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 et mise à jour de changement de valeur d'attribut dans LDAP

- 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 (EXTERNE)

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 + LN1 + BUREAUX CENTRE
- CENTRE-DIR = CENTRE + BUREAUX-DIR
- ADMIN = PERSONNEL + BUREAU SERVICE
- STAGIAIRE = PERSONNEL + LOCAUX DÉFINIS DANS SESAME
- VACATAIRE = ÉLÈVES + BARRIÈRES
- TEAM/MICROPACKS = BÂTIMENTS + BARRIÈRES + BUREAU(X) TEAM SESAME
- WE = BÂTIMENTS-HPH + LOCAUX DÉFINIS DANS SESAME
- VÉHICULES = BARRIÈRES + ACCES-HPH

Les services DSI, PMG (STE) et Infra (Gardanne) doivent avoir accès à tous les locaux sauf LN2 en HO pour gérer l'accueil des entreprises et les interventions.

Liste exhaustive des profils

Modèle des données

- Modèle des données (LDAP / SESAME / ARD)
- Nettoyage annuaire LDAP
- Documentation API SOAP
- Spécifications SESAME

From:
https://portail.emse.fr/dokuwiki/ - **DOC**

Permanent link:
https://portail.emse.fr/dokuwiki/doku.php?id=sg:gt:controleacces2017:si

Last update: **15/12/2017 08:27**