Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

Practitioner guidance for securing Microsoft Active Directory services in your organization

Practitioner

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:

Contact Centre

contact@cyber.gc.ca

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

Effective date

This publication takes effect on December 12, 2023.

Revision history

Revision	Amendments	Date
1	First release.	December 12, 2023

D97-3/60-100-2023E-PDF
978-0-660-68470-3

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. There are several directory services implementations available. However, Microsoft Active Directory (AD) includes a structured data repository very commonly used by organizations to store and manage enterprise directory data objects including policies, users, devices, credentials, and other network resources. AD is a key target to threat actors looking for ways into an organization's network to access its systems and data, as it can be considered a "keys to the kingdom" type of compromise.

This publication establishes key considerations for securing Microsoft AD services within your organization, with a focus on on-premises. 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 taken into account 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 your organization is facing a more advanced threat context, contact the Cyber Centre for additional guidance. Additional resources for configuring AD can be derived from Microsoft's best practice publications, the Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG), and Centre for Internet Security (CIS) benchmark reporting.

The recommendations provided in this document were developed with contributions from Microsoft and from general best practices for securing AD environments. Our recommendations apply to Microsoft AD environments running at least Microsoft Windows Server 2019 and above and applies to all Microsoft Active Directory Domain Services (AD DS) environments for on-premises deployments.

Servers running at least Microsoft Windows Server 2019 are eligible to be used as the main domain controllers (DCs). Some of these recommendations may apply to other frequently associated services within an enterprise environment, like the Domain Name Service (DNS), Dynamic Host Configuration Protocol (DHCP), file, and printing services.

Table of contents

1 Introduction

Directory services are critical foundational components for enterprise information technology (IT) architecture environments. They are responsible for storing and managing identity credentials and their authorizations. Network and data breaches continue to rise as sophisticated threat actors increasingly take advantage of security gaps in managed and unmanaged technologies. Directory services store critical objects, including sensitive administrative credentials that can be used to authorize access to the entire enterprise environment. As a result, directory services are high-value targets for threat actors who will seek to exploit vulnerabilities associated with the infrastructure on which these services are deployed. Due to the potential scope associated with their compromise, it is critical that organizations take the steps necessary to secure their enterprise 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 the "forest" and can be divided into subunits called "domains." Should your organization experience a compromise anywhere within a forest, it could lead to the compromise of your entire forest, as your domains can be crossed. 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. Wherever it is deployed, protecting and hardening Microsoft AD service is critical to safeguarding the enterprise network.

This publication provides best practice recommendations for securing Microsoft AD services in on-premises and self-managed deployments for managing medium confidentiality, medium integrity, and medium availability environments (reducing residual risk against medium-rated injury potential). This advice and guidance seek to address the most common threat actor scenarios whereby adversaries with moderate resources who are willing to take moderate risk, such as career criminals, rogue insiders, and common hackers would be anticipated. If an organization is facing a more advanced threat context than those specified, additional guidance is available from the Canadian Centre for Cyber Security (Cyber Centre).

As this is not a comprehensive 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. Guidance on securing directory services in cloud environments, with a focus on Azure AD, will be released on a later date.

The recommendations provided in this publication apply to Microsoft AD environments running Microsoft Windows Server 2019 and above. For organizations operating Microsoft AD on versions older than Windows Server 2019, you should consider moving them into separated "segregated" and hardened forests until you can either upgrade your environment or migrate services and information. The use of segregated environments of this nature are not intended for extended periods of a system development lifecycle (SDLC).

In Windows AD environments, functional level configuration determines security features and capabilities that are available within a domain or a forest. Functional level requirements also determine which Windows Server operating system versions can be installed on domain controllers within a domain or a forest. To implement the recommendations provided in this publication, your organization should ensure that your forest and domain functional levels are set to at least Windows Server 2016 functional levels or higher. For more information on functional levels, see Microsoft's reference document on forest and domain levels [2].

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 to separate 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 at least Windows Server 2019 and above patch state. By updating and patching your environment, you ensure that vulnerabilities and bugs are fixed and prevent threat actors from exploiting them. Your organization could alternatively choose to isolate under-maintained services away from Internet-based threats.

1.1 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)

1.1.1 Enterprise information technology 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 this publication with your enterprise IT architecture to better understand how these changes could impact your business objectives.

1.1.2 Identity, credential, and access management (ICAM)

ICAM refers to the identification, authentication, and authorization technology and processes required for users and devices to connect to and interact with an organization's IT infrastructure. This involves a set of security tools, policies, and systems that helps your organization manage, monitor, and secure access to your technology resources. The recommendations provided in this publication will impact ICAM controls within your organization. You should cross-reference this document with your organization's ICAM infrastructure to understand how these recommendations could impact ICAM operations.

1.1.3 Threat and risk assessment

Threat and risk assessment involves identifying threats, assessing risks arising from these threats, and mitigating the risks that are unacceptable to your organization's business processes and critical information. The recommendations provided in this document should be considered within your organization's risk assessment and management framework to determine the nature and scope of any changes to its risk posture. If your organization engages with a service provider to manage the implementation of 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 an organization is facing a more advanced threat context, additional guidance is available from the Cyber Centre.

1.2 Directory services threat context

Annex A provides a recommended baseline set of security controls that can be applied to the operation of directory services within an organization. The security controls provided in Annex A were selected in consideration of the following assumptions and constraints:

- The maximum possible injury or impact of compromise of the business processes and information to be supported by directory services is assumed to be medium for confidentiality, medium for integrity, and medium for availability. Business context categorization is described in Annex 1 of IT Security Risk Management: A Lifecycle Approach (ITSG-33) [1].
- The threat context for the business processes and information to be supported by directory services is assumed to include the most common threat actor scenarios that can be anticipated. If an organization is facing a more advanced threat context than those previously specified, contact the Cyber Centre for additional guidance.
- It is assumed that all applicable controls from your organization's selected baseline control profile (for example, a tailored version of ITSG-33, Annex 4A) have already been applied and assessed. It is strongly recommended that this assumption be validated and that any outstanding risks be addressed before applying the guidance in this document. A compromise of directory services will result in a global compromise of the system it supports. Therefore, the security foundation of directory services should be at least as good as its surroundings.
- Vendor and industry guidance have been used to help tailor the selection of controls and, in some cases, mechanisms and assurance practices. However, additional adaptations have been recommended to address evolving and advanced threat actor capabilities.
- Some capabilities associated with threat actors, such as privileged insiders or the development and employment of zero-day vulnerabilities, cannot be mitigated through directory services component configurations and must be addressed at an organizational level. Examples of such controls include dual authorization, physical separation, and separation of duties.

2 Guidance resources for securing Active Directory

The following resources were consulted in the preparation of this publication. Refer to these additional resources for best practices and additional guidance on securing AD.

2.1 Microsoft security best practices

Microsoft has issued a set of guidelines for securing AD based on observations and lessons learned from assisting its clients in responding to and recovering from AD infrastructure compromises. These guidelines outline common exposures within AD installations, the technical controls required to reduce the attack surface of AD environments, and continuous monitoring recommendations to detect signs of a potential compromise. This resource highlights the importance of architecting AD from a risk-based approach, emphasizing the need for separating critical assets and securing lifecycle management of systems, applications, and users. Refer to Microsoft Best Practices for Securing Active Directory [3] for more detailed information.

2.2 Defense Information Systems Agency: Security Technical Implementation Guide

DISA is a United States Department of Defense (DoD) combat support agency composed of military personnel, civilian employees, and contractors. As part of its mandate, DISA regularly provides a listing of publications referred to as the STIG. These publications range in content and focus based on a specific area or application of technology. For the purposes of this publication, DISA's Active Directory Domain Security Technical Implementation Guide (STIG) [4] was consulted.

When referring to this STIG, we recommend that the severity elements of category 1 (CAT I – High) and category 2 (CAT II – Medium) be reviewed to understand their security practices, in conjunction with the Microsoft best practices and those of the CIS benchmarks noted in the following subsection. The Active Directory Domain STIG [4] provides details on CAT I and CAT II level configurations and provides details and descriptions on how to implement the recommended security configurations.

In those areas where the guidance provided does not align with practical uses within an existing AD infrastructure, it is recommended that a risk assessment be conducted to ensure the control does not increase risk exposure or compromise to the AD infrastructure. The risk assessment will also assist you in understanding whether there may be compensating controls to address any gaps or perceived shortfalls.

2.3 Center for Internet Security (CIS)

Use of the Center for Internet Security (CIS) benchmarks listed below are recommended for augmentation and/or verification of the Microsoft AD best practices.

- Center for Internet Security (CIS) Controls version 8 [5]
- CIS Microsoft Windows Server 2019 Benchmark version 1.3.0 [6]

- CIS Microsoft Windows Server 2019 STIG Benchmark version 1.1.0 [7]

Note: Section 2.3 of the CIS benchmarks document focuses on security features, but all areas outlined are recommended for consideration.

Note: The table in each section lists implementation group (IG) designations, which are the recommended guidance to prioritize implementation of the CIS Critical Security Controls (CIS Controls). The IG's are divided into three categories: implementation group 1 (IG1), implementation group 2 (IG2), and implementation group 3 (IG3). They each provide a set of cyber defence safeguards, with a total of 153 safeguards presented. The CIS Controls offer the following guidance:

2.3.1 Implementation group 1 – Basic cyber hygiene

CIS Controls version 8 defines IG1 as essential cyber hygiene and represents an emerging minimum standard of information security for all organizations. IG1 is the baseline to the CIS Controls and consists of a foundational set of 56 cyber defence safeguards. The safeguards included in IG1 are what every organization should apply to defend against the most common cyber attacks.

IG1 organizations are typically small to medium-sized with limited IT and cyber security expertise to dedicate towards protecting IT assets and personnel. A common concern of these organizations is maintaining business operations, as they have a limited tolerance for downtime.

The sensitivity of the data that these organizations wish to protect is low and principally surrounds employee and financial information. The safeguards selected for IG1 can be implemented with limited cyber security expertise. They are meant to thwart general, non-targeted attacks. These safeguards will also typically be designed to work in conjunction with small or home office commercial off-the-shelf (COTS) hardware and software.

2.3.2 Implementation COTS group 2 – Enterprise

IG2 builds upon the safeguards identified in IG1. IG2 is comprised of 74 additional safeguards meant to assist security teams in coping with increased operational complexity. Some of the IG2 safeguards will depend on enterprise-grade technology and specialized expertise to properly install and configure.

A typical IG2 organization employs individuals who are responsible for managing and protecting IT infrastructure. These organizations typically support multiple departments with differing risk profiles based on job function and mission. There may also be units within the organization that have regulatory compliance obligations. The organizations supported by IG2 often store and process sensitive client or enterprise information but can withstand short interruptions of service. A major concern for these organizations is loss of public confidence in the event of a breach.

2.3.3 Implementation group 3 – Sensitive enterprise

IG3 builds upon the safeguards in IG1 and IG2. It is comprised of an additional 23 safeguards.

An IG3 enterprise commonly employs security experts that specialize in the different facets of cyber security, such as risk management, penetration testing, and application security. IG3 assets and data contain sensitive information or functions that are subject to regulatory and compliance oversight. An IG3 enterprise must address availability of services and the confidentiality and integrity of sensitive data. Since successful cyber attacks can cause significant harm to public welfare,

IG3 enterprises must select safeguards that will abate targeted attacks from a sophisticated threat actors and reduce the impact of zero-day attacks.

For those areas where achieving IG3 as described in the document is problematic or not possible due to current architecture or configuration on your organization's AD infrastructure, it is recommended that a risk assessment be conducted for the totality of these controls that can only achieve either IG1 or IG2 respectively.

3 About Microsoft Active Directory

Microsoft AD is a structured data repository for storing directory data objects. It can be used to manage your organization's IT resources, such as network infrastructure, email services, public key infrastructure (PKI) services, and wireless services.

Note: While this publication is focused on the Domain Services capability of AD, the suite can be used in additional roles.

Each section below establishes the various functions of AD and supplies associated references that can aid in the deployment of AD in your organization. It should be noted that our intent is not to provide a 'build book' for AD services as the deployment context for each organization varies. Rather, the information in this section contains referrals to areas of best practice that can be included for consideration and inclusion by an organization through its risk assessment findings and deployment context.

3.1 Active Directory capabilities

The following subsections provide high-level details on each of the relevant AD capabilities. Additional resources have been provided for practitioners to seek more in-depth knowledge on the capability.

3.1.1 Active Directory Domain Services

Active Directory Domain Services (AD DS) is used for user and resource management. It provides support for directory-enabled applications such as Microsoft Exchange Server. AD DS provides a distributed database that stores and manages information about resources and application-specific data from directory-enabled applications.

Refer to the following additional documents on AD DS for a deeper understanding and recommended best practices:

- Microsoft Best Practices for Securing Active Directory [3]
- Active Directory Domain Security Technical Implementation Guide (STIG) [4]

3.1.2 Active Directory Federation Services

Active Directory Federation Services (AD FS) provides identity federation and web application single sign-on (SSO) capabilities. AD FS acts as an identity provider by authenticating users to provide security tokens to applications that trust AD FS. It also acts as a federation provider by consuming tokens from other identity providers and then providing security tokens to other applications.

Refer to the following additional documents on AD FS:

- Upgrading to Active Directory Federation Service Farm in Windows Server 2019 [8]
- Microsoft Best Practices for Securing Active Directory Federation Services [9]

AD FS is a key consideration when deploying AD and, more specifically, your organization's DCs. The location and setup of federation services provide greater control of the credentials, helps establish SSO, and facilitates options for later adoptions of ICAM within cloud service provider (CSP) platforms.

3.1.3 Active Directory Certificate Services

Active Directory Certificate Services (AD CS) is used to build and manage PKI and provide public key cryptography, digital certificates, and digital signature capabilities for your organization.

Refer to the following guidance on AD CS:

- Active Directory Certificate Services Overview [10]
- Microsoft Certification Authority Guidance [11]

3.1.4 Active Directory Rights Management Services

Active Directory Rights Management Services (AD RMS) is used to support information protection using rights management within your organization. Refer to Active Directory Rights Management Services Overview for AD RMS guidance [12].

3.1.5 Active Directory Lightweight Directory Services

Active Directory Lightweight Directory Services (AD LDS) is a lightweight directory access protocol (LDAP) directory service. It provides data storage and retrieval for directory-enabled applications, without the dependencies and domain-related restrictions of AD DS. AD LDS provides the same functionality as AD DS, but it does not require deployment of domains or domain controllers. Refer to Active Directory Lightweight Directory Services Overview for AD LDS guidance [13].

3.2 Active Directory deployment architecture

AD can be deployed in different architecture modes. In many cases, AD has been deployed to manage traditional on-premises infrastructure and applications. This deployment option allows your organization to fully manage your directory service from end-to-end. The guidance in the following section is predominantly related to on-premises environments.

4 Additional hardening and mitigation strategies

Microsoft AD on-premises deployments can be protected against numerous threats by hardening defences and controls as outlined in the summaries and resources in Section 2 Guidance resources for securing Active Directory. As noted, hardening and mitigation strategies require protections for credentials, systems, processes, and identities. In the following sections, we provide additional strategies for those elements surrounding the AD itself which are integral for safeguarding purposes.

4.1 Environment considerations

In addition to any specific configuration settings as referenced in Section 3 About Microsoft Active Directory, adherence to proper protocols and established system components within the overall user environment is also key to securing your organization's AD. The following subsections outline areas of consideration and actions to be taken to ensure that your environmental factors do not impede the ability for your AD to remain in a known and secure posture.

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.

Use dedicated administrative workstations for all administrative tasks

A dedicated administrative workstation is a secured physical or thin client workstation used to perform specific and sensitive administrative tasks or tasks requiring privileged access. This device must not have Internet access and services such as email and web browsing must be turned off and prohibited. All users in your organization who perform administrative or privileged actions should do so on an approved purpose-built and dedicated administrative workstation. You should ensure that each dedicated administrative workstation is not administered by the user it is assigned to.

Your organization should configure your AD server so that privileged access can only be undertaken via a dedicated administrative workstation which cannot be shared amongst users. Each dedicated administrative workstation should be configured with the highest security configuration available, with restrictions on local administrative accounts and the applications that are permitted to be installed.

You should block privileged accounts used on dedicated administrative workstations from logging on to lower-tier trust zones. It is imperative that you prevent access to the Internet, in addition to turning off non-administrative services such as email and web browsing. Your dedicated administrative workstations should have network connections limited to those required to perform administrative tasks. To enhance security of your dedicated workstations, you should implement application allow listing tools, like AppLocker or Windows Defender Application Control, to ensure that only approved applications are installed or executed. You should also enable disk encryption on dedicated administrative workstations and devices. Please refer to the U.S. Department of Defense's Guidance on Microsoft Windows Privileged Access Workstation (PAW) STIG [14] for detailed guideline on setting these systems.

In addition to the guidance in this section, consider the following actions to secure your dedicated administrative workstations and devices:

- Consider technologies that enable hardware root of trust
  - Trusted Platform Module (TPM) 2.0
  - BitLocker Drive Encryption
  - Unified Extensible Firmware Interface (UEFI) Secure Boot
  - Kernel Direct Memory Access (DMA) I/O Protection
- Enable virtualization-based security (VBS) features
  - Hypervisor-protected Code Integrity (HVCI)
  - Credential Guard [15]
- Enable application control to allow list applications

Use separate privileged accounts for administrative tasks

Your organization should separate privileged accounts used for performing local systems administrative tasks from privileged accounts used for performing other administrative tasks. You should also ensure that no administrator account is assigned to multiple groups outside the same security domain. All domain administrator and equivalent access should be highly restricted. Service and agent accounts should be controlled with the same change control thoroughness as the access for domain administrators. You must configure privileged accounts as members of a protected user group to ensure credential protections are applied by default and to prevent plaintext credentials from being cached on devices accessed [16].

Decommission or isolate legacy active directory services and applications

Where possible, your organization should decommission systems running deprecated AD services and legacy applications. For business-critical services which cannot be immediately decommissioned, we recommend you move these applications and services into a separate and isolated segregated forest. You should prevent the use of data encryption standard (DES) for Kerberos, as well as the Server Message Block (SMB) version 1 (SMBv1) on the SMB client and server components [17].

Restrict network connections to and from Active Directory servers

You should use both a host firewall, such as Windows firewall, and network infrastructure solutions to restrict inbound and outbound connections to AD systems. You can enhance the protection of your network by using allow listing to restrict inbound connections to designated systems and approved applications only. You should block all inbound and outbound Internet access to your AD service and ensure that any remote administration is conducted exclusively from a dedicated administrative workstation, using only Transport Layer Security (TLS)-encrypted Remote Desktop Protocol (RDP).

Set up unique privilege accounts and local administrator passwords for servers and workstations

Ensure your organization creates unique Directory Service Restore Mode credentials on AD servers and unique local administrator passwords on all user access workstations. It is essential that you ensure passwords for your local administrator accounts are unique and that privileged accounts are unique to one user and employ the principle of least privilege. We strongly recommend you prevent the use of shared administrative accounts and implement AD Password Filtering [18] to block the use of compromised or bad passwords.

Enforce separation of duties for administrative tasks

Your organization can implement separation of duties by using separation of duties policies and procedures, which will look to the risk of insider threats and privilege account compromises.

Block privileged accounts from being used on unauthorized systems

We recommend you prevent the use of privileged accounts from being used on unauthorized systems. One example of executing this is by blocking privileged accounts used on a dedicated administrative workstation from being used to access lower-tier assets.

Consider managed file transfer solutions when interconnecting different domains

You should consider managed or secure file transfer solutions with similar capabilities to cross domain solution (CDS) principles for interconnections between different security posture environments. However, as a high-assurance CDS is most commonly utilized for transfers between domains of higher and lower sensitivity, it is not generally recommended in this case. Where a high-assurance CDS is required for AD on-premises separation, consultation with the Cyber Centre is recommended.

4.2 Account management

Account management addresses fundamental controls to securely manage all user and privileged account 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.

Enable multi-factor authentication for all user and administrative accounts

All access to Active Directory services must employ hardware token MFA (for example, SmartCard & keyboard, USB key) for all user and administrative accounts according to Microsoft's guidance [19] [20]. SmartCards are inexpensive to replace, and several models of keyboards provide strong phishing resistance with endpoint-independent handling of PINs for the unlocking of the private keys. Some tokens may permit a third factor in the form of a fingerprint reader for the unlocking of the private keys, but these are generally more expensive than the SmartCard and keyboard combination. "Soft token" implementations (for example, endpoint or phone) are not considered true factors as there is an ability to obtain the certificate and attempt circumvention. Thus, they are considered insufficient. All user accounts must have passwords stored using Advanced Encryption Standards (AES) keys.

Restrict membership to enterprise and domain administrator groups

Membership to the enterprise administrators (EA), domain administrators, and built-in administrators (BA) groups must be restricted. These account groups should not contain permanent memberships from user accounts. System administrators should be assigned EA membership and domain administrator rights on an as-needed basis.

Use the principle of least privilege to assign and manage administrative rights and privileges

All user and privilege accounts, including service accounts and application accounts, should be set up based on the principle of least privilege. Your organization should use managed service accounts where possible and avoid assigning service accounts in built-in privileged groups, such as the local administrators or domain administrators' groups. You should also

ensure that service accounts are used only by applications or services rather than users and deny all interactive logons. Additionally, your organization should prevent service accounts from executing batch jobs. Authorization should only be provided for the rights and privileges necessary to accomplish assigned tasks. System administrators should provision user and privileged accounts, both domain and local accounts, to ensure the least privilege principle is achieved. Privileged or administrative service accounts should start with basic user rights and additional access should be granted based on business need.

Enable just-in-time privileged account provisioning

You should enable privileged access rights only when required and implement systems to grant temporary membership in privileged groups only when required. You should also ensure that rights and privileges are removed once assigned tasks are completed and eliminate permanent membership within privileged groups.

Conduct periodic reviews of accounts and purge unused accounts

We recommend your organization conduct periodic user access and unused account reviews. You should remove access permissions that are not required, as well as remove any unused accounts. We also recommend that you deactivate stale or inactive user accounts as soon as possible and implement monitoring for events linked to the use of these accounts.

4.3 Application security

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's AD will have a more robust hardening posture. 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.

Directory service systems should only 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. Both persistent installations and memory-only applications must be prevented from executing unless they are on the application allow list.

Ensure service accounts are configured and protected securely

Where possible, the service accounts within your organization should not be members of built-in protected groups in AD. We recommend you delegate a minimum set of permissions required or assign user rights via group policy to achieve this approach. Service accounts must not cross tiers and must not to be used interactively. Your service accounts must have Kerberos pre-authentication enabled and always on. This feature should never be turned off. Where possible, you should also replace your service accounts with group managed service accounts and regularly reset keys for sensitive service accounts, such as Krbtgt. Lastly, your organization should ensure the print spooler service is turned off [21].

4.4 Logging, monitoring and auditing

Monitoring, auditing, and logging should be enabled for directory service activities. This is especially true for privileged account tasks. Your organization should log, monitor, and audit failure and success events linked to sensitive or critical server operations.

Privileged actions should be logged, monitored and audited

Your organization should ensure that all privileged or administrative accounts are monitored, logged, and audited to ensure appropriate use. The directory service is a critical asset. Monitoring and auditing of related administrative tasks should be treated with priority. Protect and monitor activities of privilege accounts. Enable system audit settings and regularly audit their accounts. Implement an Active Directory Change Auditing tool to monitor for any changes to various AD configuration items.

System log collection should be automated, isolated and protected

Your organization should automate the collection of system logs and ensure these logs are protected against potential threats. Organizational systems holding backup data should be isolated from the enterprise AD, as compromised domain credentials can delete or modify logs collected prior to the compromise. Event logs can also be forwarded to a centralized security information and event management (SIEM) server to facilitate aggregation, consolidation, and analysis of events. Automated alerting mechanisms should be implemented to identify higher impact security policy violations for faster response action.

4.5 Threat detection and response

Threat detection and response should consider potential threat scenarios, like a threat actor compromise of your AD assets, and the detection controls that need to be implemented.

Detect malicious threats using indicators of compromise and automated threat prevention technologies

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.

Enable anti-malware and anti-virus solutions

To add an additional layer of protection, your organization should enable 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.

4.6 Patching and change management

Your AD infrastructure should be maintained and kept up to date by executing updates and patches to your operating system and applications in a timely manner. Patching should be completed in increments as discussed in Section 4.1 Environment considerations. Your organization should ensure that formal change management processes are adopted to certify and validate that required updates are applied.

Enable automated patching of operating system, applications and devices

Your organization should develop a strategy statement for the automated patching of your AD server components, including the operating system, installed applications, and hardware devices. You should log any vulnerability disclosures that may have an impact on your AD and prioritize patch deployment.

Secure the change management processes

Your change management process should ensure you implement configuration management, review your regulatory compliance requirements frequently, and evaluate settings with each new hardware or software version deployed. You should ensure that configuration changes are set up to trigger immediate alerts and that these alerts are reviewed by the section within your organization responsible for authorizing configuration changes. You should also implement an AD Change Auditing tool to monitor for any changes to your AD configuration items.

4.7 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.

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. Your organization must ensure that its backups are encrypted and protected to ensure only authorized accounts have access to them. Any modification of the backups should require multiple authentication factors to access. You should also consider implementing the AD recycle bin feature to assist with the recovery of your AD objects [22].

Create, test and update incident recovery plans

As part of your overall recovery process, your organization should create, test, and update incident recovery plans to address the potential risk scenarios that could impact your organization. You should also provide training exercises or tabletop exercises for system administrators to develop and validate response and recovery plans.

Create an Active Directory forest recovery plan

The ability to recover AD services is critical to ensure restoration of services from security disruptions. Your recovery plan should focus on recovery efforts from the security incidents that could impact the integrity or availability of your AD environment. You should include system recovery procedures and documentation for the environment and ensure your

recovery plans are periodically tested. Based on your testing and lessons learned, you should update your recovery plan to reflect necessary changes in your processes, procedures, or configurations within your environment. As part of your backup and recovery planning initiatives, ensure that AD forest backups and associated documentation are stored offline. Where possible, your organization should also consider storing backups within a cloud storage solution or platform.

4.8 User education

Your organization should conduct regular security awareness training for privileged account holders and other system end users.

Educate system administrators and end users on security best practices

Your training program should be designed to continually educate all users on security best practices and promote good security awareness behaviours and proper cyber hygiene to help mitigate against unwanted risky user actions. Your organization should also establish processes to simplify the security requirements for end users, taking advantage of formal training sessions and visual aid tools.

We recommend that systems administrators within your organization be trained within a smaller scope of control and not across more than one forest, and to adopt two-person control team.

5 Active Directory and 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.

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 synchronized to a CSP's directory services. In some deployments, configurations of an AD server itself will remain the same, as the main difference or change is that a CSP's infrastructure as a service (IaaS) platform is used. 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 such a "hybrid" architecture:

a) **On-premises (within a consumer data centre):** Domain Controllers are federated to cloud services via on-premises ADFS

b) **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 and 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 possible, this is not a recommended long-term approach as there are fundamental changes to the security posture, making the outlined safeguards presented in this document not possible. This should typically be viewed as a transitory or migration strategy.

The key differences between utilizing a hybrid approach versus a full deployment using a CSP or IdP services, are as follows:

1. Control of several environment factors as noted above are within the consumer's responsibility and ability to audit and upgrade
2. A consumer can limit the amount of data points within their credentials being shared or synced with the CSP
3. By using federated services, the consumer can complete actions such as centralize control, review, and audit for the organization's credentials
4. If required, pivoting to another CSP or utilizing multiple cloud providers and services is readily available as the consumer doesn't need to confirm and work with a CSP to ensure their platform or services are compatible with other CSPs'
5. Risk assessments of the AD infrastructure are more readily achievable and visibility, to a level similar to on-premises, can be attained in this fashion as the consumer still has a large responsibility within the cloud platform (IaaS specifically) for items like patching

If your organization will be extending or trusting a forest between on-premises and IaaS deployments (as noted in the security control profile) it will be necessary to apply changes relative to a strictly-on-premises deployment. Authorities to operate (ATOs) and security assessment and authorization (SA&A) from the on-premises deployment will no longer apply, even if all configurations are functionally identical, as the underlying infrastructure has changed. In particular, the physical separations that are recommended for on-premises AD servers cannot be implemented in IaaS, and compensating alternative controls are not expected to credibly defend from below operating system-level attacks. Where IaaS deployment of an AD DS capability is needed for business purposes, your organization should separate forests.

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 user's 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.

6 Supporting content

6.1 List of abbreviations

Term	Definition
AAD	Azure Active Directory
AD	Microsoft Active Directory
AD CS	Active Directory certificate services
AD DS	Active Directory domain service
AD FS	Active Directory federation services
AD LDS	Active Directory lightweight directory services
AD RMS	Active Directory rights management services
AES	Advanced Encryption Standards
API	Application Programming Interface
ATO	Authority to operate
CIS	Center for Internet Security
COTS	Commercial off-the-shelf
CSE	Communications Security Establishment
CSP	Cloud service provider
DC	Domain controllers
DMA	Direct Memory Access
DoD	United States Department of Defense
EA	Enterprise administrators
ESAE	Enhanced Security Admin Environment
GC	Government of Canada
HVCI	Hypervisor-protected Code Integrity
IaaS	Infrastructure as a service
ICAM	Identity, Credential and Access Management
IdP	Identity provider
IG	Implementation group
IoC	Inddicator of compromise
IT	Information Technology
ITS	Information Technology Security
ITSG-33	IT Security Risk Management: A Lifecycle Approach

Term	Definition
LDAP	Lightweight directory access protocol
LoA	Level of Assurance
LoB	Line of Business
MFA	Multi-factor authentication
PKI	Public key infrastructure
RDP	Remote Desktop Protocol
SDLC	System development lifecycle
SMB	Server Message Block
SMBv1	Server Message Block Version 1
SSO	Single sign-on
TLS	Transport Layer Security
TPM	Trusted Platform Module
TRA	Threat and risk assessment
UEFI	Unified Extensible Firmware Interface
VBS	Virtualization-based security

6.2 Glossary

Term	Definition
Active Directory Domain Services (AD DS)	Enterprise-ready lightweight directory access protocol (LDAP) server that provides key features such as identity and authentication, computer object management, group policy, and trusts [23].
Azure Active Directory (Azure AD)	Cloud-based identity and mobile device management that provides user account and authentication services for resources such as Microsoft 365, the Azure portal, or SaaS applications.
Azure Active Directory Domain Services (Azure AD DS)	Cloud-based identity managed solution which provides managed domain services with a subset of fully compatible traditional AD DS features such as domain join, group policy, LDAP, and Kerberos/NTLM authentication.
Forest	This is a collection of AD trees that share a common schema and configuration and are connected through trust relationships.
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	A characteristic of an authentication system or a token that uses more than one authentication factor. The three types of authentication factors are 1) something a user knows, 2) something a user has, and 3) something a user is.

Verifier compromise resistance	Use of authenticators which requires that the verifier store a copy of the authenticator secret. For example, an OTP authenticator which requires that the verifier independently generate the authenticator output for comparison against the value sent by the claimant.
Verifier impersonation resistance	Use of authenticators that are resistant to attempts by fraudulent verifiers or RPs to fool an unwary claimant into authenticating to an impostor website. A verifier impersonation-resistant authentication protocol shall establish an authenticated protected channel with the verifier.

6.3 References

Number	Reference
1	Canadian Centre for Cyber Security. ITSG-33 IT Security Risk Management: A Lifecycle Approach. December 2014.
2	Microsoft. Forest and Domain Functional Levels. December 2021.
3	Microsoft. Best Practices for Securing Active Directory. July 2021.
4	Defense Information Systems Agency. Active Directory Domain Security Technical Implementation Guide (STIG). August 2022.
5	Center for Internet Security. Center for Internet Security (CIS) Controls version 8.
6	Center for Internet Security. CIS Microsoft Windows Server 2019 Benchmark version 1.3.0. March 2022.
7	Center for Internet Security. CIS Microsoft Windows Server 2019 STIG Benchmark version 1.1.0. March 2022.
8	Microsoft. Upgrading to Active Directory Federation Service Farm in Windows Server 2019. March 2023.
9	Microsoft. Microsoft Best Practices for Securing Active Directory Federation Services. February 2023.
10	Microsoft. Active Directory Certificate Services Overview. August 2016.
11	Microsoft. Microsoft Certification Authority Guidance. August 2016.
12	Microsoft. Active Directory Rights Management Services Overview. August 2016.
13	Microsoft. Active Directory Lightweight Directory Services Overview. July 2012.
14	United States Department of Defense. Microsoft Windows Privileged Access Workstation (PAW) STIG Version 2. October 2023.
15	Microsoft. Credential Guard. September 2023.
16	Microsoft. Protected Users Security Group. October 2021.
17	Microsoft. Disabling SMBv1, SMBv2, and SMBv3. May 2023.
18	Microsoft. Password Filter Programming Considerations. January 2021.
19	Microsoft. Microsoft Guidelines for Enabling Smart Card Logon with Third-Party Certification Authorities. August 2023.
20	Canadian Centre for Cyber Security. Calculating robustness for boundary controls (ITSP.80.032). March 2019.
21	Microsoft. Print Spooler Security Assessment. February 2023.
22	Microsoft. Active Directory Forest Recovery Guide. July 2023.
23	Microsoft. Comparing Identity Solutions. October 2023.