Enterprise Computing Solutions - Education Services

TRAINING OFFERING

Vous pouvez nous joindre ici

.

Email: training.ecs.fr@arrow.com
Phone: 01 49 97 50 00

MD-101: Managing Modern Desktops

CODE:	DURÉE:	PRIX H.T.:
MCS_MD101	40 Hours (5 Jours)	€3,030.00

Description

Course MD-101T01-A: Deploying the Modern Desktop
As desktops has evolved, so have methods for deploying and updating them. In this course, you'll learn how to plan and implement an operating system deployment strategy. This course will help you understand the various methods available, the scenarios they're suited for, as well as how to deploy Windows using modern methods. This course will also cover planning and implementing an update strategy for Windows.

Course MD-101T02-A: Managing Modern Desktops and Devices
As demand for organizations to enable workforces to be more mobile, a desktop administrator's role is really is no longer about just "desktop" management. With BYOD becoming commonplace and the need for employees to access line of business apps on personal devices, the scope of desktop administration must include both desktop and mobile devices, regardless of ownership. During this course, you'll be introduced to key components of modern management and co-management strategies. You'll examine what it takes to incorporate Microsoft Intune into your organization and how to use it to manage modern desktops and devices. You'll also learn about methods for deployment and management of apps and browser-based applications.
Course MD-101T03-A: Protecting Modern Desktops and Devices
Every day, more organizations are asking IT to support mobility in the workforce. Modern environments require the Desktop Administrator be able to manage and support phones, tablets, and computers, whether it be owned by the organization or personally owned by the employee. At the same time, IT must still be able to protect the data that these devices access. In this course, the student will be introduced to the key concepts of security in modern management. This course covers authentication, identities, and access, as well as about how to protect these categories. The student will be introduced to Azure Active Directory and learn how to use Microsoft Intune to protect devices and data with compliance policies. Finally, this course will cover key capabilities of Azure Information Protection and Windows Defender Advanced Threat Protection and how to implement these capabilities

Objectifs

Course MD-101T01-A: Deploying the Modern Desktop
After completing this course, learners should be able to:
•Develop an Operating System deployment and upgrade strategy
•Understand the different methods of deployment.
•Understand which scenarios on-premise and cloud-based solutions can be used for.
•Deploy and migrate desktops to Windows 10.
•Plan and configure Windows Update policies.

Course MD-101T02-A: Managing Modern Desktops and Devices
After completing this course, learners should be able to:
•Understand the benefits and methods of co-management strategies.
•Configuring Intune
•Enroll devices in Intune and configure device policies
•Manage user profiles and folder redirection
•Plan a mobile application management strategy
•Manage and deploy apps, including Office 365 ProPlus and Internet
•Explorer settings
Course MD-101T03-A: Protecting Modern Desktops and Devices

After completing this course, learners should be able to:
•Describe the benefits and capabilities of Azure AD.
•Manage users using Azure AD with Active Directory DS.
•Implement Windows Hello for Business.
•Configure conditional access rules based on compliance policies.
•Describe the various tools used to secure devices and data.
•Implement Windows Defender Advanced Threat Protection.

Audience

The Modern Desktop Administrator deploys, configures, secures, manages, and monitors devices and client applications in an enterprise environment. Responsibilities include managing identity, access, policies, updates, and apps. The MDA collaborates with the M365 Enterprise Administrator to design and implement a device strategy that meets the business needs of a modern organization.
The Modern Desktop Administrator must be familiar with M365 workloads and must have strong skills and experience of deploying, configuring, and maintaining Windows 10 and non-Windows devices. The MDA role focuses on cloud services rather than on-premises management technologies.

Prérequis

The Modern Desktop Administrator must be familiar with M365 workloads and must have strong skills and experience of deploying, configuring, and maintaining Windows 10 and non-Windows devices. The MDA role focuses on cloud services rather than on-premises management technologies.

Programme

Course MD-101T01-A: Deploying the Modern Desktop Module 1: Planning an Operating System Deployment Strategy
This module explains how to plan and implement a deployment strategy. It covers various methods and scenarios for deploying Windows. It discusses on-premise and cloud technologies as well as considerations for new deployments, upgrading, and migrations.
Lessons
•Overview of Windows as a service
•Windows 10 Deployment options
•Considerations for Windows 10 deployment Lab : Practice Lab - Planning Windows 10 deployment
After completing this module, students will be able to:
•Describe Windows as a Service.
•Describe the different methods for deployment.
•Understand the differences between on-premise and cloud-based solutions.
•Describe methods of dynamic provisioning.
•Describe the different tools available in the Windows Assessment and Deployment Kit.
•Describe the scenarios and limitations for in-place upgrades and migrations. Module 2: Implementing Windows 10
This module covers new modern methods for deploying Windows 10 such as Windows Autopilot and provisioning packages. This module also covers tool used in upgrade planning, application compatibility and migration methods.
Lessons Lab : Practice Lab - Implementing Windows 10
•Implementing Windows 10 by using dynamic deployment •Creating and deploying provisioning package
•Implementing Windows 10 by using Windows Autopilot •Migrating user settings
•Upgrading devices to Windows 10 •Deploying Windows 10 with AutoPilot

After completing this course, learners should be able to:
•Develop an Operating System deployment and upgrade strategy
•Understand the different methods of deployment.
•Understand which scenarios on-premise and cloud-based solutions can be used for.
•Deploy and migrate desktops to Windows 10.
•Plan and configure Windows Update policies. Module 3: Managing Updates for Windows 10
This module covers managing updates to Windows. This module introduces the servicing options for Windows 10. Students will learn the different methods for deploying updates and how to configure windows update policies.
Lessons
•Updating Windows 10 Lab : Practice Lab - Managing Updates for Windows 10
•Windows Update for Business •Manually configuring Windows Update settings
•Introduction to Windows Analytics •Configuring Windows Update by using GPOs
After completing this module, students will be able to:
•Describe the Windows 10 servicing channels.
•Configure a Windows update policy using Group Policy settings.
•Configure Windows Update for Business to deploy OS updates. Lessons
•Use Windows Analytics to assess upgrade readiness and update compliance. Module 4: Course Conclusion •Final Exam
Lab : Graded Lab After completing this module, students will be able to:

•Create a provisioning package.
•Configure an Autopilot deployment.
•Describe the tools used for planning upgrades and migrations.
•Describe the methods used to migrate user data.

Course MD-101T02-A: Managing Modern Desktops and Devices Module 1: Device Enrollment
In this module, students will examine the benefits and prerequisites for co-management and learn how to plan for it. This module will also cover Azure AD join and will be introduced to Microsoft Intune, as well as learn how to configure policies for enrolling devices. The module will conclude with an overview of device inventory in Intune and reporting using the Intune console, Power BI and Microsoft Graph.

Lessons
•Device management options
•Manage Intune device enrollment and inventory

Lab : Practice Lab - Device Enrollment and Management
•Installing the MDM Migration Analysis Tool (MMAT)
•Obtain Intune and Azure AD Premium licenses and enable device management
•Enrolling devices in Intune
•Managing devices in Intune
•Creating device inventory reports

After completing this module, students will be able to:
•Describe benefits and methods for migrating to co-management.
•Deploy an MDM with Microsoft Intune.
•Configure device enrollment.
•Enroll desktop and mobile devices in Windows Intune.
•Configure and downloads inventory reports.

Module 2: Configuring Profiles
This module dives deeper into Intune device profiles including the types of device profiles and the difference between built-in and custom profiles. The student will learn about assigning profiles to Azure AD groups and monitoring devices and profiles in Intune. The module will conclude with an overview of using Windows Analytics for health and compliance reporting.

Lessons
•Configuring device profiles
•Managing user profiles
•Monitoring devices

Lab : Practice Lab - Managing profiles
•Configuring roaming user profiles and Folder Redirection
•Create and deploy device profile based on the scenario
•Change deployed policy and monitor user and device activity
•Configuring Enterprise State Roaming

After completing this module, students will be able to:
•Describe the types of device profiles.
•Create and assign device profiles.
•Configure user profile and folder redirection.
•Monitor and report on devices using Intune and Windows Analytics.

Module 3: Application Management
In this module, students learn about application management on-premise and cloud-based solutions. This module will cover how to manage Office 365 ProPlus deployments in Intune as well as how to manage apps on non-enrolled devices. The module will conclude with an overview of Enterprise Mode with Internet Explorer and Microsoft Edge and tracking your installed applications, licenses, and assigned apps using Intune.

Lessons
•Implement Mobile Application Management (MAM)
•Deploying and updating applications
•Administering applications

Lab : Practice Lab - Managing Applications
•Deploying apps by using Intune
•Configure and deploy Office 365 ProPlus from Intune
•Configure mobile application management (MAM) policies in Intune

After completing this module, students will be able to:
•Describe the methods for application management.
•Deploy applications using Intune and Group Policy.
•Configure Microsoft Store for Business.
•Deploy Office365 ProPlus using Intune.
•Manage and report application inventory and licenses.
•Configure Internet Explorer Enterprise Mode.

Module 4: Course Conclusion

Lessons
•Final Exam Lab : Graded Lab

After completing this module, students will be able to:
•Describe the types of device profiles.
•Create and assign device profiles.
•Configure user profile and folder redirection.
•Monitor and report on devices using Intune and Windows Analytics.

Course MD-101T03-A: Protecting Modern Desktops and Devices Module 1: Managing Authentication in Azure AD
In this module, students well be introduced to the concept of directory in the cloud with Azure AD. Students will learn the similarities and differences between Azure AD and Active Directory DS and how to synchronize between the two. Students will explore identity management in Azure AD and learn about identity protection using Windows Hello for Business, as well as Azure AD Identity Protection and multi-factor authentication. The module will conclude with securely accessing corporate resources and introduce concepts such as Always On VPN and remote connectivity in Windows 10.

Lessons
•Azure AD Overview
•Managing identities in Azure AD
•Protecting identities in Azure AD
•Managing device authentication
•Enabling corporate access

Lab : Practice Lab - Managing objects and authentication in Azure AD
•Enabling and configuring Azure AD Premium with Enterprise Mobility + Security (EMS) tenant
•Creating user and group objects with UI and Windows PowerShell
•Configuring Self-service password reset (SSPR) for user accounts in Azure AD
•Joining a device to Azure AD

After completing this module, students will be able to:
•Describe the capabilities of Azure AD.
•Manage users using Azure AD with Active Directory DS.
•Implement Windows Hello for Business.
•Join devices to Azure AD.
•Describe methods of enabling access from external networks. Module 2: Managing Devices and Device Policies

In this module, students will be introduced to managing device security with Intune. Students will discover how Intune can use device profiles to manage configuration of devices to protect data on a device. Students will learn how to create and deploy compliance policies and use compliance policies for conditional access. The module concludes with monitoring devices enrolled in Intune.

Lessons
•Microsoft Intune Overview
•Managing devices with Intune
•Implement device compliance policies

Lab : Practice Lab - Managing devices
•Configuring Microsoft Intune for device management
•Configuring compliance policies and device profiles
•Enrolling Windows 10 devices and managing compliance

After completing this module, students will be able to:
•Describe mobile device management with Intune.
•Create and assign device profiles to protect data on devices.
•Deploy compliance and conditional access policies.
•Use Intune to monitor device compliance. Module 3: Managing Security

In this module, students will learn about data protection. Topics will include Windows & Azure Information Protection, and various encryption technologies supported in Windows 10. This module also covers key capabilities of Windows Defender Advanced Threat Protection and how to implement these capabilities on devices in your organization. The module concludes using Windows Defender and using functionalities such as antivirus, firewall and Credential Guard.

Lessons
•Implement device data protection
•Managing Windows Defender ATP
•Managing Windows Defender in Windows 10

Lab : Practice Lab - Managing Security in Windows 10
•Configuring Encrypting File System (EFS)
•Configuring BitLocker
•Configuring a WIP policy in Intune
•Configuring Windows Defender

After completing this module, students will be able to:
•Describe the methods protecting device data.
•Describe the capabilities and benefits of Windows ATP
•Deploy and manage settings for Windows Defender clients. Module 4: Course Conclusion

Lessons
•Final Exam Lab : Graded Lab

Test et Certification

Microsoft 365 Modern Desktop Administrator

Dates de session

Sur demande. Merci de nous contacter

Informations Complémentaires

Cette formation est également disponible sous forme de formation sur site. Veuillez nous contacter pour en savoir plus.