Le modèle de sécurité windows

Cours Windows 2008-2009

Franck Rupin - Laurent Gydé

Le modèle de sécurité windows

1 Généralités

2 Les composants du système de sécurité

3 La protection des objets

4 Audit de sécurité

1 Généralités

Pourquoi la sécurité sur un système d'exploitation :

Protéger l'accès à des données sensibles comme par exemple :

- Résultats de recherche
- Secrets industriels
- Secret médical
- Gestion du personnel

1 Généralités

La sécurité d'un système d'exploitation va reposer sur des mécanismes de base :

Couple login/mot de passe
Accès contrôlé aux objets via des listes de contrôle d'accès (ACL)

Mais aussi sur des mécanismes plus élaborés :

Droits et privilèges
Avoir un contrôle sur les actions des programmes

1 Généralités

Normes de sécurité

L'établissement de normes internationales en matière de sécurité des systèmes d'exploitation, permet de classifier ces derniers, en fonction de caractéristiques normalisées.

Par exemple, la norme Critères Communs (CC) permet une évaluation des fonctionnalités de sécurité répondant à certaines spécifications.

1 Généralités

La création de niveau de sécurité permet d'indiquer le degré de protection du système d'exploitation.

Les niveaux de sécurité TCSEC (Trusted Computer System Evaluation Criteria)

A1	Conception vérifiée
B3	Domaines de sécurité
B2	Protection structurée
B1	Protection de sécurité labellisée
C2	Protection d'accès contrôlé
C1	Protection d'accès discrétionnaire
D	Protection minimale

1 Généralités

L’utilisation de cette norme dans les systèmes informatiques de la défense et du gouvernement est obligatoire aux Etats-Unis.

Aucun système n'a atteint la norme A1 et le niveau C2 est considéré comme suffisant comme pour un système d'exploitation généraliste.

Windows est C2 et répond en plus a des exigences de niveau B

1 Généralités

Exigences de niveau C2 :

Ouverture de session sécurisée : identification des utilisateurs, accès utilisateur après authentification.

Contrôle d'accès discrétionnaire : le propriétaire d'une ressource, en contrôle l'accès.

Audit de sécurité : détection et journalisation d'événements de sécurité.

Protection contre la réutilisation d'objets : un utilisateur ne peut pas accéder à des données (fichier emplacement mémoire...) qu'un autre utilisateur a supprimé (réinitialisation des objets avant utilisation).

1 Généralités

Fonctionnalités de niveau B de Windows :

Fonctionnalité de chemin approuvé : la séquence ctrl+alt+suppr n'est pas interceptable.

Administration approuvée : rôles administratifs distincts (admin, opérateurs de sauvegarde...)

1 Généralités

Critères Communs (CC)

La norme CC est une norme plus souple que la norme TCSEC.

Dans cette norme on introduit le concept de **Protection Profile** (PP).

PP regroupe des contraintes de sécurité dans des ensembles faciles à spécifier et à comparer. Exprime le besoin sous forme standardisée.

ST (security target) correspond a un ou plusieurs PP et décrit de manière standard, l'utilité annoncée d'un produit de sécurité et des fonctionnalités qu'il fournit.

1 Généralités

Windows 2000 est certifié PP controled access (eq C2) + d'autres exigences CC :

Accès discrétionnaire basé sur des méthodes cryptographiques (EFS)

Stratégie de contrôle d'accès discrétionnaire pour les objets utilisateur (bureau fenêtres...) et active directory.

Système d'exploitation distribué : réplication multimaitre des données de sécurité

NTFS, winlogon (verrouillage de session interactives) IPSEC correction des failles.

2 Composants du système de securité

1 Généralités

2 Les composants du système de sécurité

3 la protection des objets

4 Audit de sécurité

2 Composants du système de securité

Cette partie s'attache à présenter les différents éléments qui participent au système de sécurité sous windows.

Le **SRM** : security reference monitor

Composant de l'exécutif.
Définit le jeton d'accès à présenter dans un contexte de sécurité (fichier, device, registre...).
Effectue les contrôles d'accès sur les objets.
Manipule les privilèges et les droits utilisateur.
Génère les messages d'audit de sécurité.

2 Composants du système de securité

LSASS : local security authority subsystem

Processus mode utilisateur

Chargé de la stratégie de sécurité du système local (stratégies de mots de passe, privilèges, groupes...)

2 Composants du système de securité

Base de données des stratégies LSASS :

Cette base de données, contient les paramètres de stratégie locale de sécurité : HKLM\SECURITY

Service SAM (security account manager) :

Chargé de la gestion de la base des comptes locaux.

2 Composants du système de securité

Base de données SAM :

Elle contient les informations de comptes locaux utilisateurs, groupes, login, mots de passe.

Correspond à la clé de registre : HKLM\SAM

2 Composants du système de securité

Active Directory :

Le service d'annuaire contient des informations sur les objets d'un domaine.

Active Directory est répliqué sur chaque ordinateur ayant le rôle de contrôleur de domaine.

Le serveur est exécuté dans LSASS.

2 Composants du système de securité

Packages d'authentification

Il s'agit de dll exécutées dans le contexte de LSASS.

Une dll d'authentification à la charge du contrôle du login/password lors de l'ouverture de session.

Et fournit à LSASS des informations sur l'identité de l'utilisateur.

LSASS génère un jeton d'accès à partir de ces informartions.

2 Composants du système de securité

Processus d'ouverture de session :

winlogon.exe

Processus qui s'exécute en mode utilisateur.

Chargé de répondre à la séquence SAS.

Chargé de gérer les sessions interactives.

Winlogon lance userinit sous l'identité de l'utilisateur.

2 Composants du système de securité

GINA (graphical identication and authentication) :

Dll mode utilisateur

Exécutée dans le contexte du processus winlogon

\windows\system32\msgina.dll

Cette dll est remplaçable (pgina par exemple http://www.pgina.org/ , authentification par carte à puce)

2 Composants du système de securité

Netlogon service d'ouverture de session réseau :

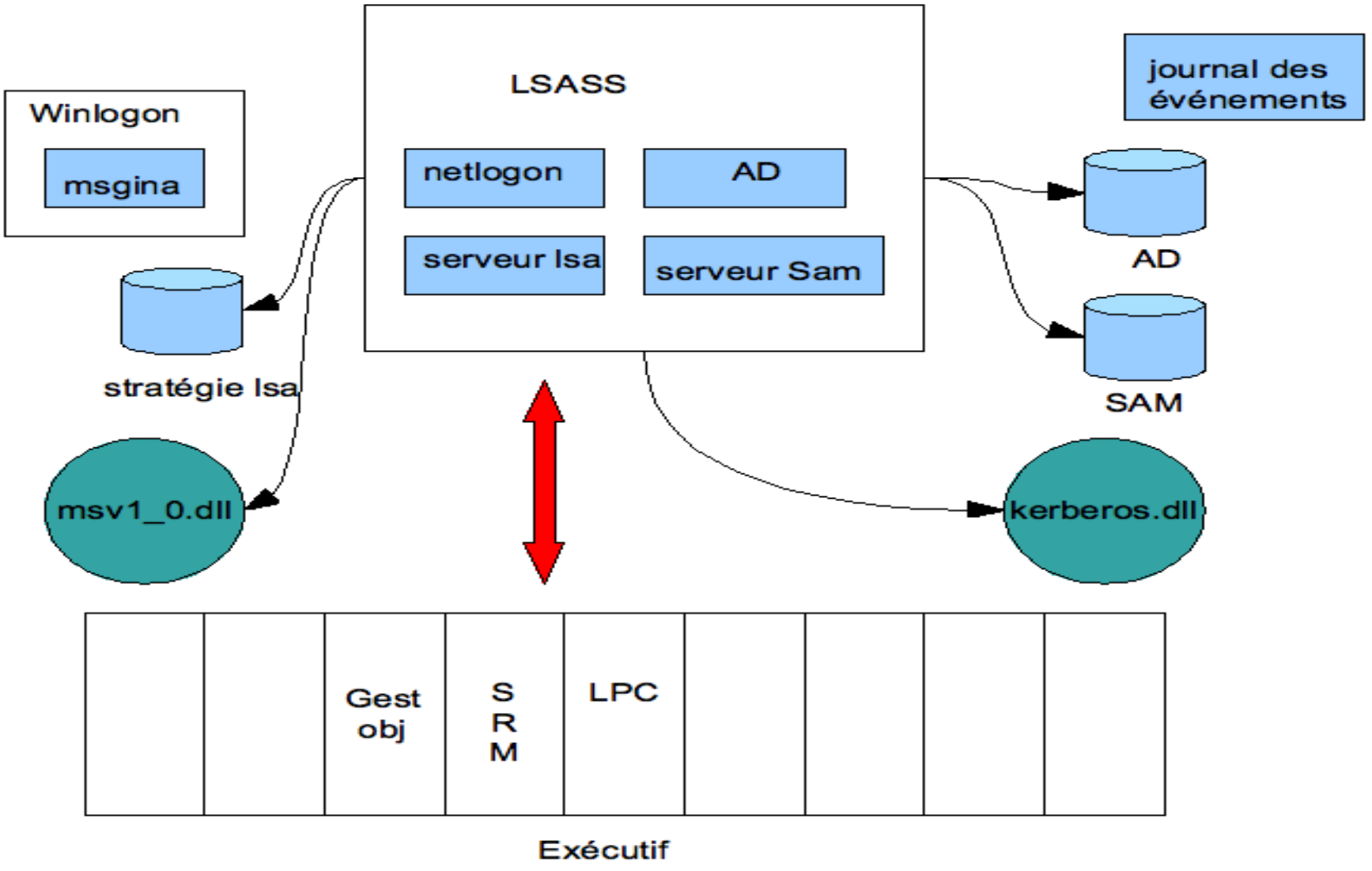
Service windows

Chargé de la création d'un canal sécurisé avec le contrôleur de domaine.

Les requêtes d'ouverture de session interactives transitent via ce canal.

2 Composants du système de securité

mode utilisateur



3 La protection des objets

1 Généralités

2 Les composants du système de sécurité

3 la protection des objets

4 Audit de sécurité

3 La protection des objets

Exemples d'objets pouvant être protégés :

Fichiers, périphériques
Processus, threads
Mutex, semaphores, section de mémoire partagée
Ports LPC, timers, jetons d'accès
Bureaux, fenêtres
Partages réseau, objets Active Directory

3 La protection des objets

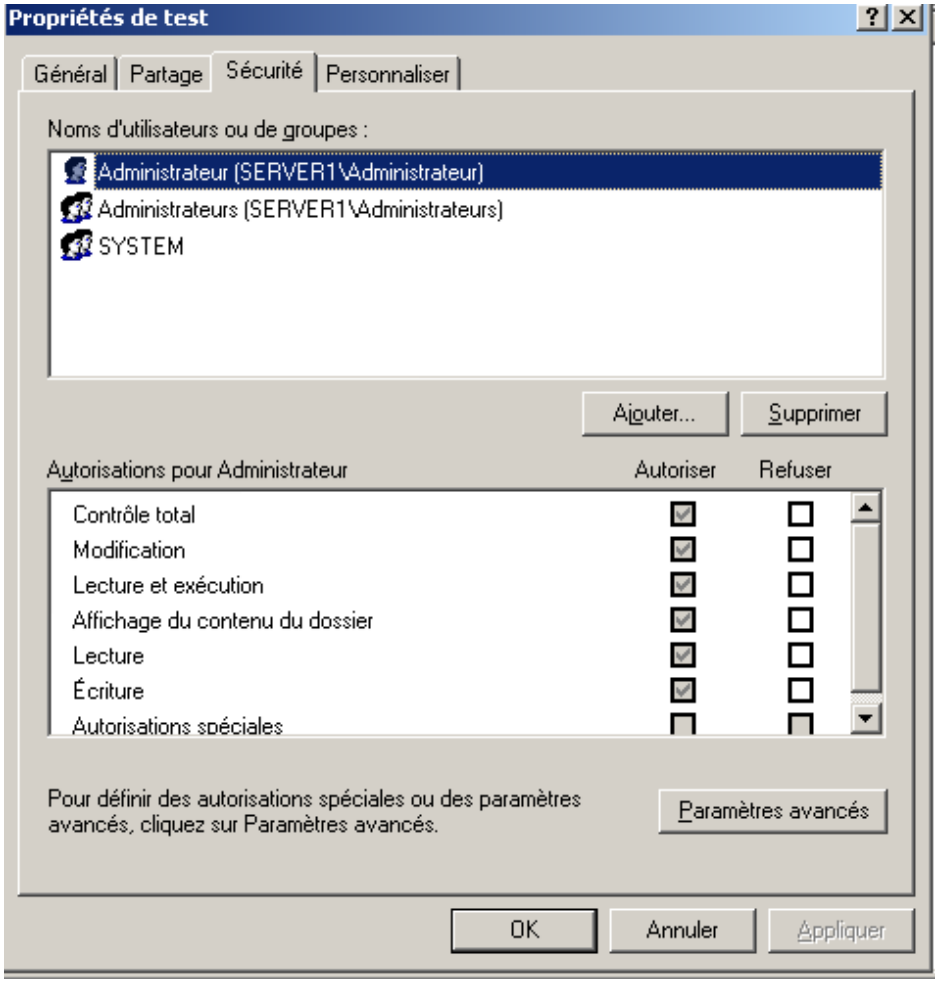
Grâce au model de sécurité de windows, des objets de nature très différente ont en commun :

Le contrôle d'accès
L'audit

Les vues suivantes montrent l'interface standard des objets.

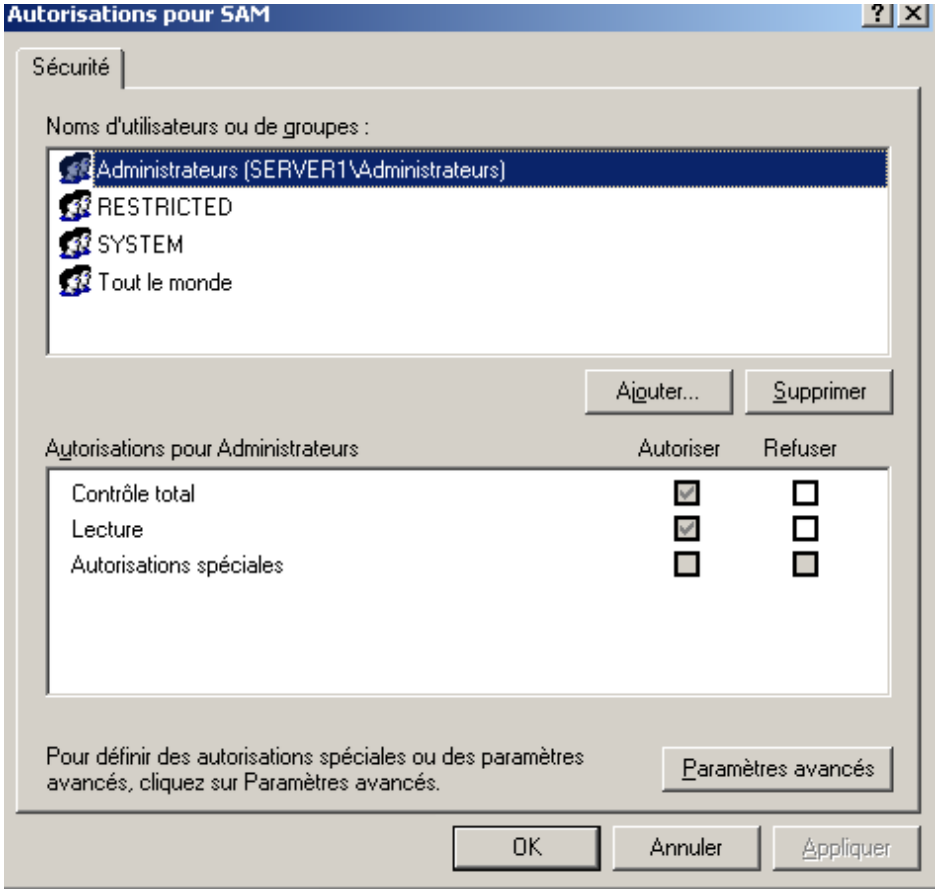
3 La protection des objets

- Liste de contrôle d'accès d'un répertoire



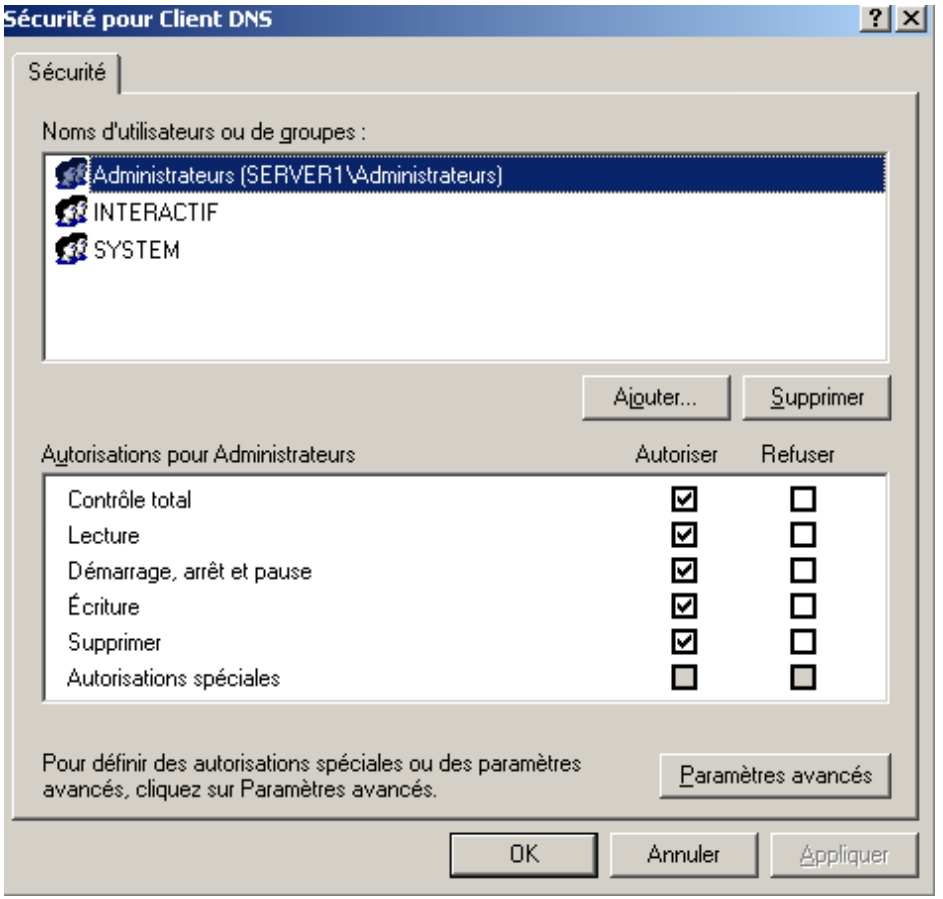
3 La protection des objets

- Liste de contrôle d'accès d'une clé de registre



3 La protection des objets

•Liste de contrôle d'accès d'un service



3 La protection des objets

Le modèle de sécurité est basé sur trois éléments fondamentaux :

L'identité d'un thread
L'accès demandé par le thread pour un objet
Les paramètres de sécurité de l'objet.

Le résultat du contrôle d'accès est oui ou non, selon que le système de sécurité accorde ou non l'accès.

3 La protection des objets

Le SID (security identifier)

Le SID représente dans le modèle de sécurité windows, un identifiant unique, permettant de distinguer une entité effectuant une action.

Un SID, permet d'identifier, des utilisateurs, des groupes, des ordinateurs, des domaines.

exemple de SID : **S-1-5-21-01234567-89012345-67890123-1033**

3 La protection des objets

Les SID sont générés aléatoirement à l'installation du système, pour :

L'ordinateur
Les comptes locaux

Un compte local est basé sur le SID de la machine + un RID (relative identifier)

3 La protection des objets

Structure d'un SID :

S : la chaine est un SID
1 : numéro de révision
5 : identifiant d'autorité (5 = NT authority)
21-01234567-89012345-67890123 : identifiant de la machine ou du domaine
1033 : RID identifie le groupe ou l'utilisateur.

3 La protection des objets

L'outil dcpromo permet lui aussi de générer des SID, c'est notamment le cas, lors de la création d'un nouveau domaine.

Le système gère des SID prédéfinis pour des groupes ou des comptes

3 La protection des objets

SID bien connus :

S-1-5-18 : local system
S-1-5-20 : network service
S-1-5-21-domain-500 : administrateur
S-1-5-21-domain-512 : administrateurs du domaine
S-1-5-21-domain-513 : utilisateurs du domaine

3 La protection des objets

Jetons d'accès :

C'est la première structure de données du mécanisme de contrôle d'accès.

Un jeton d'accès est utilisé par le SRM pour identifier le contexte de sécurité d'un processus ou d'un thread.

Un contexte de sécurité, décrit les groupes, les comptes, les privilèges du processus ou du thread.

3 La protection des objets

À l'ouverture de session, winlogon, crée un jeton représentant l'utilisateur, et l'attache à userinit.

Userinit transmet ce jeton, à tous les processus qu'il est chargé de créer.

Le SRM va utiliser les SID contenus dans le jeton pour déterminer si l'accès à un objet est autorisé ou non.

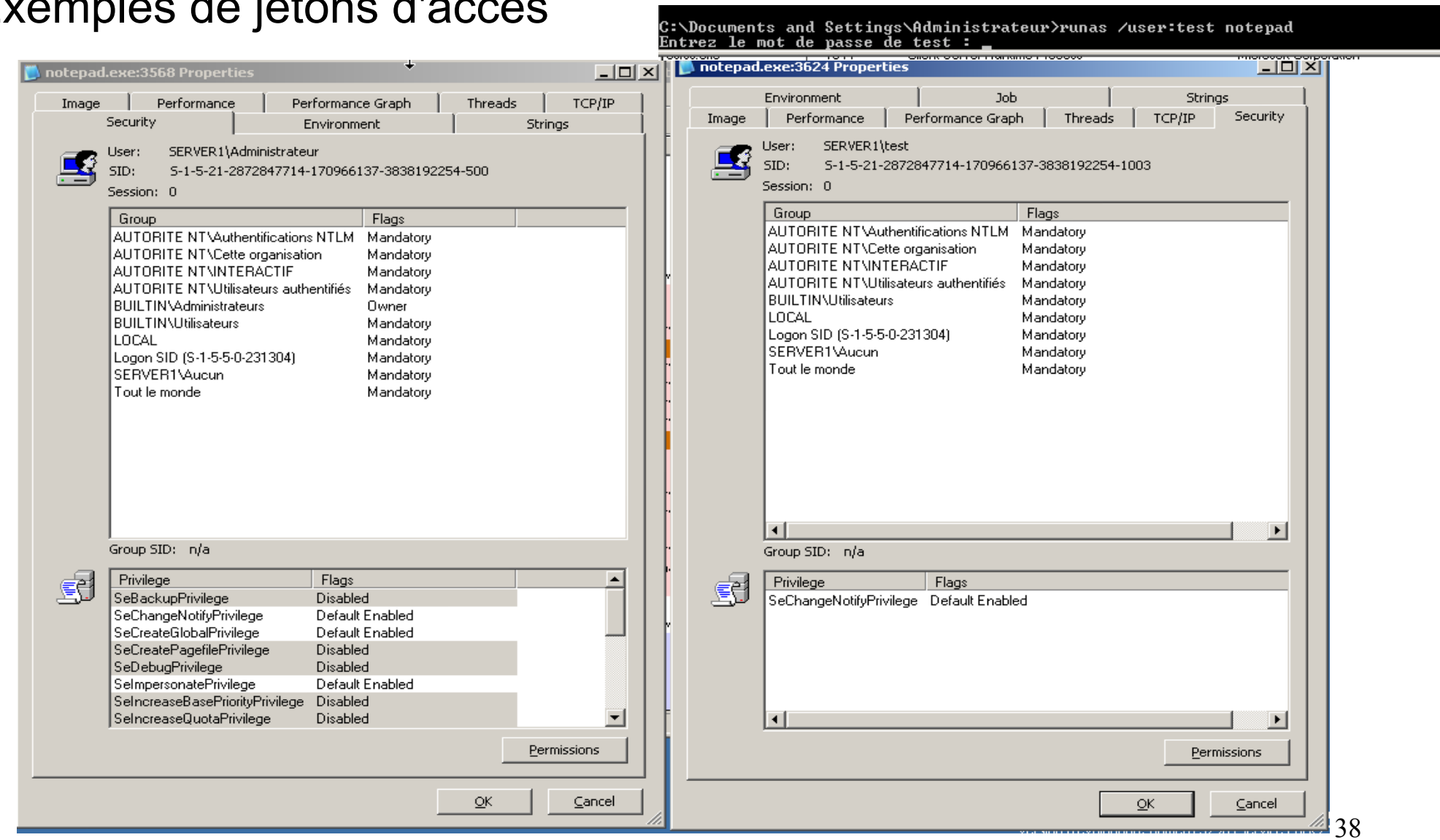
3 La protection des objets

Contenu d'un jeton :

Source du jeton	:	entité de création du jeton
Type du jeton	:	principal ou emprunt d'identité
ID	:	identifiant assigné par le SRM
ID d'auth	:	indique à quelle session interactive appartient le jeton
SID groupe	:	indique les groupes d'appartenance

3 La protection des objets

Exemples de jetons d'accès



3 La protection des objets

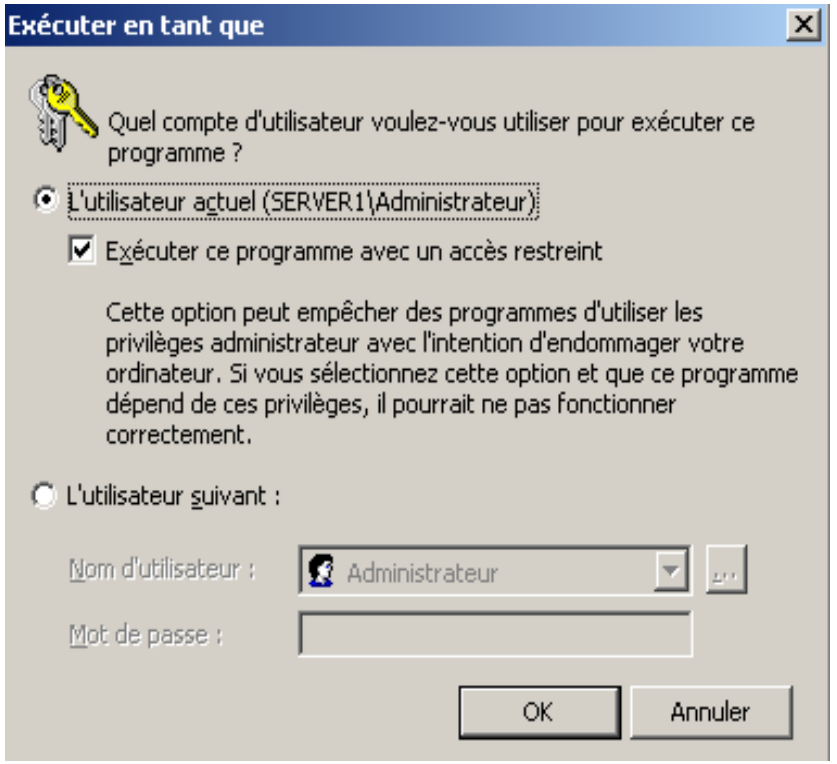
Jeton restreint :

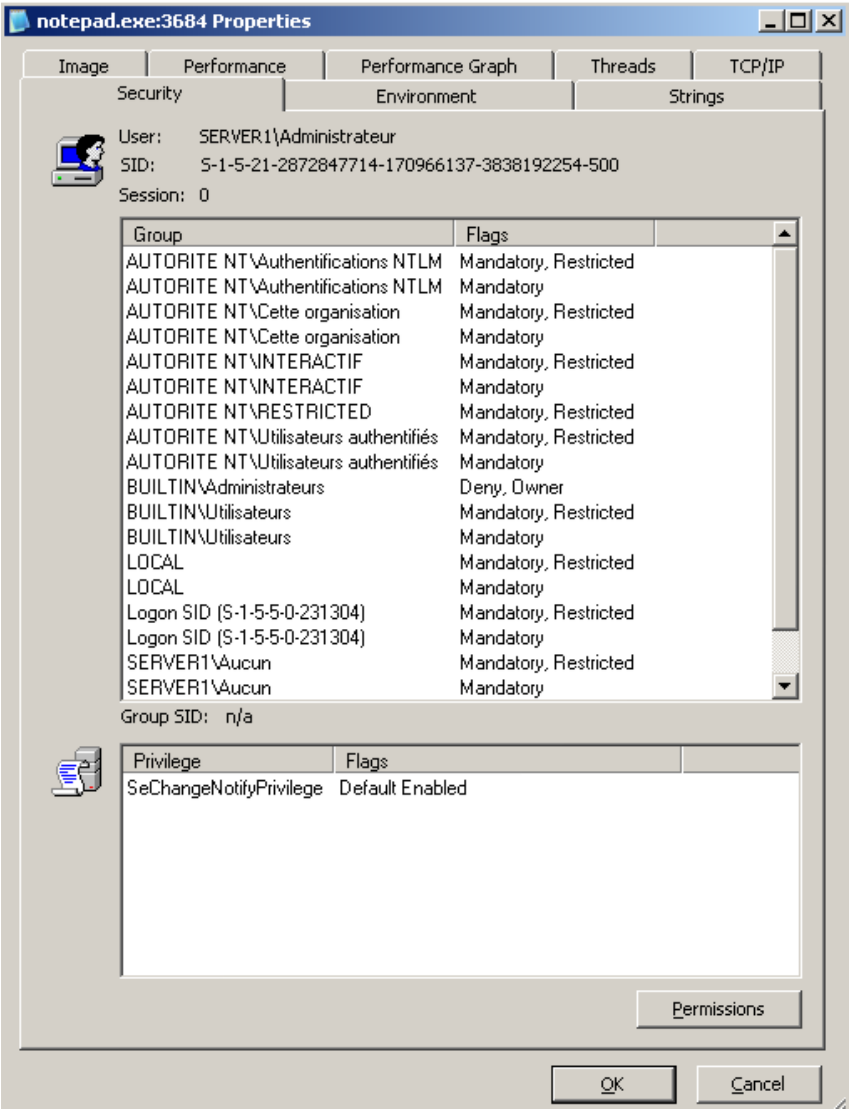
Le jeton restreint est créé à partir du jeton principal, ou d'un jeton d'emprunt.

C'est une copie modifiée
Suppression de privilèges
Marquage deny-only
Marquage restricted

L'intérêt du jeton restreint est d'exécuter une application avec un jeu de privilèges réduit.

3 La protection des objets





3 La protection des objets

Les descripteurs de sécurité :

Il s'agit de la seconde structure de données qui participe au système de sécurité Windows.

Elle décrit les informations de sécurité associées à un objet, et spécifie les actions pouvant être réalisées par telles entités.

3 La protection des objets

Structure d'un descripteur :

Numéro de révision	:	version du SRM
Flags	:	facultatif décrit le comportement du descripteur
SID propriétaire	:	identifie le propriétaire de l'objet
SID de groupe	:	utilisé par posix
DACL	:	entités ayant accès à l'objet
SACL	:	opération/utilisateur → journal audit

3 La protection des objets

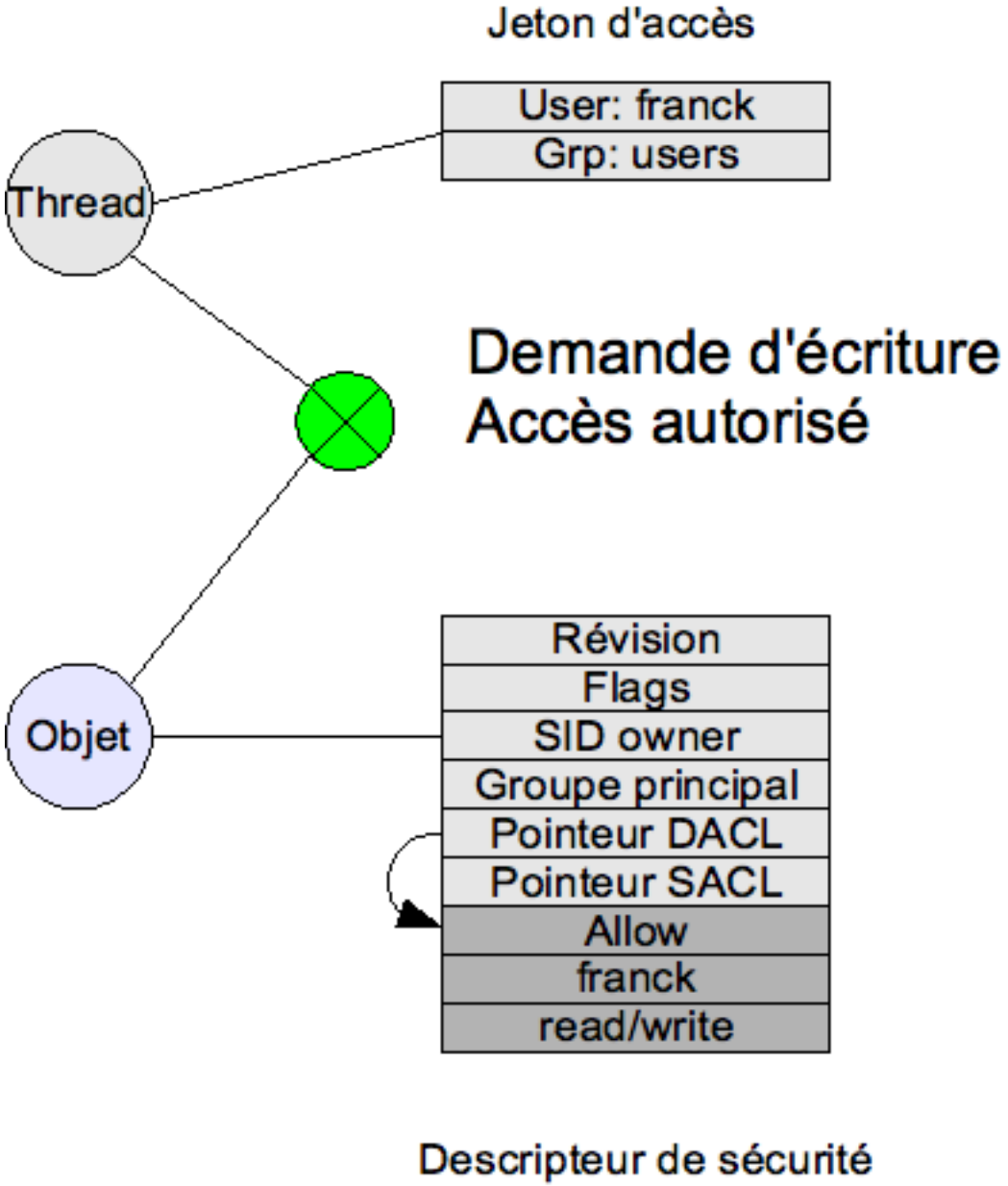
Une ACL est composée :

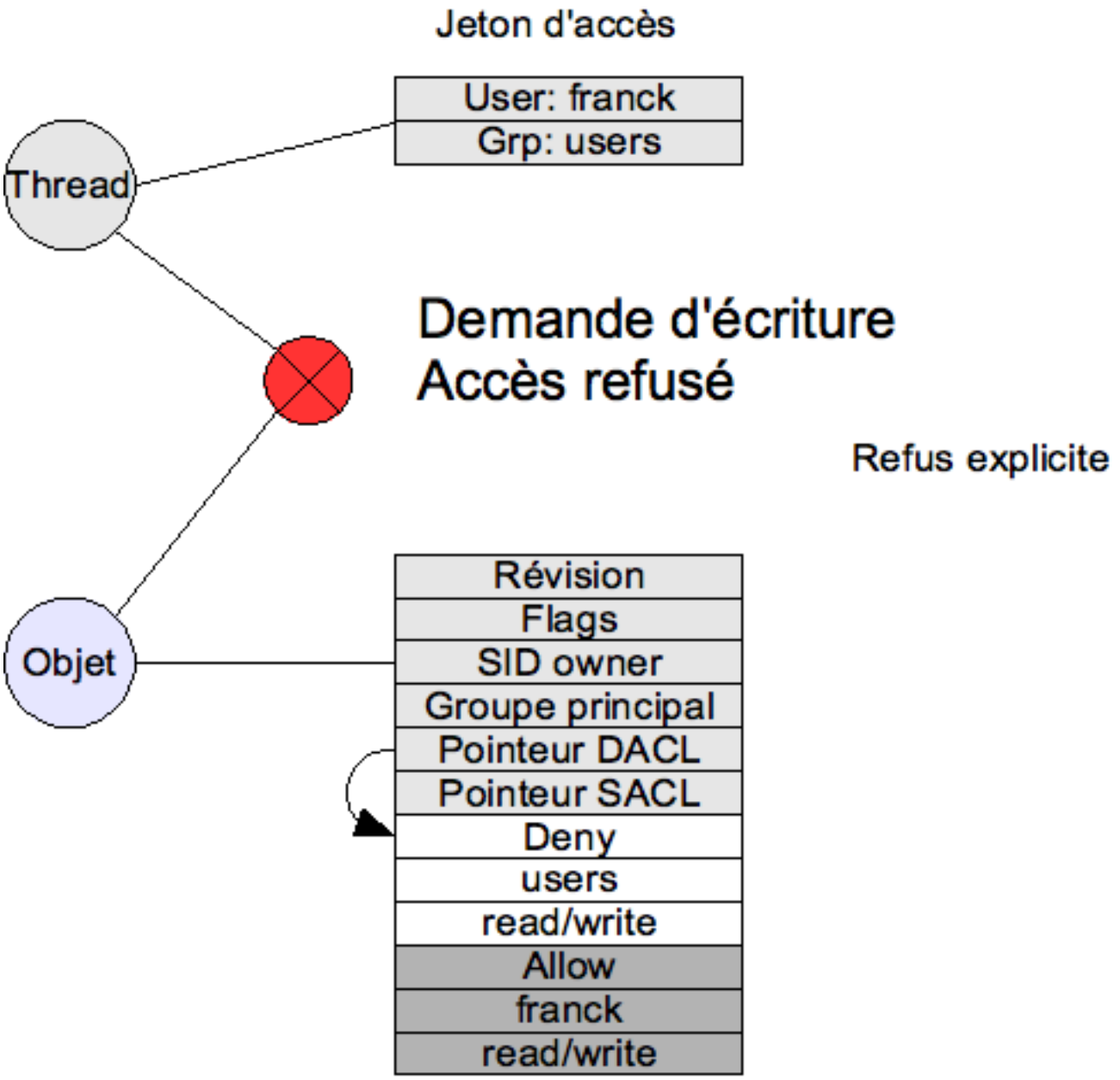
D'un en-tête
D'ACE (access control entry) → SID

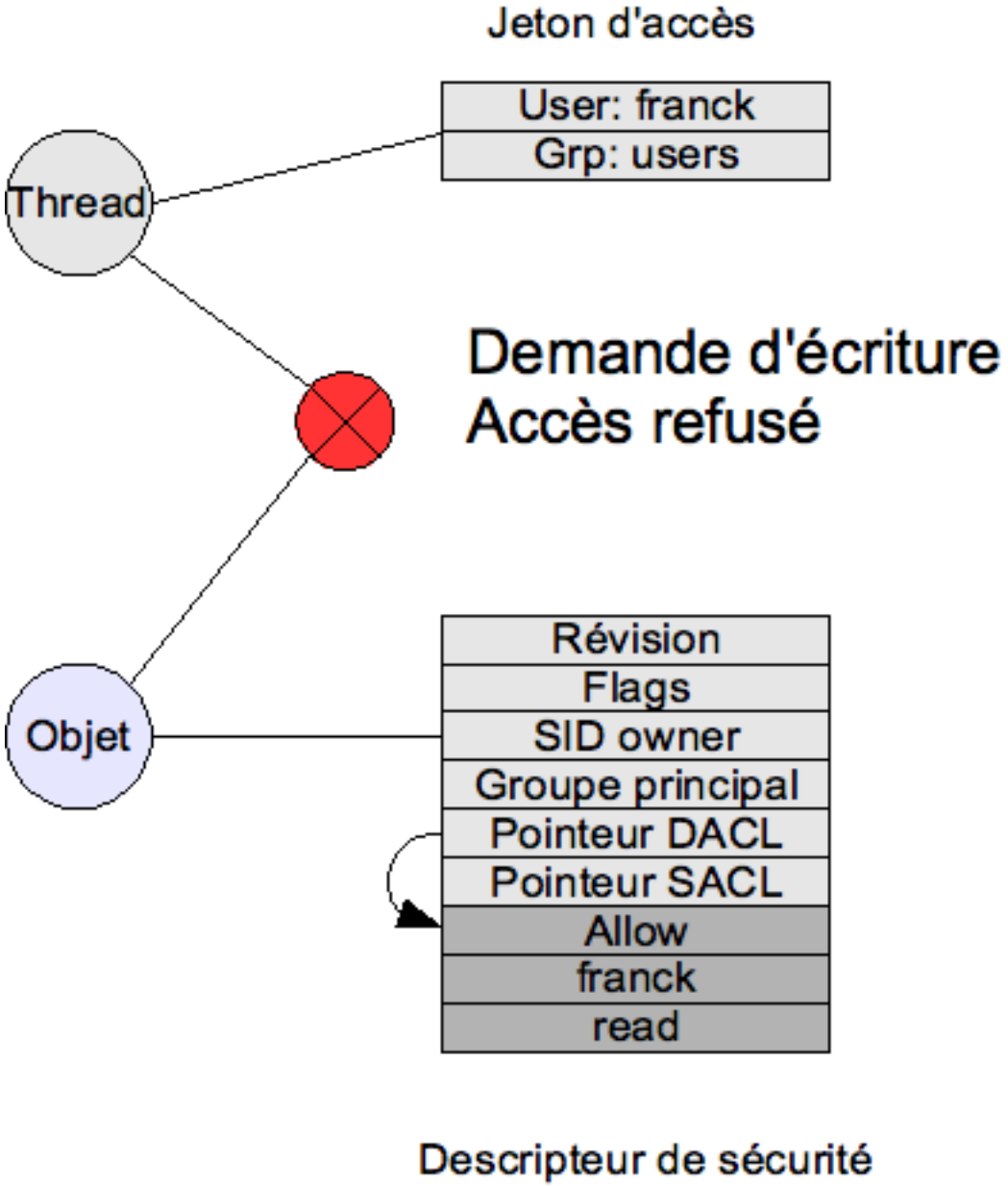
Il y a 4 types d'ACE :
Access allowed
Access denied
Allowed object → utilisé pour les objets AD
Deny object → utilisé pour les objets AD

Si la DACL est vide alors personne n'a d'accès.

S'il n'y a pas de DACL sur l'objet, alors l'accès est illimité.


Jeton d'accès
User: franck
Grp: users
Thread
Demande d'écriture
Accès autorisé
Révision
Flags
SID owner
Groupe principal
Pointeur DACL
Pointeur SACL
Allow
franck
read/write
Objet
Descripteur de sécurité


Jeton d'accès
User: franck
Grp: users
Thread
Demande d'écriture
Accès refusé
Refus explicite
Objet
Révision
Flags
SID owner
Groupe principal
Pointeur DACL
Pointeur SACL
Deny
users
read/write
Allow
franck
read/write
Descripteur de sécurité


Jeton d'accès
User: franck
Grp: users
Thread
Demande d'écriture
Accès refusé
Objet
Révision
Flags
SID owner
Groupe principal
Pointeur DACL
Pointeur SACL
Allow
franck
read
Descripteur de sécurité

3 La protection des objets

Droits et privilèges utilisateurs :

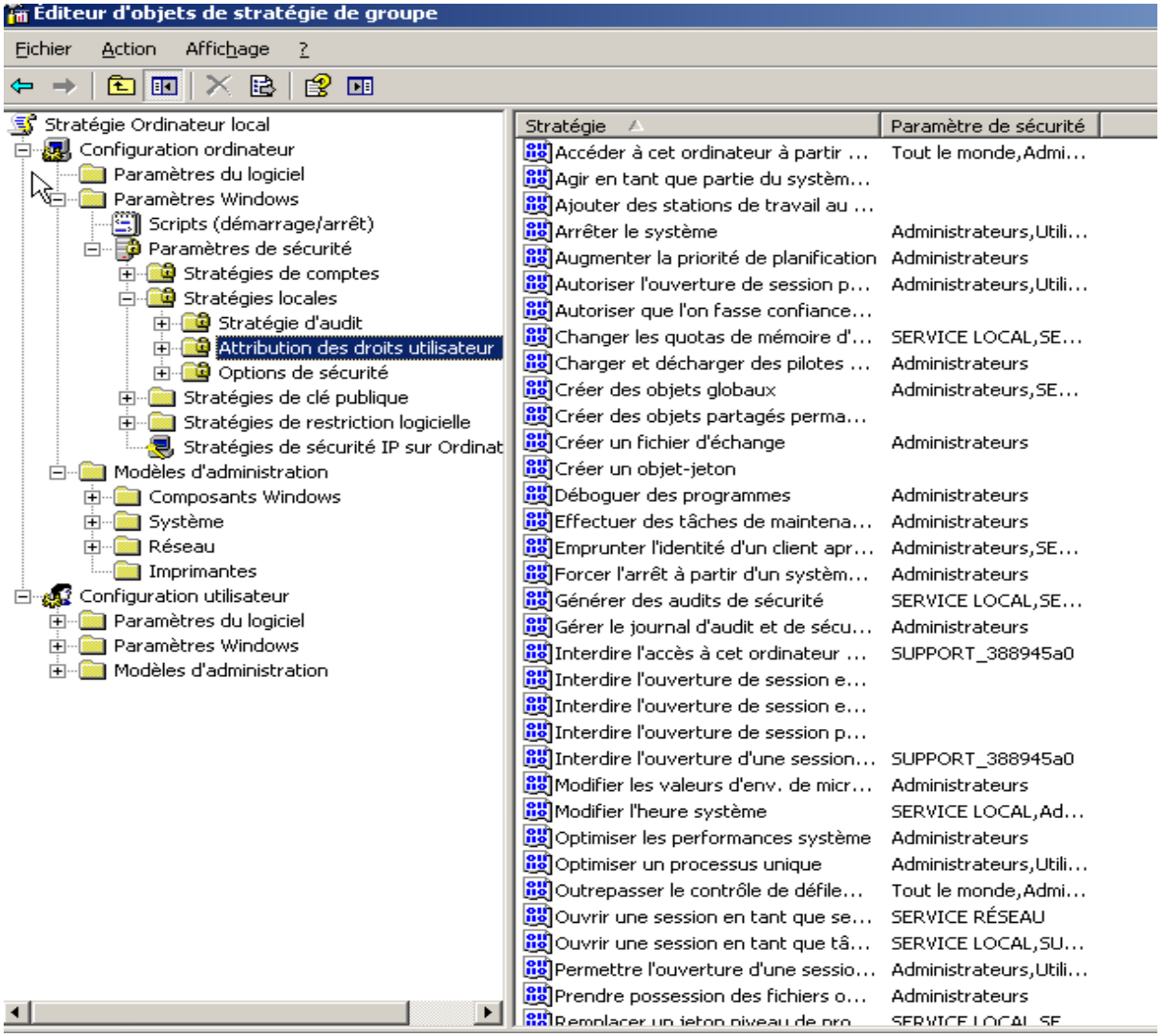
Déterminent les autorisations assignées à certains comptes, pour effectuer certaines opérations.

Par exemple arrêter l'ordinateur, ou modifier l'heure système.

La différence entre un droit et un privilège, est qu'un privilège est activable et désactivable ; alors qu'un droit non.

L'administrateur définit les droits et privilèges via une mmc.

3 La protection des objets



4 Audit de securité

1 Généralités

2 Les composants du système de sécurité

3 la protection des objets

4 Audit de sécurité

4 Audit de securité

Le système d'audit est un dispositif fondamental du système de sécurité.

Il permet de contrôler le système.

De générer des rapports sur l'accès aux différents objets audités.

Cet élément est essentiel car il permet d'analyser les comportements relatifs à la sécurité

De comprendre des incidents de sécurité à postériori.

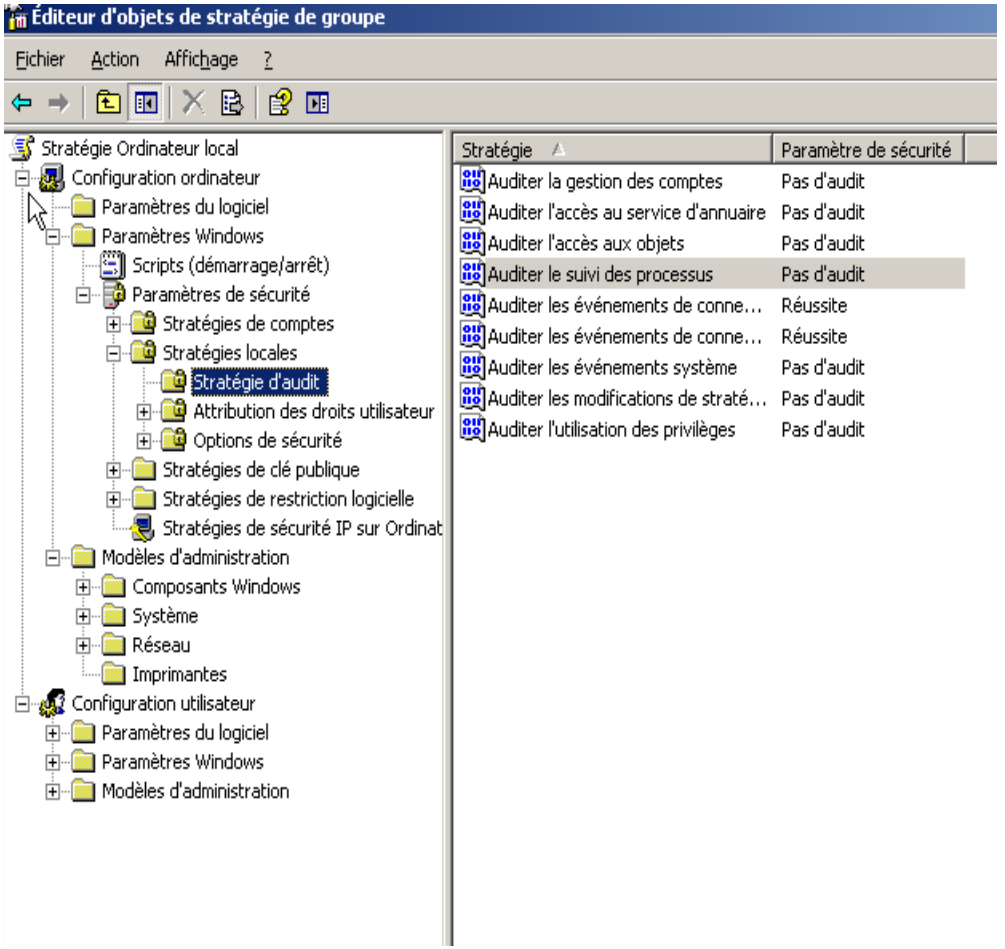
4 Audit de securité

C'est l'administrateur du système qui à la charge de paramétrer les éléments qu'il veut auditer sur le système.

Le système d'audit est couteux en ressources, c'est pourquoi il ne faut auditer que ce qui a été préalablement déterminé. Sous peine de voir les performances du système chuter considérablement.

4 Audit de securité

- Le paramétrage de l'audit se fait via une mmc



4 Audit de securité

Cette stratégie de sécurité est gérée par LSASS. Rappelons que c'est lui qui a la charge de la mise en oeuvre des stratégies de sécurité.

À l'initialisation du système LSASS informe le SRM de la stratégie d'audit.

SRM génère les enregistrement d'audit, et les envoie à LSASS, via une connexion LPC.

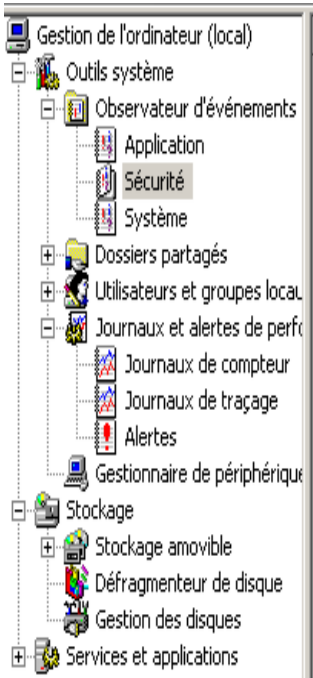
4 Audit de securité

LSASS réceptionne les enregistrements d'audit et les envoie à l'observateur d'événements.

L'observateur d'événements écrit l'enregistrement dans le journal de sécurité.

4 Audit de securité

Enregistrements dans le journal de sécurité



Type	Date	Heure	Source	Catégorie	Évén...	Utilisateur	Ordinateur
Audit des succès	20/11/2008	12:09:23	Security	Ouvertur...	538	Administrateur	SERVER1
Audit des succès	20/11/2008	12:09:23	Security	Ouvertur...	576	Administrateur	SERVER1
Audit des succès	20/11/2008	12:09:23	Security	Ouvertur...	528	Administrateur	SERVER1
Audit des succès	20/11/2008	12:09:23	Security	Ouvertur...	552	SYSTEM	SERVER1
Audit des succès	20/11/2008	12:09:23	Security	Connexio...	680	Administrateur	SERVER1
Audit des succès	20/11/2008	11:37:51	Security	Ouvertur...	538	Administrateur	SERVER1
Audit des succès	20/11/2008	11:37:51	Security	Ouvertur...	576	Administrateur	SERVER1
Audit des succès	20/11/2008	11:37:51	Security	Ouvertur...	528	Administrateur	SERVER1
Audit des succès	20/11/2008	11:37:51	Security	Ouvertur...	552	SYSTEM	SERVER1
Audit des succès	20/11/2008	11:37:51	Security	Connexio...	680	Administrateur	SERVER1
Audit des succès	20/11/2008	11:09:32	Security	Ouvertur...	538	test	SERVER1
Audit des succès	20/11/2008	11:06:51	Security	Ouvertur...	528	test	SERVER1
Audit des succès	20/11/2008	11:06:51	Security	Ouvertur...	552	Administrateur	SERVER1
Audit des succès	20/11/2008	11:06:51	Security	Connexio...	680	test	SERVER1
Audit des succès	20/11/2008	11:05:01	Security	Ouvertur...	538	Administrateur	SERVER1
Audit des succès	20/11/2008	11:05:01	Security	Ouvertur...	576	Administrateur	SERVER1
Audit des succès	20/11/2008	11:05:01	Security	Ouvertur...	528	Administrateur	SERVER1
Audit des succès	20/11/2008	11:05:01	Security	Ouvertur...	552	SYSTEM	SERVER1
Audit des succès	20/11/2008	11:05:01	Security	Connexio...	680	Administrateur	SERVER1
Audit des succès	20/11/2008	10:08:27	Security	Ouvertur...	683	SYSTEM	SERVER1
Audit des succès	20/11/2008	10:07:56	Security	Ouvertur...	538	Administrateur	SERVER1
Audit des succès	20/11/2008	10:07:56	Security	Ouvertur...	576	Administrateur	SERVER1
Audit des succès	20/11/2008	10:07:56	Security	Ouvertur...	528	Administrateur	SERVER1
Audit des succès	20/11/2008	10:07:56	Security	Ouvertur...	552	SYSTEM	SERVER1
Audit des succès	20/11/2008	10:07:56	Security	Connexio...	680	Administrateur	SERVER1
Audit des succès	20/11/2008	07:33:50	Security	Ouvertur...	538	test	SERVER1