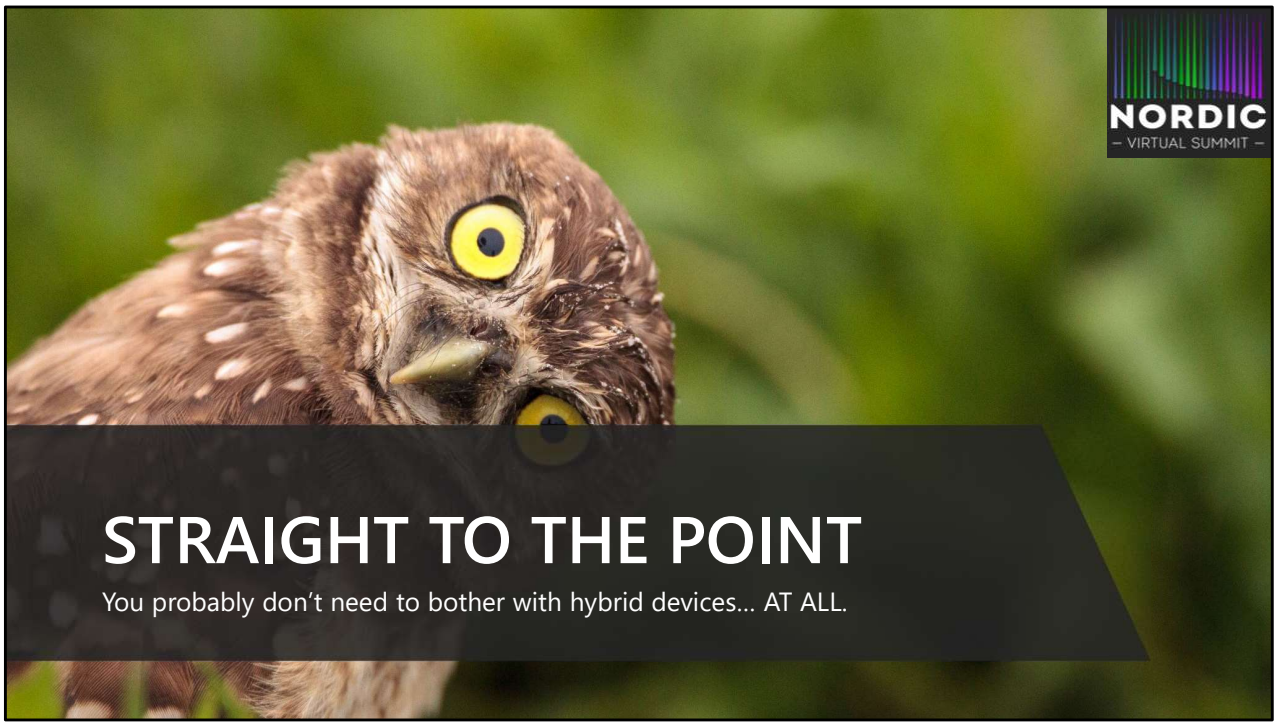
SSO to domain resources from Azure AD Joined Devices

Michael Mardahl
APENTO
@michael_mardahl

Ben Whitmore
CloudWay
@byteben

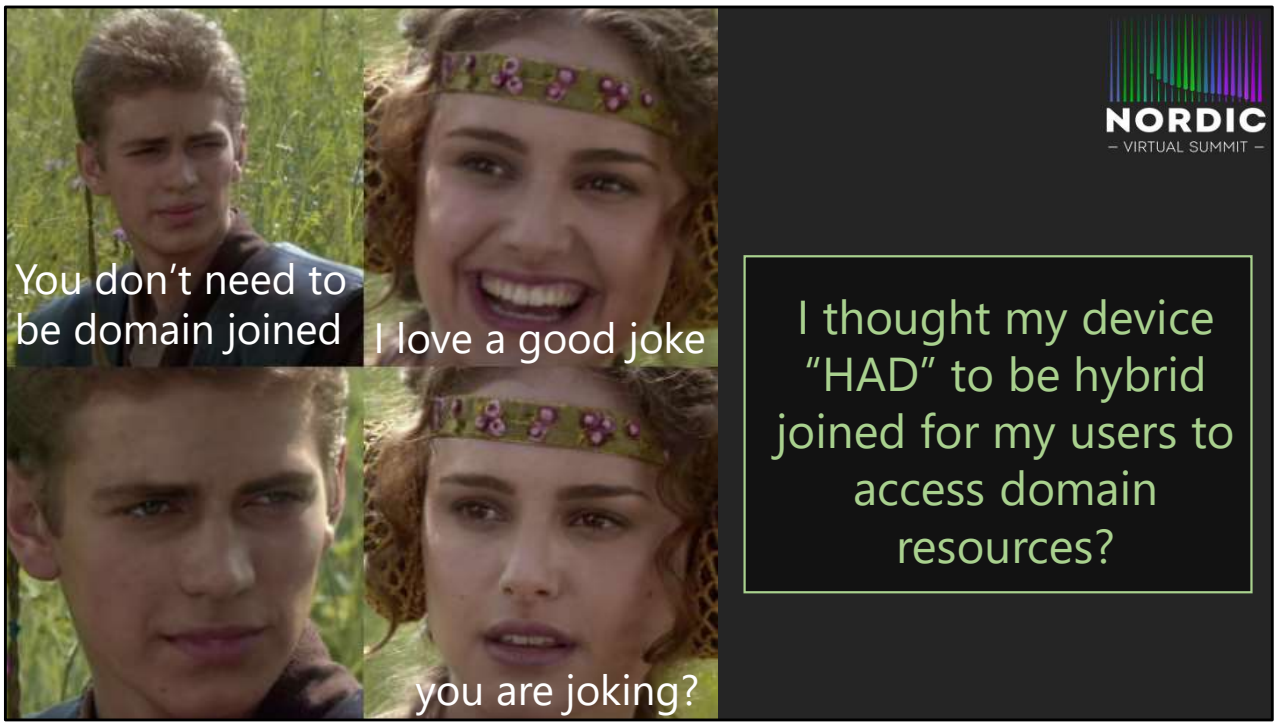
MVP Microsoft Most Valuable Professional

NORDIC — VIRTUAL SUMMIT —

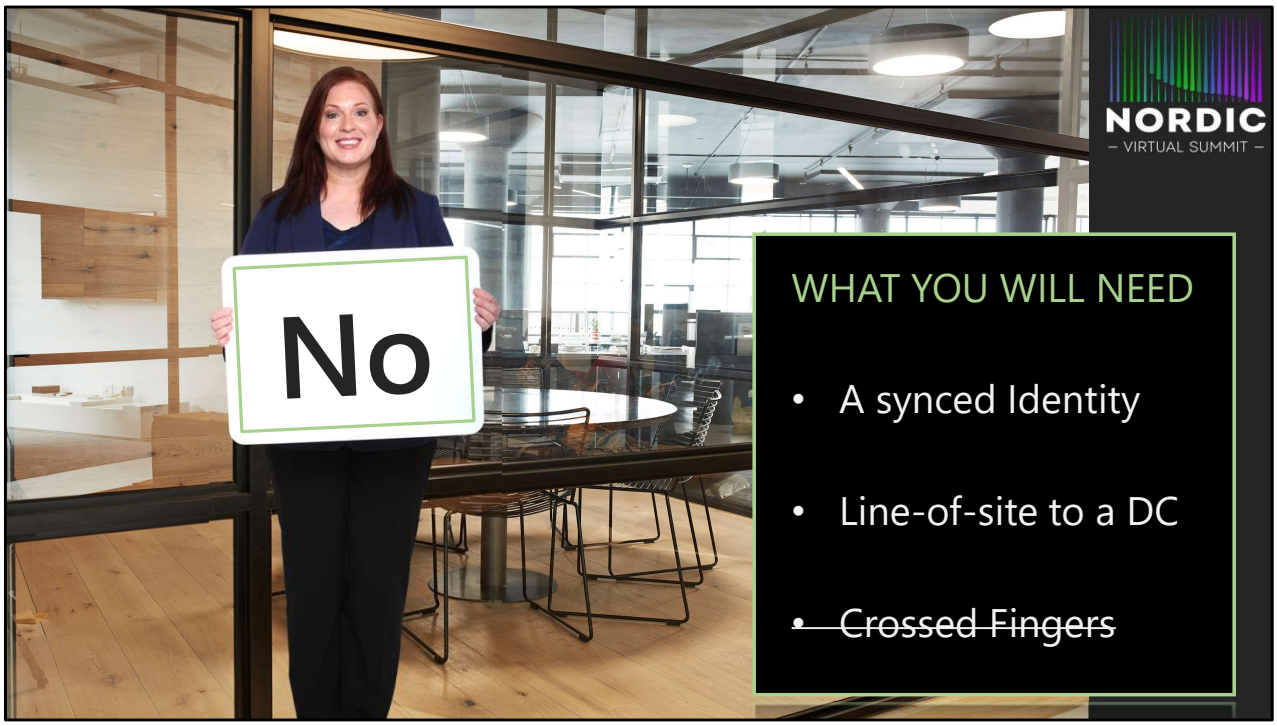


What is hybrid anyway? Why are people doing it?
Talk about moving stuff to cloud but people still need to access legacy on prem stuff
Talk about option during AutoPilot to join devices to domain. Needs VPN, can be messy, lots of failure points. DNS, Certificates, VPN, AADConnect timing

NEXT SLIDE: Your device does not need to be Hybrid Joined



Talk about device doesn't need to be domain joined.
Don't go into too much detail – quick slide



No, device does not need to be joined to your domain for the user to access domain resources

Typically, the user requests domain resources – not the device.
There are some scenarios where you “might need” to hybrid join devices. e.g.

- Device needs to exist in AD for legacy app
- Accessing resources across different forests

The only caveat is you need a synced identity, line of sight to a Domain Controller. You don’t even need luck (unless your DNS is really bad)

Why a synced Identity?

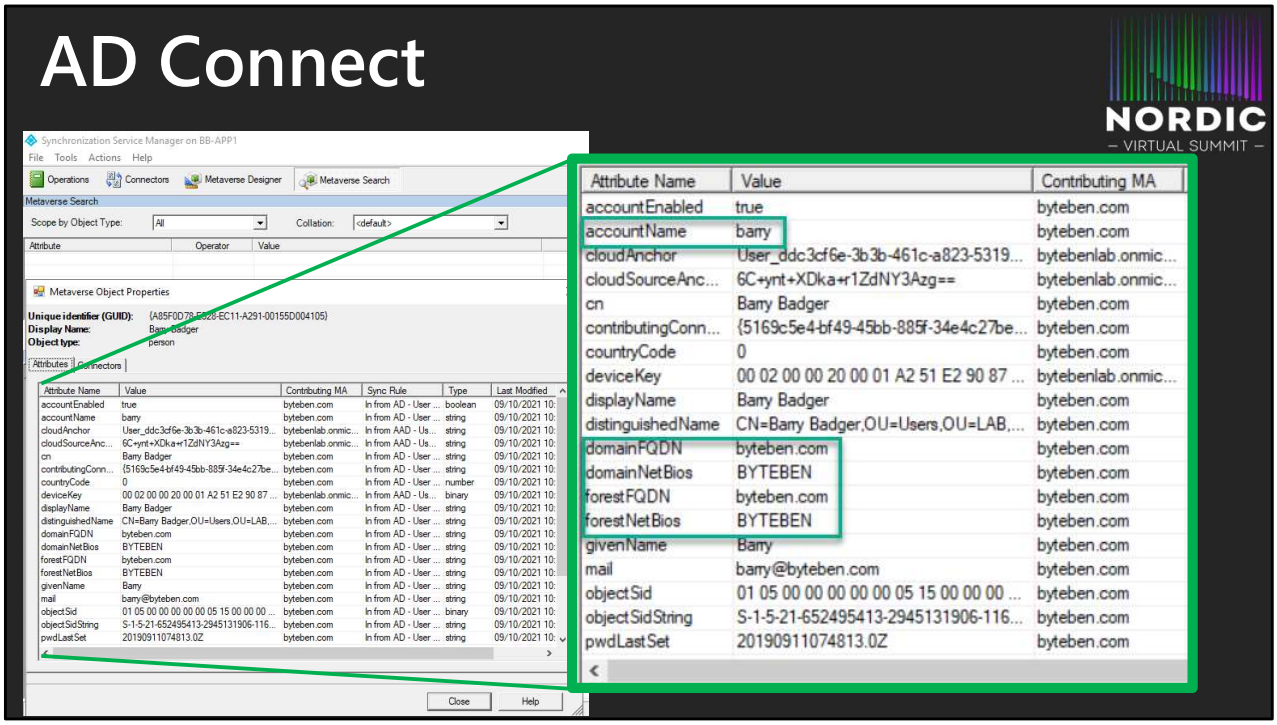
Your synced identity knows about your Domain

Our Domain Controller needs to know who we are before it will let us access on-premise resources. How does it know who we are?
The device is not domain joined, and we typically sign in with an Azure AD account

The primary source of Identity needs to be the on-premise Domain – which we kinda know already.
We need to get attributes into Azure AD so when we log on, those attributes come down with the PRT.

We can then use those attributes to begin our SSO journey to domain resources.

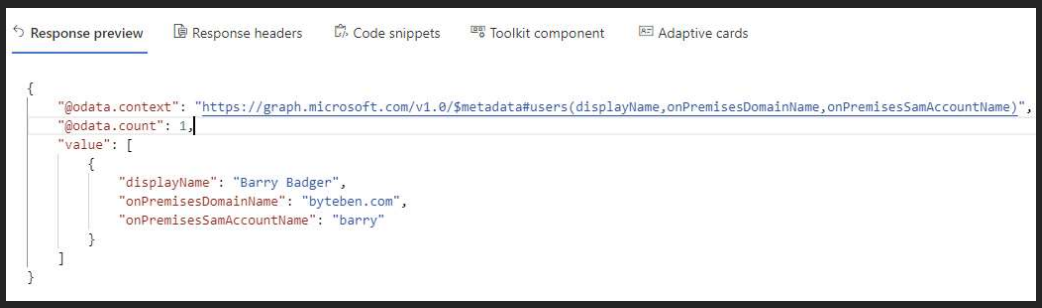
AD Connect



Talk about which attributes are synced up.

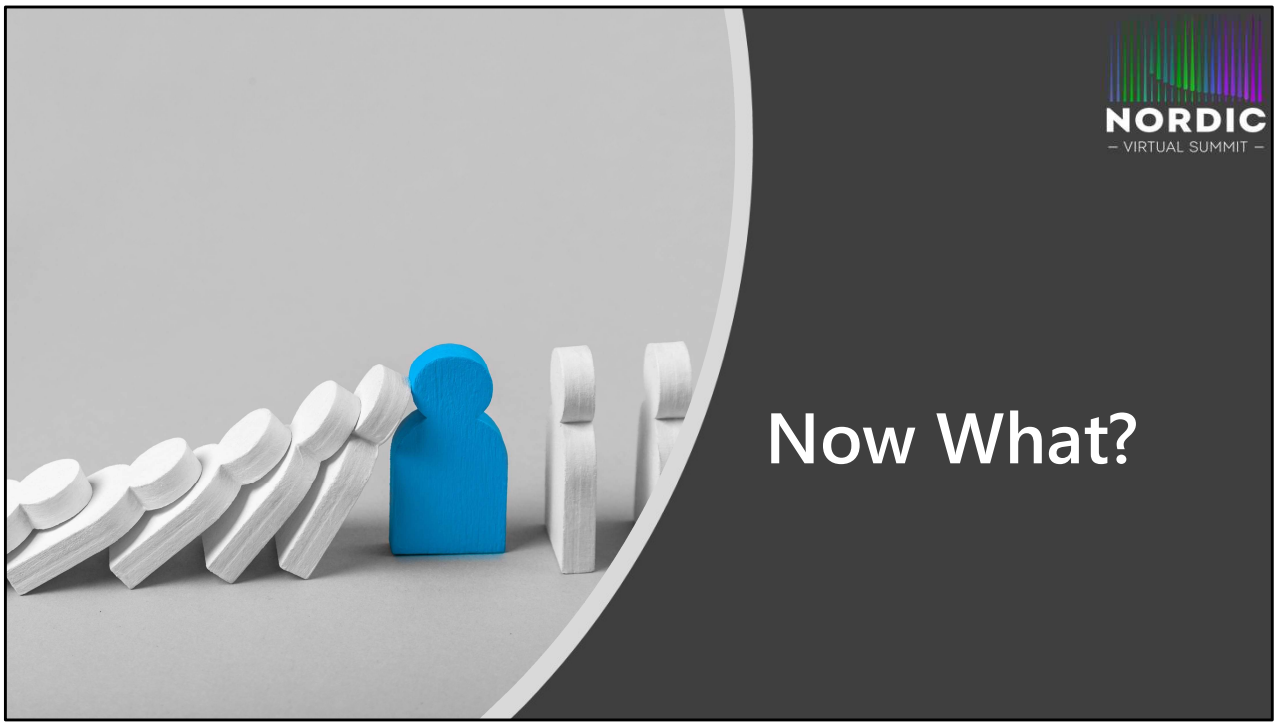
Attributes in AAD

https://graph.microsoft.com/v1.0/users?$filter=DisplayName eq 'Barry Badger'&$select=displayName, onPremisesDomainName, onPremisesSamAccountName



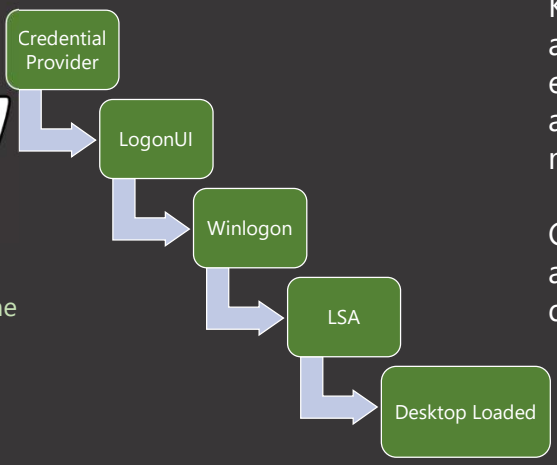
These attributes get pulled down with out Primary Refresh Token at logon

show attributes sync in AD Connect and GE


NORDIC
– VIRTUAL SUMMIT –
Now What?

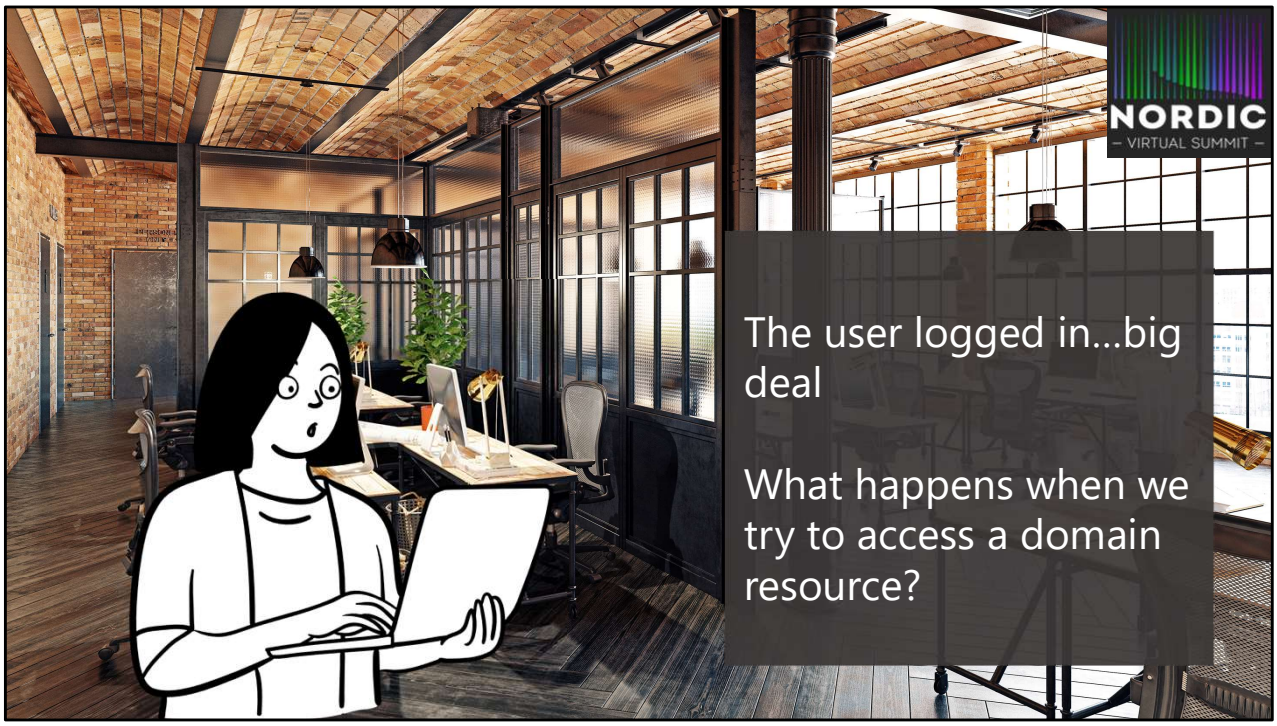
User logs in to Windows

Kim just started something awesome by logging on

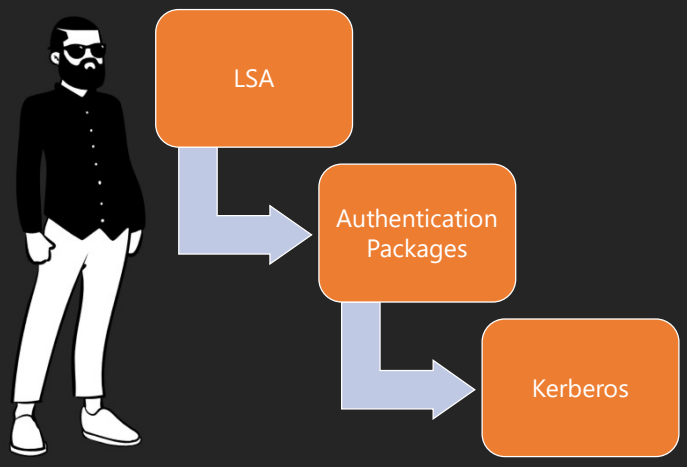


Kim, unknowingly, chooses a Credential Provider by entering their username and password and a call is made to the LSA.

Credentials are authenticated and the desktop loads.


NORDIC
– VIRTUAL SUMMIT –
The user logged in…big deal
What happens when we try to access a domain resource?

User accesses a domain resource



LSA still being serious

The LSA is asking which other authentication packages can use those credentials. The Kerberos Authentication Package puts its hand up.

We have everything we need to contact a Domain Controller – that information came down with our PRT:-

- SamAccountName
- onPremisesDomainName

Kerberos is king here.
Michael and I and fluffy the dog
Guards the hades, gates of hell, watchdog of the underworld etc..bit like guarding Windows Vista.
Came out in the 80's

Kerberos has 3 parts/heads (Michael = User, Fluffy = KDC, Ben = service)

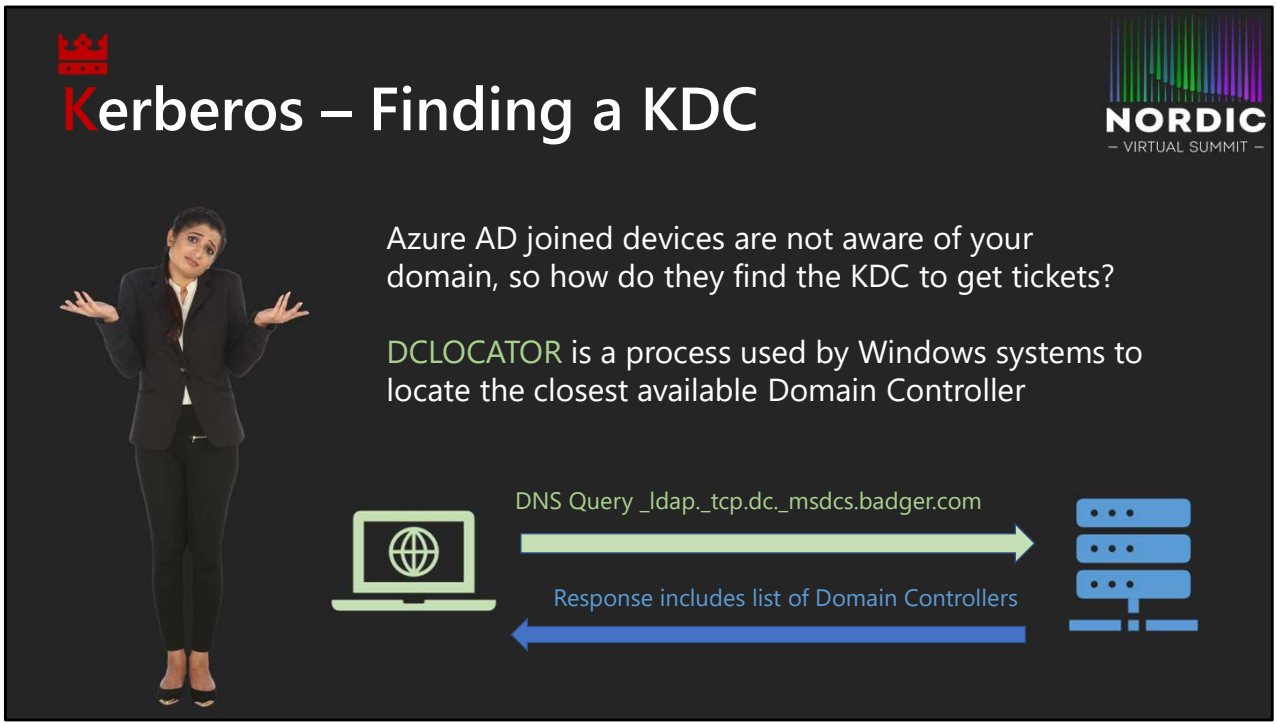
So what is Kerberos and how does it help us?

Kerberos is King

Some Kerberos basics

1. "Kerberos" is just a cryptographic ticketing system
2. In order to request tickets to domain resources, the Kerberos protocol needs to know where the "Ticket Master" is
3. The "Ticket Master" is called the Key Distribution Centre (KDC)
4. The KDC in a Windows Domain is a Domain Controller

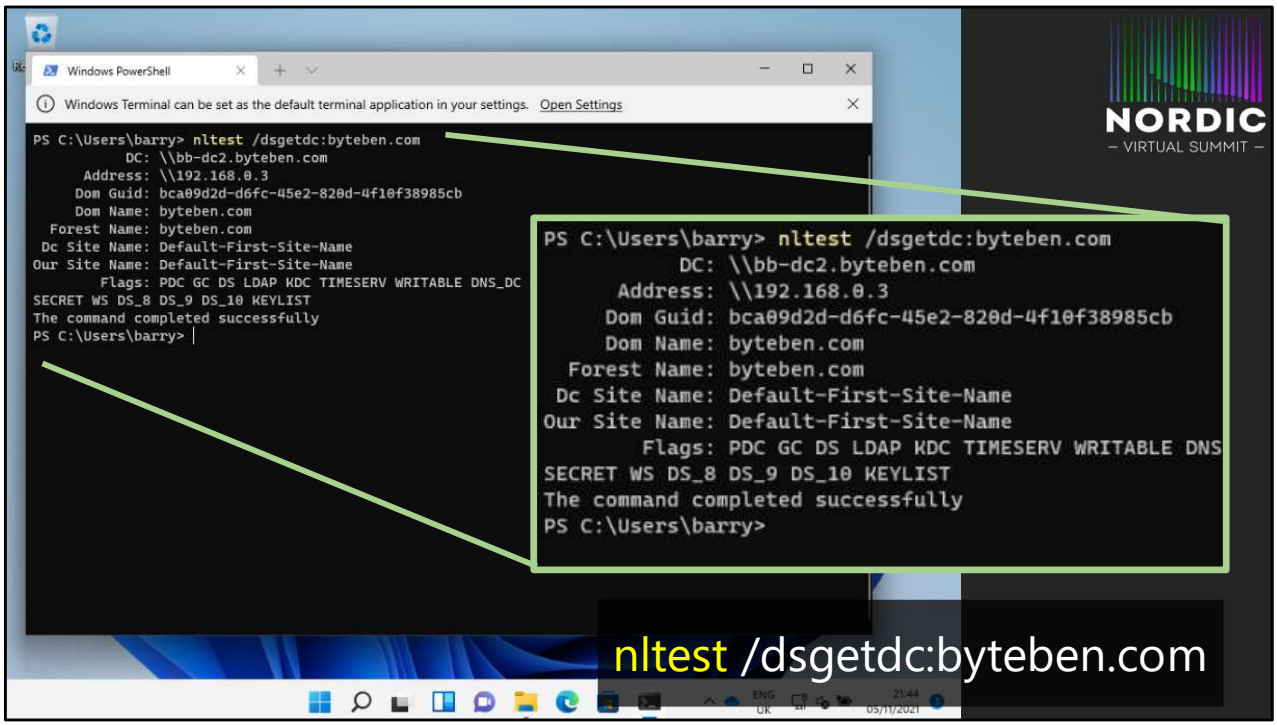
here are some basics of Kerberos. Basically I need to get a ticket from the domain controller, or KDC, to prove who I am to the service e.g. file server



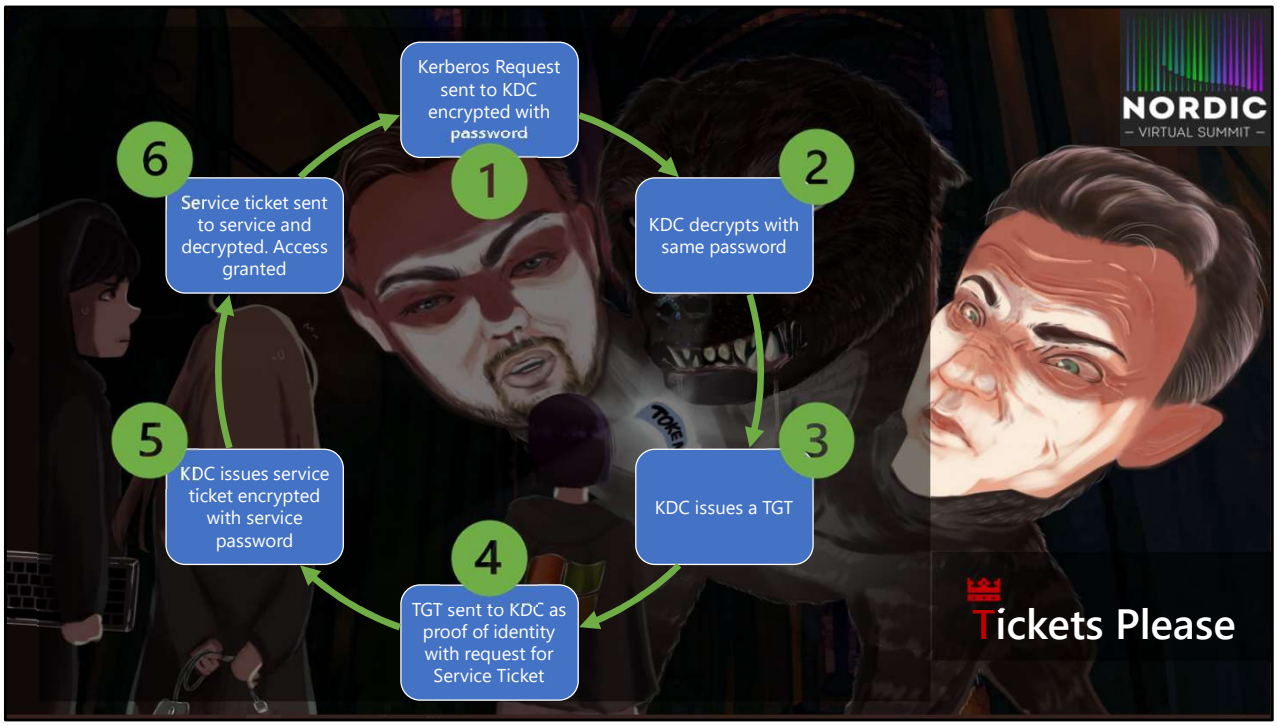
First my client needs to find the KDC, how does it do this when the client knows nothing about the domain?
Remember we have some synced attrbiutes. “OnPremise Domain Name”

DCLocator needs a domain hint, which it gets from the onpremisedomainname that came down with the PRT.
A Domain Controller (KDC) is then returned to the client

NEXT SLIDE: We can show this manually to prove DC locator works



NLTEST – show on Windows 11 device

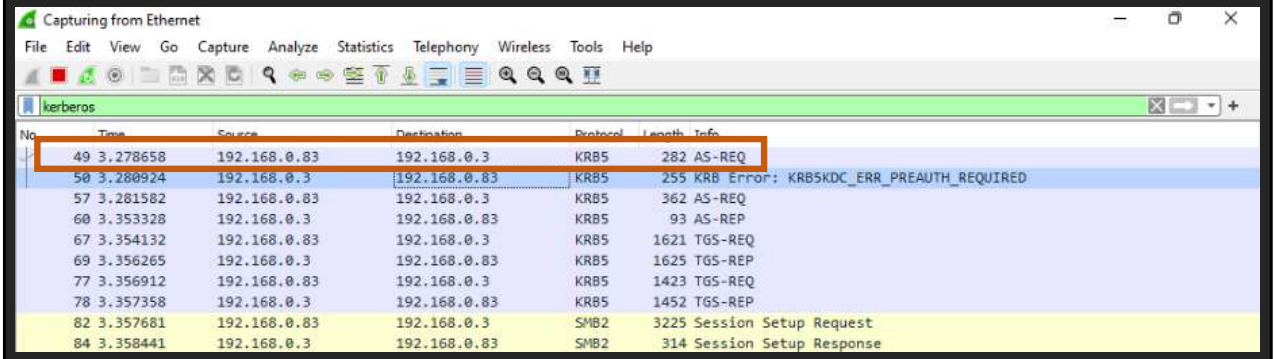


Now we know where the KDC is, lets go into a bit more detail on how Kerberos tickets work and help us access domain resources

high level

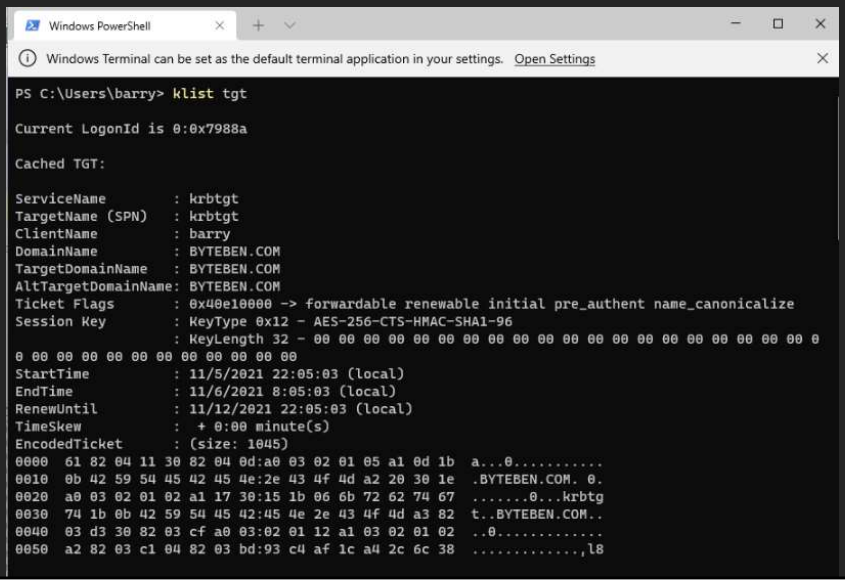
1. Kerberos request sent to the KDC. Request is encrypted with user password.
2. The KDC know the user password, its in AD, so it uses it to try and decrypt the request.
3. If it successfully decrypts it, the passwords match so the user is good. The KDC then issues a “Golden” ticket to the user. The golden tickets, or TGT is proof the user authenticated. Authentication has a lot of overhead so we don’t want to keep doing it.
4. The uer then sends that TGT (proof of they can come into the club) along with another request to access a service, like CIFS (fileshare)
5. The KDC sees the user has a valid TGT (BTW, only the KDC can decrypt the TGT) and issues a “Service Ticket”. The service ticket contains things like group membership and service requested.
6.

Kerberos – Tickets please



The client sends a request for a ticket to the KDC

Kerberos – Tickets please

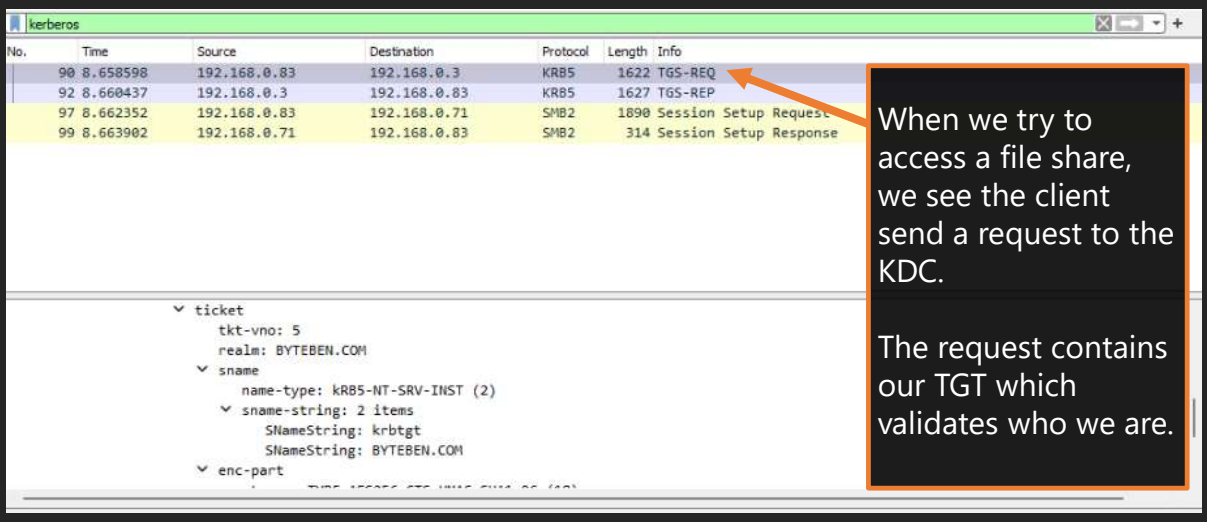


klist tgt

klist tgt allows you to view the specifics of the issued TGT

This TGT will now be used to prove identity for future AS requests in this session

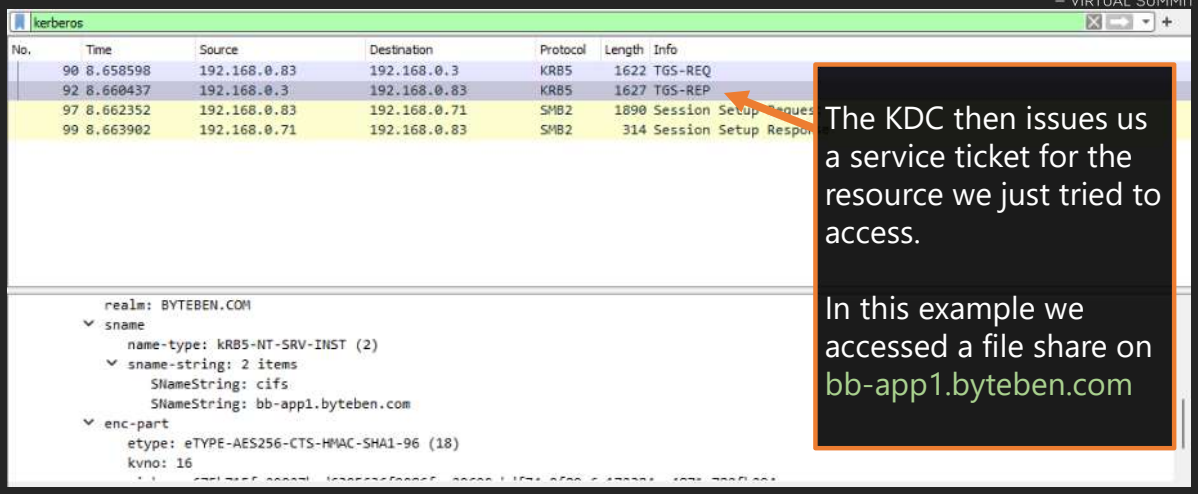
Kerberos – Tickets please



When we try to access a file share, we see the client send a request to the KDC.

The request contains our TGT which validates who we are.

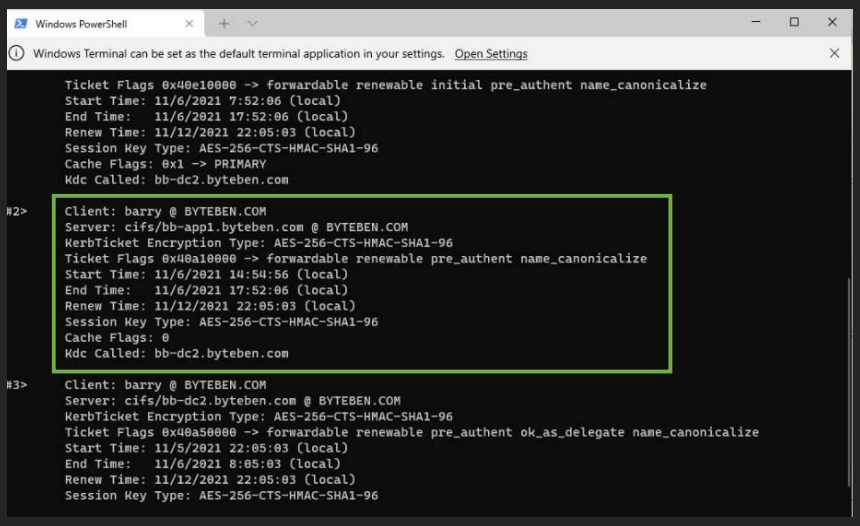
Kerberos – Tickets please



The KDC then issues us a service ticket for the resource we just tried to access.

In this example we accessed a file share on bb-app1.byteben.com

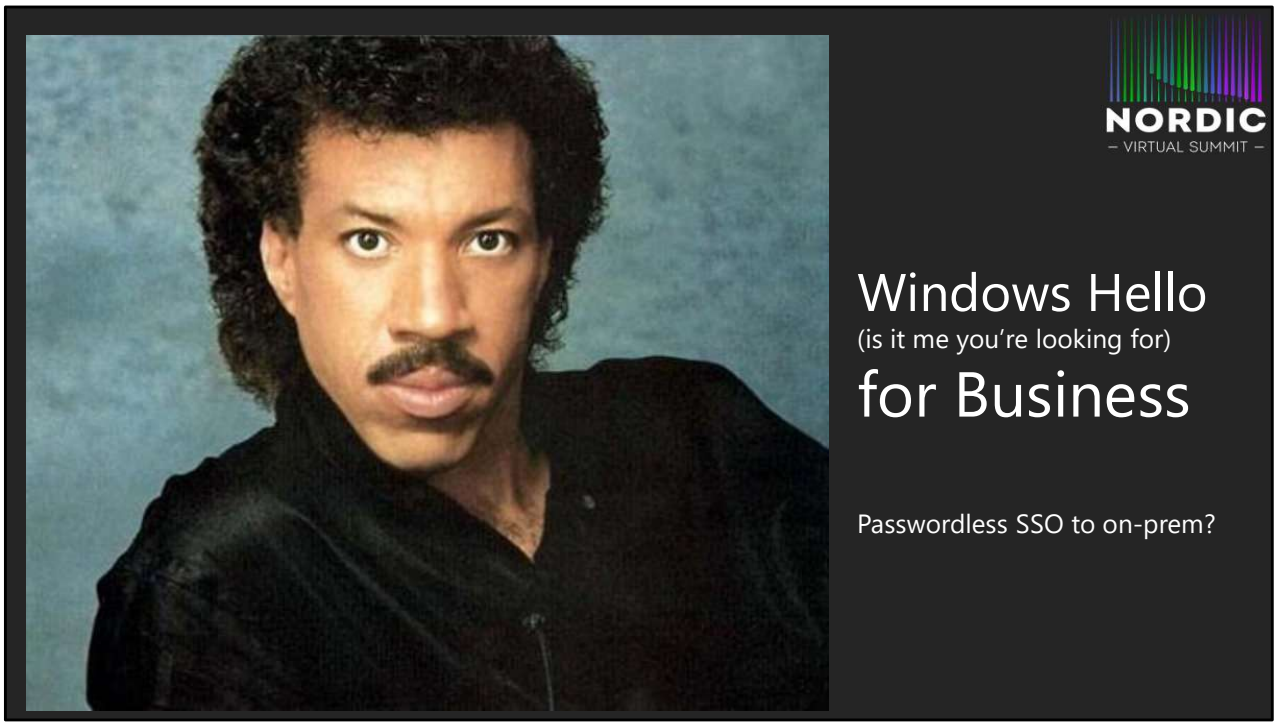
Kerberos – Tickets please



klist

klist displays all the service tickets we have been granted

Here is the service ticket we requested to access the file share

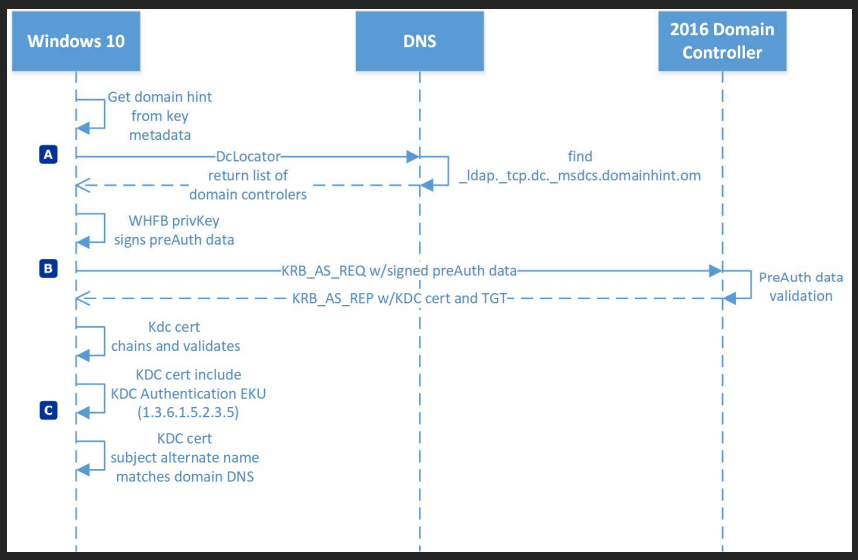


•PREREQUISITES
•https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-hybrid-aadj-sso-base

•Azure Active Directory Connect synchronization (not cloud sync!)
•Device registered in azure ad/preferably also intune managed
•Certificate Revocation List (CRL) Distribution Point (CDP)
•2016 Domain Controllers
•Domain Controller certificate
•Network infrastructure in place to reach your on-premises domain controller. If the machines are external, this can be achieved using any VPN solution.
DNS resolution!

•Demo on teamviewer

Kerberos – Windows Hello



Deepdive on WHfB auth:

https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-how-it-works-authentication

WHfB - The missing link

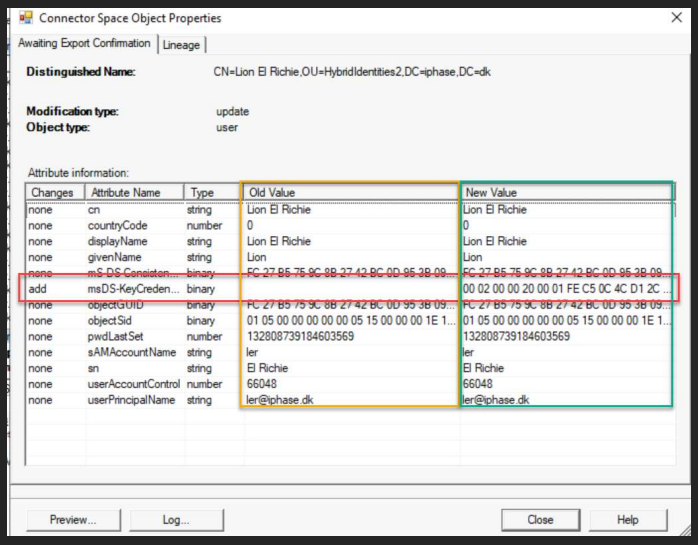
```
+----------------------------------------------------------------------+
| Device Details                                                       |
+----------------------------------------------------------------------+

             DeviceId : ce37eeff-9791-4608-bc8a-b2580052fbc9
           Thumbprint : 2C219CDD60FADC9DE70FE582DD29E43C8BFACD94
DeviceCertificateValidity : [ 2021-11-08 20:20:03.000 UTC -- 2031-11-08 20:50:03.000 UTC ]
        KeyContainerId : 99958628-c2c2-4074-be9c-6088a6978a0c
           KeyProvider : Microsoft Platform Crypto Provider
          TpmProtected : YES
      DeviceAuthStatus : SUCCESS
```

The msDS-KeyCredentialLink contains the WHfB key used complete the circle of trust.

Not available with “cloud sync” aka. “cloud provisioning”

WHfB - The missing link



The msDS-KeyCredentialLink contains the WHfB key used complete the circle of trust.

Not available with “cloud sync” aka. “cloud provisioning”

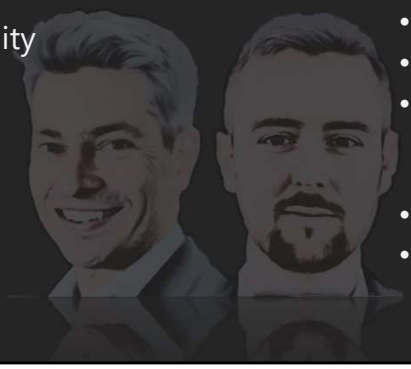

NORDIC
– VIRTUAL SUMMIT –
A moment of silence
For all the hybrid joined devices that are no longer with us after this presentation...

You have been listening to:

NORDIC
– VIRTUAL SUMMIT –

Ben «007» Whitmore

- Senior Cloud Consultant @ Cloudway
- 20+ years of ITPro experience
- MVP – Enterprise Mobility
- GOV IT experience
- BLOGGER/Writer
  - MSEndpointMgr.com
  - byteben.com
- Proud father of 3 girls
- Avid DOCS reader



Michael Mardahl

- Cloud Architect @ APENTO
- 20+ MS Certifications
- 20+ years of ITPro experience
- MVP – Enterprise Mobility
- ISO27001-LI Certified
- BLOGGER/Writer
  - MSEndpointMgr.com
  - MeasureUp!
- Proud father to an autist girl
- A bit bonkers