Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

Guidance for securing Microsoft Active Directory services in your organization

Management

TLP:CLEAR

Canada

Foreword

This is an UNCLASSIFIED publication issued under the authority of the Head of the Canadian Centre for Cyber Security (Cyber Centre). For more information, email or phone our Contact Centre at:

Contact Centre

contact@cyber.gc.ca

(613) 949-7048 or 1-833-CYBER-88

Effective date

This publication takes effect on Month XX, 20XX.

Revision history

Revision	Amendments	Date
1	First release.	Month XX, 20XX

D97-4/60-100-2023E-PDF
978-0-660-68378-2

Overview

Directory services are critical foundational components for enterprise information technology (IT) architecture environments. They are principally responsible for storing and managing identity credentials and their associated group (role) membership. Microsoft Active Directory (AD) includes a structured data repository commonly used by organizations to store and manage enterprise directory data objects, including policies, users, devices, credentials, and other network resources. AD can be an attractive target to threat actors looking for ways into your organization's network to access your systems and data.

This publication establishes an overview with key considerations for securing Microsoft AD services within your organization, with a focus on on-premises deployments. This guidance outlines recommendations for hardening and strengthening Microsoft AD on-premises deployments for managing medium confidentiality, medium integrity, and medium availability environments, as defined in Annex 2 of IT Security Risk Management: A Lifecycle Approach (ITSG-33) [1]. The most common and active threat actor scenarios have been considered within the threat model, including those adversaries with minimal resources but who are willing to take significant risk, such as unsophisticated hackers or lone cyber criminals. It is not intended to mitigate more sophisticated threats, such as zero-day attacks or expert insider threat. If an organization is facing a more advanced threat context, additional guidance is available from the Canadian Centre for Cyber Security (Cyber Centre).

As this is not a fulsome deployment and configuration guide, additional resources for configuring AD can be derived from Microsoft, the Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG), and the Centre for Internet Security (CIS) benchmark reporting.

The recommendations provided in this publication were developed based on contributions from Microsoft and general best practices for securing AD environments. The recommendations provided in this publication apply to Microsoft AD environments running at least Microsoft Windows Server 2019.

Table of contents

1 Introduction

Directory services are critical components for enterprise information technology (IT) architecture environments. Directory services are responsible for storing and managing critical objects, like identity credentials and their authorizations, and include sensitive data like administrative credentials that could authorize access to your organization's entire environment. Network and data breaches continue to rise as sophisticated threat actors increasingly take advantage of security gaps in managed and unmanaged technologies. Threat actors attempt to exploit weaknesses and configuration gaps to target assets being held within directory services. It is critical that your organization take the necessary steps to secure your directory services.

Microsoft Active Directory (AD) service is a structured data repository commonly used by organizations for storing and managing enterprise directory data objects. The basic security unit in AD is called a "forest." These forests can be divided up into subunits called "domains." Should your organization experience a compromise anywhere within a forest, it could lead to the compromise of your entire forest. The ongoing history of AD compromises demonstrates that greater security is required, which imposes potentially higher operational costs and greater effort to prevent more significant and costly breaches. Protecting and hardening the Microsoft AD service is critical to safeguarding the enterprise network.

Prior to the general acceptance of AD, credentialling was often siloed on a per-service basis. It required users to sign in for each service. AD centralized this experience, providing Single-Sign-On (SSO) for many users; however, this approach can lead to a single source of compromise. If threat actors are able to compromise credentials included in SSO, then they have the ability to use a single set of credentials to unlock other systems or data stores. There have been numerous examples of SSO compromises conducted using various attack types, such as SSO credential theft attacks. Compromising SSO is a trend that can be expected to continue.

This publication establishes an overview with key considerations for securing Microsoft AD services within your organization, with a focus on on-premises deployments. As this is not a fulsome deployment and configuration guide, additional resources for configuring AD can be derived from Microsoft, the Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) and the Centre for Internet Security (CIS) benchmark reporting.

This guidance outlines recommendations for hardening and strengthening Microsoft AD in on-prem deployments for managing medium confidentiality, medium integrity, and medium availability environments in the most active threat contexts.

The recommendations provided in this publication apply to Microsoft AD environments running at least Microsoft Windows Server 2019 and applies to all Microsoft AD Domain Services environments. This publication is strictly targeted to systems running AD Domain Services, even though some may apply to other services within an enterprise environment, like the Domain Name Service (DNS), Dynamic Host Configuration Protocol (DHCP), and file and printing services. For organizations that have environments running systems below the recommended Microsoft Windows Server 2019 version, we recommend you move them into separated "segregated" forests.

1.1 Risks to AD

The frequency and sophistication of AD attacks are on the rise, and the traditional security for AD is no longer adequate. To improve the protection of directory services, your organization will need to invest additional resources and effort. One action your organization can take is the separation of duties via procedures and policies. In particular, several security functions such as backup administrator and auditing/alerting administration should be separated from domain administration. However, organizations should remain aware that domain administrators (and certain other equivalent roles) can give themselves privileges at their discretion, as the capability to constrain these technically within AD is limited.

Your organization should also ensure you maintain your AD environment by implementing the most recent patches available to achieve the Windows Server 2019 patch state. By updating and patching your environment, you ensure that vulnerabilities and bugs are fixed, and you prevent threat actors from exploiting them. Your organization could alternatively choose to isolate under-maintained services away from Internet-based threats.

1.2 Strategic considerations

Your organization requires enterprise-wide computing resources to support your employees and deliver your mission. You should consider your specific business context and threat environment when applying the recommendations in this publication to secure your AD infrastructure. Underpinning the business enterprise environment and the threat context for directory services are the following pillars:

- Enterprise IT architecture
- Identity, credential, and access management (ICAM)
- Threat and risk assessments (TRAs)

1.2.1 Enterprise IT architecture

Enterprise IT architecture defines how the structure and operation of your organization's IT assets, with consideration for security and risks, are intended to support your strategic business goals. Enterprise IT architecture provides strategic direction on how investments in information assets would integrate and enable business processes. Your organization should cross-reference the recommendations in this publication with your enterprise IT architecture to better understand how these changes could impact your business objectives.

1.2.2 Identity, credential, and access management (ICAM)

ICAM refers to authentication and authorization processes required for users and devices to interact with, or connect to, your organization's technology resources. This involves a set of security tools, policies, and systems that help your organization manage, monitor, and secure access to your technology resources. Recommendations provided in this publication will impact ICAM controls within your organization.

For more information on ICAM, see Identity, Credential, and Access Management (ITSAP.30.018) [2].

1.2.3 Threat and risk assessment

Threat and risk assessment management involves identifying, assessing, and mitigating threats posed to IT assets. Your organization should reassess your environments and understand any potential risks associated with implementing the recommendations provided in this publication. If your organization engages with a service provider to manage the implementation of the controls, your organization remains responsible for risk management. This guidance is targeted to a threat model including those adversaries with minimal resources but who are willing to take significant risk, such as unsophisticated hackers or lone cyber criminals. It is not intended to mitigate more sophisticated threats, such as zero-day attacks or expert insider threat. If your organization is facing a more advanced threat context, contact the Cyber Centre for additional guidance.

2 Microsoft Active Directory (AD)

Microsoft AD is a structured data repository for storing directory data objects. Microsoft AD can be used to manage access to many of your organization's IT resources via role or group membership, such as your network infrastructure, email services, public key infrastructure (PKI) services, wireless services.

2.1 AD capabilities

Microsoft AD is a collection of services that allow your organization to identify, organize, and secure objects (like devices), and accounts. AD is made up of the following services which can be provisioned in whole or in part and require individual attention to gain a holistic security posture:

- AD Domain Services
- AD Federation Services (ADFS)
- AD Certificate Services
- AD Rights Management Services
- AD Lightweight Directory Services

This publication is focused on the AD Domain Services capabilities. Additional work efforts to include other listed services will be provided as addenda to this publication.

2.2 AD deployment architecture

Microsoft AD directory can be deployed in different architectures, from purely on-premises (or in a directly controlled data centre) to hybrid-cloud and complete solutions within cloud platforms.

2.2.1 AD on-premises

AD was originally intended for managing traditional on-premises infrastructure and applications. This deployment option allows your organization to fully manage your directory service from end-to-end. The hardening guidance provided in this publication focuses mainly on this deployment architecture.

2.2.2 AD cloud (on-premises, self-managed in cloud)

Hybrid cloud deployments and migrations must be considered carefully. When including any cloud service feature, it is implied that a hypervisor will be used. This can fundamentally change the security posture from the on-premises deployment as it is introducing different security concerns and networking functions that must be considered. This publication will focus on the use of AD as controlled by the consumer.

For more information on new or initial deployments of directory services within a cloud infrastructure, including those starting with the use of a CSP or third-party ICAM, see IT Practitioner Guidance for Securing Active Directory Services in Your Organization (ITSP.60.100) [3].

AD can still be used for ICAM capabilities for the cloud using existing on-premises solutions. Commonly this is referred to as 'hybrid' in nature, as certain elements are controlled and operate on-premises, while some elements are connected and then synced to CSP directory services. In some deployments, configurations of an AD server itself will remain the same, as the main difference or change is that of using a CSP's Infrastructure as a Service (IaaS) platform. In this type of deployment, control over certain physical and network aspects will change as per the shared responsibility model within cloud computing.

There are two main approaches to a hybrid architecture:

- **On-premises (within a consumer data centre):** Domain Controllers are federated to cloud services via on-premises ADFS.
- **On Premises extended (self-managed):** Domain Controllers on-premises as well as deployed in a CSP's IaaS platform.
  - Using the same forest or a forest trust, domains deployed in this manner are technically hybrid as they sync and federate from on-premises, presumably also using ADFS on-premises as well as federation.
  - In this case there is still not a direct or full sync of the identities with an identity provider (IdP) to constitute a native cloud identity.
  - While this type of architecture is possible, it is not a recommended long-term approach as there are fundamental changes to the security posture, reducing the applicability of the outlined safeguards presented in this publication and in ITSP.60.100 [3].
  - This approach should typically be viewed as a transitory or migration strategy.

2.2.3 Directory services in the cloud

Both authentication and authorization in a cloud environment can be conducted without the need for on-premises capabilities. Cloud-only authentication refers to identity and access management processes exclusively delivered via a CSP ICAM solution or a third-party hosted identity management solution. This option allows your organization to create and manage user identities, entitlement, and access control through a third-party application without having to build, own, or operate infrastructure on-premises. Cloud-only authentication solutions can be used to manage access to both public cloud workloads and privately managed on-premises applications, such as Azure AD Domain Services. Several authentication protocols govern how identities, entitlements, and authorizations are created, disseminated, and managed. Your organization should conduct a risk assessment to determine the potential risks to your business processes and data before adopting this option.

Note: The security posture in this deployment is different from the on-premises model and several controls in this publication cannot be applied.

When considering a new network deployment or the creation of a network architecture strategy for your organization, it is important to note this approach, as well as the hybrid options previously mentioned, are still valid but will require consideration of the capital expenditure and ongoing operational costs for each respectively. In the case of utilizing a CSP or

IdP service, the consumer allows the totality of the users' credential and identity to be formed and utilized within these services. There are benefits to this as aspects of patching and upgrades to the ICAM solution are conducted by the CSP as part of your organization's subscription.

However, this introduces a foundational change to the use of AD in that your organization is now fully reliant upon the services in the cloud. This will mean several of the recommendations in this publication will need to be revisited, as control of physical hardware and depth of control over other functions will fundamentally change. In addition, there is a diminished capacity for your organization to have visibility and control over the credentials, as you must work with the provider in all cases where additional measures, services, or use of the credential outside of the provider's main service functions are needed.

3 Hardening and mitigation strategies

Microsoft AD on-premises deployments can be protected against numerous threats by hardening defences and controls. Hardening and mitigation strategies require protections for credentials, systems, processes, and identities. In the following section, we provide hardening and mitigation strategies for safeguarding AD.

We recommend that your management team refer IT practitioners to initially follow the Microsoft AD setup and implementation guidance with additional inputs from the DISA STIG and CIS benchmark setup guidance documents.

3.1 System management

System management addresses controls around setting boundaries for the system and implementing a secure plan to ensure provisioning and ongoing secure access to the AD service. As such, the following should be implemented to establish a sound environment to operate the hardened AD infrastructure:

- Use dedicated administrative workstations for all administrator tasks, with hardware-token multi-factor authentication (MFA)
- Use separate privileged accounts for administrator tasks
- Decommission or segregate legacy AD services and applications
- Restrict network connections to and from AD servers – no Internet connectivity inbound or outbound
- Setup unique privileged accounts and local admin passwords for servers and workstations
- Block privileged accounts from being used on unauthorized systems
- Conduct remote administration only from a dedicated administrative workstation and only by using TLS-encrypted RDP

3.2 Account management

Account management addresses fundamental controls to securely manage all user and privileged accounts from provisioning to decommissioning within AD service environments. Some examples of privileged accounts include local and domain administrative accounts, service accounts, and built-in administrative accounts.

The following should be implemented for account management:

- Enable hardware-token MFA (for example, SmartCard & Keyboard, USB key) for all user and administrative accounts according to Microsoft's guidance at AD and on all endpoints
- Use the principle of least privilege to assign and manage administrative rights and privileges
- Enable and enforce just-in-time privileged account provisioning

- Ensure all service accounts are provided access based on the principle of least privilege and use managed service accounts where possible
- Avoid assigning service accounts in built-in privileged groups such as the local administrators or domain admins groups
- Ensure service accounts are used only by applications or services rather than users
- Prevent service accounts from being used for interactive logons and executing batch jobs
- Implement AD password filtering to block the use of compromised or bad passwords

3.3 Application security and hardening

By restricting the applications allowed on your AD servers, and only allowing or installing services and applications that are crucial in performing and supporting the directory services functions, your organization will have a more robust hardening posture for your AD. It will mean your organization has a smaller service set running on your AD servers, while co-hosted (sometimes referred to as "dogpiled") services are relocated away from your AD. Stripping down the software running to the bare minimum is a key step in hardening and reducing the attack surface. Proper change management procedures, like those found in ITIL, should be followed.

Directory service systems are only to have explicitly approved applications installed by enforcing application allow lists on servers and administrative workstations. Host-based and policy-based controls should be implemented on AD servers and dedicated administrative workstations to prevent unauthorized installation and use of applications on servers.

3.4 Logging, auditing, and monitoring

Monitoring, auditing, and logging should be enabled for directory service activities. All events should be shipped to a remote server that cannot be manipulated via core credentials. Event logs can also be forwarded to a centralized security information and event management (SIEM) server to facilitate aggregation, consolidation, and analysis of events in activity logs. Automated alerting mechanisms should be implemented to identify higher impact security policy violations for faster response action. Failure and success events linked to sensitive or critical server operations should be logged, monitored, and audited. Your organization should also remove stale or inactive user accounts and implement monitoring for events linked to the use of these accounts.

It is crucial that your organization monitor, log, and audit all privileged or administrative account use. You can enable system audit settings to regularly audit accounts with privileged or administrative access. For more information, see Microsoft Windows Server Audit Policy Recommendations [4].

3.5 Threat detection and response

Threat detection and response should consider potential threat scenarios, such as a compromise of your AD assets by a threat actor, and the detection controls to be implemented.

Your organization can improve the prevention and detection of known attack techniques using indicators of compromise (IoCs) and automated threat prevention technologies. You should monitor sensitive AD-related Windows activity events that may indicate attempted or successful compromise. By using network and endpoint threat detection and prevention solutions, your organization can detect and respond to attempts to compromise your AD.

To add an additional layer of protection, you should implement anti-malware solutions and promptly update anti-virus and anti-malware software across all systems. Your detection tools should monitor for attempts to remove or deactivate the anti-malware solutions.

3.6 Patching and change management

The AD infrastructure should be maintained and kept up to date in all cases. This includes scheduling patching, testing windows, and confirming patch compatibility with line of business applications. AD servers should be configured using an incremental strategy with a rollback capability when software maintenance material from Microsoft is available, and with minimal outage windows scheduled. This will ensure limited service disruptions should an issue with a patch be identified. It will also ensure that rollbacks can occur without affecting the whole environment. Formal change management processes also need to be adopted to certify and validate that required updates are applied.

3.7 Business continuity

Business continuity requires your organization to have contingency planning activities in place to help recover the directory service from a broad range of threats, including system disruptions or cyber security incidents. You should implement the AD Recycle Bin to assist with the recovery of your AD objects.

To assist in your business continuity efforts, you should establish processes that enable the automated collection of critical system data and information backups. Ensure your backups are tested periodically, such as quarterly or after a substantive change to validate integrity and utility. Your backup data should be isolated from the main network and considerations should be given to maintaining fully offline backups in addition to any other backup strategies you have in place.

In addition to backups, your organization should create, test, and update incident recovery plans on potential risk scenarios that could occur within your organization. You should prepare for recovery from security incidents that may impact the integrity or availability of your AD environment. You can do this by setting up system recovery procedures and documentation for your AD environment and providing training exercises or tabletop exercises for system administrators to develop and validate response and recovery plans.

3.8 User education

Your organization should conduct regular security awareness training for privileged account holders and other system end users. Your training program should be designed to continuously educate all users on current security best practices and to encourage behavioural changes and improved cyber hygiene to thwart unwanted or riskier user behaviours. Your organization should also establish processes to simplify the security requirements for end users, taking advantage of formal training sessions and visual aid tools.

4 Supporting content

4.1 List of abbreviations

Term	Definition
AD	Active directory
ADFS	AD Federation Services
API	Application programming interface
ATO	Authorization to operate
CAB	Configuration Advisory Board
CIS	Center for Internet Security
CMDB	Configuration Management Database
DHCP	Dynamic Host Configuration Protocol
DISA	Defense Information Systems Agency
DNS	Domain Name Service
DoD	United States Department of Defense
GC	Government of Canada
HTRA	Harmonized threat risk assessment
ICAM	Identity, credential, and access management
IT	Information Technology
ITS	Information Technology Security
IoC	Indicator of compromise
LoA	Level of assurance
MFA	Multi-factor authentication
SPOF	Single point of failure
SSO	Single-sign-on
STIG	Security technical implementation guide

4.2 Glossary

Term	Definition
Least privilege	The principle of giving an individual only the set of privileges that are essential to performing authorized tasks. This principle limits the damage that can result from the accidental, incorrect, or unauthorized use of an information system.
Level of assurance	The degree of confidence in the vetting process used to establish the identity of an individual and the controls used to manage the credentials entrusted to them.
Multi-factor authentication	A tactic that can add an additional layer of security to your devices and account. Multi-factor authentication requires additional verification (like a PIN or fingerprint) to access your devices or accounts. Two-factor authentication is a type of multi-factor authentication.

4.3 References

Number	Reference
1	Canadian Centre for Cyber Security. ITSG-33 IT Security Risk Management: A Lifecycle Approach. December 2014.
2	Canadian Centre for Cyber Security. Identity, Credential, and Access Management (ITSAP.30.018). August 2022.
3	Canadian Centre for Cyber Security. ITSP.60.100 IT Practitioner Guidance for Securing Active Directory Services in Your Organization. TBD.
4	Microsoft. Microsoft Windows Server Audit Policy Recommendations. July 2021.