Exam 70-412: Configuring Advanced Windows Server 2012 Services

Exam Design

Target Audience

This exam is part three of a series of three exams that test the skills and knowledge necessary to administer a Windows Server 2012 infrastructure in an enterprise environment. Passing this exam validates a candidate's ability to perform the advanced configuring tasks required to deploy, manage, and maintain a Windows Server 2012 infrastructure, such as fault tolerance, certificate services, and identity federation. Passing this exam along with the other two exams confirms that a candidate has the skills and knowledge necessary for implementing, managing, maintaining, and provisioning services and infrastructure in a Windows Server 2012 environment.

Objective Domain

Note: This document shows tracked changes that are effective as of April 19, 2018.

Configure and Manage High Availability

Configure Network Load Balancing (NLB)
Install NLB nodes; configure NLB prerequisites; configure affinity; configure port rules; configure cluster operation mode; upgrade an NLB cluster

Configure failover clustering
Configure Quorum; configure cluster networking; restore single node or cluster configuration; configure cluster storage; implement Cluster Aware Updating; upgrade a cluster; configure and optimize clustered shared volumes; configure clusters without network names; configure storage spaces

Manage failover clustering roles
Configure role-specific settings including continuously available shares; configure VM monitoring; configure failover and preference settings; configure guest clustering

Manage Virtual Machine (VM) movement
Perform Live Migration; perform quick migration; perform storage migration; import, export, and copy VMs; configure Virtual Machine network health protection; configure drain on shutdown

Configure File and Storage Solutions

Configure advanced file services
Configure NFS data store; configure BranchCache; configure File Classification Infrastructure (FCI) using File Server Resource Manager (FSRM); configure file access auditing

Implement Dynamic Access Control (DAC)
Configure user and device claim types; implement policy changes and staging; perform access-denied remediation; configure file classification; create and configure Central Access rules and policies; create and configure resource properties and lists

Configure and optimize storage
Configure iSCSI Target and Initiator; configure Internet Storage Name server (iSNS); implement thin provisioning and trim; manage server free space using Features on Demand; configure tiered storage

Implement Business Continuity and Disaster Recovery

Configure and manage backups
Configure Windows Server backups; configure Windows Azure backups; configure role-specific backups; manage VSS settings using VSSAdmin

Recover servers
Restore from backups; perform a Bare Metal Restore (BMR); recover servers using Windows Recovery Environment (Win RE) and safe mode; configure the Boot Configuration Data (BCD) store

Configure site-level fault tolerance
Configure Hyper-V Replica including Hyper-V Replica Broker and VMs; configure multi-site clustering including network settings, Quorum, and failover settings; configure Hyper-V Replica extended replication; configure Global Update Manager; recover a multi-site failover cluster

Configure Network Services

Implement an advanced Dynamic Host Configuration Protocol (DHCP) solution
Create and configure superscopes and multicast scopes; implement DHCPv6; configure high availability for DHCP including DHCP failover and split scopes; configure DHCP Name Protection; configure DNS registration

Implement an advanced DNS solution

Configure security for DNS including DNSSEC, DNS Socket Pool, and cache locking; configure DNS logging; configure delegated administration; configure recursion; configure netmask ordering; configure a GlobalNames zone; analyze zone level statistics

Deploy and manage IPAM
Provision IPAM manually or by using Group Policy; configure server discovery; create and manage IP blocks and ranges; monitor utilization of IP address space; migrate to IPAM; delegate IPAM administration; manage IPAM collections; configure IPAM database storage

Configure the Active Directory Infrastructure

Configure a forest or a domain
Implement multi-domain and multi-forest Active Directory environments including interoperability with previous versions of Active Directory; upgrade existing domains and forests including environment preparation and functional levels; configure multiple user principal name (UPN) suffixes

Configure trusts
Configure external, forest, shortcut, and realm trusts; configure trust authentication; configure SID filtering; configure name suffix routing

Configure sites
Configure sites and subnets; create and configure site links; manage site coverage; manage registration of SRV records; move domain controllers between sites

Manage Active Directory and SYSVOL replication
Configure replication to Read-Only Domain Controllers (RODCs); configure Password Replication Policy (PRP) for RODCs; monitor and manage replication; upgrade SYSVOL replication to Distributed File System Replication (DFSR)

Configure Access and Information Protection Solutions

Implement Active Directory Federation Services (AD FS)
Install AD FS; implement claims-based authentication including Relying Party Trusts; configure authentication policies; ~~configure Workplace Join~~configure multi-factor authentication

Install and configure Active Directory Certificate Services (AD CS)
Install an Enterprise Certificate Authority (CA); configure 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 to computers and users using Group Policies; configure and manage key archival and recovery

Install and configure Active Directory Rights Management Services (AD RMS)
Install a licensing or certificate AD RMS server; manage AD RMS Service Connection Point (SCP); manage RMS templates; configure Exclusion Policies, back up and restore AD RMS