RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ReCyF en pratique

GOUVERNANCE | **PROTECTION** | DÉFENSE | RÉSILIENCE | OBLIGATIONS NIS 2

Administration

La collection de fiches « ReCyF en pratique » a pour objectif d'éclairer les principales mesures de gestion de risque issues du Référentiel Français de Cybersécurité (ReCyF). Ce référentiel a pour vocation de devenir le socle de la réglementation cyber française.

La collection de fiches « ReCyF en pratique » ne se substitue pas au référentiel. Les fiches ne sont pas prescriptives et ne visent pas l'exhaustivité. Sur la base des objectifs de sécurité fixés dans Référentiel Cyber France (ReCyF), ces fiches expliquent en pratique les effets recherchés, présentent des exemples concrets d'implémentation et proposent des références utiles pour aider les entités à mettre en œuvre ces objectifs et mesures de sécurité.

Elles s'adressent à un public technique chargé de la mise en œuvre de ces objectifs de sécurité au sein des entités concernées.

Cet ensemble de fiches est organisé en cinq rubriques: Défense, Protection, Gouvernance, Résilience et Obligations NIS 2, les quatre premières constituant les piliers essentiels des mesures de gestion des risques.

Rubrique Protection
Adoptez un ensemble de mesures essentielles pour éviter la compromission de vos SI.

INDICATION DE LECTURE

Pour distinguer les passages du texte destinés aux entités importantes (EI), de ceux destinés aux entités essentielles (EE), les marques suivantes ont été placées en marge du texte:

Ce texte (sans repère en marge) est à destination des EI et des EE

Ce texte (avec repère bleu en marge) est à destination des EE uniquement

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Effets recherchés

Toute **action d'administration** effectuée sur le système d'information (SI) est **légitime**, réalisée à partir d'un compte et de ressources d'administration dédiés. Elle doit être attribuable de façon univoque à l'administrateur ou au processus automatique qui l'a effectuée.

Cet effet recherché est rendu possible par la maîtrise et la protection des comptes et des ressources d'administration :

- les **comptes d'administration** sont protégés contre des accès illégitimes en limitant la dissémination de leurs secrets en dehors du périmètre autorisé. En effet, ces comptes permettent à un administrateur d'effectuer des actions d'administration nécessitant des privilèges sur le SI. Ces comptes privilégiés sont donc particulièrement sensibles. La confiance dans le SI repose sur la confiance accordée à ces comptes.

- les **ressources d'administration** sont maîtrisées par l'entité responsable du SI, car elles peuvent contenir des secrets des administrateurs. L'intégrité du SI repose sur celle de ces ressources, et donc sur la protection des secrets qu'elles contiennent. La protection de ces secrets s'appuie notamment sur du cloisonnement en zones de confiance et au travers de ressources dédiées par niveau de sensibilité.

L'entité identifie **ses cœurs de confiance** en partant de ses annuaires, et veille à ce que l'ensemble des actions d'administration les concernant soit réalisé exclusivement depuis des comptes et des ressources dédiés.

Approche générale

L'administration sécurisée d'un SI s'appuie sur deux principes :

- la maîtrise des comptes d'administration et des privilèges, afin de limiter la capacité de propagation d'un adversaire et de limiter ses impacts ;
- la maîtrise des ressources d'administration à travers la séparation des usages et le cloisonnement des environnements, afin de limiter les risques de propagation en cas de compromission d'un environnement ou d'un compte d'administration, mais aussi les risques d'accès non autorisés.

Il est nécessaire de se référer en particulier à la fiche « Architectures sécurisées » de la collection « ReCyF en pratique », notamment le chapitre « Cloisonnement », afin de comprendre qu'il existe différentes zones pour lesquelles ces principes s'appliquent.

Ces principes font écho au modèle de cloisonnement par niveau (*tiering model*) que l'on retrouve dans le modèle de sécurité des environnements Microsoft.

De plus, dans les SI, certaines ressources (par exemple les annuaires) peuvent permettre de prendre le contrôle de la majorité des composants du SI. L'ensemble de ces ressources appartient au « cœur de confiance », dont il est primordial d'assurer la sécurité, en respectant en premier lieu les principes énoncés ci-dessus.

COMPTES D'ADMINISTRATION

Mesures ReCyF

Objectif de sécurité 11
Maîtrise de l'administration des systèmes d'information
- Comptes_administration : 11.A.1-EI/EE, 11.A.2-EI/EE, 11.A.3-EI/EE, 11.A.4-EE, 11.A.5-EI/EE, 11.A.6-EE, 11.A.7-EE

Pourquoi protéger les comptes d'administration ?

Les **comptes d'administration** permettent à un administrateur d'effectuer des actions d'administration, c'est-à-dire tout acte susceptible d'affecter le fonctionnement ou la sécurité du SI. L'installation d'un antivirus, d'agents de supervision ou la configuration d'un routeur sont des exemples de telles actions. Pour effectuer ces actions, les comptes d'administration disposent de privilèges (autorisations, droits) importants.

Pour un attaquant cherchant à contrôler un SI, disposer de ces privilèges est un moyen d'arriver à ses fins. Pour cela, l'attaquant va chercher à compromettre des comptes d'administration, et donc à obtenir les secrets associés à ces comptes.

Il est donc primordial d'assurer la protection des comptes d'administration et d'éviter la dissémination de leurs secrets en dehors du périmètre autorisé.

Des comptes (presque) comme les autres

Un **compte d'administration** est avant tout un compte du SI. À ce titre, tout compte d'administration doit respecter les mesures relatives à la gestion des identités et des accès des utilisateurs aux systèmes d'information. Ces mesures sont expliquées dans la fiche « Gestion des identités » de la collection « ReCyF en pratique ».

Les pratiques de sécurité décrites dans cette fiche constituent une base pour les comptes d'administration. Le présent document, notamment la section « Comptes d'administration », décrivent les mesures de sécurité **supplémentaires** spécifiques aux comptes d'administration et à leur usage.

Principes applicables aux comptes d'administration

Un **compte d'administration** est destiné à être utilisé pour réaliser des actions d'administration.

Il ne doit être utilisé que lors d'actes légitimes et nécessaires, et en aucun cas pour des usages autres que l'administration. C'est le « **principe de la séparation des usages** ».

Pour limiter l'impact d'une compromission d'un compte d'administration, il faut limiter au strict nécessaire les privilèges associés au compte et le périmètre (les ressources) sur lequel ce compte peut agir. C'est le **« principe du moindre privilège »**.

Ces deux principes sont détaillés dans les sections suivantes.

Ces comptes ne doivent donc pas être utilisés n'importe où, ou par n'importe qui. Autrement dit, un compte d'administration est utilisé :

- exclusivement par des personnes ou des services autorisés, désignés comme administrateurs ou disposant d'une délégation formelle ;
- uniquement sur les ressources suivantes :
  → des postes d'administration ;
  → des ressources d'administration intermédiaires (telles que des serveurs de rebonds) ;
  → des ressources administrées pour réaliser leur administration (par exemple l'interface d'administration d'un routeur).

Le principe de séparation des usages

Chaque administrateur doit disposer **d'au moins deux comptes distincts** : un compte bureautique dédié aux usages quotidiens (navigation, messagerie, production documentaire, etc.), et un ou plusieurs comptes **d'administration** utilisés exclusivement pour les opérations techniques et d'administration. Cette séparation limite le risque d'exposition du compte privilégié à des attaques triviales telles que l'hameçonnage (*phishing*).

Les **actions d'administration** étant des opérations sensibles nécessitant des privilèges et susceptibles d'affecter le fonctionnement ou la sécurité du SI, elles doivent être réalisées exclusivement au travers d'un **compte d'administration** dédié à cet usage et être liées à l'identité de l'**administrateur** qui les exécute. Inversement, les comptes d'administration sont strictement réservés aux opérations techniques et d'administration et ne doivent en aucun cas être utilisés pour des usages courants.

Cette séparation des usages est mise en place grâce à des mesures techniques (silo d'authentification, stratégie de groupe, etc.) et organisationnelles, telles que « savoir où utiliser le compte d'administration », des politiques de sécurité du SI (PSSI), des chartes informatiques dédiées, etc.

L'utilisation d'un compte sur une ressource du SI laisse des traces qui peuvent être utilisées par un attaquant pour compromettre le compte associé. De plus, les usages courants ont une forte exposition par nature. Il est donc important de distinguer ces usages des actes d'administration.

Toute action d'administration réalisée au moyen **d'un compte non dédié** à l'administration constitue une situation **dégradée**. Elle doit être strictement encadrée, justifiée formellement, et assortie de mesures compensatoires proportionnées. Ces mesures incluent au minimum :

- un périmètre d'action restreint ;
- une supervision ciblée ;
- la mise en œuvre du moindre privilège.

La récurrence de telles situations doit être évitée, leur usage étant limité à des cas exceptionnels.

Le principe de moindre privilège

Le principe du moindre privilège consiste à n'accorder à un compte (administrateur, service, script, etc.) que les droits strictement nécessaires pour réaliser une action donnée, sur un périmètre défini, et idéalement pour une durée limitée. Son contraire est le sur-privilège : attribuer des droits « par défaut » ou « au cas où » larges, durables et sans justification. Le sur-privilège augmente les capacités d'abus ou d'erreurs et, en cas de compromission, élargit le périmètre d'action d'un attaquant.

Dans *Active Directory*, ce principe s'articule avec la séparation des usages et le modèle de cloisonnement par niveau (*tiering model*) de Microsoft. Pour un administrateur, on distingue, *a minima*, un compte bureautique et un compte d'administration. Cependant, ce dernier n'a pas vocation à être « tout-puissant » : ses droits doivent être bornés à un périmètre et à des actions clairement définis, afin de limiter l'impact d'une erreur ou d'une compromission.

Concrètement, cela se traduit par une délégation fine au plus près des objets concernés (unités d'organisation [OU], objets, attributs, stratégies de groupe) à l'aide de nouveaux groupes créés pour cet usage, plutôt que de recourir à des groupes génériques existants mais trop privilégiés (i.e. administrateur du domaine), réservés à des besoins exceptionnels et qui doivent être fortement contrôlés.

Voici des illustrations de ce principe dans un environnement Active Directory :

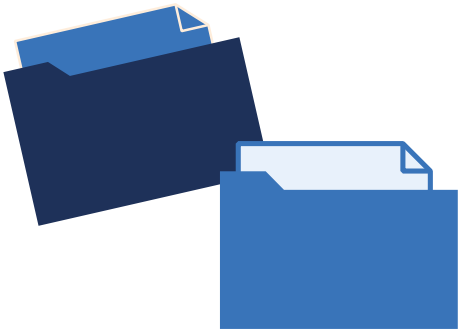
- Un support utilisateur dont le besoin se limite à réinitialiser des mots de passe et déverrouiller des comptes doit disposer de ces droits uniquement sur les OU concernées. Ce besoin ne justifie en aucun cas une appartenance au groupe « administrateurs du domaine », ni l'utilisation d'un groupe à privilèges élevés comme « opérateurs de compte[1] ».

- Une équipe « poste de travail » chargée de joindre des machines au domaine et de gérer les objets « ordinateurs » doit recevoir les droits nécessaires uniquement sur le ou les unités d'organisation « postes de travail » (création/modification/suppression des objets ordinateur). Ce besoin ne justifie en aucun cas une appartenance au groupe « administrateurs du domaine », ni l'utilisation d'un groupe à privilèges élevés comme « opérateurs de serveur.[2] ».

- Une équipe réseau chargée de la maintenance ou de l'installation d'équipements réseau ne doit pas avoir de droit dans *Active Directory*.

[1] *Opérateurs de compte* : groupe disposant de privilèges permettant de gérer les comptes utilisateur et groupes.

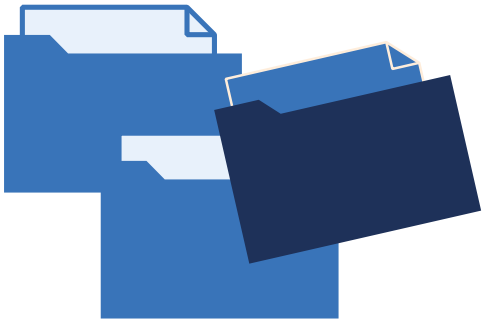
[2] *Opérateurs de serveur* : groupe disposant de privilèges permettant de gérer les objets ordinateurs.



UN COMPTE ADMINISTRATION PAR PÉRIMÈTRE D'ACTION

Un administrateur possède généralement **un ou plusieurs** comptes d'administration, suivant les zones administrées ou son périmètre d'action (serveurs du T1, station de travail du T2, équipements réseau, etc.). Par exemple, on peut envisager le cas d'un administrateur ayant plusieurs rôles techniques : administrateur système et administrateur poste de travail. Dans ce cas, il possède un compte d'administration dédié aux activités d'administrateur système et un autre compte dédié aux activités d'administrateur de poste de travail.

CLOISONNEMENT DES COMPTES SELON LES ZONES DE SÉCURITÉ



Le **cloisonnement** est un principe fondamental de la sécurité des systèmes d'information. Il consiste à séparer les équipements du SI en zones selon différents critères d'homogénéité (criticité métier, organisationnels, exposition, réglementaires, etc.), et en particulier selon leur niveau de sensibilité. Ce principe est détaillé dans la fiche « Architectures sécurisées », de la collection « ReCyF en pratique » notamment la partie « Cloisonnement ».

Ce cloisonnement se poursuit au niveau des comptes d'administration : la séparation se fait en s'assurant que chaque zone définie possède ses propres comptes d'administration.

Cette séparation permet de réduire l'impact en cas de compromission de zones exposées. Ainsi, lorsqu'une zone X est compromise, les secrets des comptes d'administration utilisés dans cette zone seront également compromis. Si ces secrets et ces comptes ne sont valables que dans la zone X, l'attaquant ne pourra pas les utiliser pour rebondir sur une autre zone.

À l'inverse, si les comptes d'administration sont communs à la zone X et à une autre zone Y, l'attaquant pourra rebondir vers la zone Y et continuer son attaque.

Par exemple, les comptes d'administration utilisés sur des serveurs d'une zone démilitarisée (DMZ), par nature exposée à Internet, doivent être distincts des comptes utilisés pour administrer une application strictement interne à l'entité. De la même manière, un compte d'administration utilisé sur les ressources du cœur de confiance (voir la section « Sécurité des annuaires ») ne doit en aucun cas être utilisé pour administrer une autre zone.

Maîtrise des comptes d'administration

Afin de maîtriser les comptes d'administration, l'ensemble de ces comptes doit être **inventorié** de manière exhaustive. Cet inventaire doit couvrir les comptes locaux, les comptes de domaine, les comptes techniques nécessaires à certaines fonctions (tâches planifiées, etc.), ainsi que les comptes spécifiques d'administration des équipements (commutateurs, routeurs, hyperviseurs, *appliances*, etc.). Le format choisi pour cette liste est à l'appréciation de chaque entité. Il peut s'agir par exemple d'un fichier texte, d'un tableur Excel ou d'un extrait régulier de la base de données *Active Directory*.

Cette liste doit être exhaustive et maintenue tout au long du cycle de vie des comptes, c'est-à-dire que toute création, modification ou suppression d'un compte d'administration doit faire l'objet d'un enregistrement systématique.

Les droits d'accès des comptes sur les ressources du SI doivent être revus et mis à jour en fonction du juste besoin opérationnel d'utilisation du compte. C'est-à-dire que les comptes d'administration doivent tendre vers le principe du moindre privilège : le compte ne doit disposer que des droits strictement nécessaires à son périmètre d'administration.

Pour faciliter la gestion des droits d'administration, il est recommandé d'utiliser des groupes de sécurité. Un groupe contient, en fonction du juste besoin opérationnel, l'ensemble des comptes d'administration devant disposer de droits d'administration homogènes sur une ou plusieurs ressources administrées. Les droits sur ces ressources sont ainsi octroyés aux groupes et non aux comptes. L'utilisation de groupes facilite notamment la gestion du cycle de vie des comptes.

Par exemple :

- un **changement de poste** au sein de l'entité. Le compte administrateur de la personne a seulement besoin d'être retiré des groupes non nécessaires à l'exercice de ses fonctions, et ajouté à ceux qui le sont. Sans l'utilisation des groupes, ce changement devrait se traduire par une mise à jour des privilèges sur chaque ressource (partage de fichiers, logiciel, etc.) ;
- en cas de **départ d'un administrateur,** son compte d'administration a seulement besoin d'être retiré des groupes auxquels il appartient, et il n'est pas nécessaire de retirer les droits de ce compte un par un sur chaque ressource administrée.

En environnement Microsoft il existe par exemple la méthode AGDLP : « *Account – Global – DomainLocal – Permissions* » représenté sur l'Image 1. Cette méthode consiste à mettre les utilisateurs dans les groupes globaux, et d'attribuer les permissions sur les groupes de domaine local, pour ensuite faire de l'inclusion de groupe.

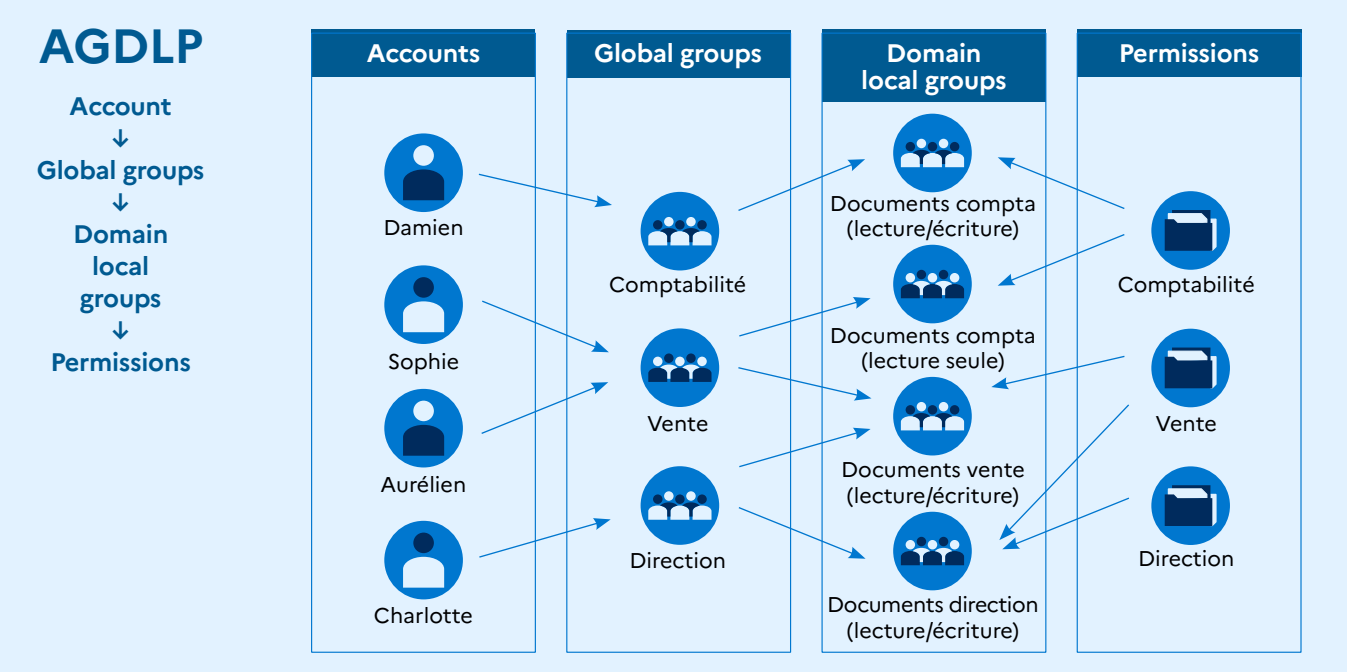


image 1: exemple d'utilisation de la méthode AGDLP en environnement Microsoft

RESSOURCES D'ADMINISTRATION

Mesures ReCyF

Objectif de sécurité 19
Administration des systèmes d'information depuis des ressources dédiées
- 19.1-EE, 19.2-EE, 19.3-EE, 19.4-EE, 19.5-EE, 19.6-EE, 19.7-EE, 19.8-EE, 19.9-EE, 19.10-EE, 19.11-EE, 19.12-EE

L'administration d'un SI repose sur un principe central : maîtriser la dissémination et l'exposition des secrets liés aux comptes d'administration.

Ces comptes possèdent parfois des privilèges très élevés. Ils doivent être strictement contrôlés et maîtrisés, c'est-à-dire qu'ils ne doivent pas être utilisés pour se connecter sur des ressources (postes, serveurs, équipements réseau, etc.) de moindre sensibilité, ni pour exécuter des tâches susceptibles de divulguer ou d'exposer leurs secrets. Chaque usage inadapté ouvre une porte supplémentaire à un attaquant potentiel.

Par exemple, dans un SI reposant sur *Active Directory,* il est impossible d'éviter complètement la dissémination de certains secrets, même avec des technologies avancées (RWDCG/WDCG[3]) ou des mesures de durcissement sur NTLMv2 ou Kerberos.

L'un des objectifs principaux est donc de cloisonner les actions d'administration par niveau de sensibilité afin de garantir que les actions d'administration ainsi que leurs secrets restent confinés dans un périmètre maîtrisé. C'est l'objet de cette section, qui détaille pourquoi les ressources d'administration (postes et réseaux d'administration) doivent être dédiées aux actions d'administration.

[3] *Remote Windows Defender Credential Guard* **(RWDCG)** et *Windows Defender Credential Guard* **(WDCG)** sont des mécanismes de protection des identifiants d'authentification visant à empêcher leur exposition et leur vol lors de compromissions locales ou d'accès à distance.

[4] **AVEC :** Apportez Votre Equipement de Communication (ou *BYOD* en anglais *« Bring Your Own Device »)*

Postes et réseaux dédiés à l'administration

Toutes les actions d'administration doivent être réalisées sur des **postes d'administration et des réseaux d'administration physiquement dédiés,** conçus uniquement pour l'administration et utilisés exclusivement à cette fin.

En effet, utiliser les réseaux et les postes pour d'autres activités (ex : production, bureautique) augmente la surface d'attaque du SI d'administration et donc le risque de compromission. Nous verrons dans le chapitre « Mutualisation des ressources » qu'il est possible **sous condition** d'utiliser des ressources non dédiées à l'administration.

Un administrateur doit savoir **où il peut utiliser son compte, avec quels outils et dans quel contexte**, sans jamais avoir d'usages sensibles sur des environnements non maîtrisés. Par exemple, il n'utilise pas un compte d'administration depuis un poste utilisé pour l'accès à Internet ou la bureautique ou depuis un poste non maitrisé par l'entité (AVEC[4]).

Chaque administrateur dispose idéalement d'un **poste d'administration unique**, correspondant au plus haut niveau de sensibilité autorisé pour ses comptes. Ce poste est utilisé pour l'ensemble des actions d'administration et permet, si nécessaire, de **se connecter à distance à d'autres machines de même sensibilité ou de sensibilité inférieure avec les secrets de cette zone moins sensible** (par exemple via RDP, ou outils équivalents). Néanmoins, il est recommandé que la connexion à des ressources moins sensibles soit **prise en compte dans une analyse de risque**, en considérant l'apparition fréquente de vulnérabilités sur les outils de connexion (RDP, navigateur [HTML5], etc.).

Dans certains cas particuliers, comme l'administration de zones très sensibles ou ayant une plus forte exposition, ou lors de l'utilisation d'outils d'administration non mutualisables, il est nécessaire d'utiliser des postes d'administration dédiés à ces activités. Il est d'autant plus important que ces postes n'aient pas d'accès à Internet. Cela permet d'éradiquer les risques liés à l'hameçonnage (*phishing*), aux logiciels et aux macros malveillantes, ou à l'exploitation d'un navigateur vulnérable depuis un environnement bureautique. En particulier, l'utilisation d'un poste d'administration dédié, sécurisé et sans accès Internet est nécessaire pour les tâches suivantes :

- **l'administration du cœur de confiance / Tier 0**, par exemple les contrôleurs de domaine d'*Active Directory* (cf. Sécurité des annuaires) ;
- **d'autres tâches d'administration spécifiques et sensibles**, selon le périmètre.

L'administration des ressources *cloud* constitue un cas particulier. Contrairement à l'administration de ressources internes, elle nécessite généralement un accès à Internet pour joindre les portails d'administration, les API des fournisseurs ou les services d'authentification fédérée.

Pour limiter les risques liés aux attaques par relai, MITM[5] ou autres intrusions, le **réseau d'administration doit être physiquement dédié à l'administration**. Un réseau physiquement dédié permet d'empêcher qu'un attaquant capable de pivoter d'un réseau X vers un réseau Y puisse atteindre le réseau d'administration si celui-ci n'est pas physiquement isolé.

Le réseau d'administration doit être **segmenté et isolé** par sensibilité ou par service (par exemple à l'aide d'un réseau local virtuel – VLAN).

Enfin, les flux sur les réseaux d'administration doivent être **contrôlés et filtrés au strict nécessaire**. Ces « exigences » sont expliquées dans la fiche « Architectures sécurisées », de la collection « ReCyF en pratique », notamment la partie « Filtrage ». Par exemple, deux ressources administrées à l'aide d'une interface dédiée (par exemple, deux serveurs) ne doivent pas pouvoir communiquer entre elles par le réseau d'administration. Elles ne doivent pouvoir recevoir que des connexions initiées depuis des ressources d'administration (par exemple, des postes d'administration).

De la même manière, la prise de contrôle d'un équipement réseau, comme un switch ou un routeur, pourrait permettre à un attaquant d'accéder à des données sensibles si d'autres précautions n'ont pas été prises. Il est donc essentiel de protéger les flux d'administration contre des interceptions et altérations.

Afin de protéger les flux d'administration en confidentialité, intégrité et authenticité, les communications associées à des actions d'administration doivent être protégées par des mécanismes de chiffrement et d'authentification conformes à l'état de l'art. Des exemples de protocoles mettant en œuvre de tels mécanismes sont HTTPS, SFTP, IPSec ou *Secure Channel* (Microsoft). Le guide relatif aux mécanismes cryptographiques propose des recommandations concernant le choix (algorithme et mode) et le dimensionnement (taille des clés) des mécanismes cryptographiques. Ce guide peut servir de référence afin de configurer correctement les protocoles mettant en œuvre les mécanismes de chiffrement et d'authentification.

Si le recours à des mécanismes de chiffrement ou d'authentification est impossible au niveau du protocole d'administration, l'entité doit mettre en œuvre des mesures permettant de protéger la confidentialité et l'intégrité de ces flux, et de renforcer le contrôle et la traçabilité des actions d'administration. Par exemple, l'encapsulation de données en clair dans un tunnel chiffré (ex : IPSec ou protocole équivalent).

Lorsque la ressource administrée (serveur, service, etc.) le permet, il est recommandé d'utiliser une **interface réseau dédiée à l'administration**. Si une **interface réseau dédiée** est mise en place pour un serveur ou un service, il est nécessaire de **désactiver toute possibilité d'administration via d'autres interfaces**, comme une carte réseau de production, afin d'éviter toute exposition accidentelle.

Enfin, toutes ces ressources d'administration doivent être **administrées par l'entité elle-même ou par un prestataire formellement mandaté**, afin de garantir leur contrôle et leur sécurité.

[5] *Man in the middle*, ou homme du milieu. Type d'attaque dans lequel un adversaire se place au milieu d'un échange réseau pour en intercepter et parfois modifier les paquets échangés.

Mutualisation des ressources

Dans certains environnements, des contraintes rendent le déploiement de **postes d'administration** et de **réseaux d'administration physiquement** dédiés partiel ou impossible.

Ces contraintes peuvent être techniques ou opérationnelles, et les exceptions qu'elles entrainent doivent être justifiées. Exemples de contraintes empêchant le déploiement de postes ou de réseaux dédiés :

- Des contraintes techniques :
  → une ressource n'offrant qu'une seule interface réseau, qui sert à la fois au trafic applicatif et aux actions d'administration (ex : automate programmable ne disposant que d'une interface réseau physique sans possibilité de créer des interfaces virtuelles) ;
  → un serveur ou un service ne supportant pas l'interface d'administration dédiée, où l'administration se fait par l'interface de production (ex : *Active Directory*).

- Des contraintes opérationnelles :
  → des effectifs d'administration limités, ne permettant pas de maintenir un parc de postes d'administration dédiés pour chaque niveau de sensibilité ;
  → des moyens financiers ou emplacements physiques limités.

Pour le **réseau d'administration** qui serait non dédié à ces usages, la sécurité doit être renforcée sur le plan **logique** en mettant en œuvre des mesures de réduction du risque conformes aux recommandations de l'ANSSI. En particulier, les éléments suivants constituent un socle minimal et doivent être mis en place :

- Une séparation logique, par exemple :
  → réseau VPN IPSec dédié ;
  → VLAN ou segmentation équivalente ;
  → interface réseau virtuelle d'administration sur les ressources administrées.

- Une gestion stricte des règles de pare-feu, par exemple :
  → règles « Interdit » (« *Deny* ») explicites entre machines ;
  → règles d'autorisation des flux strictement nécessaires entre réseaux.

À défaut d'un **poste d'administration** physiquement dédié (**R**), l'entité doit au minimum suivre l'une des recommandations alternatives (R-) du guide Recommandations relatives à l'administration sécurisée des SI, à savoir :

- **Utiliser un poste d'administration multi-environnement (R-)** : à défaut d'un poste d'administration physiquement dédié, l'emploi de technologies de virtualisation ou de conteneurisation pour obtenir un système multi-environnement peut être envisagé, dans la mesure où le cloisonnement des environnements est réalisé par des mécanismes évalués comme étant de confiance au niveau système.

- **Utiliser un poste d'administration avec accès distant au SI bureautique (R--)** : À défaut d'un poste d'administration physiquement distinct du poste bureautique ou d'un système multi-environnement de confiance, une solution d'un niveau de sécurité moindre peut consister à ce que les administrateurs :
  → utilisent un poste physique pour les actions d'administration ;
  → accèdent, par connexion à distance uniquement, à leur environnement bureautique (physique ou virtuel, par exemple : *Virtual Desktop Infrastructure*) depuis ce poste d'administration.

Dans ce cas, les fonctions permettant un échange d'informations entre les deux environnements doivent être désactivées.

SÉCURITÉ DES ANNUAIRES

Mesures ReCyF

Objectif de sécurité 11
Maîtrise de l'administration des systèmes d'information
- Sécurité des annuaires : 11.B.1-EI/EE, 11.B.2-EE, 11.B.3-EE, 11.B.4-EE, 11.B.5-EE, 11.B.6-EE, 11.B.7-EE

La sécurité d'un SI dépend en grande partie de la protection de l'annuaire (par exemple *Active Directory*) qui gère les utilisateurs, les machines et les ressources du SI.

Autour de cet annuaire, on trouve un ensemble de ressources, qu'il s'agisse de composants techniques, logiciels ou de comptes à privilèges, capables directement ou indirectement de prendre le contrôle (appelé « chemin de contrôle ») de cet annuaire et donc de prendre le contrôle du SI. Cet ensemble forme ce que l'on appelle le **cœur de confiance**[6].

Si un attaquant parvient à prendre le contrôle d'un seul de ces éléments, il obtient potentiellement la capacité d'administrer l'ensemble de ce SI.

Dans des environnements où cohabitent plusieurs systèmes d'information distincts, chacun disposant de son propre système de gestion des identités, il en résulte nécessairement **plusieurs** cœurs de confiance.

[6] Cette définition est utilisée presque exclusivement dans le référentiel ReCyF. Dans la littérature usuelle, le cœur de confiance s'étend aux équipements susceptibles de prendre le contrôle du système d'information : consoles antivirus, serveurs de mise à jour, serveurs SCADA, etc. La description détaillée de ce « véritable » cœur de confiance est disponible dans la publication ANSSI sur l'identification du cœur de confiance.

Périmètre et identification du cœur de confiance

Le cœur de confiance dans ReCyF correspond initialement aux annuaires et s'étend à **l'ensemble des ressources qui peuvent prendre le contrôle** vers ces annuaires.

Ces chemins de contrôle regroupent tout ce qui permet d'administrer l'annuaire, mais aussi tout ce qui peut intercepter, manipuler ou élever les privilèges des comptes qui l'administrent. Dès qu'un élément (compte, serveur, service ou équipement) peut influencer ou compromettre l'annuaire principal, il entre ainsi dans le cœur de confiance. Ce périmètre doit être clairement identifié et documenté en répertoriant et catégorisant l'ensemble des ressources.

L'identification est une démarche itérative : en partant d'un annuaire, on identifie les ressources directement ou indirectement capables de prendre le contrôle (appelé « chemin de contrôle ») de cet annuaire. Ces ressources sont intégrées au périmètre du cœur de confiance. On recommence alors le processus en cherchant d'autres ressources capables de prendre le contrôle des premières.

Dans un environnement *Active Directory*, le cœur de confiance correspond typiquement au **Tier 0**.

Les chemins de contrôle (les exemples « non-gras » sont donnés pour un environnement Active Directory) incluent au minimum :
- **Le ou les annuaires principaux du SI :**
  → contrôleurs de domaine Active Directory de production.

- **Les machines qui hébergent ou contrôlent techniquement l'annuaire :**
  - → hyperviseurs hébergeant les contrôleurs de domaine ;
  - → serveurs de sauvegarde capables de restaurer ou d'écraser les données de l'annuaire ;
  - → systèmes de gestion à distance qui peuvent redémarrer, provisionner ou modifier les hôtes de l'annuaire (avec ou sans agent local).

- **Les comptes ayant un pouvoir direct sur l'annuaire :**
  - → comptes administrateurs du domaine ou de la forêt ;
  - → comptes capables d'administrer les serveurs hébergeant l'annuaire (administrateurs « *Builtin* » des contrôleurs de domaine, comptes administrateur hyperviseur, comptes de sauvegarde, etc.) ;
  - → un compte de service membre du groupe « Administrateurs du domaine », ainsi que le serveur sur lequel il est utilisé.

- **Les postes et outils utilisés pour administrer l'annuaire :**
  - → postes d'administration Tier 0 ;
  - → les équipements réseaux utilisés pour administrer le cœur de confiance (switch ou pare-feux par lesquels transitent les flux d'administration).

- **Les services d'infrastructure et d'identité liés à l'annuaire :**
  - → IGC[7] interne émettant les certificats utilisés par AD ou ses services critiques ;
  - → serveur de fédération d'identité (AD-FS).

Des exemples de scénarios de compromission illustrant la nécessité de rattacher ces ressources au cœur de confiance :

- un attaquant **contrôlant l'hyperviseur** peut monter le disque d'un contrôleur de domaine et extraire la base NTDS, lui permettant de dérouler des scénarios d'attaque hors ligne ;
- un attaquant **contrôlant un serveur de sauvegarde** peut restaurer un contrôleur de domaine piégé ;
- la compromission d'un serveur ou d'un poste utilisateur contenant les **secrets** d'un compte membre « **administrateurs du domaine** » ou équivalent, permet d'obtenir des privilèges complets sur l'annuaire.

Une fois l'identification du cœur de confiance réalisée, il est essentiel de réduire autant que possible la taille du cœur de confiance. Étant donné le niveau d'exigence associé à ce périmètre, toute ressource ne nécessitant pas objectivement d'y appartenir doit en être retirée. Par exemple, un serveur SQL configuré avec un compte de service membre « d'administrateurs du domaine » doit être modifié, car son fonctionnement ne requiert pas de privilèges aussi élevés. Une fois ce chemin de contrôle supprimé, ces ressources peuvent être retirées du cœur de confiance.

Sécurisation du cœur de confiance

Tous les éléments du cœur de confiance doivent être configurés et administrés conformément aux recommandations de l'ANSSI, lorsque celles-ci existent.

C'est la composition du cœur qui détermine les recommandations à appliquer. Par exemple, lorsque le cœur de confiance possède des annuaires Active Directory, les *Recommandations pour l'administration sécurisée des SI reposant sur AD* doivent être appliquées. L'outil d'analyse de configuration « *ORADAD*[8] » peut également être utilisé pour récupérer l'état de l'AD, et les recommandations de l'outil doivent être suivies en prenant soin de comprendre les impacts de la remédiation et de mettre en place les projets adaptés.
Le cœur de confiance faisant parti du SI, des recommandations plus globales sont applicables à celui-ci telles que : les recommandations de gestion d'incident, de sauvegarde, de virtualisation, etc., mais également les autres fiches de la collection « ReCyF en pratique » de l'ANSSI.

Pour maintenir un cœur de confiance sain, une revue complète de la configuration de tous les annuaires du ou des cœurs de confiance doit être effectuée **au moins une fois par an**.

[7] Infrastructure de Gestion de Clés (*Public Key Infrastructure* [PKI] en anglais)

[8] ORADAD est un outil qui est utilisable par les entités ayant accès au service « *Active Directory Security* » (ADS), du portail *Club SSI* de l'ANSSI. En effet, cet accès est nécessaire afin d'importer le relevé de configuration et d'obtenir un rapport contenant les résultats de l'analyse de cette configuration.

Idéalement, cette revue s'appuie sur un outil automatisé afin de garantir une vision exhaustive et objective. Des outils open source comme l'outil d'analyse de configuration « *ORADAD* » de l'ANSSI, ou encore des outils commerciaux ou communautaires peuvent être utilisés pour réaliser cette revue.

Cette revue doit permettre d'identifier, a minima :

- les objets obsolètes ;
- les délégations abusives ou inutiles ;
- les comptes inactifs ou dormants ;
- les chemins de contrôle ;
- les appartenances injustifiées à des groupes à privilèges.

Ces vérifications facilitent la mise en place de mesures correctives, réduisant la surface d'attaque globale du SI (désactivation de comptes inactifs, retrait de privilèges excessifs, gestion des serveurs obsolètes, etc.).

Enfin, les annuaires doivent recevoir les correctifs de **sécurité « sans retard injustifié »**, afin de limiter au maximum leur exposition aux vulnérabilités connues. Ces correctifs, dans la plupart des cas, ne nécessitent pas de redémarrage du serveur et sont essentiels pour la sécurité.

La notion de **« sans retard injustifié »** signifie que les mises à jour doivent être appliquées dès qu'elles sont disponibles, sauf lorsqu'un report est nécessaire pour des raisons techniques réelles et proportionnées au risque. Elle exclut les retards liés à la négligence, au manque de moyens ou d'organisation, ou liés à des arbitrages non justifiés. Un retard peut être justifié par :

- Une contrainte technique empêche l'application immédiate du correctif :
  - → le correctif impacte un composant critique du système d'authentification (AD DS, AAD Connect, RADIUS, IGC) et nécessite une validation préalable à son déploiement ;
  - → le patch corrige une faille mais introduit un dysfonctionnement connu sur certaines plateformes matérielles, obligeant l'entité à attendre un correctif complémentaire.

- Une fenêtre de maintenance validée n'est pas immédiatement disponible :
  - → certaines entités ne peuvent mettre à jour leur cœur de confiance qu'en période d'arrêt planifié (nuit, week-end, période creuse), pour éviter toute indisponibilité de l'authentification. Ce retard est justifié et acceptable si la mise à jour nécessite un redémarrage.

Administration du cœur de confiance

L'administration du cœur de confiance doit respecter des exigences strictes, car toute compromission d'un élément appartenant au cœur de confiance donnerait à un attaquant la capacité de prendre le contrôle globalement ou partiellement sur le SI, notamment lorsque celui-ci se repose sur *Active Directory*.

Les actions d'administration du cœur de confiance doivent être effectuées exclusivement :

- avec des comptes d'administration dédiés ;
- depuis des postes dédiés ;
- depuis des réseaux strictement réservés à l'administration du cœur de confiance, qu'ils soient physiques ou logiques.

Dès lors que des ressources d'administration (bastions, coffres-forts de mots de passe, serveurs de rebond, VPN[9], etc.) sont utilisées pour l'administration du cœur de confiance, elles entrent immédiatement dans le périmètre du cœur de confiance et doivent respecter les mêmes règles de sécurité. Ces ressources ne doivent servir qu'à l'administration du cœur de confiance, **sans exception**. Aucun poste ou compte dédié à l'administration du cœur de confiance ne doit être utilisé pour la bureautique ou l'administration de ressources hors cœur de confiance.

Ce principe garantit qu'une compromission d'un environnement de moindre sensibilité ne puisse être utilisée comme tremplin vers le cœur de confiance.

Pour renforcer ce cloisonnement, tous les flux provenant de l'extérieur du cœur de confiance et destinés aux ressources d'administration doivent être interdits. Cette interdiction est mise en œuvre notamment par :

- les règles du pare-feu local des postes et serveurs d'administration ;
- les règles des pare-feux inter-réseaux situés en bordure du réseau d'administration.

Ces flux sont également interdits lorsque le réseau d'administration est physiquement dédié.

[9] En français : Réseau Privé Virtuel

Système d'information d'administration

Lorsqu'une entité dispose de plusieurs cœurs de confiance au sein de ses systèmes d'information de production (SIP), elle peut mettre en place un ***« système d'information d'administration »*** (SIA) dédié à la **mutualisation des moyens d'administration**, comme illustré sur l'Image 2.

Par exemple, il peut exister plusieurs cœurs de confiance quand l'entité possède :

- plusieurs SI distincts avec chacun une forêt *Active Directory* ;
- plusieurs SI distincts indépendants hors *Active Directory* (par exemple : SI Industriel, SOC, hyperviseurs, etc.).

En raison de cette centralisation, le SIA présente un niveau de sensibilité particulièrement élevé. Il doit donc respecter un niveau de sécurité à l'état de l'art, et les recommandations alternatives (R-/ R--) **ne sont pas acceptables**.

Le SIA se caractérise par son autonomie complète vis-à-vis des systèmes administrés. Il dispose notamment de sa propre base d'identités et de mécanismes d'authentification indépendants, afin d'éviter toute dépendance aux systèmes d'information qu'il administre.

La mise en œuvre d'une telle architecture nécessite toutefois une analyse préalable du besoin réel. **Le SIA est déconseillé dans la majorité des situations**. En effet, s'il est mal maîtrisé, le SIA donne un faux sentiment de sécurité. Il est principalement adapté aux entités qui opèrent plusieurs systèmes d'information avec un fort besoin de mutualisation des ressources d'administration et ayant un niveau de **maturité élevé en matière de sécurité et d'administration.**

Les SIA sont des architectures complexes qui doivent être adaptées au contexte d'administration de l'entité. Ceci est expliqué dans le chapitre 5.3 « Mutualisation de l'administration de plusieurs forêts AD » du guide ANSSI *Recommandations pour l'administration sécurisée des SI reposant sur AD*.

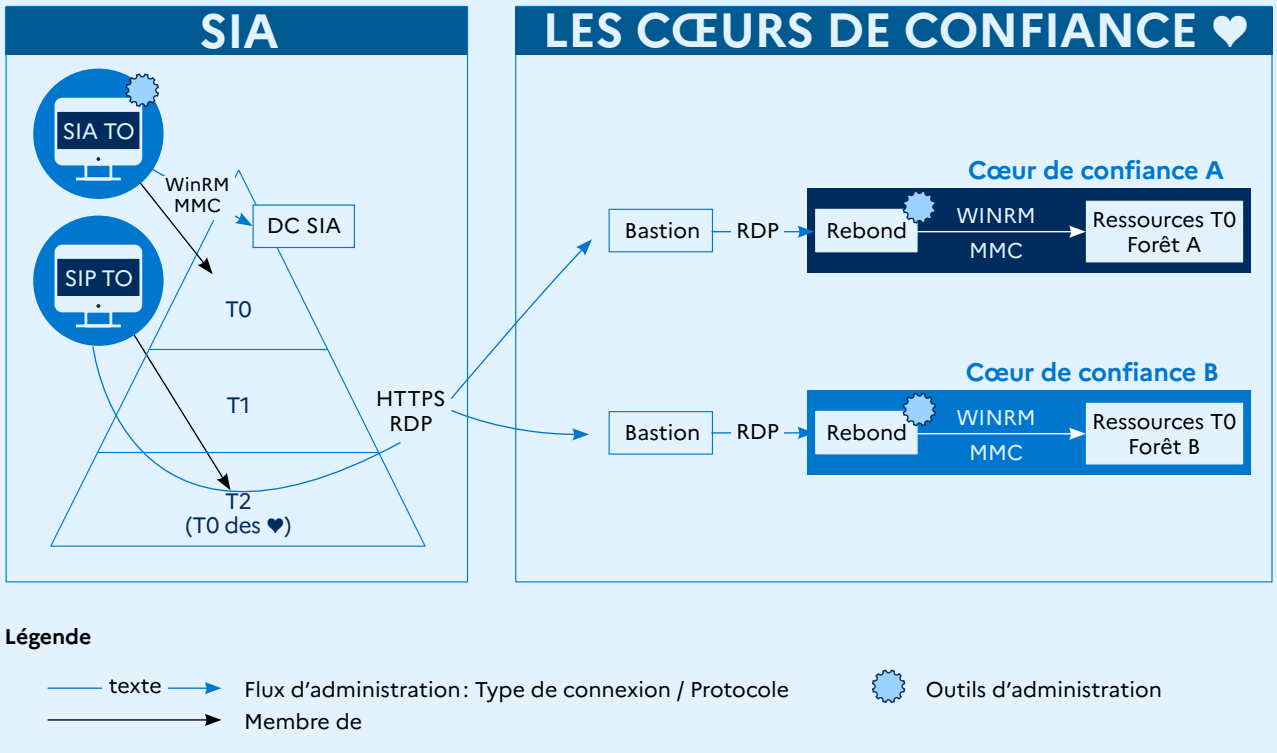
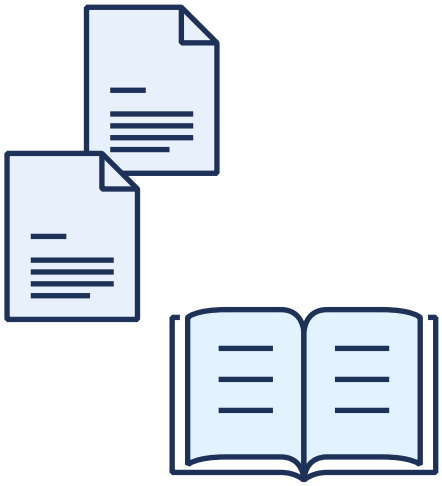


Image 2 : Représentation d'un exemple de SIA pour les cœurs de confiances

ANNEXES

Annexe 1: bibliographie



Documents ANSSI

- Recommandations pour l'administration sécurisée des SI reposant sur Active Directory
Consulter le lien

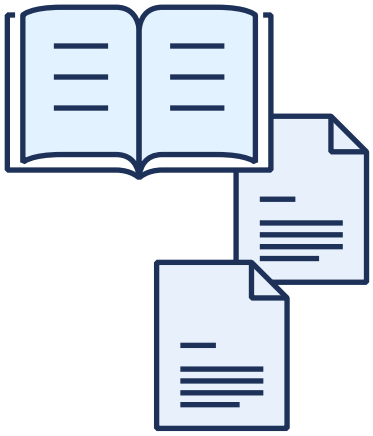
- Recommandations relatives à l'administration sécurisée des SI
Consulter le lien

- Mécanismes cryptographiques
Consulter le lien

- Recommandations de déploiement d'un service IAAS OpenStack SecNumCloud
Consulter le lien

- Piloter la remédiation d'un incident cyber
Consulter le lien

- Recommandations pour l'hébergement des SI sensibles dans le cloud
Consulter le lien



Documents éditeurs

- Implémentation de modèles d'administration selon le principe des privilèges minimum
Consulter le lien (Français)
Consulter le lien (Anglais)

- Groupes de sécurité Active Directory
Consulter le lien (Français)
Consulter le lien (Anglais)

Outils et scripts

- ORADAD de l'ANSSI
Consulter le lien

Annexe 2 : extrait du glossaire ReCyF

Mesures ReCyF	Définition
Action d'administration	Installation, suppression, modification ou consultation d'une configuration d'une ressource d'un système d'information susceptible de modifier le fonctionnement ou la sécurité de celui-ci.
Administrateur	Personne physique disposant de droits privilégiés sur un système d'information, chargée des actions d'administration ou de maintenance sur celui-ci, responsable d'un ou plusieurs domaines techniques.
Annuaire	Ressource logicielle centralisant des informations relatives aux utilisateurs, et parfois aux autres ressources d'un système d'information et fournissant des mécanismes d'identification et d'authentification. *Par exemple : Microsoft Active Directory, OpenLDAP.*
Compte d'administration	Compte disposant de privilèges nécessaires aux actions d'administration. Il peut être partagé, individuel ou de service.
Dispositif de détection	Ensemble de ressources matérielles ou logicielles capables d'identifier des indicateurs de compromission et techniques d'attaques, sur des données brutes réseau ou système, pour générer des évènements de sécurité. *Par exemple : sondes réseau, solutions EDR.*
Facteur d'authentification	Élément utilisé pour réaliser l'authentification d'un utilisateur ou d'un processus automatique, sur la base d'une information mémorisée (facteur de connaissance), d'un élément physique stockant un secret (facteur de possession) ou d'une caractéristique liée à une personne (facteur inhérent).
Interconnexion	Ressource logicielle ou matérielle rendant possible le transfert d'information entre deux systèmes d'information ou entre deux sous-systèmes par une continuité de signaux électromagnétiques. *Par exemple : câble réseau, diode optique.*
Mécanisme d'authentification	Mécanisme permettant d'authentifier un utilisateur ou un processus automatique préalablement à l'accès aux ressources des systèmes d'information. Ce mécanisme s'appuie au minimum sur un facteur d'authentification et peut mettre en œuvre une authentification multifacteur.
Règle de filtrage	Instruction implémentée au sein d'un dispositif de filtrage (par exemple : un pare-feu) visant à autoriser ou interdire les flux de données en fonction : ▸ De l'adresse IP source ou destination ; ▸ Du protocole utilisé par le flux de données (par exemple : TCP ou UDP) ; ▸ Des numéros de port source ou destination (par exemple : TCP/23) ▸ De l'applicatif.
Réseau	Ensemble de ressources interconnectées permettant de communiquer au sein d'un ou plusieurs systèmes d'information.
Réseau d'administration	Réseau dédié physiquement ou logiquement aux flux internes à ce réseau et les flux d'administration vers les systèmes d'information.
Sous-système	Ensemble de composants d'un système d'informations constitués pour assurer une fonctionnalité ou un ensemble homogène de fonctionnalités d'un système d'information ou encore pour isoler des ressources d'un système d'information ayant un même besoin de sécurité.
Système d'analyse	Système d'information exploitant les événements de sécurité à la recherche d'indicateurs de compromission et de techniques d'attaques, dans le but d'identifier des incidents de sécurité.
Système d'information	Ensemble des infrastructures et services logiciels informatiques relevant de la responsabilité de l'entité, permettant de collecter, traiter, transmettre et stocker sous forme numérique les données. Les ressources informatiques partagées ou mutualisées avec des tiers relevant du périmètre de responsabilité de l'entité, sont considérées comme faisant partie intégrante des systèmes d'information de l'entité, et sont à ce titre pleinement assujetties aux obligations de la directive NIS 2.
Système d'information d'infrastructure	Système d'information généraliste utile aux activités ou aux services de l'entité, ou nécessaire au fonctionnement de plusieurs systèmes d'information de l'entité. *Par exemple : annuaire, messagerie, téléphonie, service de résolution de nom de domaine.* Un système d'information d'infrastructure peut être un système d'information.
Systèmes d'information tiers	Système d'information ou ressource informatique partagée ou mutualisée avec l'entité qui n'est pas sous la responsabilité de l'entité. *Point d'attention : lorsque l'entité externalise tout ou partie de son système d'information, ce dernier reste sous sa responsabilité et n'est donc considéré comme un SI tiers au sens du présent référentiel.*
Utilisateur	Personnels de l'entité et prestataires agissant pour le compte de l'entité qui accèdent aux systèmes d'information.