From the trenches: Six Common Mistakes in Hybrid Identity

Sander Berkouwer

DirTeam.com

Hybrid Identity

- Hybrid Identity is extending
  - ~~On-premises~~ Active Directory ~~Domain Services~~

    to
  - ~~Microsoft's Azure Active Directory service~~ Entra ID
- Benefits include:
  - Single Sign-on (SSO) to cloud apps
  - Conditional access and multi-factor authentication

Problem 1

Choosing or sticking with the wrong authentication scenario

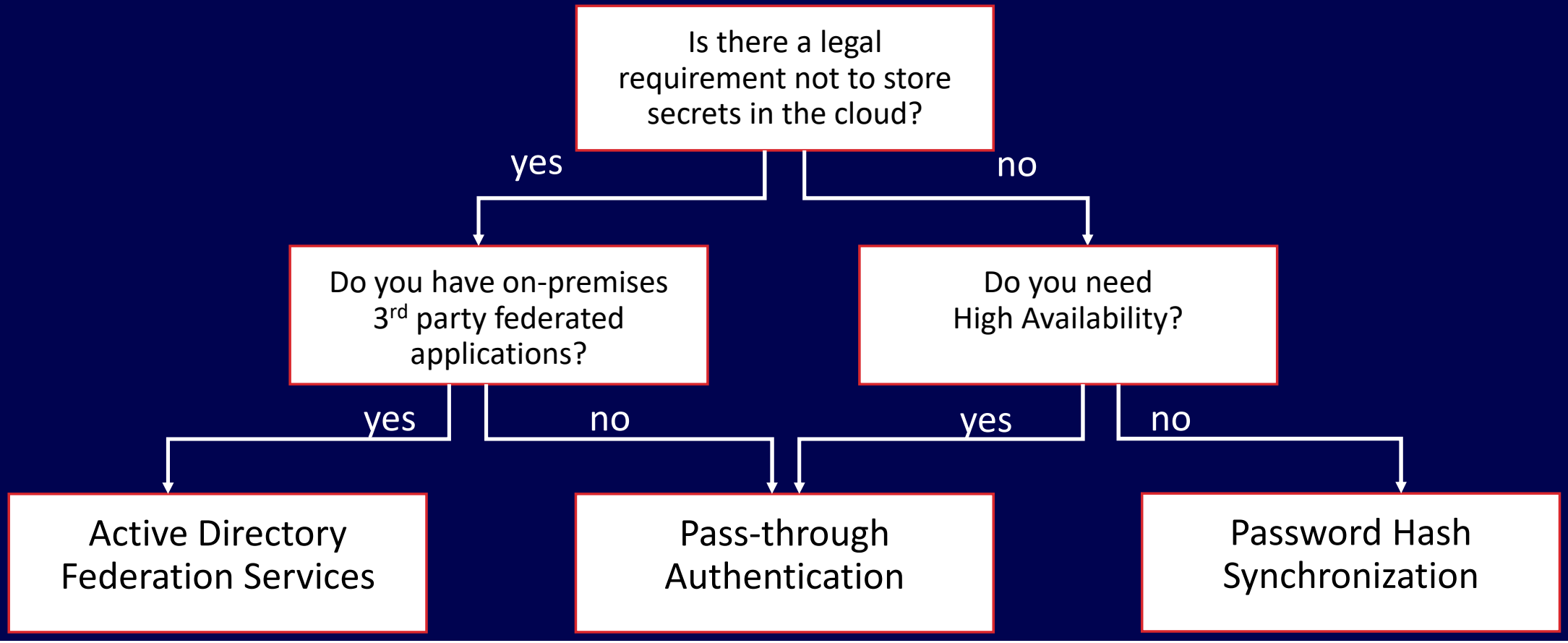
netwrix

Professional Development Systems BV

Hybrid Identity Authentication Scenarios

- Active Directory Federation Services (AD FS)
  - Single Sign-On, based on one identity in Active Directory Domain Services
  - Integrates and publishes on-premises and cloud web applications
- Password Hash Sync (PHS) (with optional Seamless Single Sign-on)
  - Same Sign-On, based on synchronization of objects and attributes
  - AES-256 OrgID Hash of the NT Hash is sync'ed with Entra ID
- Pass-through Authentication (PTA) (with optional Seamless Single Sign-on)
  - PTA Agents on-premises handling authentication requests placed on Azure Service Bus by Entra ID (Azure AD)

Choosing AD FS



netwrix

Professional Development Systems BV

Problem 2

Building upon an unhealthy Active Directory environment

netwrix

Professional Development Systems BV

Hybrid Identity is only as good as your AD DS

- Attribute integrity and lingering objects
  - Lingering objects: Objects on some Domain Controllers, not others
  - Resulting in unpredictable authentication and/or unexpected access
- Non-routable and/or non-registered top-level domains
  - DNS Domain Name for domains ending with .local, .int
  - Ideally, User Principal Name (UPN) needs to be added and changed, but Alternate Login ID is also a solution in some scenarios.
- UPN syntax mismatches
  - Critical for solutions with Entra Connect (Azure AD Connect)

Checking up on Active Directory Domain Services

- Use the free DirSync Error Remediation Tool (IdFix)
  - Use its Export functionality to make Pivot tables in Microsoft Excel
  - Apply your Entra Connect Filtering Options manually
- Use the Best Practices Analyzers
- Use Entra Connect Health for Active Directory Domain Services
- Are you a Microsoft Premier customer?
  - Request an Active Directory Risk Assessment (ADRAP)

Problem 3

Improperly configuring the AD FS and Entra Connect Service Accounts

netwrix

Professional Development Systems BV

Service Accounts

- Password changes, security implications
  - AD FS is usually internet-facing, so it benefits from extra security
  - We want regular password changes, host restrictions, etc.
- group Managed Service Accounts (gMSAs)
  - gMSAs solve ‘the service account problem’
  - gMSAs offer Automatic SPN and password management
  - AD FS and Entra Connect both support gMSAs for their services
- Windows Server 2008 DFL
  - 2008 Domain Functional Level, and above, offers automatic SPN management
  - Windows 8 and Windows Server 2012 (and up) offer Cmdlets

Entra Connect's Sync is not 100% one-way

- Entra Connect synchronizes
  - Synchronization cycles occur every 30 minutes, by default.
- The Source Anchor binds the accounts in Active Directory and Entra ID
  - Source Anchor for hard matching, e-mail addresses for soft matching
  - Source Anchor can be ObjectGUID, mS-DS-ConsistencyGUID, or other attribute of choice
- PHS, mS-DS-ConsistencyGUID and Writeback functionality require permissions
  - Password Hash Sync requires 'Replicate Changes' and 'Replicate Changes – All'
  - mS-DS-ConsistencyGUID is written with Base64 representation of first ObjectGUID
  - Password Writeback writes back passwords
  - Group Writeback provisions groups in Active Directory

Problem 4

Improperly designing the infrastructure

netwrix

Professional Development Systems BV

The Right AD FS Infrastructure

- AD FS Server Farms
  - AD FS can easily be deployed highly available, with Windows / 3rd Party NLB
  - Deploy AD FS Proxies / Web Application Proxies in perimeter networks
- Windows Internal Database or SQL Server
  - A WID farm has a limit of 30 Windows Server 2016-based federation servers, only master is writable, and does **not** support token replay detection or artifact resolution
- SQL Server High Availability
  - Take advantage of your existing SQL Server investments
  - Take advantage of database mirroring, fail-over clustering, and monitoring

The Right Entra Connect implementation

- Entra Connect is a Single Point of Failure
  - Only one Entra Connect installation can be actively syncing to a tenant
  - Entra Connect cannot be clustered
- Entra Connect Staging Mode is the answer to everything, right?
  - No, Staging Mode servers only share a little bit of configuration automatically
  - No, Entra Connect's Staging Mode offers *warm standby* only
    - Resolution time still depends on time needed to detect the fault
- Pass-through Authentication agents aren't monitored
  - PTA Agents report their status in the Entra Portal
  - This status only provides info on its connection to Azure, not to AD

Entra Connect Design Choices

- Database
  - Entra Connect uses a SQL Database to store its Metaverse
  - By default, SQL Server Express is installed, limiting the Metaverse to 100,000 objects
  - Choose SQL Server Standard, or up, for increased object limits
- Staging Mode
  - Staging Mode offers Entra Connect *warm stand-by*
  - Same settings, same rules, same metaverse, different service account, different database, different GUID
  - Use Entra Connect Configuration Diagrammer to compare Staging Mode and actively syncing install

Problem 5

Let Time take its Toll

netwrix

Professional Development Systems BV

Take Care of Proper Time Synchronization

- Time Sync within an Active Directory environment
  - W32time follows Active Directory hierarchy and sites configuration
  - Set the time for an environment through the PDCe
- Time Sync within Virtual Machines
  - Virtual machines always sync time with host on boot
  - Continuous time sync is configured with VMware tools, Hyper-V ICs, etc.
- Time Sync within Perimeter Networks
  - Could be virtual machine time sync, could be an external source
  - Will be none, if you don’t configure it…

Take Care of Proper Time Synchronization

- Time Sync within an Active Directory environment
  - W32time follows Active Directory hierarchy and sites configuration
  - Set the time for an environment through the PDCe
- Time Sync within Virtual Machines
  - Virtual machines always sync time with host on boot
  - Continuous time sync is configured with VMware tools, Hyper-V ICs, etc.
- Time Sync within Perimeter Networks
  - Could be virtual machine time sync, could be an external source
  - Will be none, if you don’t configure it…

Problem 6

Not managing Hybrid Identity (enough)

netwrix

Professional Development Systems BV

AD FS is not a Fire and Forget Scenario

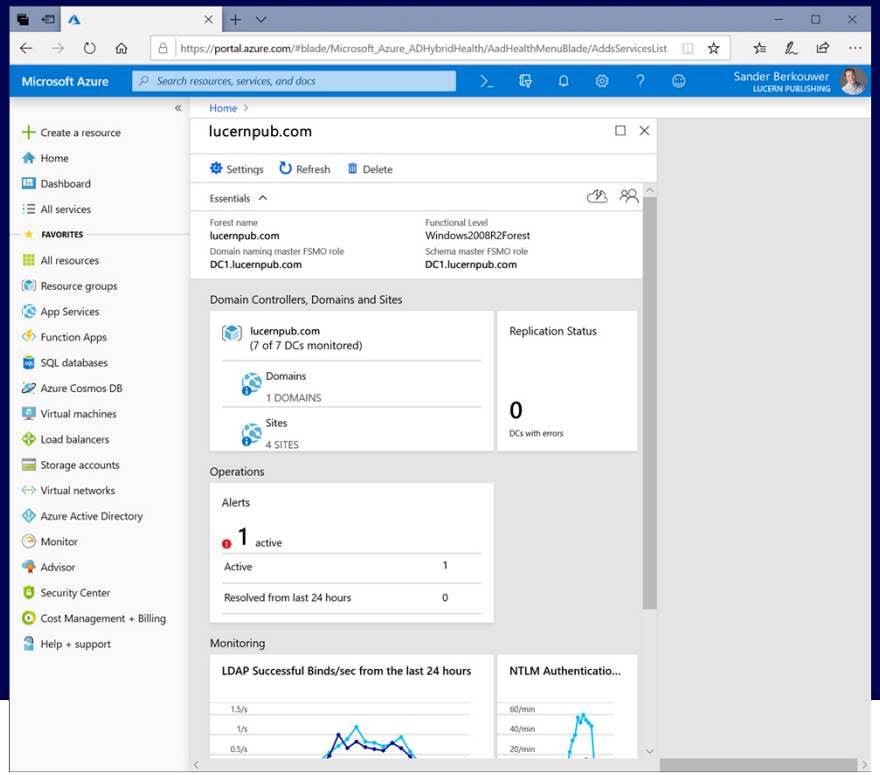
- Windows Update for Security and Reliability improvements
  - AD FS is updated on 'Patch Tuesdays'.
  - Security updates only light up after you install the AD FS role
- Monitoring AD FS
  - Use Systems Center Operations Manager (with GSM), Operations Management Suite, Entra Connect Health, (or your preferred 3rd Party solution)
- Auditing AD FS
  - AD FS offers built-in auditing and logging of errors and warnings
  - Decentralized per AD FS Server in the AD FS Farm

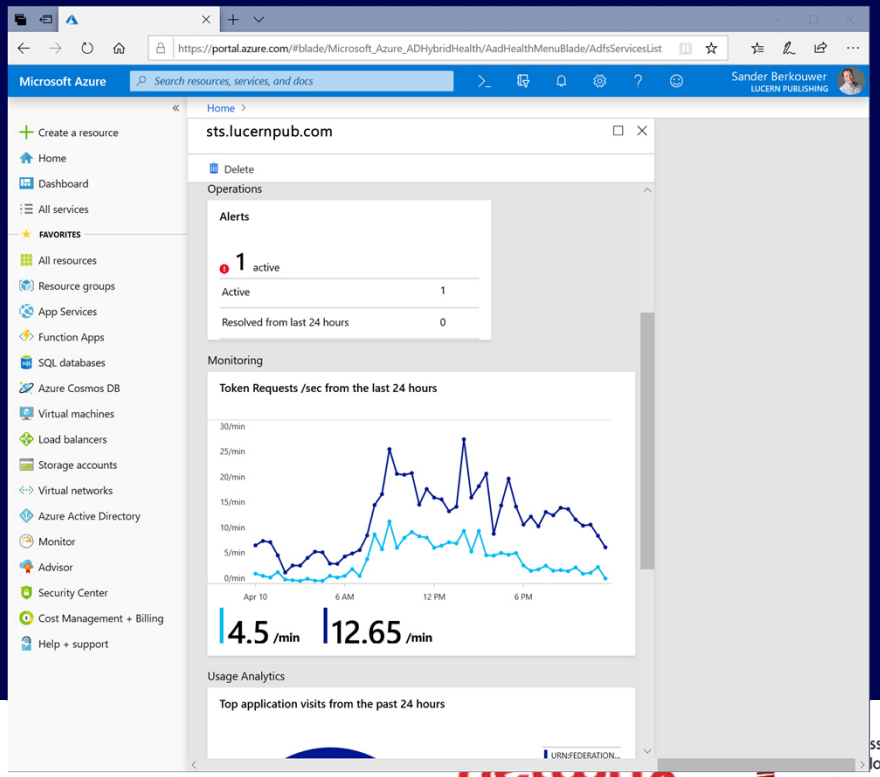
Managing AD FS with Entra Connect

- Entra Connect
  - When you want Single Sign-On with Office 365, think Entra Connect
  - Entra Connect can setup AD FS for you, can manage AD FS with you
- Management of AD FS through Entra Connect
  - Additional AD FS claims rules for device registration and mS-DS-ConsitencyGUID,
  - Management tasks made easy:
    - Repair the Relying Party Trust between AD FS and Entra ID (HowTo)
    - Add an additional DNS Domain name in Entra ID to federate (HowTo)
    - Update the AD FS Service Communications certificate (HowTo)
    - Verify AD FS Login

Entra Connect Health

- One Single Pane to Manage Hybrid Identity Challenges:





Concluding

netwrix

Professional Development Systems BV

Getting the Technology Right

- Choose the right Authentication Scenario
  - Why not go for Password Hash Sync or Pass-through Authentication?
- Design the right AD FS and Entra Connect Infrastructure
  - Getting it right the first time makes all the difference.
- Manage AD FS with Entra Connect
  - Manage with ease and leverage Entra Connect Health
- Check up on your Active Directory Domain Services, regularly

Thank you!

DirTeam.com

@SanderBerkouwer

www.linkedin.com/in/SanderBerkouwer

www.youtube.com/c/SanderBerkouwer

netwrix

Professional Development Systems BV