Bonnes pratiques

- Architecture OU Active Directory
- Organisation des droits RDS
- Gestion des rôles et droits sur VCSA

Architecture OU Active Directory

Voici la liste des ou et sous OU avec les éléments qu'elles contiendrons.

NonOrganisation (OU principale dans laquelle tous les objets et conteneurs seront rangés)

- **GMSA** (sous OU contenants les groupes et comptes gmsa)
  - **GMSAGroups** (sous OU contenants les groupes gmsa)
  - **GMSAUsers** (sous OU contenants les comptes de services gmsa)

- **Groups** (sous OU contenant les groupes)
  - **Applications** (sous OU contenant les groupes de contrôle d'accès aux applications)
    - GRP_SEC_GG_RDS-Collection*XX* (contenant les groupes des apps de cette collections)
    - GRP_SEC_GG_RDS-<AppName>

  - **DistributionList** (sous OU contenant les listes de distributions)
    - &UsersLab01
    - &UsersLab02
    - &UsersLabAlls
    - &Admins

  - **FilerManagement** (sous OU contenant les groupes de sécurité, notamment pour les filers)
    - GRP_SEC_GG_FIL_lab01_RO
    - GRP_SEC_GG_FIL_lab01_RW
    - GRP_SEC_GG_FIL_ITSources_RO
    - GRP_SEC_GG_FIL_ITSources_RW

  - **GPOFilters** (contient les groupes filtres pour l'application ou exclusion des GPO)
    - GRP_SEC_GG_GPO_INC_RDSSessionHosts
    - GRP_SEC_GG_GPO_EXL_printservers

  - **Services** (sous OU contenant les groupes de contrôle d'accès aux services. proxy, vpn, etc…)
    - GRP_SEC_GL_VPN-Admins
    - GRP_SEC_GL_VPN-Users

    - GRP_SEC_GL_PROXY-Extended
    - GRP_SEC_GL_PROXY-NoAccess
    - GRP_SEC_GL_VCSA-Restricted
    - GRP_SEC_GL_VCSA-LAB*XX*
    - GRP_SEC_GL_DOCKER-Admins
    - GRP_SEC_GL_DOCKER-Users
    - GRP_SEC_GL_DOCKER-Labs

- **Machines** (sous OU contenant les comptes machines)
    - **Computers** (sous OU contenants les ordinateurs clients du domaine)
    - **Servers** (sous OU contenant les serveurs du domaine)
        - **RDS** (sous OU contenant les serveurs RDS du domaine)

- **Users** (sous OU contenant les comptes utilisateurs & comptes de services)
    - **Admins** (sous OU contenant les comptes administrateur)
    - **Internals** (sous OU contenant les comptes utilisateurs)
        - **Site1** (sous OU contenant les comptes étudiants)
        - **Site2** (sous OU contenant les comptes du personnel éducatif)
    - **Ressources** (sous OU contenant les comptes utilisateurs ressources : salles de réunions, projecteurs, ...)
    - **SpecificsAccounts** (sous OU contenant les comptes utilisateurs spéciaux : scan, bind ldap, ...)
    - **TMA** (sous OU contenant les comptes utilisateurs Tierce Maintenance Applicative)

> **Conseil** : Il sera possible de placer des groupes dans les users par exemple pour les noms de services, etc...

Organisation des droits RDS

I. Organisation des droits RDS

image.png

Pour gérer les accès à la ferme RDS de façon granulaire, les groupes sont imbriqués comme suit :

- Le groupe '***AppsUser***' donne accès à la connexion sur la ferme RemoteApp et au portail HTML5.
- Le groupe '***VDIUsers***' donne accès à la ferme VDI.
- Le groupe '***admin***' dispose de tous les accès.

Chaque application dispose d'un groupe où sont placés les utilisateurs.

Puis comme les applications font partie de collections, le groupe de collection contient les groupes applicatifs.

Enfin les groupes globaux contiennent les groupes de collection.

Puis les droits sont posé sur chaque élément. Comme cela, intégrer un utilisateur au groupe applicatif, le restreint à la (ou aux) application(s) dont il a besoin tout en appliquant récursivement les droit pour qu'il y accède correctement.

Gestion des rôles et droits sur VCSA

> Pour la portée des droits, se référer à : VSCA - Hiérarche des droits

I. Infrastructure

Read_Only

S’applique A : ***GRP_SEC_GG_VCSA_RestrictedUsers***

Appliqué sur : datacenter & hosts

Propagation : NON

Droits :

- Defaults.

LABS404_HostsProfileCommon

S’applique A : ***GRP_SEC_GG_VCSA_RestrictedUsers***

Appliqué sur : cluster

Propagation : NON

Droits :

- Virtual machines
  - Create from existing
  - Create new

II. Ressource Pool (compute)

LABS404_RessourcePoolProfileIndividual

S’applique A : ***GRP_SEC_GG_VCSA_<LABx>***

Appliqué sur : pool de ressource LAB (LAB1, LAB2, LAB3)

Propagation : NON

Droits :

- Ressources
  - Assign vApp to ressource pool
  - Assign VM to ressource pool
- Virtual machines
  - Interaction

III. Storage

LABS404_StorageProfileCommon

S’applique A : ***GRP_SEC_GG_VCSA_RestrictedUsers***

Appliqué sur : Datastore Sources

Propagation : OUI

Droits :

- Datastore
  - Browse datastore

LABS404_StorageProfileIndividual

S’applique A : ***GRP_SEC_GG_VCSA_<LABx>***

Appliqué sur : Datastore du LAB (LAB1, LAB2, LAB3)

Propagation : OUI

Droits :

- Datastore
  - Allocate space
  - Browse datastore
  - Remove file
  - Update virtual machine files
  - Update virtualmachine metadata
  - Low Level File Opperation
- Virtual machines
  - Provisioning

IV. Folders

LABS404_FolderProfileCommon

S’applique A : ***GRP_SEC_GG_VCSA_RestrictedUsers***

Appliqué sur : Folder Template

Propagation : OUI

Droits :

- Virtual Machines
  - Clone template
  - Deploy template

LABS404_FolderProfileIndividual

S’applique A : ***GRP_SEC_GG_VCSA_<LABx>***

Appliqué sur : Folder du LAB (LAB1, LAB2, LAB3)

Propagation : OUI

Droits :

- Folder
  - All privilleges
- Virtual machines
  - all privilleges

V. Network

LABS404_NetworkProfileCommon

S’applique A : ***GRP_SEC_GG_VCSA_RestrictedUsers***

Appliqué sur : Groupe de port VLAN interco

Propagation : non

Droits :

- network
  - Assign Network

LABS404_NetworkProfileIndividual

S’applique A : ***GRP_SEC_GG_VCSA_<LABx>***

Appliqué sur : Groupe de port VLAN du LAB (LAB1, LAB2, LAB3)

Propagation : non

Droits :

- network
  - Assign Network