktur erhalten

8.1 kann aktuelle Risiken und Sicherheitsprobleme im IT-Umfeld eines KMU erläutern

8.1.1 Angriffsvektoren gegen Server-Infrastrukturen (Phishing/MFA-Fatigue, Password-Spray, Ransomware, Lateral Movement, Missbrauch von NTLM/Kerberos, Angriffe auf exponierte RDP-/VPN-Dienste) erläutern

8.1.2 Relevante Begriffe wie EDR/Defender for Endpoint, Credential Guard, LAPS, JEA, Admin-Tiering, PAW erläutern

8.1.3 Zero-Trust-/Least-Privilege-Konzept auf ein KMU herunterbrechen

8.2 kann Sicherheitseinstellungen gemäss Vorgaben vornehmen und Sicherheitsmassnahmen ausführen

8.2.1 nach Vorgaben Applikationen und Dienste (Web/HTTPS, DNS, File-/Print, DHCP, RDP-/VPN-Publikationen, SMB over QUIC) härten

8.2.2 Sicherheitsvorlagen importieren, anpassen und verteilen

8.2.3 Mit Sicherheitsvorlagen Sicherheitseinstellungen des Betriebssystems überprüfen

8.2.4 NTLM-Härtung / Abschaltung unsicherer Protokolle (SMB1, LM) durchführen

8.3 kann kryptografische Verfahren im Serverumfeld einsetzen

8.3.1 Verschiedenen grundlegende Kryptografische Verfahren und ihre grundlegende Funktionsweise mithilfe von Beispielen korrekt und nachvollziehbar erläutern

8.3.2 gemäss Vorgaben IPsec-/IKEv2-/Always-On-VPN-Richtlinien erstellen und anwenden

8.3.3 IPsec mittels Global Policies konfigurieren

8.3.4 Netzwerkkarte mit IPsec konfigurieren

8.3.5 Server-Betriebssystem als VPN-Endpunkt oder in Site-to-Site-/Remote-Access-Szenarien betreiben

8.3.6 Zertifikatsdienste oder ACME-/Let's-Encrypt-Gateway für Serverdienste konfigurieren

9 Support und Dokumentation in komplexen Netzwerkumgebungen

9.1 kann in einer Serverumgebung First- und Second-Level-Support erbringen

9.1.1 Als First- und Second-Level-Supporter Aufträge entgegennehmen, effizient und strukturiert einer Lösung zuführen und gefundene Lösung nachvollziehbar dokumentieren

9.2 kann Installationen und Konfigurationen dokumentieren

9.2.1 Wichtigkeit und Sinn einer aktuellen Dokumentation erläutern

9.2.2 Nach Installation oder Umkonfiguration einen Netzwerkplan, das Hardware-Inventar und die Systemdokumentation nachführen

9.2.3 Script-/IaC-Repository als aktuelle technische Dokumentation ergänzen

9.2.4 Betriebshandbuch-Eintrag für hybride Szenarien (AD, Entra ID, Exchange Online, Remotezugriffe) erstellen und nachführen

SP1 Server Administration

EMPFOHLENE UNTERRICHTSZEIT 60 LEKTIONEN

- Diese Empfehlung ist als Richtwert zu verstehen.
- Sie beinhaltet keine Qualitätsaussage.
- Zusätzlich ist mit Aufwand für Hausaufgaben zu rechnen (Vertiefen, Lösen von Übungsaufgaben).
- In den angegebenen Richtwerten ist die Prüfungsvorbereitung enthalten.

ÄNDERUNGSNACHWEIS

V2	01.02.2026	überarbeitete Modulidentifikation ohne Taxonomien, Technologien aktualisiert