Active Directory Maintenance Schedule

Our experts created this schedule to help you plan your own AD maintenance tasks throughout the year.

Daily Tasks

1. Take backups, including system state and Group Policies
2. Ensure IAM automated provisioning / deprovisioning of users is functioning (i.e., create, disable, and delete)
3. Review AD operational health (i.e. replication, Domain Name System (DNS), morphed Group Policy Objects (GPOs), and Domain Controller (DC) time drift)
4. Check for and remediate weak, breached, and re-used passwords

January	February	March
April	May	June
July	August	September
October	November	December

Monthly Tasks

1. Remove inactive user accounts
2. Remove inactive computer accounts
3. Perform monthly Microsoft security patching and hypervisor component patching
4. Remove unlinked GPOs
5. Validate that all privileged accounts and service accounts have a fine-grained password policy (FGPP) with strong password requirements
6. Confirm that all privileged accounts are members of the Protected Users group
7. Rotate privileged service account passwords
8. Rotate the AZUREADSSOACC Kerberos decryption key if Azure Active Directory Seamless Single Sign-On (Azure AD Seamless SSO) is in-use

January	February	March
April	May	June
July	August	September
October	November	December

Quarterly Tasks

1. Review sensitive access
2. Review/minimize privileged group membership
3. Review/limit hypervisor admin privileges
4. Test security information and event management (SIEM) for alert functionality (i.e., privileged groups and privileged users being modified)
5. Review/evaluate privileged access management (PAM) tool permissions
6. Test security controls to validate they work as expected
7. Review and remediate duplicate service principal names (SPNs)
8. Check for and remediate organizational units (OUs) not protected from accidental deletion

Quarter 1: Jan - Mar
Quarter 2: Apr - Jun
Quarter 3: Jul - Sep
Quarter 4: Oct - Dec

Semi-Annual Tasks

1. Test backups and ensure they are malware-free
2. Review GPO baselines and ensure policies are linked appropriately
3. Review domain controller (DC) build documentation
4. Review domain password policy
5. Compare and remediate baseline configurations against industry best practices (i.e., STIG, CIS, Microsoft, etc.)
6. Perform manual printer object pruning

Half 1: Jan - Jun
Half 2: Jul - Dec

Annual Tasks

1. Rotate service account passwords
2. Reset the KRBTGT account password
3. Rotate break glass account passwords and test functionality
4. Rotate Directory Services Restore Mode (DSRM) password(s)
5. Conduct a tabletop disaster recovery (DR) exercise
6. Re-certify all privileged accounts, including privileged service accounts
7. Evaluate for DC operating system upgrades
8. Evaluate for domain- and forest-functional level upgrades
9. Renew Secure Lightweight Directory Access Protocol (LDAPS) certificates issued to DCs

Year: Jan - Dec

RAVENSWOOD TECHNOLOGY GROUP