Course 50404B:

Overview of Active Directory Rights Management Services with Windows Server 2008 R2

Course Outline

Module 1: Why Rights Management

This module provides an overview of Microsoft Active Directory Rights Management Services (AD RMS). The overview describes how the product works, the business reasons for using AD RMS, and the technology that you use to deploy an AD RMS environment.

Lessons

- A Bit of History
- Business Reasons for AD RMS
- What AD RMS Does
- AD RMS Usage Scenarios
- AD RMS Technology Overview

Lab : AD RMS Demonstration

After completing this module, students will be able to:

- Understand how RMS technology has evolved on the Windows platform
- Explain the business reasons for using AD RMS.
- Explain the features AD RMS provides.
- Identify the advantages and limitations inherent in AD RMS.
- Describe how AD RMS works with public key technology.
- Describe how AD RMS works.

Module 2: AD RMS Architecture, Installation, and Provisioning

This module covers the basic architecture and concepts of AD RMS. Most of the concepts introduced in this module will be covered in more detail in other modules later in the course. The student will also learn the procedure for deploying AD RMS servers, as well as the permissions required for the accounts that are used in the deployment and management of AD RMS.

Lessons

- AD RMS Components Overview
- AD RMS Bootstrapping Process
- AD RMS Publishing and Licensing Process

- AD RMS Service Connection Point (SCP)
- AD RMS Topology
- AD RMS Prerequisites
- Installing and Provisioning AD RMS

Lab : Creating the AD RMS Service AccountLab : Installing and Provisioning AD RMS

After completing this module, students will be able to:

- Describe how AD RMS works.
- Identify the major components of AD RMS.
- Describe the types of licenses used in the AD RMS process.
- Describe the client-side software and applications required for AD RMS.
- Identify the AD RMS server hardware and software requirements.
- Install and provision an AD RMS server.
- Configure the AD RMS service connection point.

Module 3: Active Directory Rights Management Clients and Information Rights Management on Desktop Applications

This module begins by describing the AD RMS client software, its requirements, and how to deploy it. Next, the module identifies the rights management components on client machines and the bootstrapping process the AD RMS client performs for each user. The module then discusses how Information Rights Management (IRM) is provided in the Microsoft Office system, the XPS format, Window Mobile 6.0, and read-only access in Windows Internet Explorer. The module ends with a discussion of registry keys in AD RMS.

Lessons

- OS Versions and AD RMS Clients
- Microsoft Office IRM
- XPS IRM
- Rights Management Add-on for Internet Explorer and Rights-managed HTML
- Office Viewers and AD RMS

Lab : Protecting and Consuming AD RMS Protected Documents

Lab : Creating and Consuming AD RMS Content Using Microsoft Office Outlook 2007Lab : Protecting and Consuming Content Using XPS

- After completing this module, students will be able to:
- Describe AD RMS client software and its requirements.
- Deploy the Windows RMS client software in legacy clients.
- Identify the AD RMS components that are installed on client machines.
- Explain how IRM works in Microsoft Office products.
- Describe how the XPS format uses IRM, and how XPS can be used in conjunction with Microsoft Office applications.
- Explain how the Rights Management add-on for Internet Explorer enables users to view restricted files.

Module 4: Rights Policy Templates and the Super Users Group

This module provides an introduction to rights policy templates and the concepts regarding protecting and consuming content that is protected by templates. These templates are used to standardize security policies and protect information according to the latest policy.

Lessons

- Introduction to Rights Policy Templates
- Creating Rights Policy Templates
- Protecting Content Using Templates
- Consuming Content Protected by Templates
- The Super Users Group

Lab : Creating and Using a Rights Policy Template

Lab : Modifying Existing Templates

Lab : Distribute a Rights Policy Template

Lab : Configuring the Super Users Group

After completing this module, students will be able to:

- Describe the features offered in rights policy templates.
- Identify template distribution features in AD RMS.
- Describe the processes for protecting and consuming content protected by rights policy templates.
- Define rights policy templates.
- Assign users and groups to rights policy templates.
- Specify expiration policies in rights policy templates.
- Explain how to retire and back up rights policy templates.

Module 5: Information Rights Management on Server Applications

This module shows how AD RMS integrates with server-side applications, that use AD RMS to automatically protect and license content. This module covers the following server products:

- Microsoft Office SharePoint Server (MOSS) 2007

- Microsoft Exchange Server 2010

- AD RMS Bulk Protection Tool + FCI

Lessons

- Microsoft Office SharePoint Server 2007 IRM
- Email Protection in Exchange Server 2007
- New AD RMS Features in Exchange Server 2010
- AD RMS Bulk Protection Tool and File Classification Infrastructure

Lab : Integrating AD RMS and Microsoft SharePoint Server 2007

Lab : Integrating AD RMS and Microsoft Exchange Server 2010

Lab : Integrating AD RMS with Bulk Protection Tool

Lab : Protect Information Automatically Integrating AD RMS with FCI and Bulk Protection Tool

After completing this module, students will be able to:

- MOSS IRM
- Describe how MOSS works with AD RMS to protect documents stored in MOSS document libraries.
- Identify MOSS functionality.
- Describe MOSS's logical and physical architecture.
- Describe how IRM works with MOSS to provide information protection.
- Exchange Server 2010
- Explain the new features provided in Exchange 2010 around AD RMS.
- AD RMS Bulk Protection Tool + FCI
- Describe how AD RMS Bulk Protection Tool can be used.
- Describe how FCI can be used.

Module 6: Managing Trust

This module discusses the trust architecture in AD RMS, how trusted user domains operate, and the types of trusts that are available—including Active Directory Federation Services (FS).

Lessons

- Introduction to AD RMS Trust Policies
- Trusted User Domains
- Trusted Publishing Domains
- AD RMS and Active Directory Federation Services
- Windows Live ID Trust

Lab : Configuring Trusted User Domains

Lab : Configuring AD FS Trust and User Experience

After completing this module, students will be able to:

- Describe the core trust architecture in AD RMS.
- Describe Trusted User Domains and how they work.
- Explain when Trusted Publishing Domains are used and how they work.
- Describe the Active Directory Federation Service and how it works with AD RMS.
- Describe Windows Live ID and how it works.