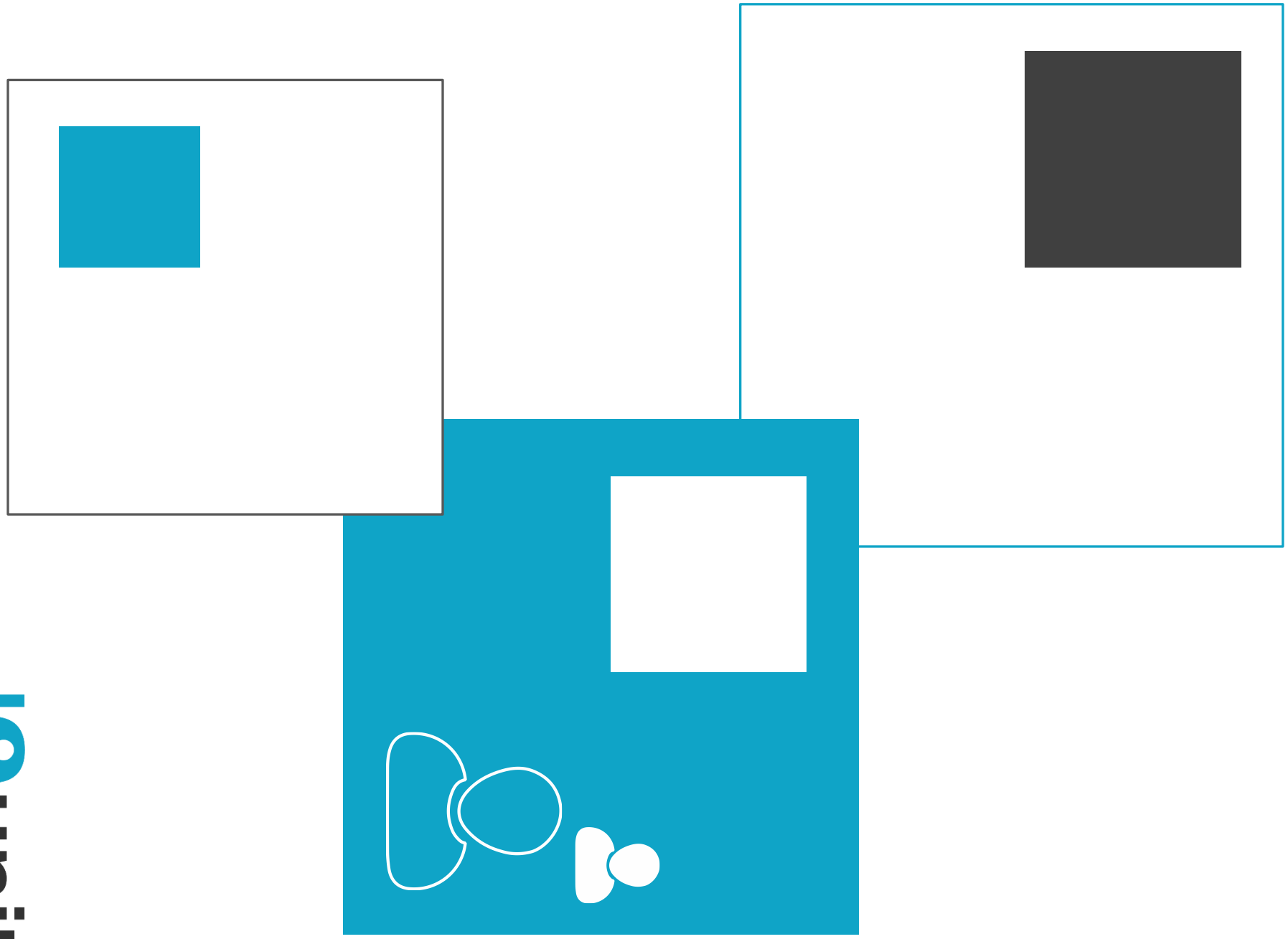


Essential Active Directory 2022 Workshop – ausführliche Informationen

Inhalt

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 begegenen.

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 Diretory 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 oparations (FSMO) und globaler Katalogserver
- Produkthistorie 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 (Enhanded Security Administrative Environment)
- Fine grainted 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 Ticktes
- 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

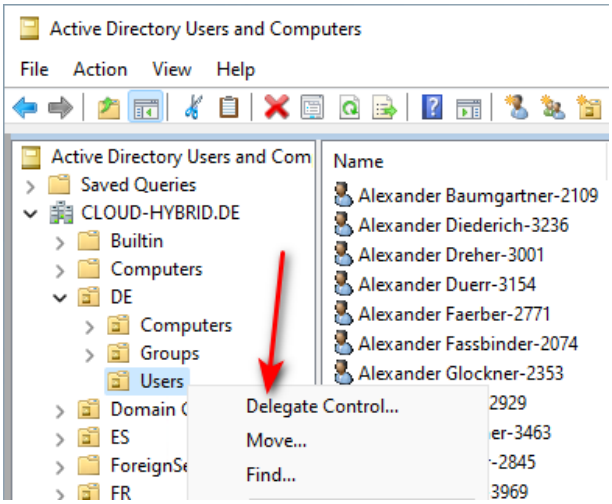
Active Directory Forest Functional Level 2016

- 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

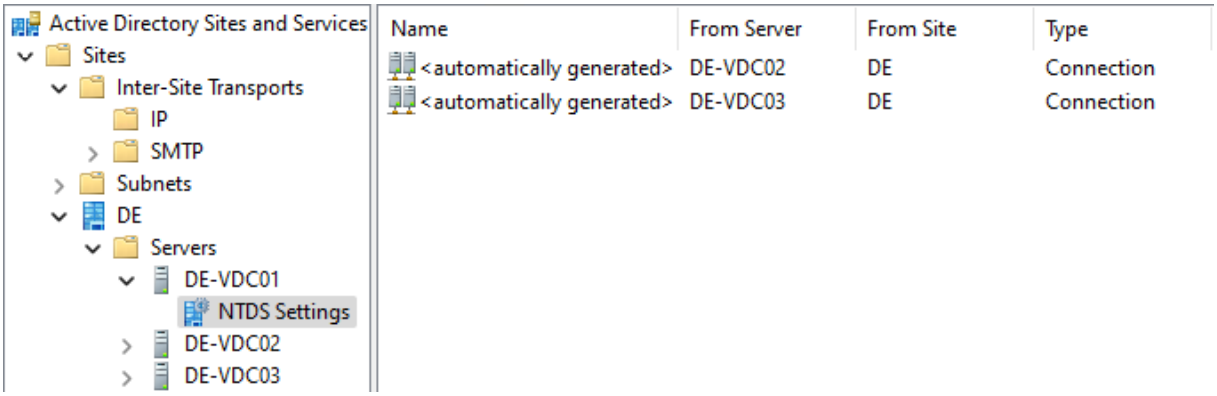
Active Directory Backup und Restore

- 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

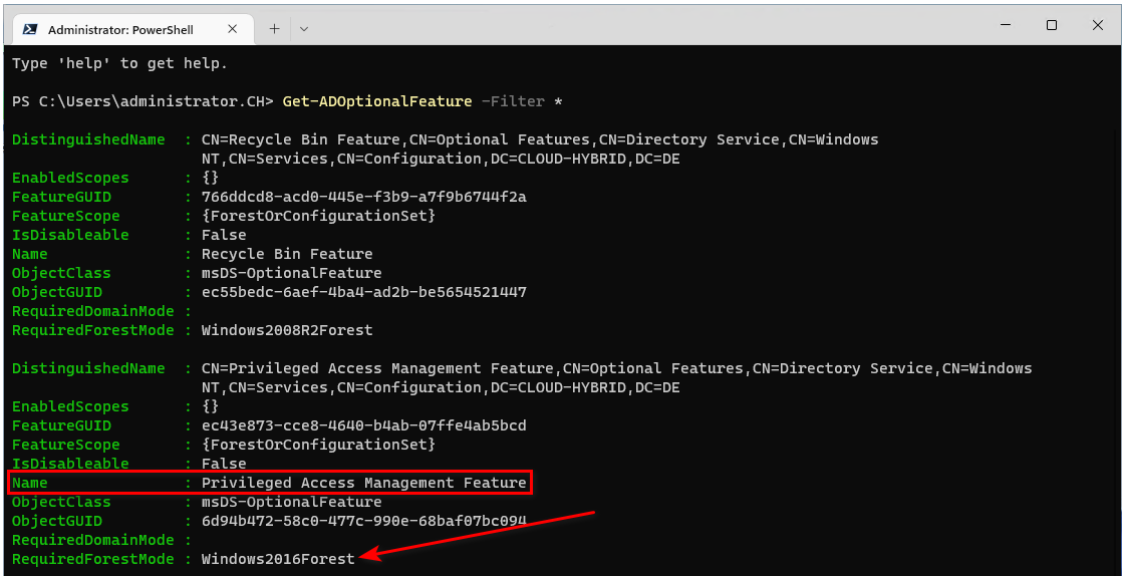
4. Bildergallerie aus den Unterlagen



Delegate Control – delegieren von Aufgaben



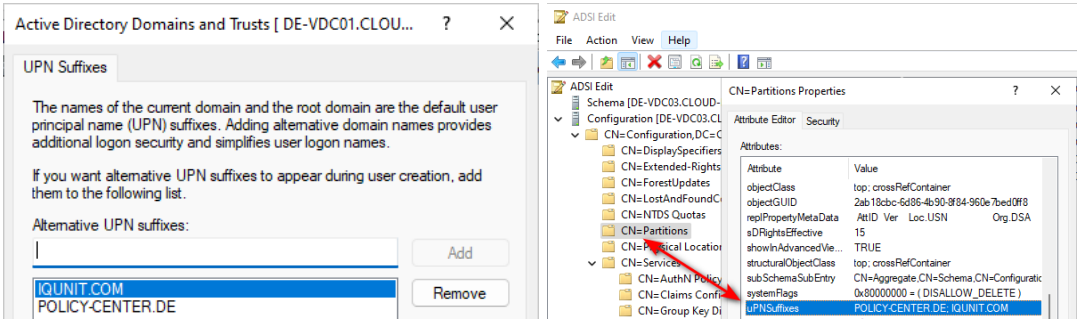
Sites and Services – der KCC hat gerechnet

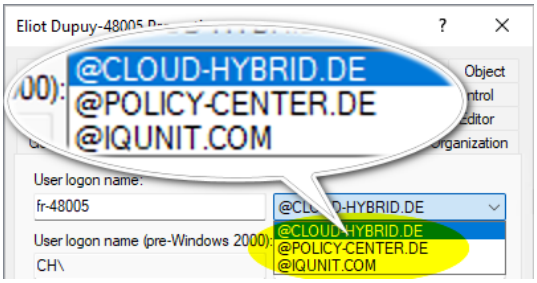


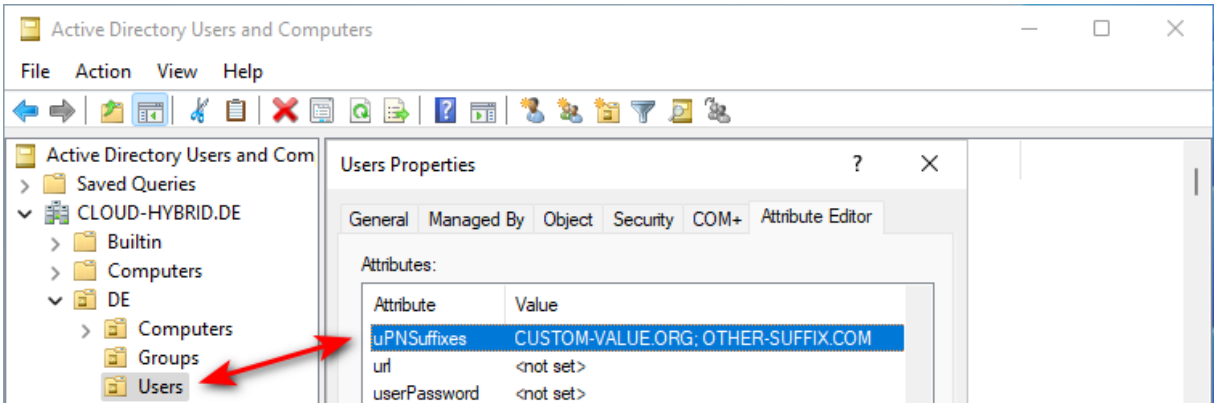
Active Directory PAM-Feature

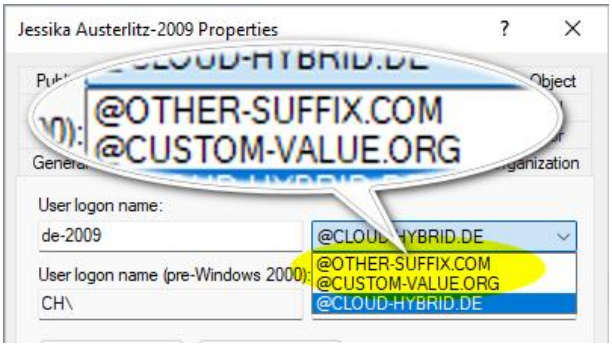
```
Administrator: PowerShell
PowerShell 7.2.6
Copyright (c) Microsoft Corporation.

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 Identfier – GUID

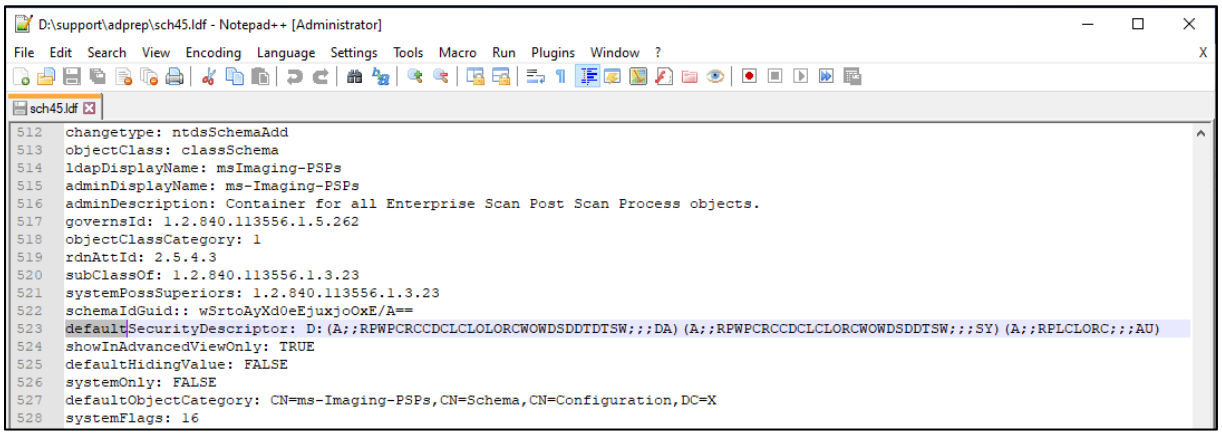




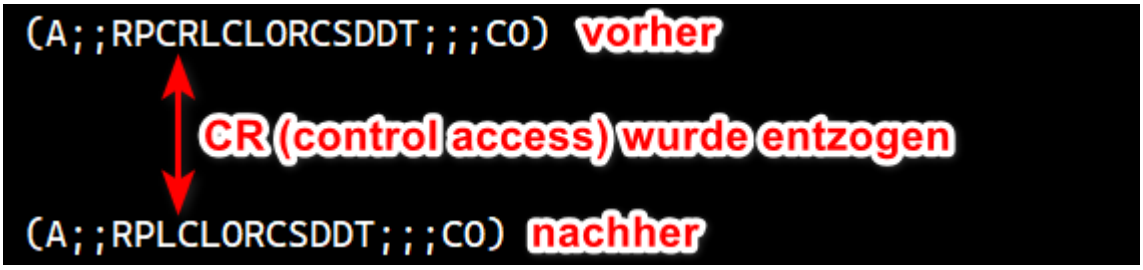




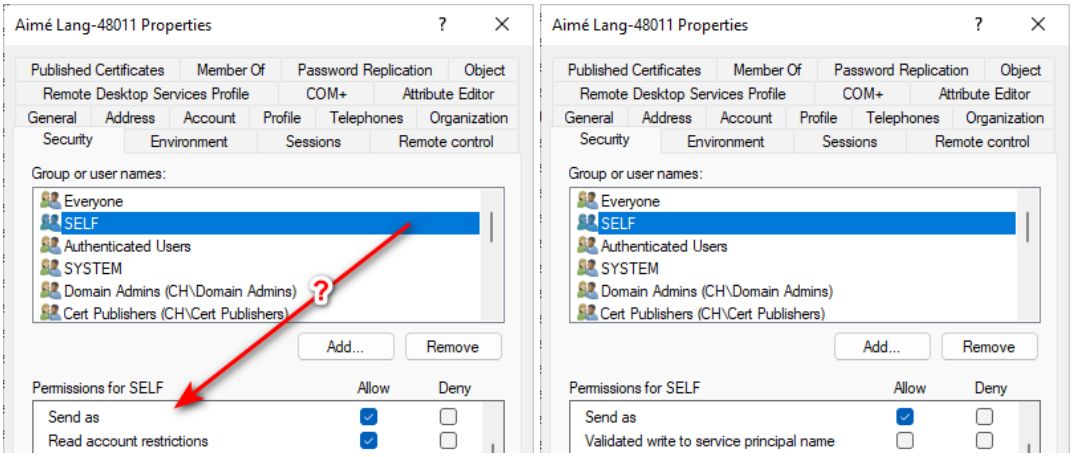
Suffixe der User Principal Names



SDDL – Default Security in einer Schema.ldf-Datei



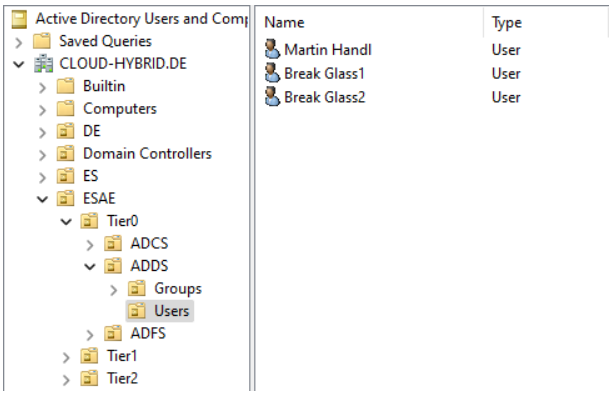
SDDL-Anpassungen wegen LAPS



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



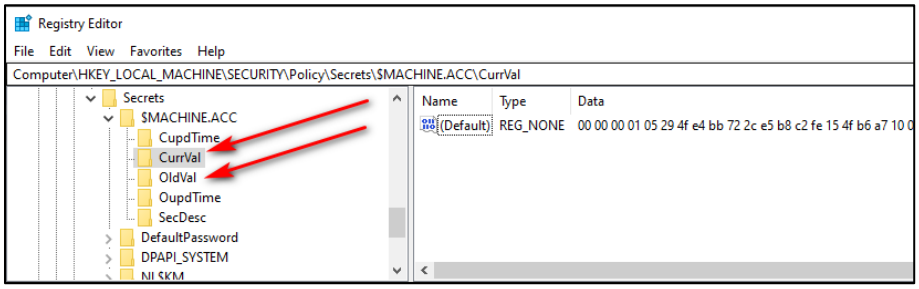
ESAE-Struktur

```
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…
```

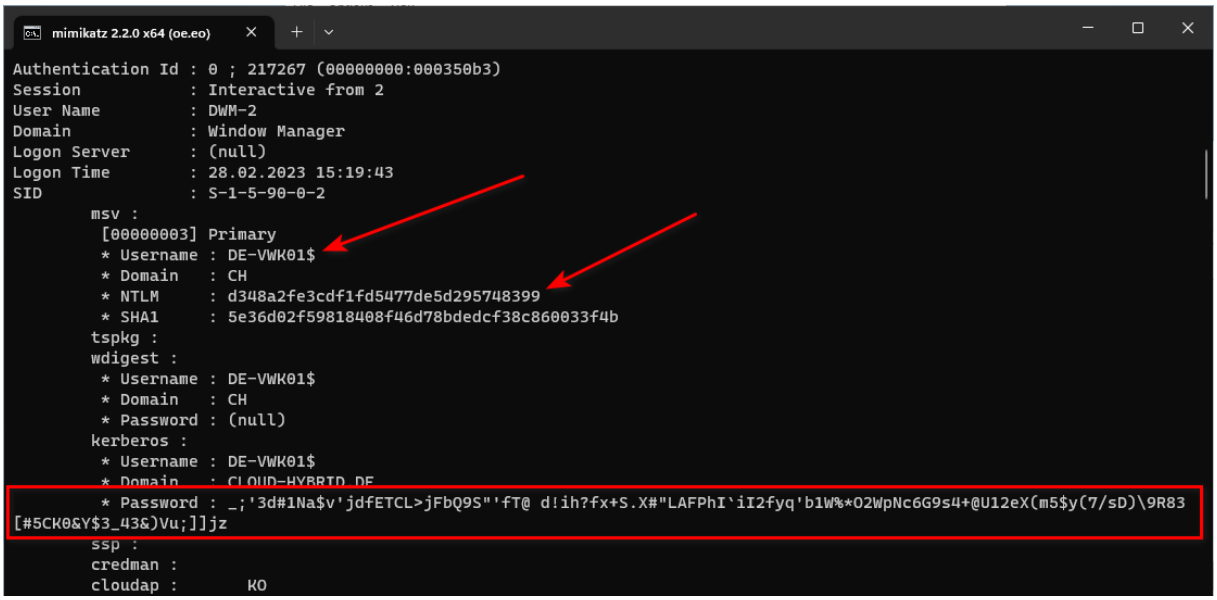
```
Administrator: PowerShell
Administrator: Windows Powe
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

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...
```

PowerShell-Profilpfade und Windows PowerShell-Profilpfade

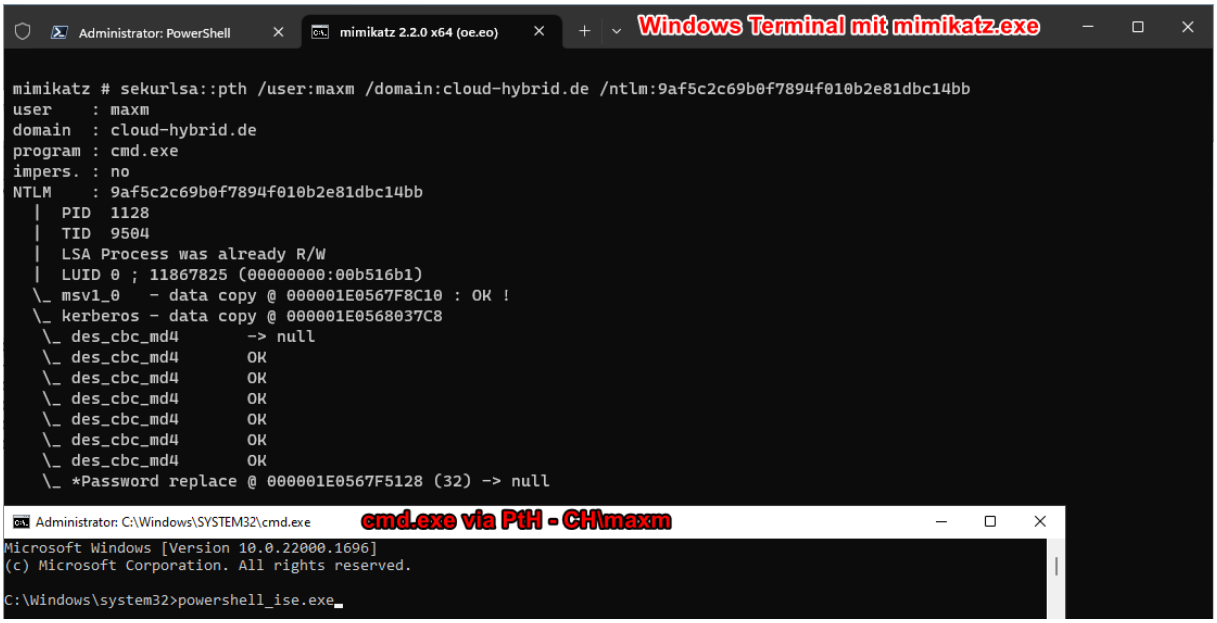
Visual Studio Code – PowerShell oder Windows PowerShell?



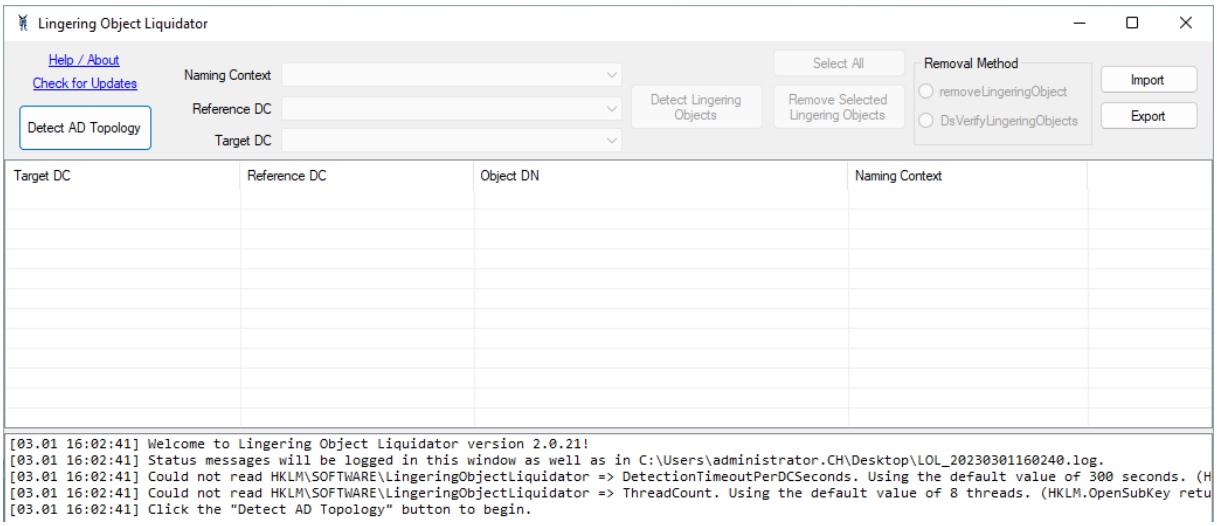
Computerkennwort



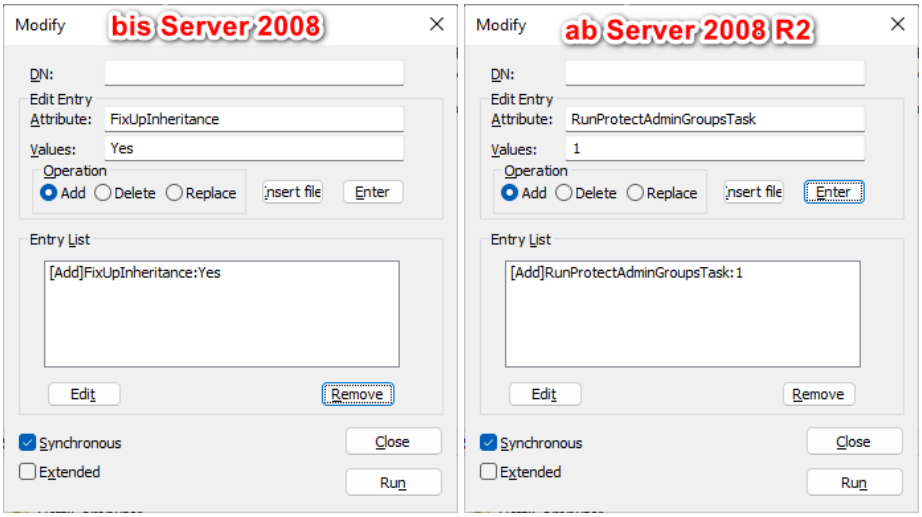
Hash des Computerkennwortes und Klartextkennwort



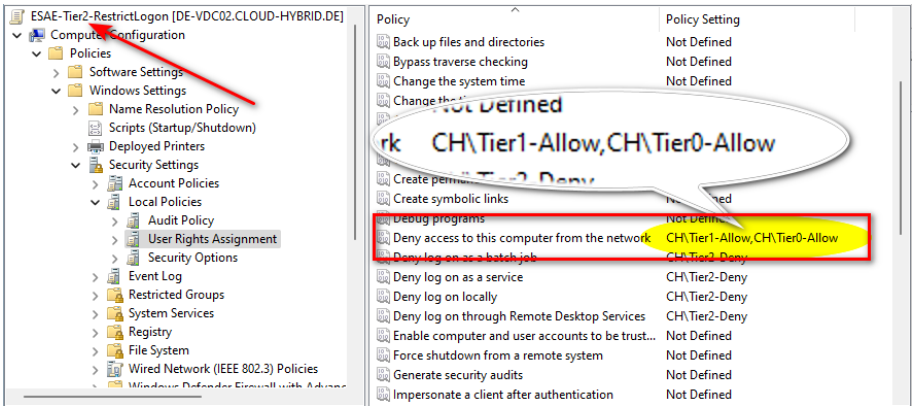
Mimikatz und Hashes



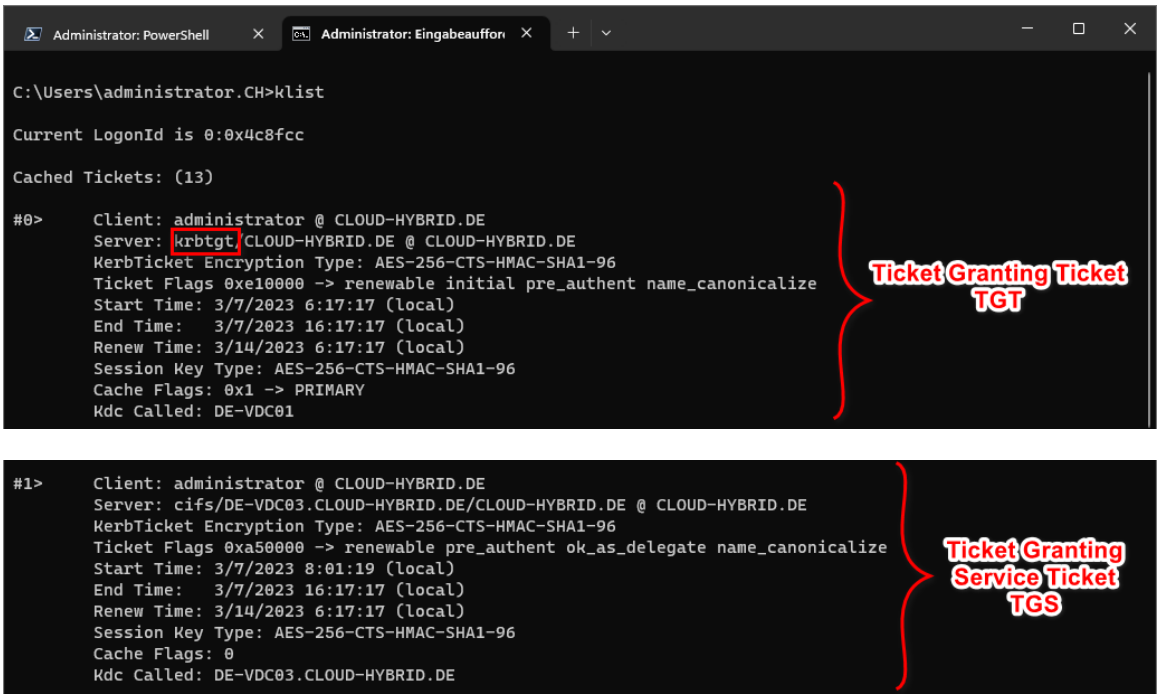
Microsoft LOL – Lingering Object Liquidator



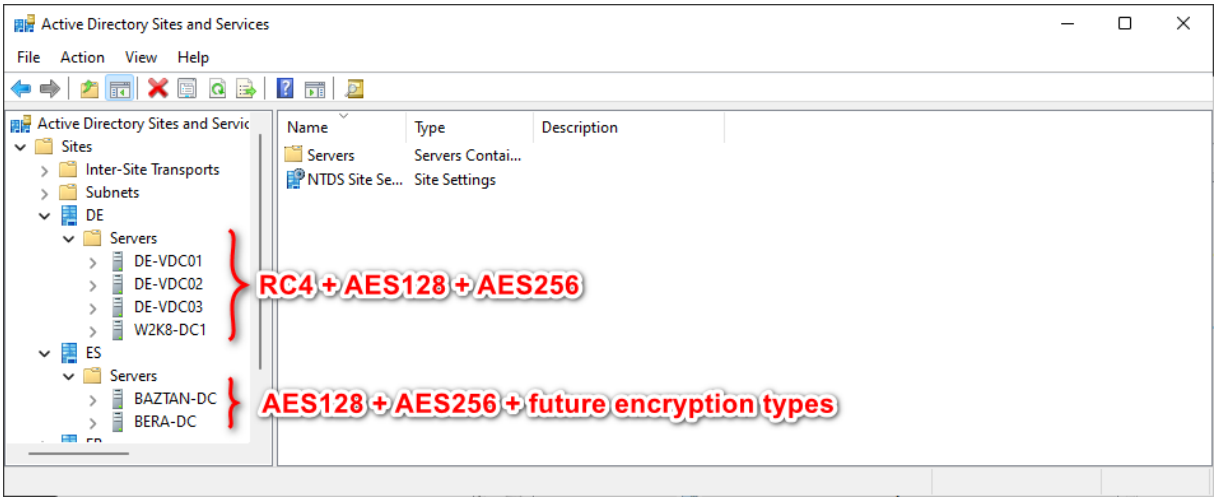
SDProp-Start



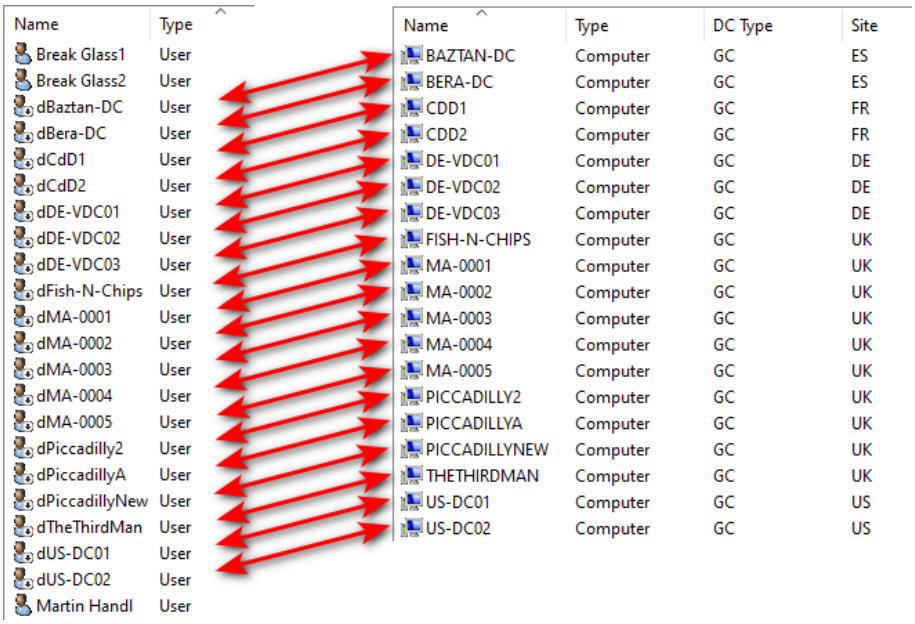
Tiering-Policy – Tier2

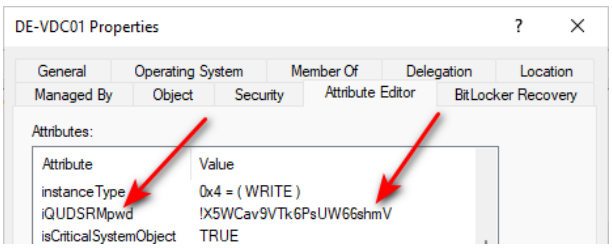


Ticket Granting Ticket und Ticket Granting Service Ticket

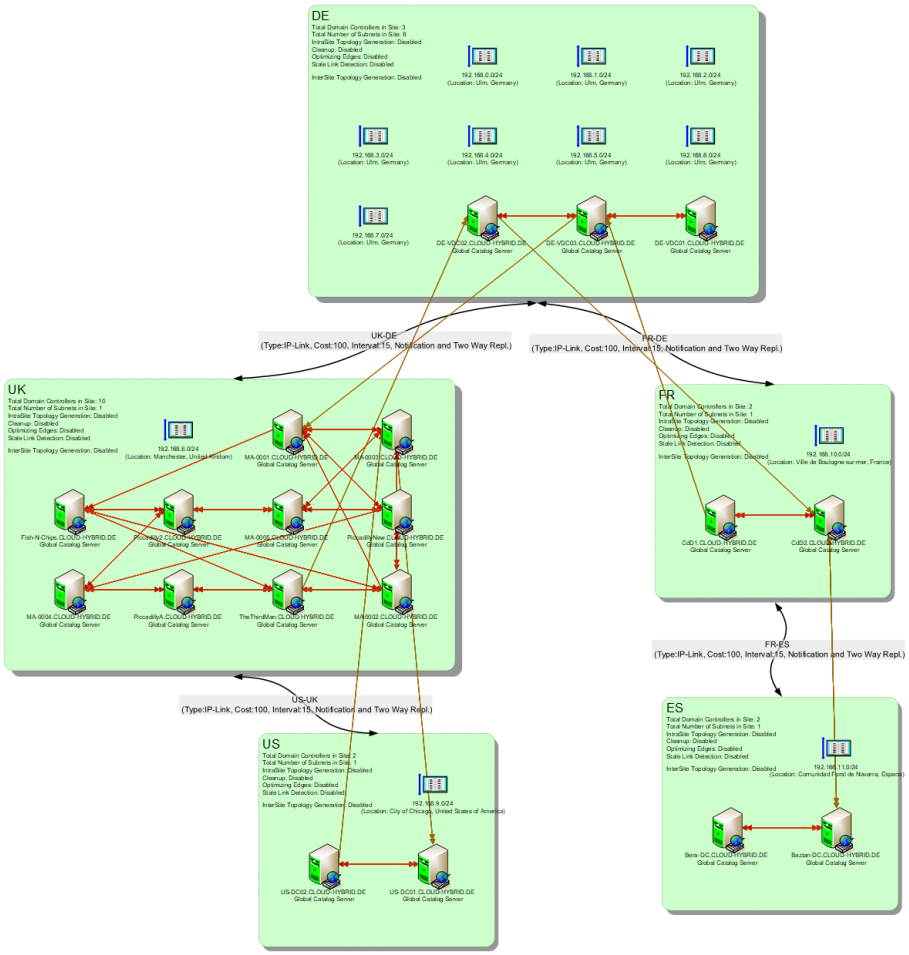


Kerberos encryption types – pro Site definiert

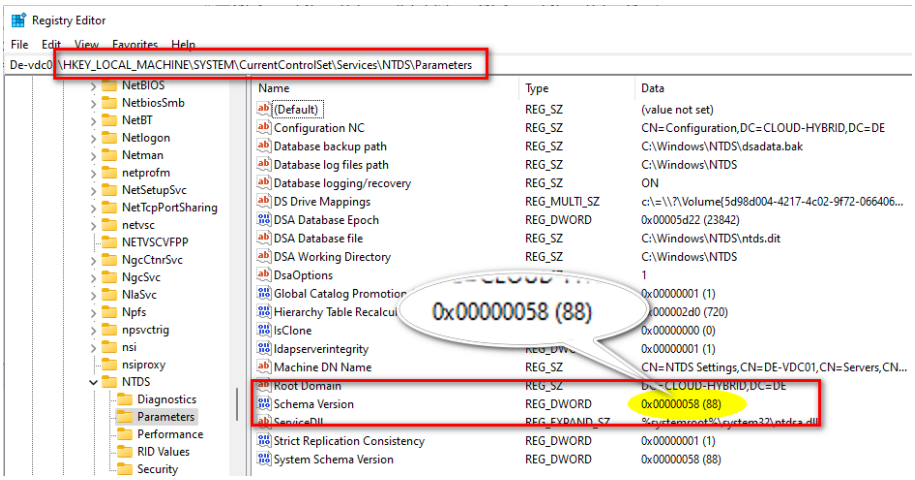




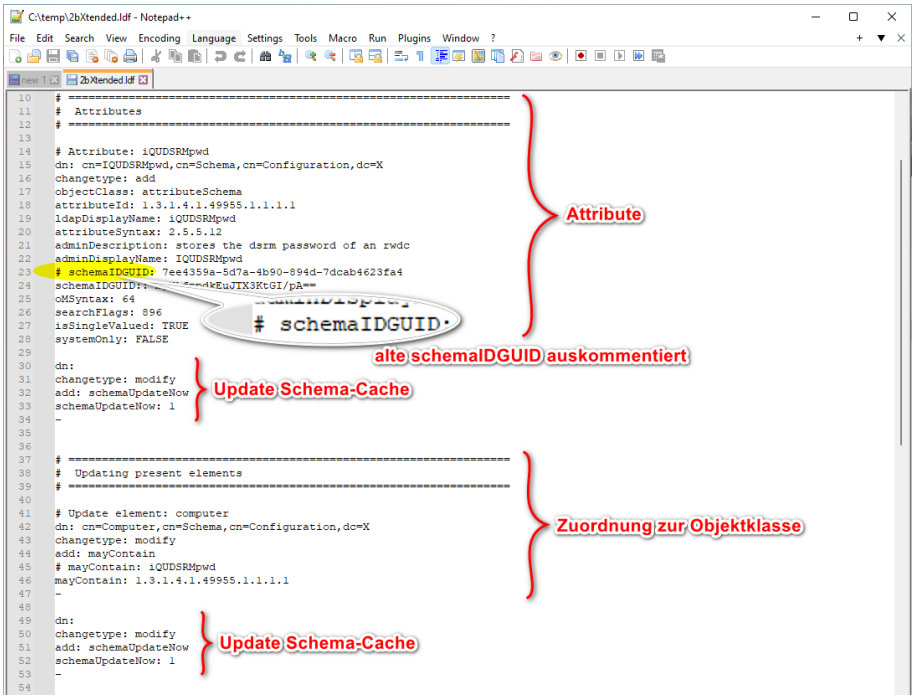
DSRM-Referenz-User im Active Directory – LAPS für Domain Controller



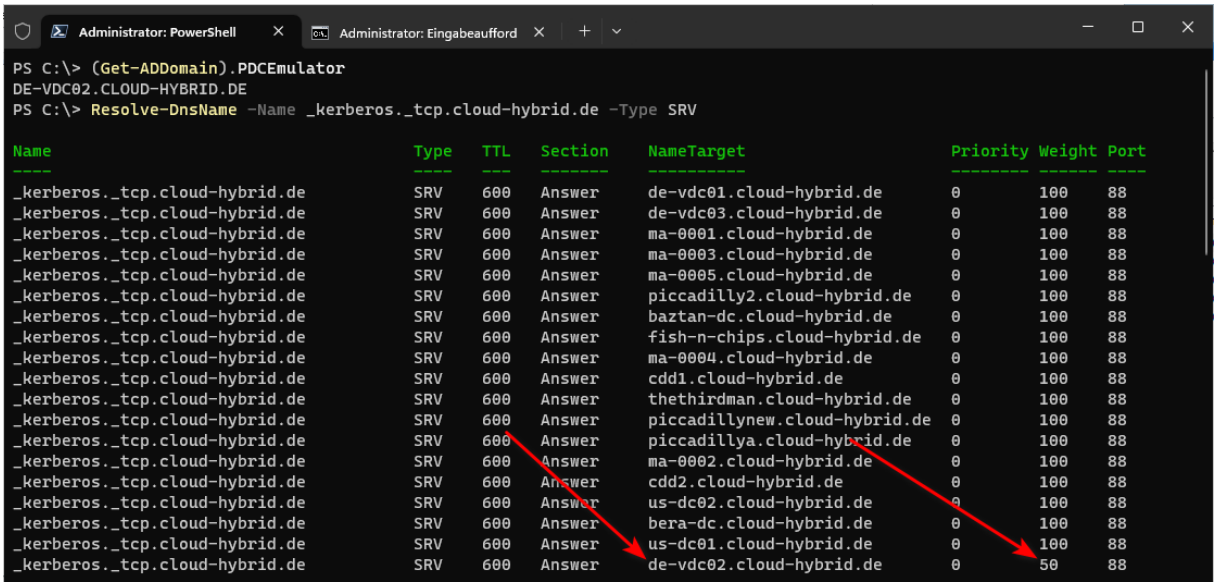
ADTD – Active Directory Topology Generator



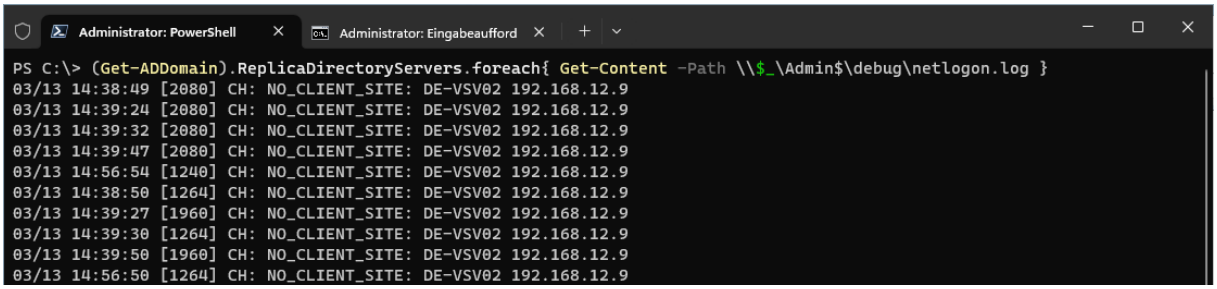
Schema-Version 88



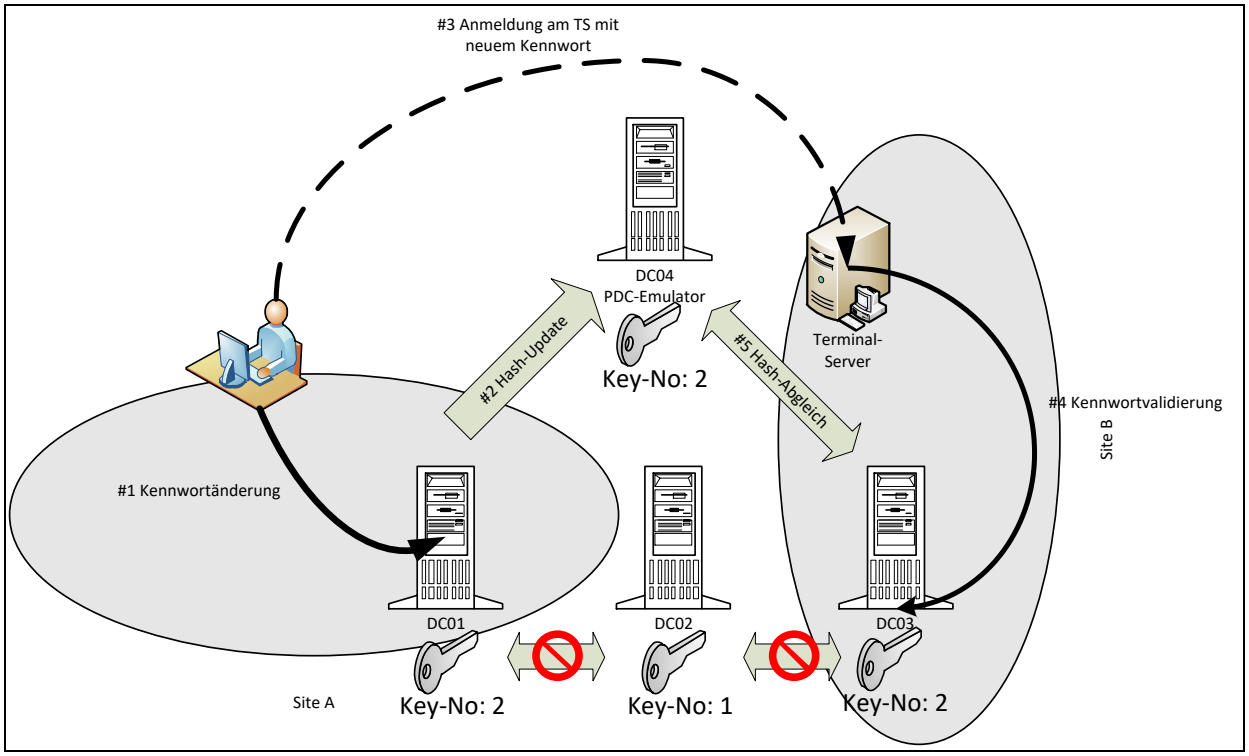
Schemaerweiterung per LDIF-Datei



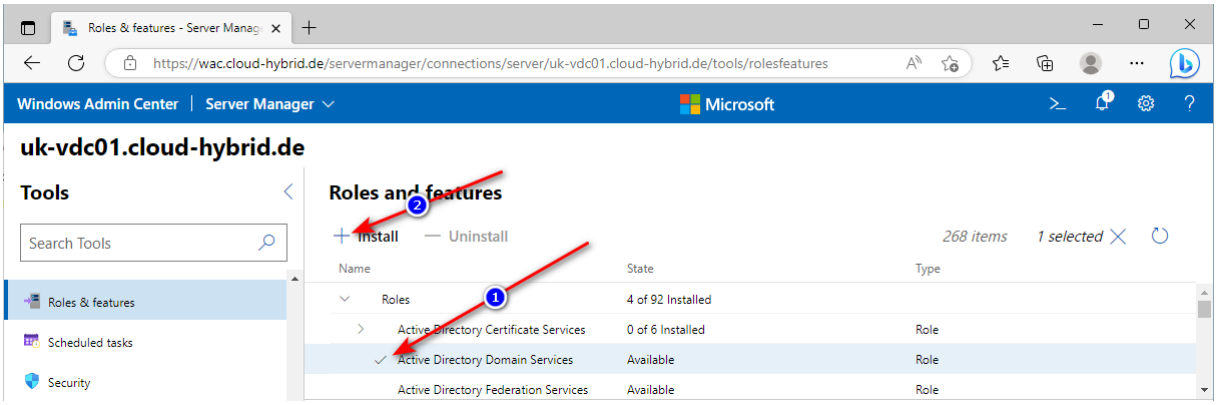
Gewicht eines DC.



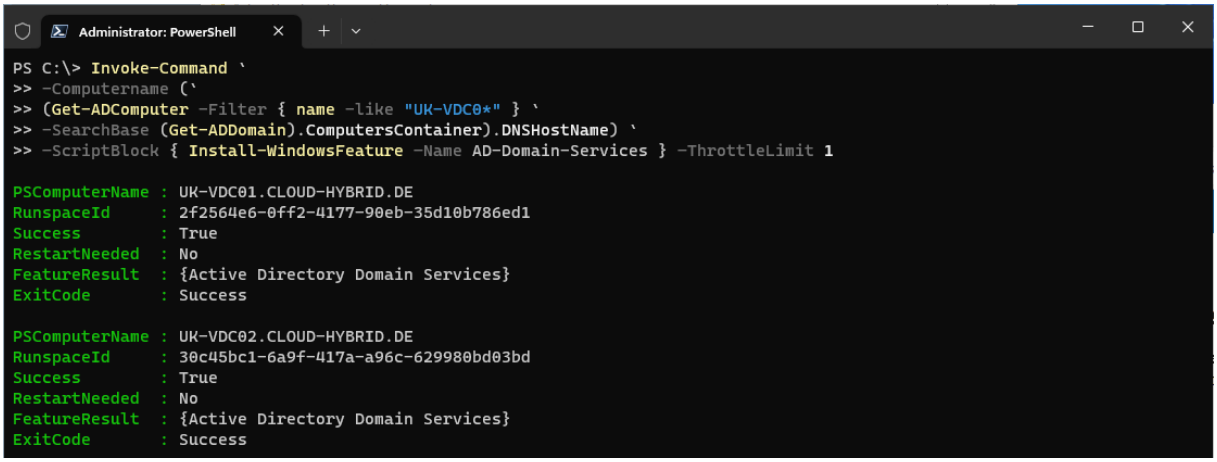
NO_CLIENT_SITE – IP-Subnetz keiner Site zugeordnet



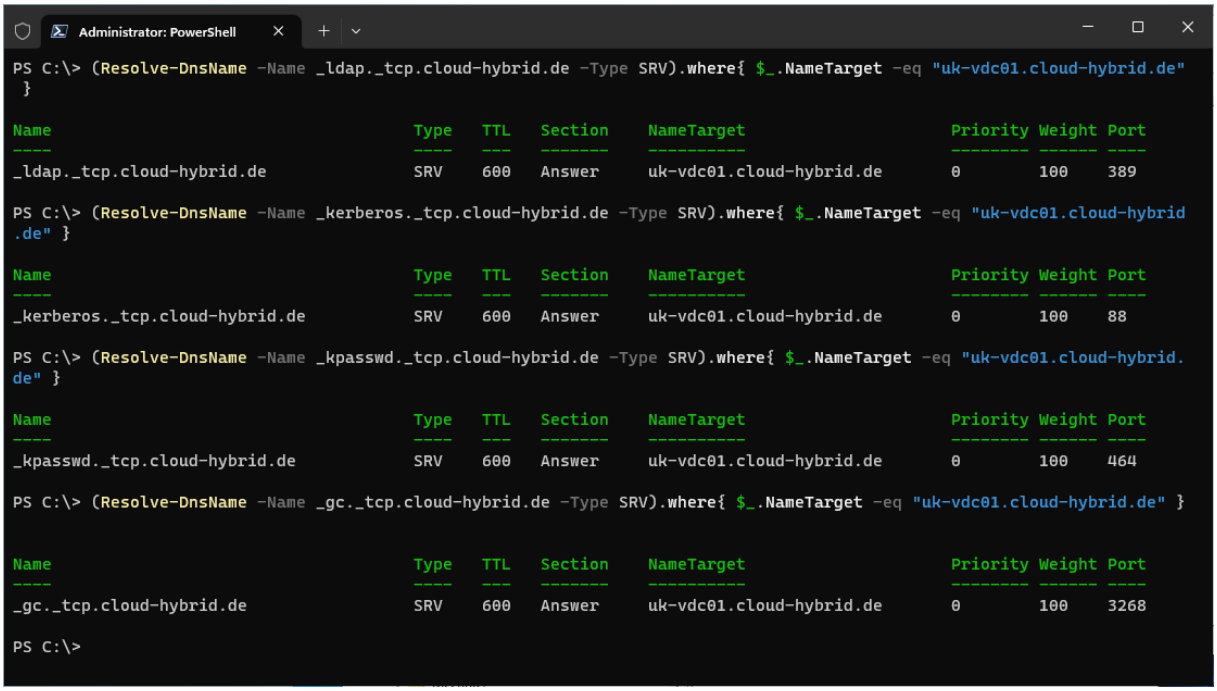
PDC-E ist der Master-Key-Server



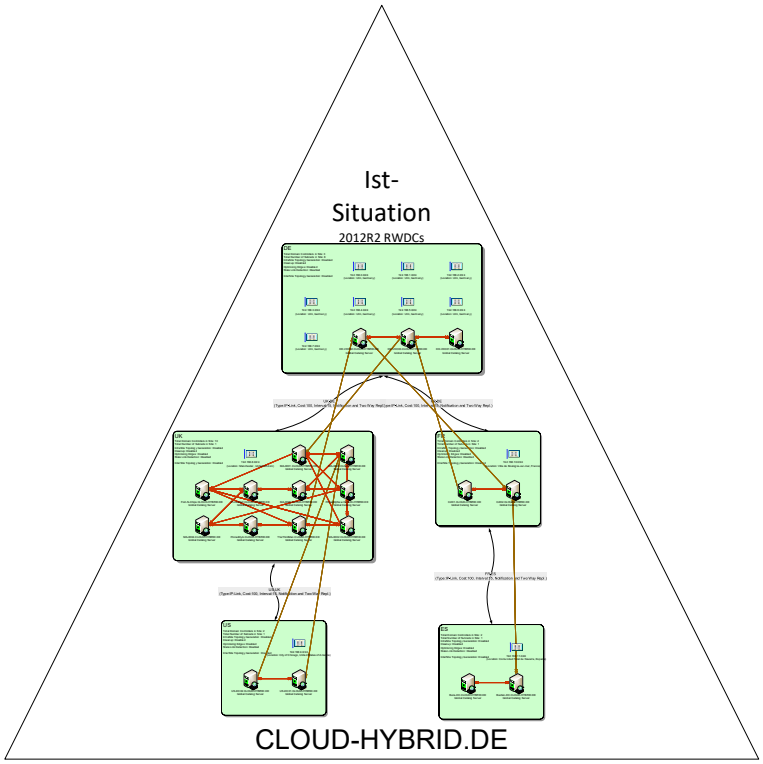
Windows Admin Center (WAC) zur Rolleninstallation nutzen.

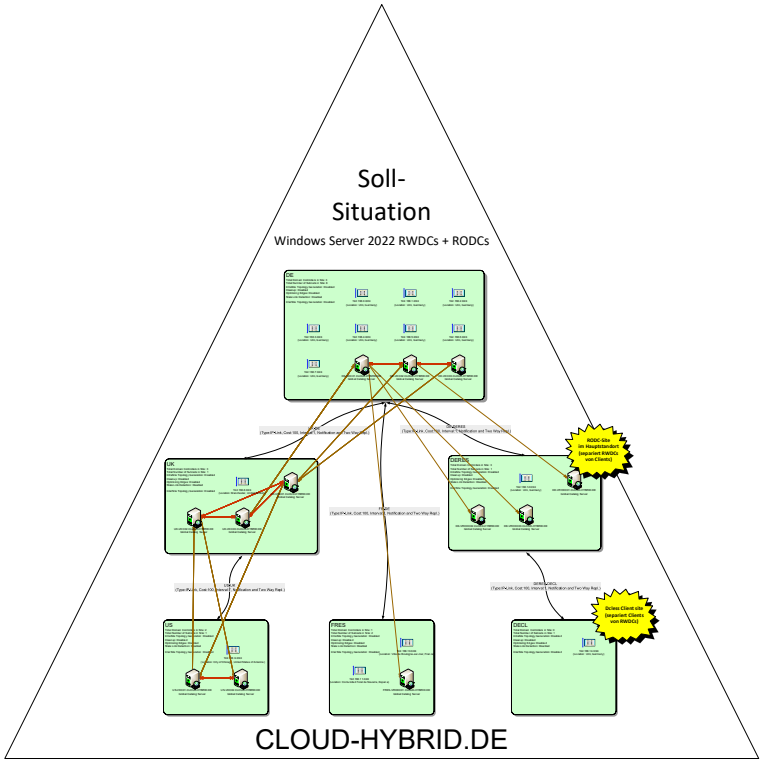


PowerShell-Remoting zur Rolleninstallation nutzen

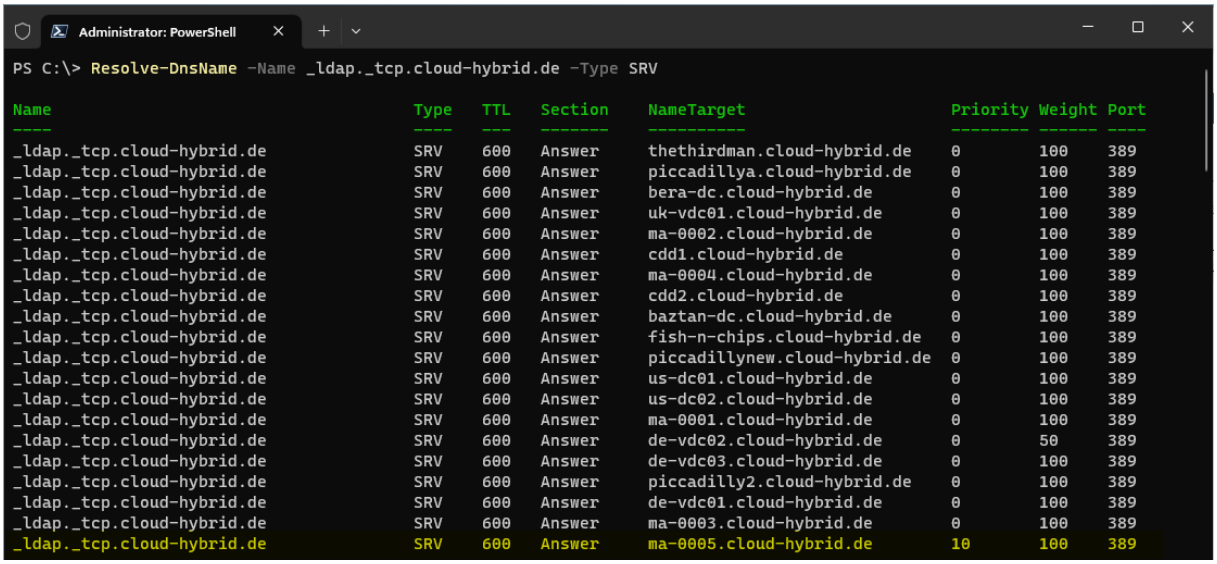


SRV-Einträge im DNS

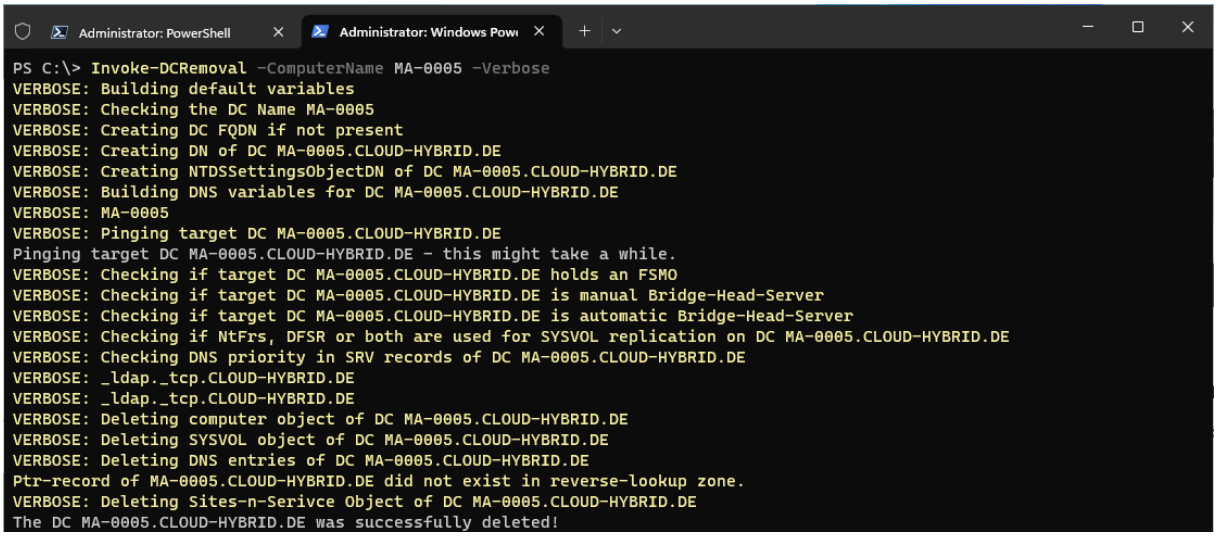




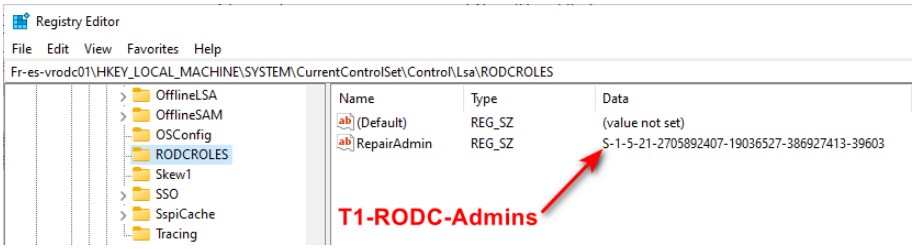
Ist-Situation und Soll-Situation



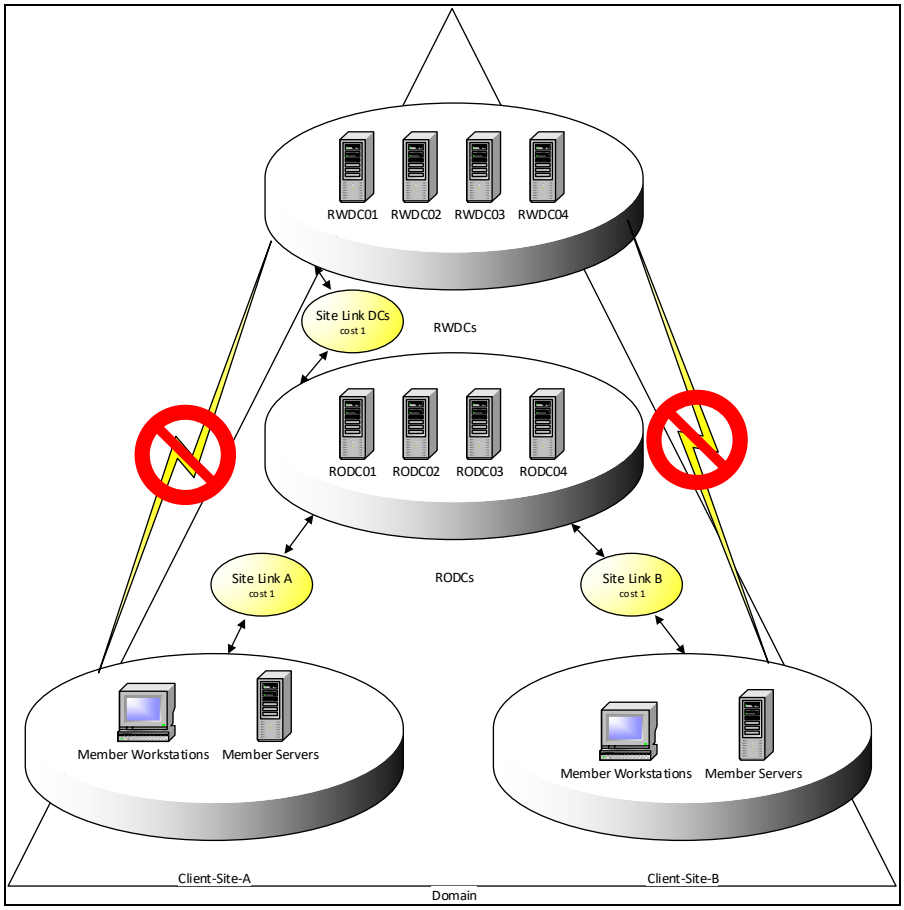
Priorität via Windows PowerShell setzen



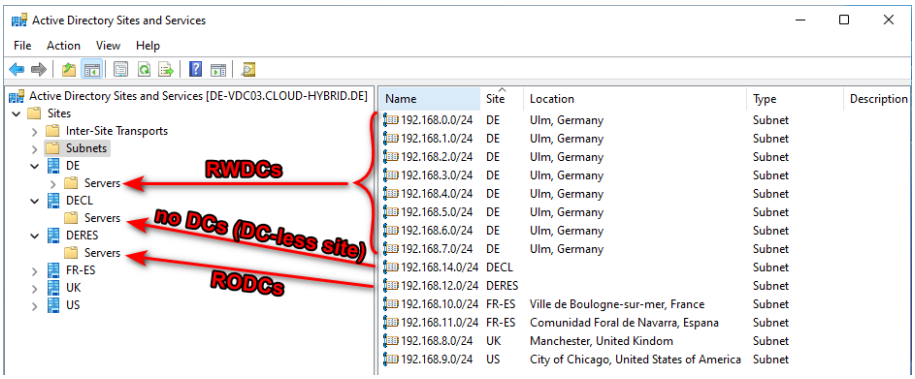
Domain Controller per Windows PowerShell entfernen



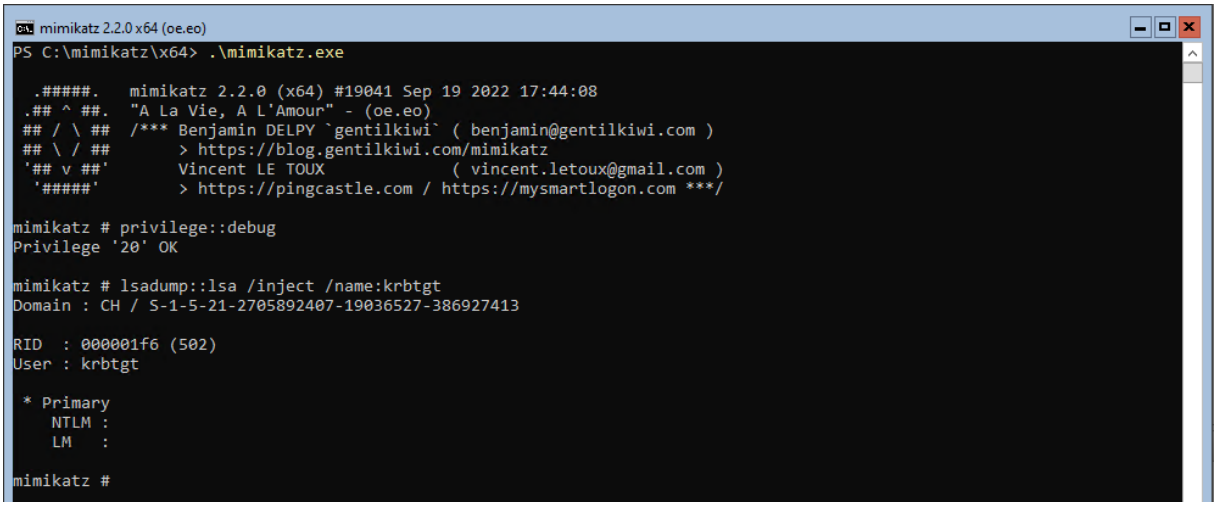
RODC-Admins



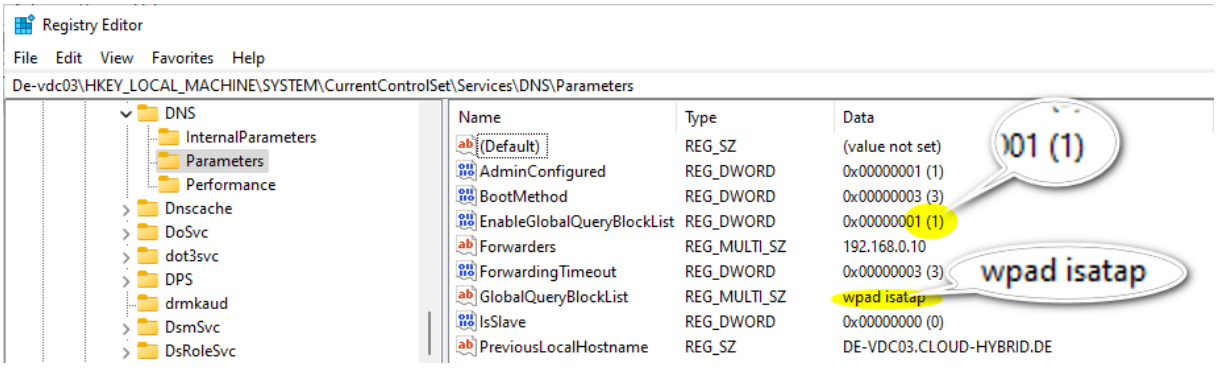
RODC als Front-End-DC



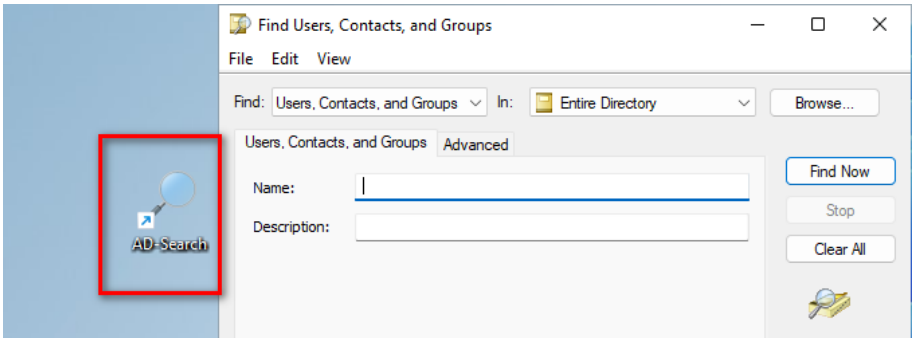
Umsetzung in den Sites



Kein Hash vom krbtgt auf einem RODC

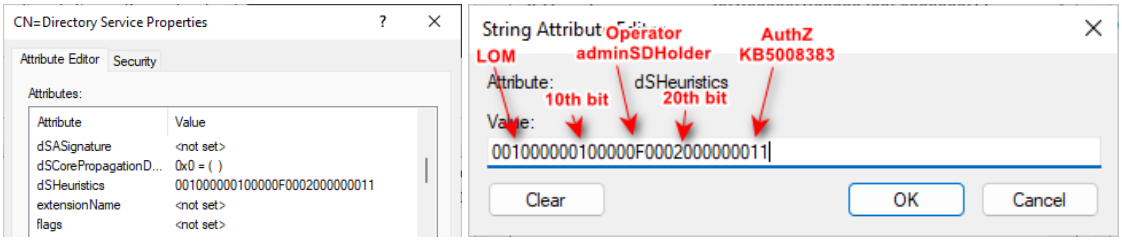


Global query block list im DNS

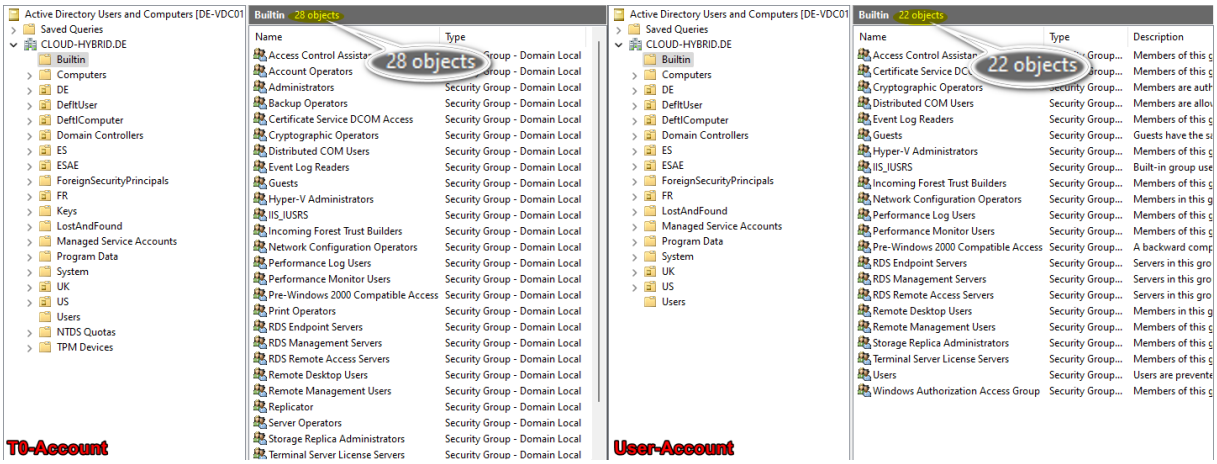


Suchen im AD vom Desktop aus – keine RSAT erforderlich

LDAP_MATCHING_RULE_IN_CHAIN um Gruppenmitgliedschaften festzustellen

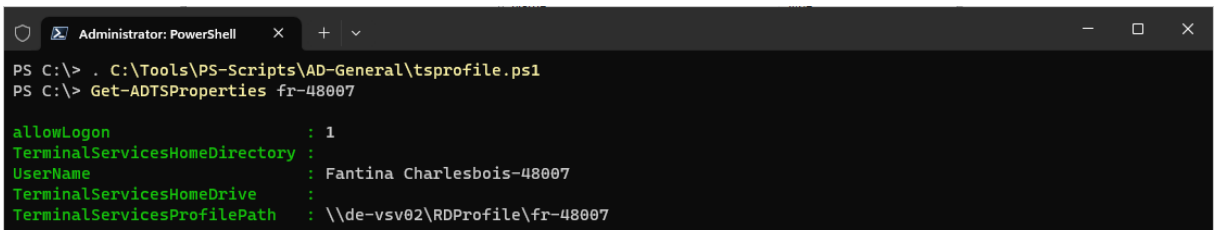


dSHeuristics



List Object Mode versteckt sensitive Konten

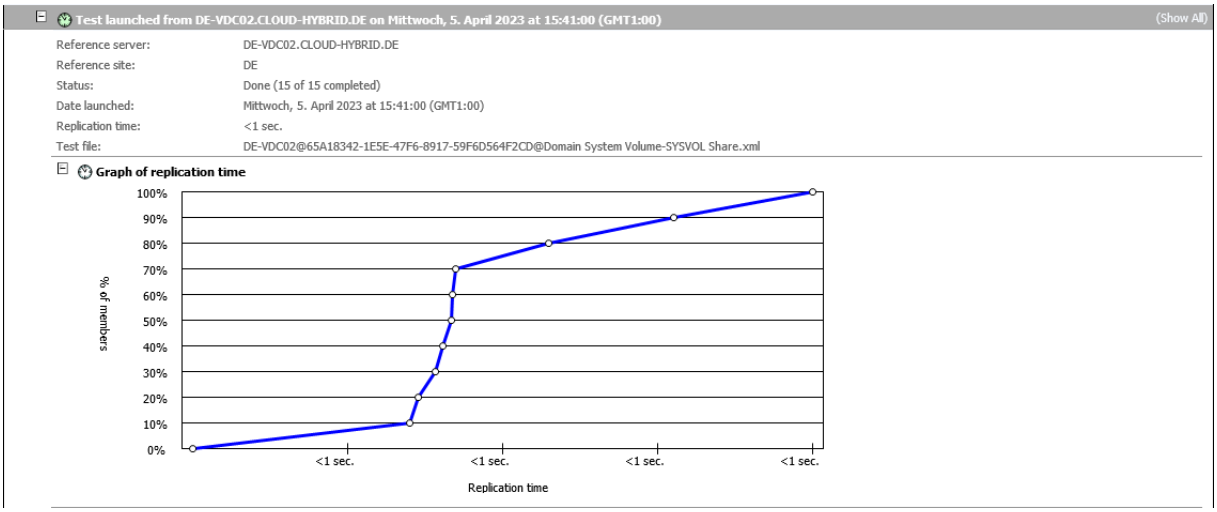
```
PACKSUBBSSOHCtxCfgPresent匱豉戦ぢCANBSSOH
CtxCfgFlags1〜てぐ＃DC2BSSOHCtxShadow▯〜〜〜〜*STXSOH
CtxMinEncryptionLevel□ <SOH
CtxWFProfilePath捧捧佗鼈摭圾ペッ圾 / ㈱捧㈱仗 \ ㈹祖笙恚掘鼈捧笙㈹摭仇
令 / / 嬢〜"xSOH
CtxWFProfilePathW捧〜捧〜佗〜鼈〜摭〜圾〜ペッ〜圾〜 / 〜㈱〜捧〜㈱〜仗
〜 \ 〜㈹〜祖〜笙〜恚〜掘〜鼈〜捧〜笙〜㈹〜摭〜仇〜令〜 / 〜 / 〜嬢〜〜〜〜
```



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
```

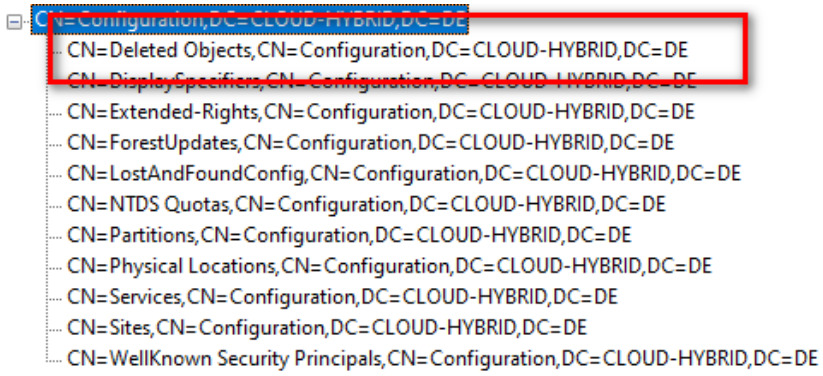
ADWS Query Policy



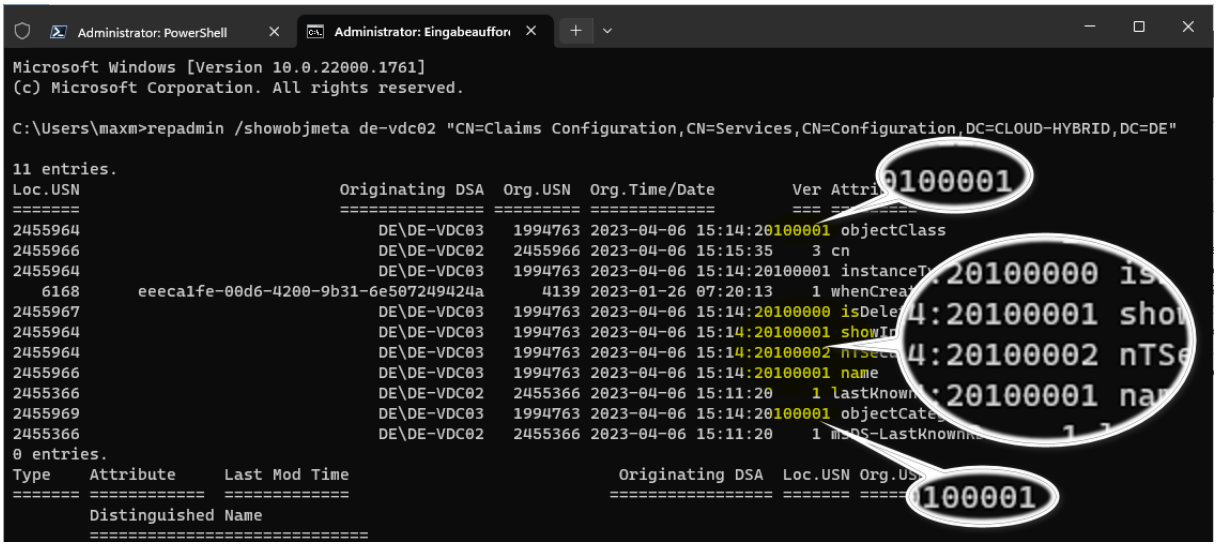
SYSVOL Propagation Time

```
Administrator: PowerShell | Administrator: Windows Powe
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:\>
```

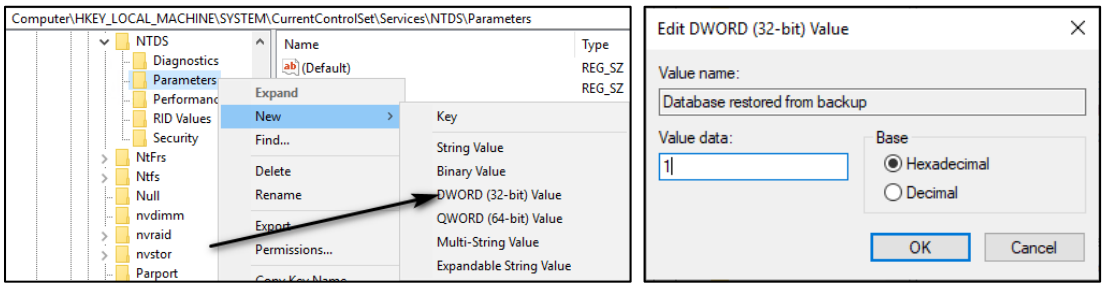
DFS-R Autorisierende Wiederherstellung



Deleted Objects



Authoritative Restore im AD



Database restored from backup – Lösung per Hand