

Essential Active Directory 2022 Workshop –
ausführliche Informationen

Inhalt

1.	ÜBERSICHT	2
2.	DETAILS	3
3.	KURSinHALTE	6
4.	BILDERGALLERIE AUS DEN UNTERLAGEN.....	12

1. Übersicht

Das Augenmerk des Kurses Active Directory 2022 liegt in der Bereinigung, Optimierung und Transition eines historisch gewachsenen Active Directory auf Domain Controller mit dem Betriebssystem Windows Server 2022. Das Bereinigen umfasst die Implementierung eines ESAE (Enhanced Security Administrative Environment)-konformen Betriebs des Active Directory, sowie das Entfernen obsoleter Altstrukturen.

Durch die Optimierung des Active Directory werden veraltete Verschlüsselungsprotokolle sicher entfernt und die Latenz für den Datenabgleich zwischen den Domain Controllern auf ein zeitgemäßes Niveau verkürzt. Mit der Transition werden alle vier Möglichkeiten beleuchtet die veralteten Domain Controller durch neue Domain Controller abzulösen, wobei sowohl Read-Write Domain Controller wie auch Read-Only Domain Controller eingesetzt werden. Der praxisnahe Einsatz von einem ESAE-konformen Active Directory im Zusammenspiel mit einem belastbaren Szenario für Backup und Restore bieten verlässliche reaktive Maßnahmen im Falle einer Konfrontation mit Ransomware.

Ein bereinigtes, gehärtetes, aufgeräumtes und sauber überführtes Active Directory bietet dann eine gute Position den sicheren Weiterbetrieb des Active Directory zu gewährleisten. Ein solch vorbereitetes Active Directory ist der perfekte Grundstein die Identitäten in Richtung AzureActive Directory durch eine Hybridstellung zu bewegen.

2. Details

Die Themen des Active Directory 2022 Kurses sind wie folgt:

- Überblick über die Active Directory Familie (Active Directory DOMAIN SERVICES, Active Directory LIGHTWEIGHT DOMAIN SERVICES, Active Directory FEDERATION SERVICES, Active Directory CERTIFICATE SERVICES) und deren historische Entwicklung
- Active Directory Administration – Delegation von administrativen Aufgaben
- Windows Powershell für Active Directory (Automatisierung von Routineaufgaben)
- Active Directory Healthcheck und Bestandsaufnahme des bestehenden Active Directory: Bereinigung, Absichern und Vorbereitung zur Transition auf Active Directory mit Server 2022
- Manuelle Schemaerweiterung und die Schemaerweiterung für Active
- Domain Controller Locator – Einfluss und Steuerung wie ein DC von Windows Clients gefunden wird.
- Installation von Read-Write Domain Controllern (RWDC) unter Server 2022 (mit grafischer Oberfläche oder wahlweise auch als Core)
- Installation von Read-Only Domain Controllern (RODC) unter Server 2022 (mit grafischer Oberfläche oder wahlweise auch als Core)
- Active Directory integriertes DNS – Replikation und Berechtigungen, sowie der Einfluss von DHCP auf das DNS
- Advanced Site Management – Mechanismen der Replikation und wie man die Replikationsgeschwindigkeit steigert.
- LDAP- und ADWS-Schnittstelle, LDAP- und ADWS-Abfragen, Limitierungen und Debugging
- DC Replication Internals – wie genau werden die Datenbank und das SYSVOL abgeglichen?
- Active Directory Domain und Forest Functional Levels – finales Erreichen von Domain Functional Level 2016 und Forest Functional Level 2016.
- Backup und Restore von Active Directory – wann und wie oft sichern? Wann ein AD-Restore?

In diesem Kurs stehen der Weiterbetrieb eines historisch gewachsenen Active Directory Forests und die Migration von älteren Versionen (Server 2012 R2 / Server 2016) sowie die Verwaltung von Active Directory im Vordergrund. Nach diesem Kurs sollten die Teilnehmer in der Lage sein, sowohl ein organisch entwickeltes Konvolut an Active Directory Forests verwalten zu können. Sie sind auch sensibilisiert auf die Sicherheitslücken von Active Directory und können grundlegende Sicherheitsmaßnahmen treffen, diesen Sicherheitslücken professionell zu begegnen.

Gleich zum Kursbeginn (Healthcheck) geben wir Ihnen einen tiefen Einblick in die aktuellen Sicherheitslücken von Active Directory und Kerberos im speziellen und die dadurch entstandenen Gefahren durch Golden Ticket / Silver Ticket. Diese Gefahr zwingt alle Administratoren dazu umzudenken und die neuen Sicherheitsfeatures ab Active Directory 2016 (Bastion Forest, Privileged Access Management (PAM), Timebased Group Membership) einzusetzen. Clientseitig tragen neue Sicherheitsmaßnahmen von Windows 10 Enterprise wie Virtualized Based Security (VBS) mit Credential Guard und Device Guard massiv dazu bei, den unerlaubten Zugang zu den "Credentials" im LSA (Local Security Authority) Cache zu unterbinden. Um aber diese Sicherheitslücken von Kerberos in Active Directory zu erkennen, zeigen wir im Kurs wie schnell ein Hacker Kerberos Golden Ticket und Silver Ticket mit falscher

Identität erzeugen kann. Diese Sicherheitslücken können im Moment nur durch den Einsatz von neuen Windows 10 Enterprise und Features ab Windows Server 2016 wie Credential Guard, Remote Credential Guard, Attack Surface Reduction und Sicherheitsmaßnahmen wie ESAE (Enhance Security Administration Environment), PAW (Privileged Access Workstation) weitgehend verhindert werden.

Die Realisierung dieser Sicherheitsmaßnahmen erfordert die Einführung eines ESAE-konformen Betrieb des Active Directory, wird unterstützt durch rollierende Kennwörter von den krbtgt-Konten und dem Abschalten von schwachen Authentifizierungsverfahren wie LM und NTLMv1. Ebenso wird im Kurs die sichere und zuverlässige Abschaltung der RC4-Verschlüsselung im Protokoll Kerberos V5 realisiert.

Anhand des bestehenden 2012 R2-Forests wird zuerst die Grundlage vermittelt und aufgefrischt. Dazu gehören die Aufgaben von Global Catalog Server, der 5 x FSMO (Flexible Single Master Operation) im Forest, der Replikation von SYSVOL innerhalb der Domäne und die DC-Replikation zwischen den verschiedenen Active Directory Sites. Dabei wird versucht, wenn es möglich ist, immer PowerShell einzusetzen. Die Verwaltung von Active Directory hier im Kurs hat weniger den Fokus auf dem Tagesgeschäft (Benutzer, Computer und Gruppen zu verwalten), sondern geht in die Tiefe des Verzeichnisdienstes.

Sie lernen, welche Berechtigungen es im Active Directory gibt und wie man diese beeinflussen kann. Neben den Berechtigungen gilt es auch zu untersuchen, wie man effizient den Verzeichnisdienst per LDAP befragen kann, wie man eigene Abfragerichtlinien etabliert und - natürlich - prüft: Wer fragt meine DCs was und wie viel CPU-Zeit kostet das. Spezielle LDAP-Suche nach Objekten und Attributen wie z.B. Bitwise AND/OR, SearchFlags, systemFlags etc. werden praktiziert. Auch die sog. LDAP Query Policy kann die Performance und Sicherheit der DC beeinflussen. Mit dem LOM (List Object Mode) ist es möglich, AD-Objekte vor LDAP-Abfrage zu verstecken, sodass nur autorisierte Personen diese finden können.

Vor der Migration auf neue DCs müssen Vorkehrungen getroffen werden. Dazu gehört unter anderem das Verständnis für den Domain Controller Locator Prozess (wie finden Memberserver und -workstations einen Domain Controller). Abgeschlossen wird der zweite Block durch etwas Aufräumen im Verzeichnisdienst und dem Optimieren und Schützen des DNS-Dienstes zur Vorbereitung der Migration. Um die Installation von Windows Server 2022 einzuleiten, müssen Veränderungen am Active Directory Schema und an den jeweiligen Domain Partition vorgenommen werden. Die Problematik liegt hierbei in der irreversiblen Veränderung (vgl. Schemaerweiterung) und in der Umkehrbarkeit des Domain Preps. Ebenso wird der Einsatz von RODCs in einer ESAE-Konformen (T1) Umgebung durchgeführt.

Damit die vielen anschließenden Praxisübungen effizient abgewickelt werden können, ist gleich vorweg ein Kernmodul die Windows Powershell. Die Windows Powershell wird im Kurs ab der Version 5.x eingesetzt, um auch größere Strukturen programmatisch administrieren zu können. Besondere Aufmerksamkeit wird in diesem Kapitel auf das Erstellen von eigenen PowerShell-Skripten und PowerShell-Modulen mit Visual Studio Code gelegt.

Der eigentlichen Migration des Active Directory auf Domain Controller mit dem Betriebssystem 2022 werden alle möglichen Migrationsszenarien in praxisgerechten Übungen durchlebt:

- Substituierende Migration (neue DC-Namen + gleiche IPv4-Adressen)
- Substituierende Migration (neue DC-Name + neue IPv4-Adressen)
- Ablösende Migration (gleiche DC-Namen + gleiche IPv4-Adressen)
- Konsolidierende Migration (Abbau von RWDCs und Aufbau von RODCs)

In jedem der vier Szenarien wird viel Aufmerksamkeit und Energie in die Automatisierung über die Windows PowerShell gelegt. Bestandteil von den Active Directory Workshop sind eigens entwickelte PowerShell-Skripte (derzeit über 60 Skripte - die Sie selbstverständlich mitnehmen dürfen – zum Beispiel ein vollautomatisiertes Deployment von Domain Controllern aus einem SYSPREP-Images heraus), welche Ihnen viele Routinearbeiten im Tagesgeschäft erleichtern.

Die Sicherung von Active Directory wie auch der Restore-Prozess sind natürlich Bestandteil des Kurses. Hier erlernen Sie, wie Sie effizient das Active Directory sichern können, welche Intervalle zu wählen sind und wie viele Domain Controller gesichert werden müssen. Die Restore-Prozesse umfassen die Nicht-Autorisierende und die Autorisierende Wiederherstellung (sollten ganze Strukturen im Active Directory versehentlich gelöscht worden sein). Besonderes Augenmerk wird zusätzlich auf den Domain Controller Secure Channel gesetzt und wie man dieses bei Domain Controllern reparieren kann.

3. Kursinhalte

Active Directory Überblick

- Active Directory Strukturen: logisch (Forest, Domäne und Organisationseinheit) und physisch (Active Directory Standorte, Subnetze und Standortverbindungen)
- Multimaster-Replikation der AD-Datenbank
- Vertrauensstellungen (Trust-Relationship) inkl. PIM-Trust
- Nameskontexte der AD-Datenbank
- Active Directory Objekte und deren Attribute
- Distinguished Names und GUIDs
- sAMAccountName und userPrincipalName
- Betriebsmaster / Flexible single master operations (FSMO) und globaler Katalogserver
- Produktgeschichte von Active Directory 2000 bis zu Active Directory 2022 (was kam wann dazu)
- Active Directory Limitierungen
- Windows Admin Center (WAC) mit Active Directory Extension

Active Directory Administration

- Überblick über administrative Grenzen und Delegationsmöglichkeiten
- SACL / DACL – Berechtigungen im Active Directory und deren Vererbung
- Extended rights / property sets / validated writes
- Delegation von administrativen Aufgaben im Active Directory
- Implementieren einer ESAE-Struktur (Enhanced Security Administrative Environment)
- Fine grained password policies (FGPP)
- Active Directory Überwachung

Powershell für Active Directory

- Powershell-Versionen
- Powershell-Grundlagen (Get-Help / Get-Command / Get-Member)
- Keyboard-Shortcuts für die 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)
- Maßnahmen gegen golden Tickets und silver Tickets
- RC4-Verschlüsselung bei Kerberos sicher und zuverlässig abschalten
- Tiering-Modell implementieren nach ESAE
- „LAPS“ für Domain Controller per eigenem Powershell-Skript
- Missbrauch von Systemprozessen unterbinden
- Korrektur der Default-Privilegien
- Active Directory „Clean-up“
- Active Directory Replikation prüfen (repadmin.exe / dcdiag.exe)
- Dokumentation der Ist-Umgebung

Active Directory Schemaerweiterung und Domainprep

- Aufbau des Active Directory Schema
- Schemaobjekte, Objektklassen und Attribute
- Vererbung im Active Directory Schema
- Object Identifier (OID)
- Regel für Struktur und Inhalt
- Schema-Master
- Korrekte manuelle Schemaerweiterung mit eigenen Attributen und Klassen
- Schemaerweiterung für Active Directory 2022
- Domainprep für Active Directory 2022

Domain Controller Locator

- Domain Controller Locator Typen
- Domain Controller stickyness prevention
- Nearest Domain Controller
- DNS-Priorität vs. DNS-Gewichtung der SRV-Einträge
- Default Site Coverage vs. Manuelle Standortabdeckung (Hub/Spoke)
- Einflussnahme auf den Locator Service (entlasten, unattraktiv gestalten und verstecken von Domain Controllern)
- Netlogon-Debugging – warum landet mein Domain Member bei diesem Domain Controller

Deployment von Active Directory Domain Controllern

- Installation der Rolle (GUI und Windows Powershell)
- Promoten eines Domain Controllers unter Windows Server 2022 per GUI und als Server Core
- Untersuchen der vier möglichen Transitionswege
- Transitionsweg 1: Substituierende Migration (neuer Name + gleiche IP)
- Transitionsweg 2: Substituierende Migration (neuer Name + neue IP)
- Transitionsweg 3: Ablösende Migration (gleicher Name + gleiche IP)
- Transitionsweg 4: Konsolidierende Migration (RODCs anstelle von RWDCs)

Read-Only Domain Controller (RODC)

- Einsatzgebiete eines RODC
- Password replication policy
- Credentials caching
- RODC filtered attribute set
- Installation eines RODC (GUI + Windows Powershell)
- Zuweisen eines RODC zum Tier 1
- Domain Join over RODC (djoin.exe)
- RODC als DC-Reverse-Proxy (Schutz der RWDCs)

Active Directory und das Domain Name System (DNS)

- Überblick über das Zusammenspiel von ADS und DNS
- DNS-Namespace, DNS-Server und DNS-Clients (Resolver)
- Installation der DNS-Rolle per GUI und Windows Powershell
- Verwalten von DNS-Zonen
- Replikation von AD-integrierten Zonen
- DNS-Alterung einrichten im Zusammenspiel mit DHCP
- Global Query Block List, Global Name Zones und Query Resolution Policies

Advanced Site Management

- Architektur der Replikation
- Replikationstopologie
- Knowledge consistency checker (KCC)
- nTDSDSA und invocationID
- Urgent replication und immediately replication
- Intra-Site Replication vs. Inter-Site Replication
- Verkürzen der Replikationslatenz Intra-Site und Inter-Site

LDAP-Query

- Einführung in das LDAP-Protokoll
- ADSI / Suchen im 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
- Replikationskonflikte
- Linked Value Replication
- SYSVOL-Replikation

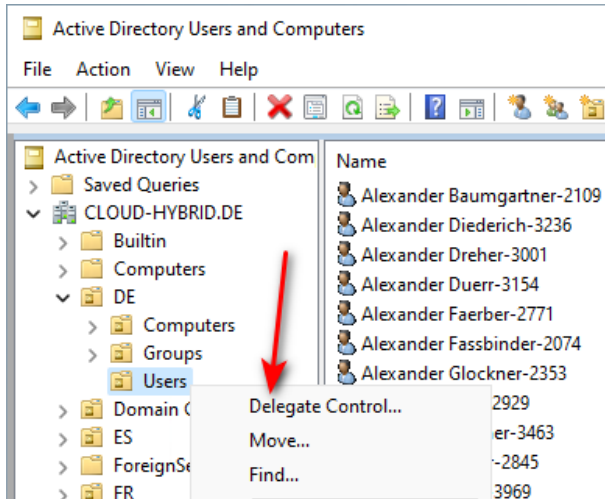
Active Directory Forest Functional Level 2016

- Bewegen der Betriebsmaster inkl. Betriebsmasterausfall
- Optimieren der DNS-Server
- Ablösen der letzten alten Domain Controller
- 2016 Domain Functional Level
- 2016 Forest Functional Level
- Privilege Access Management Feature einrichten und verwenden

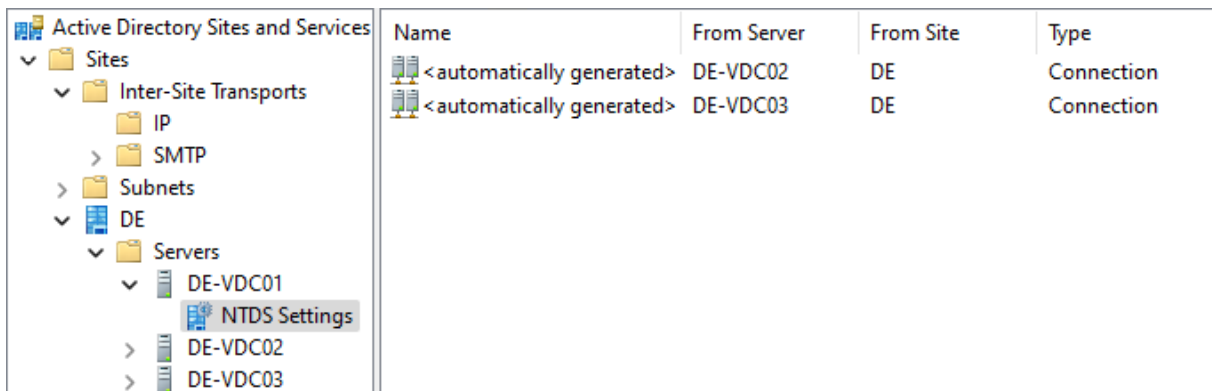
Active Directory Backup und Restore

- Voraussetzungen für das Backup – Installation der Rolle per GUI und Windows Powershell
- Sicherungsarten für Active Directory
- Richtlinien zur Sicherung von Active Directory
- Latenzintervalle bei der Sicherung von Active Directory (täglich vs. 89 Tage)
- Planen, einrichten und verteilen der Scheduled-Tasks für die Sicherung von Active Directory mit der Windows Powershell
- Sichern des Active Directory
- Wiederherstellen des Active Directory (BMR)
- Restore-Internals
- Restore-Prozess, wenn die Sicherung älter als 60 Tage ist

4. Bildergalerie aus den Unterlagen



Delegate Control – delegieren von Aufgaben



Sites and Services – der KCC hat gerechnet

```

Administrator: PowerShell
Type 'help' to get help.
PS C:\Users\administrator.CH> Get-ADOptionalFeature -Filter *

DistinguishedName : CN=Recycle Bin Feature,CN=Optional Features,CN=Directory Service,CN=Windows
NT,CN=Services,CN=Configuration,DC=CLOUD-HYBRID,DC=DE
EnabledScopes      : {}
FeatureGUID        : 766ddcd8-acd0-445e-f3b9-a7f9b6744f2a
FeatureScope       : {ForestOrConfigurationSet}
IsDisableable      : False
Name               : Recycle Bin Feature
ObjectClass        : msDS-OptionalFeature
ObjectGUID         : ec55bedc-6aef-4ba4-ad2b-be5654521447
RequiredDomainMode : Windows2008R2Forest

DistinguishedName : CN=Privileged Access Management Feature,CN=Optional Features,CN=Directory Service,CN=Windows
NT,CN=Services,CN=Configuration,DC=CLOUD-HYBRID,DC=DE
EnabledScopes      : {}
FeatureGUID        : ec43e873-cc88-4640-b4ab-07ffe4ab5bcd
FeatureScope       : {ForestOrConfigurationSet}
IsDisableable      : False
Name               : Privileged Access Management Feature
ObjectClass        : msDS-OptionalFeature
ObjectGUID         : 6d94b472-58c0-477c-990e-68baf07bc094
RequiredDomainMode : Windows2016Forest
RequiredForestMode : Windows2016Forest
  
```

Active Directory PAM-Feature

```

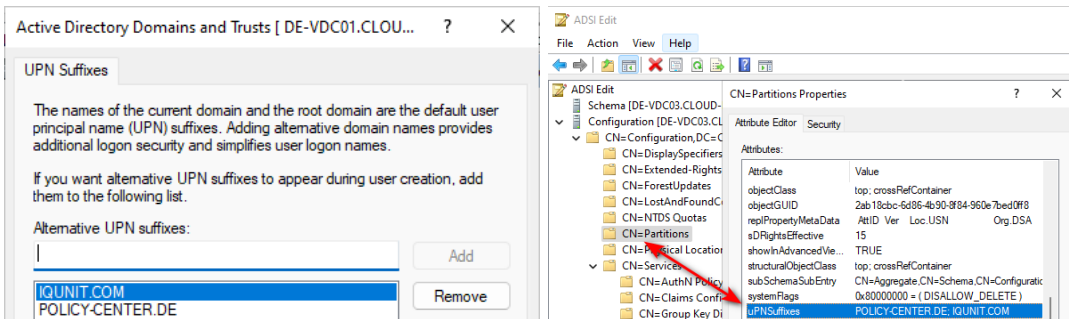
Administrator: PowerShell
PowerShell 7.2.6
Copyright (c) Microsoft Corporation.

https://aka.ms/powershell
Type 'help' to get help.

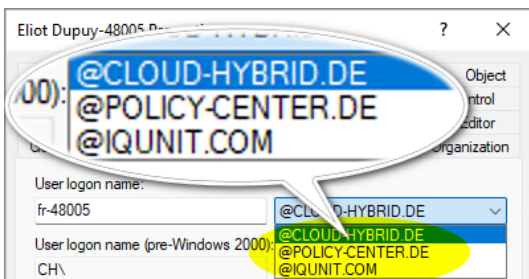
PS C:\Users\administrator.CH> Get-ADComputer -Filter { name -like "DE-*" } | Select-Object -Property Name, ObjectGUID

Name                ObjectGUID
-----
DE-VDC03            ea1e7a2c-c93c-4e19-a1b9-670543c467c7
DE-VDC01            3f0323d9-4ff5-46ce-9e29-26e4d2f4e523
DE-VDC02            fffd41c9-a7c9-4987-bf00-2bb21ccd8577
DE-VSUBCA01        83b5602a-7bdf-4a0f-9f39-148434770f95
DE-VWAC01            4857c2bf-6640-438c-a41e-2656e2bb4b76
DE-VDHCP01         2d3a1c7b-ec6e-446e-ba28-bc4ba6a7a14f
DE-VDHCP02         aad32fa9-ab4c-463b-9ba2-f39c90382ad8
DE-VWK01            15c402b4-6451-41bb-a25e-93f462cff96a
  
```

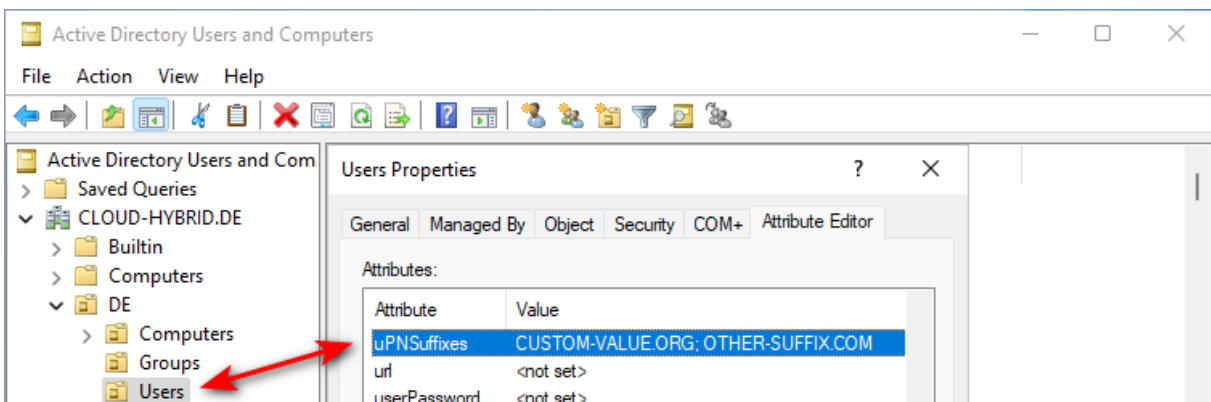
Global Unique Identifier – GUID



The image shows two windows from Active Directory. The left window, 'Active Directory Domains and Trusts', displays the 'UPN Suffixes' tab with a list containing 'IQUNIT.COM' and 'POLICY-CENTER.DE'. The right window, 'ADSI Edit', shows the 'CN=Partitions Properties' for the 'CN=Partitions' container, with a table of attributes including 'uPNSuffixes' set to 'POLICY-CENTER.DE; IQUNIT.COM'.



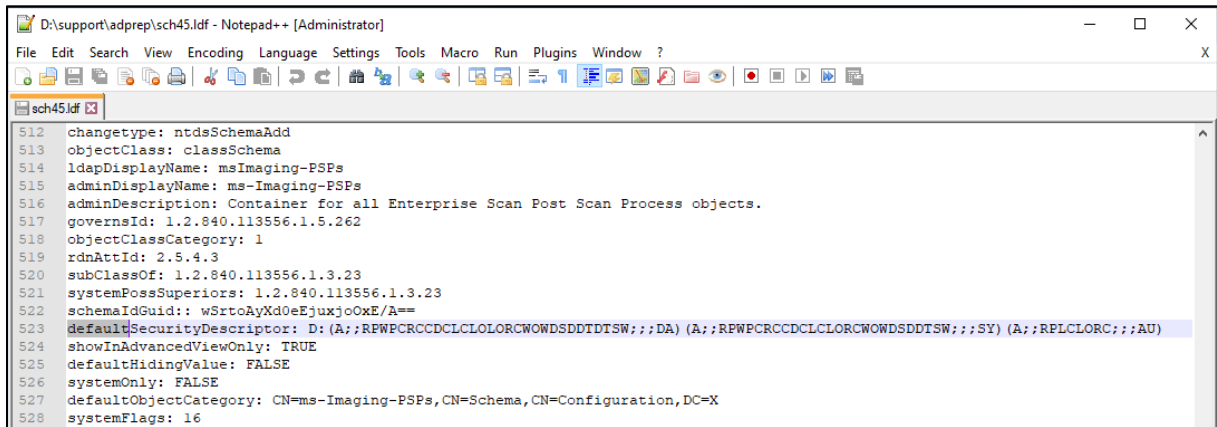
The image shows a user object 'Eliot Dupuy-48005' in Active Directory. A callout bubble highlights the user's principal name and lists the UPN suffixes: '@CLOUD-HYBRID.DE', '@POLICY-CENTER.DE', and '@IQUNIT.COM'. The user's logon name is 'fr-48005'.



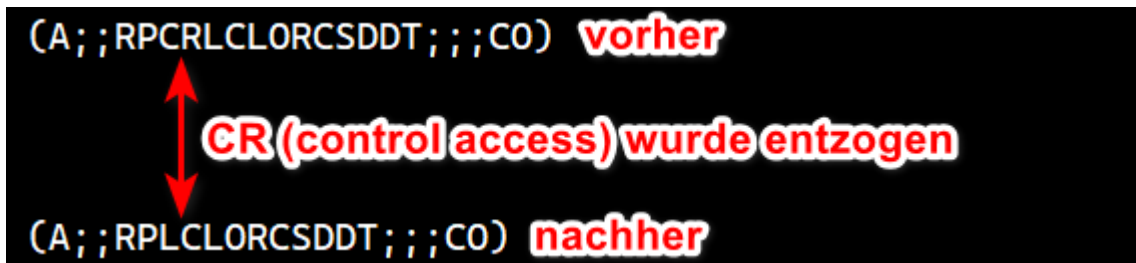
The image shows the 'Active Directory Users and Computers' console. The 'Users Properties' dialog box is open, showing the 'Attribute Editor' tab. The 'uPNSuffixes' attribute is highlighted, with a value of 'CUSTOM-VALUE.ORG; OTHER-SUFFIX.COM'. A red arrow points from the 'Users' folder in the console to the dialog box.



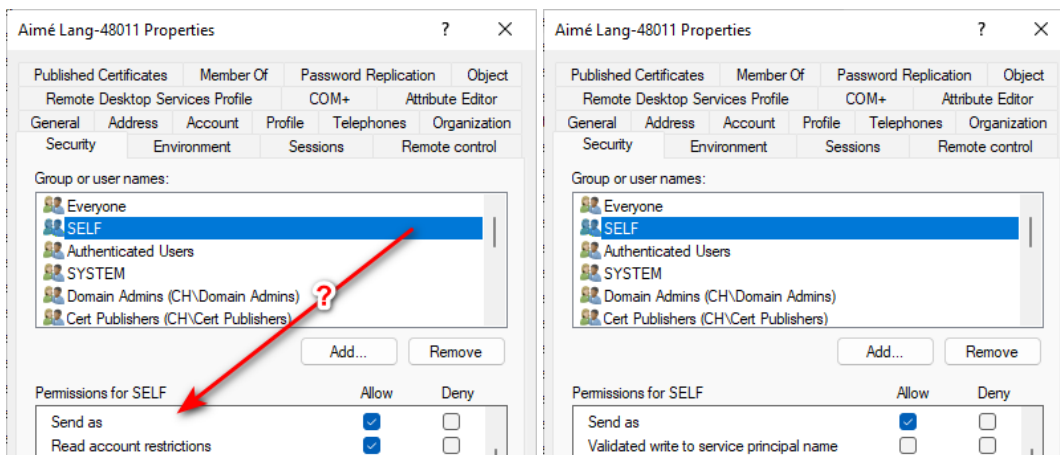
Suffixe der User Principal Names



SDDL – Default Security in einer Schema.ldf-Datei



SDDL-Anpassungen wegen LAPS



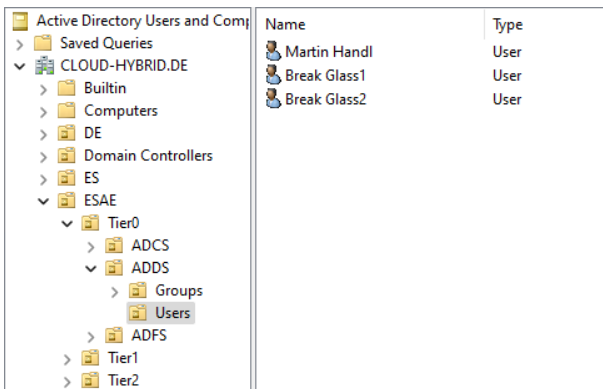
Veränderungen an der Anzeige im Reiter Security / Sicherheit

```

Administrator: PowerShell
PS C:\> ConvertFrom-SddlString -Sddl (Get-Acl -Path C:\SetupTemp\).sddl

Owner          : BUILTIN\Administrators
Group          :
DiscretionaryAcl : {BUILTIN\Administrators: AccessAllowed Inherited (ChangePermissions, CreateDirectories, Delete, DeleteSubdirectoriesAndFiles, ExecuteKey, FullControl, FullControl, FullControl, FullControl, GenericAll, GenericExecute, GenericRead, GenericWrite, ListDirectory, Modify, Read, ReadAndExecute, ReadAttributes, ReadExtendedAttributes, ReadPermissions, Synchronize, TakeOwnership, Traverse, Write, WriteAttributes, WriteData, WriteExtendedAttributes, WriteKey), NT AUTHORITY\SYSTEM: AccessAllowed Inherited (ChangePermissions, CreateDirectories, Delete, DeleteSubdirectoriesAndFiles, ExecuteKey, FullControl, FullControl, FullControl, FullControl, GenericAll, GenericExecute, GenericRead, GenericWrite, ListDirectory, Modify, Read, ReadAndExecute, ReadAttributes, ReadExtendedAttributes, ReadPermissions, Synchronize, TakeOwnership, Traverse, Write, WriteAttributes, WriteData, WriteExtendedAttributes, WriteKey), BUILTIN\Users: AccessAllowed Inherited (GenericWrite, ListDirectory, Read, ReadAndExecute, ReadAttributes, ReadExtendedAttributes, ReadPermissions, Synchronize, Traverse), NT AUTHORITY\Authenticated Users: AccessAllowed Inherited (CreateDirectories, Delete, ExecuteKey, GenericExecute, GenericRead, GenericWrite, ListDirectory, Modify, Read, ReadAndExecute, ReadAttributes, ReadExtendedAttributes, ReadPermissions, Synchronize, Traverse, Write, WriteAttributes, WriteData, WriteExtendedAttributes, WriteKey)}
SystemAcl      : {}
RawDescriptor  : System.Security.AccessControl.CommonSecurityDescriptor
  
```

SDDL mit der PowerShell betrachtet



ESAE-Struktur

```

Administrator: PowerShell
PS C:\Users\administrator.CH> $PROFILE | Get-Member -MemberType NoteProperty

TypeName: System.String

Name           MemberType Definition
-----
AllUsersAllHosts NoteProperty string AllUsersAllHosts=C:\Program Files\PowerShell\7\profile.ps1
AllUsersCurrentHost NoteProperty string AllUsersCurrentHost=C:\Program Files\PowerShell\7\Microsoft.PowerShell_prof...
CurrentUserAllHosts NoteProperty string CurrentUserAllHosts=C:\Users\administrator.CH\Documents\PowerShell\profile...
CurrentUserCurrentHost NoteProperty string CurrentUserCurrentHost=C:\Users\administrator.CH\Documents\PowerShell\Micro...
  
```

l\7\profile.ps1

```

Administrator: PowerShell
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\administrator.CH> $PROFILE | Get-Member -MemberType NoteProperty

TypeName: System.String

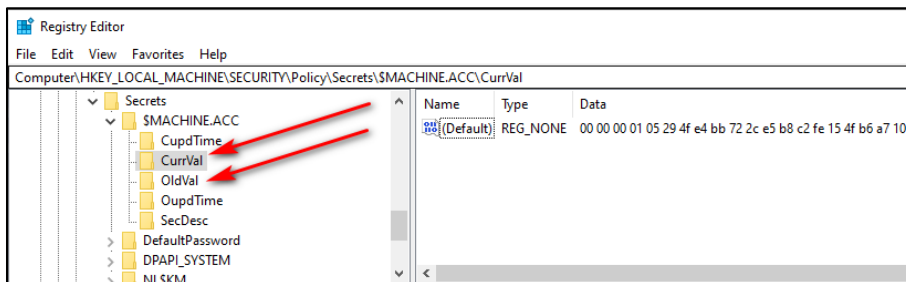
Name           MemberType Definition
-----
AllUsersAllHosts NoteProperty string AllUsersAllHosts=C:\Windows\System32\WindowsPowerShell\v1.0\profile.ps1
AllUsersCurrentHost NoteProperty string AllUsersCurrentHost=C:\Windows\System32\WindowsPowerShell\v1.0\Microsoft...
CurrentUserAllHosts NoteProperty string CurrentUserAllHosts=C:\Users\administrator.CH\Documents\WindowsPowerShell...
CurrentUserCurrentHost NoteProperty string CurrentUserCurrentHost=C:\Users\administrator.CH\Documents\WindowsPowerSh...
  
```

m32\WindowsPowerShell\v1.0

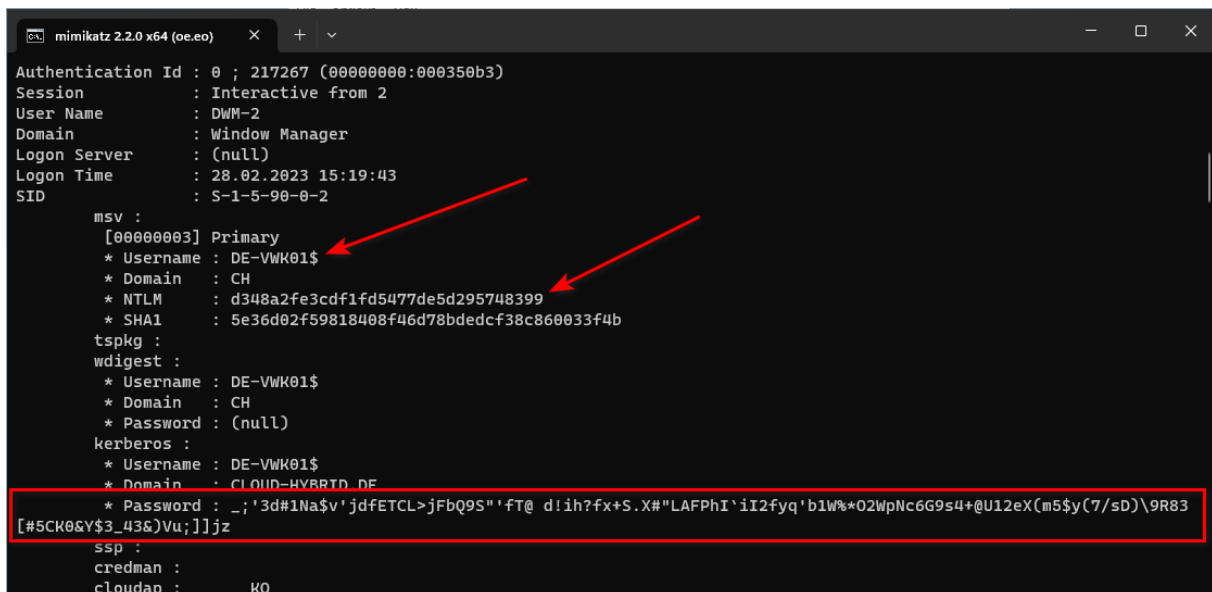
PowerShell-Profilpfade und Windows PowerShell-Profilpfade



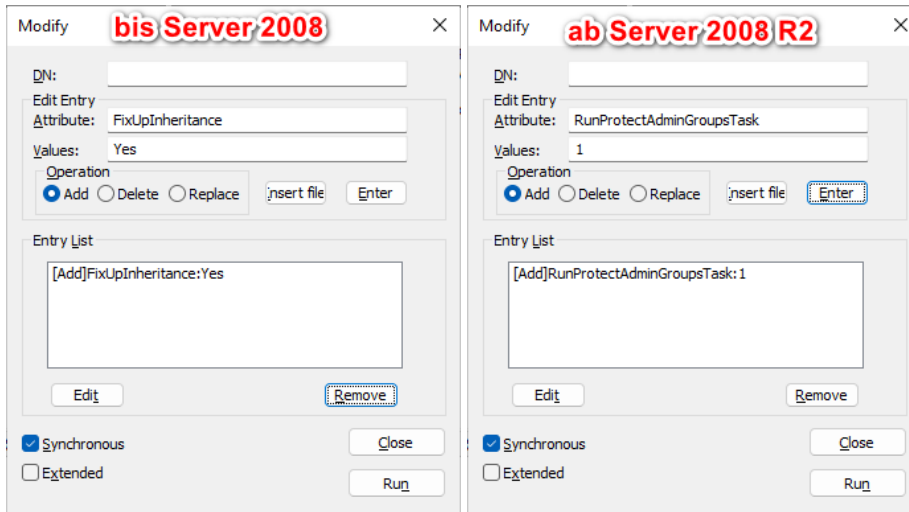
Visual Studio Code – PowerShell oder Windows PowerShell?



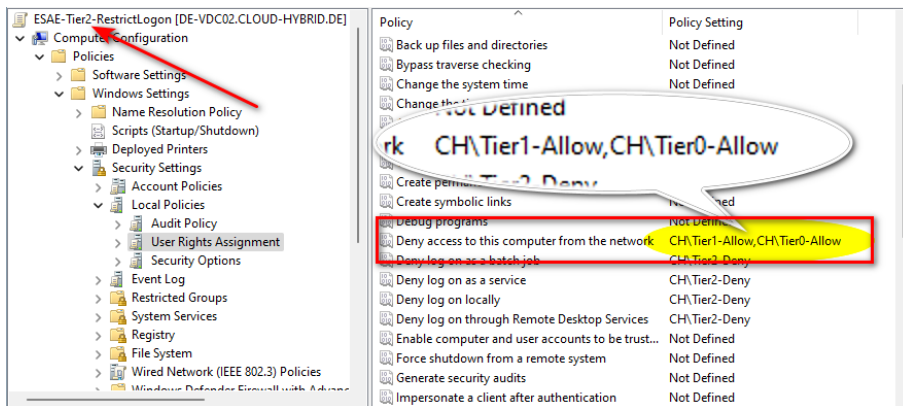
Computerkennwort



Hash des Computerkennwortes und Klartextkennwort



SDProp-Start



Tiering-Policy – Tier2

```
Administrator: PowerShell x Administrator: Eingabeauffor... x
C:\Users\administrator.CH>klist

Current LogonId is 0:0x4c8fcc

Cached Tickets: (13)

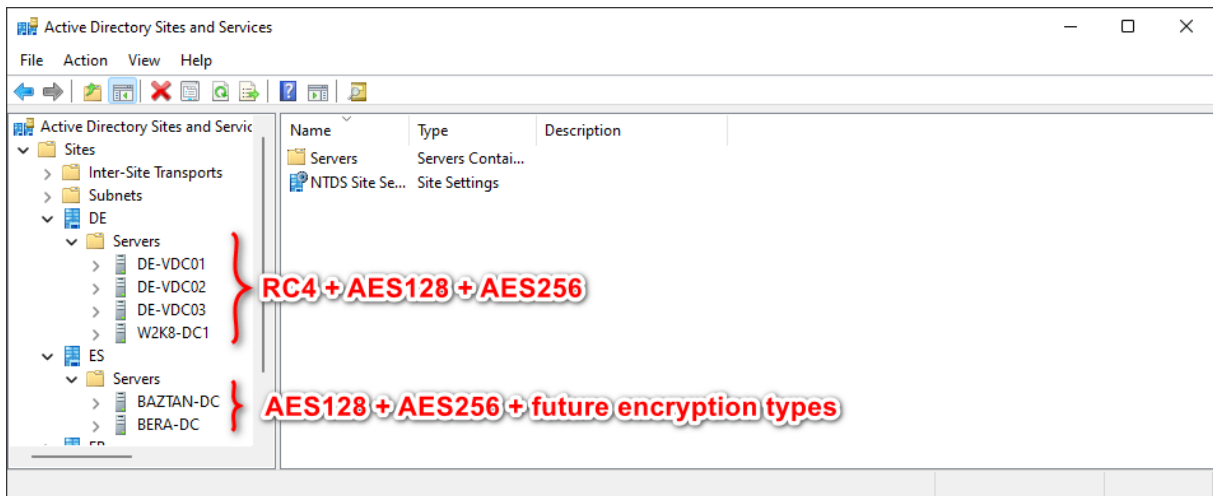
#0> Client: administrator @ CLOUD-HYBRID.DE
Server: krbtgt, CLOUD-HYBRID.DE @ CLOUD-HYBRID.DE
KerberosTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0xe10000 -> renewable initial_pre_authent name_canonicalize
Start Time: 3/7/2023 6:17:17 (local)
End Time: 3/7/2023 16:17:17 (local)
Renew Time: 3/14/2023 6:17:17 (local)
Session Key Type: AES-256-CTS-HMAC-SHA1-96
Cache Flags: 0x1 -> PRIMARY
Kdc Called: DE-VDC01
```

**Ticket Granting Ticket
TGT**

```
#1> Client: administrator @ CLOUD-HYBRID.DE
Server: cifs/DE-VDC03.CLOUD-HYBRID.DE/CLOUD-HYBRID.DE @ CLOUD-HYBRID.DE
KerberosTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0xa50000 -> renewable_pre_authent ok_as_delegate name_canonicalize
Start Time: 3/7/2023 8:01:19 (local)
End Time: 3/7/2023 16:17:17 (local)
Renew Time: 3/14/2023 6:17:17 (local)
Session Key Type: AES-256-CTS-HMAC-SHA1-96
Cache Flags: 0
Kdc Called: DE-VDC03.CLOUD-HYBRID.DE
```

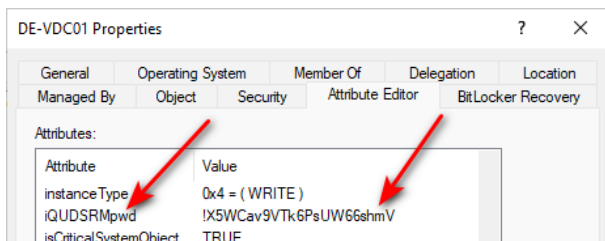
**Ticket Granting
Service Ticket
TGS**

Ticket Granting Ticket und Ticket Granting Service Ticket

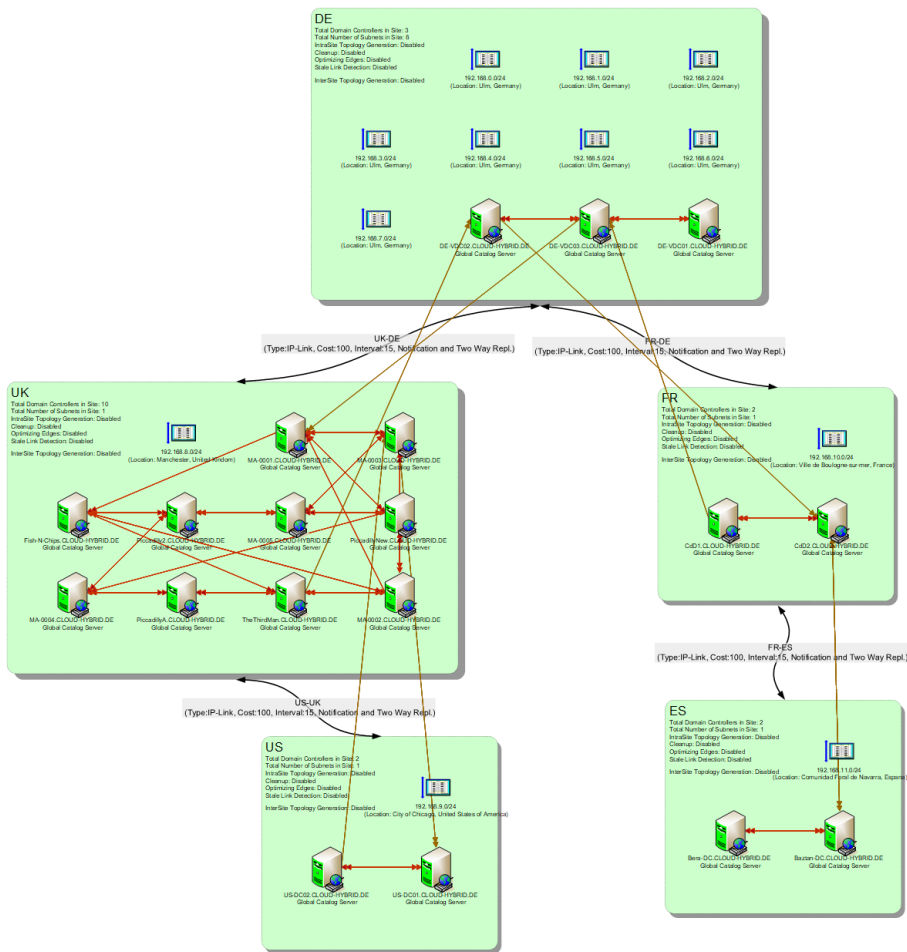


Kerberos encryption types – pro Site definiert

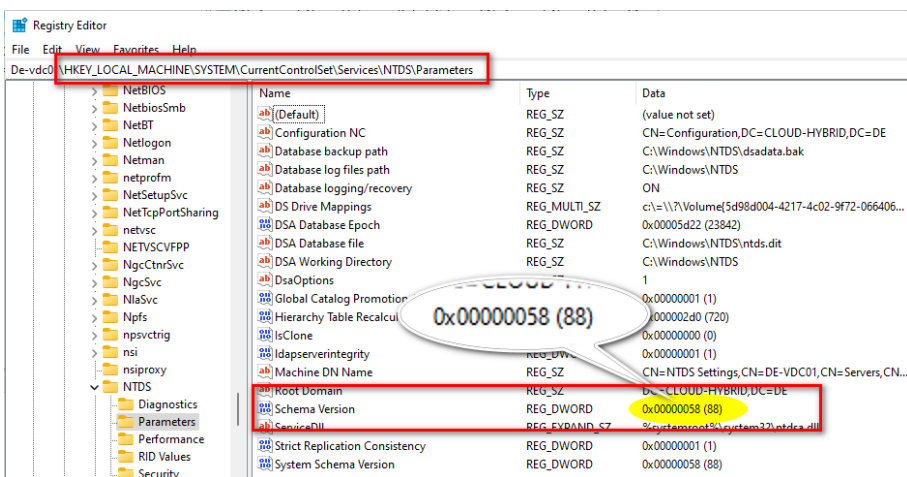
Name	Type	Name	Type	DC Type	Site
Break Glass1	User	BAZTAN-DC	Computer	GC	ES
Break Glass2	User	BERA-DC	Computer	GC	ES
dBaztan-DC	User	CDD1	Computer	GC	FR
dBera-DC	User	CDD2	Computer	GC	FR
dCdD1	User	DE-VDC01	Computer	GC	DE
dCdD2	User	DE-VDC02	Computer	GC	DE
dDE-VDC01	User	DE-VDC03	Computer	GC	DE
dDE-VDC02	User	FISH-N-CHIPS	Computer	GC	UK
dDE-VDC03	User	MA-0001	Computer	GC	UK
dFish-N-Chips	User	MA-0002	Computer	GC	UK
dMA-0001	User	MA-0003	Computer	GC	UK
dMA-0002	User	MA-0004	Computer	GC	UK
dMA-0003	User	MA-0005	Computer	GC	UK
dMA-0004	User	PICCADILLY2	Computer	GC	UK
dMA-0005	User	PICCADILLYA	Computer	GC	UK
dPiccadilly2	User	PICCADILLYNEW	Computer	GC	UK
dPiccadillyA	User	THETHIRDMAN	Computer	GC	UK
dPiccadillyNew	User	US-DC01	Computer	GC	US
dTheThirdMan	User	US-DC02	Computer	GC	US
dUS-DC01	User				
dUS-DC02	User				
Martin Handl	User				



DSRM-Referenz-User im Active Directory – LAPS für Domain Controller



ADTD – Active Directory Topology Generator



Schema-Version 88

```

10 # -----
11 # Attributes
12 # -----
13
14 # Attribute: IQUDSRMpwd
15 dn: cn=IQUDSRMpwd,cn=Schema,cn=Configuration,dc=X
16 changetype: add
17 objectClass: attributeSchema
18 attributeId: 1.3.1.4.1.49955.1.1.1.1
19 ldapDisplayName: IQUDSRMpwd
20 attributeSyntax: 2.5.5.12
21 adminDescription: stores the dsrm password of an zwdc
22 adminDisplayName: IQUDSRMpwd
23 # schemaIDGUID: 7ee4359a-5d7a-4b90-894d-7dcab4623fa4
24 schemaIDGUID: 7ee4359a-5d7a-4b90-894d-7dcab4623fa4
25 oMSyntax: 64
26 searchFlags: 896
27 isSingleValued: TRUE
28 systemOnly: FALSE
29
30 dn:
31 changetype: modify
32 add: schemaUpdateNow
33 schemaUpdateNow: 1
34
35
36 # -----
37 # Updating present elements
38 # -----
39
40
41 # Update element: computer
42 dn: cn=Computer,cn=Schema,cn=Configuration,dc=X
43 changetype: modify
44 add: mayContain
45 # mayContain: IQUDSRMpwd
46 mayContain: 1.3.1.4.1.49955.1.1.1.1
47
48
49 dn:
50 changetype: modify
51 add: schemaUpdateNow
52 schemaUpdateNow: 1
53
54

```

Attribute (lines 14-28)

alte schemaIDGUID auskommentiert (line 23)

Update Schema-Cache (lines 32-33)

Zuordnung zur Objektklasse (lines 42-46)

Update Schema-Cache (lines 51-52)

Schemaerweiterung per LDIF-Datei

```

PS C:\> (Get-ADDomain).PDCEmulator
DE-VDC02.CLOUD-HYBRID.DE
PS C:\> Resolve-DnsName -Name _kerberos._tcp.cloud-hybrid.de -Type SRV

```

Name	Type	TTL	Section	NameTarget	Priority	Weight	Port
_kerberos._tcp.cloud-hybrid.de	SRV	600	Answer	de-vdc01.cloud-hybrid.de	0	100	88
_kerberos._tcp.cloud-hybrid.de	SRV	600	Answer	de-vdc03.cloud-hybrid.de	0	100	88
_kerberos._tcp.cloud-hybrid.de	SRV	600	Answer	ma-0001.cloud-hybrid.de	0	100	88
_kerberos._tcp.cloud-hybrid.de	SRV	600	Answer	ma-0003.cloud-hybrid.de	0	100	88
_kerberos._tcp.cloud-hybrid.de	SRV	600	Answer	ma-0005.cloud-hybrid.de	0	100	88
_kerberos._tcp.cloud-hybrid.de	SRV	600	Answer	piccadilly2.cloud-hybrid.de	0	100	88
_kerberos._tcp.cloud-hybrid.de	SRV	600	Answer	baztan-dc.cloud-hybrid.de	0	100	88
_kerberos._tcp.cloud-hybrid.de	SRV	600	Answer	fish-n-chips.cloud-hybrid.de	0	100	88
_kerberos._tcp.cloud-hybrid.de	SRV	600	Answer	ma-0004.cloud-hybrid.de	0	100	88
_kerberos._tcp.cloud-hybrid.de	SRV	600	Answer	cdd1.cloud-hybrid.de	0	100	88
_kerberos._tcp.cloud-hybrid.de	SRV	600	Answer	thethirdman.cloud-hybrid.de	0	100	88
_kerberos._tcp.cloud-hybrid.de	SRV	600	Answer	piccadillynew.cloud-hybrid.de	0	100	88
_kerberos._tcp.cloud-hybrid.de	SRV	600	Answer	piccadillya.cloud-hybrid.de	0	100	88
_kerberos._tcp.cloud-hybrid.de	SRV	600	Answer	ma-0002.cloud-hybrid.de	0	100	88
_kerberos._tcp.cloud-hybrid.de	SRV	600	Answer	cdd2.cloud-hybrid.de	0	100	88
_kerberos._tcp.cloud-hybrid.de	SRV	600	Answer	us-dc02.cloud-hybrid.de	0	100	88
_kerberos._tcp.cloud-hybrid.de	SRV	600	Answer	bera-dc.cloud-hybrid.de	0	100	88
_kerberos._tcp.cloud-hybrid.de	SRV	600	Answer	us-dc01.cloud-hybrid.de	0	100	88
_kerberos._tcp.cloud-hybrid.de	SRV	600	Answer	de-vdc02.cloud-hybrid.de	0	50	88

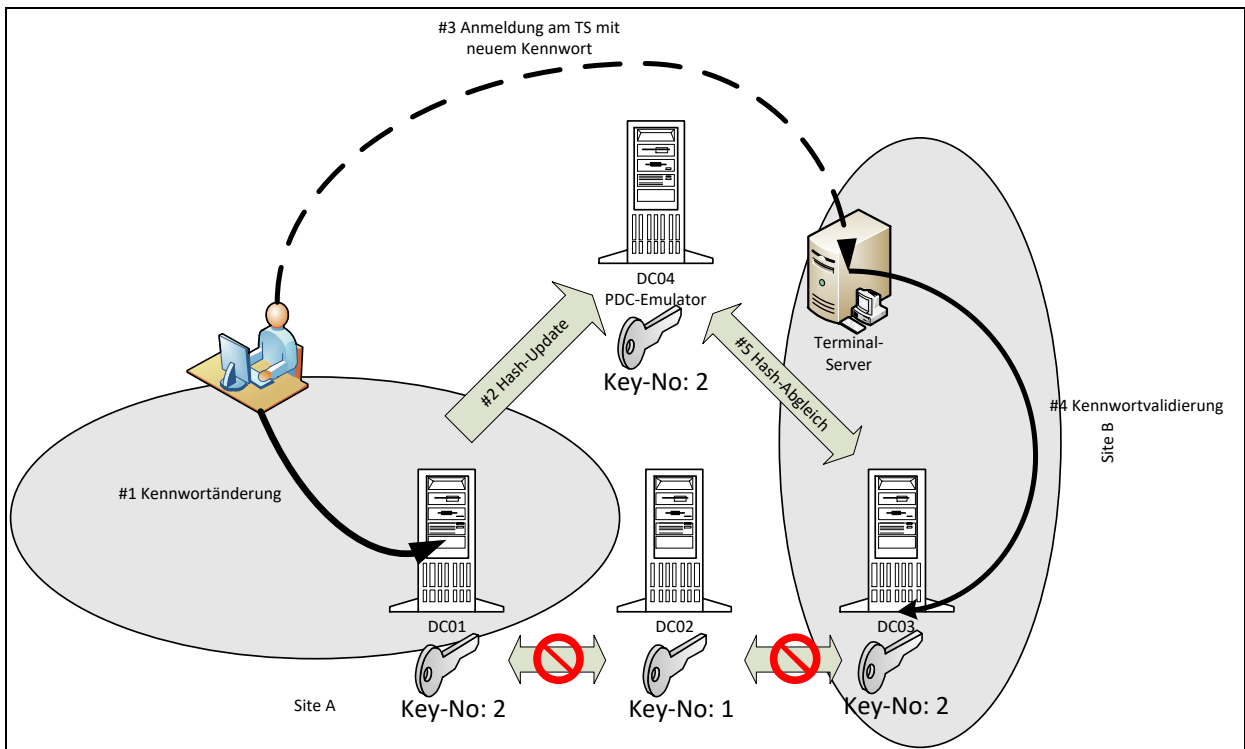
Gewicht eines DC.

```

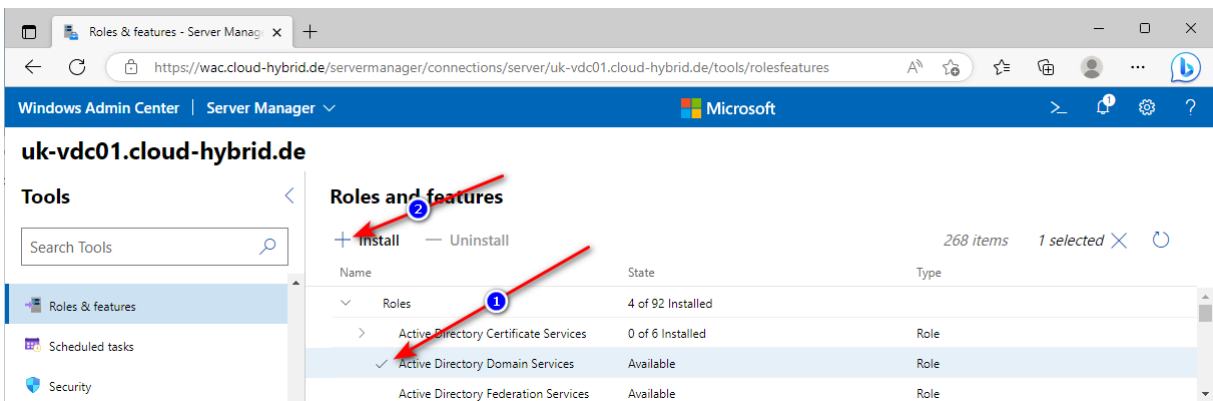
PS C:\> (Get-ADDomain).ReplicaDirectoryServers.foreach{ Get-Content -Path \\$_\Admin$\debug\netlogon.Log }
03/13 14:38:49 [2080] CH: NO_CLIENT_SITE: DE-VSV02 192.168.12.9
03/13 14:39:24 [2080] CH: NO_CLIENT_SITE: DE-VSV02 192.168.12.9
03/13 14:39:32 [2080] CH: NO_CLIENT_SITE: DE-VSV02 192.168.12.9
03/13 14:39:47 [2080] CH: NO_CLIENT_SITE: DE-VSV02 192.168.12.9
03/13 14:56:54 [1240] CH: NO_CLIENT_SITE: DE-VSV02 192.168.12.9
03/13 14:38:50 [1264] CH: NO_CLIENT_SITE: DE-VSV02 192.168.12.9
03/13 14:39:27 [1960] CH: NO_CLIENT_SITE: DE-VSV02 192.168.12.9
03/13 14:39:30 [1264] CH: NO_CLIENT_SITE: DE-VSV02 192.168.12.9
03/13 14:39:50 [1960] CH: NO_CLIENT_SITE: DE-VSV02 192.168.12.9
03/13 14:56:50 [1264] CH: NO_CLIENT_SITE: DE-VSV02 192.168.12.9

```

NO_CLIENT_SITE – IP-Subnetz keiner Site zugeordnet



PDC-E ist der Master-Key-Server



Windows Admin Center (WAC) zur Rolleninstallation nutzen.

```

Administrator: PowerShell
PS C:\> Invoke-Command `
>> -Computername ( `
>> (Get-ADComputer -Filter { name -like "UK-VDC0*" } `
>> -SearchBase (Get-ADDomain).ComputersContainer).DNSHostName) `
>> -ScriptBlock { Install-WindowsFeature -Name AD-Domain-Services } -ThrottleLimit 1

PSComputerName : UK-VDC01.CLOUD-HYBRID.DE
RunspaceId      : 2f2564e6-0ff2-4177-90eb-35d10b786ed1
Success         : True
RestartNeeded   : No
FeatureResult   : {Active Directory Domain Services}
ExitCode        : Success

PSComputerName : UK-VDC02.CLOUD-HYBRID.DE
RunspaceId      : 30c45bc1-6a9f-417a-a96c-629980bd03bd
Success         : True
RestartNeeded   : No
FeatureResult   : {Active Directory Domain Services}
ExitCode        : Success
  
```

PowerShell-Remoting zur Rolleninstallation nutzen

```

Administrator: PowerShell
PS C:\> (Resolve-DnsName -Name _ldap._tcp.cloud-hybrid.de -Type SRV).where{ $_.NameTarget -eq "uk-vdc01.cloud-hybrid.de" }

Name                Type  TTL  Section  NameTarget                Priority Weight Port
-----
_ldap._tcp.cloud-hybrid.de  SRV   600  Answer  uk-vdc01.cloud-hybrid.de    0      100  389

PS C:\> (Resolve-DnsName -Name _kerberos._tcp.cloud-hybrid.de -Type SRV).where{ $_.NameTarget -eq "uk-vdc01.cloud-hybrid.de" }

Name                Type  TTL  Section  NameTarget                Priority Weight Port
-----
_kerberos._tcp.cloud-hybrid.de  SRV   600  Answer  uk-vdc01.cloud-hybrid.de    0      100  88

PS C:\> (Resolve-DnsName -Name _kpasswd._tcp.cloud-hybrid.de -Type SRV).where{ $_.NameTarget -eq "uk-vdc01.cloud-hybrid.de" }

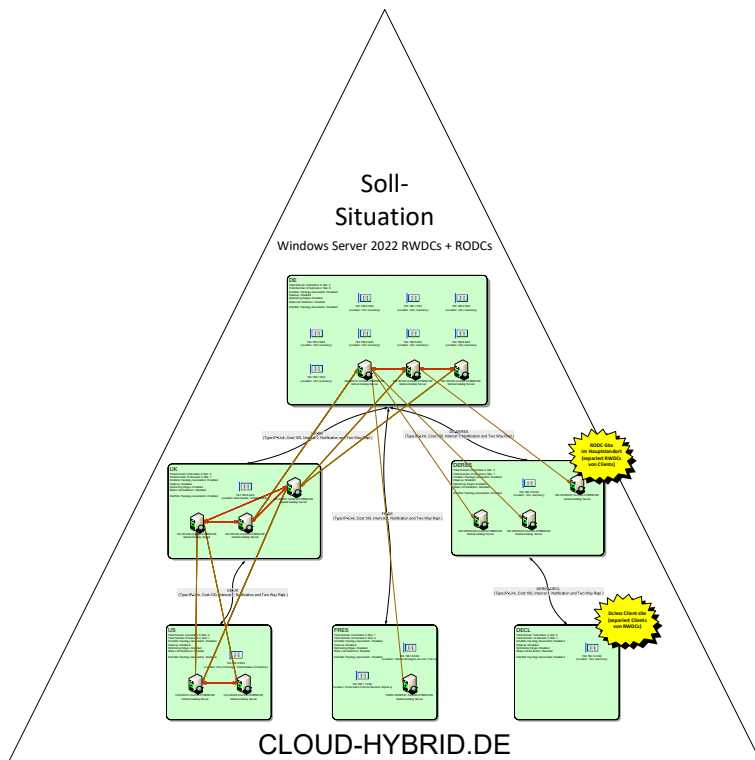
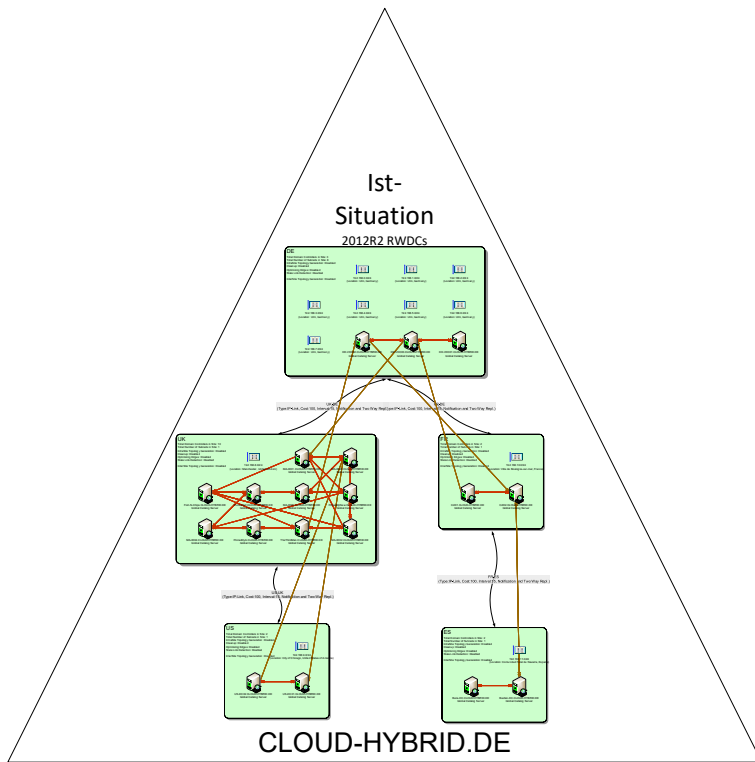
Name                Type  TTL  Section  NameTarget                Priority Weight Port
-----
_kpasswd._tcp.cloud-hybrid.de  SRV   600  Answer  uk-vdc01.cloud-hybrid.de    0      100  464

PS C:\> (Resolve-DnsName -Name _gc._tcp.cloud-hybrid.de -Type SRV).where{ $_.NameTarget -eq "uk-vdc01.cloud-hybrid.de" }

Name                Type  TTL  Section  NameTarget                Priority Weight Port
-----
_gc._tcp.cloud-hybrid.de      SRV   600  Answer  uk-vdc01.cloud-hybrid.de    0      100  3268

PS C:\>
  
```

SRV-Einträge im DNS



Ist-Situation und Soll-Situation

```

PS C:\> Resolve-DnsName -Name _ldap._tcp.cloud-hybrid.de -Type SRV

```

Name	Type	TTL	Section	NameTarget	Priority	Weight	Port
_ldap._tcp.cloud-hybrid.de	SRV	600	Answer	thethirdman.cloud-hybrid.de	0	100	389
_ldap._tcp.cloud-hybrid.de	SRV	600	Answer	piccadillya.cloud-hybrid.de	0	100	389
_ldap._tcp.cloud-hybrid.de	SRV	600	Answer	bera-dc.cloud-hybrid.de	0	100	389
_ldap._tcp.cloud-hybrid.de	SRV	600	Answer	uk-vdc01.cloud-hybrid.de	0	100	389
_ldap._tcp.cloud-hybrid.de	SRV	600	Answer	ma-0002.cloud-hybrid.de	0	100	389
_ldap._tcp.cloud-hybrid.de	SRV	600	Answer	cdd1.cloud-hybrid.de	0	100	389
_ldap._tcp.cloud-hybrid.de	SRV	600	Answer	ma-0004.cloud-hybrid.de	0	100	389
_ldap._tcp.cloud-hybrid.de	SRV	600	Answer	cdd2.cloud-hybrid.de	0	100	389
_ldap._tcp.cloud-hybrid.de	SRV	600	Answer	baztan-dc.cloud-hybrid.de	0	100	389
_ldap._tcp.cloud-hybrid.de	SRV	600	Answer	fish-n-chips.cloud-hybrid.de	0	100	389
_ldap._tcp.cloud-hybrid.de	SRV	600	Answer	piccadillynew.cloud-hybrid.de	0	100	389
_ldap._tcp.cloud-hybrid.de	SRV	600	Answer	us-dc01.cloud-hybrid.de	0	100	389
_ldap._tcp.cloud-hybrid.de	SRV	600	Answer	us-dc02.cloud-hybrid.de	0	100	389
_ldap._tcp.cloud-hybrid.de	SRV	600	Answer	ma-0001.cloud-hybrid.de	0	100	389
_ldap._tcp.cloud-hybrid.de	SRV	600	Answer	de-vdc02.cloud-hybrid.de	0	50	389
_ldap._tcp.cloud-hybrid.de	SRV	600	Answer	de-vdc03.cloud-hybrid.de	0	100	389
_ldap._tcp.cloud-hybrid.de	SRV	600	Answer	piccadilly2.cloud-hybrid.de	0	100	389
_ldap._tcp.cloud-hybrid.de	SRV	600	Answer	de-vdc01.cloud-hybrid.de	0	100	389
_ldap._tcp.cloud-hybrid.de	SRV	600	Answer	ma-0003.cloud-hybrid.de	0	100	389
_ldap._tcp.cloud-hybrid.de	SRV	600	Answer	ma-0005.cloud-hybrid.de	10	100	389

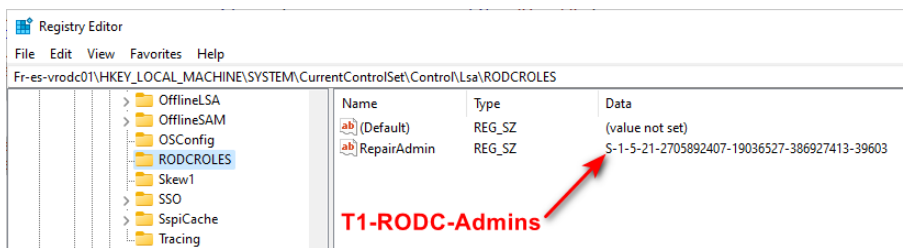
Priorität via Windows PowerShell setzen

```

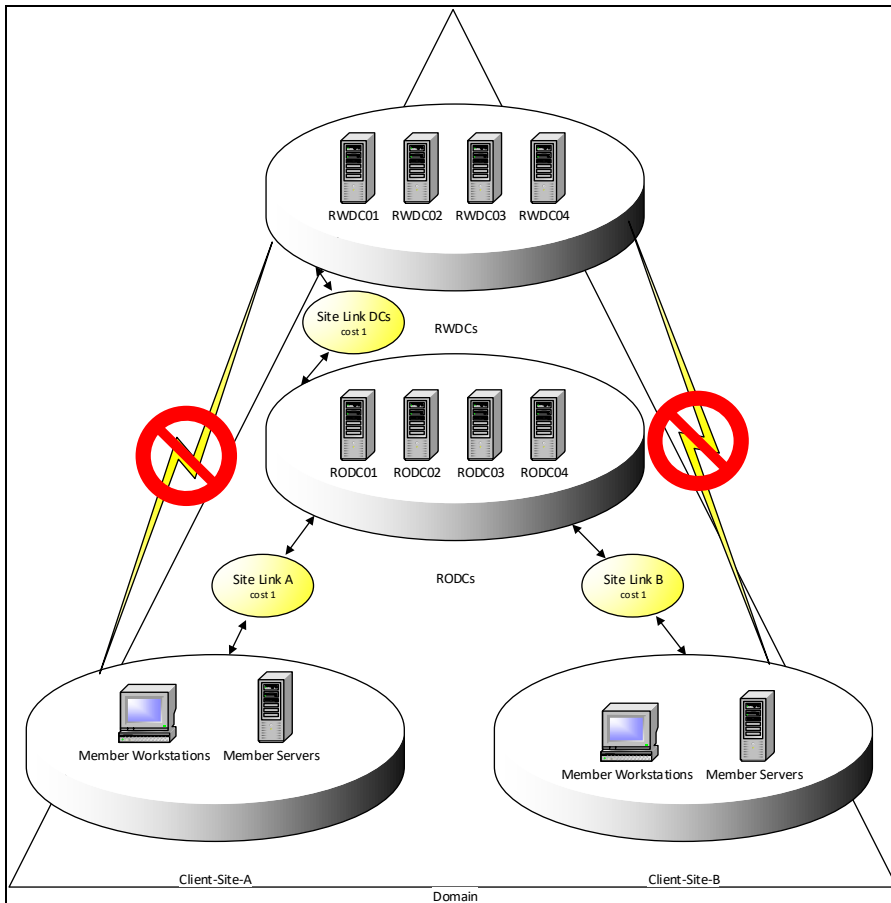
PS C:\> Invoke-DCRemoval -ComputerName MA-0005 -Verbose
VERBOSE: Building default variables
VERBOSE: Checking the DC Name MA-0005
VERBOSE: Creating DC FQDN if not present
VERBOSE: Creating DN of DC MA-0005.CLOUD-HYBRID.DE
VERBOSE: Creating NTDSSettingsObjectDN of DC MA-0005.CLOUD-HYBRID.DE
VERBOSE: Building DNS variables for DC MA-0005.CLOUD-HYBRID.DE
VERBOSE: MA-0005
VERBOSE: Pinging target DC MA-0005.CLOUD-HYBRID.DE
Pinging target DC MA-0005.CLOUD-HYBRID.DE - this might take a while.
VERBOSE: Checking if target DC MA-0005.CLOUD-HYBRID.DE holds an FSMO
VERBOSE: Checking if target DC MA-0005.CLOUD-HYBRID.DE is manual Bridge-Head-Server
VERBOSE: Checking if target DC MA-0005.CLOUD-HYBRID.DE is automatic Bridge-Head-Server
VERBOSE: Checking if NtFrs, DFSR or both are used for SYSVOL replication on DC MA-0005.CLOUD-HYBRID.DE
VERBOSE: Checking DNS priority in SRV records of DC MA-0005.CLOUD-HYBRID.DE
VERBOSE: _ldap._tcp.CLOUD-HYBRID.DE
VERBOSE: _ldap._tcp.CLOUD-HYBRID.DE
VERBOSE: Deleting computer object of DC MA-0005.CLOUD-HYBRID.DE
VERBOSE: Deleting SYSVOL object of DC MA-0005.CLOUD-HYBRID.DE
VERBOSE: Deleting DNS entries of DC MA-0005.CLOUD-HYBRID.DE
Ptr-record of MA-0005.CLOUD-HYBRID.DE did not exist in reverse-lookup zone.
VERBOSE: Deleting Sites-n-Service Object of DC MA-0005.CLOUD-HYBRID.DE
The DC MA-0005.CLOUD-HYBRID.DE was successfully deleted!

```

Domain Controller per Windows PowerShell entfernen



RODC-Admins



RODC als Front-End-DC

Active Directory Sites and Services

Name	Site	Location	Type	Description
192.168.0.0/24	DE	Ulm, Germany	Subnet	
192.168.1.0/24	DE	Ulm, Germany	Subnet	
192.168.2.0/24	DE	Ulm, Germany	Subnet	
192.168.3.0/24	DE	Ulm, Germany	Subnet	
192.168.4.0/24	DE	Ulm, Germany	Subnet	
192.168.5.0/24	DE	Ulm, Germany	Subnet	
192.168.6.0/24	DE	Ulm, Germany	Subnet	
192.168.7.0/24	DE	Ulm, Germany	Subnet	
192.168.14.0/24	DECL		Subnet	
192.168.12.0/24	DERES		Subnet	
192.168.10.0/24	FR-ES	Ville de Boulogne-sur-mer, France	Subnet	
192.168.11.0/24	FR-ES	Comunidad Foral de Navarra, Espana	Subnet	
192.168.8.0/24	UK	Manchester, United Kindom	Subnet	
192.168.9.0/24	US	City of Chicago, United States of America	Subnet	

Annotations in the screenshot:
 - Red arrows point to subnets 192.168.0.0/24 through 192.168.7.0/24, labeled **RWDCs**.
 - A red arrow points to subnet 192.168.14.0/24, labeled **no DCs (DC-less site)**.
 - A red arrow points to subnet 192.168.12.0/24, labeled **RODCs**.

Umsetzung in den Sites

```

C:\mimikatz2.2.0x64 (oe.eo)
PS C:\mimikatz\x64> .\mimikatz.exe

.#####.  mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
.## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
## / \ ##  /** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##   > https://blog.gentilkiwi.com/mimikatz
'## v ##'   Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'   > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # privilege::debug
Privilege '20' OK

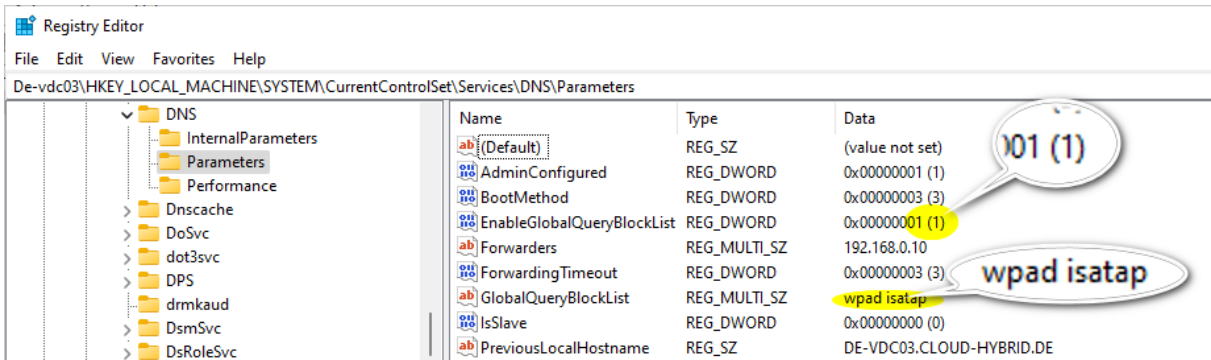
mimikatz # lsadump::lsa /inject /name:krbtgt
Domain : CH / S-1-5-21-2705892407-19036527-386927413

RID : 000001f6 (502)
User : krbtgt

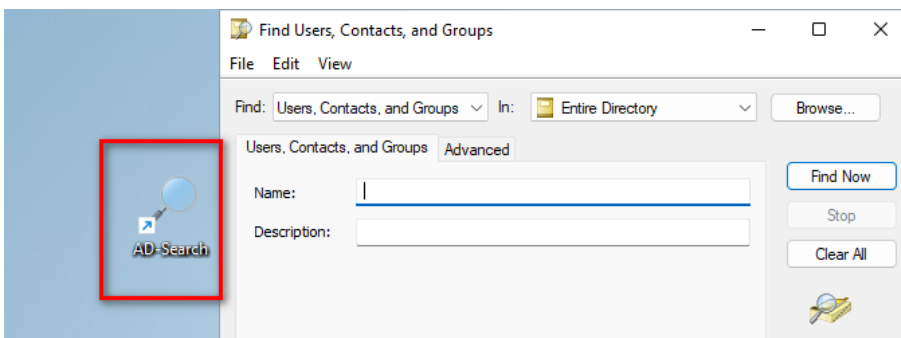
* Primary
NTLM :
LM :

mimikatz #
  
```

Kein Hash vom krbtgt auf einem RODC



Global query block list im DNS

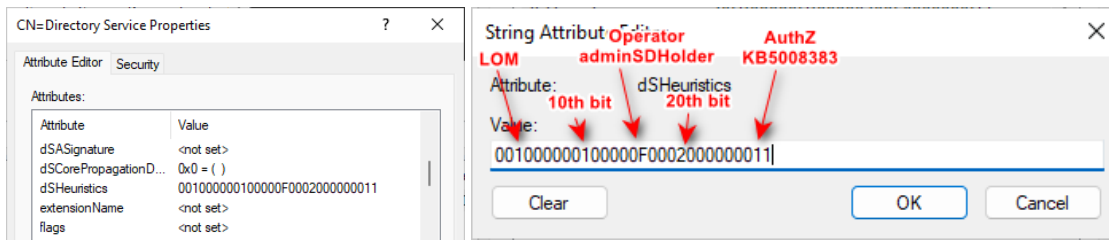


Suchen im AD vom Desktop aus – keine RSAT erforderlich

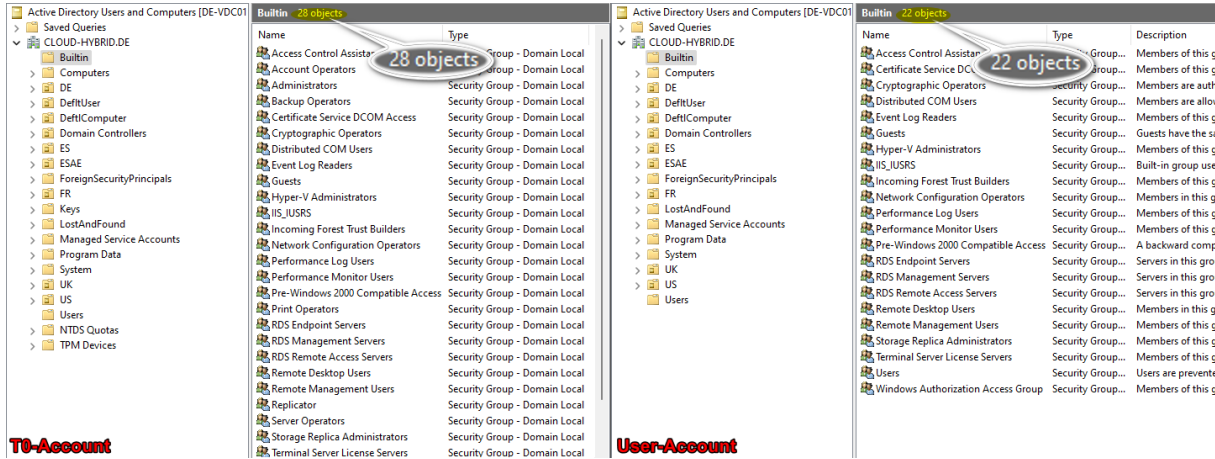
```

Administrator: PowerShell
PS C:\> $dn = (Get-ADUser -Identity "de-4885").DistinguishedName
PS C:\> (Get-ADObject -LDAPFilter "(member:1.2.840.113556.1.4.1941:=$dn)").Name | Sort-Object
Backup Operators
T1-DERES-RODC-Allow
Tier0-Deny
Tier0-Hide
Tier1-Deny
Tier2-Allow
UG-All-DE-Users
  
```

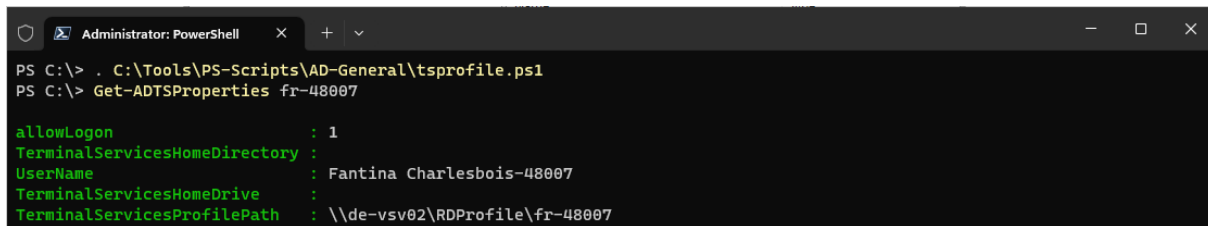
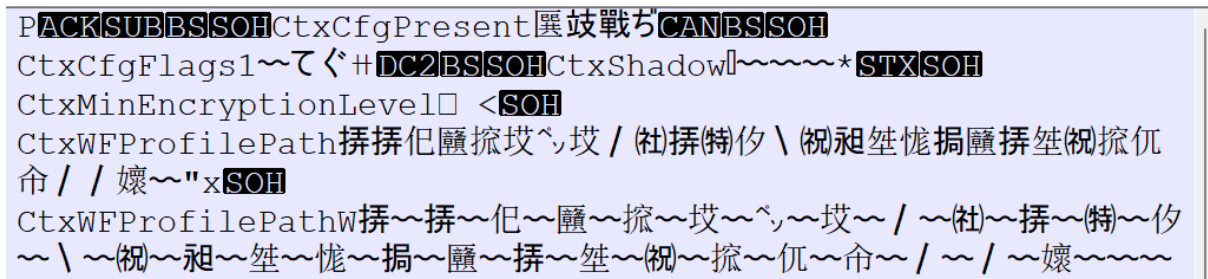
LDAP_MATCHING_RULE_IN_CHAIN um Gruppenmitgliedschaften festzustellen



dSHeuristics



List Object Mode vesteckt sensitive Konten



Tsprofile.ps1

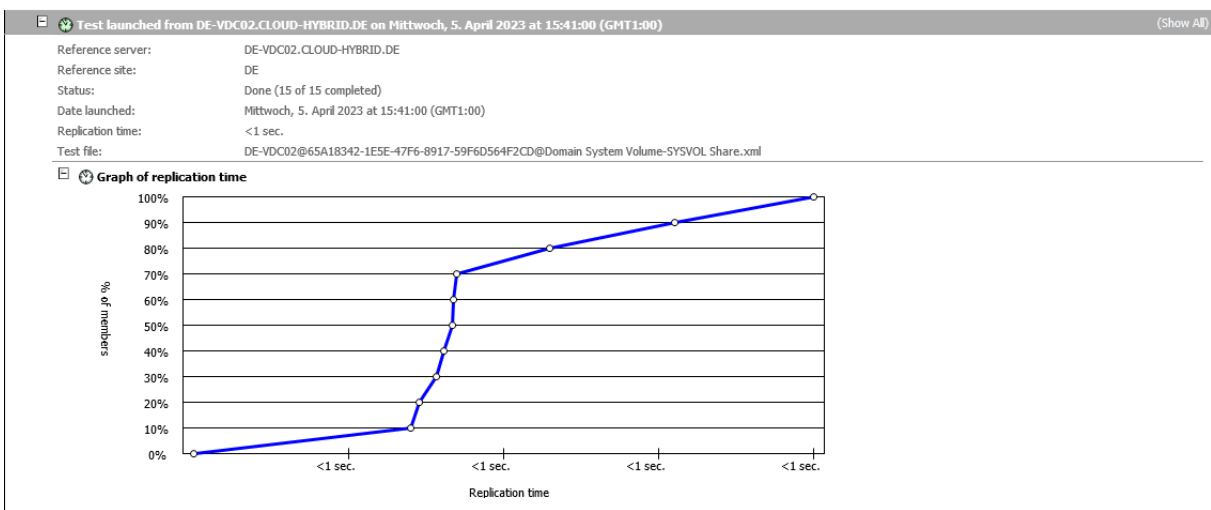
```

Administrator: PowerShell
PS C:\> [xml]$ADWS = Get-Content -Path "\\de-vdc02\admin$\ADWS\Microsoft.ActiveDirectory.WebServices.exe.config"
PS C:\> $ADWS.configuration.appsettings.add

key                               value
----                               -
MaxPoolConnections                10
MaxPercentageReservedConnections 50
MaxConnectionsPerUser             5
MaxEnumContextExpiration          00:30:00
MaxPullTimeout                   00:02:00
MaxEnumCtxsPerSession            5
MaxEnumCtxsTotal                 100
MaxConcurrentCalls               32
MaxConcurrentSessions            500
OperationTimeout                 00:02:00

```

ADWS Query Policy



SYSVOL Propagation Time

```

Administrator: PowerShell
Administrator: Windows Pow
Loading personal and system profiles took 11101ms.
PS C:\> Invoke-SYSVOLDFSReplicationRepair -AuthoritativeRestore
Group Policy amount in SYSVOL: 15 DE-VDC02.CLOUD-HYBRID.DE <--- PDCE
Group Policy amount in SYSVOL: 15 UK-VDC01.CLOUD-HYBRID.DE
Group Policy amount in SYSVOL: 15 US-VDC01.CLOUD-HYBRID.DE
Group Policy amount in SYSVOL: 15 US-VDC02.CLOUD-HYBRID.DE
Group Policy amount in SYSVOL: 15 UK-VDC02.CLOUD-HYBRID.DE
Group Policy amount in SYSVOL: 15 UK-VDC03.CLOUD-HYBRID.DE
Group Policy amount in SYSVOL: 15 DE-VDC03.CLOUD-HYBRID.DE
Group Policy amount in SYSVOL: 15 DE-VDC01.CLOUD-HYBRID.DE

Beginning authoritative restore of SYSVOL
An authoritative restore of the SYSVOL share has been performed.
Either because you selected this by parameter or it was necessary (or both - who knows?).
PS C:\>

```

DFS-R Autorisierende Wiederherstellung

- [-] CN=Configuration,DC=CLOUD-HYBRID,DC=DE
- [-] CN=Deleted Objects,CN=Configuration,DC=CLOUD-HYBRID,DC=DE
- [-] CN=DisplaySpecifiers,CN=Configuration,DC=CLOUD-HYBRID,DC=DE
- [-] CN=Extended-Rights,CN=Configuration,DC=CLOUD-HYBRID,DC=DE
- [-] CN=ForestUpdates,CN=Configuration,DC=CLOUD-HYBRID,DC=DE
- [-] CN=LostAndFoundConfig,CN=Configuration,DC=CLOUD-HYBRID,DC=DE
- [-] CN=NTDS Quotas,CN=Configuration,DC=CLOUD-HYBRID,DC=DE
- [-] CN=Partitions,CN=Configuration,DC=CLOUD-HYBRID,DC=DE
- [-] CN=Physical Locations,CN=Configuration,DC=CLOUD-HYBRID,DC=DE
- [-] CN=Services,CN=Configuration,DC=CLOUD-HYBRID,DC=DE
- [-] CN=Sites,CN=Configuration,DC=CLOUD-HYBRID,DC=DE
- [-] CN=WellKnown Security Principals,CN=Configuration,DC=CLOUD-HYBRID,DC=DE

Deleted Objects

```

Administrator: PowerShell x Administrator: Eingabeauffor x
Microsoft Windows [Version 10.0.22000.1761]
(c) Microsoft Corporation. All rights reserved.

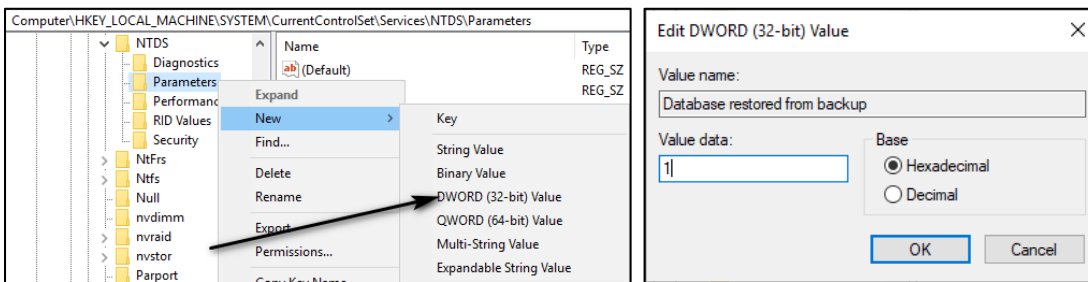
C:\Users\maxm>repadmin /showobjmeta de-vdc02 "CN=Claims Configuration,CN=Services,CN=Configuration,DC=CLOUD-HYBRID,DC=DE"

11 entries.
Loc.USN          Originating DSA  Org.USN  Org.Time/Date  Ver Attri
=====
2455964          DE\DE-VDC03     1994763  2023-04-06 15:14:20 100001 objectClass
2455966          DE\DE-VDC02     2455966  2023-04-06 15:15:35 3 cn
2455964          DE\DE-VDC03     1994763  2023-04-06 15:14:20 100001 instanceType
6168            eeeca1fe-00d6-4200-9b31-6e507249424a 4139    2023-01-26 07:20:13 1 whenCreated
2455967          DE\DE-VDC03     1994763  2023-04-06 15:14:20 100000 isDeleted
2455964          DE\DE-VDC03     1994763  2023-04-06 15:14:20 100001 showIn
2455964          DE\DE-VDC03     1994763  2023-04-06 15:14:20 100002 nTSecurity
2455966          DE\DE-VDC03     1994763  2023-04-06 15:14:20 100001 name
2455366          DE\DE-VDC02     2455366  2023-04-06 15:11:20 1 LastKnownParent
2455969          DE\DE-VDC03     1994763  2023-04-06 15:14:20 100001 objectCategory
2455366          DE\DE-VDC02     2455366  2023-04-06 15:11:20 1 msDS-LastKnownParent

0 entries.
Type  Attribute  Last Mod Time  Originating DSA  Loc.USN  Org.USN
=====
Distinguished Name
=====

```

Authoritative Restore im AD



Database restored from backup – Lösung per Hand