MS-203: Microsoft 365 Messaging

Microsoft - Microsoft 365

Promoção: **Curso com 15% de desconto**Aproveite já!

Live Training (também disponível em presencial)

- **Localidade:** Imprimir Curso
- **Data:** 16 May 2022
- **Preço:** 1720 € (Os valores apresentados não incluem IVA. Oferta de IVA a particulares e estudantes.)
- **Horário:** Laboral das 9h00 - 17h00
- **Nível:** Intermédio
- **Duração:** 35h

Sobre o curso

This course examines the key elements of Microsoft 365 messaging administration, including message transport and mail flow, messaging security, hygiene, and compliance, messaging infrastructure, and hybrid messaging. This course is designed for IT Professionals who deploy and manage the messaging infrastructure for Microsoft 365 in their organization.

Skills gained:

- Configure and manage the transport pipeline
- Manage and troubleshoot mail flow and transport issues
- Manage message hygiene and compliance
- Manage authentication for messaging
- Configure organizational settings and sharing
- Manage mobile devices
- Manage role-based permissions
- Create and manage recipient objects and resources
- Plan, implement, and troubleshoot public folders
- Plan a hybrid environment
- Perform mailbox migrations
- Deploy and troubleshoot a hybrid environment

Destinatários

The Messaging Administrator deploys, configures, manages, and troubleshoots recipients, permissions, mail protection, mail flow, and public folders in both on-premises and cloud enterprise environments. Responsibilities include managing message hygiene, messaging infrastructure, and hybrid configuration and migration. To implement a secure hybrid topology that meets the business needs of a modern organization, the Messaging Administrator must collaborate with the Security Administrator and Microsoft 365 Enterprise Administrator. The Messaging Administrator should have a working knowledge of authentication types, licensing, and integration with Microsoft 365 applications.

Pré-requisitos

This course is designed for persons who are aspiring to the Microsoft 365 Messaging Administrator role.

Programa

- Managing the Transport Pipeline
- Managing and Troubleshooting Mail Flow
- Managing Message Hygiene
- Managing Compliance
- Managing Organizational Settings
- Managing Mobile Devices
- Managing Role-Based Permissions
- Managing Recipient Objects and Resources
- Managing Public Folders
- Planning a Hybrid Environment
- Performing Mailbox Migrations
- Deploying and Troubleshooting a Hybrid Environment

Module 1: Managing the Transport Pipeline

In this module, you will learn about the different transport components of Exchange, how the message routing works, and how to configure the message flow for your organization. You will examine the tasks that messaging administrators must complete to configure message transport. You will review the message transport options and learn how to configure domains and connectors and how to implement an approval workflow for messaging. You will also learn how to manage transport rules, which are a very

powerful configuration to control the message flow in your organization.

Lessons

- Overview of Transport Services
- Configuring Message Transport
- Managing Transport Rules

Lab : Configure Message Transport

- Create Connectors

After completing this module, students will be able to:

- Describe the transport components of Exchange
- Plan an effective message routing for your organization
- Modify message flow for your organization
- Describe which transport agents exist and what they do
- Configure the different transport options
- Plan and set up domains for your organizations
- Understand how receive and send connectors work
- Describe how message moderation for different recipients work
- Understand what transport rules are
- Describe how transport rules are working
- Configure custom transport rules
- Describe how transport rules can be used for data loss prevention

Module 2: Managing and Troubleshooting Mail Flow

In this module, you will examine the components of mail flow, and you will learn how to manage your mail flow, which is a crucial task for every Exchange administrator. You will study the differences between managing mail flow in Exchange Online, Exchange Server, and Exchange Hybrid deployments. From managing mail flow, you will transition to troubleshooting mail flow issues such as emails not being routed correctly in or outside your organization, or when secure connections cannot be established successfully. Yo will learn about the tools Microsoft provides to help you find the root cause of your issues and fix your mail flow. You will then transition from troubleshooting mail flow to troubleshooting transport issues, such as network-based issues, connector and agent issues, and architectural issues, as well as how to troubleshoot in coexistence. Finally, you will learn how to check event, protocol, and tracking logs when all troubleshooting for service availability and message transport has finished and an issue still persists, or if you must find historical data about issues in the past.

Lessons

- Managing Mail Flow
- Troubleshooting Mail Flow
- Troubleshooting Transport Issues
- Troubleshooting with Logs

Lab : Conditional Mail Routing

- Create Mail Flow Rules

After completing this module, students will be able to:

- Manage mail flow in organizations
- Understand mail flow for Exchange Servers
- Manage mail flow for Exchange Online
- Describe and manage mail flow in hybrid environments
- Understand how to troubleshoot SMTP mail flow issues
- Describe how to troubleshoot issues with a shared namespace
- Describe how to troubleshoot encryption issues with TLS
- Perform troubleshooting for network-based issues
- Describe troubleshooting procedures for connector and agent issues
- Plan troubleshooting for architectural issues
- Understand how to perform troubleshooting in coexistence
- Create searches for the message tracking log
- Describe how to troubleshoot using the protocol logs
- Understand how to work with the event logging for Exchange

Module 3: Managing Message Hygiene

In this module, you will learn about Microsoft Exchange Online Protection (EOP) features and functionality. You will also learn how to plan messaging routing for this service, which provides anti-malware and anti-spam policies that protect your organization against spam and malware and safeguards your organization from messaging-policy violations. You will then review the anti-malware and anti-spam protection that Exchange Server and Online Protection provide, and you will learn how to configure SPAM and malware filters, policies, and settings to provide protection for your users. You will conclude the module by examining Advanced Threat Protection (ATP) and how it extends the protection provided by EOP by filtering targeted attacks that could pass through EOP’s line of defenses, including advanced threats such as zero-day attacks in email attachments and Office documents and time-of-click protection against malicious URLs. You will learn how Microsoft 365 ATP protects users from advanced threats through features such as safe attachments and safe links, and how it generates reports which provide administrators with insight into attacks targeting their tenants through email.

Lessons

- Planning for Message Hygiene
- Managing Anti-Malware and Anti-Spam Policies
- Managing Advanced Threat Protection

Lab : Managing Messaging Hygiene

- Create Hygiene Filters

After completing this module, students will be able to:

- Explain the use and features of Exchange Online Protection
- Plan message routing for Exchange Online Protection
- Investigate the available EOP reports and logs
- Understand the different message header fields relevant for spam and spoofing protection
- Configure anti-spam and anti-malware filters in Exchange Server
- Using additional features for outbound spam filtering and quarantine
- Implementing protection features against phishing and spoofing
- Create transport rules for custom requirements
- Describe the features of Advanced Threat Protection
- Describe the protection provided by Safe Attachment and Safe Links policies
- Understand the spoof intelligence features
- Know how ATP anti-phishing policies work

Module 4: Managing Compliance

This module begins by describing the different compliance features in the Security & Compliance Center (SCC) that messaging administrators can use to comply with legal and regulatory requirements. This module supports compliance in Exchange by examining the compliance features available in the Exchange Admin Center for Exchange Server and hybrid deployments. Because of the complex retention requirements of modern messaging environments, this module focuses on how archiving is performed with Exchange so that you can provide an efficient and compliant environment to your users. You will also examine how additional archive storage is provided to your users, how messages are automatically processed and archived, and how audit logging in Exchange that provides information about administrator, delegate, and user actions in user mailboxes and your Exchange organization. Finally, because organizations must adhere to legal discovery requirements (related to organizational policy, compliance, or lawsuits), you will examine how eDiscovery for Microsoft Exchange can help you perform discovery searches for relevant content within mailboxes.

Lessons

- Messaging Compliance in the SCC

- Messaging Compliance in Exchange
- Managing Exchange Online Archiving and Auditing
- Managing Content Search

After completing this module, students will be able to:

- Describe different policy and compliance features for messaging
- Evaluate the different roles in the Security & Compliance Center
- Plan retention policies for Exchange Online mailboxes
- Configure data loss prevention (DLP) policies for data in Microsoft 365
- Create message traces to understand the mail flow in your Exchange Online organization
- Describe litigation and in-place holds in Exchange Server
- Plan retention and deletion with Message Records Management (MRM)
- Protect your mail flow with data loss prevention policies in Exchange Server
- Investigate the message tracking log in your Exchange organization
- Describe what in-place archiving is and how it works
- Understand the differences between journaling and archiving
- Know what the mailbox and administrator audit logs are used for
- Understand content searches to search for messages in your organization
- Describe eDiscovery cases and in-place eDiscovery for Exchange
- Manage Advanced eDiscovery cases in the Security & Compliance Center

Module 5: Managing Organizational Settings

This module begins with an examination on how to manage authentication for messaging. This module focuses on how to ensure that user accounts are well protected and secure, and how to deploy multiple security features that do not introduce unnecessary complexity in users' everyday work, which can result in lower business productivity and new security risks. You will then transition from messaging authentication to organizational settings, where you will learn how to configure settings that apply to the entire organization or to many users in the organization. Finally, you will examine how to configure organizational sharing.

Lessons

- Managing Authentication for Messaging
- Configuring Organizational Settings
- Configuring Organizational Sharing

After completing this module, students will be able to:

- Configure password policy options
- Configure self-service password management

- Implement multi-factor authentication
- Plan password policies
- Configure workload policies and throttling
- Configure quota configurations
- Configure Exchange Server and Skype for Business integration
- Deploy Office 365 add-ins
- Provide an overview of Exchange federated delegation sharing features
- Describe federated sharing components
- Explain considerations for designing and implementing federation trusts and certificates
- Implement organization relationships
- Implement sharing policies

Module 6: Managing Mobile Devices

In this module, you will begin by examining Mobile Device Management in Microsoft 365, as well as how Exchange ActiveSync and mobile device mailbox policies support this effort. You will then examine how to manage and troubleshoot mobile device access. This module then examines how to configure both access and infrastructure for mobile devices, understanding the implications of mobile device remote wipe, and learning about alternative methods for mobile device management.

Lessons

- Mobile Device Mailbox Policies
- Managing Mobile Device Access

Lab : Implement ActiveSync

- Implement Active Sync for single and multiple mailboxes

After completing this module, students will be able to:

- Describe how Exchange ActiveSync works
- Configure mobile device mailbox policies
- Understand Mobile Device Management in Microsoft 365
- Configure access for mobile devices
- Understand components of mobile device infrastructure
- Tell how a mobile device remote wipe works
- Describe alternatives for mobile device management
- Troubleshoot mobile device access

Module 7: Managing Role-Based Permissions

This module examines how messaging administrators manage role-based permissions, which is an

essential task for any messaging administrator. Since Exchange Server and Exchange Online both use the Role Based Access Control (RBAC) permission model, this module examines the basics of RBAC management. The module concludes by examining how a messaging administrator must plan and configure permissions carefully so as not to put their environment or their entire Active Directory at risk.

Lessons

- Managing Admin Roles
- Managing User Roles
- Exchange Setup – RBAC and AD Split Permission

Lab : Manage Roles and Permission Policies

- Manage Roles and Permission Policies

After completing this module, students will be able to:

- Describe how RBAC is used to assign roles to users
- Understand what management role group for administrative tasks are
- Assign the built-in management roles for administration
- Create custom management roles and assign them through role assignment policies to users
- Troubleshoot RBAC management roles
- Describe the built-in end-user roles
- Configure role assignment policies
- Create new custom roles and role assignment policies
- Understand the differences between shared permissions and split permissions
- Describe multi-forest permissions
- Identify the differences between the permission models

Module 8: Managing Recipient Objects and Resources

This module examines some of the most common tasks that messaging administrators perform – creating and configuring email recipients, lists, and resources. This module examines the different types of Exchange Server recipients, including how they differ from each other. The module then focuses on the various tasks that require you to create and manage Exchange recipients in Exchange, including user mailboxes, resource mailboxes, shared mailboxes, mail contacts, and mail users. You will also learn how to manage permissions for recipients, and how to create and manage groups.

Lessons

- Exchange Recipients
- Creating and Managing Exchange Recipients
- Managing Email Addresses, Lists, and Resources

Lab : Create Recipient Objects and Resources

- Create Exchange Recipients
- Create Groups

After completing this module, students will be able to:

- Describe the different recipient objects in Exchange
- Describe resource mailboxes
- Describe shared mailboxes
- Describe linked mailboxes and site mailboxes
- Describe groups
- Create and manage Mailbox settings
- Create and manage Resource and Shared mailboxes
- Create and manage Mail contacts and mail users
- Create and manage Recipient permissions
- Create and manage Groups
- Describe address lists
- Explain how to configure address lists
- Describe address book policies
- Explain how to configure offline address books
- Describe email address policies

Module 9: Managing Public Folders

In this module, you will learn about public folders in Exchange, review the planning considerations for deploying public folders, and discuss alternatives to public folders. You will also learn how to implement and manage public folder mailboxes, public folders, and public folder permissions, as well as how to create and manage mail-enabled public folders. The module concludes by examining how to monitor and troubleshoot Public Folder-related issues.

Lessons

- Planning the Public Folder Hierarchy
- Implementing and Managing Public Folders
- Troubleshooting Public Folders

Lab : Implement Public Folders

- Create Public Folders
- Manage Public Folders

After completing this module, students will be able to:

- Describe public folders in Exchange
- Plan a public folder hierarchy
- Plan public folder mailboxes
- Explain public folder quotas
- Evaluate alternatives to public folders
- Describe considerations for implementing Public Folders
- Deploy public folder mailboxes
- Manage public folder permissions
- Create and manage mail-enabled public folders
- Monitor public folders
- Troubleshoot public folders
- Troubleshoot public folder access

Module 10: Planning a Hybrid Environment

In this module you will examine the requirements necessary to implement a hybrid deployment, and you will learn about the features and components that are required when implementing a hybrid deployment. This module examines all planning aspects that are required before running the Hybrid Configuration Wizard. This includes the configuration options of the HCW, as well as the details on Organization Configuration Transfer (OCT) and the Hybrid Agent. The module concludes with a review of the mail flow options for a hybrid deployment.

Lessons

- Exchange Hybrid Deployment Requirements
- Planning to Run the Hybrid Configuration Wizard

Lab : Prepare Azure AD for Hybrid Synchronization

- Prepare Azure AD for Hybrid Synchronization

After completing this module, students will be able to:

- Describe connection options that are available for connecting on-premises Exchange to Microsoft 365
- List and describe components of a hybrid deployment
- Describe Azure Active Directory Connect (Azure AD Connect)
- Identify Microsoft 365 identity options for Exchange hybrid
- Compare Exchange delegated federation vs. OAuth
- Plan for Exchange Hybrid configuration
- Describe Organization Configuration Transfer
- Explain Exchange Modern Hybrid and Hybrid Agent
- Plan mail flow options for a hybrid deployment

Module 11: Performing Mailbox Migrations

This module examines the options that are available for migrating email to Exchange Online, such as performing a migration or using FastTrack to move mailboxes from your existing mail servers to Exchange Online. This module summarizes the migration and co-existence options and recommends when to use which option. The module then examines the requirements for running an IMAP migration, the migration options that are available, and the steps that are performed during a migration. The module then examines how to plan and perform both a cutover and staged migration. It compares each of these two migration approaches, and you will learn about the requirements, planning activities, and migration process for each option. The module concludes by examining important additional migration tasks, such as migrating a PST file and the considerations for a Public Folder migration.

Lessons

- Planning Mailbox Migrations
- Performing IMAP Migrations
- Performing Cutover and Staged Migrations
- Performing Advanced Migrations

After completing this module, students will be able to:

- Describe the migration and coexistence strategies with Exchange Online
- Use FastTrack to move mailboxes
- Describe the requirements for an IMAP migration and how it’s carried out
- Move mailbox data using an IMAP migration
- Describe the requirements for both cutover and staged migrations
- Perform a migration and move mailboxes either with a cutover or staged migration
- Import PST Files to Exchange Online mailboxes
- Migrate Public Folders to Exchange Online

Module 12: Deploying and Troubleshooting a Hybrid Environment

In this module you will learn the key areas to plan for regarding Edge Transport servers. You will then learn about the requirements and best practices to configure a hybrid deployment, which is the first step for your Exchange organization, regardless of whether you want to connect your Exchange on-premises and Exchange Online organizations for long-term coexistence or as part of a cloud migration strategy. In this module, you will then examine how to manage a hybrid deployment and implement advanced hybrid functionality. You will cover the features that require a successful hybrid deployment such as Public Folder coexistence or OneDrive for Business attachment storage for on-premises mailboxes. This module concludes with an introduction to troubleshooting techniques for a hybrid deployment. You will learn how to troubleshoot directory synchronization issues including pass-through authentication (PTA) and single sign-on, Exchange transport, and client access troubleshooting as well as mailbox replication

service troubleshooting.

Lessons

- Deploying and Managing an Edge Transport Server
- Configuring a Hybrid Deployment using the HCW
- Implementing Advanced Hybrid Functionality
- Troubleshooting Hybrid Deployments

Lab : Deploy a Hybrid Environment

- Set Up your Hybrid Deployment
- Test your Hybrid Deployment

After completing this module, students will be able to:

- Describe the purpose and functionality of Edge Transport servers
- Explain the infrastructure requirements for Edge Transport servers
- Describe EdgeSync
- Plan for message flow with an Edge Transport server
- Describe the prerequisites to run the Office 365 Hybrid Configuration Wizard
- Explain best practices for implementing a hybrid deployment
- Manage a hybrid deployment
- Describe when you must configure Public Folder coexistence with Office 365
- Explain how to configure Oauth for a mixed Exchange environment
- Describe how to configure OneDrive for Business attachments for on-premises mailboxes
- Troubleshoot Directory synchronization
- Troubleshoot Pass-Through Authentication and Single Sign-On
- Troubleshoot Transport with Exchange Online
- Troubleshoot Client Access in Coexistence
- Troubleshoot Mailbox Replication Service