Master Class: Active Directory Deep Dive – Installation, Configuration and Operation (SADDD-L0)

ID SADDD-L0 **Prix** CHF 5 900,– (Hors Taxe) **Durée** 5 jours

A qui s'adresse cette formation

This course is intended for (prospective) system administrators, consultants and Active Directory designers. After this seminar you will be able to design, implement, support and consult Active Directory.

Pré-requis

At least 2 ***years*** experience with Microsoft servers **and** client systems

Objectifs

This master class course will focus on Active Directory.

From getting started, to history, to troubleshooting, everything is learned in this course.

The environment is built independently by each participant live in the course and runs in a highly secure data center in Helsinki on their own hardware.

Highly responsive training environments paired with the best trainers and consultants available in the Schengen area: THIS is our MasterClass Active Directory

Active Directory offers a high potential target for cyberattacks in your organization, so with this training, we'll help you understand, maintain, and properly administer this environment.

Contenu

Active Directory Overview

- Active Directory structures: logical (forest, domain, and organizational unit) and physical (Active Directory sites, subnets, and site connections)
- Multimaster replication of the AD database
- Trust Relationship incl. PIM Trust
- Name contexts of the AD database
- Active Directory objects and their attributes
- Distinguished Names und GUIDs
- sAMAccountName und userPrincipalName
- Operation master / Flexible single master oparations (FSMO) and global catalog server
- Product history from Active Directory 2000 to Active Directory 2022 (what was added when)
- Active Directory Limitierungen
- Windows Admin Center (WAC) mit Active Directory Extension

Active Directory Administration

- Overview of administrative boundaries and delegation options
- SACL / DACL - permissions in Active Directory and their inheritance
- Extended rights / property sets / validated writes
- Delegation of administrative tasks in Active Directory
- Implementing an Enhanced Security Administrative Environment (ESAE) structure
- Fine grainted password policies (FGPP)
- Active Directory Monitoring

Powershell für Active Directory

- Powershell-Versionen
- Powershell basics (Get-Help / Get-Command / GetMember)
- Keyboard shortcuts for Powershell
- Powershell-Variablen, -Aliase und -Pipelining
- Powershell-Profile
- Active Directory Web Services
- Powershell-Scripting für Active Directory

Active Directory Security Check und Health Check

- Secure Channel Check (unicodepwd / ntpwdhistory)
- Measures against golden tickets and silver tickets
- Securely and reliably disable RC4 encryption for Kerberos
- Implement tiering model according to ESAE
- "LAPS" for Domain Controller via own Powershell script

- Prevent misuse of system processes
- Default privileges correction
- Active Directory „Clean-up“
- Check Active Directory replication (repadmin.exe / dcdiag.exe)
- Documentation of the actual environment

Active Directory schema extension and domainprep

- Structure of the Active Directory schema
- Schema objects, object classes and attributes
- Inheritance in Active Directory Schema
- Object Identifier (OID)
- Rule for structure and content
- Schema Master
- Correct manual schema extension with custom attributes and classes
- Schema extension for Active Directory 2022
- Domainprep für Active Directory 2022

Domain Controller Locator

- Domain Controller Locator Typen
- Domain Controller stickyness prevention
- Nearest Domain Controller
- DNS priority vs. DNS weighting of SRV records
- Default Site Coverage vs. Manual Site Coverage (Hub/Spoke)
- Influence on the locator service (relieve, make unattractive and hide domain controllers)
- Netlogon debugging - why does my domain member end up at this domain controller?

Deployment von Active Directory Domain Controllern

- Installation of the role (GUI and Windows Powershell)
- Promoting a Domain Controller on Windows Server 2022 via GUI and as Server Core
- Examine the four possible transition paths
- Transition path 1: Substituting migration (new name + same IP)
- Transition path 2: Substitution migration (new name + new IP)
- Transition path 3: Replacement migration (same name + same IP)
- Transition path 4: Consolidating migration (RODCs instead of RWDCs)

Read-Only Domain Controller (RODC)

- Fields of application of a RODC
- Password replication policy
- Credentials caching
- RODC filtered attribute set
- Installation of a RODC (GUI + Windows Powershell)
- Assigning an RODC to Tier 1
- Domain Join over RODC (djoin.exe)
- RODC as DC reverse proxy (protection of RWDCs)

Active Directory and the Domain Name System (DNS)

- Overview of the interaction between ADS and DNS
- DNS namespace, DNS servers and DNS clients (resolvers)
- Installing the DNS role via GUI and Windows Powershell
- Manage DNS zones
- Replication of AD-integrated zones
- Set up DNS aging in interaction with DHCP
- Global Query Block List, Global Name Zones und Query Resolution Policies

Advanced Site Management

- Replication architecture
- Replication topology
- Knowledge consistency checker (KCC)
- nTDSDSA und invocationID
- Urgent replication und immediately replication
- Intra-Site Replication vs. Inter-Site Replication
- Reduce replication latency intra-site and inter-site

LDAP-Query

- Introduction to the LDAP protocol
- ADSI / Search in ADS via TCP 389 / TCP 636
- Searchflags / Systemflags / SchemaFlagsEx
- List Object Mode (LOM)
- Domain Controller LDAP-Query-Policy
- Active Directory Web Services Config
- Tracking LDAP-Searches on Domain Controllers
- Hardening LDAP Channel Binding

Replication Internals

- Replication Meta Data
- nTDSDSA-GUID vs. InvocationID
- Up-to-dateness-vector und High-Watermark
- Replication conflicts
- Linked Value Replication
- SYSVOL Replication

Active Directory Forest Functional Level 2016

- Moving the operation masters incl. operation master failure
- Optimize the DNS servers
- Replacing the last old domain controller
- 2016 Domain Functional Level
- 2016 Forest Functional Level
- Set up and use Privilege Access Management feature

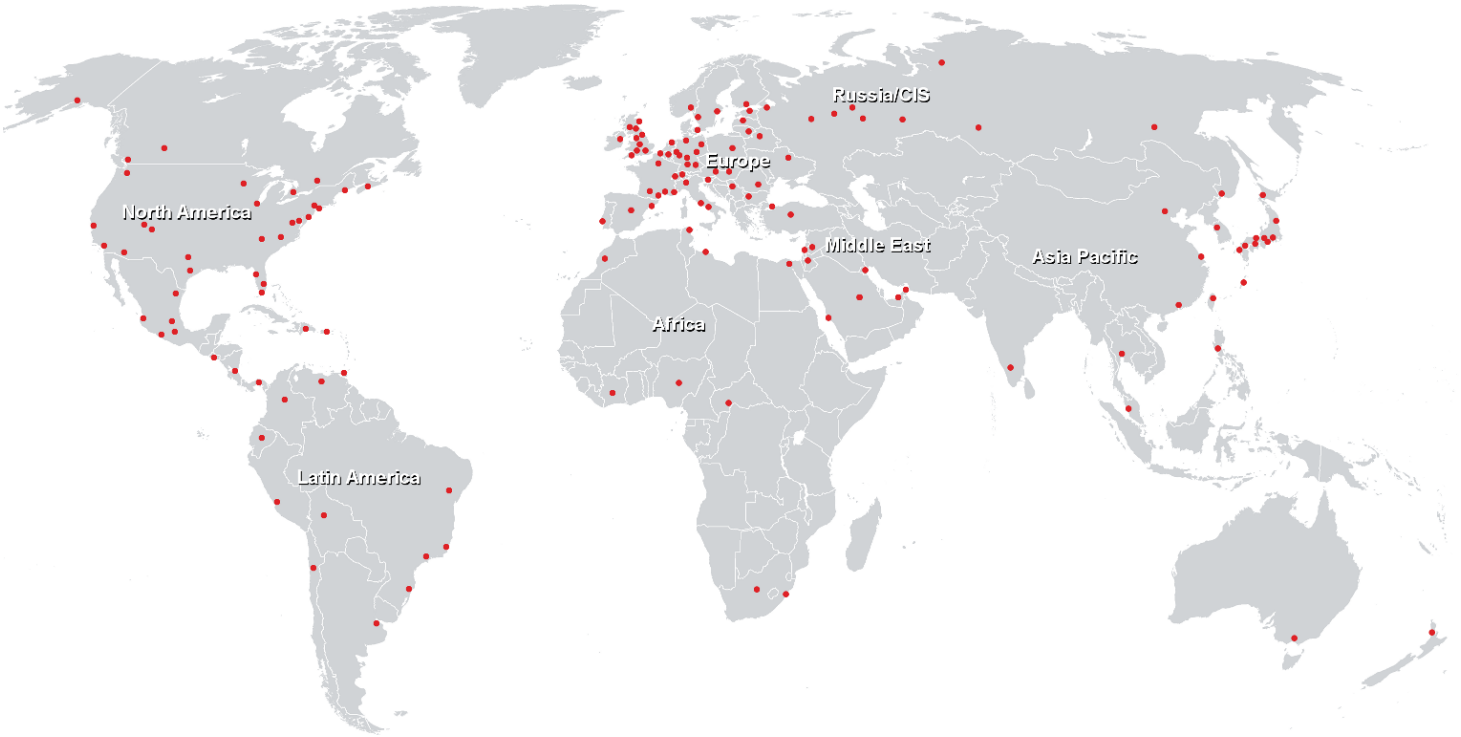
Master Class: Active Directory Deep Dive – Installation, Configuration and Operation (SADDD-L0)

Active Directory Backup und Restore

- Requirements for the backup - installation of the role via GUI and Windows Powershell
- Backup types for Active Directory
- Policies for securing Active Directory
- Latency intervals for Active Directory backup (daily vs. 89 days)
- Schedule, set up, and deploy scheduled tasks for Active Directory backup using Windows Powershell.
- Sichern des Active Directory
- Restore Active Directory (BMR)
- Restore Internals
- Restore process if the backup is older than 60 days
- Questions from the participants

Master Class: Active Directory Deep Dive – Installation, Configuration and Operation (SADDD-L0)

Centres de formation dans le monde entier





Fast Lane Institute for Knowledge Transfer (Switzerland) AG

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, https://www.flane.ch