MC2MC

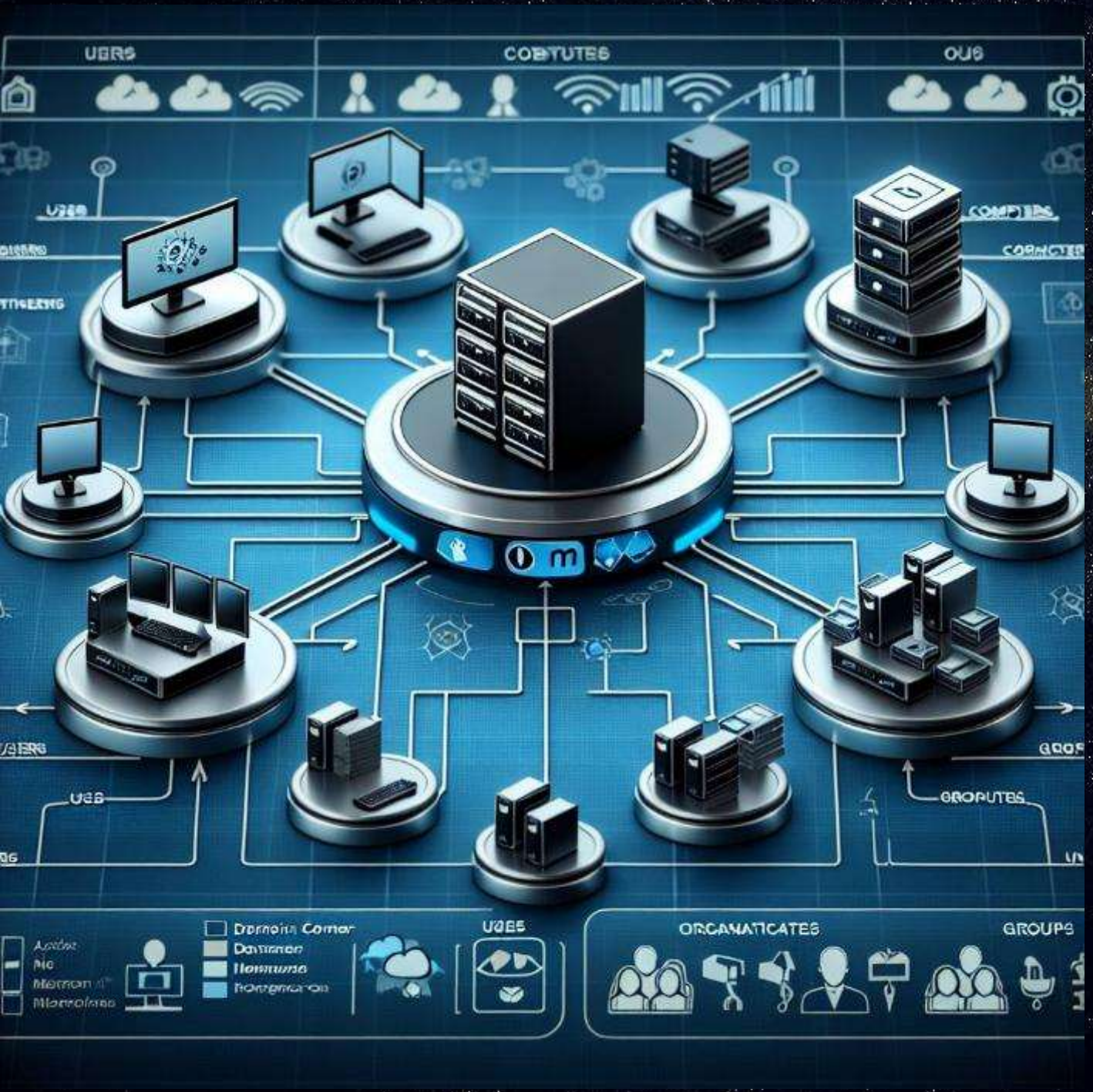
What’s new in Active Directory 2025

Erwin Derksen

DerkIT

Intro

That bit of structure & clarity


USERS
COMPUTERS
OUS
USERS
GROUPS
USERS
GROUPS
ORGANIZATIONS
GROUPS

AD by AI

The FUTURE of AD in AI

8 x Relevant New

3+1 x Core Security Tip

2,5 x Upgrading


After the session


Active Directory
“Still going strong” Revival Tour

Relevant New Features

Finally, since 2016!


Hotpatch
Only
SECURITY
updates

Hotpatch, (still) requiring ARC…

Monthly security patches (no reboot)

Quality & Feature updates quarterly (at baseline)

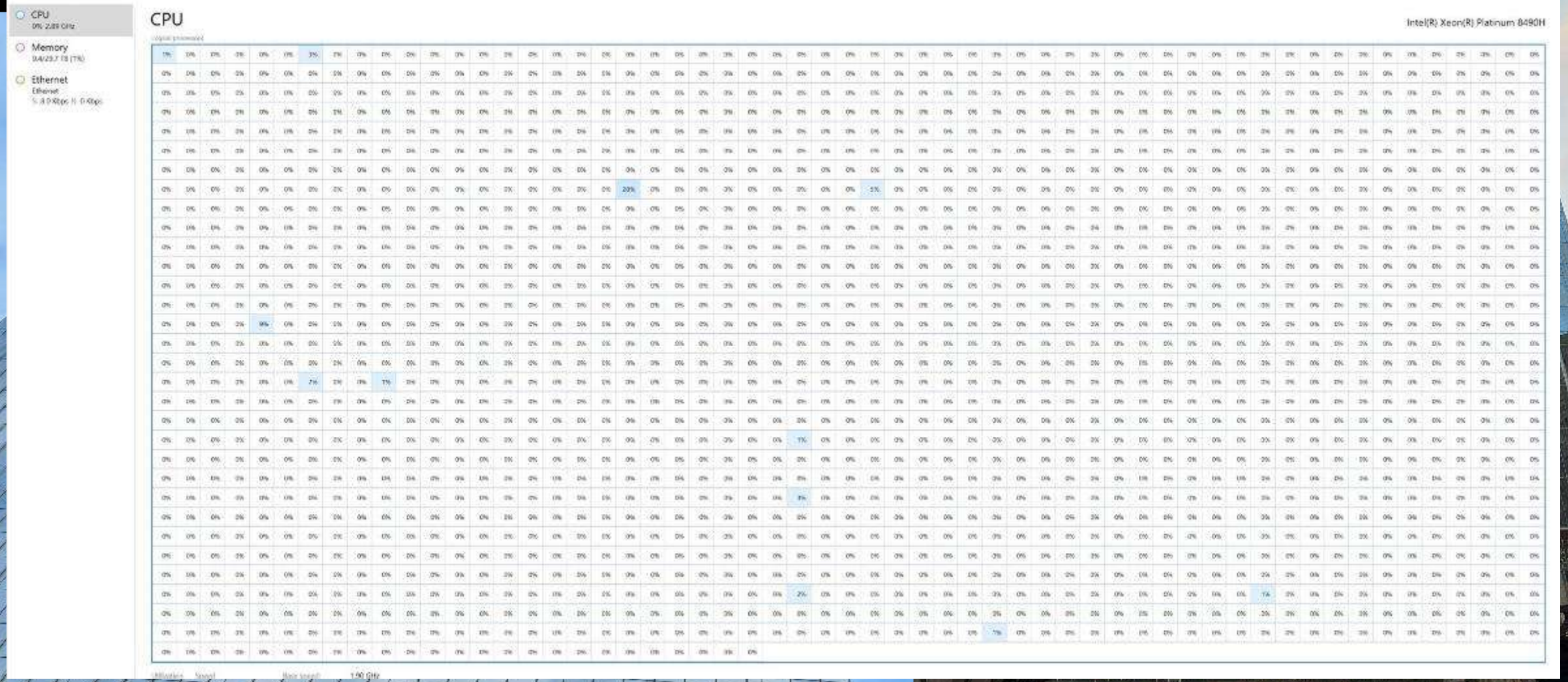
Reboots at Baseline

.NET updates & Drivers not part of Hotpatching

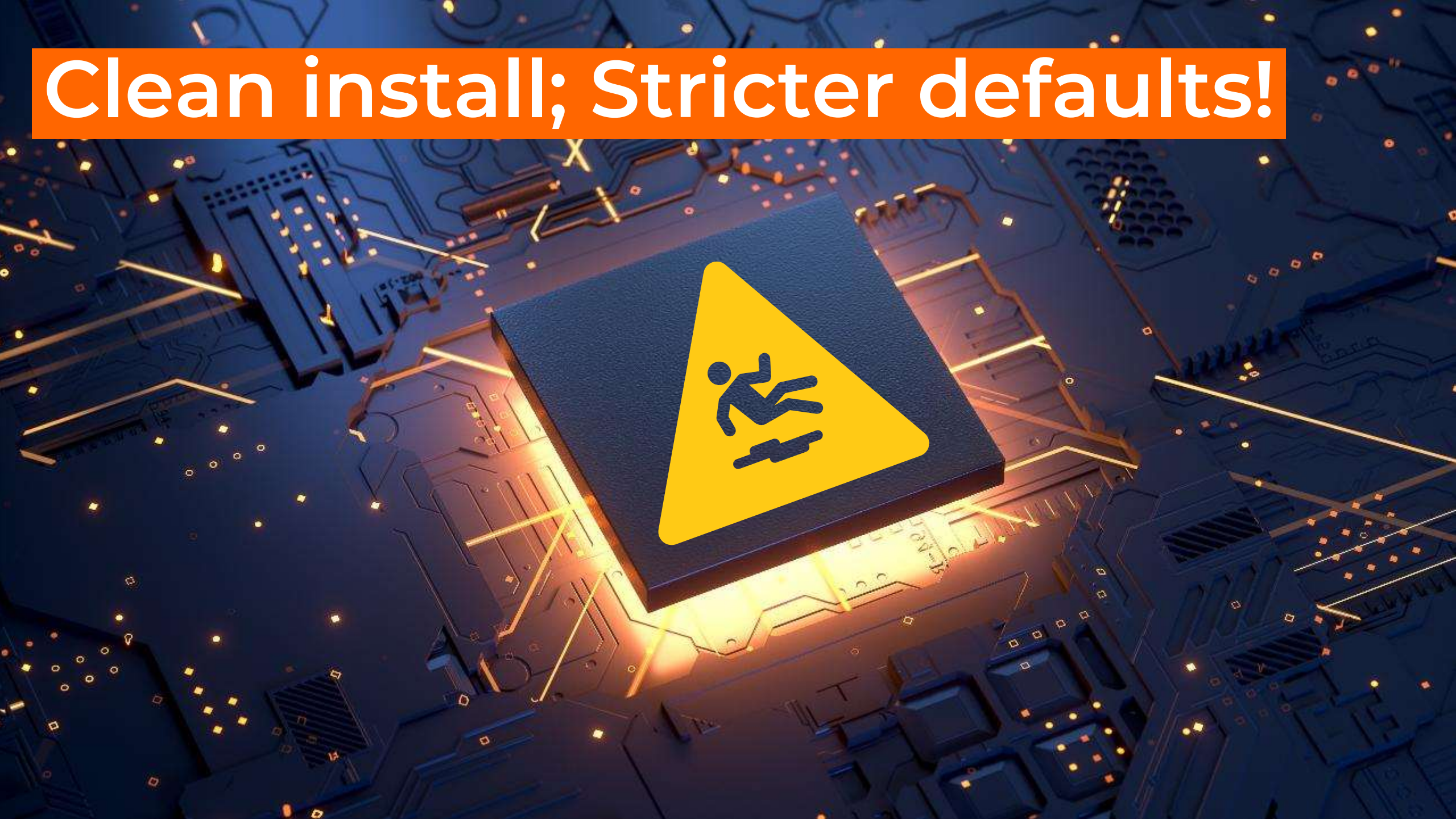
[Baseline] **[Baseline]** **[Baseline]**

No Reboot Reboot

scalable



Clean install; Stricter defaults!

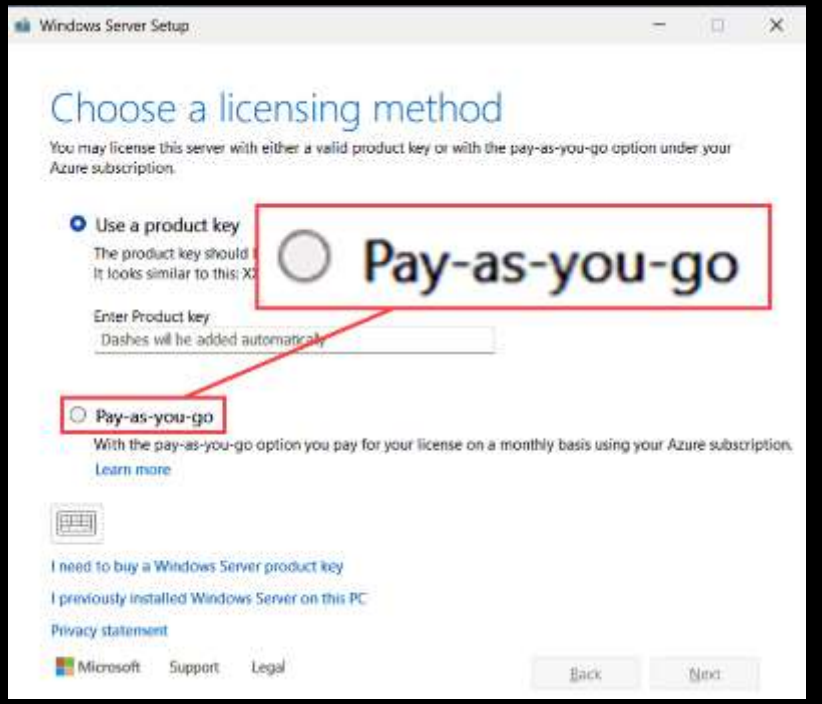


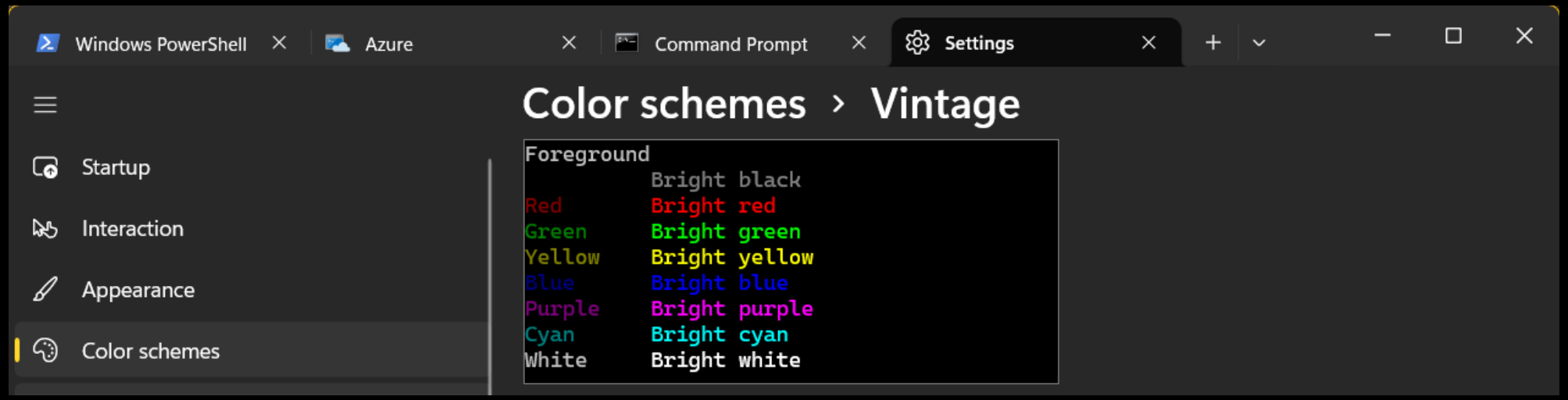
SMB Authentication Rate Limiter

"5 minutes becomes 50 hours"

Other

Windows 11





New 2025 Domain & Forest functional Level

JET Database NTDS.DIT 8k → 32k pages

Enable 32k mode in 2025 functional level

```
Get-ADObject -LDAPFilter "(ObjectClass=nTDSDSA)" -SearchBase
"CN=Configuration,DC=YOURDOMAIN,DC=ADDOM"
-properties msDS-JetDBPageSize | FL distinguishedName,msDs-
JetDBPageSize
```

Check your restore capacity…

```
$params = @{
Identity = 'Database 32k pages feature'
Scope = 'ForestOrConfigurationSet'
Server = ‘YOURDC'
Target = ‘YOURDOMAIN.ADDOM'
}
Enable-ADOptionalFeature @params
```

msDS-JetDBPageSize =

Null
= <Server 2022

8192
= 8k

32768
= **32k**


NTLM has to go….

Reducing NTLM Negotiation

Initial and Pass-Through Authentication Using Kerberos (IAKerb)

Local KDC

“Keepin’ it Kerb”

Other Improvements

- NUMA aware
- New Perfmon counters
- Random machine passwords used
- New DC ‘NETBIOS to UPN’ locator
- Replication Priority Boost
- WINS & MAILSLOTS deprecated

Security Improvements

LDAP support for TLS 1.3

Improved security for confidential attributes

LDAP prefers encryption by default

Kerberos support for AES SHA256/384

Changes to default behavior of legacy SAM RPC password change methods

Kerberos & PKINT support cryptographic agility

dMSA
gMSA

Managed Service Accounts

“Automated password management
and specific permission delegation.”

Erwin Derksen

- HEAO-BI, since 1999 in IT
- Only Pragmatic Projects
- Business and Technology
- Presentation skills
- **AD since AD exists**

DerkIT
ICT - Change - Communication

Erwin Derksen

- HEAO-BI, since 1999 in IT
- Only Pragmatic Projects
- Business and Technology
- Presentation skills
- **AD since AD exists**

DerkIT
ICT - Change - Communication

Core Security Tips

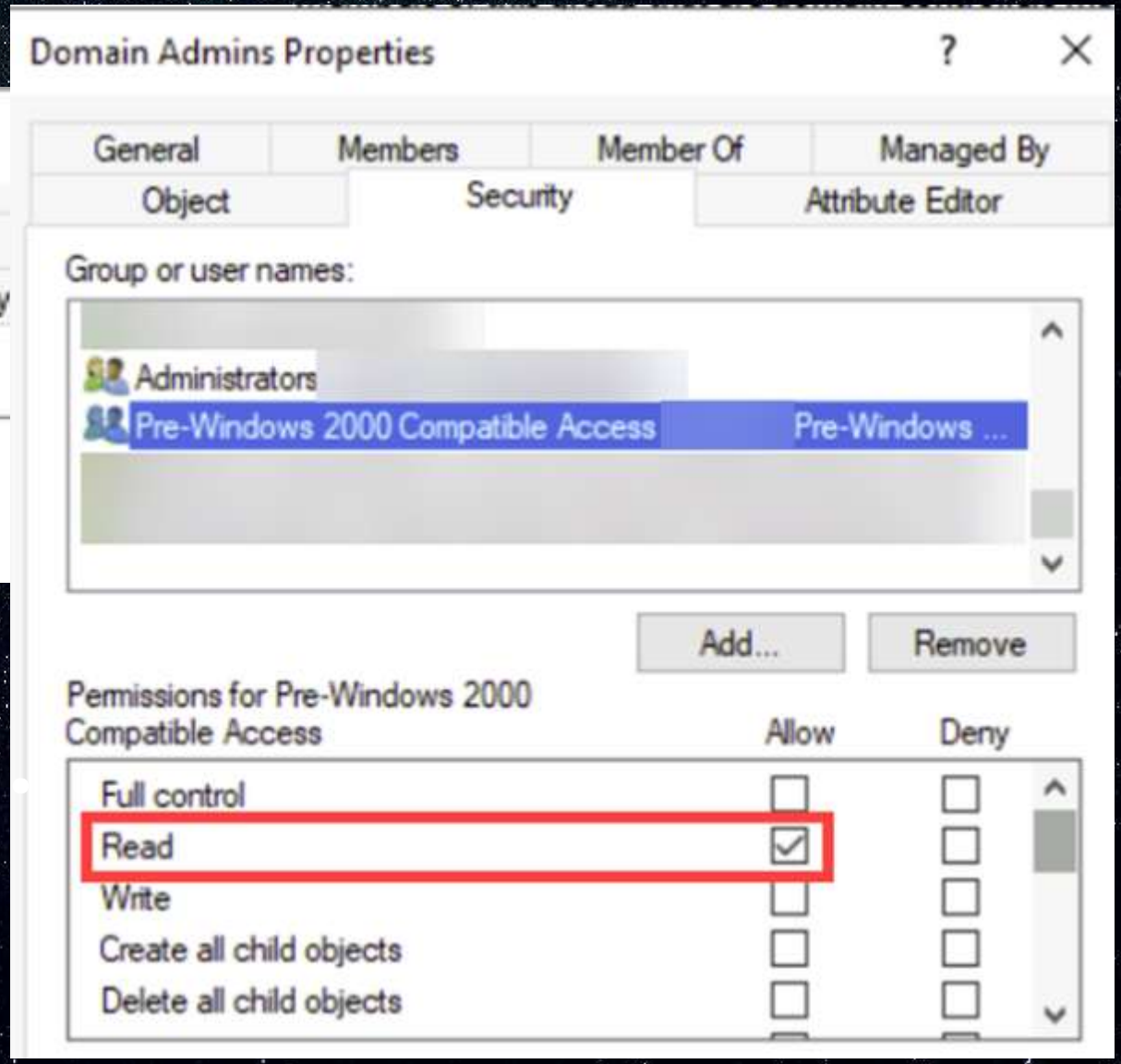
Please do this tomorrow!

Every Object is a risk...

Reduce the attack surface.


Clean = Key

Clear Pre-Windows 2000 Group



Once contained…
‘**Everyone**’ ;-)

RESET KRBTGT-account

KRBTGT password reset (Twice)

krbtgt Properties

```
[2025-05-26 08:36:28] : +++++
[2025-05-26 08:36:28] : +++ Processing KrbTgt Account....: 'krbtgt' | 'CN=krbtgt,C
[2025-05-26 08:36:28] : +++ Used By RWDC.................: 'All RWDCs' +++
[2025-05-26 08:36:28] : +++++
[2025-05-26 08:36:28] :
[2025-05-26 08:36:28] :    --> RWDC To Reset Password On.............:       -DC01
[2025-05-26 08:36:28] :    --> sAMAccountName Of KrbTgt Account......: 'krbtgt'
[2025-05-26 08:36:28] :    --> Distinguished Name Of KrbTgt Account..: 'CN=krbtgt,C
[2025-05-26 08:36:28] :    --> Number Of Chars For Pwd Generation....: '64'
[2025-05-26 08:36:29] :
[2025-05-26 08:36:29] :    --> Previous Password Set Date/Time.......: '2024-08-27
[2025-05-26 08:36:29] :    --> New Password Set Date/Time...........: '2025-05-26
[2025-05-26 08:36:29] :
[2025-05-26 08:36:29] :    --> Previous Originating RWDC............:       -DC01
[2025-05-26 08:36:29] :    --> New Originating RWDC.................:       -DC01
[2025-05-26 08:36:29] :
[2025-05-26 08:36:29] :    --> Previous Originating Time............: '2024-08-27
[2025-05-26 08:36:29] :    --> New Originating Time.................: '2025-05-26
[2025-05-26 08:36:29] :
[2025-05-26 08:36:29] :    --> Previous Version Of Attribute Value...: '5'
[2025-05-26 08:36:29] :    --> New Version Of Attribute Value.......: '6'
[2025-05-26 08:36:29] :
[2025-05-26 08:36:29] :    --> The new password for [CN=krbtgt,CN=Users,
[2025-05-26 08:36:29] :
[2025-05-26 08:36:29] :
[2025-05-26 08:36:29] :    ================================================
[2025-05-26 08:36:29] :
[2025-05-26 08:36:29] :    - Contacting DC in AD domain ...[      -DC01.          ]
[2025-05-26 08:36:29] :       * DC is Reachable...
[2025-05-26 08:36:29] :       * The (new) password for Object [CN=krbtgt,CN=Users,
```

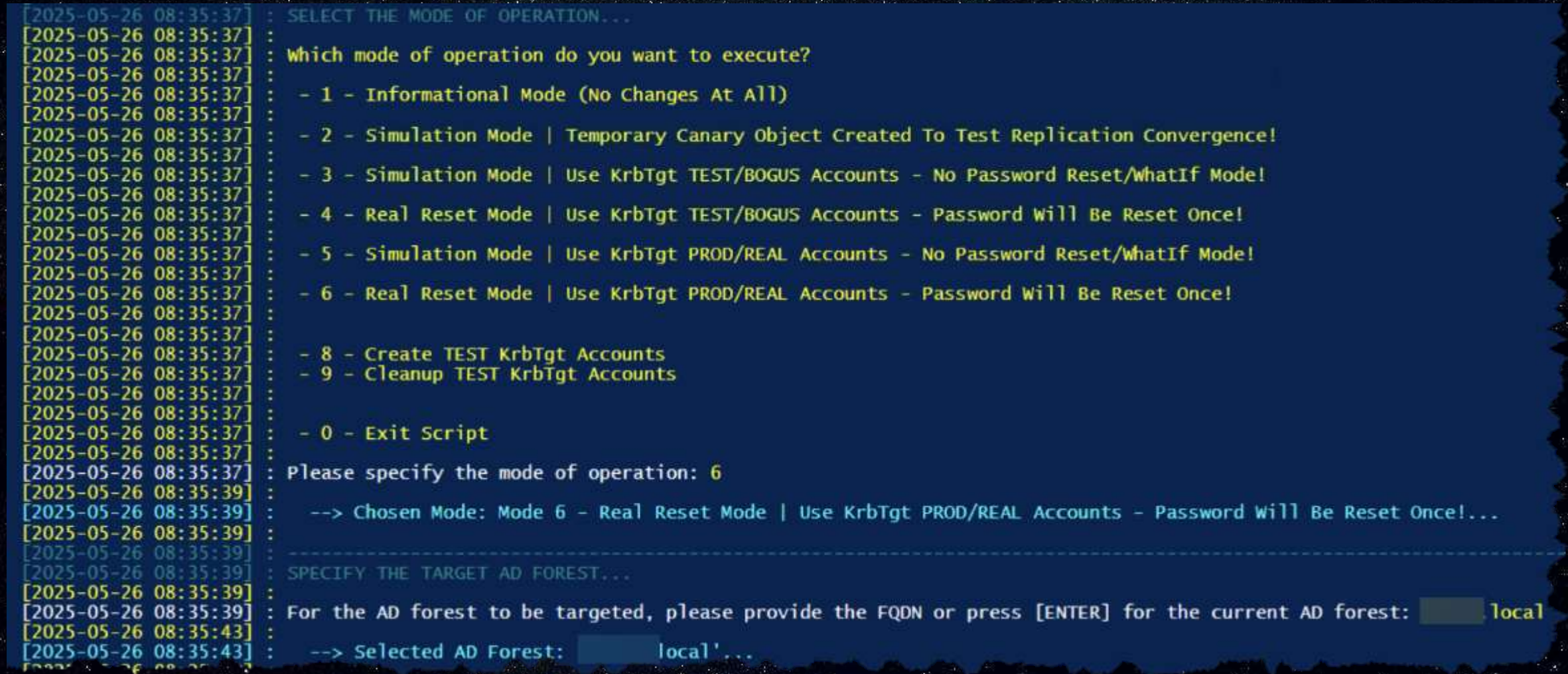
krbtgt Properties

Organization | Published Certificates | Member Of | Password Replication
Dial-in | Object | Security | Environment | Sessions
General | Address | Account | Profile | Telephones | Delegation
Remote control | Remote Desktop Services Profile | COM+ | Attribute Edito

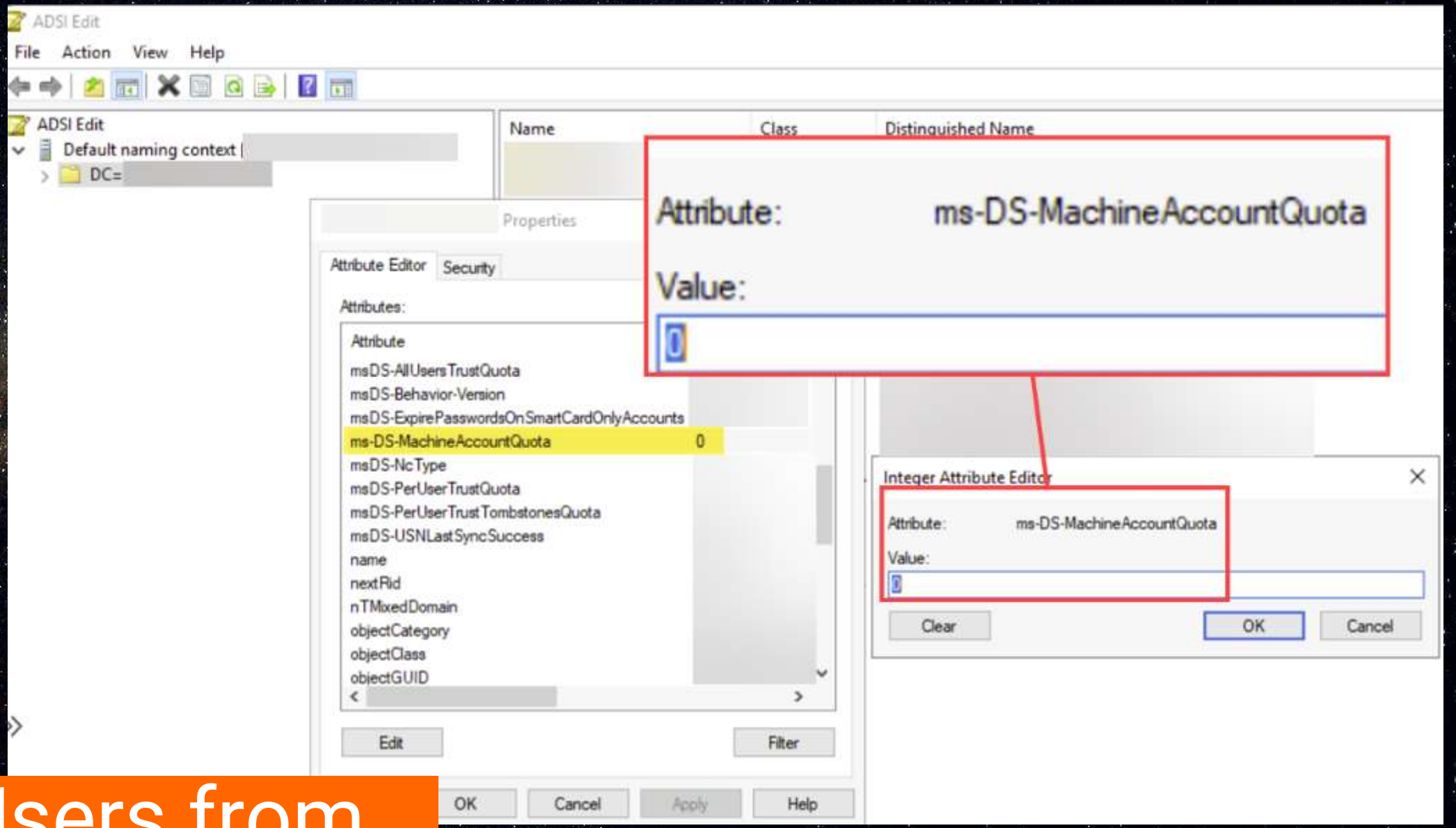
Attributes:

Attribute	Value
primaryGroupID	513 = (GROUP_RID_USERS)
pwdLastSet	5/26/2025 8:36:28 AM SA Western Standar
replPropertyMetaData	AttID Ver Loc.USN Org.DSA
sAMAccountName	krbtgt
sAMAccountType	NORMAL_USER_ACCOUNT
servicePrincipalName	pw
showInAdvancedVie...	
streetAddress	
userAccountControl	UNTDISABLE | NORMAL_A
uSNChanged	
uSNCreated	
whenChanged	5/26/2025 8:36:28 AM SA Western Standar
whenCreated	4/16/2012 1:33:11 PM SA Western Standar

Reset script is safe

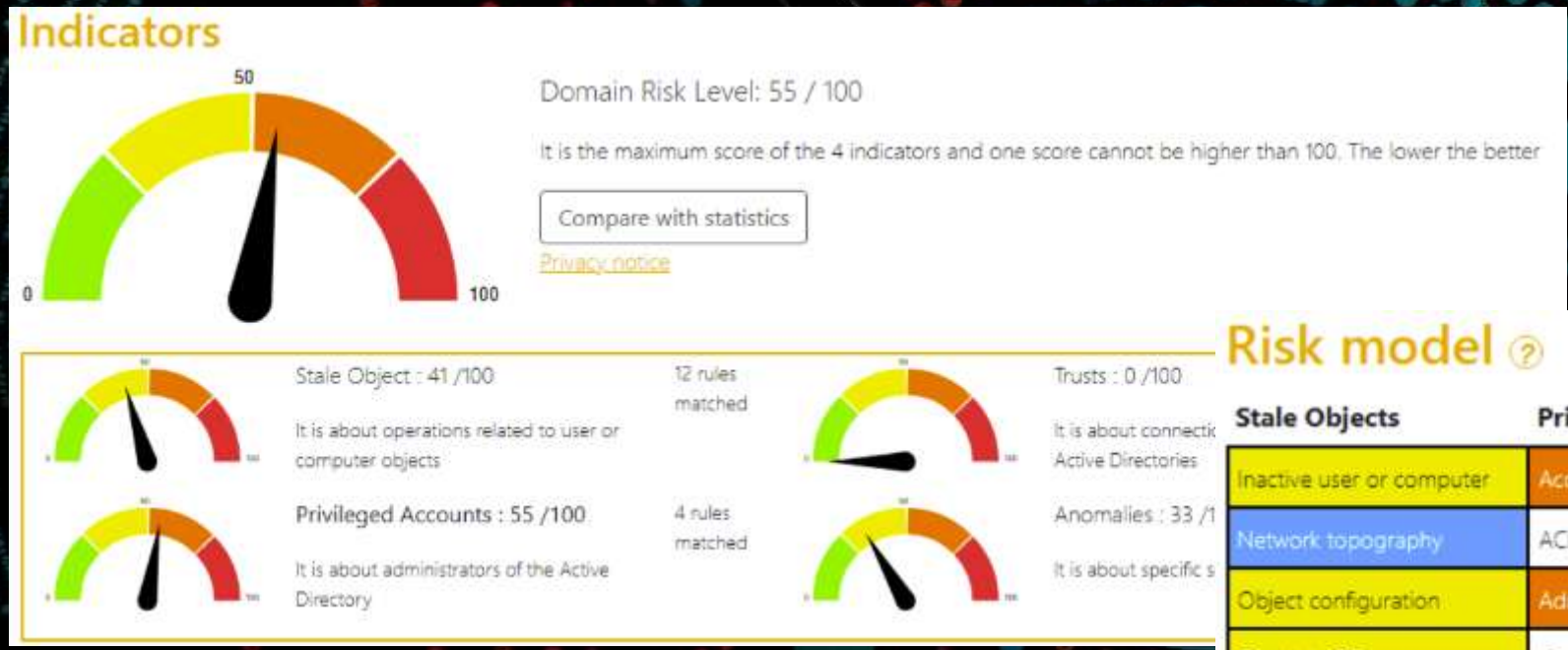


Thanx to Jorge de Almeida Pinto



Block Users from **adding Computers**

Run PingCastle



PING CASTLE BY netwrix

Risk model

Stale Objects	Privileged accounts	Trusts	Anomalies
Inactive user or computer	Account take over	Old trust protocol	Audit
Network topography	ACL Check	SID Filtering	Backup
Object configuration	Admin control	SIDHistory	Certificate take over
Obsolete OS	Control paths	Trust impermeability	Golden ticket
Old authentication protocols	Delegation Check	Trust inactive	Local group vulnerability
Provisioning	Irreversible change	Trust with Azure	Network sniffing
Replication	Privilege control		Pass-the-credential
Vulnerability management	Read-Only Domain Controllers		Password retrieval
			Reconnaissance
			Temporary admins
			Weak password

Also for Entra-ID

Upgrading

One way, or another….

Win a Active Directory Book

What is the AD Schema version of Windows Server **2019**?

objectVersion attribute

Version	Operating system
91	Windows Server 2025
88	Windows Server 2022
88	Windows Server 2019
87	Windows Server 2016
69	Windows Server 2012 R2
56	Windows Server 2012
47	Windows Server 2008 R2
44	Windows Server 2008 RTM
31	Windows Server 2003 R2
30	Windows Server 2003 RTM, Windows 2003 Service Pack 1, Windows 2003 Service Pack 2

88 Windows Server 2019

Server 2016 Functional level required...

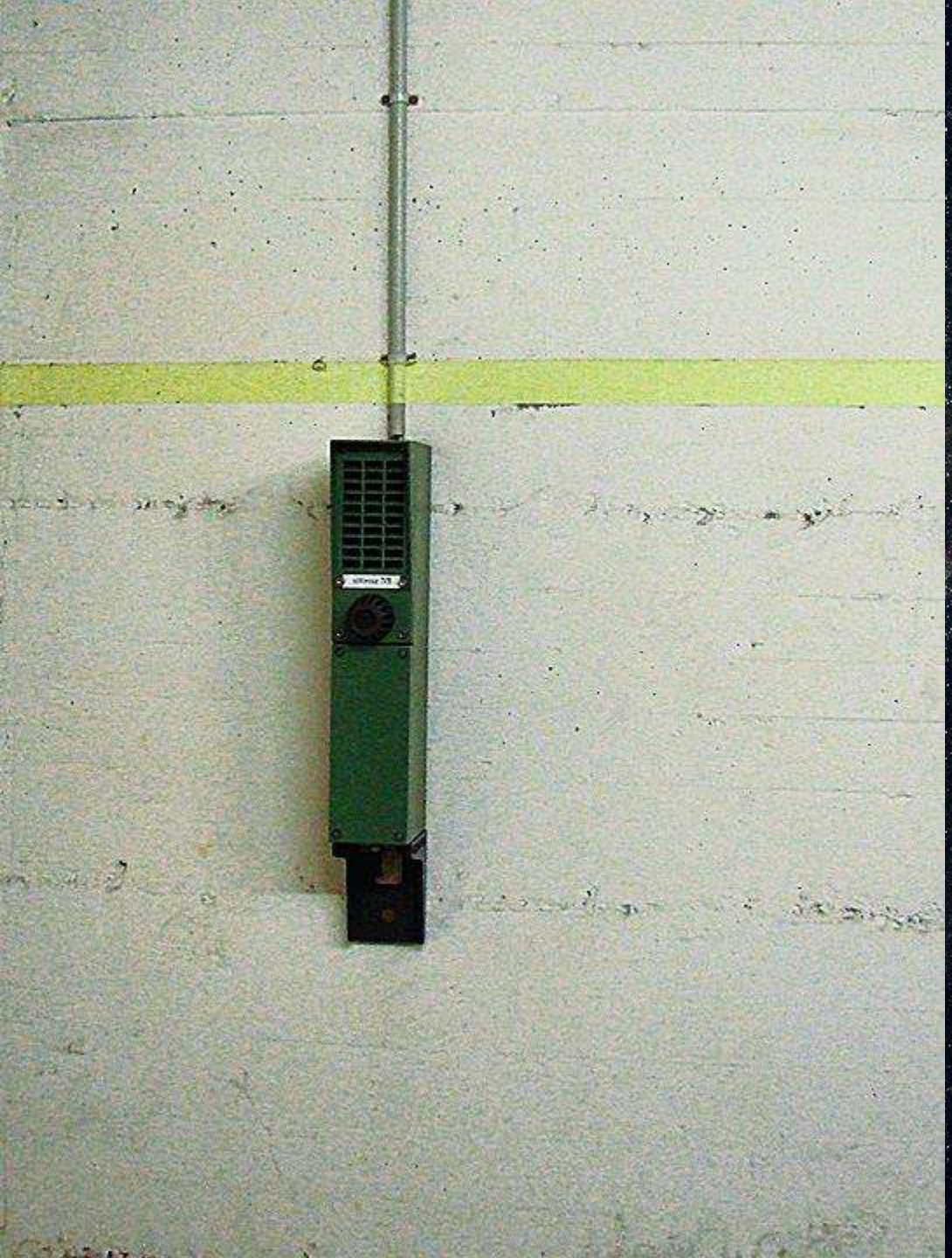
~~RESTORE~~ **Recover** from your AD Backup…

Perfect
DR-test
&
opportunity
to document ;-)


One Way?
Or Another

Generic Upgrade path advice

Advice: Harden M O R E



All IT

Alert

& Available

New Domain Controllers

Microsoft

The Microsoft Way

- Plain, Simple, but unreal for many situations…

The Realistic Way

DHCP / DHCP Failover

- A bit more complex
- Less risks, less stress, planned downtime

The Microsoft Way

- Add new DC with NEW name and NEW IP
- Transfer the FSMO Roles
- Change all references to that DC
- Live in misery for a while
- Restore DFS/DNS/DHCP etc.
- Decommission the old DC

Upgrading: Old Situation

Bunker A

DC01
WS
2016

DC02
WS
2019

Bunker B

DC03
WS
2016

DC04
WS
2016

Upgrading: Microsoft Strategy

Bunker A

NEW_DC01
WS 2025
New IP

NEW_DC02
WS 2025
New IP

Demoted DC01 + DC02
Now Memberservers

Bunker B

NEW_DC03
WS 2025
New IP

NEW_DC04
WS 2025
New IP

Demoted DC03 + DC04
Now Memberservers

Upgrading: Microsoft Desired New Situation

Bunker A

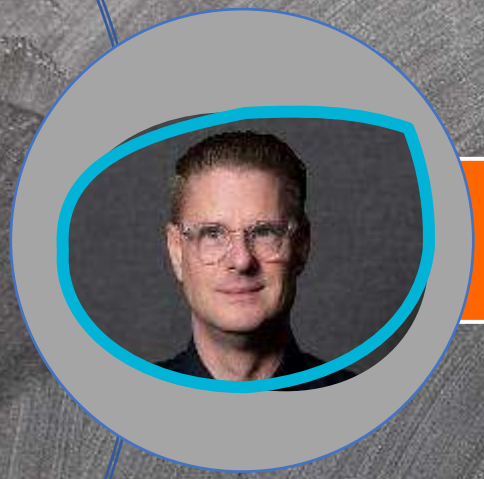
NEW_DC01
WS 2025
New IP

NEW_DC02
WS 2025
New IP

Bunker B

NEW_DC03
WS 2025
New IP

NEW_DC04
WS 2025
New IP



The realistic Way

- Add temporary server with temporary name & IP
- Transfer FSMO roles & Demote the production DC
- You have downtime now on that name & IP…
- Reboot, change name & IP to a temporary, reboot
- Rename temp server to old DC name and configure old IP
- Reboot, promote to DC, reboot
- You’re up & Running with this fresh DC
- Configure services like DFS, DNS, DHCP
- ! Rejoin to backup / AV / monitoring consoles etc. !

Upgrading: Old Situation

Bunker A

DC01
WS 2016

DC02
WS 2019

Bunker B

DC03
WS 2016

DC04
WS 2016

Upgrading: Realistic Scenario

Bunker A

DC01
WS 2016

DC02
WS 2019

NEW_DC01
WS 2025
NEW TEMP IP

NEW_DC02
WS 2025
NEW TEMP IP

Bunker B

DC03
WS 2016

DC04
WS 2016

NEW_DC03
WS 2025
NEW TEMP IP

NEW_DC04
WS 2025
NEW IP

Upgrading: Realistic New Situation

Bunker A

DC01
WS 2025
Old IP

DC02
WS 2025
Old IP

Demoted tmp01/02
Now Memberservers

Bunker B

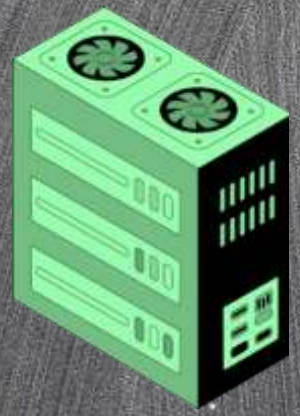
DC03
WS 2025
Old IP

DC04
WS 2025
Old IP

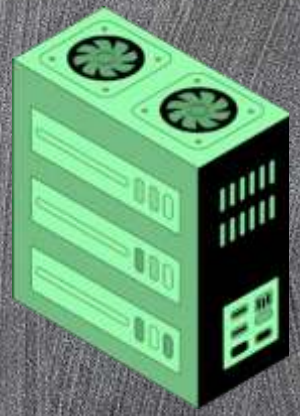
Demoted tmp03/04
Now Memberservers

Upgrading: REAL Desired Situation

Bunker A

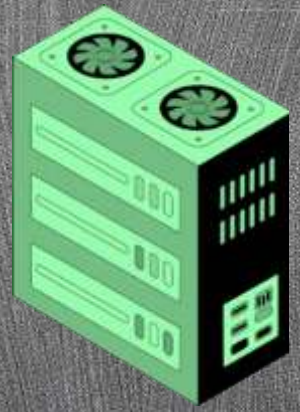


DC01
WS 2025
Old IP

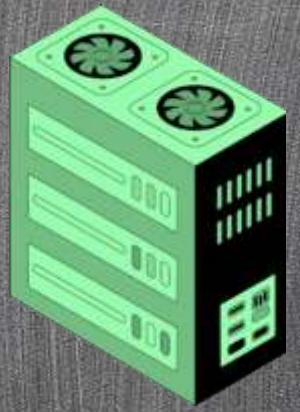


DC02
WS 2025
Old IP

Bunker B



DC03
WS 2025
Old IP



DC04
WS 2025
Old IP

N-4 Media Upgrade Support

Media upgrade to Windows Server 2025 from:

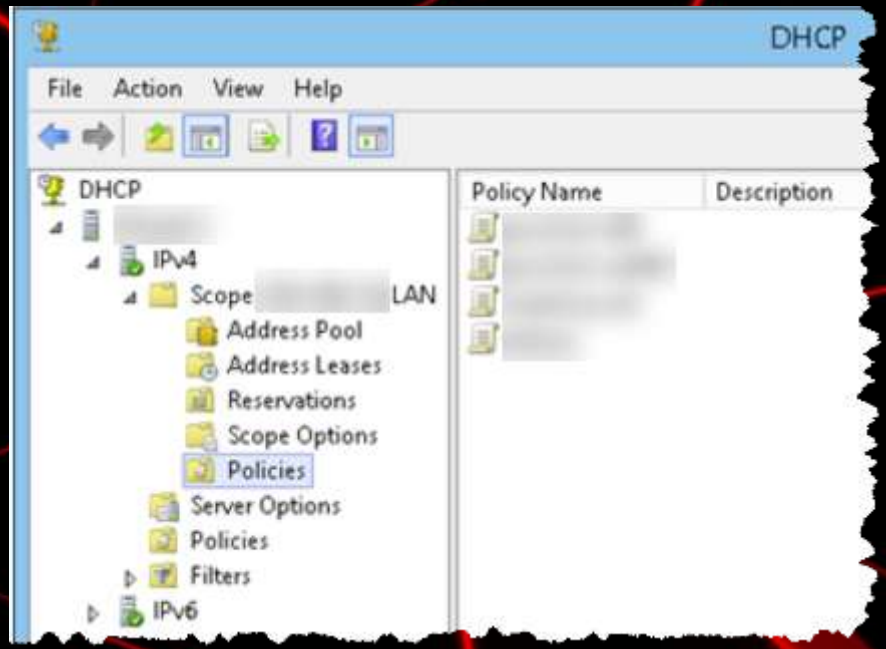
- ✓Windows Server 2012 R2
- ✓Windows Server 2016
- ✓Windows Server 2019
- ✓Windows Server 2022

For In Place upgrading, even 'like an update' from 2019/2022

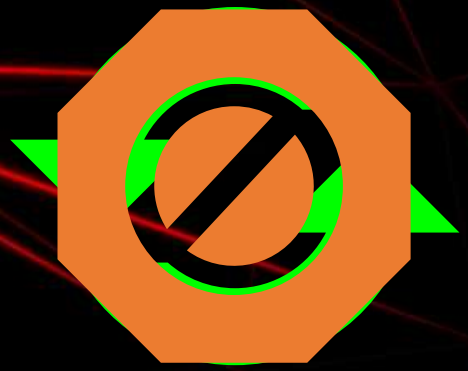
Be fully patched, Backup/snapshot is encouraged

New **Fresh** DC's

Restore ALL settings



Fix DHCP failover




Physical DC? Fine!

To Conclude

One way, or another….


It’s a (responsible) job, but you will be ready for years to come.
Thank you!
Chill
DerkIT


End.