

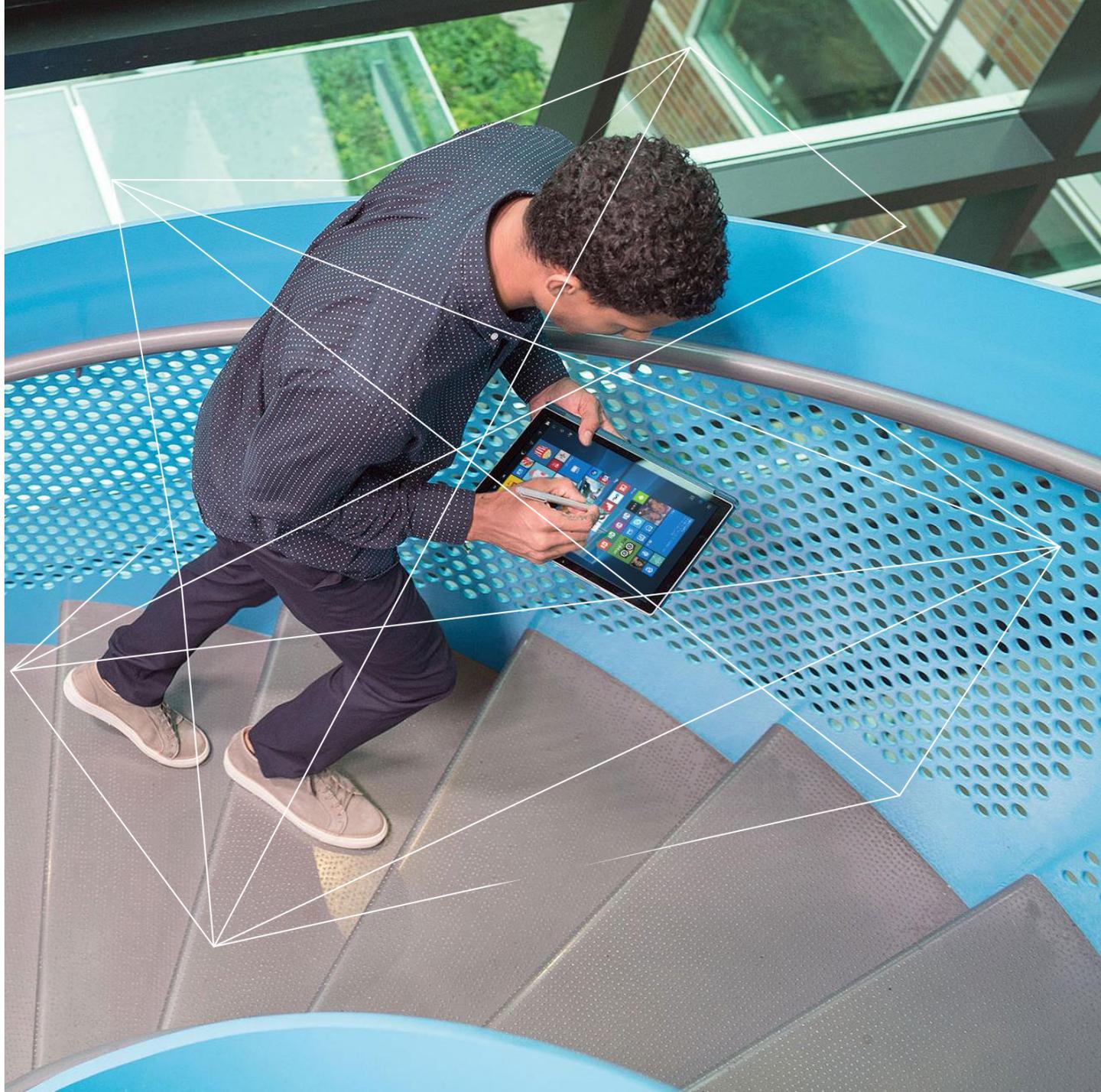


# Azure File Sync

Elvis Guštin, MVP  
EM-Soft sistemi d.o.o.



#ntk18



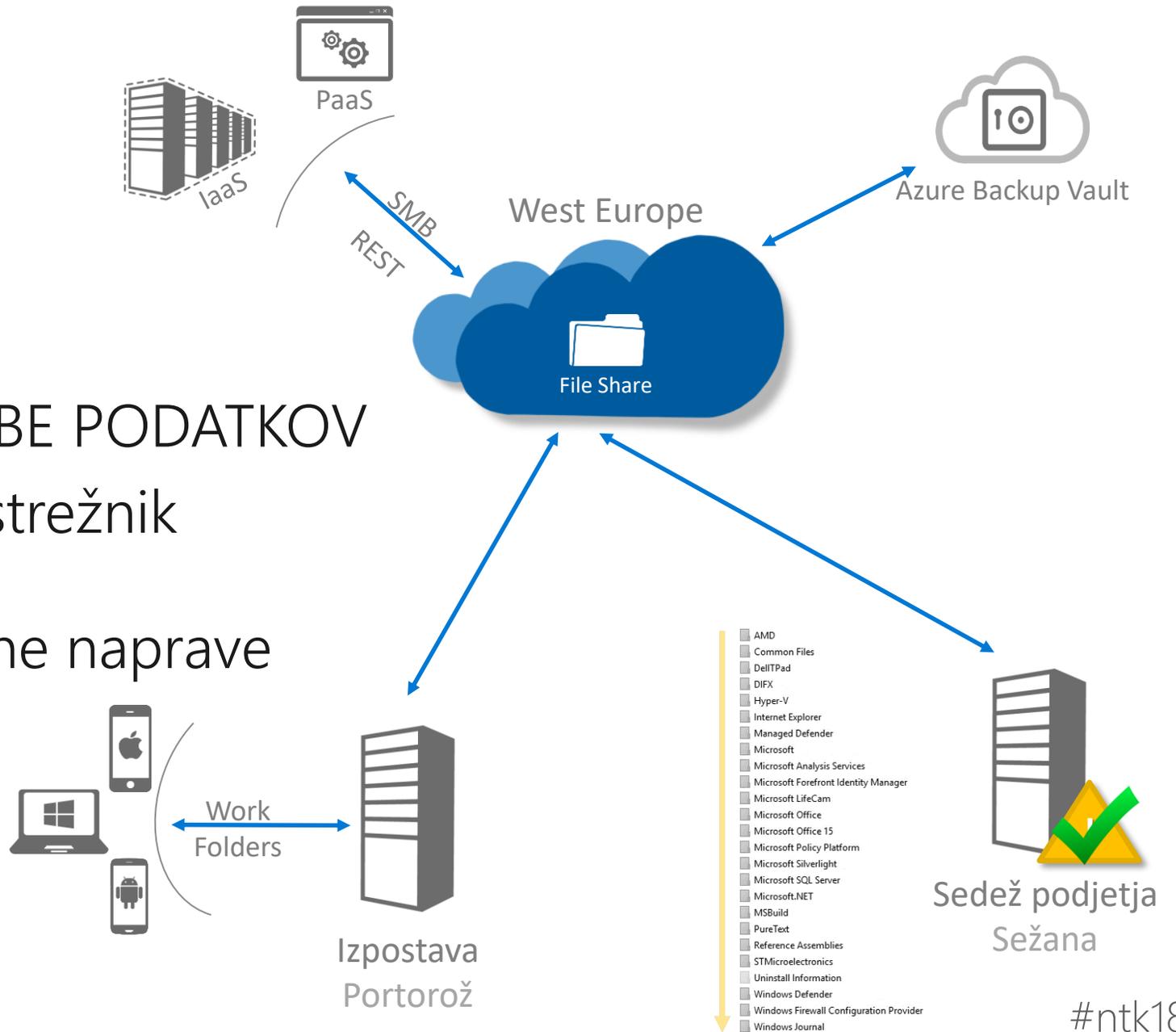
# Zakaj imamo še vedno na lokalnih strežnikih?

- Imamo kar nekaj prijemov
  - OneDrive, SharePoint
  - Dropbox, ...
- Zahteve aplikacij
  - Aplikacije, ki uporabljajo te datoteke ne znajo delati s Cloud-om
  - Path – včasih se vse malo zakomplicira; posebni znaki
  - Performančni problemi in latence (pomislite na kakšen AutoCad...)
- Problemi, ki jih imamo
  - DR scenariji
  - Backup plani in njihova centralizacija
  - Imeti shranjene vse stare podatke (Cold data)
  - Kapacitete / imeti vedno LE PRAVE podatke na pravem mestu



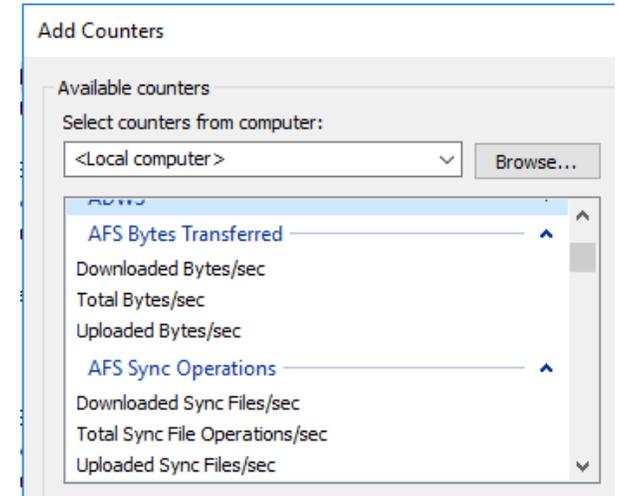
# AFS strategija?

- Glavni strežnik je poln
- Vzpostavimo AFS
  - Določimo strategijo „cache-a“
- V primeru okvare ni IZGUBE PODATKOV
- Kadarkoli lahko dodamo strežnik
  - Tudi v drugi domeni / Workgroup
- Lahko uporabljamo različne naprave
- Pazi BACKUP in AV!!!
- Dodatne možnosti DR



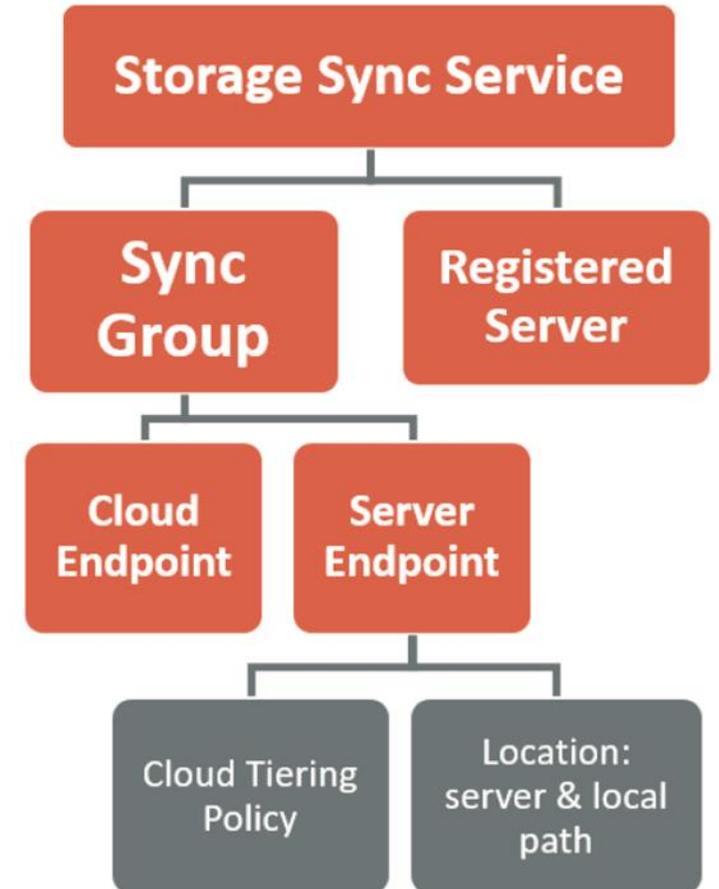
# Uporabni scenariji Azure File Sync

- Multi site sync
  - Uporabniki po različnih lokacijah uporabljajo različne podatke
  - Multimaster sync (uporabnik bo obveščen v primeru, ko nekdo uporablja datoteko)
  - Shranjena je zadnja verzija
  - Sinhronizira vedno celotne datoteke
  - Counterji za optimizacijo (lokalni strežnik)
- Cloud tiering / access
  - Tiering (caching) je nastavljen glede na zahtevan prosti prostor, ne na velikost podatkov
  - Različne lokacije lahko uporabljajo različne datoteke v cache-u in različne nastavitve
  - Dostop tudi direktno iz Clouda (REST ali SMB) – pozor na ACL!!!
- Backup in DR
  - Imamo point in time točke (Checkpoint-i)
  - DR je instanten, samo povežemo namespace na nov server (cache tu še ni prisoten)



# Tehnologija Azure File Sync

- Storage Sync Service
  - Glavna komponenta, narejena znotraj Azure Resource Group
  - Lahko imate več Storage Sync Service-ov
- Registered Server
  - On Premises strežnik ali Cluster, ki je definiran kot lokalni endpoint
  - Dodajate lahko več strežnikov glede na potrebe
  - Predstavlja „trusted relationship“ med strežnikom (clustrom) in Sync grupo
  - Vsak strežnik je lahko registriran le v eni Storage Sync Service storitvi
- Sync Group
  - Definira sync topologijo za set datotek, ki se sinhronizirajo
  - Storage Sync Service ima lahko več Sync Group – odvisno od vaših potreb



# Tehnologija Azure File Sync

- Cloud Endpoint

- Lokacija podatkov v Azure-u
- Vsaka Sync Group-a ima lahko samo en Cloud Endpoint

- Server Endpoint

- Predstavlja lokacijo na Registered Server-ju; mapa, volume ali mountpoint\*
- Endpointov je lahko več, na vsakem strežnik konfiguriran drugače
- Na vsakem strežniku se lahko konfigurira tiering drugače
- Na strežnik je potrebno namestiti agenta (update skozi Windows update)

Opozorilo: You can create a server endpoint on the system volume but, there are two limitations:

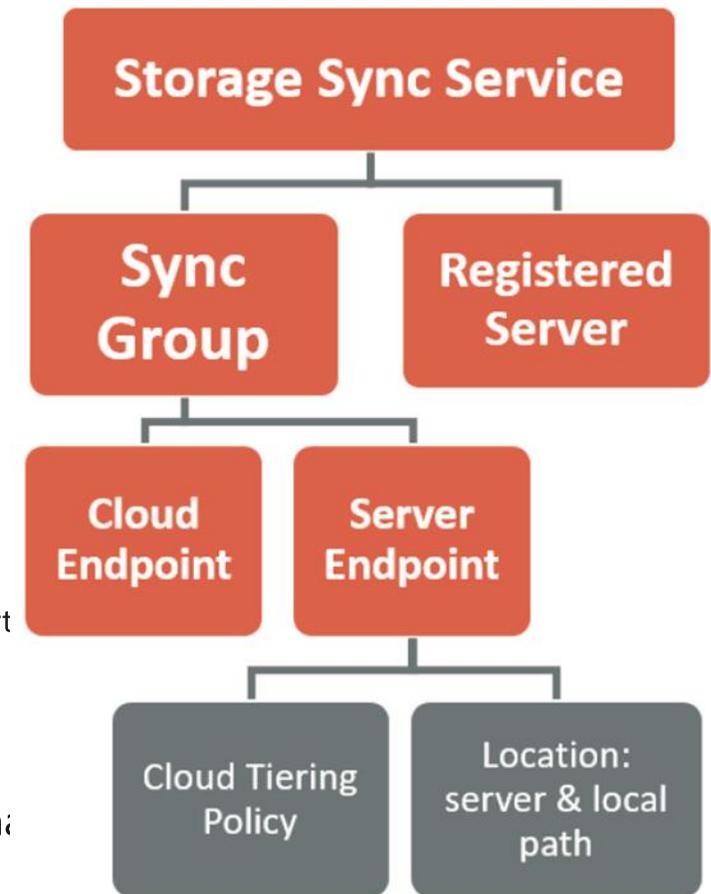
- Cloud tiering cannot be enabled.
- Rapid namespace restore (where the system quickly brings down the entire namespace and then start to recall content) is not performed

- AFS Agent – vsebina

- **FileSyncSvc.exe**: Servis, odgovoren za sinhronizacijo, odkrivanje sprememb na strežniku in inicializacijo sync-a v Azure
- **StorageSync.sys**: file system filter odgovoren za tiering v Azure



**PowerShell cmdlet-i**: Modul, ki se instalira z agentom



# Cloud Tiering

- Je opcija AFS, ki poskrbi za pravilno vsebino Server Endpoint-ov
  - Deluje na datotekah do katerih uporabniki niso dostopali v zadnjem času
  - Datoteke morajo biti večje od 64KB – manjših se ne dotika
  - Take datoteke se umaknejo iz lokanega storage-a
- Datoteka se zamenja s Pointer-jem, ki kaže v cloud
  - Pointer je v bistvu URL naslov do Azure lokacije
  - Na NTFS je vpisan „offline“ atribut, da lahko aplikacije uporabljajo datoteko, kot da bi bila prisotna
  - Lokalno ostanejo metadata podatki (ACL)
  - Ko uporabnik odpre datoteko, se ta prenese iz oblaka, brez da uporabnik to ve
  - Funkcija je poznana kot Hierarchical Storage Management (HSM)
- Sistemski volume-i nemorejo uporabljati tiering-a



# Kaj podpira Azure File Sync

- Zaščita podatkov
  - Podprt Bitlocker
  - Podprt Azure RMS in Windows RMS
  - Azure Information protection (<https://docs.microsoft.com/en-us/azure/information-protection/understand-explore/what-is-information-protection>)
  - NI podprt EFS
  - Podatki so v transportu in na Azure-ju vedno šifrirani
- Protivirusna zaščita
  - Odvisno od ponudnika, mora znati delati z „offline“ datotekami
  - Nekateri ponudniki so preverjeno podprti (preglejte nastavitve za offline scanning):
    - Symantec Endpoint Protection
    - McAfee EndPoint Security
    - Kaspersky Anti-Virus
    - Sophos Endpoint Protection
    - TrendMicro OfficeScan



# Kaj podpira Azure File Sync

- Windows Failover Cluster
  - Podpira sinhronizacijo „File Share for general use“
  - Ne podpira synca CSV share-a
  - Ne podpira Scale Out File Server-ja
- Data deduplication je podprt
  - Lokalna deduplikacija ne manjša prostora v Cloudu
  - Cloud Tiering ni podprt (še)
- Podprti sistemi Windows Server 2012R2 in 2016
  - Full GUI install – ne CORE verzija
  - Standard in Datacenter različica



# Kaj podpira Azure File Sync

Feature	Support status	Notes
Access control lists	Fully supported	Windows ACLs are preserved by Azure File Sync, and are enforced by Windows Server on Server Endpoints. Windows ACLs are not (yet) supported by Azure Files if files are accessed directly in the cloud.
Hard links	Skipped	
Symbolic links	Skipped	
Mount points	Partially supported	Mount points might be the root of a Server Endpoint, but they are skipped if they are contained in a Server Endpoint's namespace.
Junctions	Skipped	
Reparse points	Skipped	
NTFS compression	Fully supported	
Sparse files	Fully supported	Sparse files sync (are not blocked), but they sync to the cloud as a full file. If the file contents change in the cloud (or on another server), the file is no longer sparse when the change is downloaded.
Alternate Data Streams (ADS)	Preserved, but not synced	

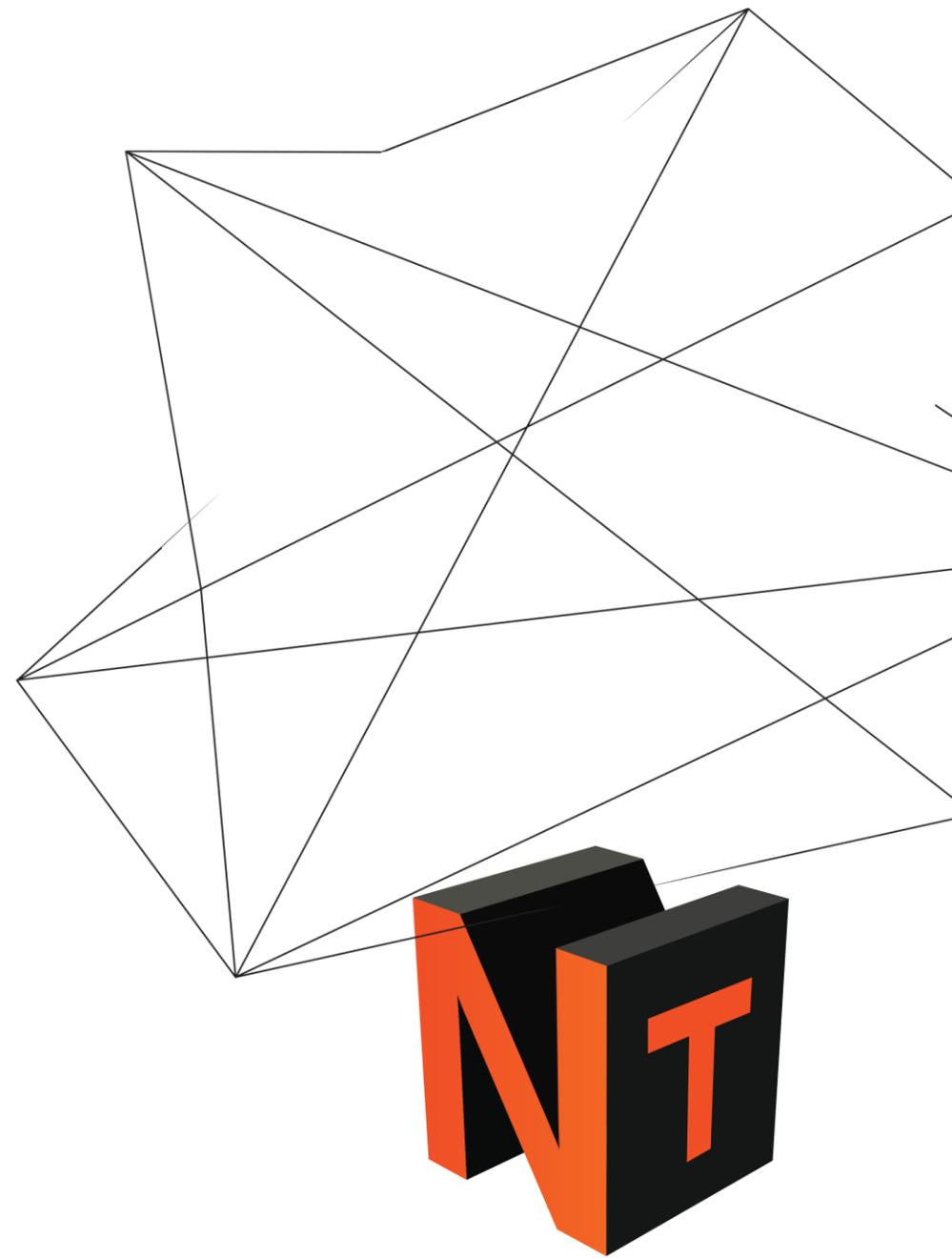


# Kaj NE podpira Azure File Sync

- Path dolžine več kot 2048 znakov
- DACL security descriptor daljši od 2K ali več kot 40 ACE na single item
- SACL del, ki je namenjen auditingu
- Extended attributes
- Reparse points in hard links
- Deduplicirane datoteke
  - deduplikacija se ne prenaša v Azure
- EFS Enkripcija
  - Agent v tem primeru ne more brati datotek
  - Datoteka se preskoči ob sinhronizaciji



# Demo



#ntk18

# Vprašanja

Elvis Guštin

[elvis@em-soft.si](mailto:elvis@em-soft.si)

#ntk18

