Exam 70-413: Designing and Implementing a Server Infrastructure – Skills Measured

Audience Profile

This exam is part one of a series of two exams that test the skills and knowledge necessary to design, implement, and maintain a Windows Server 2012 infrastructure in an enterprise scaled, highly virtualized environment. Passing this exam validates a candidate's ability to plan, configure, and implement the Windows Server 2012 services, such as server deployment, server virtualization, and network access and infrastructure. Passing this exam along with the other exam confirms that a candidate has the skills and knowledge necessary for designing, deploying, and maintaining infrastructure services in a Windows Server 2012 environment.

Skills Measured

NOTE: The bullets that appear below each of the skills measured are intended to illustrate how we are assessing that skill. This list is not definitive or exhaustive.

NOTE: In most cases, exams do NOT cover preview features, and some features will only be added to an exam when they are GA (General Availability).

Plan and deploy a server infrastructure (20–25%)

Design and plan an automated server installation strategy

- design considerations including images and bare metal/virtual deployment; design a server implementation using Windows Assessment and Deployment Kit (ADK); design a virtual server deployment
- plan for deploying servers to Microsoft Azure infrastructure as a service (IaaS); plan for deploying servers to public and private cloud by using AppController and Windows PowerShell; plan for multicast deployment; plan for Windows Deployment Services (WDS)

Implement a server deployment infrastructure

- configure multi-site topology and transport servers; implement a multi-server topology, including stand-alone and Active Directory–integrated Windows Deployment Services (WDS) servers; deploy servers to Microsoft Azure IaaS; deploy servers to public and private cloud by using AppController and Windows PowerShell

Plan and implement server upgrade and migration

- plan for role migration; migrate server roles; migrate servers across domains and forests; design a server consolidation strategy; plan for capacity and resource optimization

Plan and deploy Virtual Machine Manager services

- design Virtual Machine Manager service templates; plan and deploy profiles, operating system profiles, hardware and capability profiles, application profiles, and SQL profiles; plan and manage services including scaling out, updating and servicing services; configure Virtual Machine Manager libraries; plan and deploy services to non-trusted domains and workgroups

Plan and implement file and storage services

- planning considerations include iSCSI SANs, Fibre Channel SANs, Virtual Fibre Channel, storage spaces, storage pools including tiered storage and data de-duplication; configure the Internet Storage Name server (iSNS); configure Services for Network File System (NFS); plan and implement SMB 3.0 based storage; plan for Windows Offloaded Data Transfer (ODX)

Design and implement network infrastructure services (20–25%)

Design and maintain a Dynamic Host Configuration Protocol (DHCP) solution

- design considerations including a highly available DHCP solution including split scope, DHCP failover, and DHCP failover clustering, DHCP interoperability, and DHCPv6; implement DHCP filtering; implement and configure a DHCP management pack; maintain a DHCP database

Design a name resolution solution strategy

- design considerations including Active Directory integrated zones, DNSSEC, DNS Socket Pool, cache locking, disjoint namespaces, DNS interoperability, migration to application partitions, IPv6, Single-Label DNS Name Resolution, zone hierarchy, and zone delegation

Design and manage an IP address management solution

- design considerations including IP address management technologies including IPAM, Group Policy based, manual provisioning, and distributed, centralized, hybrid placement, and database storage; configure role-based access control; configure IPAM auditing; migrate IPs; manage and monitor multiple DHCP and DNS servers; configure data collection for IPAM; integrate IPAM with Virtual Machine Manager (VMM)

Design and implement network access services (15–20%)

Design a VPN solution

- design considerations including certificate deployment, firewall configuration, client/site to site, bandwidth, protocol implications, connectivity to Microsoft Azure IaaS and VPN deployment configurations using Connection Manager Administration Kit (CMAK)

Design a DirectAccess solution

- design considerations including deployment topology, migration from Forefront UAG, One Time Password (OTP), and use of certificates issued by enterprise Certificate Authority (CA)

Design a Web Application Proxy solution

- design considerations including planning for applications, authentication and authorization, Workplace Join, devices, multifactor authentication, multifactor access control, single sign-on (SSO), certificates, planning access for internal and external clients

Implement a scalable remote access solution

- configure site-to-site VPN; configure packet filters; implement packet tracing; implement multi-site Remote Access; configure Remote Access clustered with Network Load Balancing (NLB); implement an advanced DirectAccess solution, configure multiple RADIUS server groups and infrastructure, configure Web Application Proxy for clustering

Design and implement network protection solution

- design considerations including Network Access Protection (NAP) enforcement methods for DHCP, IPSec, VPN, and 802.1x, capacity, placement of servers, firewall, Network Policy Server (NPS), and remediation network, configure NAP enforcement for IPsec and 802.1x, monitor for compliance

Design and implement an Active Directory infrastructure (logical) (20–25%)

Design a forest and domain infrastructure

- design considerations including multi-forest architecture, trusts, functional levels, domain upgrade, domain migration, forest restructure, Microsoft Azure Active Directory and DirSync

Implement a forest and domain infrastructure

- configure domain rename; configure Kerberos realm trusts; implement a domain upgrade; implement a domain migration; implement a forest restructure; deploy and manage a test forest including synchronization with production forests

Design a Group Policy strategy

- design considerations including inheritance blocking, enforced policies, loopback processing, security, and WMI filtering, site-linked Group Policy Objects (GPOs), slow-link processing, group strategies, organizational unit (OU) hierarchy, and Advanced Group Policy Management (AGPM), and Group Policy caching

Design an Active Directory permission model

- design considerations including Active Directory object security and Active Directory quotas; customize tasks to delegate in Delegate of Control Wizard; deploy administrative tools on the client devices; delegate permissions on administrative users (AdminSDHolder); plan for Kerberos delegation

Design and implement an Active Directory infrastructure (physical) (20–25%)

Design an Active Directory sites topology

- design considerations including proximity of domain controllers, replication optimization, and site link; monitor and resolve Active Directory replication conflicts

Design a domain controller strategy

- design considerations including global catalog, operations master roles, Read-Only Domain Controllers (RODCs), partial attribute set, and domain controller cloning, and domain controller placement

Design and implement a branch office infrastructure

- design considerations including RODC, Universal Group Membership Caching (UGMC), global catalog, DNS, DHCP, and BranchCache; implement confidential attributes; delegate administration; modify filtered attributes set; configure password replication policy; configure hash publication