



Lesson Plans

Windows Server 2008 Enterprise Administrator

(Exam 70-647)

Version 2.1

Table of Contents

Table of Contents	1
Course Overview	2
Section 0.1: Introduction.....	3
Section 1.1: IP Addressing.....	4
Section 1.2: Name Resolution.....	6
Section 1.3: Legacy Name Resolution.....	8
Section 1.4: NPAS	9
Section 1.5: Remote Access.....	11
Section 1.6: NAP	13
Section 1.7: Terminal Services	15
Section 1.8: Application Delivery.....	17
Section 2.1: Active Directory Design	19
Section 2.2: Functional Levels.....	20
Section 2.3: Trusts	21
Section 2.4: Operation Masters.....	23
Section 2.5: Sites.....	25
Section 2.6: Groups.....	27
Section 2.7: Group Policy	29
Section 2.8: Authentication.....	31
Section 3.1: Upgrade and Migration.....	32
Section 3.2: Branch Office Design	34
Section 3.3: PKI Design.....	36
Section 3.4: Interoperability.....	38
Section 4.1: High Availability	40
Section 4.2: AD DS Recovery	41
Section 4.3: Update Infrastructure	42
Section 4.4: Auditing	43
Section 4.5: Virtualization	45
Section 4.6: Data Security and Access	47
Section 4.7: Collaboration	49
Practice Exams.....	50

Course Overview

This course prepares students for Exam 70-647: MCITP Windows Server 2008 Enterprise Administrator. It focuses on designing strategies for managing and protecting the IT environment and architecture.

Module 0 – Introduction

This module introduces the instructor, the course, and the MCITP: Windows Server Enterprise Administrator Exam: 70-647.

Module 1 – Network and Application Services

This module discusses network and application services that can be deployed. Students will become familiar with configuring IPv4 and IPv6 configuration settings, resolving name resolution of host names, replacing a legacy name resolution, and using Network Policy and Access Services (NPAS). They will also learn about remote access options, the role of Network Access Protection (NAP), terminal services technologies, and methods for application deployment.

Module 2 – Core Identity and Access Management

This module examines Active Directory design, functional levels, trusts, operation master roles, site design, permission assignments using groups and group policies, and Active Directory authentication.

Module 3 – Support Identity and Access Management

In this module students will learn about upgrade and migration, branch office design, the elements of PKI design, and interoperability issues.

Module 4 – Business Continuity and Data Availability

This module teaches the students topics that support business continuity and data availability; tools for high availability, Active Directory Domain Services recovery, tools for keeping a Microsoft system up to date, auditing tools and guidelines, strategies for virtualization, solutions for data security and access, and collaboration tools.

Practice Exams

In Practice Exams students will have the opportunity to test themselves and verify that they understand the concepts and are ready to take the certification exam.

Section 0.1: Introduction

Summary

This section introduces the student to the instructor, the course, and the MCITP: Windows Server Enterprise Administrator Exam: 70-647.

The certificate requirements for MCITP: Enterprise Administration include:

- 70-620 – TS: Configuring Microsoft Windows Vista Client
- 70-640 – MCTS: Windows Server 2008 Active Directory
- 70-642 – MCTS: Windows Server 2008 Network Infrastructure, Configuring
- 70-643 – MCTS: Windows Server 2008 Applications Infrastructure, Configuring
- 70-647 – MCITP: Windows Server 2008, Enterprise Administrator

Time

About 3 minutes

Section 1.1: IP Addressing

Summary

In this section the students will learn the basics of designing and deploying IP addressing. Students will become familiar with methods to configure IPv4 configuration settings on a host system:

- Static (manual) assignment
- Dynamic Host Configuration Protocol (DHCP)
- Automatic Private IP Addressing (APIPA)
- Alternate IP configuration

Methods to configure IPv6 configuration settings include:

- Static full assignment
- Static partial assignment
- Stateless autoconfiguration
- DHCPv6

Strategies to provide DHCP for multiple subnets are:

- DHCP server on each subnet
- Multihomed DHCP server
- BOOTP forwarding
- DHCP relay agent

Strategies to provide fault tolerance for a DHCP server include:

- Split scope
- Failover clustering

Strategies for deploying IPv6:

- Dual stack
- Tunneling
 - Manually configured tunnel
 - Intra-site Automatic Tunnel Addressing Protocol (ISATAP)
 - 6-to-4 tunneling
 - Teredo tunneling
- PortProxy

Students will learn how to:

- Configure static and automatic IPv4 addressing.

- Specify an alternate IPv4 configuration.
- Configure split scopes on multiple DHCP servers.
- Configure a DHCP relay agent.

Windows Server 2008 Enterprise Administrator Objectives

- 101. Plan for name resolution and IP addressing.

Lecture Focus Questions:

- When does a Windows computer use APIPA? What are its limitations?
- What is the purpose of an alternate IPv4 configuration?
- How can you provide DHCP services to clients on subnets that do not have a DHCP server?
- What is the difference between placing a DHCP server on each subnet and using a multihomed server?
- How many DHCP relay agents should be placed on a single subnet?
- What limitations does ISATAP have for IPv6 implementation?
- Which IPv6 tunneling methods work through NAT?
- When should you implement Teredo?

Time

About 50 minutes

Lab/Activity

- Configure Automatic and Alternate Addressing
- Add a DHCP Server for Fault Tolerance
- Configure a DHCP Relay Agent

Number of Exam Questions

6 questions

Section 1.2: Name Resolution

Summary

This section discusses using DNS to resolve host names. DNS configuration options include:

- Primary zone
- Secondary zone
- Zone delegation
- Active Directory-integrated zone
- Stub zone
- Conditional forwarding
- Forwarders
- Root hints
- Root zone
- Primary read-only zone
- Background zone loading
- Reverse lookup zone
- Dynamic DNS
- Caching-only server
- Link-Local Multicast Name Resolution (LLMNR)
- HOSTS file

Methods for configuring DNS namespace include:

- Same internal and external domain name
- Different internal and external domain names
- External domain name with an internal subdomain

Students will learn how to:

- Create and configure DNS zones.
- Implement DNS solutions to customize name resolution for a branch office.

Windows Server 2008 Enterprise Administrator Objectives

- 101. Plan for name resolution and IP addressing.
- 302. Design the branch office deployment.

Lecture Focus Questions:

- What are the advantages of using Active Directory-integrated zones over primary or secondary zones?

- What is the replication scope and how does it control the availability of DNS zone data?
- When should you use conditional forwarding instead of a standard forwarder?
- What is the difference between a stub zone and a forwarder? Which one is dynamic?
- When using internal and external DNS, what are the three possible scenarios for the DNS namespace? What are the advantages and disadvantages of each of the three methods?
- What are the goals of any split namespace design?

Time

About 70 minutes

Lab/Activity

- Configure Name Resolution
- Implement a Namespace Strategy

Number of Exam Questions

10 questions

Section 1.3: Legacy Name Resolution

Summary

This section explores strategies to integrate or replace a legacy name resolution system:

- WINS-integrated zone
- GlobalNames zone
- Link-Local Multicast Name Resolution (LLMNR)
- HOSTS file

Students will learn how to:

- Create and configure WINS-integrated zones.
- Configure the GlobalNames zone to provide single-label name resolution.

Windows Server 2008 Enterprise Administrator Objectives

- 101. Plan for name resolution and IP addressing.

Lecture Focus Questions:

- Why might you choose to not replicate WINS data in a DNS zone?
- When can you use the GlobalNames zone to replace a WINS server?
- When should you *not* use a GlobalNames zone to replace a WINS server?
- What type of records do you create in the GlobalNames zone?
- Which strategies can you use to provide single-label name resolution for IPv6 hosts?

Time

About 20 minutes

Lab/Activity

- Enable WINS Replication

Number of Exam Questions

2 questions

Section 1.4: NPAS

Summary

This section discusses using Network Policy and Access Services (NPAS) to configure network access for LAN and remote clients. NPAS includes the following role services:

- Network Policy Server (NPS)
- Remote Access Service
- Routing
- Health Registration Authority (HRA)
- Host Credential Authorization Protocol (HCAP)

Concepts about consolidating network policies using a Remote Authentication Dial-In User Service (RADIUS) server are presented:

- RADIUS client
- RADIUS server
- RADIUS proxy
- Configuring a RADIUS solution

Students will learn how to:

- Add Network Policy and Access Services role services based on server requirements.

Windows Server 2008 Enterprise Administrator Objectives

- 102. Design for network access.

Lecture Focus Questions:

- Which role service must you add to allow remote clients to access the private network, and not just the resources on the remote access server?
- Which role service do you add to configure network policies on a server?
- Which specific implementation requires the Health Registration Authority role service?
- When using a RADIUS solution, where are network access policies configured?
- What is the difference between a RADIUS client and a remote access client?

Time

About 20 minutes

Lab/Activity

- Add Role Services for a RADIUS Server

Number of Exam Questions

3 questions

Section 1.5: Remote Access

Summary

In this section students will learn options for remote access; VPNs and SSL. VPN protocols supported by Windows Server 2008 and Vista include:

- Point-to-Point Tunneling Protocol (PPTP)
- Layer Two Tunneling Protocol (L2TP)
- Secure Socket Tunneling Protocol (SSTP)

Use the Network Policy Server console to configure the following types of network policies:

- Conditions
- Constraints
- Permissions
- Settings

Concepts about designing firewalls for the following situations are presented:

- Connecting a private network to the Internet
- Creating a demilitarized zone (DMZ)
- Allowing Internet host to access the private network through the screened subnet
- Allowing servers inside the screened subnet to communicate with other servers

Students will learn how to:

- Configure a server for remote access, including configuring network access policies.
- Configure VPN ports on a remote access server.
- Configure RADIUS servers and clients.

Secure Sockets Layer (SSL) provides encryption of network traffic between two devices and is used by the following services:

- Internet Information Services (IIS)
- TS Gateway
- Internet Security and Acceleration server (ISA)
- RPC over HTTP/S

Windows Server 2008 Enterprise Administrator Objectives

- 102. Design for network access.

Lecture Focus Questions:

- How do network policy *constraints* differ from *conditions*? When would you use the same setting in a constraint instead of a condition?
- Why does the policy application order affect whether or not clients can connect to a remote access server?
- What advantages does using SSTP have over using either PPTP or L2TP for a VPN connection?
- What ports must you open in a firewall to allow SSTP?
- What type of servers would you place inside a demilitarized zone (DMZ)? Which type of servers are typically *not* located in the DMZ?
- How can you prevent a client computer from showing a message that the issuing CA is not trusted when using a self-signed certificate or a certificate issued from your private CA?

Time

About 50 minutes

Lab/Activity

- Configure a Remote Access Server

Number of Exam Questions

4 questions

Section 1.6: NAP

Summary

This section examines using Network Access Protection (NAP) to regulate network access or communication based on a computer's compliance with health requirement policies. NAP uses the following components:

- NAP client
- NAP server
- Enforcement server (ES)
- Remediation server

There are five different enforcement point types:

- DHCP
- TS Gateway
- Remote Access
- EAP (802.1x)
- IPsec

The following logical networks are defined when designing a NAP solution:

- Boundary (untrusted)
- Restricted (boundary isolation)
- Secure (isolation)

Two types of isolation configuration are described:

- Domain isolation
- Server isolation

Students will learn how to:

- Add the necessary role services to implement Network Access Protection (NAP).
- Enable NAP on an enforcement point.
- Create domain and server isolation rules.
- Configure system health validator and health policy settings.

Windows Server 2008 Enterprise Administrator Objectives

- 102. Design for network access.

Lecture Focus Questions:

- How do remediation servers and auto-remediation help clients become compliant?
- What server role service do you add to configure a server as an enforcement point for NAP?
- How do you define the quarantine network when using 802.1x enforcement?
- Which enforcement method uses a Health Registration Authority (HRA)?
- What type of communication occurs in the boundary network when using IPsec enforcement?

Time

About 40 minutes

Lab/Activity

- Add Role Services for NAP

Number of Exam Questions

8 questions

Section 1.7: Terminal Services

Summary

This section provides information about the role services included in Terminal Services.

- Terminal Server
- TS Licensing
- TS Session Broker
- TS Gateway
- TS Web Access

Use the Windows System Resource Manager to allocate resources on the terminal server.

Students will learn how to:

- Add Terminal Server role services to meet server requirements.
- Configure terminal servers as part of a TS Session Broker farm.
- Activate the licensing server, add licenses, and configure the licensing mode on a terminal server.
- Control user and session resource use with WSRM.

Windows Server 2008 Enterprise Administrator Objectives

- 104. Plan for Terminal Services.

Lecture Focus Questions:

- Which role service enables access through the Internet past most firewalls?
- What ports are used by TS Web Access?
- What operating system(s) can you use to issue licenses to terminal servers running Windows Server 2008?
- What is the difference between a per-user license and a per-device license? When would a per-device license be a better choice?
- Which licensing discovery mode would you use if you needed to issue licenses to both domain and non-domain members?
- If you are using the domain discovery mode, where must the licensing server be installed for terminal servers to be able to automatically locate the licensing server?
- What is the difference between the equal per user profile and the equal per session profile? How can a user overcome the restrictions enforced by the equal per session profile?

Time

About 40 minutes

Lab/Activity

- Add Terminal Services Role Services
- Configure a TS Licensing Server

Number of Exam Questions

15 questions

Section 1.8: Application Delivery

Summary

This section discusses methods that can be used to simplify and centralize application deployment:

- Group Policy
- System Center Configuration Manager
- Application Server
- Terminal Services
- Microsoft Application Virtualization (SoftGrid)

Students will learn how to:

- Deploy software packages using Group Policy.
- Make applications available using TS RemoteApp and TS Web Access.
- Create .rdp and .msi files for TS RemoteApp applications.

Windows Server 2008 Enterprise Administrator Objectives

- 103. Plan for application delivery.

Lecture Focus Questions:

- Which application deployment methods do *not* install applications on the client computer?
- What is the difference between publishing and assigning software using Group Policy?
- How is using System Center Configuration Manager similar to using Group Policy for software distribution?
- How do you add TS RemoteApp support to a terminal server?
- What are the three ways you can use to make applications visible to terminal server clients? Which method requires no configuration on the client computer?
- How can you run applications using SoftGrid without installing client software on each computer?
- Which application delivery solutions allow for running multiple versions of the software at the same time on a client computer?
- What are the different strategies you can use to run applications while preventing conflicts on the client computer?

Time

About 40 minutes

Lab/Activity

- Deploy Software with Group Policy
- Configure Remote Applications

Number of Exam Questions

8 questions

Section 2.1: Active Directory Design

Summary

This section presents guidelines for designing the components of an Active Directory logical structure:

- Forest
- Tree
- Domain
- Organizational Unit (OU)

Students will learn how to:

- Create OUs based on departments or for delegated administration.
- Delegate common administrative tasks for specific object types.

Windows Server 2008 Enterprise Administrator Objectives

- 201. Design Active Directory forests and domains.
- 203. Design the Active Directory administrative model.

Lecture Focus Questions:

- Why should you assume that most Active Directory implementations will have a single domain?
- What are business and technical reasons for having multiple forests and domains?
- Why shouldn't you put much thought into planning trees in Active Directory?
- Why might you design a nearly empty forest root domain?
- What should you use instead of domains in most cases to delegate authority?
- How does the principle of least privilege apply when delegating administrative permissions?

Time

About 35 minutes

Lab/Activity

- Delegate Administrative Control

Number of Exam Questions

2 questions

Section 2.2: Functional Levels

Summary

This section lists the features that are available at both the domain functional level and the forest functional level of the following:

- 2000 Native
- 2003
- 2008

Students will learn how to:

- Identify the current domain and forest functional levels.
- Raise the functional levels of domains and forests.

Windows Server 2008 Enterprise Administrator Objectives

- 201. Design Active Directory forests and domains.

Lecture Focus Questions:

- Which functional level is required to enable selective authentication?
- What forest functional level(s) let you rename domains?
- What features do you get by enabling a Windows Server 2008 functional level?
- When would you raise the domain functional level?
- What are the domain controller operating system requirements for raising a domain functional level to Windows Server 2008?

Time

About 30 minutes

Lab/Activity

- Raise Functional Levels
- Raise the Domain and/or Forest Levels

Number of Exam Questions

3 questions

Section 2.3: Trusts

Summary

In this section students will explore using trusts to allow mutual authentication, communication and access to resources between the domains. Properties of trusts include:

- Direction of trust
 - One-way trust
 - Two-way trust
- Direction of resource access
- Transitivity
 - Transitive trust
 - Non-transitive trust

Types of trusts that can be created manually include:

- Shortcut
- External
- Realm
- Forest
- Active Directory Federation Services (AD FS)

Authentication security settings that can be applied to trusts include:

- Selective authentication
- Domain-wide authentication
- Forest-wide authentication

Students will learn how to:

- Create external, shortcut, and forest root trusts.

Windows Server 2008 Enterprise Administrator Objectives

- 201. Design Active Directory forests and domains.
- 301. Plan for domain or forest migration, upgrade, and restructuring.
- 305. Plan for interoperability.

Lecture Focus Questions:

- What is the difference between a one-way trust and a two-way trust?
- Domain A trusts domain B. Users in which domain will be able to access resources in which domain? What is the relationship between the direction of trust and the direction of access?

- What is a *transitive* trust? Which trust types are transitive by default?
- When are trusts created automatically? What are the properties of those trusts?
- When should you use a shortcut trust?
- What are the domain and forest functional level requirements for creating a forest root trust? What type of trust would you use if you couldn't create a forest root trust?

Time

About 45 minutes

Lab/Activity

- Create a Shortcut Trust
- Create a Forest Root Trust
- Design Trusts

Number of Exam Questions

10 questions

Section 2.4: Operation Masters

Summary

This section discusses operation master roles; which are specialized domain controller tasks assigned to a domain controller in the domain or forest. At the forest level the following roles can be assigned:

- Schema master
- Domain naming master

At the domain level the following roles can be assigned:

- Relative ID (RID) master
- Primary Domain Controller (PDC) emulator
- Infrastructure master

Students will learn how to:

- Transfer operation master roles among domain controllers.
- Seize an operation master role in the case of a failed role operations master.

Windows Server 2008 Enterprise Administrator Objectives

- 202. Design the Active Directory physical topology.

Lecture Focus Questions:

- What is the purpose of an operation master role server?
- What is the function of a PDC emulator? What does the infrastructure master do?
- Which operations master roles are located at the forest level? How many of these roles are there in a forest?
- How many domain operations masters are in a forest?
- You are installing a new domain controller in a new domain in an existing forest. How many operation master roles will that server hold?
- What might happen if the RID master becomes unavailable?
- Which role(s) should be placed on a global catalog server? Which roles should not?
- What is the difference between *transferring* a role and *seizing* a role?

Time

About 35 minutes

Lab/Activity

- Transfer RID and PDC Masters
- Transfer the Infrastructure Master
- Troubleshoot Operations Masters

Number of Exam Questions

3 questions

Section 2.5: Sites

Summary

This section examines design considerations when implementing sites. Sites and services distinguishes between two types of replication:

- Intrasite replication
- Intersite replication

When implementing sites consider:

- Replication protocol
 - Directory Services Remote Procedure Call (DS-RPC)
 - Inter-Site Messaging-Simple Mail Transfer Protocol (ISM-SMTP)
- Preferred bridgehead server
- Replication frequency
- Link costs
- Site link bridging
- Global catalog/Universal Group Membership Caching

Students will learn how to:

- Create sites and subnets. Move servers into sites.
- Create site links and configure site link properties to customize replication.
- Customize intersite and intrasite replication frequencies and schedules.
- Designate preferred bridgehead servers.

Windows Server 2008 Enterprise Administrator Objectives

- 202. Design the Active Directory physical topology.

Lecture Focus Questions:

- What is the purpose of a site link?
- What is the purpose of a site link bridge?
- What are the differences between intrasite and intersite replication?
- What does a site link cost do?
- When would you use the SMTP protocol for replication?
- What is the function of the bridgehead server?
- How is a preferred bridgehead server determined?

Time

About 55 minutes

Lab/Activity

- Manage Sites and Subnets
- Configure Intersite Replication

Number of Exam Questions

14 questions

Section 2.6: Groups

Summary

In this section students will learn about using groups to simplify permission assignments. The membership and use of the following security group scopes are presented:

- Global groups
- Domain local groups
- Universal groups

Additional groups discussed include:

- Security groups
- Distribution groups

Strategies that are recommended for managing users, groups, and permissions include:

- UGLR
- UGULR
- ULR

Other concepts discussed include:

- Best practices for implementing universal groups
- Best practices for implementing Restricted Group policies
- Best practices when using groups for granting administrative privileges

Students will learn to:

- Implement a group strategy following Microsoft's recommendations for group membership and nesting.

Windows Server 2008 Enterprise Administrator Objectives

- 203. Design the Active Directory administrative model.

Lecture Focus Questions:

- What are the advantages of using groups when setting permissions?
- What type of objects can be made members of a universal group? A domain local group?
- Based on Microsoft's recommendations, which group scope is added to the ACL for an object and assigned the permissions?
- Based on Microsoft's recommendations, which group scope type would you use to add user accounts as members?

- When is it appropriate to use universal groups? In which scenarios are they unnecessary?

Time

About 35 minutes

Lab/Activity

- Implement a Group Strategy

Number of Exam Questions

11 questions

Section 2.7: Group Policy

Summary

This section examines the application and design of Group Policy used to assign permissions.

- Order in which GPOs are applied
- Effective GPO settings
- GPO settings categories
- Computer policies
- User policies
- Effective account policies for domain users

Methods used to customize how GPO settings are applied include:

- Block inheritance
- Enforced
- Loopback processing
- WMI filtering
- GPO permissions

Methods to use templates when creating new GPOs include:

- Administrative templates
- Starter GPOs
- GPO copy or import

Students will learn how to:

- Link GPOs to appropriate objects to take advantage of inheritance.
- Customize Group Policy application using block inheritance and no override.
- Use GPO permissions to limit the application of GPOs.
- Configure WMI filters and loopback processing.

Windows Server 2008 Enterprise Administrator Objectives

- 204. Design the enterprise-level group policy strategy.

Lecture Focus Questions:

- How does inheritance affect Group Policy settings?
- What are the advantages of the .admx file format?
- What is the Administrative Template central store? What advantages do you gain by enabling the central store?

- What is the difference between using a starter GPO and copying an existing GPO?
- If a setting is configured in a GPO linked to the domain and a GPO linked to an OU, which setting will be in effect?
- If there is more than one group policy linked to a domain, what controls the order of application?
- How is the **Block Inheritance** setting affected by the **No Override** setting?
- How does *loopback processing* affect computer settings?

Time

About 65 minutes

Lab/Activity

- Control GPO Inheritance
- Configure GPO Permissions

Number of Exam Questions

9 questions

Section 2.8: Authentication

Summary

In this section students will learn solutions to customize Active Directory authentication.

- Account policies
- Smart card
- Fine-grained password policies
- Authorization Manager

Students will learn how to:

- Configure and manage Account Policy settings.
- Use ADSI Edit to configure granular password policy settings.

Windows Server 2008 Enterprise Administrator Objectives

- 204. Design the enterprise-level group policy strategy.

Lecture Focus Questions:

- What happens when you configure Account Policies settings in a GPO linked to an OU?
- How can you configure different account policy settings for different users?
- Which object types can you associate with a granular password policy?
- A user has a granular password policy applied directly to the user account, and a different policy applied to a group of which the user is a member. Which policy will be in effect?

Time

About 30 minutes

Lab/Activity

- Configure Account Policies
- Create a Fine-grained Password Policy

Number of Exam Questions

3 questions

Section 3.1: Upgrade and Migration

Summary

This section discusses upgrade and migration facts. Tools used to perform migration tasks include:

- Active Directory Migration Tool (ADMT)
- MoveTree
- Dsmove
- User State Migration Tool (USMT)

Other concepts concerning migration management include:

- Retaining the SID history
- Using the InetOrg object in Active Directory
- Selecting the UPN suffix for the user account
- Migrating objects between forests

Tools used to prepare forest and domain support for Windows Server 2008 include:

- adprep/forestprep
- adprep/domainprep
- adprep/rodcprep

Students will learn how to:

- Prepare an existing forest and domain for installation of a Windows Server 2008 domain controller.

Windows Server 2008 Enterprise Administrator Objectives

- 301. Plan for domain or forest migration, upgrade, and restructuring.

Lecture Focus Questions:

- Which forest and domain functional levels are required before installing a Windows Server 2008 domain controller?
- When do you use the **adprep /domainprep /gpprep** command instead of the **adprep /domainprep** command?
- On which domain controller should you run the **adprep /domainprep** command?
- What is the difference between the Active Directory Migration Tool (ADMT) and the User State Migration Tool (USMT)?
- Which tool works only within a domain to move Active Directory objects?

- When should you worry about preserving the SID history when migrating objects?

Time

About 35 minutes

Number of Exam Questions

8 questions

Section 3.2: Branch Office Design

Summary

This section provides information about designing a branch office, a remote network with limited WAN connectivity. Students will become familiar with the following concepts:

- Performance issues
- Authentication issues
- Minimizing WAN traffic
- The role of a read-only domain controller (RODC)
- Implementing encryption through BitLocker or Encrypting File System (EFS)
- Configuring a password caching policy
- Reducing the services running on a server
- Securing data that crosses the WAN link
- Balancing the speed of DNS name resolution vs. the reduction in WAN traffic

When implementing an RODC the following considerations must be addressed:

- Installation requirements
- Active Directory replication issues
- Password caching issues
- Administrative role separation issues

Students will learn how to:

- Pre-create RODC accounts in Active Directory.
- Configure password caching and replication for an RODC.

Windows Server 2008 Enterprise Administrator Objectives

- 302. Design the branch office deployment.
- 303. Configure the read-only domain controller (RODC).

Lecture Focus Questions:

- How can you minimize WAN traffic when installing a domain controller in a branch office?
- When would you use Universal Group Membership Caching (UGMC) instead of a global catalog server?
- What advantages does using an RODC in a branch office have over using a full domain controller? When would you need a full domain controller instead of using an RODC?
- What is the purpose of administrator role separation?

- How does using an RODC allow for domain logon in the event of a WAN link failure?
- How can you protect data as it travels across the WAN link?
- What advantages does a stub zone have over using conditional forwarders? What advantages does using a forwarder have over a stub zone?
- What are the domain and forest functional level requirements for installing an RODC?
- What command would you run to prepare for installing a read-only domain controller (RODC)?

Time

About 40 minutes

Number of Exam Questions

12 questions

Section 3.3: PKI Design

Summary

In this section students will learn the basics of designing a PKI solution. Concepts covered include:

- Root CA
- Subordinate CA
- Trusting the issuing CA
- Using Active Directory Certificate Services (AD CS) roles
 - Certification Authority
 - Certification Authority Web Enrollment
 - Online Responder
 - Network Device Enrollment Service (NDES)
- Comparing the features of a standalone vs. an enterprise CA.
- Suite B capabilities add support for
 - SHA-2 hashing (SHA-256 (256-bits) and SHA-384)
 - The Advanced Encryption Standard (AES) (AES-GMAC-128, 192, and 256 for data integrity; AES-GCM-128, 192, and 256 for data integrity and encryption)
 - Elliptical Curve Cryptography (ECC) (ECDSA-P246 and P284 signing for certificates used for authentication)

Common designs used for PKI infrastructure when deploying multiple CAs include:

- Offline standalone root CA with online enterprise subordinate CAs
- Internal PKI for internal certificates and a third-party CA for external certificates.

Other concepts covered include the role of:

- Autoenrollment
- Key archival
- Policy module
- CRL distribution Point (CDP)
- Authority Information Access (AIA)
- CA manager
- Enrollment agent
- Enterprise PKI snap-in

Students will learn how to:

- Add Certificate Services role services to meet the network requirements.

Windows Server 2008 Enterprise Administrator Objectives

- 302. Design the branch office deployment.
- 304. Design and implement public key infrastructure.

Lecture Focus Questions:

- What are the advantages of using an enterprise CA over a standalone CA?
- How does Web enrollment differ from autoenrollment?
- Which role service lets you centralize certificate revocation requests? What advantages does this service provide over clients using CRLs?
- What does the registration authority do when using NDES?
- Which servers and clients are capable of using Suite B encryption?
- Which certificate version is capable of using Suite B encryption?
- What is the advantage of taking the root CA offline?
- Why shouldn't you take an enterprise CA offline? How can you use an offline root CA but still use enterprise CAs?

Time

About 50 minutes

Lab/Activity

- Add Role Services for AD CS 1
- Add Role Services for AD CS 2

Number of Exam Questions

13 questions

Section 3.4: Interoperability

Summary

This section covers interoperability issues. The following solutions are involved with managing authentication and resource access between organizations:

- Trusts
- Active Directory Federation Services (AD FS)
- Identity Lifecycle Manager (ILM)

For UNIX interoperability, Microsoft provides the following solutions:

- Realm trust
- Identity management for UNIX
- Subsystem for UNIX-based Applications (SUA)
- Services for Network File System (NFS)
- LPR Port Monitor

Students will learn how to:

- Configure trusts for inter-organizational authentication and authorization.
- Add role services and features to support UNIX interoperability.

Windows Server 2008 Enterprise Administrator Objectives

- 305. Plan for interoperability.

Lecture Focus Questions:

- What are the requirements for using a forest root trust?
- What is the difference between an external trust and a realm trust?
- What is a domain map used in UNIX? How can you configure a Windows Server 2008 domain controller to hold UNIX maps?
- When would you use the Subsystem for UNIX-based Applications feature?
- When would you use the LPR Port Monitor feature? When should it *not* be used?

Time

About 30 minutes

Lab/Activity

- Add UNIX Integration Services 1
- Add UNIX Integration Services 2

Number of Exam Questions

6 questions

Section 4.1: High Availability

Summary

This section discusses using Network Load Balancing (NLB) and Failover Clustering to provide high availability by increasing the performance and fault tolerance for network services.

Windows Server 2008 Enterprise Administrator Objectives

- 401. Plan for business continuity.
- 404. Design for data management and data access.

Lecture Focus Questions:

- How is Failover Clustering different from NLB?
- Which application types are best used with NLB and not failover clustering?
- What happens to traffic not identified by a port rule? How can you control which cluster host responds?
- Which client affinity option should you use when clients connect to a NLB cluster using multiple proxy servers?
- Which quorum mode should be used if you have an even number of cluster hosts? Why?
- Which quorum mode allows the cluster to continue operating even if only one cluster host is still available?

Time

About 25 minutes

Number of Exam Questions

9 questions

Section 4.2: AD DS Recovery

Summary

In this section students will learn about Active Directory Domain Services (AD DS) recovery. Concepts the students will become familiar with include:

- Authoritative restore
- Non-authoritative restore
- Update Sequence Number (ISN)
- Directory Services Restore Mode (DSRM)
- Tombstone
- Tombstone lifetime
- Restartable Active Directory
- Snapshots
- Transfer of operations masters

Students will learn how to:

- Add Windows Server Backup to your server.
- Perform an authoritative restore of Active Directory objects.
- View, transfer, and seize operation master roles.

Windows Server 2008 Enterprise Administrator Objectives

- 401. Plan for business continuity.

Lecture Focus Questions:

- What is the difference between an authoritative and a nonauthoritative restore?
- How does the tombstone lifetime affect Active Directory backups? When would you need to be concerned with changing this setting?
- How can snapshots help you preserve Active Directory data? Why are they not as useful as a backup when you need to restore large numbers of objects?
- Which backup type should you perform if you want to back up the Active Directory database?
- When would you seize rather than transfer an operations master role?

Time

About 15 minutes

Number of Exam Questions

4 questions

Section 4.3: Update Infrastructure

Summary

This section discusses the solutions used to update the infrastructure of a Microsoft network. The tools for keeping a system up to date are:

- Windows Update
- Microsoft Update
- Windows Server Update Service (WSUS)
- Automatic Updates

Students will learn how to:

- Configure a client for automatic updates.
- Configure a replica WSUS server.

Windows Server 2008 Enterprise Administrator Objectives

- 402. Design for software updates and compliance management.

Lecture Focus Questions:

- What is the difference between Windows Update and Microsoft Update?
- How do clients receive updates in the absence of WSUS? What are the disadvantages that this method poses for your network?
- When should you deploy multiple, independent WSUS servers? How is this configuration similar to a single WSUS server?
- How would you deploy WSUS when an Internet connection is not allowed for an isolated network?
- What is the difference between synchronizing updates, downloading updates, and approving updates?

Time

About 20 minutes

Lab/Activity

- Configure a Downstream Server

Number of Exam Questions

4 questions

Section 4.4: Auditing

Summary

This section discusses tools and guidelines used in auditing a system to look for abnormal activities and to ensure that it meets the security policy requirements. Microsoft provides the following tools for security auditing:

- Microsoft Baseline Security Analyzer (MBSA)
- Security Configuration Wizard (SCW)
- Security Configuration and Analysis snap-in
- Microsoft Security Assessment Tool (MSAT)
- Audit Policy
- Snapshots

Enable auditing by configuring audit policies on a local system or through Group Policy. Audit policies that are configurable through Group Policy include:

- Account logon
- Account management
- Directory service access
- Logon
- Object access
- Policy change
- Privilege use
- Process tracking
- System

Students will learn how to:

- Use the Security Configuration Wizard (SCW) to customize server security and create security policies.
- Use the Microsoft Security Baseline Analyzer (MBSA) to scan computer security settings.

Windows Server 2008 Enterprise Administrator Objectives

- 402. Design for software updates and compliance management.

Lecture Focus Questions:

- Which tools can you use to make changes to the system configuration and export your settings to customize multiple servers at once?
- What types of system vulnerabilities can you find with MBSA?

- Which tool helps you assess your organization-wide security and makes recommendations based on industry-accepted standards?
- What is the difference between auditing for success and auditing for failure?
- What additional step must you complete in order to audit NTFS file access?
- How can you configure auditing to track changes to Active Directory objects?
- What are the results of excessive auditing?
- How can snapshots be used for auditing purposes?

Time

About 30 minutes

Number of Exam Questions

5 questions

Section 4.5: Virtualization

Summary

This section explores strategies for installing and configuring virtualization. Microsoft has the following virtualization products:

- Virtual PC
- Virtual Server
- Hyper-V

Design concepts discussed about installing and configuring virtual machines include:

- Hyper-V
 - Supported operating systems
 - Supported CPUs
 - Supports virtual machine snapshots
 - Supported virtual disk types
 - Fixed
 - Dynamically expanding
 - Differencing
 - Pass-through
 - Supports virtual switches and VLAN IDs
- Virtual networking allows you to control the network communication of virtual machines:
 - External network
 - Internal network
 - Private network
 - No network

The following tools can be used to manage virtual machines:

- System Center Operations Manager (SCOM)
- System Center Virtual Machine Manager (SCVMM)
- Hyper-V Manager
- Windows System Resource Manager (WSRM)

Windows Server 2008 Enterprise Administrator Objectives

- 403. Design the operating system virtualization strategy.

Lecture Focus Questions:

- What is the main difference between Hyper-V and Virtual PC or Virtual Server?
- What is disk *pass-through*? What does this allow you to do when configuring virtual machines?
- Which virtual disk type offers the best performance? Which type minimizes disk space use?
- What is the difference between an *internal* virtual network and a *private* virtual network?
- When would you need to use a legacy virtual network adapter?
- What advantages does using System Center VMM have over using Hyper-V Manager?
- What is the difference between migration and conversion of virtual machines?
- Which conversion scenario requires that the source machine be offline during the conversion process? Why?

Time

About 20 minutes

Number of Exam Questions

8 questions

Section 4.6: Data Security and Access

Summary

This section examines solutions for designing security and availability for data access.

- NTFS permissions
- Encrypting File System (EFS)
- BitLocker
- Active Directory Rights Management Services (AD RMS)
- Distributed File System (DFS)
- File Server Resource Manager (FSRM)
- Storage Area Network (SAN)

Concepts covered about implementing a DFS solution include:

- Namespace
 - Standalone
 - Domain-based
- Folders
- Folder target
- Replication
 - File Replication Service (FSR)
 - DFS replication
 - Remote Differential Compression (RDC)
- Storage area network (SAN) technologies
 - iSCSI
 - Fibre Channel

Students will learn how to:

- Add role services as required to support DFS and the appropriate replication method.
- Create a DFS namespace with folders and targets.

Windows Server 2008 Enterprise Administrator Objectives

- 404. Design for data management and data access.

Lecture Focus Questions:

- What are the main differences between EFS and BitLocker?
- Which encryption feature encrypts system files?
- What functions are performed by the Trusted Platform Module (TPM)? What BitLocker features are only available when using a TPM?

- Which data access feature can you use to control file access for files that are copied or shared outside of your organization?
- What is the difference between the namespace root and a folder within DFS?
- If you have multiple namespace servers, which namespace type should you implement?
- Which namespace type and mode would you choose to support access-based enumeration?
- If you have a single namespace server and that server fails, what happens to client access for folders within the DFS structure? Why?
- What are the advantages of using DFS replication over FRS replication?

Time

About 60 minutes

Lab/Activity

- Add Role Services for Replication
- Create a DFS Structure

Number of Exam Questions

14 questions

Section 4.7: Collaboration

Summary

This section provides information about SharePoint which provides collaboration tools and a platform for developing Web-based applications.

- Windows SharePoint Services (WSS) is a free version with limited features.
- Microsoft Office SharePoint Server (MOSS) is a commercial version with advanced features.

Concepts covered about SharePoint include:

- Deploying WSS
 - Stand-alone configuration
 - Advanced configuration
- Site collection
- Document library
- Web part
- E-mail integration
- Combining SharePoint with Active Directory Rights Management Services (AD RMS)

Windows Server 2008 Enterprise Administrator Objectives

- 404. Design for data management and data access.

Lecture Focus Questions:

- What additional features do you get with Microsoft Office SharePoint Server (MOSS) compared to Windows SharePoint Services (WSS)?
- What are the requirements for using multiple WSS servers in a farm?
- When would you use the internal database for WSS?
- What feature would you use in conjunction with SharePoint to increase the security on shared content?

Time

About 10 minutes

Number of Exam Questions

2 questions

Practice Exams

Summary

This section provides information to help prepare students to take the exam and to register for the exam.

Students will also have the opportunity of testing their mastery of the concepts presented in this course to reaffirm that they are ready for the certification exam. For example, all questions that apply to **Objective 100. Network and Application Services** are grouped together and presented in practice exam **100. Network and Application Services, All Questions**. Students will typically take about 60-90 minutes to complete each of the following practice exams.

- 100. Network and Application Services, All Questions (56 questions)
- 200. Core Identity and Access, All Questions (54 questions)
- 300. Support Identity and Access Management, All Questions (38 questions)
- 400. Business Continuity and Data Availability, All Questions (51 questions)

The *Certification Practice Exam* consists of 52 questions that are randomly selected from the above practice exams. Each time the Certification Practice Exam is accessed different questions may be presented. The Certification Practice Exam has a time limit of 90 minutes -- just like the real certification exam. A passing score of 95% should verify that the student has mastered the concepts and is ready to take the real certification exam.