May 31 – June 2, Oslo Spektrum

10th anniversary

Properly securing Azure AD Connect Sync and Azure AD Connect Cloud Sync

Sander Berkouwer
Raymond Comvalius

Introducing Raymond en Sander

- Raymond Comvalius
  - Independent IT-architect
  - Microsoft Certified Trainer since 1999
  - Windows & Devices for IT MVP since 2011

- Sander Berkouwer
  - CTO at SCCT
  - Enterprise Mobility MVP since 2009
  - Microsoft Certified Trainer since 2014
  - Veeam Vanguard since 2016
  - VMware vExpert since 2018

Azure AD Connect Sync vs. Azure AD Connect Cloud Sync

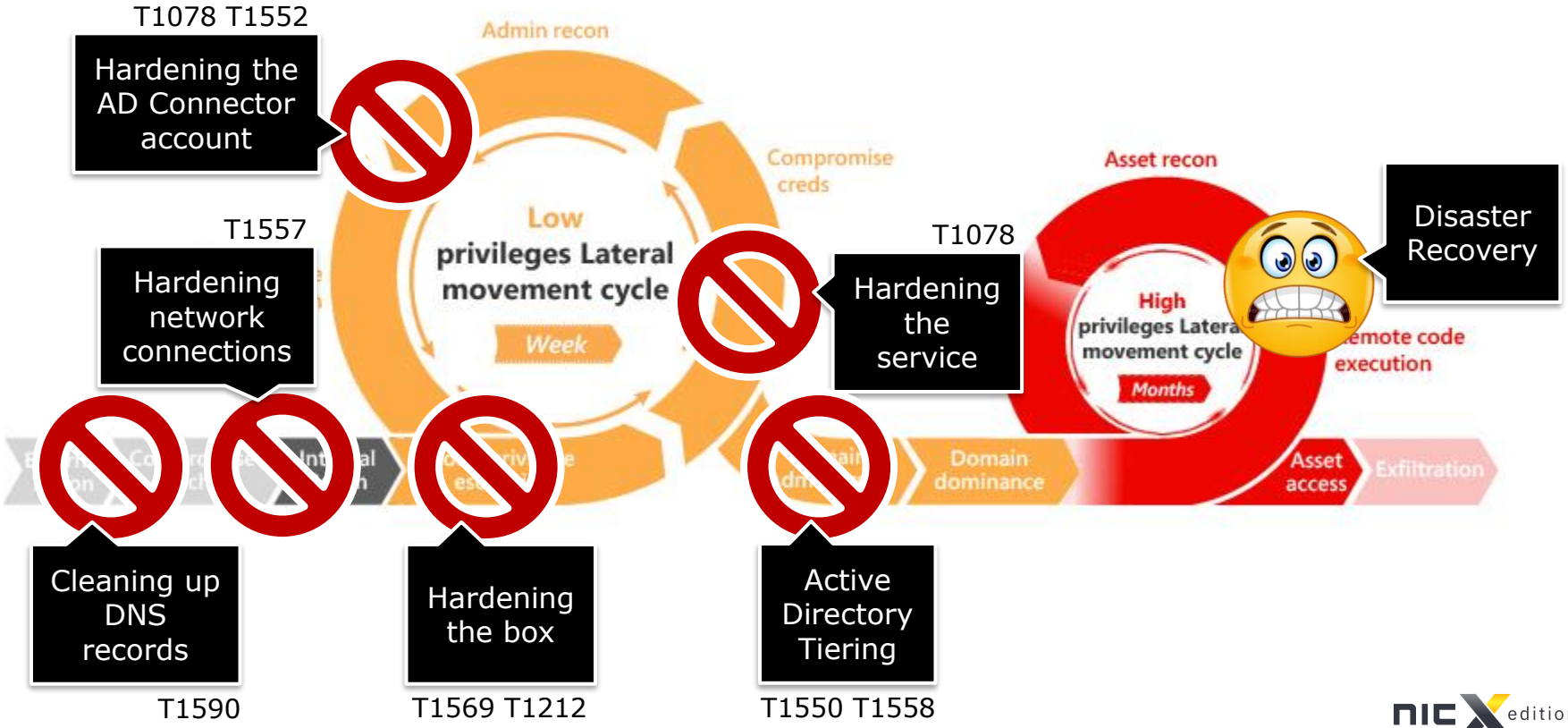
- Azure AD Connect Sync
  - Install a software package on an on-premises Windows Server
    - It runs an engine and keeps a database
    - All configuration is done on-premises

- Azure AD Connect Cloud Sync
  - Install a software package on one or multiple on-premises Windows Servers
    - It runs an agent, but does not run an engine or keep a database
    - The engine run as part of Azure Active Directory
    - All configuration is done in the Azure AD Portal

Limits on Azure AD Cloud Sync

- Cannot connect to LDAP directories
- No support for device objects
- No support for custom schema extensions
- No support for Pass-Through authentication
- No filter on objects' attribute values
- No support for device or group writeback
- No support for merging user attributes from multiple domains
- No Azure AD Domain Services support
- No support for Exchange Hybrid
- Maximum of 150.000 objects per AD domain

Active Directory Kill Chain



Cleaning up DNS records

Cleaning up DNS records

- When verifying a custom domain name in Azure AD
  - Create a TXT record to verify ownership: MS=*
  - After verification… the DNS record is no longer needed. Delete it.

- When using AD FS with Azure AD Connect
  - AD FS farm name is usually adfs.*, sts.*, signin.* or fs.*
  - When decommissioning AD FS, delete these DNS records

- When migrating from Skype for Business to Teams
  - The _sipfederationtls._tcp.* record is no longer needed. Delete it.

Hardening Network Connections

Hardening the network connections

- Enable TLS 1.2 and disable SSL 3.0, TLS 1.0 and TLS 1.1
  - TLS 1.2 is not enabled, by default, on Windows Server 2012, 2012 R2 and 2016
  - Enable TLS 1.2 in your entire network, before removing the older protocols
    - Your Domain Controllers need to run it, so everything needs to run it.
  - Azure AD and Microsoft 365 only accept TLS 1.2 connections going forward

- Disable NTLM
  - Use Group Policy to disable outbound NTLM connections
    - Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers Deny All
  - Use Group Policy to make exceptions
    - Network security: Restrict NTLM: Add remote server exceptions for NTLM authentication
    - When Azure AD Connect leverages a database on a remote SQL Server

Hardening the Box

Hardening the box

- Azure AD Connect runs on Windows Server
  - Unfortunately, Azure AD Connect cannot be installed on Server Core
  - Azure AD Connect and Azure AD Connect Cloud Sync cannot be run in containers
- On Windows Server 2016, you can disable 40 services and 2 tasks
  - For Azure AD Connect, these services don’t add anything but attack surface
  - Two default tasks exist to synchronize Xbox save games…
- On Windows Server 2022, disable at least the Print Spooler service

Hardening the Service

Hardening the service

- Azure AD Connect runs as a virtual service account (vsa)
  - The service account runs the service and connects to the database
  - It can be run as a service account or as a group Managed Service Account (gMSA)

- The benefits of using a group Managed Service Account (gMSA)
  - Passwords are changed automatically every 30 days
  - Renaming of Azure AD Connect server doesn't mess up delegation **2008 R2 FFL+**

- On Domain Controllers, Azure AD Connect always uses a gMSA
- With remote SQL Servers, always use a gMSA

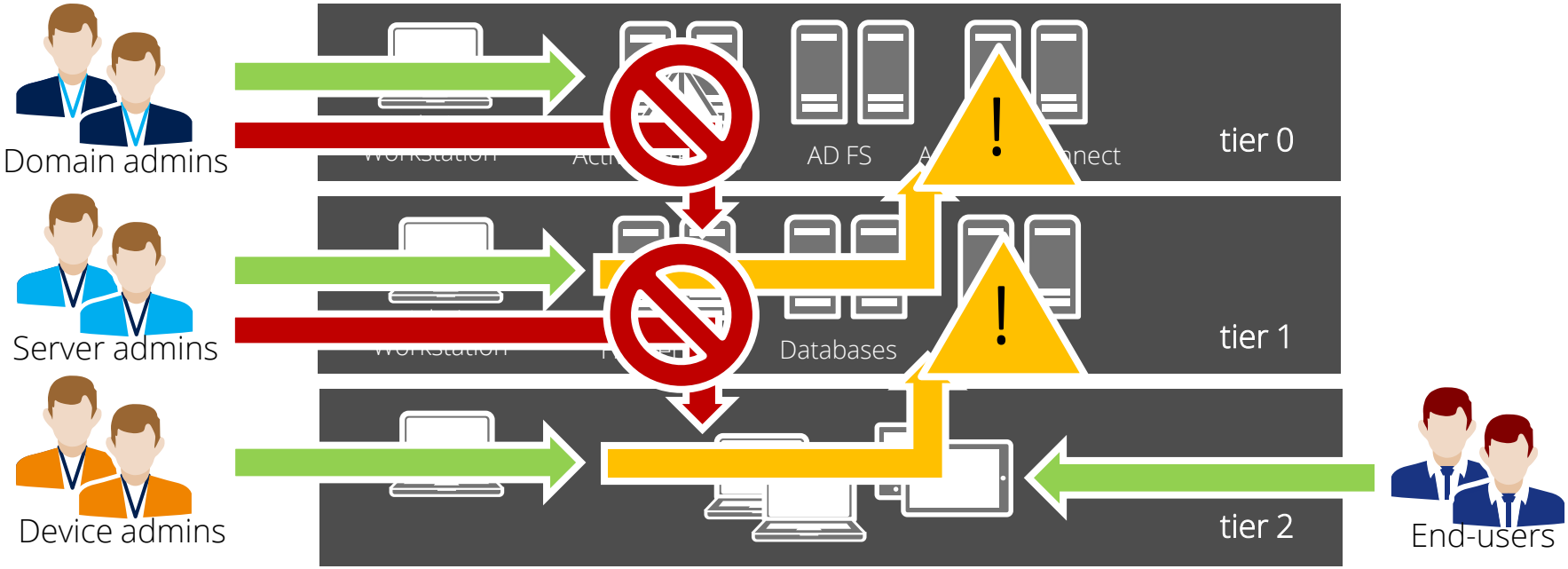
Hardening the AD Connector Account

Hardening the AD Connector account

- The AD Connector account communicates with Active Directory
  - By default, Microsoft delegates the following permissions to the AD Connect account:
    - Read and write permissions on all user and inetorgperson objects *
    - Reset password permissions on all user objects *
    - Read and write permissions on all groups and contacts
    - The **`Replicate Directory Changes`** and **`Replicate Directory Changes All`** permissions
- Inheritance is disabled, by default, on the AD Connector account
- Microsoft recommends delegation based on groups and memberships
- Microsoft recommends least privileged access
  - Both recommendations are not met with the default approach
    - **`Replicate Directory Changes (All)`** permissions are only needed with Password Hash Synchronization (PHS)
  - Delegate permissions granularly using **`dsacls.exe`**

Applying the Active Directory Administrative Model

The Active Directory Administrative Model



Consequences of using the model

- Azure AD Connect needs to run in tier 0
  - Treat Azure AD Connect as you would a Domain Controller or AD FS server
    - Any agent with SYSTEM permissions needs to be exclusive to tier 0
    - Virtualization, backup, monitoring, anti-malware, etc. need to be configured separately for tier 0
  - End user devices should not have a line of sight with Azure AD Connect

- Only Domain Admins should be able to manage Azure AD Connect
  - Set up an Authentication Policy to prevent other admins from signing in
  - Delegate Azure AD Connect permissions granularly using the four Azure AD Connect groups

- Azure AD Connect needs to connect through a web proxy
  - This weakens the mutual TLS protection of the traffic, but allows traffic inspection
  - Tier 0 isn't recommended to be disconnected from the Internet anymore

Disaster Recovery for Azure AD Connect

Disaster Recovery for Azure AD Connect

- Restore from Backups
  - Azure AD Connect holds all your configuration information.
  - Azure AD Connect leverages a SQL Server database.
    - Create backups using the volume shadow writers (application consistent backups)
  - Azure AD Connect Cloud Sync has all its configuration stored in Azure AD
    - There is no supported way to create backups. Documentation is your only option.

- Rebuild from scratch
  - Azure AD Connect leverages objectGUI or mS-DS-ConsistencyGUID as source anchor attribute
    - The source anchor attribute ties the objects in Active Directory and Azure AD together
    - The value for mS-DS-ConsistencyGUID is the base64 representation of the first seen objectGUID value
    - The source anchor attribute is now stored in Azure AD and Azure AD Connect offers ‘Let Azure AD decide’ choice
  - Azure AD Connect Cloud Sync does not offer mS-DS-ConsistencyGUID as source anchor

Concluding

From the field

- Upgrade to Azure AD Connect v2 before August 31st, 2021
  - Many benefits, but requires Windows Server 2016, or up
  - No current Automatic Upgrades

- Azure AD Connect Staging Mode
  - Staging Mode offers a warm standby. It’s not redudancy. It doesn’t automatically fail over
  - Staging Mode is useful for release management

- Full Syncs vs. Attribute integrity
  - In large environments, a Full Synchronization can take multiple hours

Questions?

Thank you!


ITBros.nl


@ITBrosNL


NextXpert.com


@NextXpert


www.linkedin.com/in/
RaymondComvalius


DirTeam.com


@SanderBerkouwer


www.linkedin.com/in/
SanderBerkouwer

Slides and demos from the conference will be available at

https://github.com/nordicinfrastructureconference/2022