Publication date : 06/03/2024

Course : Active Directory Federation Services (ADFS 4.0)

Practical course - 4d - 28h00 - Ref. ADL
Price : 2630 € E.T.

Single sign-on (SSO) allows users to authenticate only once and access multiple distributed resources. This course presents Active Directory Federation Services (AD FS), a Microsoft solution for implementing SSO.

Teaching objectives

At the end of the training, the participant will be able to:

- Install and configure a public key infrastructure for ADFS
- Deploy ADFS to provide claims-based authentication in a single organization
- Deploying ADFS to provide authentication in a business-to-business federation
- Design and deploy advanced scenarios, including high availability and SAML interoperability
- Use the claims rules language to create custom rules
- Troubleshooting ADFS

Intended audience

System administrator.

Prerequisites

Basic knowledge of network and operating systems. Knowledge of backup and restore principles in a Windows Server environment. Experience of Active Directory.

Practical details

Hands-on work

Training alternating theory and practice.

Course schedule

PARTICIPANTS

System administrator.

PREREQUISITES

Basic knowledge of network and operating systems. Knowledge of backup and restore principles in a Windows Server environment. Experience of Active Directory.

TRAINER QUALIFICATIONS

The experts leading the training are specialists in the covered subjects. They have been approved by our instructional teams for both their professional knowledge and their teaching ability, for each course they teach. They have at least five to ten years of experience in their field and hold (or have held) decision-making positions in companies.

ASSESSMENT TERMS

The trainer evaluates each participant's academic progress throughout the training using multiple choice, scenarios, hands-on work and more.
Participants also complete a placement test before and after the course to measure the skills they've developed.

1 Introduction to Active Directory Federation Service

- Understand claim-based authentication.
- Overview of ADFS components and deployment scenarios.
- Understand ADFS protocols (SAML, WS-Federation, WS-Trust, OAuth).
- Understanding the AD FS WID and SQL database.
- Understanding ADFS FARM with WID.
- Understanding ADSF FARM with SQL.

2 Implementing an ADFS cluster

- Requirements for deploying ADFS services.
- Understand and implement a public key infrastructure for an ADFS cluster.
- Request a server communication certificate for ADFS.
- Install and configure the ADFS cluster with WID as resource provider.
- Check ADFS cluster configuration.
- Understanding ADFS endpoints.
- Install and configure a secondary ADFS server in the cluster - modify the server role.
- Understand failover to the secondary server.

3 Understanding and implementing the ADFS attribute store, approvals and claims

- Understand the different types of attribute store - AD, LDAP and SQL.
- Understanding the claim provider trust.
- Understanding relying party trust.
- Understanding claim rules: emission transformation rule.
- Understand claim rules: authorization rule, delegation authorization rule.

4 Configuring an application based on SAML claims

- Installation and configuration of a web server in an organization integrating a resource provider.
- Installation and configuration of the Windows Identity Foundation SDK.
- Conversion of a web application into a claim-based application using the Windows identity base.

5 Implementing claim-based authentication

- Create a relying party trust for a claims-based application.
- Integrate an "issuance transform rule" into the relying party trust.
- Integrate an "Issuance acceptance rule" in the claims producer.

6 Additional ADFS configuration scenarios

- Understanding Azure Active Directory.
- Claim-providing organization versus resource-providing organization.
- Create a "Relying Party Trust" between two organizations.
- Custom domain configuration.
- Create a relying party trust.
- Create a "claim provider trust" between two organizations.
- Create an emission transformation rule in the relying party trust.
- Create an ADFS backup.
- Configuration of rapid restore tool.
- Create an emission acceptance rule in the claim provider trust.

TEACHING AIDS AND TECHNICAL RESOURCES

• The main teaching aids and instructional methods used in the training are audiovisual aids, documentation and course material, hands-on application exercises and corrected exercises for practical training courses, case studies and coverage of real cases for training seminars.
• At the end of each course or seminar, ORSYS provides participants with a course evaluation questionnaire that is analysed by our instructional teams.
• A check-in sheet for each half-day of attendance is provided at the end of the training, along with a course completion certificate if the trainee attended the entire session.

TERMS AND DEADLINES

Registration must be completed 24 hours before the start of the training.

ACCESSIBILITY FOR PEOPLE WITH DISABILITIES

Do you need special accessibility accommodations? Contact Mrs. Fosse, Disability Manager, at psh-accueil@orsys.fr to review your request and its feasibility.

7 WAP service implementation

- What is a WAP (Web Application Proxy)?
- How does WAP work?
- Configure a WAP server.
- Publish a relying party on a WAP server.

8 Implementing ADFS authentication for an on-cloud application

- Understanding Azure Active Directory.
- Custom domain configuration.
- Create a relying party trust.

9 ADFS backup

- Create an ADFS backup.
- Configuration of rapid restore tool.

Dates and locations

REMOTE CLASS
2026 : 23 June