

Deploying and Managing Active Directory Federation Services in Microsoft Windows Server 2003 R2

Course 4358: Two days; Instructor-Led Introduction

This two-day instructor-led course provides the students with the knowledge and skills that they need to effectively deploy and manage Active Directory Federation Services using Microsoft Windows Server 2003 R2. Specifically, students learn what ADFS is and how it can be used to provide Web-based single-sign-on (SSO) for users to authenticate to multiple Web applications over the life of a single online session.



Audience

The target audience for this course is primarily the Enterprise level IT Specialist, or the Mid Market IT Generalist. Attendees should have at least 2-3 years experience using Windows Server 2003 or Windows Server 2003 R2.



At Course Completion

After completing this course, students will gain the skills to:

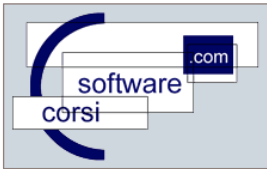
- Understand the business need for Active Directory Federation Services.
- Implement and manage the ADFS server components.
- Plan and implement an authentication and authorization strategy using ADFS.
- Implement ADFS in a B2B scenario using Active Directory and claims-aware applications.
- Implement ADFS in an extranet scenario using multiple directory stores, and Windows NT token-based applications.



Prerequisites

Before attending this course, students must have:

- Experience managing users, roles, computers, and groups - e.g. identify and modify a



- group and manage group membership.
- Experience using the Windows interface to locate, create and manipulate folders and files.
 - General knowledge of computer hardware components such as memory, hard disk drives and central processing units.
 - General knowledge of networking concepts such as network operating system, server-client relationship, and local area network (LAN), and understand the basics of networking in a Windows 2003 environment.
 - The ability to identify the tools used to perform common administrative tasks.
 - Experience managing and maintaining an Active Directory infrastructure-for example, create a forest root domain.
 - Some experience in planning and implementing an Active Directory infrastructure.



Course Outline

Module 1: Active Directory Federation Services Overview

This module provides information about the business benefits of ADFS and the various scenarios that can benefit from deploying an ADFS solution. This module also provides an overview of the underlying standards and technologies that are used by ADFS.

Lessons

- ADFS Business Benefits
- ADFS Technologies
- ADFS Deployment Scenarios

After completing this module, students will be able to:

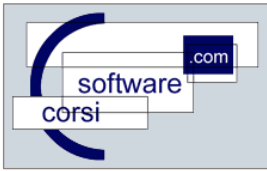
- Describe the business benefits of deploying ADFS.
- Describe the underlying technologies and standards used by ADFS.
- Explain the ADFS deployment scenarios.

Module 2: Deploying and Managing the ADFS Components

This module describes the prerequisite components that must be installed, and how to deploy and manage the ADFS components. This module also provides guidance on planning the ADFS component deployment.

Lessons

- Deploying the ADFS Prerequisite Components
- Implementing the ADFS Server Components
- Managing the ADFS Server Components



- Planning the ADFS Server Component Deployment

After completing this module, students will be able to:

- Deploy the prerequisite components required to support an ADFS solution.
- Implement each of the ADFS server components.
- Manage the ADFS server components.
- Describe general guidelines to assist in planning an ADFS server component deployment.

Module 3: Planning and Implementing Authentication and Authorization by Using ADFS

This module provides an overview of how authentication and authorization works in ADFS, and then describes how to implement a federated solution.

Lessons

- Understanding Authentication and Authorization in ADFS
- Implementing ADFS Trust Policies
- Implementing ADFS Claims
- Planning ADFS Identity Federation Solutions

After completing this module, students will be able to:

- Describe how authentication and authorization works in ADFS.
- Implement ADFS trust policies.
- Implement ADFS claims between partner organizations.
- Plan the implementation of an identity federation solution.

Module 4: Implementing ADFS in a B2B Scenario

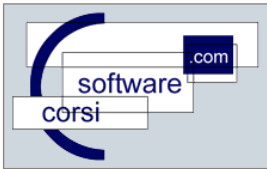
This module provides detailed steps for how to deploy ADFS in a business-to-business scenario where the organizations want to exchange authentication and authorization information so that users can share specific information.

Lessons

- Deploying ADFS Components in a B2B Scenario
- Implementing ADFS Authentication and Authorization in a B2B Scenario
- Lab: Implementing ADFS in a B2B Scenario

After completing this module, students will be able to:

- Describe the configuration components required to deploy ADFS in a B2B scenario.



- Describe Authentication and Authorization in a B2B scenario.
- Implement ADFS in a B2B scenario.

Module 5: Implementing ADFS in an Extranet Scenario

This module provides detailed steps for how to deploy ADFS in an extranet scenario where the users are accessing information from an organization's extranet Web site, but the organization does not want to be responsible for maintaining or synchronizing user passwords from external organizations.

Lessons

- Deploying ADFS Components in an Extranet Scenario
- Implementing ADFS Authentication and Authorization in an Extranet Scenario
- Lab: Implementing ADFS in an Extranet Scenario

After completing this module, students will be able to:

- Describe the configuration components required to deploy ADFS in an extranet scenario.
- Describe Authentication and Authorization in an extranet scenario.
- Implement ADFS in an extranet scenario.