ACCUEIL CONTRÔLE D'ACCÈS 2017

Contrôle d'Accès : Système d'Information

- Prévoir les plans d'adressage à partir d'un document qui sera fourni par ARD
- Chef de Projet : David JAUSSAUD david.jaussaud@ard.fr

Solution Informatique

Configuration serveur

- Serveur centralisé : VM LINUX
- Hyperviseur HyperV
- Prévoir 32G / 8 CPU dans un premier temps (☐ étendre à 64G dès que possible)
    - Procédure d'installation ARD

Configuration réseau

- Serveur dans le VLAN17 (ard.emse.fr has address 193.49.172.251)
- Réseau UTL Saint-Étienne isolé sur le Firewall (VLAN 14 → 192.168.14.0/24)
- Réseau UTL Gardanne isolé sur le Firewall (VLAN 153 → 192.168.153.0/24)
- ☐ Prévoir VPN site à site entre 192.168.153.0/24 et 193.49.172.251 (Florent BITSCHY)

Principes Généraux

Fonctionnement

Le contrôle d'accès reposera sur 3 briques :

1.- Référentiel utilisateur LDAP

- Point de vérité données utilisateurs (création de comptes : ARRIVANTS, CREENS, DOCGEST)
- Synchronisation automatique des utilisateurs avec SESAME basée sur des filtres

2.- Application maison SESAME

- **Point de vérité droits d'accès des utilisateurs**
- Application maison PHP / Mysql + CRON pour interactions avec ARD
- Attribution de droits initiaux en fonction des attributs LDAP lors de la création de l'utilisateur

- Interface d'attribution, de modification et de suppression de droits LN2, locaux spécifiques, accès exceptionnels (workflow), accès à durée limité (workflow)…
- Interface utilisateurs de visualisation des droits d'accès en cours, des attributs LDAP, de déclaration de perte/vol de badge, de demande d'autorisation de droits (via WORKFLOW)

3.- ARD Accès

- **Point de vérité “badges”, “Points d'Accès, Groupes d'utilisateurs**
- Gestion manuelle de droits non automatisés

Groupes Principaux de locaux

- BÂTIMENTS = portes extérieurs + SAS Fauriel
- BÂTIMENTS-HPH = accès BÂTIMENTS Hors Plages Horaires
- ACCES-HPH = accès pour véhicules Hors Plages Horaires
- SC = Salles de cours
- SV = Salles de visio
- SR = Salles de réunions
- BARRIÈRES = barrières parking
- BUREAUX = bureaux
- BUREAUX-DIR = bureaux des responsables de centre/département (CENTRE)
- LN1 = Laboratoires Niveau 1
- LN2= Laboratoires Niveau 2

Groupes Principaux d'usagers

- ÉLÈVE = BÂTIMENTS + SC
- PERSONNEL = BÂTIMENTS + BARRIÈRES + SC/SR/SV
- CENTRE = PERSONNEL + L1 + BUREAUX CENTRE
- CENTRE-DIR = CENTRE + BUREAUX-DIR
- ADMIN = PERSONNEL + BUREAU SERVICE
- STAGIAIRE = PERSONNEL + LOCAUX DÉFINIS DANS SESAME
- VACATAIRE = ÉLÈVES + BARRIÈRES
- TEAM = BÂTIMENTS + BARRIÈRES + BUREAU(X) TEAM SESAME
- WE = BÂTIMENTS-HPH + LOCAUX DÉFINIS DANS SESAME
- VÉHICULES = BARRIÈRES + ACCES-HPH

Nom du groupe	Filtre LDAP correspondant
ELEVE	(&(supannActivite=ACTIF)(businessCategory=ELEVE))
PERSONNEL	(&(supannActivite=ACTIF)(|(businessCategory=ADMIN)(businessCategory=CIS)(businessCategory=CMP-GC)(businessCategory=FAYOL)(businessCategory=SMS)(businessCategory=SPIN)))
VACATAIRE	(&(supannActivite=ACTIF)(businessCategory=VACATAIRE))
STAGIAIRE	(&(supannActivite=ACTIF)(|(businessCategory=ADMIN)(businessCategory=CIS)(businessCategory=CMP-GC)(businessCategory=FAYOL)(businessCategory=SMS)(businessCategory=SPIN))(employeeType=Stagiaire))
…	

ÉTUDIANTS

Droits initiaux = 1 an (carte d'étudiant)

- businessCatégory = ELEVE

TEAM

Droits accès aux batiments / accès aux salles communes / accès bureau dédié à l'équipe

EXTERNE

Attribut trop large à ce jour (PERSONNEL MDE / VACCATAIRE) Transfert des anciens élèves en ADMIN

AUTRE

- A détruire

Les Profils

Créations d'attributs spécifiques

- Date de création du compte (type date)
- Date d'expiration du badge (type date)
- Date d'expiration du mot de passe (type date)
- Profils d'accès géographique (texte multivalué)
- Profile d'accès Services (texte multivalué)
- Statut du contrôle d'accès (multivalué = ACTIF / INACTIF / ASUPPRIMER) : **SuppannActivite**
- N° BADGE (injecté depuis ARD ACCESS si possible)

Opération préalable sur annuaire LDAP

Nettoyage annuaire LDAP

- Repérage **DOCTORANTS** : EduPersoAffiliation = student + researcher (OK)
- Repérage **STAGIAIRES** : EmployeType=stagiaire (pris en compte dans process actuel de création de compte
  - Modification process affectation de badges
  - If EmployeType=stagiaire : affectation des droits dans application “Droits Particuliers”
- Remplir **SuppannActivite** : filtre = BusinessCategory (ADMIN/ CIS / SMS / CMP / SPIN / FAYOL / ELEVE) ET employeNumber
  - EmployeNumber = 0 ⇒ INACTIF = pas de demande de badges initial

    - EmployeNumber # 0 ⇒ ACTIF = demande de création de badge
    - A VERIFIER : les doctorants

- Remplir Fin de droits de badges
    - Attributs type date à trouver (demande IANNA en cours)
    - Prévoir action automatique à expiration de la date : modification SuppannActivite = ADETRUIRE

Modification des application de création de comptes

- SuppannActivite

Prévoir une interface d'attribution de profil