



Assessing the Security of Your Active Directory: Privileged Account Risks and Controls

Sponsored by

netwrix

Thanks to

- Made possible by

netwrix

Preview of key points

- Routes to privileged access in Active Directory
- Key controls to assess
- Visibility

Routes to privileged access in Active Directory

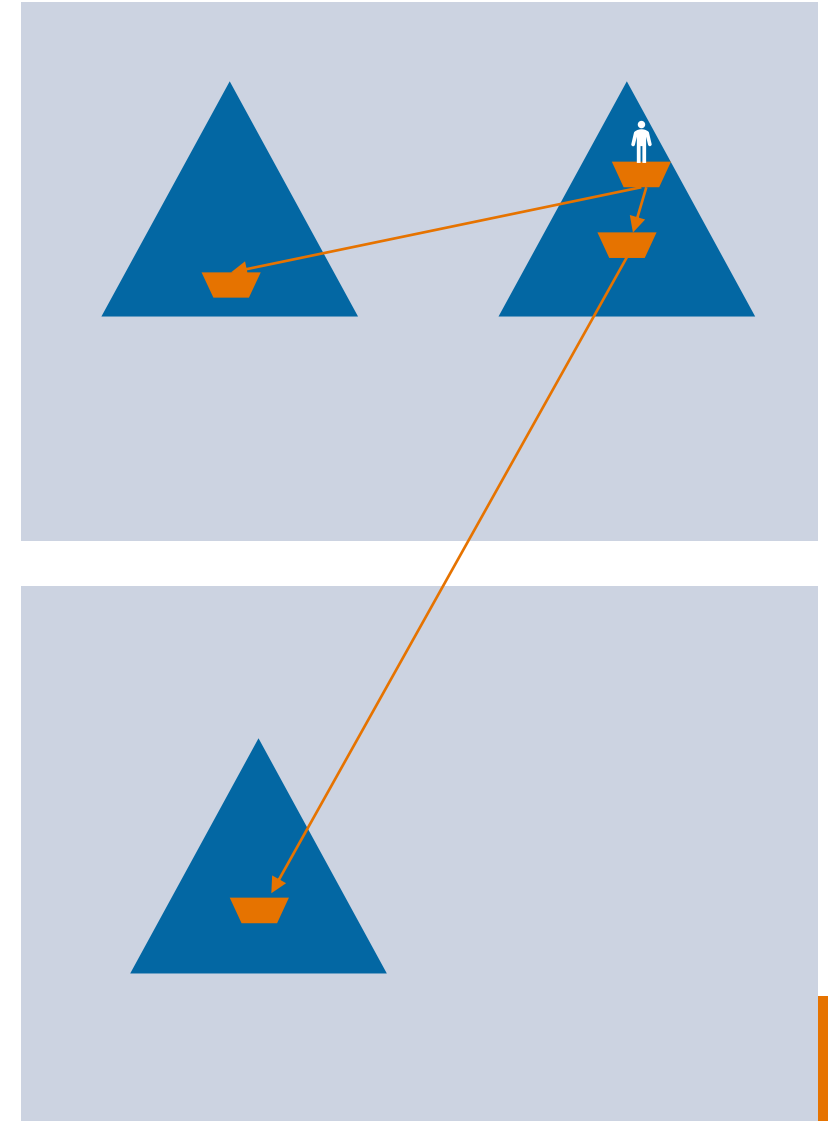
- Group memberships taking into account nesting and domain boundaries
- Admin-equivalent user rights on domain controllers
- Compromise of workstations where admins have logged on in the past or present
- Access to non-DC infrastructure applications
- The right directory object permissions to certain
 - Groups
 - Users
 - Group Policy Objects
 - Organizational Units
- Access to virtualization infrastructure
- Physical access to domain controllers

Physical access to domain controllers

- More difficult than in the past to compromise DCs via physical access
- Read Only DCs does not eliminate all risks
- Best defense is TPM based BitLocker / SecureBoot

Group memberships taking into account nesting and domain boundaries

- Administrators
- Domain Admins
- Enterprise Admins
- Account Operators
- Group Policy Creator Owners
- And all other admin and operator groups



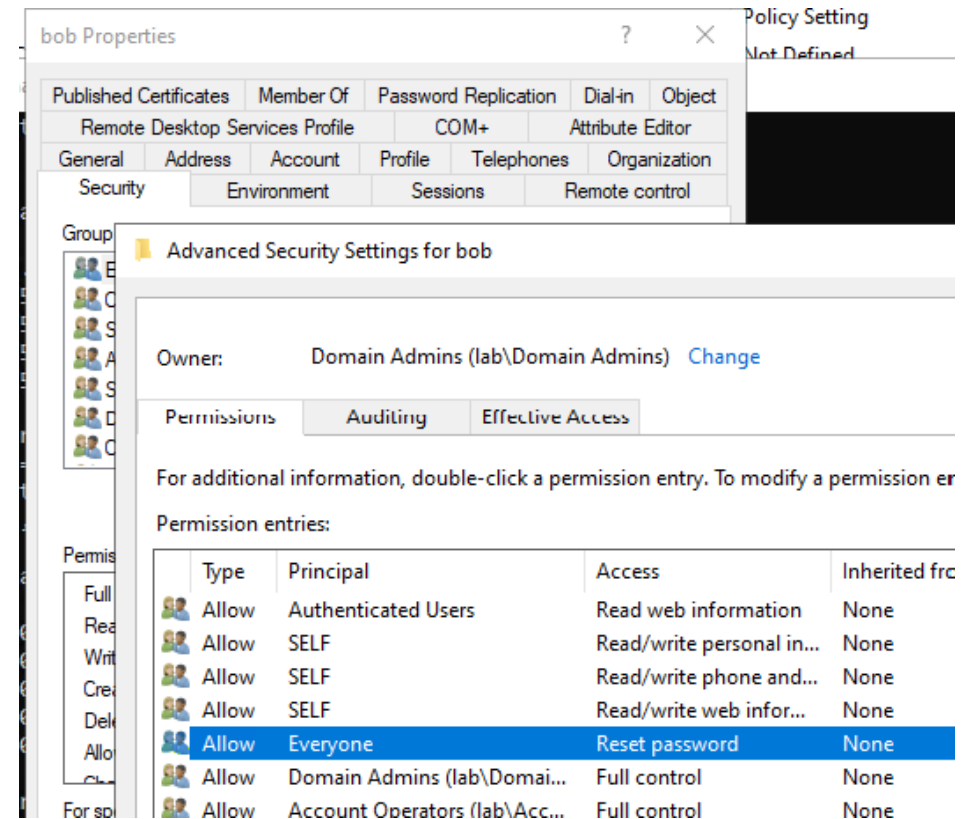
Admin-equivalent user rights on domain controllers

Policy	Policy Setting
Access Credential Manager as a trusted caller	Not Defined
Access this computer from the network	Everyone,Administrators,Authe...
Act as part of the operating system	Not Defined
Add workstations to domain	Authenticated Users
Adjust memory quotas for a process	LOCAL SERVICE,NETWORK SER...
Allow log on locally	Administrators,Backup Operato...
Allow log on through Remote Desktop Services	Not Defined
Back up files and directories	Administrators,Backup Operato...
Bypass traverse checking	Everyone,LOCAL SERVICE,NETW...
Change the system time	LOCAL SERVICE,Administrators,...
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,*S-1-5-32-549
Generate security audits	LOCAL SERVICE,NETWORK SER...
Impersonate a client after authentication	Not Defined
Increase a process working set	Not Defined
Increase scheduling priority	Administrators,Window Manag...
Load and unload device drivers	Administrators,Print Operators
Lock pages in memory	Not Defined
Log on as a batch job	Administrators,Backup Operato...
Log on as a service	Not Defined
Manage auditing and security log	Administrators
Modify an object label	Not Defined
Modify firmware environment values	Administrators
Obtain an impersonation token for another user in the same session	Not Defined
Perform volume maintenance tasks	Not Defined
Profile single process	Administrators
Profile system performance	Administrators,NT SERVICE\Wdi...
Remove computer from docking station	Administrators
Replace a process level token	LOCAL SERVICE,NETWORK SER...
Restore files and directories	Administrators,Backup Operato...
Shut down the system	Administrators,Backup Operato...
Synchronize directory service data	Not Defined
Take ownership of files or other objects	Administrators

Permissions to directory objects

- Permission on sensitive AD objects at the object level or on parent organizational units

User account	Reset password
Group	Write membership
Group Policy Object	Write
Organizational Unit	All of the above Create user accounts



bob Properties

Published Certificates Member Of Password Replication Dial-in Object
Remote Desktop Services Profile COM+ Attribute Editor
General Address Account Profile Telephones Organization
Security Environment Sessions Remote control

Group

Advanced Security Settings for bob

Owner: Domain Admins (lab\Domain Admins) [Change](#)

Permissions Auditing Effective Access

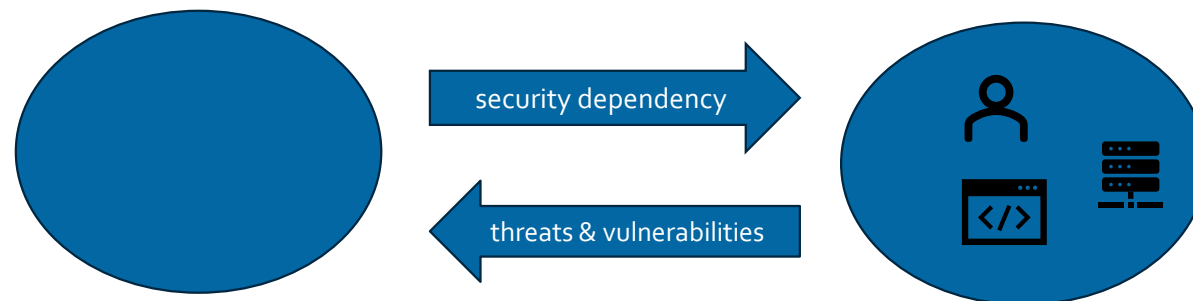
For additional information, double-click a permission entry. To modify a permission entry, double-click a permission entry.

Permission entries:

Type	Principal	Access	Inherited from
Allow	Authenticated Users	Read web information	None
Allow	SELF	Read/write personal information	None
Allow	SELF	Read/write phone and fax information	None
Allow	SELF	Read/write web information	None
Allow	Everyone	Reset password	None
Allow	Domain Admins (lab\Domain Admins)	Full control	None
Allow	Account Operators (lab\Account Operators)	Full control	None

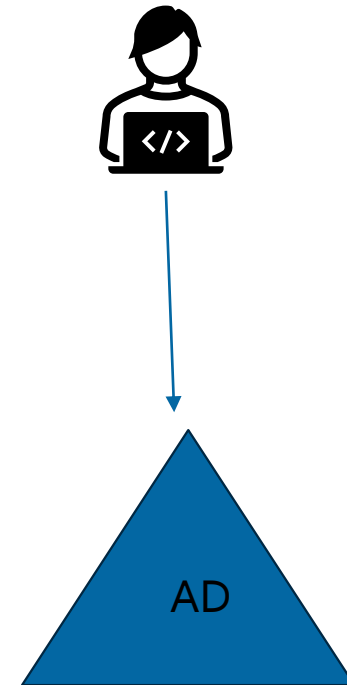
Compromise of any system/ application upon which AD has a security dependency

- Examples
 - Entra Connect
 - Backup and AD recovery tools
 - Identity and Access Management systems
 - Virtualization infrastructure
 - Systems management
- All such systems are same security tier zero as domain controllers

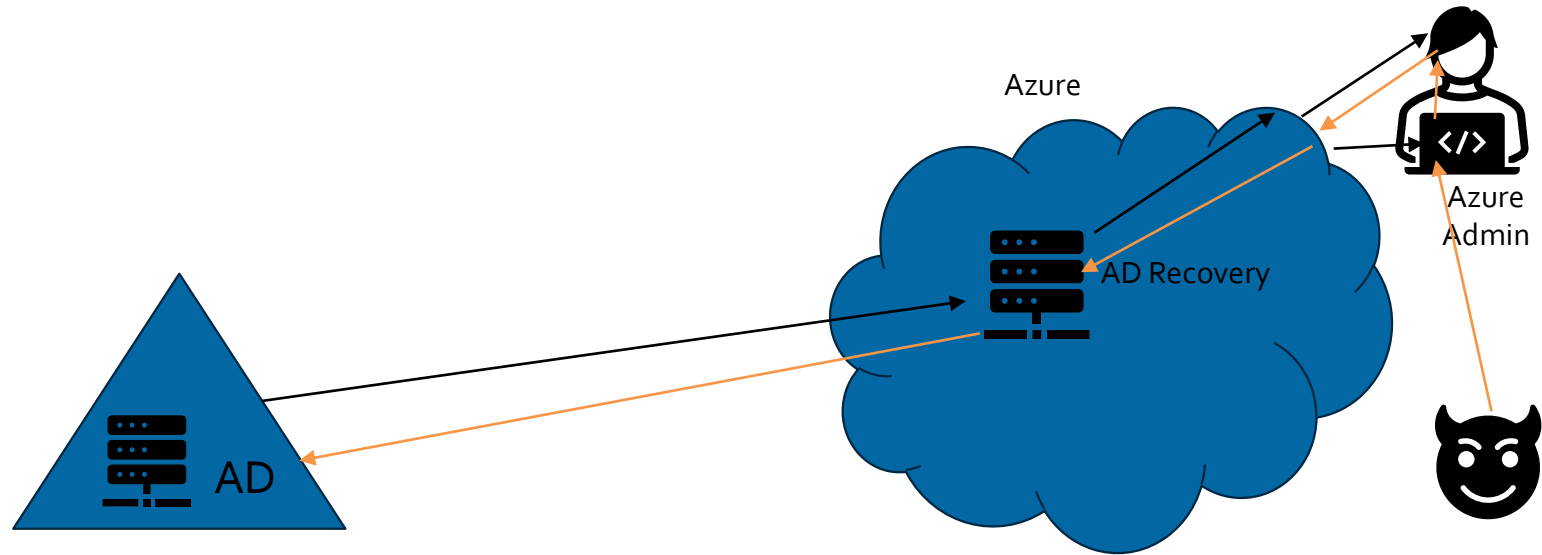


Workstations and any other system where privileged user logs on

- Logon to a computer with AD admin authority
 - That computer becomes same security tier as domain controller
- Pass-the-Hash
 - Other credential harvesting attacks
- Execution
- Privileged elevation

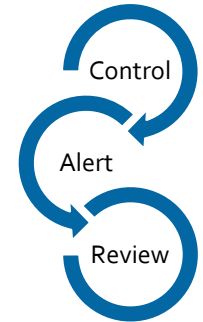


Compromise
of any system/
application
upon which AD
has a security
dependency



Key controls to assess

- Group membership
- Rights assignments on domain controllers
- Permission changes to key objects in AD
- Endpoint logon activity by privileged users
 - Strictly enforce Secure Admin Workstations (SAW)
- Continuous discovery of all adjacent and lower tier systems
 - Logical
 - Physical



Visibility

- It's not a simple matter to get a list of all privileged users in AD
- Let alone
 - All applications, systems and accounts upon which AD has a security dependency
- Requires vigilance and detective work
- Visibility into
 - Security logs
 - Rights
 - Permissions
 - Logon activity
 - AD objects
 - Users
 - Groups
 - Ous
 - Permissions

Next Up

- Jennifer Taufan, Solutions Engineer at Netwrix, will show you how to use Netwrix Auditor to:
 - Report on privileged accounts in Active Directory, including object permissions
 - Monitor logons of your users and alert you to suspicious activity
 - Generate audit trails and reports for privileged activities
 - Prepare for audits and prove compliance

Netwrix Auditor

Product Demonstration

Detect security threats, prove compliance and increase IT team efficiency with IT audit software from Netwrix



Jennifer Taufan,
Solutions Engineer at Netwrix

Next Steps

Risk Assessment – Overview

Risk name	Current value	Risk level
Users and Computers		
User accounts with passwords never expires	2	Medium (1-4)
User accounts with passwords not required	0	Low (0)
Disabled computer accou		
Inactive user accounts	← Search	WHO ACTION WHAT WHEN WHERE
Inactive computer accou	What "\\\\fs1\\shared\\Finance\\Forecast_2022.pptx" x	
Permissions	Open in new window SEARCH Advanced mode	
User accounts with admin		
Administrative groups	Who Object type Action What Where When Classes	
Empty security groups	ENTERPRISE\\T.Simpson File Removed \\\\fs1\\shared\\Finance\\Forecast_2022.pptx fs1 9/14/2021 8:56:10 AM PCI DSS, PII, GDPR	
Data	Date created: "8/30/2021 4:02:14 PM"	
Shared folders accessible		
File names containing ser	ENTERPRISE\\T.Simpson File Modified \\\\fs1\\shared\\Finance\\Forecast_2022.pptx fs1 9/14/2021 8:55:45 AM PCI DSS, PII, GDPR	
	ENTERPRISE\\J.Rogers File Added \\\\fs1\\shared\\Finance\\Forecast_2022.pptx fs1 8/30/2021 4:02:14 PM PCI DSS, PII, GDPR	

Download a Free 20-Day Trial of Netwrix Auditor Here:

netwrix.com/auditor.html

Audit your most important IT systems from a centralized platform
Are you tired of juggling multiple auditing and reporting tools in an attempt to collect audit information from all your on-premises and cloud-based systems? Do you need a software solution that delivers that information in a unified and consistent way? Netwrix Auditor provides a consolidated audit trail across a wide variety of IT systems, including Active Directory, Windows Server, Oracle Database and network devices.

Next Steps



Learn more about **Active Directory Security Best Practices**

netwrix.com/active-directory-best-practices.html



Read our **New SysAdmin Magazine**
Managing Active Directory Groups
- Beyond the Basics

netwrix.com/sysadmin-magazine-july-2024.html