Enterprise Computing Solutions - Education Services

OFERTA FORMATIVA

Detalles de contacto

Avda Europa 21, 28108 Alcobendas

Email: formacion.ecs.es@arrow.com
Phone: +34 91 761 21 51

Identity with Windows Server 2016

CÓDIGO:	DURACIÓN:	Precio:
MCS_20742	40 Hours (5 días)	A consultar

Description

This five-day instructor-led course teaches IT professionals how to deploy
and configure Active Directory Domain Services (AD DS) in a distributed environment,
how to implement Group Policy, how to perform backup and restore, and how to monitor and troubleshoot Active Directory–related issues with Windows Server 2016. Additionally, this course teaches students how to deploy other Active Directory server roles, such as Active Directory Federation Services (AD FS) and Active Directory Certificate Services (AD CS).

Objetivos

After completing this course, students will be able to:•Install and configure domain controllers.
•Manage objects in AD DS by using graphical tools and Windows PowerShell.•Implement AD DS in complex environments.
•Implement AD DS sites, and configure and manage replication.•Implement and manage Group Policy Objects (GPOs).
•Manage user settings by using GPOs.•Secure AD DS and user accounts.
•Implement and manage a certificate authority (CA) hierarchy with AD CS.•Deploy and manage certificates.
•Implement and administer AD FS.•Implement and administer Active Directory Rights Management Services (AD RMS).
•Implement synchronization between AD DS and Azure AD.
•Monitor, troubleshoot, and establish business continuity for AD DS services.

Público

This course is primarily intended for existing IT professionals who have some AD DS
knowledge and experience and who aim to develop knowledge about identity and access
technologies in Windows Server 2016. This would typically include:
- AD DS administrators who are looking to train in identity and access technologies
with Windows Server 2012 or Windows Server 2016.
- System or infrastructure administrators with general AD DS experience and knowledge who are looking to cross-train in core and advanced identity and access technologies in Windows Server 2012 or Windows Server 2016.
The secondary audience for this course includes IT professionals who are looking to
consolidate their knowledge about AD DS and related technologies, in addition to
IT professionals who want to prepare for the 70-742 exam

Requisitos Previos

efore attending this course, students must have:
•Some exposure to and experience with AD DS concepts and technologies in Windows Server 2012 or Windows Server 2016.
•Experience working with and configuring Windows Server 2012 or Windows Server 2016
•Experience and an understanding of core networking technologies such as IP addressing, name resolution, and Dynamic Host Configuration Protocol (DHCP).
•Experience working with and an understanding of Microsoft Hyper-V and basic server virtualization concepts.
•An awareness of basic security best practices.
•Hands-on working experience with Windows client operating systems such as Windows 7, Windows 8, Windows 8.1, or Windows 10.
•Basic experience with the Windows PowerShell command-line interface.

Programa

Module 1: Installing and configuring domain controllers
This module describes the features of AD DS and how to install domain controllers (DCs). It also covers the considerations for deploying DCs.

Lessons
•Overview of AD DS
•Overview of AD DS domain controllers
•Deploying a domain controller
Lab : Deploying and administering AD DS
•Deploying AD DS
•Deploying domain controllers by performing domain controller cloning
•Administering AD DS
After completing this module, students will be able to:
•Describe AD DS and its main components.
•Describe the purpose and roles of domain controllers.
•Describe the considerations for deploying domain controllers.Module 2: Managing objects in AD DS
This module describes how to use various techniques to manage objects in AD DS. This includes creating and configuring user, group, and computer objects.
Lessons
•Managing user accounts
•Managing groups in AD DS
•Managing computer objects in AD DS
•Using Windows PowerShell for AD DS administration
•Implementing and managing OUs
•Delegate administration for OUs
•Creating and modifying AD DS objects with Windows PowerShellAfter completing this module, students will be able to:
Lab : Managing AD DS objects
•Creating and managing groups in AD DS
•Creating and configuring user accounts in AD DS
•Managing computer objects in AD DS
Lab : Administering AD DS
•Manage user accounts in AD DS.
•Manage groups in AD DS.
•Manage computer objects in AD DS.
•Use Windows PowerShell for AD DS administration.
•Implement and manage OUs.
•Administer AD DS.
Module 3: Advanced AD DS infrastructure management
This module describes how to plan and implement an AD DS deployment that includes multiple domains and forests. The module provides an overview of the components in an advanced AD DS deployment, the process of implementing a distributed AD DS environment, and the procedure for configuring AD DS trusts.
Lessons
•Overview of advanced AD DS deployments
•Deploying a distributed AD DS environment
•Configuring AD DS trusts
Lab : Domain and trust management in AD DS
•Implementing forest trusts
•Implementing child domains in AD DS
•Describe the components of an advanced AD DS deployment.
•Deploy a distributed AD DS environment..
After completing this module, students will be able to:•Configure AD DS trusts.
Module 4: Implementing and administering AD DS sites and replication
This module describes how to plan and implement an AD DS deployment that includes multiple locations. The module explains how replication works in a Windows Server 2016 AD DS environment.
Lab : Implementing AD DS sites and replication
Lessons
•Overview of AD DS replication
•Configuring AD DS sites
•Configuring and monitoring AD DS replication
•Modifying the default site
•Creating additional sites and subnets
•Configuring AD DS replication
•Monitoring and troubleshooting AD DS replication
•Describe how AD DS replication works.
•Configure AD DS sites to help optimize authentication and replication traffic.
After completing this module, students will be able to:•Configure and monitor AD DS replication.
Module 5: Implementing Group Policy
This module describes how to implement a GPO infrastructure. The module provides an overview of the components and technologies that compose the Group Policy framework.
Lessons
•Introducing Group Policy
•Implementing and administering GPOs
•Group Policy scope and Group Policy processing
•Troubleshooting the application of GPOs
Lab : Implementing a Group Policy infrastructure
•Creating and configuring GPOs
•Managing GPO scope
Lab : Troubleshooting Group Policy infrastructure
•Verify GPO application
•Troubleshooting GPOs
After completing this module, students will be able to:
•Explain what Group Policy is.
•Implement and administer GPOs.
•Describe Group Policy scope and Group Policy processing.
•Troubleshoot GPO application.
Module 6: Managing user settings with Group Policy
This module describes how to configure Group Policy settings and Group Policy preferences. This includes implementing administrative templates, configuring folder redirection and scripts, and configuring Group Policy preferences.
Lab : Managing user settings with GPOs
Lessons
•Implementing administrative templates
•Configuring Folder Redirection, software installation, and scripts
•Configuring Group Policy preferences
•Using administrative templates to manage user settings
•Implement settings by using Group Policy preferences
•Configuring Folder Redirection
•Planning Group Policy (optional)

•Implement administrative templates.
•Configure Folder Redirection, software installation, and scripts.
After completing this module, students will be able to:•Configure Group Policy preferences.

Module 7: Securing Active Directory Domain Services
This module describes how to configure domain controller security, account security, password security, and Group Managed Service Accounts (gMSA).
Lessons
•Securing domain controllers
•Implementing account security
•Implementing audit authentication
•Configuring managed service accounts
Lab : Securing AD DS
•Implementing security policies for accounts, passwords, and administrative groups
•Deploying and configuring an RODC
•Creating and associating a group MSA
•Secure domain controllers.
•Implement account security.
•Implement audit authentication.
After completing this module, students will be able to:•Configure managed service accounts (MSAs).
Module 8: Deploying and managing AD CS
This module describes how to implement an AD CS deployment. This includes deploying, administering, and troubleshooting CAs.
Lessons
•Deploying CAs
•Administering CAs
•Troubleshooting and maintaining CAs
Lab : Deploying and configuring a two-tier CA hierarchy
•Deploying an offline root CA
•Deploying an enterprise subordinate CA
•Deploy CAs.
•Administer CAs.
After completing this module, students will be able to:•Troubleshoot and maintain CAs.
Module 9: Deploying and managing certificates
This module describes how to deploy and manage certificates in an AD DS environment. This involves deploying and managing certificate templates, managing certificate revocation and recovery, using certificates in a business environment, and implementing smart cards.
Lessons
•Deploying and managing certificate templates
•Managing certificate deployment, revocation, and recovery
•Using certificates in a business environment
•Implementing and managing smart cards
Lab : Deploying and using certificates
•Configuring certificate templates
•Enrolling and using certificates
•Configuring and implementing key recovery
•Deploy and manage certificate templates.
•Manage certificates deployment, revocation, and recovery.
•Use certificates in a business environment.
After completing this module, students will be able to:•Implement and manage smart cards
Module 10: Implementing and administering AD FS
This module describes AD FS and how to configure AD FS in a single-organization scenario and in a partner-organization scenario.
Lessons
•Overview of AD FS
•AD FS requirements and planning
•Deploying and configuring AD FS
•Web Application Proxy Overview
Lab : Implementing AD FS
•Configuring AD FS prerequisites
•Installing and configuring AD FS
•Configuring an internal application for AD
•Configuring AD FS for federated business partners
•Describe AD FS.
•Explain how to deploy AD FS.
•Explain how to implement AD FS for a single organization.
•Explain how to extend AD FS to external clients.
After completing this module, students will be able to:•Implement single sign-on (SSO) to support online services.
Module 11: Implementing and administering AD RMS
This module describes how to implement an AD RMS deployment. The module provides an overview of AD RMS, explains how to deploy and manage an AD RMS infrastructure, and explains how to configure AD RMS content protection.
Lessons
•Overview of AD RMS
•Deploying and managing an AD RMS infrastructure
•Configuring AD RMS content protection
Lab : Implementing an AD RMS infrastructure
•Installing and configuring AD RMS
•Configuring AD RMS templates
•Using AD RMS on clients
•Describe AD RMS.
•Deploy and manage an AD RMS infrastructure. .
After completing this module, students will be able to:•Configure AD RMS content protection.
Module 12: Implementing AD DS synchronization with Microsoft Azure AD
This module describes how to plan and configure directory syncing between Microsoft Azure Active Directory (Azure AD) and on-premises AD DS. The modules describes various sync scenarios, such as Azure AD sync, AD FS and Azure AD, and Azure AD Connect.
Lessons
•Planning and preparing for directory synchronization
•Implementing directory synchronization by using Azure AD Connect
•Managing identities with directory synchronization

Lab : Configuring directory synchronization
•Preparing for directory synchronization
•Configuring directory synchronization
•Managing Active Directory users and groups and monitoring directory synchronization
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 13: Monitoring, managing, and recovering AD DS
This module describes how to monitor, manage, and maintain AD DS to help achieve high availability of AD DS.
Lessons
•Monitoring AD DS
•Managing the Active Directory database
•Active Directory backup and recovery options for AD DS and other identity and access solutions
Lab : Recovering objects in AD DS
•Backing up and restoring AD DS
•Recovering 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 access solutions.

Fechas Programadas

A petición. Gracias por contactarnos.

Información Adicional

Esta formación también está disponible en modalidad presencial. Por favor contáctenos para más información.