Active Directory IT Audit Checklist

Mouhyi Eddine Lahlali

This enhanced checklist provides a detailed framework for auditing an Active Directory environment, focusing on security, compliance, and operational efficiency. Regularly performing such audits can significantly reduce security risks and help maintain a robust, secure, and efficient AD infrastructure.

Advanced Security Settings

- Enable Advanced Audit Policy Configuration to ensure detailed auditing of events that matter most.
- Check for the existence of any Null SID in security permissions which could allow anonymous access.
- Audit the use of Service Accounts to ensure they are configured with the principle of least privilege and have appropriate service principal names (SPNs) set up.
- Implement LDAP Signing and LDAPS (LDAP over SSL) to protect against man-in-the-middle attacks.

Privileged Access Management

- Review and implement Just Enough Administration (JEA) policies to limit powershell command usage based on role.
- Audit the use of Privileged Access Workstations (PAWs) for handling sensitive tasks to reduce attack surfaces.
- Ensure implementation of Administrative Tier Model for segregating administrative accounts based on their scope of administration.

Account Security Practices

- Enforce User Account Control (UAC) settings to mitigate the impact of a malware attack.
- Implement Multi-Factor Authentication (MFA) for all administrative and sensitive user accounts.
- Review and apply Account Lockout Policies to protect against brute force attacks.

Fine-Grained Password Policies

- Check for and implement Fine-Grained Password Policies (FGPP) to apply different password policies within the same domain, especially for high-privileged user accounts.

DNS and Network Protection

- Audit DNS zones and settings for security configurations and ensure Dynamic DNS updates are secured.
- Review and secure AD-integrated DNS zones by applying access control list (ACL) restrictions.
- Ensure that Domain Controllers are properly isolated in the network to prevent unauthorized access.
- Time Synchronization
- Verify that all Domain Controllers and member servers are synchronized with a reliable time source to prevent Kerberos authentication issues.

Delegation of Control

- Review delegations to ensure only necessary permissions are granted and use administrative roles for delegation where possible.
- Audit custom delegated permissions for potential over-privilege and ensure segregation of duties.

Group Policy Objects (GPOs) Management

- Review and clean up unused GPOs and unlinked GPOs.
- Audit GPO permission settings to ensure only authorized users can modify high-impact GPOs.
- Implement GPO version control and change management practices to track changes and their impact.

Critical System and Object Protection

- Protect critical AD objects with Administrative SDHolder and Security Descriptor Propagator to prevent unauthorized changes.
- Enable Recycle Bin Feature in AD to recover deleted objects.
- Audit and secure the Default Domain Policy and Default Domain Controllers Policy by reviewing their settings and ensuring they are applied correctly.
- Verify that AD backups are performed regularly and test recovery procedures to ensure they are effective.
- Review the Disaster Recovery Plan (DRP) for Active Directory to ensure it's up-to-date and comprehensive.

Logging, Monitoring, and Auditing

- Ensure that AD auditing is enabled for key events such as account creation, deletion, and modification.
- Review security logs for suspicious activities or policy violations.
- Implement a centralized logging solution for better analysis and monitoring of AD-related events.

Backup and Recovery

- Verify that AD backups are performed regularly and test recovery procedures to ensure they are effective.
- Review the Disaster Recovery Plan (DRP) for Active Directory to ensure it's up-to-date and comprehensive.

Replication and Site Topology

- Check AD replication for errors or issues using tools like REPADMIN or AD Replication Status Tool.
- Review site topology to ensure it reflects the current network infrastructure and optimizes replication traffic.

Schema Management

- Audit changes to the AD schema to ensure they are authorized and documented.
- Review the schema version and compare it against the current AD DS version for compatibility.