ACTIVE DIRECTORY SECURITY ASSESSMENT CHECKLIST

VERSION FRANÇAISE

INTRODUCTION

Active Directory is a critical component of Microsoft based information systems ; it provides unified management features for user accounts, resources and access rights or permissions. Gaining high privileges in this context instantly grants full control over all resources that are managed through the Active Directory infrastructure.

Recently observed adversary tactics shed light on regained interest for targeting Active Directory infrastructures, given their essential role in most information systems. Attackers who have gained high privileges are be able to deploy malware at scale throughout the whole network, leveraging GPOs or direct connections (`psexec`, `wmiexec`). Weak security controls in such environments pose a real systemic threat to the whole IT system in organizations.

ANSSI regularly meets a critical lack of cyber security maturity when applied to Active Directory environments. The observed security level weakens significantly with time, loose day-to-day operations and management.

To address this growing risk, ANSSI has implemented and publishes an assessment checklist and corrective measures. This is intended for CTOs and CISOs, helping them track the actual security level of their Active Directory infrastructures. This collection will be improved upon on a regular basis, benefiting from ongoing research, observed practical constraints and solutions during audits, as well as threat intelligence.

Each assessment item aims at ensuring no dangerous practices either pose a threat to the infrastructure or may have already been exploited by an attacker. Based on found weaknesses, each Active Directory forest is given a score, or level:

- [1] Critical weaknesses and misconfigurations pose an immediate threat to all hosted resources. Corrective actions should be taken as soon as possible;
- [2] Configuration and management weaknesses put all hosted resources at risk of a short-term compromise. Corrective actions should be carefully planned and implemented shortly;
- [3] The Active Directory infrastructure does not appear to have been weakened from what default installation settings provide;
- [4] The Active Directory infrastructure exhibits an enhanced level of security and management;
- [5] The Active Directory infrastructure correctly implements the latest state-of-the-art administrative model and security features.

To gain any given level, an Active Directory forest must pass all of the lower assessment items. A level 5 forest successfully passed the full assessment checklist.

Each assessment item provides the following guidance information:

- Assigned security level and item title;
- Item identifier;
- A detailed description of the vulnerability or weakness assessed during the audit;
- Resolution guidance and references to pass the current item and properly harden the Active Directory infrastructure.

Official documentation resources are provided when applicable .

Built upon years of internal research and experience, the ADS (Active Directory Security) assessment service provides regulated infrastructure operators and the public sector with a fully-fledged Active Directory audit capability. It aims at restoring visibility and maturity with respect to actual cyber security exposure of their environments. Practical, progressive measures and agency support are intended to help improve security and track changes in the long run. The agency's ADS assessment service implements every item listed herein.

CONTEXT: CONTROL PATH EXPOSURE

A control path materializes through a set of granted access permissions: each granted permission can be expressed as one object controlling another through a specific property, attribute or setting. Control paths reveal how an attacker could leverage a chain of defective or dangerous permissions to gain control of some targets. They can also be leveraged to quickly identify domain mismanagement, to validate the actual security boundary of a particular scope (making sure some object of interest cannot be taken over by unauthorized users through misconfiguration). Indicators of compromise may also be found through control path review.

CONTEXT: PRIVILEGED GROUPS

Privileged groups include administrator groups and operator groups which have full control over the Active Directory forest either by design, or by granting themselves such privileges:

- « Administrators »;
- « Schema Admins »;
- « Enterprise Admins »;

- « Domain Admins »: these administrators are able to read the authentication database and extract password hashes and other secrets of all privileged accounts;
- « Account Operators »: these operators can manage user accounts, machine accounts and groups except accounts protected by the `adminSDHolder` mechanism;
- « Server Operators »: these operators can manage domain controllers, which grants them the ability to recover privileged user secrets directly from the authentication database;
- « Backup Operators »: these operators can backup a domain controller, which grants them the ability to recover privileged user secrets from that backup;
- « Print Operators »: these operators can load arbitrary printer drivers on domain controllers, which grants them the ability to recover privileged user secrets directly from the authentication database (by loading a malicious driver).

The « operators » groups are empty by default and must not have any member.

ASSESSMENT ITEM LIST

An assessment item may appear at multiple Active Directory security levels. The higher the level, the stricter its rules. Only items from security levels 1 through 3 are published so far. Future updates of this document will bring items from higher levels.
This list helps navigate the Active Directory security assessment checklist:

[1] [2] Dangerous control paths expose a naming context root
[1] [2] Dangerous permissions on the adminSDHolder object
[1] [2] Dangerous control paths expose domain controllers
[1] [2] Dangerous control paths expose DPAPI keys
[1] [2] Dangerous control paths expose gMSA keys
[1] [2] Dangerous control paths expose DFSR settings of the SYSVOL share
[1] [2] Dangerous control paths expose schema objects
[1] Dangerous control paths expose MicrosoftDNS servers
[1] Dangerous control paths expose GPOs applied to privileged group members
[1] [2] Dangerous control paths expose members of privileged groups
[1] Large privileged group member count
[1] Domain controllers in inconsistent state
[1] Constrained authentication delegation to a domain controller service
[1] Constrained delegation with protocol transition to a domain controller service
[1] Resource-based constrained delegation on domain controlers
[1] Kerberos pre-authentication disabled for privileged accounts
[1] Privileged accounts with SPN
[1] Privileged accounts with never-expiring passwords
[1] Privileged account passwords age too old
[1] Domain controllers with passwords unchanged for more than 45 days
[1] Inactive domain controllers
[1] Dangerous control paths expose certificate containers
[1] [2] Dangerous control paths expose certificate templates
[1] Accounts with PrimaryGroupID lower than 1000
[1] [2] [3] Weak or vulnerable certificates
[1] DnsAdmins group members
[1] [3] Misconfigured DNS zones
[1] [2] Dangerous dsHeuristics settings
[1] Unfiltered outbound domain trust relationship
[1] Outbound forest trust relationships with sID History enabled
[1] Dormant accounts
[2] Privileged group members with weak password policy
[2] Unconstrained authentication delegation
[2] Kerberos pre-authentication disabled
[2] Use of Kerberos with weak encryption
[2] Accounts with never-expiring passwords
[2] Servers with passwords unchanged for more than 90 days
[2] SYSVOL replication through NTFRS
[2] Bad Active Directory versions
[2] The "Pre-Windows 2000 Compatible Access" group includes "Anonymous"
[2] Krbtgt account password unchanged for more than a year
[2] Privileged users revealed on RODC
[2] Accounts or groups with unexpected SID history
[2] Trust account passwords unchanged for more than a year
[3] Servers with passwords unchanged for more than 45 days
[3] Inactive servers
[3] Accounts with modified PrimaryGroupID
[3] Use of the "Pre-Windows 2000 Compatible Access" group
[3] Incorrect object owners
[3] Privileged accounts outside of the Protected Users group
[3] Accounts with passwords stored using reversible encryption
[3] Dangerous configuration of read-only domain controllers (RODC) (neverReveal)
[3] Dangerous configuration of read-only domain controllers (RODC) (reveal)
[3] Dangerous configuration of replication groups for read-only domain controllers (RODCs) (allow)
[3] Dangerous configuration of replication groups for read-only domain controllers (RODCs) (denied)
[3] Accounts or groups with SID history set
[3] Inbound trust relationships with delegation

1 2 DANGEROUS CONTROL PATHS EXPOSE A NAMING CONTEXT ROOT

FR EN

ID : `vuln1_permissions_naming_context vuln2_permissions_naming_context`

DESCRIPTION

Dangerous control paths expose the root of Active Directory *naming contexts*.

These permissions grant the trusted *Principal* complete control over the Active Directory.

RECOMMENDATIONS

An Active Directory has several naming contexts:

- `Domain`, contains domain object information, such as users, groups, computers, ...;
- `Configuration`, contains forest configuration settings;
- `Schema`, contains object attribute definitions;
- `DomainDns`, contains domain-level DNS zones;
- `ForestDns`, contains forest-level DNZ zones.

Changing default permissions to these various naming context roots is strongly discouraged. They should be reverted to default permissions. The fix is usually applied through the `adsiedit.msc` or `ldp` utilities.

Some of these access rights, especially regarding the Microsoft Exchange service, can be fixed by relevant security updates which must be applied. It is notably the case for the following principals:

- Exchange Windows Permissions
- Exchange Trusted Subsystem

- For Exchange Server related issues: https://support.microsoft.com/en-us/help/4490059/using-shared-permissions-model-to-run-exchange-server
- For Azure ADConnect Accounts (MSOL): https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-configure-ad-ds-connector-account Use the cmdlet `Set-ADSyncRestrictedPermissions`.

If special permissions are required, delegated groups or accounts should be considered as privileged. Therefore, they must comply with appropriate protection measures, and their own access control list should be at least as strict as that of the `adminSDHolder` object. "Secure" ACLs should therefore be implemented on these delegated groups, which will not open a new control path exposure. To remove inheritance and restrict ACEs, the following command may be used: `Set-ADSyncRestrictedPermissions` found in the `AdSyncConfig.psm1` module from Azure AD Connect.

Example: applying "secure" permission on a privileged account through `Set-ADSyncRestrictedPermissions`:

```
Import-Module .\AdSyncConfig.psm1
$credential = Get-Credential
Set-ADSyncRestrictedPermissions -ADConnectorAccountDN "CN=PRIVACCOUNT,CN=Users,DC=exemple,DC=ads" -
Credential $credential
```

Note: the `AdSyncConfig.psm1` module may be extracted from the Azure AD Connect installer with `msiexec`: `msiexec /a "AzureADConnect.msi" /qb TARGETDIR=c:\temp\`

The installation package may be downloaded from https://go.microsoft.com/fwlink/?LinkId=615771.

1 2 DANGEROUS PERMISSIONS ON THE ADMINSDHOLDER OBJECT

FR EN

ID : `vuln1_permissions_adminsdholder vuln2_permissions_adminsdholder`

DESCRIPTION

Dangerous permissions are set on the `adminSDHolder` object. Permissions set on this object may grant trusted objects full control over the Active Directory. In a tiered administrative model, these permissions allow compromise of Tier 0 objects from lower trust tiers.

RECOMMENDATIONS

GENERAL CASE

Permissions set on the `adminSDHolder` object are periodically copied to all protected AD objects (privileged built-in group members). By default, only privileged objects are granted access rights on the `adminSDHolder` object. This mechanism protects the most privileged Active directory users and groups from accidental misconfigurations.

Modifying default permissions set on this object is strongly discouraged. Removing dangerous permissions is strongly advised to return the object to its default state. Fixing usually requires using `adsiedit.msc` or the `ldp` utility.

SPECIFIC CASES

When deploying an administration forest, granting access rights on the `adminSDHolder` object to a group is tolerated given the following cumulative criterias are met:

- access rights on the trusted group are stricter than those initially granted on the `adminSDHolder` object;
- permission inheritance is disabled for the trusted group.

If a flagged access right relates to Exchange, (such as WRITE_SPN), the latest relevant cumulative updates must be applied. Documentation on access rights granted to Exchange Server is available at the following URL:

- https://support.microsoft.com/en-us/help/4490059/using-shared-permissions-model-to-run-exchange-server
  Note: if flagged, the WRITE_ALT_IDENTITY access right granted to `Exchange Trusted Subsystem` is a configuration defect that will be fixed by Microsoft in an upcoming update.

If a flagged access right relates to an Azure adconnect account (MSOL), its relevant access rights must be reconfigured. Documentation is available at the following URL:

- https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-configure-ad-ds-connector-account
  PowerShell cmdlets `Set-ADSyncRestrictedPermissions` and `-SkipAdminSdHolders` may be used during the configuration phase.

Objects with access rights on the `adminSDHolder` object must, themselves, be protected by the `SDProp` mechanism.

Consequently, only members of administrative or operator groups can be delegated such access rights.

In the case of administrative forest deployments, adding access rights on`adminSDHolder` is tolerated if the following conditions are met:

- delegated groups must be of `DOMAIN LOCAL` type
- permissions on that group must be stricter than those applied to `adminSDHolder`

- For Exchange related issues: https://support.microsoft.com/en-us/help/4490059/using-shared-permissions-model-to-run-exchange-server
  The control from `Exchange Trusted Subsystem` with `WRITE_ALT_IDENTITY` should be fixed by Microsoft in a future release.
- For Azure ADConnect Accounts (MSOL): https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-configure-ad-ds-connector-account
  Use the cmdlet `Set-ADSyncRestrictedPermissions` and `-SkipAdminSdHolders` in configuration commands.

1 2 DANGEROUS CONTROL PATHS EXPOSE DOMAIN CONTROLLERS

FR EN

ID : `vuln1_permissions_dc vuln2_permissions_dc`

DESCRIPTION

GENERAL CASE

Dangerous control paths expose domain controllers. Accounts granted these permissions can take full control over the Active Directory. An attacker could replicate all secrets from the user database (including Domain Admins), reuse them and gain full control over the domain.

READ-ONLY DOMAIN CONTROLLERS (RODC)

When the flagged domain controller is a RODC, an attacker can replicate all of the secrets it is allowed to store locally and can become local administrator. The `MANAGED_BY` attribute grants local administration privileges on a RODC.

RECOMMENDATIONS

Accounts which are granted permissions on domain controllers must be considered privileged. Therefore, they must be protected through the `adminSDHolder` mechanism. These accounts must belong to either the Enterprise Admins or the Domain Admins group.

When deploying an administration forest, granting access rights on domain controllers is tolerated given the following cumulative criterias are met:

- delegated groups must be of `DOMAIN LOCAL` type
- permissions on that group must be stricter than those applied to `adminSDHolder`

1 2 DANGEROUS CONTROL PATHS EXPOSE DPAPI KEYS

FR EN

ID : `vuln1_permissions_dpapi vuln2_permissions_dpapi`

DESCRIPTION

Dangerous control paths expose `DPAPI` keys. An attacker could recover all domain data encrypted via DPAPI, if he gains access to such data.

RECOMMENDATIONS

Microsoft Windows provides a data protection feature (`DPAPI`) which usually aims at encrypting user files or passwords, or that of a privileged system process. `DPAPI` is used by the Windows password manager, web browsers, mail or instant messaging clients, Wi-Fi passphrase or certificate storage among others. Data is encrypted with a master key, itself protected by its user password or a domain backup key. Note: `DPAPI` is considered strong and not questioned by the issue raised in this item.

Editing access control lists of these objects is not recommended. Thus, access rights on `DPAPI` keys need to be carefully reviewed or reverted to their default state. The fix is usually applied through the `adsiedit.msc` or `ldp` utilities.

1 2 DANGEROUS CONTROL PATHS EXPOSE GMSA KEYS

FR EN

ID : `vuln1_permissions_gmsa_keys vuln2_permissions_gmsa_keys`

DESCRIPTION

Dangerous control paths expose *group managed service accounts* (gMSA) keys. An attacker gaining access to those keys will be able to recover their associated gMSA passwords.

RECOMMENDATIONS

gMSA member accounts inherit some user and computer class attributes which eases service account management. gMSA leverage the key distribution service (KDS) to create and manage account passwords. These passwords are derived from a KDS-managed key.

Editing access control lists of these objects is strongly discouraged. Thus, access rights on gMSA keys need to be carefully reviewed or reset to their default values. If these modifications are required, trusted *Principals* they delegate access rights to should be protected by the `adminSDHolder` mechanism.

To restore default permission the following command may be used: `Dsacls <DN> /S /T`. This command restores the permissions from the schema.

1 2 DANGEROUS CONTROL PATHS EXPOSE DFSR SETTINGS OF THE SYSVOL SHARE

FR EN

ID : `vuln1_permissions_dfsr_sysvol vuln2_permissions_dfsr_sysvol`

DESCRIPTION

Dangerous control paths expose DFSR settings of the SYSVOL share. An attacker could register a new DFS replication group member, gaining the ability to modify SYSVOL contents and force its synchronization across the group. Group policies and/or scripts modified this way could then be applied through linked GPOs, making it possible to fully compromise the domain.

RECOMMENDATIONS

Editing access control lists of these objects is not recommended. Thus, access rights on DFSR SYSVOL settings must be carefully reviewed or reverted to their default state. If these modifications are required, trusted *Principals* they delegate access rights to should be protected by the `adminSDHolder` mechanism. The fix is usually applied through the `adsiedit.msc` or `ldp` utilities.

If special permissions are required, delegated groups or accounts should be considered as privileged. Therefore, they must comply with appropriate protection measures, and their own access control list should be at least as strict as that of the `adminSDHolder` object. "Secure" ACLs should therefore be implemented on these delegated groups, which will not open a new control path exposure. To remove inheritance and restrict ACEs, the following command may be used: `Set-ADSyncRestrictedPermissions` found in the `AdSyncConfig.psm1` module from Azure AD Connect.

Example: applying "secure" permission on a privileged account through `Set-ADSyncRestrictedPermissions`:

```
Import-Module .\AdSyncConfig.psm1
$credential = Get-Credential
Set-ADSyncRestrictedPermissions -ADConnectorAccountDN "CN=PRIVACCOUNT,CN=Users,DC=exemple,DC=ads" -
Credential $credential
```

Note: the `AdSyncConfig.psm1` module may be extracted from the Azure AD Connect installer with `msiexec`: `msiexec /a "AzureADConnect.msi" /qb TARGETDIR=c:\temp\`

The installation package may be downloaded from https://go.microsoft.com/fwlink/?LinkId=615771.

1 2 DANGEROUS CONTROL PATHS EXPOSE SCHEMA OBJECTS

FR EN

ID : `vuln1_permissions_schema vuln2_permissions_schema`

DESCRIPTION

Dangerous control paths expose schema objects. These permissions grant the trusted *Principal* complete control over the Active Directory.

RECOMMENDATIONS

Schema is one of three main Active Directory naming context. It contains every object attribute definitions of the forest.

Changing default permissions to these various naming context roots is strongly discouraged. They should be reverted to default permissions. To restore default permission the following command may be used: `Dsacls <DN> /S /T`. This command restores the permissions from the schema.

If special permissions are required, delegated groups or accounts should be considered as privileged. Therefore, they must comply with appropriate protection measures, and their own access control list should be at least as strict as that of the `adminSDHolder` object. "Secure" ACLs should therefore be implemented on these delegated groups, which will not open a new control path exposure. To remove inheritance and restrict ACEs, the following command may be used: `Set-ADSyncRestrictedPermissions` found in the `AdSyncConfig.psm1` module from Azure AD Connect.

Example: applying "secure" permission on a privileged account through `Set-ADSyncRestrictedPermissions`:

```
Import-Module .\AdSyncConfig.psm1
$credential = Get-Credential
Set-ADSyncRestrictedPermissions -ADConnectorAccountDN "CN=PRIVACCOUNT,CN=Users,DC=exemple,DC=ads" -
Credential $credential
```

Note: the `AdSyncConfig.psm1` module may be extracted from the Azure AD Connect installer with `msiexec`: `msiexec /a "AzureADConnect.msi" /qb TARGETDIR=c:\temp\`

The installation package may be downloaded from https://go.microsoft.com/fwlink/?LinkId=615771.

1 DANGEROUS CONTROL PATHS EXPOSE MICROSOFTDNS SERVERS

FR EN

ID : `vuln1_permissions_msdns`

DESCRIPTION

Dangerous control paths expose Microsoft DNS servers.

Accounts granted permission to write the `CN=MicrosoftDNS,CN=System` container attributes have the ability to run arbitrary code on the DNS service, which is typically run on domain controllers. `DnsAdmins` group members have this permission by default.

RECOMMENDATIONS

The `DnsAdmins` must not be used: manual DNS zone delegations must be used instead to manage the service (zone creation/deletion, record management, ...). These delegations are usually granted through the `ldp` utility. This is a two-step process:

STEP 1: ALLOW ACCESS TO RPC USED BY DNS MANAGEMENT MMC SNAP-INS

In the domain naming context, under the `CN=System` container, set the following access rights on the `CN=MicrosoftDNS` container:

FR EN

☑ Read property	☐ Write Property	☐ Create Child	☐ Control access
☑ List	☐ Write DACL	☐ Delete child	☐ Extended write
☑ List object	☐ Write owner	☐ Delete	
☑ Read permissions	☐ Write SACL	☐ Delete tree	

STEP 2: ALLOW DNS ZONE MODIFICATIONS

In the `DC=DomainDnsZones` naming context, on every zone you wish to delegate management, enable inheritance and set the following access rights on the `CN=MicrosoftDNS` container:

FR EN

☑ Read property	☐ Write Property	☑ Create Child	☐ Control access
☑ List	☐ Write DACL	☑ Delete child	☐ Extended write
☑ List object	☐ Write owner	☑ Delete	
☑ Read permissions	☐ Write SACL	☑ Delete tree	

Note: to change the current *naming context* in `ldp`, go to `View,Tree` and use the drop-down list to select `DomainDnsZones`.

If special permissions are required, delegated groups or accounts should be considered as privileged. Therefore, they must comply with appropriate protection measures, and their own access control list should be at least as strict as that of the `adminSDHolder` object. "Secure" ACLs should therefore be implemented on these delegated groups, which will not open a new control path exposure. To remove inheritance and restrict ACEs, the following command may be used: `Set-ADSyncRestrictedPermissions` found in the `AdSyncConfig.psm1` module from Azure AD Connect.

Example: applying "secure" permission on a privileged account through `Set-ADSyncRestrictedPermissions`:

```
Import-Module .\AdSyncConfig.psm1
$credential = Get-Credential
Set-ADSyncRestrictedPermissions -ADConnectorAccountDN "CN=PRIVACCOUNT,CN=Users,DC=exemple,DC=ads" -
Credential $credential
```

Note: the `AdSyncConfig.psm1` module may be extracted from the Azure AD Connect installer with `msiexec`: `msiexec /a "AzureADConnect.msi" /qb TARGETDIR=c:\temp\`

The installation package may be downloaded from https://go.microsoft.com/fwlink/?LinkId=615771.

1 DANGEROUS CONTROL PATHS EXPOSE GPOS APPLIED TO PRIVILEGED GROUP MEMBERS

FR EN

ID : `vuln1_permissions_gpo_priv`

DESCRIPTION

Dangerous control paths expose GPOs that are applied to privileged group members. An attacker gaining access to these GPOs may execute code on those privilege account workstations to escalate their privileges.

RECOMMENDATIONS

GPO LDAP object permissions should be reviewed.

The fix is usually applied through the `adsiedit.msc` or `ldp` utilities.

1 2 DANGEROUS CONTROL PATHS EXPOSE MEMBERS OF PRIVILEGED GROUPS

FR EN

ID : `vuln1_privileged_members_perm vuln2_privileged_members_perm`

DESCRIPTION

Dangerous control paths expose members of privileged groups. These access rights grant non-privileged users the ability to take control of privileged accounts.

RECOMMENDATIONS

Most of the items shown here are due to the "`Dangerous permissions on the adminSDHolder object`" and "`Dangerous control paths expose domain controllers`" checks. Fixing it will take care of most of these items.

For all remaining control paths, relevant dangerous permissions should be removed. The fix is usually applied through the `adsiedit.msc` or `ldp` utilities.

If special permissions are required, delegated groups or accounts should be considered as privileged. Therefore, they must comply with appropriate protection measures, and their own access control list should be at least as strict as that of the `adminSDHolder` object. "Secure" ACLs should therefore be implemented on these delegated groups, which will not open a new control path exposure. To remove inheritance and restrict ACEs, the following command may be used: `Set-ADSyncRestrictedPermissions` found in the `AdSyncConfig.psm1` module from Azure AD Connect.

Example: applying "secure" permission on a privileged account through `Set-ADSyncRestrictedPermissions`:

```
Import-Module .\AdSyncConfig.psm1
$credential = Get-Credential
Set-ADSyncRestrictedPermissions -ADConnectorAccountDN "CN=PRIVACCOUNT,CN=Users,DC=exemple,DC=ads" -
Credential $credential
```

Note: the `AdSyncConfig.psm1` module may be extracted from the Azure AD Connect installer with `msiexec`: `msiexec /a "AzureADConnect.msi" /qb TARGETDIR=c:\temp\`

The installation package may be downloaded from https://go.microsoft.com/fwlink/?LinkId=615771.

1 LARGE PRIVILEGED GROUP MEMBER COUNT

FR EN

ID : `vuln1_privileged_members`

DESCRIPTION

The forest contains more than 50 privileged accounts.

A large number of accounts in privileged groups prevents keeping track of them: this can lead to poor accountability of privileged users that are absolutely necessary, problems with deactivating or deleting an unused account, etc.

RECOMMENDATIONS

Active Directory Privileged Groups grant their member accounts all rights and privileges on the forest. Except for the « Administrators » and « Domain Admins » groups, use of the privileged groups gives a false sense of security.

Implementing an administrative model which allows minimizing the number of privileged accounts is crucial, especially by establishing well-separated administrative roles. In doing so, administrative actions should be inventorized and affected to specific accounts through relevant rights delegations. For instance, a user management account that needs to be able to create and delete user accounts will benefit from the following delegations:

- child object creation;
- child object deletion;
- write to object attribute;
- reset password.

This is usually applied through the `ldp` utility.

Note : the Active Directory "Delegation of Control" Wizard also helps delegating access rights. While of easier use, this wizard grants excessive access rights for some delegation categories. `ldp` should therfore be preferred.

The overall model must follow the following rules regarding group membership:

- operator groups must be empty;
- replication groups must be empty;
- forest-level administrative groups (enterprise and schema) must be empty and only temporarily populated during operations which require those privileges;
- domain-level administrative groups must not contain any service account.

1 DOMAIN CONTROLLERS IN INCONSISTENT STATE

FR EN

ID : `vuln1_dc_inconsistent_uac`

DESCRIPTION

Some domain controllers in the forest have inconsistent attributes. Inconsistencies can either occur upon manual or software-induced misconfiguration. They could also reveal malicious activity.

RECOMMENDATIONS

"Writable" domain controllers must have the following setup:

- The `userAccountControl` attribute of their computer object must have the `SERVER_TRUST_ACCOUNT (0x00002000)` flag set;
- An object of type `server` must exist in the configuration partition and have a `serverReference` attribute containing the computer account DN;
- Their `server` object must have a child `NTDS Settings` object of type `nTDSDSA`.

Read-Only Domain Controllers (RODC) must have the following setup:

- The `userAccountControl` attribute of their computer object must have the `PARTIAL_SECRETS_ACCOUNT (0x04000000)` flag set;

- An object of type `server` must exist in the configuration partition and have a `serverReference` attribute containing the computer account DN;
- Their `server` object must have a child `NTDS Settings` object of type `nTDSDSARO`.

This fix is usually applied through the `ldp` utility.

Note: some publishers may introduce such deviations when installing their products. Riverbed is such a known case.

1 CONSTRAINED AUTHENTICATION DELEGATION TO A DOMAIN CONTROLLER SERVICE FR EN

ID : `vuln1_delegation_a2d2`

DESCRIPTION

Some accounts have constrained authentication delegations to services of domain controllers. These grant the subject account the ability to elevate its privileges on the domain controller.

RECOMMENDATIONS

Constrained authentication delegation allows an account to authenticate to a Kerberos service with the identity of a third-party user who has authenticated to that account. If such a delegation is authorized to a privileged resource (including domain controllers), it allows that account to elevate privileges and compromise the forest.

Constrained authentication delegation to any domain controller service must not be allowed.

For each of the aforementioned accounts, all *Service Principal Names* (SPNs) referencing domain controllers must be removed from their `msDS-AllowedToDelegateTo` attribute. This can be performed through the "Delegation" tab of the Active directory Users and Computers management console.

1 CONSTRAINED DELEGATION WITH PROTOCOL TRANSITION TO A DOMAIN CONTROLLER SERVIC FR EN

ID : `vuln1_delegation_t2a4d`

DESCRIPTION

Some accounts have constrained authentication delegations with protocol transition to a domain controller service. These grant the subject account the ability to elevate its privileges on the domain controller.

RECOMMENDATIONS

Constrained delegation with protocol transition allows an account to temporarily act on behalf of any user or computer. If that delegation is authorized to a privileged resource (including domain controllers), it allows the account to assume the privileges of that resource and compromise the forest.

Constrained delegation with protocol transition to a domain controller service must not be allowed.

For each of the aforementioned account, all *Service Principal Names* (SPNs) referencing domain controllers must be removed from their `msDS-AllowedToDelegateTo`attribute. This can be performed through the "Delegation" tab of the Active directory Users and Computers management console.

1 RESOURCE-BASED CONSTRAINED DELEGATION ON DOMAIN CONTROLERS FR EN

ID : `vuln1_delegation_sourcedeleg`

DESCRIPTION

Resource-based constrained delegation is configured on domain controllers. This configuration grants some accounts with a complete delegation to domain controllers:

RECOMMENDATIONS

Delegation mechanisms towards privileged resources (such as domain controllers) should not be used.

Unlike other delegation types based on a *Service Principal Name* (SPN), resource-based constrained delegation is configured through a security descriptor on the target resource. This security descriptor is stored in the `msDS-AllowedToActOnBehalfOfOtherIdentity` attribute of the target computer object. To remove this delegation, the attribute must be deleted.

This can be fixed with PowerShell. The following command can be used to remove such a delegation on a target computer named `COMPUTER`: `Set-ADComputer COMPUTER -PrincipalsAllowedToDelegateToAccount $Null`.

1 KERBEROS PRE-AUTHENTICATION DISABLED FOR PRIVILEGED ACCOUNTS FR EN

ID : `vuln1_kerberos_properties_preauth_priv`

DESCRIPTION

The DONT_REQUIRE_PREAUTH flag is set for some privileged users.

RECOMMENDATIONS

Kerberos pre-authentication ensures that users requesting a Ticket Granting Ticket (TGT) know a given authentication secret. Without pre-authentication, it is possible to acquire a ticket encrypted with one of the Kerberos keys associated with the requested account. It is then possible to carry out a brute-force or dictionary guessing attack to crack an account password, if it is not strong enough.

All affected accounts must have their `DONT_REQUIRE_PREAUTH` flag unset then their password changed immediately.

By default, all user accounts require pre-authentication because their `DONT_REQUIRE_PREAUTH` flag is not set. That property was designed for backward compatibility with older Kerberos implementations. It must never be set for privileged domain accounts. Any incompatible software must be upgraded.

1 PRIVILEGED ACCOUNTS WITH SPN

FR EN

ID : `vuln1_spn_priv`

DESCRIPTION

The `servicePrincipalName` (SPN) attribute is set on some privileged user accounts.

An attacker could use this to attempt a bruteforce password cracking attempt, which may succeed for accounts with weak passwords.

RECOMMENDATIONS

The `servicePrincipalName` (SPN) attribute allows linking Kerberos service names to accounts. Whenever an account owns a Kerberos service name, it becomes possible for any user to request a ticket for that service. In that case, the received ticket is encrypted with one of the corresponding account Kerberos encryption keys. Thus, it is possible to start an offline brute-force attack on the ticket to recover the account password, if it is not strong enough. By default, only computer accounts have SPNs and the attribute must remain empty for all privileged accounts.

GENERAL CASE: CLEAR SPNS

In the event that accounts currently with an SPN set must be privileged, their `servicePrincipalName` attribute must be cleared and their password must be changed.

Note: a privileged account may hold an SPN granted the following criterias are met:

- the account is a *Managed Service Account* (`sMSA` / `gMSA`);
- **OR**
  - a *Password Settings Object* (PSO) applies to that account with a **32** or more character length requirement;
  - a *Password Settings Object* (PSO) applies to that account with an expiration period of less than **3 years**;
  - the account password was changed since the last PSO modification;
- the account can only use AES encryption algorithms.

SPECIFIC CASES: REMOVE THE ACCOUNT FROM PRIVILEGED GROUPS

In the event that accounts currently with an SPN set do not required their current privileged group membership, they should be removed from those groups and be granted the relevant access rights delegations.

1 PRIVILEGED ACCOUNTS WITH NEVER-EXPIRING PASSWORDS

FR EN

ID : `vuln1_dont_expire_priv`

DESCRIPTION

Some privileged accounts have passwords that never expire.

If no security mechanism enforces a periodic password rotation, taking over an account allows any malicious user to keep their access rights in the domain for extended periods of time.

RECOMMENDATIONS

GENERAL CASE

Passwords should be periodically changed for all privileged group members (at most every 3 years). To enforce application of the domain password policy on these accounts, their `DONT_EXPIRE` flag should not be set. This account flag should then be unset, usually by unchecking the "password never expires" option in the "Account" tab of the user properties. Their passwords should then be rolled immediately.

Important note: passwords should not be renewed too often. Enforcing short password lifespans compells users to choose statistically weaker passwords, which negates the intended benefits. Password lifespan should be determined by taking into account multiple factors such as usage context. The password policy may be globally enforced on all domain accounts or scoped to select accounts, through the Password Settings Object (PSO) mechanism.

SPECIFIC CASES

If the `DONT_EXPIRE` flag has been set on accounts with difficult-to-change passwords, it may mean these accounts are not used for administration purposes (i.e. service accounts). These accounts shall not belong to any privileged group. The following must be done:

- remove those accounts from privileged groups;
- grant these accounts the required rights delegations for proper operation;
- document a specific password change procedure;
- remove the `DONT_EXPIRE` flag.

UNUSED ACCOUNTS

Unused accounts should be disabled. The following procedure provides similar benefits than deletion, while retaining information relevant to audit traces. To properly disable an account:

- disable the account;
- remove all of its group memberships;
- randomly change its password. To enforce a random password, one can check the *smart card is required for interactive logon* flag in the account properties. This is equivalent to manually setting the ADS_UF_SMARTCARD_REQUIRED flag of its `userAccountControl` attribute;
- optionally, move the account to a dedicated OU;
- optionally, update the account description field to mention the context for disabling (date, reason, etc.).

1 PRIVILEGED ACCOUNT PASSWORDS AGE TOO OLD

FR EN

ID : `vuln1_password_change_priv`

DESCRIPTION

Some privileged accounts in the forest have not changed their password for more than three years.

RECOMMENDATIONS

GENERAL CASE

Passwords should be periodically changed for all privileged group members (at most every 3 years). To enforce application of the domain password policy on these accounts, their DONT_EXPIRE flag should not be set. This account flag should then be unset, usually by unchecking the "password never expires" option in the "Account" tab of the user properties. Their passwords should then be rolled immediately.

The built-in Administrator account (RID 500, used as a last resort only) must also have its password changed at most every 3 years. It is crucial to periodically ensure this account is in working condition and that its usage guidelines and procedures are up-to-date.

Important note: passwords should not be renewed too often. Enforcing short password lifespans compells users to choose statistically weaker passwords, which negates the intended benefits. Password lifespan should be determined by taking into account multiple factors such as usage context. The password policy may be globally enforced on all domain accounts or scoped to select accounts, through the Password Settings Object (PSO) mechanism.

SPECIFIC CASES

If the DONT_EXPIRE flag has been set on accounts with difficult-to-change passwords, it may mean these accounts are not used for administration purposes (i.e. service accounts). These accounts shall not belong to any privileged group. The following must be done:

- remove those accounts from privileged groups;
- grant these accounts the required rights delegations for proper operation;
- document a specific password change procedure;
- remove the DONT_EXPIRE flag.

UNUSED ACCOUNTS

Unused accounts should be disabled. The following procedure provides similar benefits than deletion, while retaining information relevant to audit traces. To properly disable an account:

- disable the account;
- remove all of its group memberships;
- randomly change its password. To enforce a random password, one can check the *smart card is required for interactive logon* flag in the account properties. This is equivalent to manually setting the ADS_UF_SMARTCARD_REQUIRED flag of its `userAccountControl` attribute;
- optionally, move the account to a dedicated OU;
- optionally, update the account description field to mention the context for disabling (date, reason, etc.).

1 DOMAIN CONTROLLERS WITH PASSWORDS UNCHANGED FOR MORE THAN 45 DAYS

FR EN

ID : `vuln1_password_change_dc_no_change`

DESCRIPTION

Some domain controllers have not changed their password for more than 45 days, indicating their secrets are not renewed.

RECOMMENDATIONS

Default domain controller settings have them change their passwords automatically every 30 days. The reason for this change not to occur properly must be investigated as it may be indicative of a compromise.

First, check the following registry values:

- `HKLM\System\CurrentControlSet\Services\Netlogon\Parameters\DisablePasswordChange`: must be set to 0 or inexistent;
- `HKLM\System\CurrentControlSet\Services\Netlogon\Parameters\MaximumPasswordAge`: must be set to 30.

Incorrect values should be reset to their default setting, and GPOs must be checked ot ensure they do not override those.

1 INACTIVE DOMAIN CONTROLLERS

FR EN

ID : `vuln1_password_change_inactive_dc`

DESCRIPTION

Some domain controllers have not authenticated themselves for more than 45 days.

RECOMMENDATIONS

Domain controller must authenticate and change their passwords at least every 30 days.

Lack of domain authentication reveals out-of-sync machines. Out-of-sync domain controllers must be either reinstalled or removed. When reinstalling an out-of-sync domain controller, care must be taken not to introduce a new OWNER control path exposing its computer account. To avoid doing so, use of the Djoin utility is advised.

1 DANGEROUS CONTROL PATHS EXPOSE CERTIFICATE CONTAINERS

FR EN

ID : `vuln1_adcs_control`

DESCRIPTION

Dangerous control paths expose certificate containers. These control paths allow adding a malicious certificate authority, which allow an attacker to autheticate as arbitrary users or services.

RECOMMENDATIONS

A user installing a Microsoft PKI server will have these permissions automatically delegated to these containers.

Dangerous permissions on these containers should be removed to revert them to a default state. Fixing usually requires using `adsiedit.msc` or the `ldp` utility.

1 2 DANGEROUS CONTROL PATHS EXPOSE CERTIFICATE TEMPLATES

FR EN

ID : `vuln1_adcs_template_control vuln2_adcs_template_control`

DESCRIPTION

Dangerous control paths expose certificate templates.

Controlling certificate templates allows one to have the certificate authority issue an arbitrary certificate. It becomes possible to obtain a smartcard authentication certificate for any user, thus stealing his identity.

At level 1 only the templates published by at least one ADCS server are processed. At level 2 all templates are processed.

RECOMMENDATIONS

Dangerous permissions on these containers should be removed to revert them to a default state. Fixing usually requires using `adsiedit.msc`, `pkiview.msc` or the `ldp` utility.

1 ACCOUNTS WITH PRIMARYGROUPID LOWER THAN 1000

FR EN

ID : `vuln1_primary_group_id_1000`

DESCRIPTION

Some users or computers have a `primaryGroupId` attribute lower than 1000. `primaryGroupId` values lower than 1000 are usually privileged.

RECOMMENDATIONS

The `primaryGroupId` attribute of a user or computer account grants implicit membership to a group. Membership through this attribute does not appear in the list of group members in some interfaces. This attribute may be used as an attempt to hide group membership.

Reset the `primaryGroupId` attributes of users and computers to their default values:

- user accounts: 513 (Domain Users) or 514 (Domain Guests);
- computer accounts: 515 (Domain Computers);
- domain controller accounts: 516 (Domain Controllers);
- read-only domain controller (RODC) accounts : 521 (Read-only Domain Controllers).

1 2 3 WEAK OR VULNERABLE CERTIFICATES

FR EN

ID : `vuln1_certificates_vuln vuln2_certificates_vuln vuln3_certificates_vuln`

DESCRIPTION

Some certificates are problematic and must not be used anymore. This vulnerability might appear on levels 1, 2 and 3 depending on the following issues:

- 1 Use of DSA algorithm: *Digital Signature Algorithm* (DSA), is a NIST standard signature algorithm, part of the 1993 *Digital Signature Standard*(FIPS 186). The proposed FIPS 186-5 draft deprecates the use of DSA and will forbid its usage for digital signature purposes;
- 1 Very weak RSA key length (< 1024): using a modulus shorter than 1024 bits is considered insufficient to provide any meaningful security;
- 1 Key vulnerable to the ROCA vulnerability: this allows recovering the private key associated with a public key;
- 2 Certificate impossible to parse: this suggests the stored certificate is either stored in an invalid format and probably unused;
- 3 Weak RSA key length (< 2048): the French General Security Regulation (RGS) mandates a minimum key size of 2048 bits for cryptographic usage before 2030, and 3072 bits for usage after 2030;
- 3 Weak signature algorithm (not SHA2 or SHA3): algorithms such as MD5 or SHA1 are vulnerable to collision attacks;
- 3 Weak RSA exponent (< 65537): RSA encryption and decryption operations involve two other parameters than a modulus: a public exponent and a secret exponent. The French General Security Regulation (RGS) mandates usage of public exponents greater than 65536.

RECOMMENDATIONS

CASE 1: VALID, NON-EXPIRED CERTIFICATION AUTHORITIES

Problematic certificates must be revoked and re-issued. Children certificates must also be re-issued. Expired certificates should also be purged from trusted certificate stores.

When issuing a new certificate, the following requirements should be met:

- DSA algorithm is not used for certificate signature (RSA or ECDSA should be preferred);
- RSA key length is greater or equal to 2048 bits and public exponents are greater than 65536;
- an up-to-date library is used to generate the RSA key (to prevent currently known weaknesses, such as ROCA).

CASE 2: EXPIRED CERTIFICATION AUTHORITIES

If the certificate is expired, it should be purged from the trusted authorities list of the Active Directory. For binary code signature usage, the certificate authority can be re-deployed locally through GPO management.

1 DNSADMINS GROUP MEMBERS

FR EN

ID : `vuln1_dnsadmins`

DESCRIPTION

The `DnsAdmins` group includes some member accounts.

Members of the `DnsAdmins` group are granted access rights to manage a Microsoft DNS service. One of these rights allows the user to make the DNS service run arbitrary code, when this service is often hosted on domain controllers. This would allow a trivial privilege escalation to Domain Admins.

RECOMMENDATIONS

The `DnsAdmins` must not be used: manual DNS zone delegations must be used instead to manage the service (zone creation/deletion, record management, ...). These delegations are usually granted through the `ldp` utility. This is a two-step process:

STEP 1: ALLOW ACCESS TO RPC USED BY DNS MANAGEMENT MMC SNAP-INS

In the domain naming context, under the `CN=System` container, set the following access rights on the `CN=MicrosoftDNS` container:

FR EN

☑ Propriété de lecture	☐ Propriété d'écriture	☐ Créer un enfant	☐ Contrôler l'accès
☑ Liste	☐ DACL d'écriture	☐ Supprimer un enfant	☐ Écriture étendue
☑ Afficher la liste pour l'objet	☐ Accès en écriture au propriétaire	☐ Supprimer	
☑ Autorisations de lecture	☐ Écrire la liste SACL	☐ Supprimer l'arborescence	

STEP 2: ALLOW DNS ZONE MODIFICATIONS

In the `DC=DomainDnsZones` naming context, on every zone you wish to delegate management, enable inheritance and set the following access rights on the `CN=MicrosoftDNS` container:

FR EN

☑ Propriété de lecture	☐ Propriété d'écriture	☑ Créer un enfant	☐ Contrôler l'accès
☑ Liste	☐ DACL d'écriture	☑ Supprimer un enfant	☐ Écriture étendue
☑ Afficher la liste pour l'objet	☐ Accès en écriture au propriétaire	☑ Supprimer	
☑ Autorisations de lecture	☐ Écrire la liste SACL	☑ Supprimer l'arborescence	

Note: to change the current *naming context* in `ldp`, go to `View`,`Tree` and use the drop-down list to select `DomainDnsZones`.

Additionally, the following operations must be carried out on the `DnsAdmins`group:

- empty it of all its members;
- make sure the group is owned by Domain Admins;
- add an Access Control Entry forbidding Everyone to change its owner, change its access rights, and write its list of members.

If special permissions are required, delegated groups or accounts should be considered as privileged. Therefore, they must comply with appropriate protection measures, and their own access control list should be at least as strict as that of the `adminSDHolder` object. "Secure" ACLs should therefore be implemented on these delegated groups, which will not open a new control path exposure. To remove inheritance and restrict ACEs, the following command may be used: `Set-ADSyncRestrictedPermissions` found in the `AdSyncConfig.psm1` module from Azure AD Connect.

Example: applying "secure" permission on a privileged account through `Set-ADSyncRestrictedPermissions`:

```
Import-Module .\AdSyncConfig.psm1
$credential = Get-Credential
Set-ADSyncRestrictedPermissions -ADConnectorAccountDN "CN=PRIVACCOUNT,CN=Users,DC=exemple,DC=ads" -
Credential $credential
```

Note: the `AdSyncConfig.psm1` module may be extracted from the Azure AD Connect installer with `msiexec`: `msiexec /a "AzureADConnect.msi" /qb TARGETDIR=c:\temp\`

The installation package may be downloaded from https://go.microsoft.com/fwlink/?LinkId=615771.

[1] [3] MISCONFIGURED DNS ZONES

FR EN

ID : `vuln1_dnszone_bad_prop vuln3_dnszone_bad_prop`

DESCRIPTION

Some DNS zones are misconfigured:

For instance, a value of [ZONE_UPDATE_UNSECURE] (for the `DSPROPERTY_ZONE_ALLOW_UPDATE` attribute) allows updating a DNS record anonymously. An attacker could leverage this vulnerability to:

- arbitrarily add a new DNS record;
- replace an existing record to spoof a management interface, then wait for incoming connections in order to steal credentials.

Note: at level [1] only local domain zones and `_msdcs` zones are checked; at level [3] all zones are checked.

RECOMMENDATIONS

If the `DSPROPERTY_ZONE_ALLOW_UPDATE` property is set to [ZONE_UPDATE_UNSECURE], reconfigure DNS zones to only allow secure updates, using the following command:

```
dnscmd <servername> /Config <zone> /AllowUpdate 2
```

[1] [2] DANGEROUS DSHEURISTICS SETTINGS

FR EN

ID : `vuln1_dsheuristics_bad vuln2_dsheuristics_bad`

DESCRIPTION

Dangerous values are set for the `dSHeuristics` attribute. Depending on severity, this issue can be raised at levels [1] or [2]:

- [1] if `fAllowAnonNSPI` differs from 0 ;
- [1] if `dwAdminSDExMask` differs from 0 ;
- [2] if `fLDAPBlockAnonOps` equals 2 .

The following values are set in the `dSHeuristics` attribute:

RECOMMENDATIONS

The `dSHeuristics` attribute defines some heuristics later used to alter some Active Directory mechanisms. For instance:

- `fLDAPBlockAnonOps` enables unauthenticated LDAP operations;
- `fAllowAnonNSPI` controls anonymous access to the Name Service Provider Interface (NSPI).
- `dwAdminSDExMask` defines which groups are covered by the SDProp mechanism.

These dangerous `dSHeuristics` settings must be reset to their default value.

- `fLDAPBlockAnonOps` should not be set or should have any value other than 2;
- `fAllowAnonNSPI` should be set to 0;
- `dwAdminSDExMask` should be set to 0.

The fix is usually applied through the `adsiedit.msc` or `ldp` utilities.

[1] UNFILTERED OUTBOUND DOMAIN TRUST RELATIONSHIP

FR EN

ID : `vuln1_trusts_domain_notfiltered`

DESCRIPTION

Some domains in the forest are currently trusting a third-party domain without quarantine.

An attacker having compromised the remote domain can spoof any user or machine on the local domain (except for accounts with a RID lower than 1000, excluding built-in accounts and groups). This attacker can therefore access every resource on the local domain. If a dangerous control path is exposed to any "spoofable" account (virtually any account other than the built-in ones), the attacker could also escalate his privileges up to "Domain Admins" and compromise the entire forest.

RECOMMENDATIONS

[Windows 2003] introduces the ability to quarantine a trusted external domain (also called "filtering"). This prevents any user from the trusted domain from spoofing a user of another. Each relevant trust relationship must have this feature enabled individually. This can be done by issuing the following command:`netdom trust <local domain> /domain:`

`<external trusted domain> /Quarantine:yes`.

Setting up outbound trust relationships to lower trust level domains is strongly discouraged.

Note: each trust relationship type is defined by flags set within some of their LDAP attributes. This issue focuses on relationships lacking the `WITHIN_FOREST` flag. In some cases, particularly with legacy / old forests, internal trust relationships may not bear the `WITHIN_FOREST` flag. Should this occur the various flags must be manually set on all relevant relationships.

1 OUTBOUND FOREST TRUST RELATIONSHIPS WITH SID HISTORY ENABLED

FR EN

ID : `vuln1_trusts_forest_sidhistory`

DESCRIPTION

The forest currently trusts an external forest with diminished filtering.

An attacker having compromised the remote domain can spoof any user or machine on the local domain (except for accounts with a RID lower than 1000, excluding built-in accounts and groups). This attacker can therefore access every resource on the local domain. If a dangerous control path is exposed to any "spoofable" account (virtually any account other than the built-in ones), the attacker could also escalate his privileges up to "Domain Admins" and compromise the entire forest.

RECOMMENDATIONS

Any outbound trust extends the trusting forest security boundary to include a third-party forest. By default, forest trusts are filtered. However, it is possible to relax these restrictions, and enable the `sIDHistory` mechanism. In that case, the trusting forest is endangered by the trusted forest.

The rationale behind the current configuration (`TREAT_AS_EXTERNAL`) should first be clarified. It might be set for an ongoing migration which requires the `sIDHistory` mechanism. Otherwise, filtering should be restored to its defaults through the command: `netdom trust <forest> /domain:<other trusted forest> /EnableSIDHistory:no`.

1 DORMANT ACCOUNTS

FR EN

ID : `vuln1_user_accounts_dormant`

DESCRIPTION

More than 25% of forest accounts are dormant. This type of user or computer accounts are not disabled, and did not authenticate against the Active Directory for more than a year. Dormant accounts are either legitimate accounts which are rarely used, or obsolete accounts.

Obsolete accounts grant users illegitimate accesses (e.g. after they left the company) or be stealthily used by attackers, which is even more problematic if the accounts are privileged. Their mere existence also makes user and access rights accountability much harder.

RECOMMENDATIONS

Without an account management policy, obsolete accounts can remain for extended periods of time in the domain. This can be due to a person leaving the company or changing roles, or an application or computer being retired.

Dormant accounts have had no activity in the domain in the past year. Obsolete accounts are dormant accounts which do not have a purpose anymore.

Obsolete accounts (computer, user, administrator, or service alike) must be disabled, or even deleted.

Two criteria can help enumerate dormant accounts in a domain:

- accounts whose password expires and whose last password change date is older than a year (the `pwdLastSet` attribute);
- accounts which have not authenticated to the domain for more than a year (the `LastLogonTimestamp` attribute). Beware this attribute is only updated if the domain functional level is `Windows 2003` or more.

Obsolete accounts must be distinguished from other dormant accounts. As a matter of fact, part of the accounts in the list can be legitimate dormant accounts (for instance, accounts used in case of emergency) or used to create Exchange mailboxes read through access delegations. Such functional Exchange accounts should be disabled and put in a dedicated OU.

Unused accounts should be disabled. The following procedure provides similar benefits than deletion, while retaining information relevant to audit traces. To properly disable an account:

- disable the account;
- remove all of its group memberships;
- randomly change its password. To enforce a random password, one can check the *smart card is required for interactive logon* flag in the account properties. This is equivalent to manually setting the `ADS_UF_SMARTCARD_REQUIRED` flag of its`userAccountControl` attribute;
- optionally, move the account to a dedicated OU;
- optionally, update the account description field to mention the context for disabling (date, reason, etc.).

2 PRIVILEGED GROUP MEMBERS WITH WEAK PASSWORD POLICY

FR EN

ID : `vuln2_privileged_members_password`

DESCRIPTION

Some privileged accounts have a weak password policy enforced.

RECOMMENDATIONS

For privileged accounts, enforcing a password policy with the following requirements is recommended:

- forced change at most every 3 years
- length of 8 or more characters

Important note: passwords should not be renewed too often. Enforcing short password lifespans compells users to choose statistically weaker passwords, which negates the intended benefits.

2 UNCONSTRAINED AUTHENTICATION DELEGATION

FR EN

ID : `vuln2_delegation_t4d`

DESCRIPTION

Some accounts in the forest have been granted unconstrained authentication delegations. This grants them the ability to act as any user that will authenticate against them.

RECOMMENDATIONS

Unconstrained authentication delegation allows an account to authenticate to any Kerberos service acting on behalf of any user who has tried to authenticate to that account. It allows that account to elevate privileges and compromise the forest. By default, unconstrained authentication delegation is only granted to domain controllers, and must not be granted to any other account.

For all of the accounts listed above, remove the `TRUSTED_FOR_DELEGATION` flag in their `userAccountControl` attribute. This can be performed through the "Delegation" tab of the Active directory Users and Computers management console. If a Kerberos delegation really is required, use a constrained one.

2 KERBEROS PRE-AUTHENTICATION DISABLED

FR EN

ID : `vuln2_kerberos_properties_preauth`

DESCRIPTION

Some accounts have Kerberos pre-authentication disabled. Without pre-authentication, it is possible to acquire a ticket encrypted with one of the Kerberos keys associated with the requested account. It is then possible to carry out a brute-force or dictionary guessing attack to crack an account password, if it is not strong enough.

RECOMMENDATIONS

Kerberos pre-authentication ensures that users requesting a Ticket Granting Ticket (TGT) know a given authentication secret. By default, all user accounts require pre-authentication because their `DONT_REQUIRE_PREAUTH` property is not set. That property was designed for backward compatibility with older Kerberos implementations.

GENERAL CASE

The `DONT_REQUIRE_PREAUTH` property must be removed from these accounts. If an application is not compatible with this change, it must be upgraded.

SPECIFIC CASES

Any incompatible software must be upgraded. This issue can be mitigated as follows:

- defining a refined password policy through *Password Settings Objects* (PSO), enforcing a minimum password length of **32** characters;
- defining a refined password policy through *Password Settings Objects* (PSO), enforcing a maximum expiration duration of **3 years**;
- changing the affected user passwords after modifying the PSO settings;
- enforcing AES usage for the affected account.

2 USE OF KERBEROS WITH WEAK ENCRYPTION

FR EN

ID : `vuln2_kerberos_properties_deskey`

DESCRIPTION

The `USE_DES_KEY_ONLY` flag is set for some users. This flag allows domain controllers to issue Kerberos tickets encrypted with the DES algorithm. This property was designed for backward compatibility with older Kerberos implementations. The DES algorithm is considered weak and must not be used anymore. This flag weakens the security of distributed Kerberos tickets significantly, and speeds up bruteforce cracking attempts.

RECOMMENDATIONS

Default operating system support of cipher groups is as follows:

- Windows XP and Windows Server 2003: DES and RC4;
- Windows Vista and Windows Server 2008: DES, RC4 and AES;

- Windows 7, Windows Server 2008 R2 and later: RC4 and AES. DES is still supported but disabled by default.

The USE_DES_KEY_ONLY flag must be unset from `userAccountControl` attribute of each affected account. This can be performed by unchecking the "Use Kerberos DES encryption types for this account" options in the user account properties.

Any incompatible software must be upgraded.

2 ACCOUNTS WITH NEVER-EXPIRING PASSWORDS

FR EN

ID : `vuln2_dont_expire`

DESCRIPTION

Some accounts have passwords which never expire. Should an attacker compromise one of these accounts, he would be able to maintain long-term access to the Active Directory domain.

RECOMMENDATIONS

GENERAL CASE

In order to make Active Directory enforce periodic password change, accounts must not have the DONT_EXPIRE flag set. This account flag should then be unset, usually by unchecking the "password never expires" option in the "Account" tab of the user properties. Their passwords should then be rolled immediately.

SERVICE ACCOUNTS

In order to be able to change passwords of service accounts and trace their usage, it is required to document how they are used. Thus, a list of all service accounts and their use must be kept up to date. It must include, for each service account:

- all information about the account (`samAccountName`, description, AD group membership, specificities, etc.);
- applications or systems using that account;
- the last time its password was changed;
- a procedure to change its password;
- a person or a team responsible for its lifecycle.

2 SERVERS WITH PASSWORDS UNCHANGED FOR MORE THAN 90 DAYS

FR EN

ID : `vuln2_password_change_server_no_change_90`

DESCRIPTION

Some servers have not changed their passwords for more than 90 days, indicating their secrets are not renewed.

RECOMMENDATIONS

Default server settings have them change their passwords automatically every 30 days. The reason for this change not to occur properly must be investigated as it may be indicative of a compromise.

First, check the following registry values:

- `HKLM\System\CurrentControlSet\Services\Netlogon\Parameters\DisablePasswordChange`: must be set to 0 or inexistent;
- `HKLM\System\CurrentControlSet\Services\Netlogon\Parameters\MaximumPasswordAge`: must be set to 30.

Incorrect values should be reset to their default setting, and GPOs must be checked ot ensure they do not override those.

2 SYSVOL REPLICATION THROUGH NTFRS

FR EN

ID : `vuln2_sysvol_ntfrs`

DESCRIPTION

Some domain controllers are configured to use the NTFRS protocol to replicate the SYSVOL file share. This protocol is obsolete, and exposes unnecessary additional administration interfaces to domain controllers. Furthermore, latest Windows Server versions have dropped support of NTFRS altogether, blocking upgrades for existing infrastructures pending migration to DFSR.

RECOMMENDATIONS

Distributed File System Replication (DFSR) should be used for share replication, including SYSVOL replication.

Note: support for NTFRS has been dropped in latest Windows Server versions. Migration to DSFR is documented at the URL below: https://docs.microsoft.com/en-us/windows-server/storage/dfs-replication/migrate-sysvol-to-dfsr.

2 BAD ACTIVE DIRECTORY VERSIONS

FR EN

ID : `vuln2_adupdate_bad`

DESCRIPTION

The current schema update is at revision 15. This specific update mistakenly introduces a control path exposing the Active Directory to full takeover by some builtin user groups.

RECOMMENDATIONS

The schema update with revision 15 is problematic. It sets overly permissive Access Control Entries (ACEs) on groups `Key Admins`and `Enterprise Key Admins`. The schema update provided by Windows Server version 1709 (and later) fixes this issue.

This operation is usually performed with the `adprep` utility, found on any up-to-date Windows Server installation media. The following commands are used to update the Active Directory schema: `adprep /ForestPrep` followed by `adprep /DomainPrep`.
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd464018(v=ws.10)

---

2 THE "PRE-WINDOWS 2000 COMPATIBLE ACCESS" GROUP INCLUDES "ANONYMOUS"

FR EN

ID : `vuln2_compatible_2000_anonymous`

DESCRIPTION

The pre-Windows 2000 compatibility mechanism ensures Windows NT domains are still supported. It is enabled by adding the `Anonymous` SID (`S-1-5-7`) to the `Pre-Windows 2000 Compatible Access` group, which allows anonymous access to some of Active Directory contents on domain controllers.

RECOMMENDATIONS

The `Pre-Windows 2000 Compatible Access` group used to serve backward compatibility purposes for systems prior to Windows 2000 (Windows NT 4.0). This group must only include`Authenticated Users` (`S-1-5-11`).

---

2 KRBTGT ACCOUNT PASSWORD UNCHANGED FOR MORE THAN A YEAR

FR EN

ID : `vuln2_krbtgt`

DESCRIPTION

The `krbtgt` account password has not been changed for more than a year.

The `krbtgt` Kerberos infrastructure account in all Active Directory domains is used as a support for key storage in all Kerberos Key Distribution Centers (KDC).

Taking over a `krbtgt` account allows an attacker to forge Kerberos tickets of *Ticket Granting Ticket* (TGT) type (so-called *golden tickets*), then authenticate to any resource (server, workstation, etc.) in the domain with full administrative privileges in a more or less stealth manner.

The `krbtgt` account does not change its password automatically, so if the account database was extracted (for instance, by a former administrator, during an audit, or for a password strength assessment), it is possible to use information from that database to extract the `krbtgt` secrets. A malicious user can then compromise all Active Directory services many years after the information was extracted.

RECOMMENDATIONS

The `krbtgt` Kerberos infrastructure account in all Active Directory domains is used as a support for key storage in all Kerberos Key Distribution Centers (KDC). In order to renew Kerberos keys used ot encrypt TGTs, the `krbtgt` account must have its password manually changed periodically. Using the Microsoft-provided script is recommended. For the script to work properly on computers configured with the french locale, the following changes must be applied:

- line 62: replace `"*completed*"` by `"*effectués*"` ;
- line 84: replace `"*Successfully replicated object*"` by `"*a été correctement répliqué*"`.

The password change must be carried out twice in a row to effectively prevent fraudulent usage of previous passwords (the current and previous passwords are both valid at any one time).

Warning: any password change operation for the `krbtgt` account must be carried out in an Active Directory environment with working, healthy domain controller replication. A sufficient delay must be observed between the two consecutive password changes for the values to be replicated to all domain controllers.

The `krbtgt` can be manually rolled, the same way one can force change of a user password. If the provided script is not used, a delay of 24 hours should be observed between the two consecutive password changes as well as ensuring replication is properly working between all domain controllers. An alternative strategy could be rolling this password only once every 6 months, thus ensuring proper revocation of all previous passwords every year.

---

2 PRIVILEGED USERS REVEALED ON RODC

FR EN

ID : `vuln2_rodc_priv_revealed`

DESCRIPTION

Some privileged accounts have been revealed on some RODCs, which means their authentication secrets are cached there. If those RODCs are compromised (they are usually more exposed than regular DCs), the full domain may be at risk.

RECOMMENDATIONS

RODCs cache some domain authentication secrets. Members of privileged groups are not revealed (i.e. cached) on RODCs by default. This helps restrict malicious access only to accounts which are revealed. Privileged users should not be revealed on RODCs to prevent compromise.

RODCs must therefore include the following objects in their `msDS-NeverRevealGroup` attribute:

- « Administrators » ;
- « Domain Admins » ;
- « Account Operators » ;
- « Server Operators » ;
- « Backup Operators » ;
- « Denied RODC Password Replication Group ».

This can be done through the "Password Replication Policy" tab of each RODC computer account properties window.

2 ACCOUNTS OR GROUPS WITH UNEXPECTED SID HISTORY

FR EN

ID : `vuln2_sidhistory_dangerous`

DESCRIPTION

Several accounts or groups in the forest have unexpected `sIDHistory`attribute values (either a well-known SID or a domain-level privileged SID). This can be exploited by an attacker to grant themselves illegitimate access rights.

RECOMMENDATIONS

The `sIDHistory` attribute allows appending an additional security identifier (SID) in their group list. This mechanism is mainly used during migrations from one domain to another, to keep access to previous resources.

An investigation into the reasons for these unexpected SIDs being granted to users should be carried out. The `sIDHistory` attribute must then be erased for all the aforementioned users and computers.

2 TRUST ACCOUNT PASSWORDS UNCHANGED FOR MORE THAN A YEAR

FR EN

ID : `vuln2_trusts_accounts`

DESCRIPTION

Trust account passwords have not been changed for more than a year. This may be indicative of deleted trust relationships while their corresponding trust accounts are still present.

RECOMMENDATIONS

DELETED TRUST RELATIONSHIP

Some *trust* accounts may remain while their *trust* relationships have been removed. They should be deleted manually.

ACTIVE TRUST RELATIONSHIP

Trust passwords should be changed at least once a year. That change must be automatic for *trust* relathionships between Microsoft environments. The cause for the lack of automatic renewal should be investigated.

3 SERVERS WITH PASSWORDS UNCHANGED FOR MORE THAN 45 DAYS

FR EN

ID : `vuln3_password_change_server_no_change_45`

DESCRIPTION

Some servers have not changed their passwords for more than 45 days, indicating their secrets are not renewed.

RECOMMENDATIONS

Default server settings have them change their passwords automatically every 30 days. The reason for this change not to occur properly must be investigated as it may be indicative of a compromise.

First, check the following registry values:

- `HKLM\System\CurrentControlSet\Services\Netlogon\Parameters\DisablePasswordChange`: must be set to 0 or inexistent;
- `HKLM\System\CurrentControlSet\Services\Netlogon\Parameters\MaximumPasswordAge`: must be set to 30.

Incorrect values should be reset to their default setting, and GPOs must be checked ot ensure they do not override those.

3 INACTIVE SERVERS

FR EN

ID : `vuln3_password_change_inactive_servers`

DESCRIPTION

Some servers have not authenticated themselves for more than 90 days.

RECOMMENDATIONS

Servers must authenticate and change their passwords at least every 30 days.

Lack of domain authentication reveals out-of-sync machines. Out-of-sync servers must be either reinstalled or removed. When reinstalling an out-of-sync server, care must be taken not to introduce a new OWNER control path exposing its computer account. To avoid doing so, use of the Djoin utility is advised.

3 ACCOUNTS WITH MODIFIED PRIMARYGROUPID

FR EN

ID : `vuln3_primary_group_id_nochange`

DESCRIPTION

Some users or computers have a modified `primaryGroupId` attribute.

RECOMMENDATIONS

The `primaryGroupId` attribute of a user or computer account grants implicit membership to a group. Membership through this attribute does not appear in the list of group members in some interfaces. This attribute may be used as an attempt to hide group membership.

Reset the `primaryGroupId` attributes of users and computers to their default values:

- user accounts: 513 (Domain Users) or 514 (Domain Guests);
- computer accounts: 515 (Domain Computers);
- domain controller accounts: 516 (Domain Controllers);
- read-only domain controller (RODC) accounts : 521 (Read-only Domain Controllers).

3 USE OF THE "PRE-WINDOWS 2000 COMPATIBLE ACCESS" GROUP

FR EN

ID : `vuln3_compatible_2000_not_default`

DESCRIPTION

The *Pre-Windows 2000 Compatible Access* group contains additional identifiers to the default ones. This grants these group members access to some RPC calls. Specific system parameters may have the Everyone group include anonymous users, which may increase risk if it belongs to the *Pre-Windows 2000 Compatible Access* group.

RECOMMENDATIONS

The `Pre-Windows 2000 Compatible Access` group used to serve backward compatibility purposes for systems prior to Windows 2000 (Windows NT 4.0). This group must only include`Authenticated Users` (`S-1-5-11`).
Note: ADCS servers are automatically added to this group upon installation. They can be removed in most instances as it is likely not useful. This operation is easily reversible.

3 INCORRECT OBJECT OWNERS

FR EN

ID : `vuln3_owner`

DESCRIPTION

Some objects have non-standard owners. Note: Only the first 20 objects are shown.

RECOMMENDATIONS

All objects (users, groups, sMSA, gMSA, computers, OU, GPO) must be owned by one of the following objects:

- « Domain Admins » ;
- « Enterprise Admins » ;
- « Administrators » ;
- « Local System ».

3 PRIVILEGED ACCOUNTS OUTSIDE OF THE PROTECTED USERS GROUP

FR EN

ID : `vuln3_protected_users`

DESCRIPTION

Some privileged accounts are not protected by the `Protected Users` group.

RECOMMENDATIONS

Privileged users must be members of the `Protected Users` group so as to:

- enforce Kerberos authentication;
- reduce Kerberos ticket lifetime;

- enforce usage of strong encryption algorithms (AES);
- prevent caching of passwords on workstations;
- prevent any type of Kerberos delegation.

Warning : use of the `Protected Users` group comes with significant functional impacts.
Reference : https://docs.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/protected-users-security-group.

3 ACCOUNTS WITH PASSWORDS STORED USING REVERSIBLE ENCRYPTION FR EN

ID : `vuln3_reversible_password`

DESCRIPTION

Some accounts have their passwords stored in Active Directory using reversible encryption.

With administrator privileges, it becomes possible to retrieve cleartext passwords of all affected accounts.

RECOMMENDATIONS

To avoid common downward spirals in password management, it is important to remove dangerous properties regarding user account passwords (*Active Directory Users and computers* console):*reversible password storage* (`ENCRYPTED_TEXT_PASSWORD_ALLOWED` flag in the `userAccountControl` attribute). The checkbox *Store password using reversible encryption* must be left unchecked in the *Account* tab of each account properties.
If these settings have a legitimate use, it should be documented, for instance in the account description attribute.

3 DANGEROUS CONFIGURATION OF READ-ONLY DOMAIN CONTROLLERS (RODC) (NEVERREVEAL) FR EN

ID : `vuln3_rodc_never_reveal`

DESCRIPTION

Read-only domain controllers (RODCs) are used in the forest with dangerous secret revelation settings. Some default groups are missing from the `msDS-NeverRevealGroup` attribute of some RODCs.

RECOMMENDATIONS

The `msDS-NeverRevealGroup` attribute can be used to list objects whose secrets are prevented from being revealed on a RODC (these objects are recursively parsed).

Read-only domain controllers must have their `msDS-NeverRevealGroup`attribute set to include, at least:

- Administrators;
- Server Operators;
- Account Operators;
- Backup Operators;
- Denied RODC Password Replication Group.

3 DANGEROUS CONFIGURATION OF READ-ONLY DOMAIN CONTROLLERS (RODC) (REVEAL) FR EN

ID : `vuln3_rodc_reveal`

DESCRIPTION

Read-only domain controllers (RODCs) are used in the forest with dangerous secret revelation settings. Some privileged groups or users are included in the `msDS-RevealOnDemandGroup` attribute of some RODC.

RECOMMENDATIONS

The `msDS-RevealOnDemandGroup` attribute defines users and groups allowed to be revealed on a RODC.

Read-only domain controllers must not have groups in their `msDS-RevealOnDemandGroup` attribute whose RID is lower than 1000.

3 DANGEROUS CONFIGURATION OF REPLICATION GROUPS FOR READ-ONLY DOMAIN CONTROLLE (RODCS) (ALLOW) FR EN

ID : `vuln3_rodc_allowed_group`

DESCRIPTION

The `Allowed RODC Password Replication Group` group is not empty.

RECOMMENDATIONS

Accounts belonging to the Allowed RODC Password Replication Group group have their password hashes revealed on all RODCs.

This group should be emptied, and dedicated groups should only be added to the*Password Replication Policy* of each relevant RODC.

3 DANGEROUS CONFIGURATION OF REPLICATION GROUPS FOR READ-ONLY DOMAIN CONTROLLE FR EN (RODCS) (DENIED)

ID : `vuln3_rodc_denied_group`

DESCRIPTION

Some default groups are missing from the Denied RODC Password Replication Group.

RECOMMENDATIONS

The Denied RODC Password Replication Group must include the following members:

- Domain Controllers ;
- Read-only Domain Controllers ;
- Group Policy Creator Owners ;
- Domain Admins ;
- Cert Publishers ;
- Enterprise Admins ;
- Schema Admins ;
- KRBTGT.

3 ACCOUNTS OR GROUPS WITH SID HISTORY SET FR EN

ID : `vuln3_sidhistory_present`

DESCRIPTION

Several accounts or groups in the forest have their `sIDHistory`attribute set.

Whenever set, the `sIDHistory` attribute causes Windows event IDs 4665 et 4666 to be generated uselessly, which can make log monitoring more difficult. Moreover, its legitimate use weakens the security of Kerberos trusts.

RECOMMENDATIONS

The `sIDHistory` attribute allows appending an additional security identifier (SID) in their group list. This mechanism is mainly used during migrations from one domain to another, to keep access to previous resources. It can also be exploited by attackers to grant themselves illegitimate access rights.

The `sIDHistory` attribute must be erased for all accounts and groups aforementioned, as soon as domain migrations are completed.

3 INBOUND TRUST RELATIONSHIPS WITH DELEGATION FR EN

ID : `vuln3_trusts_tgt_deleg`

DESCRIPTION

Some trust relationships currently allow Kerberos delegation. By design, inbound trusts allow delegating Kerberos tickets, which allows third-party resources to authenticate as the account that authenticated to them. This may lead to privilege escalation from the trusted external domain to the trusting local domain.

RECOMMENDATIONS

Inbound trust relationships allow a domain to be trusted by a third-party domain or forest. This allows accounts to use third-party resources outside their forest.

Any inbound trust must deny Kerberos delegation to the trusting resource. It is possible to disable TGT delegation with **Windows 2012** and later, through the command: `netdom trust <domain> /domain:<trusted domain> /EnableTGTDelegation:no`