There’s Something About Service Accounts

hub.trimarcsecurity.com/post/there-s-something-about-service-accounts

Sean Metcalf March 21, 2019

Service accounts are that gray area between regular user accounts and admin accounts that are often highly privileged. They are almost always over-privileged due to documented vendor requirements or because of operational challenges (“just make it work”).

We can discover service accounts by looking for user accounts with Kerberos Service Principal Names (SPNs) which I call SPN Scanning. Service accounts without SPNs can also be discovered by querying AD accounts for ‘SVC’, or ‘Service’, or common vendor product names.

The following PowerShell commands require the Active Directory PowerShell module.

Discover service accounts (user accounts with SPNs):

```
get-aduser -filter {ServicePrincipalName -like “*”} -Properties
PasswordLastSet,LastLogonDate,ServicePrincipalName,TrustedForDelegation,TrustedtoAu
```

```
PS C:\Windows\system32> Get-ADUser -filter {ServicePrincipalName -like "*"} -property serviceprincipalname



DistinguishedName    : CN=krbtgt,CN=Users,DC=lab,DC=adsecurity,DC=org
Enabled              : False
GivenName            :
Name                 : krbtgt
ObjectClass          : user
ObjectGUID           : 6fd9529f-0805-4f3c-bb4d-29ad2ac377ef
SamAccountName       : krbtgt
serviceprincipalname : {kadmin/changepw}
SID                  : S-1-5-21-1473643419-774954089-2222329127-502
Surname              :
UserPrincipalName    :

DistinguishedName    : CN=svc-SQLAgent01,OU=Service Accounts,DC=lab,DC=adsecurity,DC=org
Enabled              : True
GivenName            :
Name                 : svc-SQLAgent01
ObjectClass          : user
ObjectGUID           : eba3c611-6ea6-46bc-b68c-c8f28685e7f5
SamAccountName       : svc-SQLAgent01
serviceprincipalname : {MSSQLSvc/ADSAPPSQL03.lab.adsecurity.org:1433,
                       MSSQLSvc/ADSAPPSQL02.lab.adsecurity.org:1433,
                       MSSQLSvc/ADSAPPSQL01.lab.adsecurity.org:1433}
SID                  : S-1-5-21-1473643419-774954089-2222329127-1606
Surname              :
UserPrincipalName    : svc-SQLAgent01@lab.adsecurity.org

DistinguishedName    : CN=svc-MSSQLServer01,OU=Service Accounts,DC=lab,DC=adsecurity,DC=org
Enabled              : True
GivenName            :
Name                 : svc-MSSQLServer01
ObjectClass          : user
ObjectGUID           : 2260906f-6985-404b-b6ea-fbed5d573bff
SamAccountName       : svc-MSSQLServer01
serviceprincipalname : {MSSQLSvc/adsmswin2k8r2:1433, MSSQLSvc/adsmswin2k8r2.lab.adsecurity.org:1433}
SID                  : S-1-5-21-1473643419-774954089-2222329127-1613
Surname              :
UserPrincipalName    : svc-MSSQLServer01@lab.adsecurity.org
```

Discover probable AD Admin accounts (user accounts with AdminCount set to 1):

```
get-aduser -filter {AdminCount -eq 1} -Properties
Name,AdminCount,ServicePrincipalName,PasswordLastSet,LastLogonDate,MemberOf
```

```
PS C:\> get-aduser -filter {AdminCount -eq 1} -prop * |
select name,Created,PasswordLastSet,LastLogonDate

name            Created              PasswordLastSet      LastLogonDate
----            -------              ---------------      -------------
ADSAdministrator 8/27/2015 7:09:40 PM 6/10/2016 6:41:42 PM 6/10/2016 6:29:50 PM
krbtgt          8/27/2015 7:10:22 PM 8/27/2015 7:10:22 PM
LukeSkywalker   8/29/2015 7:21:11 PM 8/29/2015 7:26:02 PM 8/29/2015 7:29:52 PM
Kylo Ren        6/11/2016 2:12:41 PM 6/11/2016 2:12:41 PM
```

While Domain Admins is the most commonly used AD admin group, there are several others that could be used.

Common privileged AD groups that may contain Service Accounts:

- Administrators: full administrative rights to the AD domain and Domain Controllers.
- Domain Admins: full administrative rights to computers joined to the domain (default) and full administrative rights to the AD domain and DCs (through membership in the Administrators group).
- Backup Operators: default rights to backup and restore Active Directory and Domain Controllers.
- Server Operators: able to logon to Domain Controllers and provides ability to perform some administrative actions on Domain Controllers.
- Enterprise Admins: full administrative rights to all domains and Domain Controllers in the AD forest (through membership in the Administrators group). Also has special forest admin rights such as DHCP. In a single domain forest, this group should remain empty until needed.
- Schema Admins: able to modify the AD schema for the forest. This group should remain empty until needed.

Rarely does a service account actually require Domain Admin level rights. I reviewed vendor documentation across multiple products and found that there were many things in common.

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

Eventually a pattern emerged…

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

When we perform Active Directory Security Assessments for customers, we almost always discover service accounts in Domain Admins (and sometimes other privileged AD groups) and help the customer (and sometimes the vendor) figure out how to reduce the rights for the service account so it can be removed from Domain Admins.

Common Service Accounts in Domain Admins (or other AD Admin groups):

Microsoft AGPM:

Used to manage group policy objects (GPOs) in AD. This account does not need to be in Domain Admins or a highly privileged AD group.

Delegation guidance: https://blogs.technet.microsoft.com/askds/2008/12/16/agpm-least-privilege-scenario/

Altiris/ADBackup/Backup/BackupExec/CommVault/NetBackup/etc:

Backing up AD (and/or Domain Controllers) only requires membership in the Backup Operators group in AD. This group is specific to Active Directory and does not provide backup rights to other systems in the domain (default). These accounts should not require membership in Domain Admins. The caveat to this is that there are scenarios where a backup service account may require more rights than being a member of Backup Operators, such as when restoring user attributes in AD. This is for more advanced restoration scenarios and AD backup accounts should only be a member of the Backup Operators group (not Domain Admins) to start.

Service accounts that backup anything other than AD or DCs does not require membership in the AD Backup Operators group.

Archive:

Typically an Exchange service account for archiving Exchange mailboxes. There is no reason for an Exchange related service account to be a member of privileged AD groups.

AV/McAfee/Trend:

AV service accounts never need Domain Admin rights.

Azure:

This account may be used for Azure AD Connect (which should be granted rights on the domain root by the installer) or another Azure purpose.

There is no reason for this account to be in Domain Admins.

BES:

This is for the Blackberry Enterprise Server service account which does not require Domain Admin rights (and may no longer be active on the network).

CyberArk/Reconcile/SecretServer:

CyberArk started as an enterprise password vault and has grown its offering into other security controls.

Entrust/PKI:

There are specific groups for PKI products to enable certificate actions. These should be used instead of Domain Admins.

Exchange/EXAdmin/Mail:

Exchange service accounts never need Domain Admin rights.

Fax:

No. This does not require Domain Admin rights ever and should be removed immediately.

Imanami:

Imanami provides group membership management capability (among others) and some products. These service accounts should be custom delegated to the OUs containing the objects that require modification.

Landesk:

Landesk is used for computer management and should not be in Domain Admins.

Quest:

There are several Quest products that may require privileged rights on Domain Controllers. These rights need to be reviewed and determined if appropriate.

PaloAlto:

Typically this is used to match domain users to computers to identify a person to network and internet activity. There is a better way to configure systems that need to perform this mapping which usually involves reading the Domain Controller security log: https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-admin/user-id/create-a-dedicated-service-account-for-the-user-id-agent

Patch/Shavlik:

Many patching systems tend to use Domain Admins since it provides administrative rights to every computer. This is not the best way to do this.

Break out patching by system type and ensure that there is a different service account for each one:

- Workstations
- Servers
- Domain Controllers

ServiceNow:

Required rights depend on the desired capability. Ensure that least privilege is followed and break out service accounts by computer type:

- Workstations
- Servers
- Domain Controllers

Qualys/Nessus/Rapid7Scan/Scanner/VulnScan/VulnScanner:

Vulnerability scanning system service accounts are often placed in Domain Admins in order to have administrative rights on every computer in the domain.

Split scanning into different scan “buckets”

- Workstations with a VulnScan-wrk service account
- Servers with a VulnScan-srv service account

- Domain Controllers with a VulnScan-DC service account.

SCCM/Management/Mgmt/etc:

Microsoft System Center Management is typically used to deploy applications, update system settings, patch operating systems and applications, etc.

SCOM/Health/Insight/MOM/Management/Mgmt/etc: Microsoft System Center Operations Management is a monitoring tool provided by Microsoft which monitors system and application health via event logs and “Management Packs”.

There is often a standard service account which runs the system and then a separate “action account” used on Domain Controllers which enables a tiered server operator the ability to “click resolve” issues on a Domain Controller without being a member of Domain Admins.

SQL:

There is no reason for SQL to ever be in a privileged AD group (like DA).

We have also found SQL Service Principal Names (SPNs) configured on the default domain Administrator account which is even worse due to the risk of Kerberoasting.

Unity:

Cisco service accounts never need Domain Admins. Cisco updated the documentation for Cisco service accounts in late 2018, so check for the updated guidance.

Varonis:

Varonis is mostly used for tracking Windows system share permissions and access. This service account may be placed in Domain Admins in order to support a Varonis service on Domain Controllers. There may be a way to run this service account as a member of Server Operators instead.

VCenter/VMWare:

There is no reason for VMWare service account to be a member of Domain Admins (or any other privileged AD group)

VPN:

There is no good reason to have a VPN service account in Domain Admins. We have seen a VPN related service account in Domain Admins before just to support users connecting via VPN who have expired passwords. With DA rights, the VPN solution can inform the user of an expired password, request a new password, and update the password for the user's AD account on behalf of the user in AD.

The VPN service account does not require Domain Admin rights to change passwords on behalf of the user. These rights can be easily delegated on the OU containing users who will connect via VPN.

We have a Kerberos Service Principal Name (SPN) list here at ADSecurity.org which is regularly updated (a few times a year) which maps known SPNs to applications. This is a great way to discover enterprise applications deployed on a network.

Conclusion A vendor saying that their service account needs to be in Domain Admins is not a requirement. Push back and ask for the specific rights that are required. Any service accounts that "require" Domain Controller rights should be severely limited – no service account should get membership in Domain Admins just for DC install. Any system/agent that can install/run code on a Domain Controller can elevate to Domain Admin, this includes all accounts that manage that system.

The following items can be custom delegated without too much issue which is better than adding service accounts to Domain Admin.

- add computer to the domain (facilitated through a user rights assignment on a DC GPO)
- delegated user rights – facilitated through custom delegation on user objects in an OU
- service account on Domain Controllers – question why this is necessary. If it is, this could be facilitated with an agent or using a service account that is a member of Server Operators (or Administrators if required).
- local administrator rights on all workstations – create a group called "Workstation Local Admins" (or similar) and add to the local Administrators group with Restricted Groups via a linked GPO to the OU that contains the workstations.

- local administrator rights on servers – create a group called "____ Server Local Admins" (or similar) and add to the local Administrators group with Restricted Groups via a linked GPO to the OU that contains the servers.

By Sean Metcalf

Trimarc provides leading expertise in security solutions including security reviews, strategy, architecture, and implementation. Our methodology leverages our internal research and custom tooling which better discovers multiple security issues attackers could exploit to compromise the environment. Trimarc security services fit between traditional compliance/audit reviews and standard penetration testing/red teaming engagements, providing deep understanding of Microsoft technologies, typical security issues and misconfigurations, and provide recommendations based on our own best practices custom-tailored to balance operational and security challenges.