

REMEDIA  
TION  
COLLECTION

# **CYBER ATTACKS AND REMEDIATION**

## REMEDIA TION OF ACTIVE DIRECTORY TIER 0



---

# CONTENTS

<b>INTRODUCTION</b>	<b>4</b>
<b>1- PURPOSE AND SCOPE OF THE DOCUMENT</b>	<b>5</b>
<b>2- DOCUMENT RECIPIENTS</b>	<b>7</b>
<b>3- LIMITS OF THE DOCUMENT</b>	<b>7</b>
<b>4- KEY CONCEPTS</b>	<b>8</b>
a - Tiered administration model	8
b - Trusted core	9
c - Privileged groups	10
d - Control path	11
e - List of Active Directory assessment items	11
<b>5- STRUCTURE OF THE DOCUMENT</b>	<b>12</b>
<b>PART I - TECHNICAL ACTIONS FOR INVESTIGATION OF ACTIVE DIRECTORY TIER 0</b>	<b>13</b>
<b>PART II - TECHNICAL ACTIONS FOR EVICTION FROM ACTIVE DIRECTORY TIER 0</b>	<b>15</b>
<b>1- INTRODUCTION</b>	<b>16</b>
<b>2- RECAP TABLE OF TECHNICAL ACTIONS FOR EVICTION FOR THE DIFFERENT SCENARIOS</b>	<b>17</b>
<b>3- ENSURE NO TIER 0 MACHINES ARE COMPROMISED</b>	<b>20</b>
a - Reinstall all domain controllers	20
b - Reinstall all Tier 0 machines	22
c - Remove dangerous control paths to domain controllers	22
d - Remove dangerous control paths to infrastructure elements with impact on Tier 0	23
e - Remove dangerous control paths to MicrosoftDNS servers	23
f - Remove delegated authentications from domain controllers	24
g - Secure Read-Only Domain Controllers (RODCs)	25

---

<b>4 - RENEW SECRETS TO PREVENT ATTACKER USE OF COMPROMISED ACCOUNTS</b>	<b>25</b>
a - Default administrator account	25
b - krbtgt account	26
c - Directory Service Restoration Mode (DSRM) administrator account	26
d - KDS keys	27
e - Secrets of trust relationships	27
f - Other secrets enabling takeover of Tier 0	27
g - Suspected compromised accounts identified during the investigation	28
<b>5 - CONFIGURE THE ACTIVE DIRECTORY WITH NO WEAKNESSES ALLOWING TAKEOVER OF TIER 0</b>	<b>28</b>
a - Increase the functional level of the forest	28
b - Harden the directory configuration	30
c - Remove dangerous control paths to the directory's privileged objects	30
d - Remove dangerous permissions on the <i>adminSDHolder</i> object	31
e - Use the DFSR protocol for SYSVOL replication	31
<b>6 - HARDEN THE DIRECTORY'S PRIVILEGED OBJECTS</b>	<b>32</b>
a - Secure privileged account attributes	32
b - Reset admincount attributes	32
<b>7 - CLEAN UP GPOs APPLICABLE TO OBJECTS</b>	<b>33</b>
a - Secure configuration for GPOs applicable to the domain root	33
b - Secure configuration for GPOs applicable to Tier 0 machines	34
c - Remove attack paths to GPOs applicable to privileged objects	34
<b>8 - ELIMINATE WEAKNESSES IN THE CONFIGURATION OF TRUST RELATIONSHIPS</b>	<b>34</b>
<b>9 - CONFIGURE PRIVILEGED SERVICES NOT CAUSING TIER 0 TO BE COMPROMISED</b>	<b>35</b>
<b>10 - ADOPT SECURE ADMINISTRATION PRACTICES</b>	<b>36</b>
a - Organisational Unit (OU) structure consistent for securing Tier 0	36
b - Use dedicated accounts for administration	37

---

c - Robust password policy for privileged accounts	37
d - Reduce the number of privileged accounts	37
e - Delete control paths to members of privileged groups	38
f - Create secure administration workstations	38
g - Apply administration practices preventing the presence of privileged account secrets in the memory of non-Tier 0 machines	39

<b>PART III - TECHNICAL ACTIONS FOR SUPERVISION OF ACTIVE DIRECTORY TIER 0</b>	<b>41</b>
<b>APPENDICES</b>	<b>44</b>

# INTRODUCTION

---

# 1 PURPOSE AND SCOPE OF THE DOCUMENT

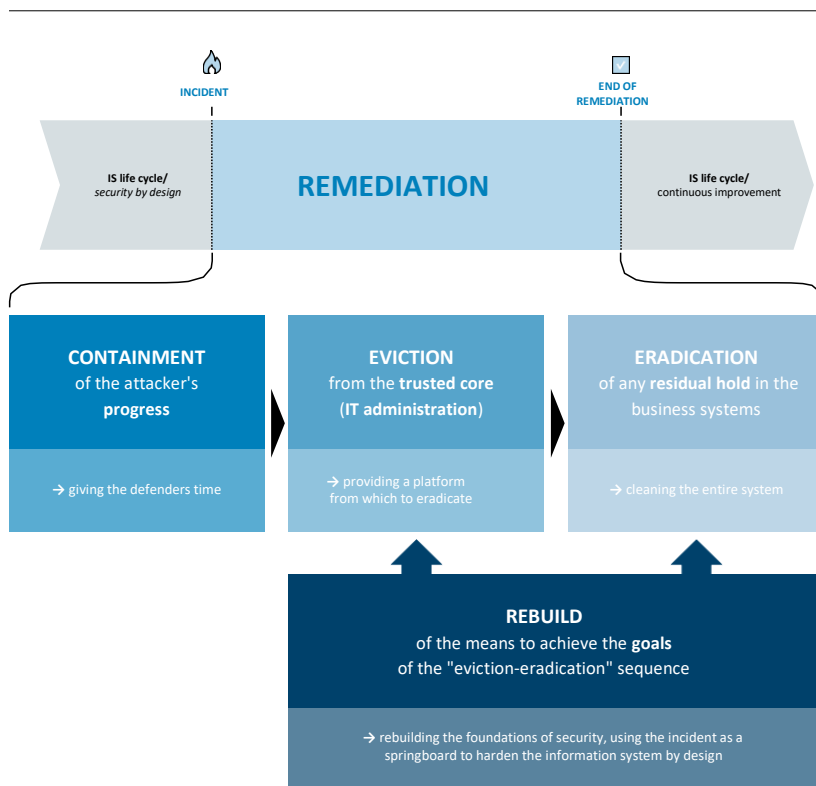
The purpose of this publication is to provide a conceptual framework for remediation operations following a major IT security breach. For the purposes of this document, remediation is taking back control of a compromised information system and restoring a sufficient level of operation.

This document is part of the technical component of the ANSSI corpus on remediation. It provides a technical base presenting the foundations of the operation to rebuild the trusted core<sup>1</sup> of the Active Directory. It is intended to assist in the progress of the remediation plan by providing a brief set of key measures to implement. As such, it is mainly intended for the technical teams in charge of implementing reconstruction operations.

Using the same terminology as the operational section of this corpus, remediation can be summarised by the sequence: containment, eviction, eradication, rebuild, known collectively as “CEER”. The remediation operations of the Active Directory's trusted core are included in the different phases of this sequence. This step is central to remediation, since it puts the defender in a position to completely eradicate the IS attacker.

---

<sup>1</sup> See the definition in chapter 4. Key concepts, b. Trusted core.



The purpose of this document is to provide a framework for remediation operations, according to the three scenarios presented in the strategic and operational components:

Scenario 1: "Restore mission-critical services as quickly as possible"

Scenario 2: "Take back control of the IS"

Scenario 3: "Seize the opportunity to pave the way for enduring IS control"



---

Depending on the chosen scenario, objectives must be defined for the safe eviction and securing of Tier 0<sup>2</sup>. These objectives can then be achieved through the technical actions presented in this document.

## **2 DOCUMENT RECIPIENTS**

This document is intended for information system and IS security managers who must steer the technical aspects of a remediation following an information system security incident.

It is also intended for those managers' contacts: administrators, consultants, service providers involved in remediation operations and carrying out the actions described in the document.

## **3 LIMITS OF THE DOCUMENT**

This document is not a step-by-step remediation procedure.

Each security incident has its own specific features: the attacker's tactics modus operandi, business imperatives, etc. The remediation roadmap must assimilate this information and use it to adapt this document's technical points of interest.

In addition, the safety and security objectives can sometimes be guaranteed using different methods. It is therefore important to work with Active Directory experts (vendor manuals, service providers, etc.) to carry out and adapt the actions described in this document, as well as to diagnose and address unforeseen events. Production requirements and the unfolding crisis must not give rise to improvised

---

<sup>2</sup> See the operational component of the corpus, *Cyber Attacks and Remediation: Steering Remediation*.

---

technical measures, which could jeopardise proper system operation to the detriment of its security.

The technical eviction actions explained in this document address the control paths most commonly used by attackers. Additional actions specific to the ongoing attack may be required to complete the eviction.

## 4 KEY CONCEPTS

### a – Tiered administration model

The tiered administration model focuses on managing unauthorised escalation of privileges in an Active Directory environment. This model, initially proposed by Microsoft, defines three administration tiers:

**Red level, or Tier 0**, or the trusted core of the Active Directory, which contains all the resources that control the company's identities and integrated resources. A process for defining the elements to be integrated in T0 is detailed in the appendix<sup>3</sup>.

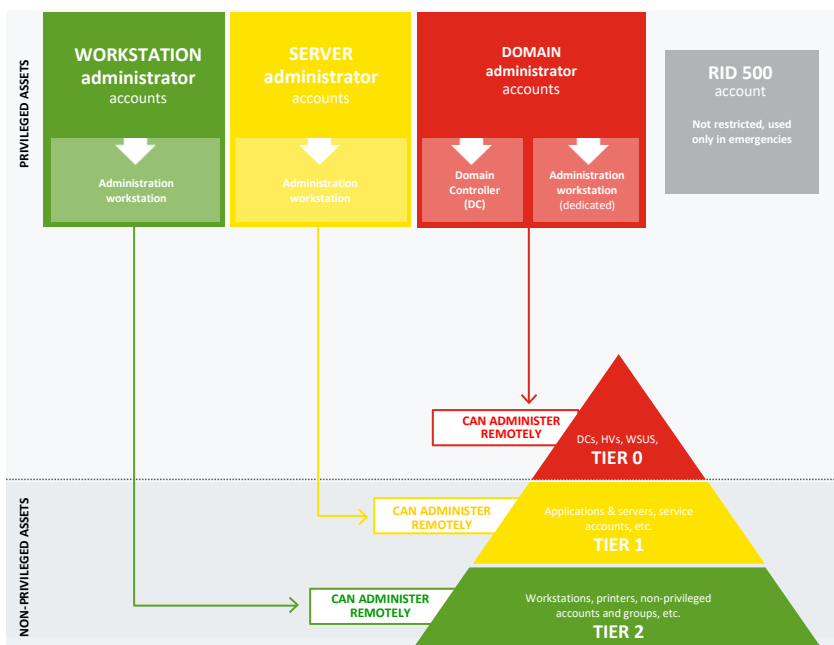
**Yellow level, or Tier 1**, which contains all resources controlling the business values, including the company's servers and applications.

**Green level, or Tier 2**, which contains all resources controlling user workstations and other devices (e.g. printers).

---

<sup>3</sup> See Appendix A. Approach for defining the scope of the Active Directory Tier 0.

*The principles of a finalised Third-Party administrator model are represented in the following figure:*



## b – Trusted core

In this document, the term “trusted core” is used to refer to the part of an IS that, if compromised by an attacker, would lead to suspect that the entire IS is compromised. The trusted core contains, among other things: identity management, virtualisation management, administration, and components providing security supervision. Secure architectures aim to minimise the size and complexity of the trusted core so as to simplify its security and reduce the risk of configuration errors. The minimalistic nature of the trusted core is particularly important in an incident, as each part may have been compromised.

---

In an Active Directory environment, the trusted core contains the authentication repository and, by extension, all Tier 0 resources as defined in the previous section<sup>4</sup>.

## c – Privileged groups

In an Active Directory environment, privileged native groups are the administration and operational groups that have maximum rights and privileges over the forest, or that can assign themselves these rights:

- “administrators”;
- “domain controllers”;
- “schema administrators”;
- “enterprise administrators”;
- “domain administrators”: these administrators have privileges to read the secrets database of all accounts and thus extract the secrets of all privileged accounts;
- “key administrators”;
- “enterprise key administrators”: these administrators can set arbitrary values to attributes relating to Windows Hello for Business, for all users except those protected by the *adminSDHolder* mechanism. If certificate-based authentication has been activated, they can generate a certificate under their control, assign it to a privileged account (e.g., a domain controller), and authenticate themselves as such;
- “account operators”: these operators can administer all user accounts, machines and groups, with the exception of accounts protected by the *adminSDHolder*;

---

<sup>4</sup> Through misuse of language, the term “trusted core” will sometimes be used in this document to refer to Tier 0 domain controllers and resources. Although part of the “trusted core”, these resources are only a subset of it with regard to the definition given in this section.

- 
- "server operators": these operators can administer the domain controllers, and therefore recover the secrets of all privileged accounts;
  - "backup operators": these operators can back up a domain controller and therefore extract the secrets of all privileged accounts from this backup;
  - "print operators": these operators can load print drivers onto domain controllers and therefore load a malicious driver to, for instance, extract the secrets of all privileged accounts.

An attacker taking control of one of these groups<sup>5</sup> could compromise the entire forest, which explains why they are a priority target in many attacks.

## d – Control path

A control path consists of a set of direct control relationships, where each relationship reflects how one entity controls another through a particular property. Thus, control paths represent the means for an attacker to reach their targets. Analysing these paths makes it possible to identify deviations in domain management, validate the application of a security perimeter around the targets considered, as well as reveal the means of persistence an attacker left behind after an intrusion.

## e – List of Active Directory assessment items

This document makes several references to the list of Active Directory assessment items, published on the CERT-FR website<sup>6</sup> to address the growing risk these environments face. This list will be updated regularly to benefit from ongoing research, practices observed during

---

<sup>5</sup> This list is not comprehensive.

<sup>6</sup> The list is available on the CERT-FR website: <https://cert.ssi.gouv.fr/dur/CERTFR-2020-DUR-001/> (English version at [https://www.cert.ssi.gouv.fr/uploads/ad\\_checklist.html](https://www.cert.ssi.gouv.fr/uploads/ad_checklist.html))

---

audits, and analyses of attackers' modus operandi.

## **5 STRUCTURE OF THE DOCUMENT**

This document has a four-part structure:

→ **"Technical actions for investigation of Active Directory Tier 0"**

- During remediation, it is necessary to make sure that key elements are not compromised.
- They must be assessed to identify on which IS resources eviction needs to be carried out.

→ **"Technical actions for eviction from Active Directory Tier 0"**

- This section proposes a set of technical objectives, according to the chosen remediation scenario. These objectives aim to overcome security weaknesses of the Active Directory that could lead to further compromise post-eviction.

→ **"Technical actions for supervision of Active Directory Tier 0"**

- At the same time as remediation, implementing appropriate supervision is key. This supervision is based on various elements presented in this section.

→ **"Appendices"**

- The appendices provide practical documents to implement the options discussed in the body of the document.

PART I

**TECHNICAL  
ACTIONS FOR  
INVESTIGATION  
OF ACTIVE  
DIRECTORY TIER 0**

The technical objectives for investigation of the Active Directory Tier 0 are to ensure that no malicious element is replicated from the compromised domain controller to the pivot domain controllers (domain controller used during remediation to allow the Active Directory to be modified in an isolated environment) and rebuilt.

The investigations are based in particular on network captures and collection of system elements on the domain controllers.

Main objectives of these analyses:

→ **At network level:**

- Ensure that no malicious script or program, user account manipulation, attempt to exploit vulnerabilities or behaviour akin to illegitimate traffic occurs during replications (between compromised controller and pivot, as well as between pivot and rebuilt controller).
- Pay strict attention to behaviours that could be lateral movements between the two servers where replication is in progress.

→ **At system level:**

- Check that no binary, malicious script or persistence mechanism from an intruder is present on the pivot and reconstructed domain controllers. A differential analysis of the pivot domain controller before and after replication is done to spot and examine potential differences.

Suspect points are analysed to qualify any behaviours that are unknown or do not match expectations. These technical investigations are necessary to guarantee a successful eviction from the Active Directory Tier 0.



PART II

**TECHNICAL  
ACTIONS FOR  
EVICTION FROM  
ACTIVE  
DIRECTORY  
TIER 0**

---

# 1 INTRODUCTION

The technical actions for eviction from the Active Directory Tier 0 described in this document are distributed according to the three remediation scenarios detailed in the strategic and operational documents of this corpus of documents<sup>7</sup>.

For the trusted core of the Active Directory, these three scenarios have different objectives :

## Scenario 1: "Restore mission-critical services as quickly as possible".

The objective is a rapid resumption of activity, by removing the attacker's access identified during analysis and by restoring a minimum trusted core.

## Scenario 2: "Take back control of the IS".

The aim is to eliminate the attacker's access, but also to secure the Active Directory against the most frequently used attack patterns.

## Scenario 3: "Seize the opportunity to pave the way for enduring IS control".

The objective is to take advantage of the attacker's eviction to take back control of IS management. Various measures aimed at reducing the risk of persistence of the attacker's backdoors are then put in place, thus making it possible to regain a good degree of confidence in the integrity and security of Tier 0.

It should be noted that in an Active Directory environment, the security limit is the forest, not the domain. The technical eviction objectives defined in this guide can therefore be considered to be met only when they have been attained in all areas of a compromised

---

<sup>7</sup> See Appendix C: Structure of the corpus of documents.

forest<sup>8</sup>. In addition, this must be done at the same time, to prevent a domain that has already undergone remediation being compromised from a domain that has not yet done so.

The technical actions listed here only address the control paths most commonly used by attackers. Additional actions specific to the ongoing attack may be required to complete the eviction.

## 2 RECAP TABLE OF TECHNICAL ACTIONS FOR EVICTION FOR THE DIFFERENT SCENARIOS

TECHNICAL ELEMENT	SCENARIO 1	SCENARIO 2	SCENARIO 3
Ensure no Tier 0 machines are compromised			
Reinstall all domain controllers.		✓	✓
Reinstall all Tier 0 machines.		✓	✓
Remove dangerous control paths to domain controllers.	✓	✓	✓
Remove dangerous control paths to infrastructure elements with impact on domain controllers.		✓	✓
Remove dangerous control paths to MicrosoftDNS servers.	✓	✓	✓

<sup>8</sup> Depending on the Active Directory's architecture, several forests may therefore potentially have to be rebuilt.

Remove all delegated authentications from domain controllers.	✓	✓	✓
Secure RODCs.	✓	✓	✓
<b>Renew secrets to prevent the use of compromised accounts</b>			
Default administrator account.	✓	✓	✓
<i>krbtgt</i> account.	✓	✓	✓
Other secrets enabling takeover of Tier 0.	✓	✓	✓
Compromised accounts or those suspected to be compromised.	✓	✓	✓
Secrets of trust relationships.	✓	✓	✓
DSRM account.			✓
KDS keys.		✓	✓
<b>Configure the Active Directory with no weaknesses allowing takeover of Tier 0</b>			
Increase the functional level of the forest.		✓	✓
Harden the directory configuration.		✓	✓
Remove dangerous control paths to the directory's privileged objects.	✓	✓	✓
Remove dangerous permissions on the <i>adminSDHolder</i> object.	✓	✓	✓

Use the DFSR protocol for SYSVOL replication.		✓	✓
<b>Harden the directory's privileged objects</b>			
Secure privileged account attributes.		✓	✓
Reset <i>admincount</i> attributes.			✓
<b>Clean up GPOs applicable to privileged objects</b>			
Secure configuration for GPOs applicable to the domain root.		✓	✓
Secure configuration for GPOs applicable to Tier 0 machines.		✓	✓
Remove attack paths to GPOs applicable to privileged objects.	✓	✓	✓
<b>Eliminate weaknesses in the configuration of trust relationships</b>			
Eliminate weaknesses in the configuration of trust relationships.		✓	✓
<b>Configure privileged services not causing Tier 0 to be compromised</b>			
Configure privileged services not causing Tier 0 to be compromised.		✓	✓

Adopt secure administration practices			
OU structure consistent for securing T0.		✓	✓
Use dedicated accounts for T0 administration.	✓	✓	✓
Robust password policy for administration accounts.	✓	✓	✓
Reduce the number of privileged accounts.	✓	✓	✓
No control paths to members of privileged groups.	✓	✓	✓
Create secure administration workstations.	✓	✓	✓
Apply administration practices preventing the presence of privileged account secrets in the memory of non-T0 machines.		✓ (organisational measures)	✓ (technical measures)

## 3 ENSURE NO TIER 0 MACHINES ARE COMPROMISED

### a – Reinstall all domain controllers

Domain controllers are central to the Active Directory, since it is these servers that host it. In this respect, an attacker with persistence on one of the domain controllers will have the ability to compromise the Active Directory once again, immediately after eviction.

---

To prevent the attacker from returning through this medium, all domain controllers must be reinstalled. Reinstalled operating systems must be updated to ensure that there are no known vulnerabilities on the new systems.

This can be done without service interruption, by reinstalling the domain controllers one by one and relying on the robust availability currently offered by Active Directory architectures, or by accepting a service interruption, through a pivot domain controller.

When reinstalling domain controllers without service interruption, it should be noted that there is a risk that the attacker will compromise the new domain controllers during their deployment.

For reinstallation of domain controllers with service interruption, several principles must be applied for it to be fully effective:

- The new domain controllers that will run the Active Directory following eviction must not be directly exposed to the former domain controllers. For example, a pivot domain controller can be used, on which the Active Directory data is replicated and then cleaned up, according to other measures provided in this document. This pivot domain controller must be specifically protected and/or supervised to provide the safety guarantees required by the victim (no persistence on the disk, operation in memory, etc.). The new domain controllers then replicate the data from this pivot.
- A domain controller must never be in service at the same time as its replacement.

An example of eviction including reinstallation of domain controllers with service interruption is provided in the appendix<sup>9</sup>.

---

<sup>9</sup> See Appendix B. Example of the progress of a single-domain Active Directory Tier 0 eviction operation.

---

## **b – Reinstall all Tier 0 machines**

Following the implementation of the tier administration model, administrators with the highest level of rights and privileges, also known as Tier 0 administrators, are required to log onto the different machines of this Tier. The domain controllers covered in the previous point are a case of Tier 0 machines, but they are not the only ones. Other examples of these machines are the Tier 0 administrator workstations, or the AD Connect servers.

If an attacker has a privileged means of persistence on one of these machines, it would be possible for them to recover from the memory the secrets of a Tier 0 administrator. Recovering such secrets amounts to compromising the Active Directory.

To protect the system against the attacker's potential return, all Tier 0 machines must be reinstalled to ensure that there is no persistence.

The process for identifying the machines to be included in the Active Directory Tier 0 is detailed in the appendix<sup>10</sup> of this document.

## **c – Remove dangerous control paths to domain controllers**

The presence of a control path to a domain controller gives the accounts concerned full control of the Active Directory. An attacker could, for instance, replicate all secrets (including those of domain administrators), reuse them and thus take full control of a domain.

During remediation, all control paths to domain controllers should be removed from users who are not members of privileged groups and confirmed as legitimate.

---

<sup>10</sup> See Appendix A. Approach for defining the scope of the Active Directory Tier 0.



---

## d – Remove dangerous control paths to infrastructure elements with impact on Tier 0

Different infrastructure components can allow Tier 0 elements to be controlled, in particular:

- WSUS update services applicable to domain controllers or other Tier 0 machines;
- hypervisors hosting domain controllers or other Tier 0 machines;
- vendor products using an agent deployed on the domain controller or other Tier 0 machines, such as anti-virus software.

In the context of eviction from Tier 0, and in order to prevent escalating privileges through these services, it is necessary to:

- remove items not required to secure Tier 0, e.g., agents deployed on domain controllers;
- dedicate strictly necessary Tier 0 infrastructure services and administer them using Tier 0 administration accounts.

## e – Remove dangerous control paths to MicrosoftDNS servers

Accounts with rights to write *CN=MicrosoftDNS,CN=System* container properties can have the DNS service execute arbitrary code. This service is usually hosted on a domain controller. By default, members of the *DnsAdmins* group have this right and can therefore take over any domain controller with the DNS role.

It is recommended to remove write to *CN=MicrosoftDNS,CN=System* container properties access rights from accounts with such control paths.

---

If such access has been granted for DNS management, a delegation can be created manually. If specific rights are required, it should be considered that the delegated accounts or groups are themselves privileged. Thus, they must be properly protected and their rights must be at least as restrictive as those applied to the *adminSDHolder*.

Despite the availability of a patch from Microsoft<sup>11</sup>, these dangerous features can still be re-enabled. It is therefore impossible to assess setting safety just by studying the configuration in the Active Directory, just as it is impossible to verify with certainty that all Microsoft DNS servers are up to date. Additional information on this point can be found in the list of Active Directory assessment items<sup>12</sup>.

## f – Remove delegated authentications from domain controllers

Delegated authentications on domain controllers can be of several types:

- constrained on a domain controller's service;
- constrained with protocol transition to a domain controller service;
- resource-based constrained , on domain controllers.

These different types of delegations, which are detailed in the list of Active Directory assessment items, can allow accounts with these delegations to escalate their privileges to domain controllers. These delegations must therefore be deleted during the remediation phase.

---

<sup>11</sup> <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40469>

<sup>12</sup> See the Active Directory assessment items on the CERT-FR website: <https://cert.ssi.gouv.fr/dur/CERTFR-2020-DUR-001/> (English version at [https://www.cert.ssi.gouv.fr/uploads/ad\\_checklist.html](https://www.cert.ssi.gouv.fr/uploads/ad_checklist.html))

---

## g – Secure Read-Only Domain Controllers (RODCs)

RODCs carry some of the Active Directory secrets and may, if compromised, result in full takeover of the IS.

During the remediation phase, various potential RODC configuration weaknesses should be corrected, and in particular:

- dangerous configuration of read-only domain controllers (RODC) (*reveal*);
- dangerous configuration of read-only domain controllers (RODC) (*neverReveal*);
- dangerous configuration of replication groups for read-only domain controllers (RODCs) (*allow*);
- dangerous configuration of replication groups for read-only domain controllers (RODCs) (*denied*).

## 4 RENEW SECRETS TO PREVENT ATTACKER USE OF COMPROMISED ACCOUNTS

### a – Default administrator account

The “Integrated Administrator” account (RID 500) is completely exempt from some security strategies. This allows it to be used, as a last resort, to correct any configuration error. This account has a “break glass” role and must never be used on a daily basis.

For this account, it is recommended to generate a complex, random password and keep it in a vault that can be accessed if control of the Active Directory is lost. The password must also be tested to ensure that it can be used when it becomes necessary. It is recommended to


---

change it once it has been used. Finally, since this account is not used on a daily basis, setting up alerts regarding its use may help detect intrusions.

## b – krbtgt account

The *krbtgt* account is an infrastructure account used to store the keys to Kerberos key distribution centres. A compromised *krbtgt* account allows an attacker to forge Kerberos tickets (often called *golden tickets*) and thus obtain access to any resource (server, workstation, etc.) in the Active Directory domain with administration rights, in a relatively discreet manner. As the password of the *krbtgt* account is not changed automatically, if the Active Directory account database has been extracted (e.g., by a former administrator, during an audit or for a password robustness test), the information contained in the database can be used to extract its secrets as long as this password has not been changed. An attacker can thus use it for authentication on all services of the Active Directory domain several years after extraction of the database.

The *krbtgt* account's password must be changed twice to be effective.

 **Caution:** any operation to change the password of the *krbtgt* account must only be carried out in an Active Directory environment where replication between the domain controllers is nominal. Thus, it is essential to wait long enough for replication of the change before the second password change.

## c – Directory Service Restoration Mode (DSRM) administrator account

*Directory Services Restore Mode* (DSRM) is a feature of Active Directory domain controllers used to preserve “break glass” access to these machines. The password of the account used by the service may be different for each of the domain controllers.

---

If the domain controllers are not reinstalled, it is recommended to renew the DSRM account password on each of the controllers.

If the domain controllers are reinstalled, assign the DSRM account a password different from the previous one.

As for the default administrator account, it is recommended to generate a complex, random password and keep it in a vault that can be accessed if control of the Active Directory is lost. The password must also be tested to ensure that it can be used when it becomes necessary.

#### **d – KDS keys**

To ensure there are no backdoors using group administered service accounts (gMSA), it is necessary to add a new root key to the key distribution service (KDS) and then renew all group administered service accounts that are part of Tier 0.

#### **e – Secrets of trust relationships**

The secrets of the different trust relationships configured between the forest domains and those of other forests must also be renewed. To do so, it is necessary to renew the secrets on the inbound approval and then use the same password on the outbound approval.

#### **f – Other secrets enabling takeover of Tier 0**

To protect the Active Directory from further direct compromise by using an account controlled by the attacker prior to eviction, it is necessary to renew all secrets (passwords, smart card certificates, etc.) that may directly or indirectly allow control of Tier 0 to be obtained. This includes user accounts, as well as service accounts and machine accounts.

---

For example, the following secrets must be renewed if present in the infrastructure:

- an MSOL account used by the AD Connect service;
- private keys used by certification authorities present in the *NtAuthCertificate* container;
- a WSUS server machine account used to update domain controllers.

#### g – Suspected compromised accounts identified during the investigation

Similarly, it is recommended to renew the secrets of all suspect accounts identified during investigations, so that they cannot be reused.

## 5 CONFIGURE THE ACTIVE DIRECTORY WITH NO WEAKNESSES ALLOWING TAKEOVER OF TIER 0

#### a – Increase the functional level of the forest

In Active Directory environments, some mechanisms are linked to functional levels that may be present at forest or domain level. The functional levels are characterized by a number ranging from 0 (Windows 2000) to 7 (Windows 2016/2019/2022). To benefit from the latest security features, it is important to increase the functional levels of both domains and forest. Each functional level provides security features:

- 
- **Functional level 2** (Windows 2003): adds forest trust relationships and read-only domain controller (RODC) support.
  - **Functional level 3** (Windows 2008): supports robust encryption algorithms such as AES and DFS for SYSVOL share replication.
  - **Functional level 4** (Windows 2008R2): enables use of the AD recycle bin (protecting against accidentally deleting objects).
  - **Functional level 5** (Windows 2012): enables the use of advanced Kerberos features such as compound authentication and claims support.
  - **Functional level 6** (Windows 2012R2): introduces many security features such as authentication policies, authentication policy silos and the Protected Users group.
  - **Functional level 7** (Windows 2016/2019/2022): improves account security when smart card authentication is used and adds Privileged Identity Management (PIM) trust relationships between forests.

To increase a domain's functional level, all domain controllers must be upgraded to an operating system supporting the target level and then migrated to the higher functional level.

Similarly, to increase the functional level of a forest, all the domains must have an equivalent or higher functional level.



**Note:** the compatibility must be checked between the functional level and the software used in the IS, for instance Microsoft Exchange<sup>13</sup>.

---

<sup>13</sup> See Microsoft's website, "Exchange Server supportability matrix": <https://docs.microsoft.com/en-us/exchange/plan-and-deploy/supportability-matrix?view=exchserver-2019>

---

## b – Harden the directory configuration

The directory configuration parameters affecting the security of the Active Directory environment must be set to values that do not jeopardise Tier 0. For instance, the dangerous parameters configured in the *dSHeuristics* property must be changed and reset to their default value:

- *fLDAPBlockAnonOps* must not be configured or have a value other than 2;
- *fAllowAnonNSPI* must be equal to 0;
- *dwAdminSDExMask* must be equal to 0.

## c – Remove dangerous control paths to the directory's privileged objects

Having a control path to a privileged object in the directory may allow an attacker to take full control of the Active Directory. Some of these privileged objects are:

- the root of the *naming contexts*;
- DPAPI keys;
- gMSA keys;
- SYSVOL DFSR settings;
- the objects of the schema.

The control paths to these objects must therefore be corrected for all objects not legitimately belonging to Tier 0.



---

## d – Remove dangerous permissions on the adminSDHolder object

The permissions of the *adminSDHolder*<sup>14</sup> object are regularly applied to all protected objects (members of administrative and operational groups) of the Active Directory. By default, only privileged objects have rights to the *adminSDHolder* object. Thus, this mechanism protects the most privileged users and groups of the Active Directory.

We strongly advise against changing the default permissions of this object, as the presence of dangerous permissions can break the segregation of Tier 0 in a tiered administration model.

Thus, it is recommended to remove dangerous permissions on the *adminSDHolder* object in order to return to a default state.

## e – Use the DFSR protocol for SYSVOL replication

It is recommended to use only the *Distributed File System Replication* (DFSR) mechanism to synchronise directories on different servers, especially for SYSVOL replication.

The NTFRS protocol is obsolete and unnecessarily adds administration interfaces to domain controllers. In addition, this protocol is no longer supported by the latest versions of Windows Server, which prevents migration to the latest versions. It is therefore recommended to disable this protocol.

Microsoft provides information on the migration process to DFSR<sup>15</sup>.

---

<sup>14</sup> See Microsoft's website, "Exchange Server supportability matrix", <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/appendix-c-protected-accounts-and-groups-in-active-directory#adminsldholder>

<sup>15</sup> See Microsoft's website, "Exchange Server supportability matrix", <https://docs.microsoft.com/en-us/windows-server/storage/dfs-replication/migrate-sysvol-to-dfsr>

---

## 6 HARDEN THE DIRECTORY'S PRIVILEGED OBJECTS

### a – Secure privileged account attributes

Privileged accounts must be protected to prevent them from being compromised following eviction. To do so, a number of attributes must be looked at. The list of Active Directory assessment items details the various dangerous attributes of user accounts, in particular through the following assessment items:

- privileged accounts without Kerberos pre-authentication;
- use of Kerberos with weak encryption;
- accounts or groups with unexpected SID history;
- privileged accounts with SPN;
- accounts with modified PrimaryGroupID;
- privileged accounts with passwords that never expire;
- accounts with password stored using reversible encryption.

### b – Reset admincount attributes

The *admincount* attribute set on user objects indicates the user's current or past membership of one of the protected groups<sup>16</sup>. When a user is added to one of these protected groups, the *admincount* attribute is set to 1. This value "1" is then reapplied every hour, as long as the user belongs to at least one of these groups.

---

<sup>16</sup> See Microsoft's website, "Appendix C: Protected Accounts and Groups in Active Directory", <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/appendix-c--protected-accounts-and-groups-in-active-directory>

---

When the user is removed from all protected groups to which they belong, the *admincount* attribute is no longer changed and retains the value "1". This mechanism can thus be used to identify a temporary escalation in an account's privileges in one of the protected groups.

Once Tier 0 is evicted, it is then necessary to process accounts with an *admincount* attribute value "1" that are no longer members of a protected group. To ensure there is no risk to such accounts, it is necessary to:

- disable the account;
- remove it from all the groups it belongs to;
- change its password randomly;
- possibly move the account to a dedicated OU;
- if necessary, update the account description field to indicate the context for disabling it (date, reason, etc.).

If disabling the account is not an acceptable option, it is possible to manually reset the value of the *admincount* attribute to 0 and re-enable the legacy permissions.

## **7 CLEAN UP GPOs APPLICABLE TO OBJECTS**

### **a – Secure configuration for GPOs applicable to the domain root**

GPOs that apply to the domain root, apply by default to all objects in the domain, including privileged objects. These GPOs must be checked to ensure that the configuration they apply does not result in security weaknesses that could allow attackers to take control of privileged objects.

---

## **b – Secure configuration for GPOs applicable to Tier 0 machines**

Similarly, GPOs that apply to Tier 0 machines, such as domain controllers, must be checked to ensure that the configuration they apply does not result in security weaknesses that could allow attackers to take control of these machines.

## **c – Remove attack paths to GPOs applicable to privileged objects**

An attacker with control of a GPO can escalate their privileges by using it to execute code on the machines of the users to whom it applies.

The permissions set on GPOs that apply to privileged objects must therefore be reviewed to prevent any repeat intrusion in the Active Directory by this means.

# **8 ELIMINATE WEAKNESSES IN THE CONFIGURATION OF TRUST RELATIONSHIPS**

Trust relationships with an external domain may be gateways for attack if they have configuration weaknesses. An attacker compromising an external domain may impersonate any user or machine in the domain (except accounts with RID below 1000, which excludes default users or groups). The attacker can then access all data in the domain. If there is a control path for the spoofed account, the attacker can also escalate privileges to "Domain Administrators" and compromise the entire forest.

---

The list of Active Directory assessment items details the various dangerous configurations to avoid for trust relationships, in particular through the following assessment items:

- unfiltered outbound domain trust relationships;
- outbound forest trust relationships with sID History enabled;
- inbound trust relationships with delegation;
- trust relationship accounts with passwords unchanged for more than a year.

## **9 CONFIGURE PRIVILEGED SERVICES NOT CAUSING TIER 0 TO BE COMPROMISED**

In addition to domain controllers and domain administrator accounts, Tier 0 must include all accounts, machines and services that can allow maximum privilege escalation on the domain.

By default, various services have significant privileges that can compromise the Active Directory trusted core. This is, for instance, the case of:

- the DNS service, often installed on the domain controllers, which has some configurations that could cause Tier 0 to be compromised;
- the Active Directory Certificate Services (ADCS), which, if incorrectly configured, may lead to the presence of control paths to the containers or certificate templates;
- the AD Connect service, which in some configurations has replication privileges for all domain users;

- 
- WSUS servers, from which the domain controllers or other Tier 0 machines retrieve their updates;
  - Active Directory backup servers;
  - many vendor services requiring significant delegations of privileges on the domain for installation, sometimes even domain administrator accounts.

For all services that can escalate privileges on the Active Directory trusted core, in order of importance it is necessary to:

- limit privileges as much as possible by setting up strictly necessary delegations of privileges, in order to restrict dangerous delegations that are often unnecessary for proper department operation;
- consider the services as belonging to Tier 0 and apply to them the same hardening principles as for the other Tier 0 assets (administration by Tier 0 administrators, and from Tier 0 administration workstations in particular).

## **10 ADOPT SECURE ADMINISTRATION PRACTICES**

### **a – Organisational Unit (OU) structure consistent for securing Tier 0**

To facilitate management and security of Tier 0 elements, it is recommended to set up a clear organisational unit structure that complies with the following principles:

- the organisation of the organisational units (OU) in the directory must allow applying GPOs to privileged objects only, and ensure that GPOs of other elements of the domain

---

do not apply to the privileged objects (outside the default domain GPO);

- domain controllers must be retained in their default organisational unit.

## **b – Use dedicated accounts for administration**

Tier 0 element administration must use dedicated accounts, identified as Tier 0 administrators. These administrator accounts with maximum domain privileges (domain administrator privileges) must be particularly secure. Moreover, these accounts must only be used for administration actions requiring the highest levels of rights and privileges. They must only connect to Tier 0 machines to avoid jeopardising them; no exceptions are tolerated.

## **c – Robust password policy for privileged accounts**

As indicated in the previous point, privileged accounts must be especially secure, starting with the implementation of a robust password policy<sup>17</sup>.

## **d – Reduce the number of privileged accounts**

The proliferation of privileged accounts is bad practice. It complicates their supervision, increases the risk of account configuration, disabling or deleting errors, broadens the control paths, etc.

Privileged Active Directory groups give member users all rights and privileges over the forest. Using these groups, other than the “Administrators” and “Domain Administrators” groups, therefore engenders a false sense of security.

---

<sup>17</sup> See also the Recommendations on the secure administration of information systems on the ANSSI website: <https://cyber.gouv.fr/publications/recommandations-relatives-ladministration-securisee-systemes-dinformation>

---

An administration model must be set up to reduce the number of privileged accounts. To do so, reference the administration needs of each account and make the delegations *ad hoc*.

### e – Delete control paths to members of privileged groups

The presence of a control path to a member of privileged groups is a direct route for an attacker to regain control of the Active Directory.

During remediation, all control paths to members of the domain's privileged groups should be identified and removed to prevent further compromise through them.

### f – Create secure administration workstations

Tier 0 administration actions, performed by Tier 0 administrators, must be initiated from dedicated administration machines. These machines, called Tier 0 administration workstations, must be secured in accordance with the following principles<sup>18</sup>:

- These workstations must be controlled, and BYOD practices banned.
- If the workstation combines a Tier 0 administration environment and one or more other environments (e.g., office usage) through a virtualisation or containerisation mechanism, the environments must be partitioned by mechanisms assessed as trusted at system level. In particular, it should be impossible to switch from low sensitivity (one of the other environments) to high sensitivity (the Tier 0 administration environment).

---

<sup>18</sup> See also the Recommendations on the secure administration of information systems on the ANSSI website: <https://cyber.gouv.fr/publications/recommandations-relatives-ladministration-securee-des-systemes-dinformation>



- 
- If a remote access solution is used, it must not allow the switch from low sensitivity (e.g., office network ) to high sensitivity (e.g., Tier 0 administration workstation).
  - The administration workstation must have no Internet access, and in particular, no e-mail.
  - The workstation must be hardened regarding its software platform and configuration.
  - The hard disk of the administration workstation must be encrypted.
  - The workstation operating system must be supported and kept updated by the same mechanism as domain controllers (e.g., same WSUS server).

### g – Apply administration practices preventing the presence of privileged account secrets in the memory of non-Tier 0 machines

Tier 0 administration practices, which in most cases contributed somewhat to the incident being remedied, must change to protect the Active Directory's trusted core from a new breach.

This change is intended to ensure Tier 0 is not jeopardised by administrative practices allowing the presence of privileged secrets on machines not belonging to this Tier 0.

In a first approach, organisational measures can be put in place to train administrators to use Tier 0 administration accounts exclusively on Tier 0 machines.

Subsequently, different technologies can be weighed to prevent any deviation (deliberate or accidental) from these organisational measures. For example, some technologies are:

- 
- setting up authentication silos;
  - "Restricted Admin" mode for RDP connections;
  - the LAPS (*Local Administrator Password Solution*) solution;
  - the "djoin" mechanism for creating and joining new machines;
  - use of the "Protected Users" security group.

# PART III

## **TECHNICAL ACTIONS FOR SUPERVISION OF ACTIVE DIRECTORY TIER 0**

---

As part of Tier 0 implementation, secrets are renewed because they may potentially be in the attacker's possession. If the attacker tries to use the old secrets, errors will be generated and logged.

For example, the following traces could be generated by an attacker:

- authentication error when using a renewed password;
- Kerberos ticket request error in case of stolen *krbtgt*;
- authentication error on an account in a silo from an unauthorised machine.

These events may make it possible to identify an attacker that still has access to the IS. Extending the scope to all compromised systems, or even to the entire IS, makes it possible to identify in what areas the attacker is still present and what activities they are using to pursue their objectives or to take back control of Tier 0.

In this case, implementing a logging policy at the right level must be considered. Microsoft log centralisation technologies are useful to deploy in this context because they are robust and silent as regards the system.

To implement such logging, ANSSI has published a guide<sup>19</sup> and provides resources<sup>20</sup> such as configuration scripts and a selection of events relevant to intrusion detection. This guide explains how to set up a server to act as a log collector, and how to deploy a GPO so that all computers in the domain send their logs to the collectors.

Once logging has been set up, the data must be indexed in a log collector or SIEM. Each provider has tools for ingesting logs and

---

<sup>19</sup> Guide de l'ANSSI Recommandations de sécurité pour la journalisation des systèmes Microsoft Windows en environnements Active Directory (ANSSI security recommendations guide for logging Microsoft Windows systems in Active Directory environments), 2022.

<sup>20</sup> ANSSI GitHub: <https://github.com/ANSSI-FR/guide-journalisation-microsoft>

---

standardising data. In addition, these SIEMs come with a set of default rules that need to be refined to avoid generating too many false positives<sup>21</sup>.

---

<sup>21</sup> See Appendix C of the ANSSI guide: *Recommandations de sécurité pour l'architecture d'un système de journalisation* (Security recommendations for the architecture of a logging system), 2022.

# APPENDICES

---

## **A APPROACH FOR DEFINING THE SCOPE OF THE ACTIVE DIRECTORY TIER 0**

The Active Directory Tier 0 is defined as all resources having control over the company's identities, and thus over all resources integrated in the AD. To define it precisely, an iterative examination is required to identify resources that can take control of those included in the scope of the current Tier 0, until this scope no longer increases.

For example, resources to be integrated into Tier 0 should be identified based on the following considerations (among others; many other dependencies may exist that cause resources to be integrated into Tier 0):

1. Domain controllers are automatically included in Tier 0 as they run the Active Directory.
2. Domain administrator accounts can act on domain controllers, and must therefore also be added to Tier 0.
3. These accounts are used from dedicated administration workstations, to which they log on, thus leaving authentication data. The administration workstations must therefore also be added to Tier 0.
4. In addition, some domain controllers are virtualised. Having privileges on the hypervisor then makes it possible to, for instance, access the disk or memory of the domain controllers. Hypervisors on which domain controllers are virtualised must therefore also be added to the scope.

- 
5. Some domain controllers have iLO interfaces that can be accessed to retrieve directory data. These interfaces and the associated accounts are therefore included in Tier 0.
  6. An anti-virus is installed on the domain controllers. From the anti-virus console, it is possible to execute code on machines with an agent, in this case domain controllers. The anti-virus console, as well as the server on which it is installed, must therefore also be added to the scope of Tier 0.
  7. The update servers of the different machines of Tier 0 may allow code execution on them. They must therefore also be integrated in Tier 0.

Following this identification, it is recommended to minimise the scope of Tier 0 by setting an initial objective of limiting it to Microsoft resources only, and only adding exceptions deemed necessary. These exceptions, such as a backup solution for domain controllers, must then be administered according to the same principles as the other Tier 0 machines and must not jeopardise it. Thus it is often recommended to dedicate these solutions solely to Tier 0 machines.

In the previous example, hypervisors are included in the scope of Tier 0. If guarantees were required against a threat of virtual machine escape (hypervisor or virtual machine compromised from another virtual machine), it would then be necessary to dedicate the hypervisors in question to Tier 0 machines only.

As domain controllers are the most critical elements of the IS, it is also appropriate to limit or even ban the use of third-party software on them. Such software increases the attack surface of domain controllers and can often be substituted by configuration or scripts. For example, it is preferable to export the event logs from the domain controllers to a dedicated machine, to generate and encrypt backups



---

locally before sending them to a storage solution, to only use the anti-virus solutions integrated in the operating system, etc.

## **B EXAMPLE OF THE PROGRESS OF A SINGLE-DOMAIN ACTIVE DIRECTORY TIER 0 EVICTION OPERATION**

Guarantees regarding the safety and security of a remediation operation can be obtained in different ways. Thus, the following example does not seek to impose a methodology, or even provide a full, detailed procedure, but to show the key stages in an example of an eviction operation on a single-domain forest with service interruption.

Before any eviction operation, it is recommended to completely shut down the IS in order to limit applications whose operation may be permanently altered due to the absence of domain controllers. For example, Exchange servers may be unrecoverable if they are not shut down during the operation. Indeed, Microsoft does not support the use of Exchange without domain controllers.

→ The stages of this eviction are as follows:

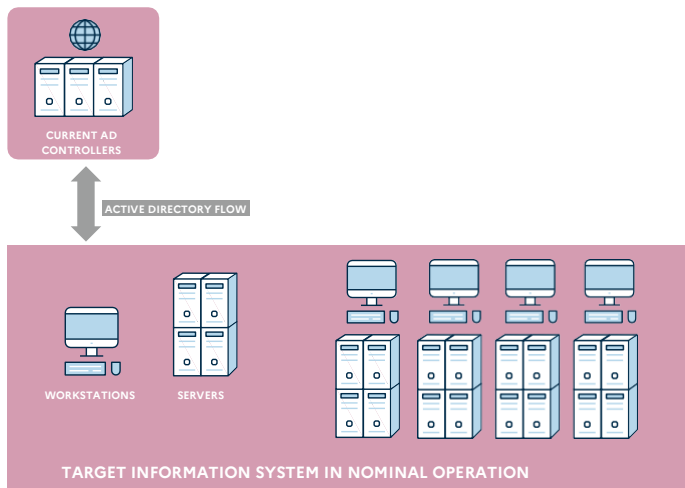
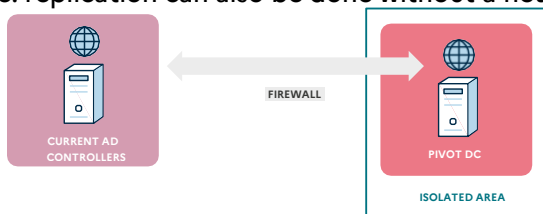


Figure 1: Information system prior to switch-over

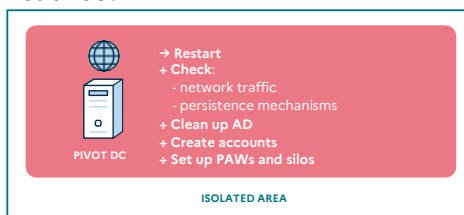
- 1 - Install a new server to act as pivot domain controller. This server must be updated and can be hardened using tools such as WDAC. It must also be isolated from the production network, either through a filtering policy or by assigning it its own site.
- 2 - Shut down the entire IS except the last domain controller, to which all roles have previously been transferred. Beforehand, check that all partitions have been replicated to this last domain controller.
- 3 - Replicate the last domain controller to the pivot domain controller.

*Figure 2: Replicate the last production domain controller to the pivot domain controller*

**Note: replication can also be done without a network link**



- 4 - Once replication has been completed correctly, isolate the pivot domain controller from the last domain controller.
- 5 - At the same time as hardening the Active Directory as indicated in the following point, analyse the system and network on the pivot domain controller in order to confirm that it is not compromised.
- 6 - Carry out the Active Directory hardening actions on the pivot domain controller until the desired security level has been reached.



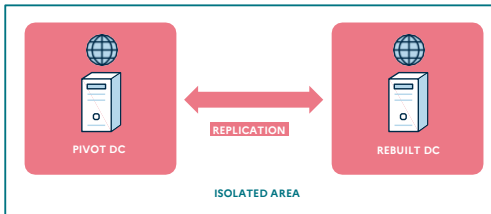
*Figure 3: Clean up and secure the Active Directory*

- 7 - At the same time, install new servers to replace the old domain controllers (all domain controllers must be replaced). To

---

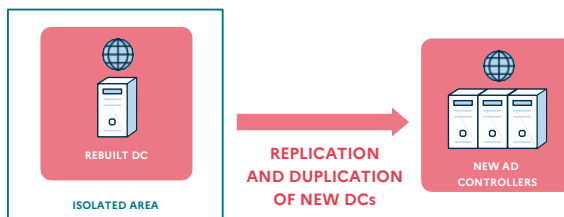
minimise start-up problems, new DCs must use the same DNS, Netbios and IP names as the old ones.

- 8 - Replicate the pivot domain controller to a first rebuilt domain controller, which recovers all roles.



*Figure 4: Replicate to a first rebuilt domain controller*

- 9 - Demote and securely dispose of the pivot domain controller that has the new production secrets.
- 10 - Promote the newly reinstalled domain controllers and replicate from the first rebuilt domain controller.



*Figure 5: Replicate to new domain controllers*

---

11 - Reopen traffic flows and restart the IS.

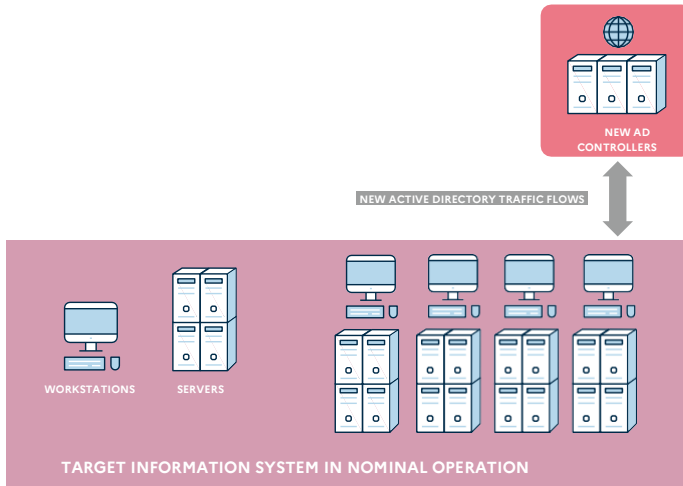
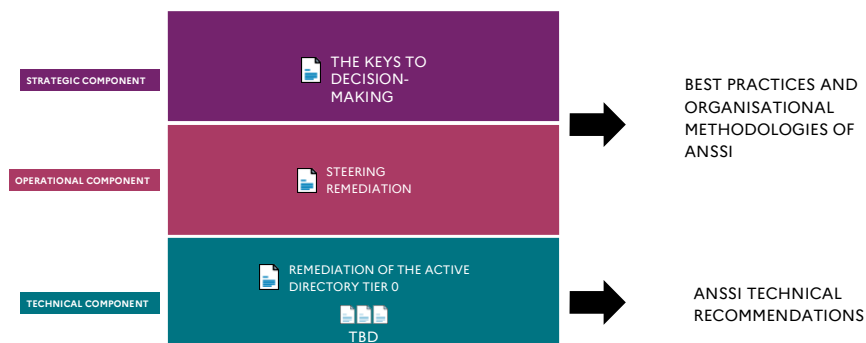


Figure 6: Reopen traffic flows

---

## C STRUCTURE OF THE CORPUS OF DOCUMENTS





Remediation is defined as the project to regain control of a compromised information system and restore a sufficient operating state. The technical component, which deals with reconstruction of the trusted core of an information system based on Microsoft Active Directory, presents the key measures required for reconstruction. Properly managed, the incident can provide the opportunity for significant improvement.

Remediation, along with investigation and crisis management, is one of the key aspects of the response to a cyberattack (business disruption or espionage). It begins as soon as the intruder has been contained and can last several months.

Building on its extensive experience supporting organisations that suffered cyber security incidents, ANSSI has published a set of remediation guides describing the principles of remediation management and its proper implementation: the strategic component, the operational component and the technical component.

This technical component presents the investigation, eviction and supervision actions of the Active Directory Tier 0 in order to take back control of an IS.

---

Version 1.0 – March 2025

**Registered: March 2025**

Paper ISBN: 978-2-11-167193-5

Digital ISBN: 978-2-11-167192-8

*Licence Ouverte/Open Licence (Etalab — V1)*

**AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION**

ANSSI — 51, boulevard de la Tour-Maubourg — 75 700 PARIS 07 SP

[www.cyber.gouv.fr](http://www.cyber.gouv.fr)

