mismo™
SYSTEMS

STRATEGIC IT SERVICES

ACTIVE DIRECTORY REVIEW

Enhance Security and Efficiency with ADDS Insights

Active Directory Review: Gap Analysis

SECURITY REVIEW

AD HARDENING REVIEW

- Disabling unnecessary services
- Enforcing strong password policies
- Limiting administrative privileges to reduce the attack surface

OPERATIONAL PROCESSES REVIEW

- Review the effectiveness of current operational procedures & ensuring they align with security best practices

PRIVILEGED ACCOUNTS/GROUPS MEMBERSHIP REVIEW

- Regularly checking the membership of privileged accounts and groups to ensure proper account hygiene
- Service account review
- Review of stale accounts

FOREST AND DOMAIN TRUSTS REVIEW

- Evaluating the trust relationships between forests and domains to prevent authorised access

OPERATING SYSTEM CONFIGURATION REVIEW

- Ensuring that security patches and updates are applied, and configurations align with Microsoft's recommended guidance

DOMAIN AND DOMAIN CONTROLLER CONFIGURATION REVIEW

- Comparing the current domain and domain controller configurations against best practices and recommended guidelines

ACTIVE DIRECTORY OBJECT PERMISSION DELEGATION REVIEW

- Examining the permissions delegated to Active Directory objects to prevent excessive privileges

AD MONITORING TOOL/METHODS REVIEW

- Check the implementation and configuration of monitoring tool/methods and ensuring they align with best practices

SECURITY AUDIT

- Audit user activities: Track changes to AD objects, user logins, and account lockouts.
- Review permissions: Ensure that permissions are correctly set and follow the principle of least privilege.
- Review Audit Policies to check critical changes are being monitored

PERFORMANCE REVIEW

CAPACITY PLANNING REVIEW

- Review hardware and resources capacity considering current and future load.
- Review Domain Controllers redundancy and reliability

MONITORING AND LOGGING

- Review performance metric to monitor CPU, memory, and network usage.
- Review logs for unusual activities or errors.

SITE AND SERVICES CONFIGURATION AND REPLICATION REVIEW

- Number of Sites, domain controller placement, and subnet binding
- Inter-site and intra-site replication configuration review
- DC Replication health review

DOMAIN CONTROLLER HEALTH

- Check the health of domain controllers and identify issues.
- Verify dependency services
- Detect unsecure LDAP binds

PERFORMANCE TUNING

- Fine tune settings for domain controllers to handle the load efficiently.
- Update software: Ensure that all AD-related software is up to date to benefit from the latest performance improvements.

BACKUP AND RECOVERY

- Review AD backup solution and recovery procedures.
- Review periodically tests of recovery plans to ensure they work as expected.

FSMO ROLE REVIEW

- FSMO Roles health and placement review

REVIEW DNS CONFIGURATION

- Review DNS settings and name resolution
- Review DNS forwarders and root hints are set up correctly
- Review Aging and Scavenging settings

GROUP POLICY MANAGEMENT

- Review Group Policy Objects (GPOs) to ensure they are applied correctly and do not conflict.
- Review GPO performance impact on login times and system performance.

DOCUMENTATION REVIEW

- Review Active Directory implementation documentation, Standard Operating Procedure (SOP) documents records

UPGRADE READINESS REVIEW

PREPARATION AND PLANNING

- Clearly outline the goals of the upgrade or migration, such as consolidating domains, improving security, or upgrading to a newer version of Windows Server.
- Define a high-level project plan that includes timelines, milestones, and resource allocation

CURRENT ENVIRONMENT ASSESSMENT

- Document the existing AD infrastructure, including domain controllers, sites, Organisational Units (OUs), Group Policies, and trust relationships.
- Evaluate the health of your current AD environment. Ensure there are no replication issues, DNS problems, or other errors.

COMPATIBILITY AND REQUIREMENTS

- Verify the current hardware and software are compatible with the new AD version.
- Check if the current AD schema and functional levels meet the requirements for the upgrade.

RISK ASSESSMENT AND MITIGATION

- Conduct a risk assessment to identify potential issues that could arise during the upgrade.

DEPENDENCY ANALYSIS

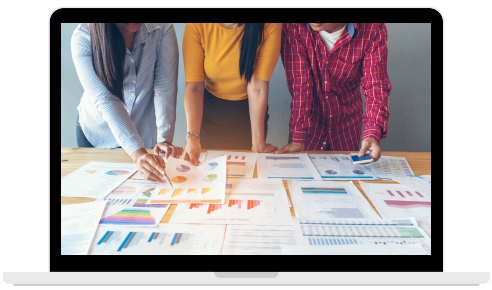
- Identify applications and services that depend on AD and ensure they are compatible with the new version.
- Map out interdependencies within your AD environment to understand the impact of the upgrade.

BACKUP AND RECOVERY

- Review AD backup solution and recovery procedures.
- Review periodically tests of recovery plans to ensure they work as expected.

TESTING AND VALIDATION

- Set up a test environment that mirrors your production environment to validate the upgrade process.



Deliverable: Gap Analysis & Recommendation Report

Duration: 2 Weeks

REPORT: KNOW WHAT'S INCLUDED:

Active Directory Audit and Gap Analysis Report

TABLE OF CONTENT

INTRODUCTION

<Customer> has engaged Mismo Systems to undertake a comprehensive review of their Active Directory (AD) environment. This initiative aims to assess the health, performance, and security of the AD infrastructure, and to identify any existing gaps or areas for improvement.

Active Directory Health Assessment: The review will include a thorough examination of the AD environment to identify any existing issues or potential areas of concern. This involves checking the overall health of domain controllers, replication status, and the integrity of AD objects.

Active Directory Performance Assessment: Mismo Systems will analyze the performance of the AD infrastructure to ensure it meets the organization's needs. This includes assessing response times, query performance, and the efficiency of AD operations. Recommendations will be provided to optimize performance where necessary

Active Directory Security Assessment: A critical component of the review is the security assessment. This involves identifying vulnerabilities, misconfigurations, and potential threats within the AD environment. The goal is to fortify the AD infrastructure against both internal and external security risks.

ACTIVE DIRECTORY INFRASTRUCTURE OVERVIEW

Active Directory | Current State

- <Customer> operates from five locations: Chennai, Chandigarh, Mumbai, Kolkata, and Gurugram, all interconnected via IPsec tunnels. An Active Directory site is created for each of these locations, and each site has 2 domain controllers.
- Windows server 2012 R2 is the OS of the Domain Controllers,
- Gurdc01 Domain Controller, located in Gurugram is holding all FSMO roles.
- Both Forest and Domain functional levels are set to Windows Server 2008.
- All default services are enabled and running on Domain Controllers.
- FRS service is used for Sysvol replication.
- All Domain Controllers are Global Catalog (GC) servers.
- AD Recycle Bin is not enabled.
- Some OUs are not protected from accidental deletion.
- VM level backup for Domain Controllers is configured.
- The Directory Services Restore Mode (DSRM) password is not known.
- Internet browsing is enabled on both Domain Controllers.

Active Directory | Current State

- A workflow exists for user creation. IT team receives user creation forms from HR team.
- When users leave the organization, the IT team disables their user accounts but never delete them.
- Administrators are using their regular accounts to perform administrative tasks on Domain Controllers
- There are many privileged users in the Domain Admins and Enterprise Admins groups.
- There are many service accounts in use, however there is no proper list available with <Customer> team, except for those used in LDAP configuration of applications.
- There are multiple UPN suffixes configured: <list of UPN suffixes>
- There is no external time server source configured on PDC; instead, it relies on the local hardware clock to maintain system time.
- Delegations are configured on OUs
- The "Default Domain Policy" is unlinked from the domain and not in use. Instead, a new policy has been created to configure password and account lockout settings.
- Group Policies are not properly managed.
- DNS scavenging is not configured properly. There are many old static records exists, and no cleanup was performed for a long time.

ACTIVE DIRECTORY GAPS & RECOMMENDATION

Active Directory | Gaps & Recommendations

Gap	Recommendation	Criticality	Complexity
The Domain Controllers are running on Windows Server 2012 R2, which reached its end of life on October 10, 2023.	The OS will no longer receive security updates, non-security updates, bug fixes, technical support, or online technical content updates. It is highly recommended to upgrade all the domain controllers to Windows Server 2022 or Windows Server 2025 for enhanced performance, stability, improved security, and access to the latest AD features.	High	High
Both Domain and Forest functional levels are set to Windows Server 2008	It is recommended to raise both Forest and Domain functional levels to the latest available after upgrading the OS, for enhanced performance, stability, improved security, and access to the latest AD features	Medium	Medium
FRS is being used for SYSVOL replication	It is recommended migrating from FRS to DFSR, FRS is a legacy service.	Medium	High
All default services are enabled and running.	To harden the AD DS environment, disable the unnecessary services running on all the Domain Controllers along with the 3rd party application services, which are not needed to be installed on the domain controller only.	Medium	Low
Password Policy is not aligned with best practices	• The "Default Domain Policy" is not in use • Password history is currently set to 5 days, it should be set to 24 • Maximum Password age is set to 45 days, it should be 42 days • Minimum password length is currently set to 8 Character, it should be set to 14 characters	Medium	Medium
AD Recycle Bin is not enabled	It is recommended to enable AD Recycle Bin. It helps recover accidentally deleted objects quickly and easily, minimizing downtime and data loss.	High	Low
All OUs are not protected from accidental deletion	All the OUs in the domain should be protected from accidental deletion.	High	Low

Active Directory | Gaps & Recommendations

Gap	Recommendation	Criticality	Complexity
Internet browsing is allowed on all Domain Controllers	Internet browsing must be block on all Domain Controller to improve Security, minimize attach surface, preventing unauthorized changes and compliance.	High	Low
System State backup for Domain Controllers is not configured	It is recommended to take a daily system state backup of one of the Domain Controllers (DCs). Specifically, take the system state backup of the DC holding all the FSMO roles.	High	Medium
<Customer> team doesn't delete any user accounts. As part of the offboarding process, they only disable the user account and keep it forever.	As part of the offboarding process, <Customer> should disable the user account for 30 days, followed by deletion within 30 to 90 days. As a workaround, if <Customer> needs to retain the user's mailbox for an extended period, move the account to a non-syncing OU. This will remove the user account from Azure AD (O365 Admin Center). After deletion, restore the account from the deleted users' section, which will convert it into a cloud-only user. **Note:** You can restore the deleted user's mailbox within 30 days, ensuring their mailbox data is retained.	Medium	Medium
Many stale and obsolete objects exist.	Review all the stale objects and perform the clean up as no clean-up has been performed for the environment. Also, make it a practice to do the cleanup every 3-6 months.	Medium	Medium
<Customer> team does not have the Directory Services Restore Mode (DSRM) password	The Directory Service Restore Mode (DSRM) password is essential for performing Active Directory restores from backups. It is highly recommended to reset this password and store it securely in password management tool	High	Low
There is no Secure Access Workstation (SAW) to administer Domain Controllers	Access and administrate Domain Controllers from a dedicated physical secure workstation.	Medium	Medium

→ **REPORT: KNOW WHAT'S INCLUDED:**

Active Directory Audit and Gap Analysis Report

Active Directory | Gaps & Recommendations

Gap	Recommendation	Criticality	Complexity
Too many users are part of Domain Admins and Enterprise Admins Groups	• Minimize the domain admin and Enterprise Admin groups memberships. • Only user objects should be added to these groups. • Service account shouldn't be a part of these groups. • We recommend using the concept of principle of least privilege (PoLP).	High	Low
Administrators are using their regular accounts for administrative purpose.	All IT administrators must have two AD accounts. A regular account for day-to-day tasks such as checking email, browsing the internet, ticket system etc., and ADM account for carrying out Active Directory administrative tasks.	Medium	Low
No regular password reset for krbtgt account	It is highly recommended to reset the krbtgt account password regularly, ideally every 6 to 12 months. krbtgt account maintains two passwords, so it is recommended to reset the password twice after an interval of 12-24 hours. **Note:** *Password reset for krbtgt account must be done carefully. Before resetting krbtgt account password, please ensure that all Domain Controllers are powered on, Active Directory is healthy replication is happening properly.*	Medium	High
There might be some unused UPN suffixes created	Review the UPN suffixes and delete the suffixes which are not in use.	Low	Medium
Site and Services are not properly configured	Create AD site for each location where local Domain Controller is required with respective subnets.	Medium	Medium

Active Directory | Gaps & Recommendations

Gap	Recommendation	Criticality	Complexity
Only specific security patches are being installed on Domain Controllers	Microsoft recommends installing all updates, including security patches, on domain controllers. This ensures that your systems are protected against vulnerabilities and benefit from improvements in stability and performance. Here are some key points: • **Security Patches**: Always prioritize these to protect against known vulnerabilities. • **Critical Updates**: These address significant issues that could impact the functionality of your domain controllers. • **Stability and Performance Updates**: These updates help improve the overall performance and reliability of your system. Microsoft advises testing updates in a controlled environment before deploying them to production to avoid potential disruptions.	High	Medium
Server Message Block v1 (SMBv1) is currently enabled.	SMBv1 is outdated and vulnerable to several exploits, including the EternalBlue attack used in the WannaCry ransomware. It is recommended to disable SMBv1 and use later versions (SMBv2 or SMBv3), which are more secure and are the standard for file-sharing services. **Note:** *Ensure that no applications are dependent on SMBv1, as disabling it may cause them to malfunction.*	Medium	Low
There is no external time server source configured on PDC	Configuring Network Time Protocol (NTP) on the Domain Controller holding the PDC emulator role is recommended for proper time synchronization and authentication across the organization	Medium	Low
Delegations configured on OUs	Remove the delegations that are no longer in use. Revisit all the delegations from the above attached and remove the unwanted delegations.	High	Medium

Active Directory | Gaps & Recommendations

Gap	Recommendation	Criticality	Complexity
Service account management is inadequate	• Review all the service accounts and their group membership. Service accounts should have least privileges unless it requires a specific privileged role to carry out a desired task. • Place service accounts in a dedicated OU to simplify management and apply consistent policies. Identify all the service accounts and review their group membership. • Service accounts should have least privileges unless it requires a specific privileged role to carry out a desired task. • Each service account should have its description. Description should state the purpose for which the service account is created.	Medium	Medium
DNS Scavenging is not configured properly and there are many static old records	Set DNS scavenging on DNS Zones and DNS servers to maintain a clean and accurate DNS database by removing outdated records that are no longer valid. Also, manually delete static records no longer needed	Medium	Low
DHCP role is configured on sone of the Domain Controllers	It's generally recommended not to run any additional roles on your domain controller other than DNS. This helps to reduce the attack surface and avoid performance issues	Medium	Medium
Extend Active Direcotry on Cloud	Evaluate extending Active Directory to Microsoft cloud by putting root Domain Controllers on Microsoft Azure and protect, secure and monitor using Microsoft Azure services	Medium	Medium
Domain Controllers are not properly hardening	Domain Controllers hardening should be done following CIS security Benchmark for Windows Server	Medium	Medium

GENERAL RECOMMENDATIONS

Active Directory | General Recommendations

- Educate users to use long passwords and passphrases. Passphrases are simply two or more random words put together.
- IT administrators must have two AD accounts. A regular account for day-to-day tasks such as checking email, browsing the internet, ticket system etc., and ADM account for carrying out Active Directory administrative tasks.
- It is recommended to assign resource access to groups rather than individual accounts, as this simplifies resource management.
- Do not name your security groups with generic names. Instead, use descriptive names that state the purpose of the security group.
- Active Directory Auditing and Log management (SIEM) solution should be implemented.
- MFA should be configured to RDP on all Domain Controllers
- When privileged accounts, such as Domain Admin access, are needed, temporarily place the account in the necessary Administrator Groups and remove it after the work is completed.
- Active Directory events should be monitored to detect compromising and abnormal behaviour on the network.
- Patch management and vulnerability scanning should be regularly performed.

Active Directory | General Recommendations

- Follow Microsoft's recommended naming conventions for creating objects in Active Directory.
- Monitor DHCP logs for connected devices.
- Monitor DNS logs for malicious network activity.
- Configure the following audit policies:
  - Audit computer account management (success/failure).
  - Audit security group management (success/failure).
  - Audit sensitive privilege use (success/failure).
  - Audit audit policy changes (success/failure).
  - Audit authentication policy changes (success/failure).
- Use descriptive GPO names to quickly identify the GPO by name and make group policy management easier.
- Do not modify the default domain and default domain controller policies.
- Speed up GPO processing by disabling unused computer and user configurations. For example, if a GPO has computer settings configured but no user settings, disable the user configuration for that GPO to speed up group policy processing.
- Use small GPOs to simplify administration. Small GPOs make troubleshooting, managing, designing, and implementing much easier.
- Regularly review the GPOs and disable the group policies that are not in use.

NEXT STEPS

- Prepare a roadmap for remediating all the identified gaps

CONTACT US

Over the years, we have helped many organisations to digitally transform business processes, drive insights from business data and implement an efficient, secure, and scalable IT Infrastructure using the power of technology innovations. We are eager to connect with you and add value.

+911204978056 | +447435425513

connect@mismosystems.com

www.mismosystems.com

India (Noida, Dehradun) | United Kingdom (London)

INDIA | Corporate Office
A-35, Second Floor, Sector 2, Gautam Buddha Nagar, Noida, Uttar Pradesh- 201301

INDIA | R&D Center
2043, Ground Floor, Doon Express Business Park, Subhash Nagar, Dehradun, Uttarakhand - 248002

UK | London Office
First Floor, The Urban Building, 3-9 Albert Street, Slough, United Kingdom, SL1 2BE

SECURING YOUR TOMORROW, TODAY.

STAY IN TOUCH WITH US!

Website
www.mismosystems.com

Phone
+911204978056 | +44 (0) 74354 25313

E-mail
connect@mismosystems.com

India | Corporate Office
A-35, Second Floor, Sector 2,
Gautam Buddha Nagar, Noida,
Uttar Pradesh- 201301

India | R&D Center
2043, Ground Floor, Doon Express
Business Park, Subhash Nagar,
Dehradun, Uttarakhand - 248002

UK | London Office
First Floor, The Urban Building,
3-9 Albert Street, Slough,
United Kingdom, SL1 2BE