Masterclass: Administering and Configuring ADFS & Managing ADFS for Multiple Organizations

Duration: 5 Days **Course Code: ADFS** **Delivery Method: Company Event**

Overview:

This course will teach you the **Active Directory Federation Services** course and the **Managing Active Directory Federation Services** course.

Included in the course:

Active Directory Federation Services and Claims workshop is the best way to learn how to implement the most business oriented server role!

Federated Identity and claims based applications are becoming more and more popular – they simplify the resource access both for your employees and business partners. The course focuses on implementation scenarios, including practice in the newest technologies and solutions delivered with Windows Server 2012 R2. When the world becomes more focused on solving 'Bring Your Own Device' issues, it is time to become more up to date with the newest technology capabilities: Active Directory Federation Services and Active Directory Domain Services have been extended to comprehend the most popular mobile devices and provide conditional access and access policies. With these policies in place, you can control access based on users, devices, locations, and access times. Come and learn how to establish partnerships with your business parties, how to implement Single Sign On to access corporate resources, how to manage access to devices and how to implement capabilities to work from anywhere in the world!

This course is intended for IT professionals who would like to implement and administer Active Directory Federation Services within the organization. Prerequisite for the course is to have a medium level knowledge about Active Directory Domain Services.

All exercises are based on Windows Server 2012 R2 and Windows 8.1. Some examples are also shown on Windows Server 2012 to accommodate the difference.

Multi organization Active Directory Federation Services is a perfect course if you need to implement Active Directory Federation Services across different organizations!

Federated Identity is the most discussed topic in terms of organization cooperation right now, and with this course you will get all the knowledge you will need when you are planning to host services that will connect users across different organizations.

As an add-on course, we will extend previous labs with multi organizations trust, discover problems arising from connecting remote parties and find an automated way to make sure that everything is working smoothly. Using Active Directory Federation Services 3.0 on Windows 2012 R2, we will connect parties using various active directory topologies and versions, to simulate all the problems that you will be facing in real world deployment. As a CQURE course, we will focus on security of Active Directory Federation Services, and show a way to solve common access problems – from hacking the user identity, to solving permission problems.

A good enterprise implementation is not complete if we do not think about backup and scripting – so after implementing business partner connectivity, we will focus on scripting the implementation, which will not only allow us to quickly backup and restore our servers, but also allow us to prepare automatic configuration scripts for remote party.

The last part of this course is focused on large Active Directory Federation Services implementations, where load-balancing client traffic is a must. You will not only learn how to load balance Active Directory Federation Services farm, but also get to known Microsoft load balancer included in IIS.

This course is intended for IT professionals who would like to implement and administer Active Directory Federation Services across the organizations. Prerequisite for the course is to have a medium level knowledge about Active Directory Domain Services, basic knowledge of Windows PowerShell and DNS.

Company Events

These events can be delivered exclusively for your company at our locations or yours, specifically for your delegates and your needs. The Company Events can be tailored or standard course deliveries.

Target Audience:

Enterprise administrators, infrastructure architects, security professionals, systems engineers, network administrators, IT professionals, security consultants and other people responsible for implementing network and perimeter security.

ADFS

Objectives:

- **ADF**
- **After completing this course you should be able to:**
- Design AD Federation Services infrastructure and identify the implementation requirements
- Deploy AD Federation Services to provide claims-aware authentication in a single organization
- Implement AD Federation Services high availability
- Deploy Web Application Proxy (previous: AD Federation server proxy) to securely publish web applications
- Deploy Device Registration Service to enable control of user devices
- Deploy Claims-enabled ACLs on File Servers

- **ADS**
- **After you complete this course you will be able to:**
- Deploy AD Federation Services to provide claims-aware authentication for multiple organizations.
- Implement AD Federation Services high availability and load balancing.
- Implement Claims filtering and processing, to secure multi-organization enabled application.
- Script and backup ADFS environment.
- Automate business partner setup procedure for ADFS.
- Configure Active Directory for ADFS

Prerequisites:

Attendees should meet the following prerequisites:

- Good hands-on experience in administering a Windows infrastructure.

Testing and Certification

Recommended as preparation for the following exams:

- There are no exams currently aligned to this course.

Content:

ADF

Module 1

- Introduction
- What are Claims
- Dynamic Access Control
- LAB: Dynamic Access Control in 2016
- LAB (optional): DAC and Groups

Module 2

- What are current authentication mechanism in use
- LAB: Working with SPN
- Services Accounts – threats and gMS
- LAB: Enabling gMSA creation
- LAB (optional): Service credentials recovery (Windows)
- LAB (optional): IIS app pool password recovery
- PKI: Quick Overview of certification services – internal and 3rd party
- LAB: Requesting certificates
- LAB: Installing ADFS

Module 3

- Designing Modern Authentication
- ADFS Overview
- LAB (optional/demo): Installing ADFS Cluster

Module 4

- Working with ADFS – enable applications
- LAB: Install Simple Claims applications
- LAB (optional): Verify application config
- ADFS Basics – Rules and Rule flow
- LAB: Configuring Issuing rules

Module 5

- Thick applications, and working with multiple Relaying Parties
- LAB: Configuring Dynamics CRM
- LAB: Testing with Outlook
- LAB (optional): Testing with Windows 10
- Attribute Stores
- LAB: Configuring application Store
- LAB: Configuring authorization rules
- LAB (optional): Using groups in authorization rules

Module 6

- Web Application Proxy
- LAB: Installing WAP
- LAB: Configuring ADFS publishing
- LAB: Configuring Claims-aware application
- LAB (optional): Configure via application
- LAB (optional): Configure pass-through application

Module 7

- Customizing ADFS
- LAB: ADFS Customization
- Troubleshooting ADFS
- LAB: ADFS Troubleshooting
- Working with MFA

Module 8

- Enabling Device Registration Service
- LAB: Enabling Device Registration Service and working with claims
- Summary and review
- Exchange and claims (additional content)
- SharePoint and claims (additional content)
- Work Folders (additional content)

ADS

Module 1

- Working with external parties
- LAB: Installing ADFS in Forest/Domain trust environment
- LAB (optional): Install ADFS in 2003 domain-level environment
- LAB: Testing simple web application
- LAB: Testing thick application

Module 2

- Home Realm Discovery
- LAB: Hacking ADFS Claims
- LAB: Authorizing users
- Working with groups
- LAB: Adding additional claims
- LAB: Multiple roles and claims
- CpT and rules
- LAB: Per-CpT Rules
- LAB: MFA and CpT

Module 3

- Scripting ADFS
- LAB: Backup ADFS Config
- LAB: Export RP and CpT
- LAB: Unattended Installation

Module 4

- Working with clients
- LAB: Creating automatic client configuration scripts
- Working with IE Security Zones
- LAB: Creating GPO for IE zones
- LAB: Creating automated Claim Provided Trust configuration for clients

Module 5

- Load Balancing ADFS
- Setting up ADFS Farm
- LAB: Using IIS ARR to load-balance ADFS
- LAB (optional): Clustering IIS ARR