THEME: Management et identification d'accès (IAM)

Présenté par:
Hamid Sougour Ardane

les encadrants:

ENASTIC TCHAD

July 25, 2023

Sommaire

ENASTIC
Ecole Nationale Supérieure des TIC

Sommaire

ENASTIC
Ecole Nationale Supérieure des TIC

Sommaire

ENASTIC
Ecole Nationale Supérieure des TIC

Sommaire

ENASTIC
Ecole Nationale Supérieure des TIC

Introduction

La gestion des identités et des accès (IAM) est la pratique qui consiste à s'assurer que les personnes et les entités ayant une identité numérique ont le bon niveau d'accès aux ressources de l'entreprise comme les réseaux et les bases de données,des applications,la gestion des droits ou des habilitations. Les rôles d'utilisateur et les privilèges d'accès sont définis et gérés par un système IAM.

ENASTIC
Ecole Nationale Supérieure des TIC

À quoi sert une solution IAM?

Une solution IAM permet aux administrateurs informatiques de gérer de manière sûre et efficace les identités numériques des utilisateurs et les privilèges d'accès associés.Grâce à l'IAM, les administrateurs peuvent définir et modifier les rôles d'utilisateur, suivre et rendre compte de l'activité des utilisateurs, mais aussi appliquer les politiques de conformité réglementaire et de l'entreprise pour protéger la sécurité et la confidentialité des données.

ENASTIC
Ecole Nationale Supérieure des TIC

Les solutions

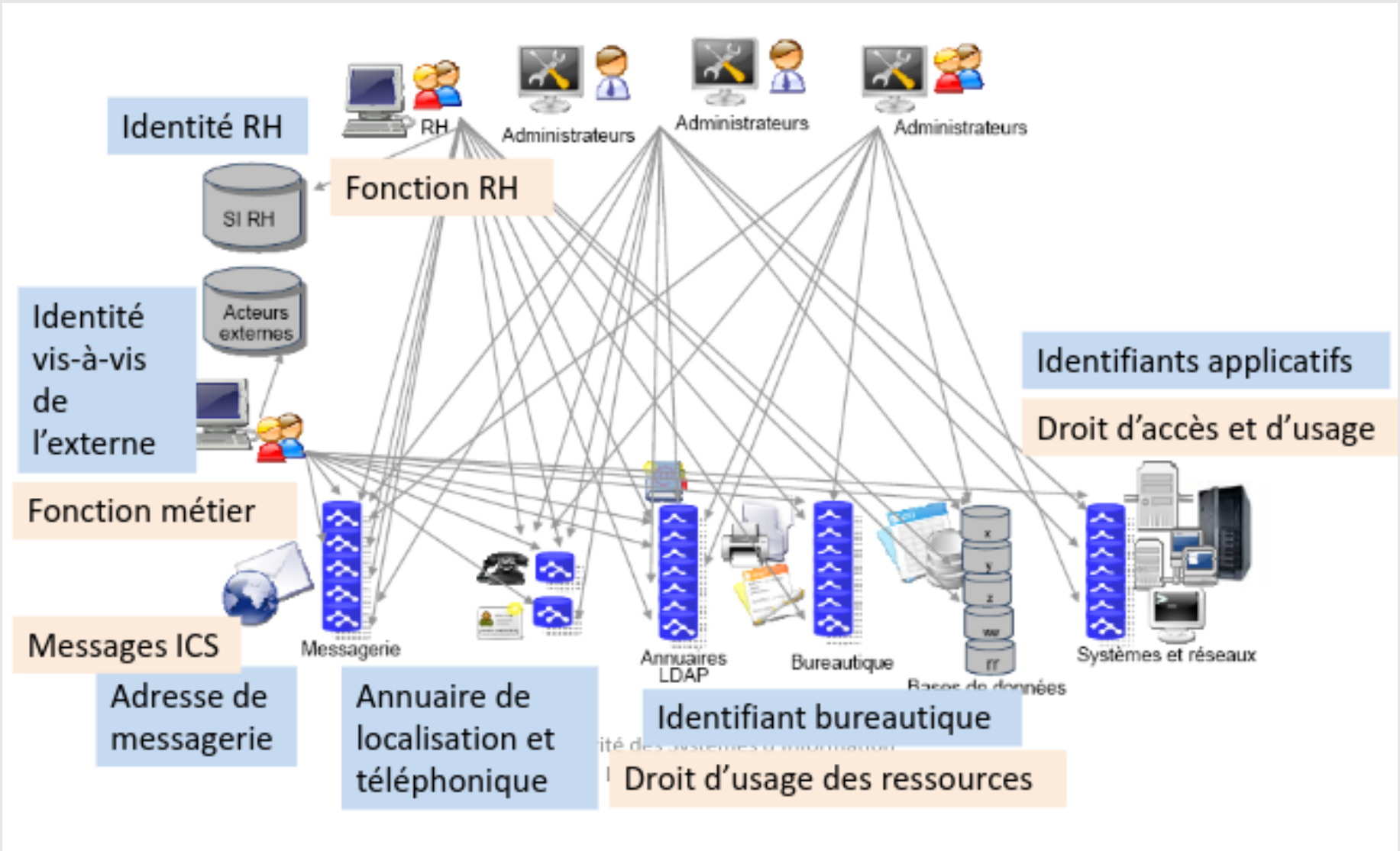
De nos jours,le travail hybride est plus courant et les collaborateurs ont besoin d'un accès sécurisé aux ressources de l'entreprise(les applications,les fichiers et les données), qu'ils travaillent sur site ou à distance. C'est là que la gestion des identités et des accès entre en jeu. Le service informatique de l'entreprise a besoin d'un moyen de contrôler ce à quoi les utilisateurs peuvent et ne peuvent pas accéder afin que les données et les fonctions sensibles soient limitées aux seules personnes et composants qui en ont besoin.

ENASTIC
Ecole Nationale Supérieure des TIC

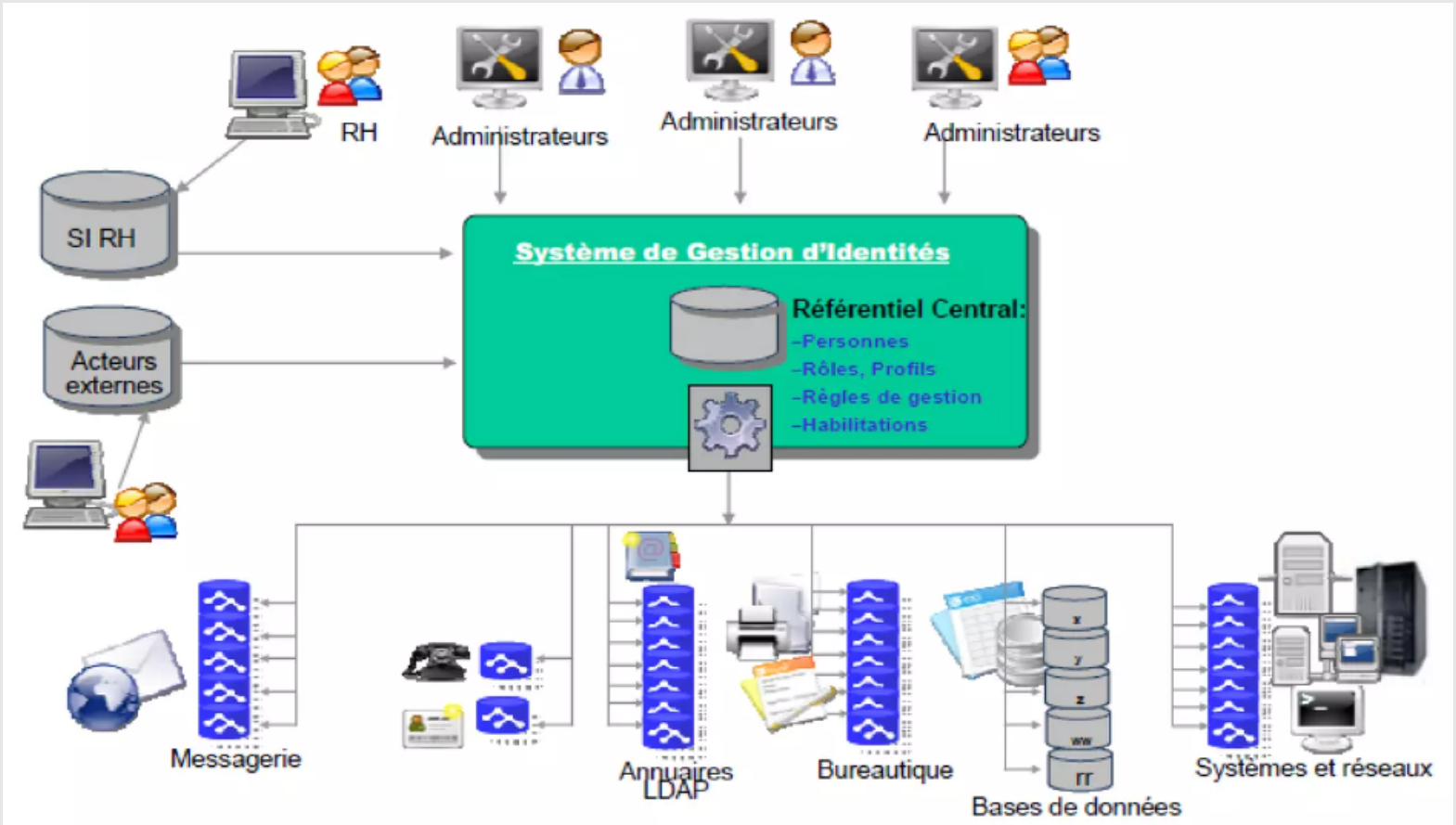
Les solutions

Elle inclut également les prestataires, les fournisseurs, les partenaires commerciaux et les collaborateurs travaillant sur des appareils personnels. La gestion des identités et des accès s'assure que chaque personne qui doit disposer d'un accès a le niveau d'accès approprié au moment opportun et sur la machine appropriée. C'est pour cette raison et également à cause du rôle qu'elle joue dans la cybersécurité d'une entreprise que la gestion des identités et des accès est un élément essentiel des services informatiques modernes.

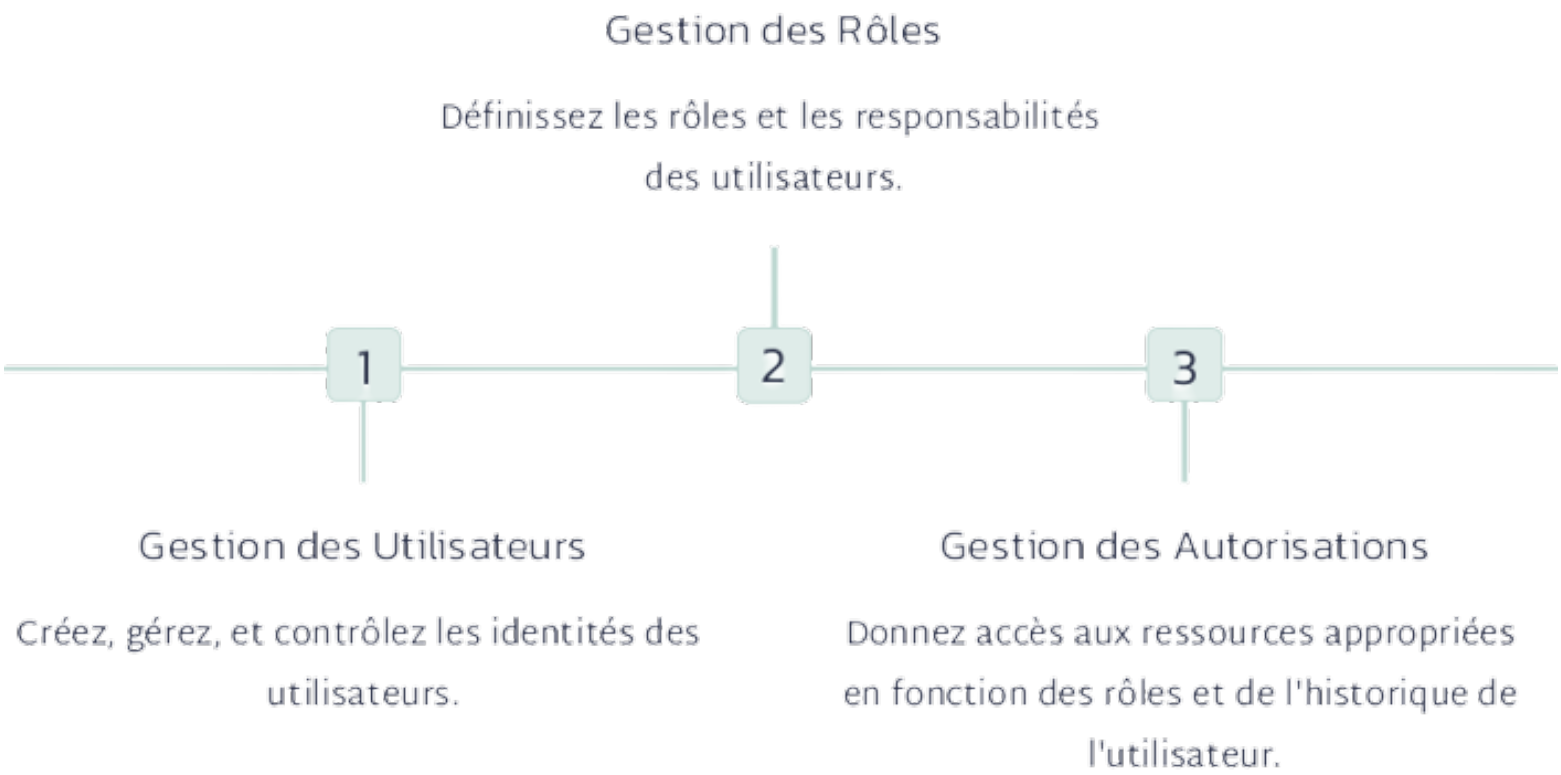
Les solutions



Les solutions



Les Processus Impliqués dans la Gestion des Identités



Meilleures pratiques de gestion des identités et des accès

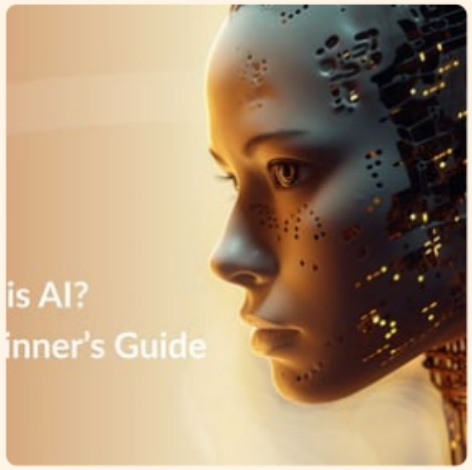
Les tendances actuelles de l'IAM

Sécurité mobile

Les appareils mobiles sont de plus en plus utilisés pour effectuer des tâches critiques, ce qui nécessite de plus en plus de solutions IAM mobiles.

Sécurité IoT

Les objets connectés nécessitent également des stratégies de gestion des identités et des accès pour empêcher les utilisations frauduleuses.



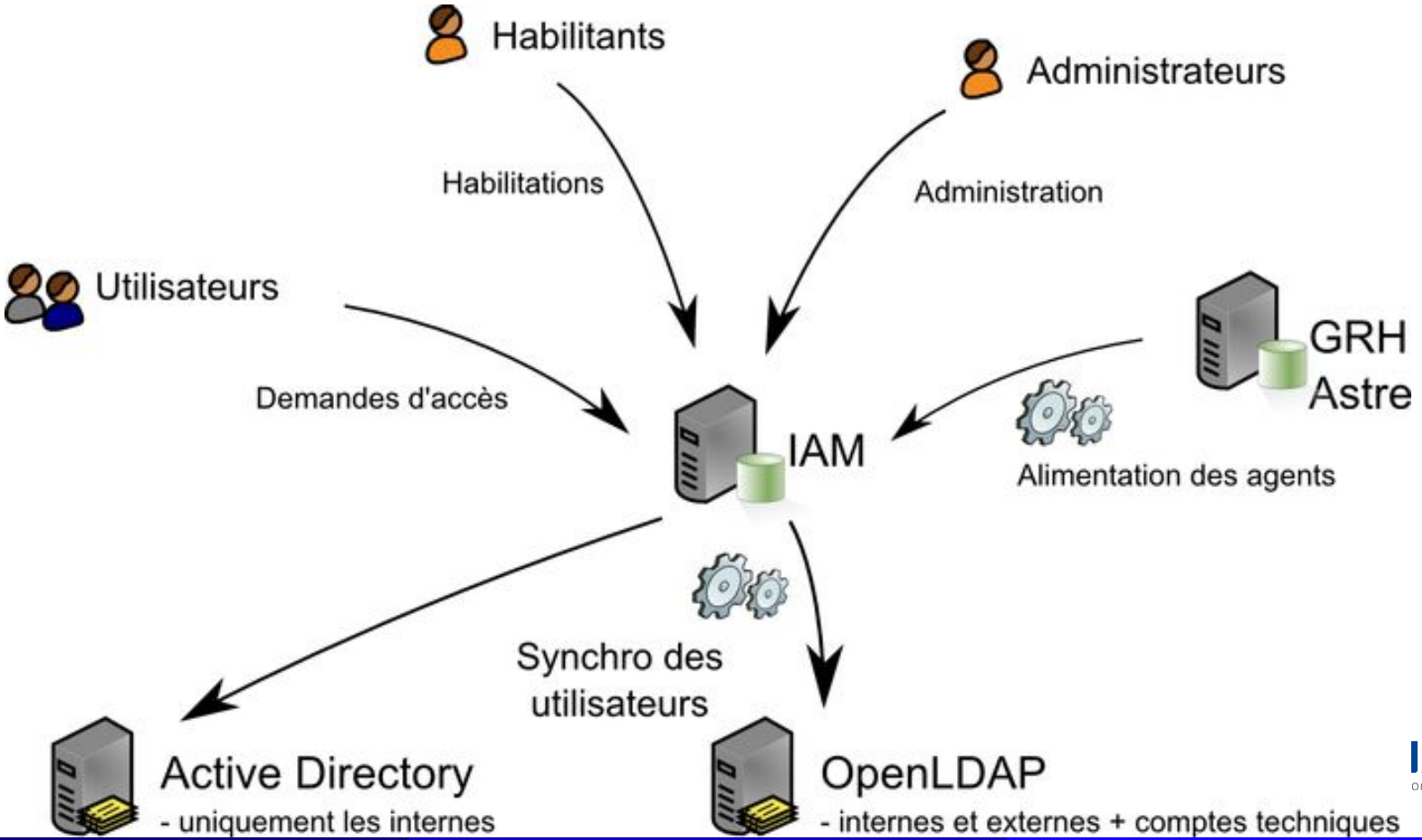
Intelligence artificielle

L'IA est de plus en plus utilisée pour la gestion des identités et des accès, permettant d'automatiser certains processus et de détecter les menaces plus rapidement.

ENASTIC
Ecole Nationale Supérieure des TIC

les matérielles utilise pour la mis en place du projet

Un système de gestion des identités et accès(Identity and Access Management-IAM) repose sur plusieurs materiaux physiques et logiques pour etres mis en place de maniere plus securise et efficace



- **Serveurs:**
  Les serveurs constituent l'infrastructure de base pour héberger les composants du système IAM. Ils sont responsables du stockage des données d'identification, des politiques d'accès, des journaux d'audit
- **Bases des données:** Les bases de stockage fournissent un espace de stockage sécurisé et évolutif pour les données d'identification et les informations d'accès tel que les nom des utilisateurs,les mots de passe,les rôles de utilisateurs,les privilèges associer.les bases données permet le sauvegarde pour assurer la disponibilité et l'intégrité des données.

les Équipement réseau:

Un réseau robuste et sécurisé est essentiel pour prendre en charge la communication entre les différents composants du système IAM.

- les commutateurs
- les routeurs
- les pare-feu
- les VPN (réseaux privés virtuels)

d'autres dispositifs de réseau nécessaires pour assurer la connectivité, la confidentialité et la sécurité des données.

Dispositifs d'authentification

Cela peut inclure des lecteurs de cartes à puce, des scanners d'empreintes digitales, des scanners de rétine ou d'iris, des clés de sécurité matérielles (comme les clés USB de sécurité), des jetons d'authentification à usage unique (OTP), etc. Ces dispositifs permettent de renforcer la sécurité lors de l'authentification des utilisateurs.

Infrastructure de sécurité physique:

Pour garantir la sécurité physique du système IAM, il peut être nécessaire de mettre en place des mesures telles que des salles sécurisées, des systèmes de surveillance vidéo, des systèmes de contrôle d'accès, des systèmes de sauvegarde d'énergie (UPS), etc. Ces mesures contribuent à protéger les équipements et les données sensibles contre les intrusions physiques.

les équipements de sauvegarde :

La sauvegarde régulière des données du système IAM est cruciale pour prévenir la perte de données et faciliter la reprise après un incident.On peut utiliser des périphériques de sauvegarde tels que:

- des bandes magnétiques;
- des disques durs externes;
- des systèmes de stockage en réseau (NAS) ;
- des services de sauvegarde basés sur le cloud

ENASTIC
Ecole Nationale Supérieure des TIC

les protocoleS authentification

LDAP(Lightweight Directory Access Protocol) ;

SAML(Security Assertion Markup Language);

OAuth(Open Authorization);

OpenID Connect;

ENASTIC
Ecole Nationale Supérieure des TIC

les failles du IAM

- Risque d'utilisation illicite d'un accès à la suite du départ de l'organisme d'un employé
- Risque de destruction ou de modification de données, sans autorisation
- Risque de fuite de données confidentielles
- Risque d'usurpation des accès par une personne autre que celle autorisée

Figure: ■

les failles du IAM

- Risque d'utilisation illicite d'un accès à la suite du départ de l'organisme d'un employé
- Risque de destruction ou de modification de données, sans autorisation
- Risque de fuite de données confidentielles
- Risque d'usurpation des accès par une personne autre que celle autorisée

Figure: ■

les failles du IAM

- Risque d'utilisation illicite d'un accès à la suite du départ de l'organisme d'un employé
- Risque de destruction ou de modification de données, sans autorisation
- Risque de fuite de données confidentielles
- Risque d'usurpation des accès par une personne autre que celle autorisée

Figure: ■

les failles du IAM

- Risque d'utilisation illicite d'un accès à la suite du départ de l'organisme d'un employé
- Risque de destruction ou de modification de données, sans autorisation
- Risque de fuite de données confidentielles
- Risque d'usurpation des accès par une personne autre que celle autorisée

Figure: ■

ENASTIC
Ecole Nationale Supérieure des TIC