55378A: Identity with Windows Server

Course Details

Course Code: 55378A

Duration: 4 days

Notes:

- This course syllabus should be used to determine whether the course is appropriate for the students, based on their current skills and technical training needs.
- Course content, prices, and availability are subject to change without notice.
- Terms and Conditions apply

Elements of this syllabus are subject to change.

About this course

In this four-day course, Skillable has reimagined this popular Windows Server course using our modern challenge-centric instructional design model. Live hands-on labs are at the forefront of this course allowing learners to learn while doing and include additional reference materials and post class access to Challenge Labs to further promote and enable continuous learning. In this course, learners will validate their skills related to management of identities using the functionalities in Windows Server, such as: install, configure, manage, and maintain Active Directory Domain Services (AD DS) as well as implement Group Policy Objects (GPOs).

It should be noted all hands-on labs will be performed using Windows Server 2022, however all concepts apply to Windows Server 2016 and Windows Server 2019.

Audience Profile

This course is intended for an IT professional who to support Administrators who manage identities using the functionalities in Windows Server and install, configure, manage, and maintain Active Directory Domain Services (AD DS) as well as implement Group Policy Objects (GPOs).

At Course Completion

- Migration of Server and Workloads.
- Disk Management.
- iSCSI and Multipath I/O Configuration.
- Storage Creation and Management.
- Hyper-V Virtual Machine and Switch Configuration.
- Container Image Deployment.
- Failover Clustering Implementation.
- Windows Server Monitor and Management

Prerequisites

Functional understanding or working experience and knowledge of…

- Networking fundamentals
- Security best practices
- Active Directory Domain Services (AD DS) concepts
- Configuration of Windows client operating systems
- Server hardware

Academy IT Pty Ltd
Level 4, 45 Grenfell Street
ADELAIDE 5000

Email: sales@academyit.com.au
Web: www.academyit.com.au

Phone: 08 7324 9800
Brian: 0400 112 083

Academy IT

Table of Contents

experience and network utilization within your organization. First, install and configure an additional domain controller in the domain, and then rename the default site object and create a subnet object for the site. Next, create additional sites and subnets, and then configure site links to control replication traffic. Finally, move a server to a new site, and install another domain controller to monitor the replication traffic.

Lessons
See module description

Lab 1: Implement and Administer AD DS Sites and Replication
- Modify the AD DS Default Site.
- Created additional sites and subnets.
- Configure AD DS Replication.
- Monitor and Troubleshoot AD DS Replication.

After completing this module, students will be able to:

- Describe how AD DS replication works.
- Configure AD DS sites to help optimize authentication and replication traffic.
- Configure and monitor AD DS replication.

Module 5: Implement Group Policy
In this hands-on adaptive module, learners will configure group policy for an organization. First, explore the tools and commands available, and then delegate group policy administration to selected users. Next, create Group Policy objects, and assign to the domain and organizational units in the organization, and then configure filters to control the application of policies. Finally, perform analysis of and create reports for group policy application, and then review event logs to troubleshoot group policy application.

Lessons
See module description

Lab 1: Implement Group Policy
- Delegate administration of Group Policy.
- Linked GPOs.
- Filter Group Policy Application.
- Review Group Policy Event Logs.

After completing this module, students will be able to:

- Explain what Group Policy.
- Describe the process to implement.
- Discuss how to administer GPOs.
- Describe Group Policy scope and Group Policy processing.
- Troubleshoot GPO application.

Module 6: Manage User Settings with Group Policy
In this hands-on adaptive module, learners will configure standard desktop environments in an organization by using Group Policy. First, configure standard user settings by using administrative templates, and then configure the Central Store for consistency when applying settings from administrative templates. Next, configure specific user settings for Folder Redirection, and then apply scripts for execution by way of Group Policy

Lessons
See module description

Lab 1: Manage User Settings with Group Policy
- Configure settings with Administrative Templates.
- Configure the Central Store.
- Configure folder redirection.
- Configure scripts with GPOs.
- Configure group policy preferences.

After completing this module, students will be able to:

- Implement administrative templates.
- Configure Folder Redirection, software installation, and scripts.
- Configure Group Policy preferences

Module 7: Secure Active Directory Domain Services
In this hands-on adaptive module, learners will provide additional levels of security across an Active Directory Domain Services (AD DS) infrastructure. First, configure domain wide account and password policies to meet the organization's security requirements, and then configure specific password policies for administrative users. Next, create account restriction policies and configure administrative auditing for AD directory object access, and then

configure authentication auditing for logon events. Finally, configure the settings to prestige Read Only Domain Controllers (RODCs), and then configure a group Managed Service Account, and apply it.

Lessons
See module description

Lab 1: Secure Active Directory Domain Services
- Implement security policies for accounts and passwords.
- Implement audit policies for authentication.
- Deploy and configure a RODC.
- Create and associate a group Managed Service Account (MSA).

After completing this module, students will be able to:

- Secure domain controllers.
- Implement account security.
- Implement audit authentication.
- Configure managed service accounts (MSAs).

Module 8: Deploy and Manage AD CS
this hands-on adaptive module, learners will create and configure a Public Key Infrastructure (PKI) by using Windows Server that can be used to deploy and manage digital certificates. First, prepare an infrastructure to support the deployment of Active Directory Certificate Services (AD CS) including configuring DNS records and configuring web servers as required by the PKI. Next, configure Active Directory with custom policy extensions and then install and configure an offline root CA. Finally, install a subordinate enterprise CA and complete a number of configuration tasks to ensure that the PKI is healthy and ready to deploy certificates to users and devices.

Lessons
See module description

Lab 1: Deploy and Manage AD CS
- Configure DNS records to support host name resolution required by the PKI.
- Configure issuance policies in Active Directory.
- Install and configure an offline root CA.
- Install and configure a subordinate enterprise CA.
- Configure scheduled tasks to automate CRL renewal and distribution to HTTP certificate distribution points.
- Verify the health of the PKI.

After completing this module, students will be able to:

- Deploy certification authorities (CAs).
- Administer CAs.
- Troubleshoot and maintain CAs.

Module 9: Deploy and Manage Certificates
In this hands-on adaptive module, learners will deploy and manage digital certificates. First, configure certificate templates that publish to your production network. Next, enable Key Recovery and Archival of private keys, and then enrol an SSL certificate and bind it to a web site. Finally, configure a group policy to auto enrol certificates for end users, and then simulate the loss of a private key used for encryption and recover the key from the Certification Authority (CA) database.

Lessons
See module description

Lab 1: Deploy and Manage Certificates
- Configure and publish certificate templates
- Configure and enable Key Recovery and Archival
- Issue an SSL certificate and bound it to a web site
- Configure a group policy to auto enrol certificates
- Configure a group policy for Encrypting File System (EFS)
- Verify the functionality of signing and encryption certificates.

After completing this module, students will be able to:

- Deploy and manage certificate templates.
- Manage certificate deployment, revocation, and recovery.
- Use certificates in a business environment.

Module 10: Implement and Administer Active Directory Federation Services (AD FS)

In this hands-on adaptive module, learners will configure Active Directory Federation Services (AD FS). First, configure DNS for AD FS, and then configure the required certificates. Next, install and configure the AD FS role, create the AD FS trust relationships, and then test the connection.

Lessons

See module description

Lab 1: Implement and Administer Active Directory Federation Services (AD FS)

- Configure the required DNS settings.
- Create and install the required certificates.
- Install and configure AD FS in the resource domain and account's domain.
- Configure the required trust relationships.

After completing this module, students will be able to:

- Describe Active Directory Federation Services (AD FS).
- Explain how to deploy AD FS.
- Describe how to implement AD FS for a single organization.
- Explain how to extend AD FS to external clients.
- Implement single sign-on (SSO) to support online services.

Module 11: Implement AD DS Synchronization

In this hands-on adaptive module, learners will install and configure Azure AD Connect. First, configure the prerequisites for AD Connect, and then install AD Connect. Next, configure synchronization, filter attributes, and then verify the settings.

Lessons

See module description

Lab 1: Implement AD DS Synchronization

- Create required accounts for AD Connect.
- Install AD Connect.
- Configure initial synchronization.
- Filter attributes that are being synchronized

After completing this module, students will be able to:

- Plan and prepare for directory synchronization.
- Implement directory synchronization by using Microsoft Azure Active Directory Connect (Azure AD Connect).
- Manage identities with directory synchronization.

Module 12: Monitor, Manage, and Recover AD DS

In this hands-on adaptive module, learners will manage an organization's domain controllers. First, configure Performance Monitor to monitor AD DS, and then perform an offline defrag of the domain controller's AD DS database. Next, create an Active Directory snapshot, and then install Windows Server Backup. Finally, perform a backup of the Active Directory environment.

Lessons

See module description

Lab 1: Monitor, Manage, and Recover AD DS

- Monitor AD DS.
- Perform an offline defrag of AD database.
- Create a snapshot of the AD database.
- Back up and restore AD DS.
- Recover objects in AD DS

After completing this module, students will be able to:

- Monitor AD DS.
- Manage the Active Directory database.
- Describe the backup and recovery options for AD DS and other identity and access solutions.