

Active Directory Services with Windows Server



Purpose of the training

The training addressed to people responsible for Active Directory infrastructure management in Windows Server 2012/2012R2 and who would like to acquire skills necessary for better managing and protecting access to data and information, simplifying deployment and identity infrastructure management, as well as providing safer access to data including configuring some key Active Directory functions, such as domain services in Active Directory (AD DS), group policies, Dynamic Access Control (DAC), work folders, onboarding, certification services, Rights Management Services (RMS), federation services, as well as integrating local environment with cloud-based technologies, such as Windows Azure Active Directory. The course is especially intended for IT technology specialists, who are experienced in Active Directory Domain Services (AD DS) and seek one and only course thanks to which they could further expand their knowledge and skills using the technology of access and information protection in Windows Server 2012 and Windows Server 2012 R2. Target audience of the course are AD DS administrators, who would like to further develop their skills from the latest access and information protection in Windows Server 2012 and Windows Server 2012 R2, system or infrastructure administrators with general expertise in AD DS, who would like to use their fundamental knowledge and move to more advanced Active Directory technologies in Windows Server 2012 and Windows Server 2012 R2, IT specialists, who participated in: MS 10967: Fundamentals of a Windows Server Infrastructure course.



Benefits of completing the training

Acquiring knowledge and practical skills from Active Directory domain services management in Windows Server 2012R2. This includes:

- Available solutions to identity management.
- Deploying and administering AD DS in Windows Server 2012.
- Secure AD DS deployment.
- Deploying and configuring AD DS locations, as well as replication management.

- Deploying and managing group policies.
- Managing user settings with group policies.
- Implementing CA hierarchy with AD CS services and CA management methods.
- Deploying and managing certificates.
- Deploying and managing AD RMS.
- Deploying and managing AD FS services.
- Securing and providing access to data with technologies such as Dynamic Access Control, working folders and onboarding.
- Monitoring, troubleshooting processes and providing AD DS. service operation continuity.
- Implementing Windows Azure Active Directory.
- Deploying and managing Active Directory Lightweight Directory Services (AD LDS).



Expected Listener Preparation

Minimal level:

- Experience in working with Active Directory Domain Services (AD DS), experience in working with corporate Windows Server Infrastructure environment, experience in working with fundamental network infrastructure technologies and troubleshooting, such as name detection, IP addressing, Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP), experience in working with Hyper-V and server virtualization concepts, awareness and understanding general security best practices, experience in working with Windows Client operational systems, such as Windows 7, Windows 8 and Windows 10.

Expected level:

- Participants should have at least 2 years of experience in IT industry or more, and participating in courses related to Windows Server 2008 or 2012, or equivalent knowledge is recommended. Solid, practical understanding of network fundamentals including TCP/IP, User Datagram Protocol (UDP) and Domain Name System (DNS), excellent, practical comprehension of Active Directory Domain Services (AD DS) principles, very good, practical understanding of Microsoft Hyper-V virtualization fundamentals, understanding the rules of Windows Server security, and an ability to use PowerShell commands.

An ability to use materials in English.

To make your work more convenient and training more effective, we suggest using an additional screen. Lack of such screen does not exclude participation in the training, however it significantly influences

working comfort during classes.

You can find information and requirements of participation in Distance Learning trainings at:

<https://www.altkomakademia.pl/distance-learning/#FAQ>



Training Language

- **Training:** English
- **Materials:** English



Training Includes

- Electronic materials available at: <https://www.altkomakademia.pl/>
- Access to Altkom Akademia student portal



Duration

5 days / 35 hours

Training agenda

1. Review of access and information protection
 - Introduction to solutions from information access and protection in business
 - Discussing AIP solutions in Windows Server 2012
 - Review of FIM 2010 R2
2. Advanced AD DS deployment and administration.
 - AD DS. deployment
 - Deploying and cloning domain virtual controllers
 - Deploying domain controllers in Windows Azure
 - AD DS administration
3. Securing AD DS
 - Securing domain controllers

- Deploying accounts security
- Deploying control authentication
- 4. Deploying and administering AD DS. locations and replication
 - Discussing AD DS. replication
 - Configuring AD DS. websites
 - Configuring and monitoring AD DS replication
- 5. Deploying group policies
 - Introduction to group policies
 - Deploying and administering GPO objects
 - Scope and processing group policies
 - Troubleshooting with group policies objects appliance
- 6. Managing user settings with group policies
 - Deploying administration templates
 - Configuring folder and script redirection
 - Configuring preferences of group policies
- 7. Deploying and managing AD CS services
 - Deploying CAs
 - Administering CAs
 - Troubleshooting CAs maintenance and monitoring
- 8. Deploying and managing certificates
 - Using certificates in business environment
 - Deploying and managing certificate templates
 - Managing deployment, annulment and recovery of certificates
 - Deploying and managing intelligent cards
- 9. Deploying and managing AD RMS
 - Discussing AD RMS
 - Deploying and implementing AD RMS infrastructure
 - Configuring content protection
 - Configuring external access to AD RMS
 - Wdrażanie i zarządzanie usługami AD FS
 - Discussing AD FS services
 - Deploying AD FS services
 - Implementing AD FS for single organisation
 - Deploying AD FS services in federation scenario between companies
 - Expanding AD FS services to external Clients
- 10. Deploying secure access to shared file
 - Review of Dynamic Access Control
 - Deploying DAC components

- Deploying DAC to access control
 - Deploying Access Denied Assistance
 - Deploying and managing working folders
 - Onboarding deployment
11. Monitoring, managing and AD DS. recovery.
- Monitoring AD DS
 - AD DS database management.
 - Back-up and AD DS recovery options, as well as other identity and access solutions
12. Implementing Windows Azure Active Directory
- Discussing Windows Azure AD
 - Managing Windows Azure AD accounts
13. Deploying and managing AD LDS
- Review of AD LDS
 - Deploying AD LDS services
 - Configuring AD LDS instances and partitions
 - Configuring AD LDS service replication
 - Integrating AD LDS with AD DS