

Document de cadrage

SAE Cyber.312

Concevoir un réseau informatique sécurisé multi-sites

Mise en place d'un serveur de mail et d'un annuaire AD DS sur une architecture sécurisée

Sommaire

I. Compétences ciblées :	4
II. Descriptif	4
III. Objectif	5
Description du projet – cahier de charges	5
I. Contexte	6
II. Architecture du réseau	6
III. Virtualisation des services	8
IV. Plan d'adressage IP	8
V. Câblage et configuration	9
VI. Configuration SSH et sécurité	9
VII. Configuration des VLAN	9
VIII. Haute disponibilité – niveau 2	10
IX. Configuration du routage	10
X. Configuration du NAT	10
XI. Haute disponibilité – niveau 3	10
XII. Service DNS:	10
XIII. Service DHCP:	10
XIV. Service de messagerie :	10
XV. Sécurité et ACL	11
XVI. Annuaire Active Directory	11
AD DS du Campus de l'Université de Hogwarts	12
I. Configuration de l'architecture AD DS sur le site Hogwarts-Ouest	12
II. A faire dans le domaine hogwards.edu sur le site Hogwarts-Ouest	13
A. Etapes pour la mise en place du domaine hogwards.edu.	13
1. Création du site, du domaine et du DC (Domaine Controller) (voir le chapitre Managing sites and subnets)	13
2. Créations des OUs, Groups (voire Section III et Annex 2),	13
3. Création des comptes utilisateurs (voire Section III et Annex 1)	13
4. Création des comptes ordinateurs (Section III et le chapitre Managing Computer Account)	13
B. Etapes pour la personnalisation de la configuration du domaine butrtX.lan	13

1. Sécurisation des mots de passe – création des PSOs.	13
2. Création des GPOs pour les configurations Utilisateur et Ordinateur	13
III. Description du site Hogwards-Ouest	13
1. Description du site, du domaine et du DC (Domaine Controller)	14
2. Description des OUs, Groups, comptes Users et Ordinateurs	14
IV. Description des GPOs et FGPP pour le site Hogwards-Ouest	17
1. Politique de mot de passe (Fine-Grained Password Policies)	17
2. GPO pour la personnalisation des comptes utilisateur des professeurs	17
3. Install GPO – Configuration de l'installation d'une application	18
4. logon GPO – Configuration à la connexion	18
5. Startup GPO – Configuration démarrage de l'ordinateur	18
Bonus – création du site Hogwards-Nord	19
V. Description du site Hogwards-Nord	19
VI. A faire dans le domaine geii.butrtX.lan	19
Annexe – Virtualisation des services	19
Annexe – Adressage	20
Annexe – Convertir un fichier .exe en .msi	21

Problématique professionnelle et objectifs

Le professionnel R&T spécialisé en Cybersécurité doit mettre en œuvre une infrastructure multi-sites sécurisée et justifier les solutions apportées à partir d'un cahier des charges spécifiant les besoins du réseau d'une entreprise. Il prête une attention particulière aux vulnérabilités potentielles et connues des équipements réseaux et du système d'information installés.

I. Compétences ciblées :

- Administrer un système d'information sécurisé
- Surveiller un système d'information sécurisé
- Administrer les réseaux et l'Internet
- Connecter les entreprises et les usagers

II. Descriptif

A partir d'un cahier des charges spécifiant les besoins du réseau d'une entreprise, le professionnel Cyber doit mettre en œuvre une infrastructure multi-sites en justifiant les solutions apportées notamment en termes de cybersécurité. Cette infrastructure repose :

- sur les concepts fondamentaux du réseau :
 - routage, filtrage inter-VLAN;
 - redondance (STP, routage dynamique, VRRP);
 - services avancés;
- sur la mise en place et la configuration des équipements;
- sur les besoins spécifiques en termes de cybersécurité, en utilisant les outils mis en place dans le cadre de la SAÉ3.Cyber.04 "Découvrir le pentesting" notamment les tests de pénétration et les techniques de durcissement et de remédiation permettant de renforcer la robustesse du réseau informatique;
- sur une documentation détaillée de l'infrastructure mise en œuvre et de son niveau de sécurité.

III. Objectif

L'objectif de cette SAé est de mettre en place un réseau de CAMPUS redondé avec un service de messagerie ainsi qu'un service d'annuaire

Description du projet – cahier de charges

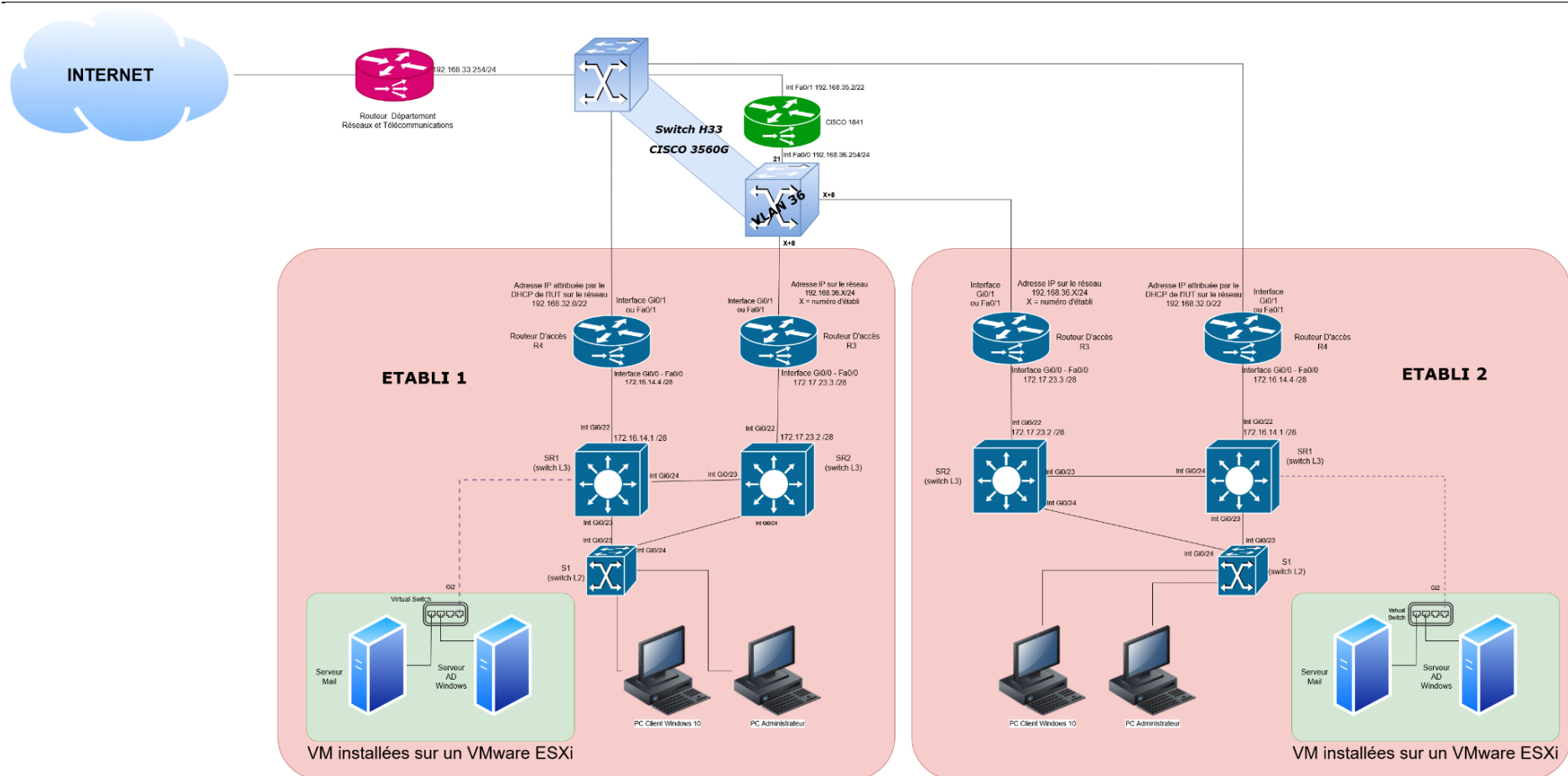
I. Contexte

L'Université de Hogwards dispense différentes formations sur un site dont l'architecture physique est représentée dans le schéma suivant.

Pour une meilleure gestion du réseau, un serveur de mail et un annuaire AD DS seront mis en place.

II. Architecture du réseau

L'architecture du réseau sera la suivante :



Vous configurerez uniquement l'infrastructure d'un seul établissement, l'ETABLI 1 et 2 de l'illustration sont dessinés pour contextualiser.

II. Virtualisation des services

Si vous êtes en H33, les serveurs Windows et Linux Ubuntu seront placés dans un hyperviseur VMware Esxi. Le serveur HP Proliant possède 2 interfaces Gi1 et Gi2.

Seule l'interface Gi2 sera utilisée pour connecter les VM de cette SAE à votre réseau.

L'interface Gi1 sera utilisée pour la gestion de l'ESXi. Elle est raccordée à la prise murale et ne doit jamais être déconnectée.

Vous possédez un compte (etudiant) avec des droits limités mais qui vous permet de créer/supprimer/modifier des VM. Les VM seront connectées sur le *vSwitch1* et seront reliées au réseau par l'interface physique *vmnic1*. (voir document ressource).

Les adresses IP de gestion des ESXi sont 192.168.35.1X/24, (X étant le numéro de votre établi). Les login/Mdp sont etudiant/Velizy78!.

Le datastore de l'hyperviseur contient les fichiers iso des OS à installer.

III. Plan d'adressage IP

L'adresse réseau entre SR1 et R4 sera 172.16.14.0/28

L'adresse réseau entre SR2 et R3 sera 172.17.23.0/28

L'adresse réseau *Data* sera 192.168.10.0/24 et l'adresse réseau *Server* sera 192.168.20.0/24

La réseau opérateur de R3 sera sur le réseau 192.168.36.0/24 et R4 sur le réseau du département R&T, l'adresse « Wan » sera attribuée par un serveur DHCP.

Voici ci-dessous une synthèse de l'adressage IP.

Sous-réseau	Adresse	
Gestion de l'ESXi	192.168.35.1X/24 (X étant le numéro de votre établi)	login/Mdp : etudiant/Velizy78!
AD Windows, Serveur Mail,	VLAN Server, VLAN ID : 20 192.168.20.252/24	
PCs	VLAN Data, VLAN ID : 10 192.168.10.252/24	
SR1 – R4	172.16.14.0/28	
SR2 - R3	172.16.23.0/28	
R4 – Routeur Département RT	sur le réseau du département R&T, l'adresse « Wan » sera attribuée par un serveur DHCP	
R3- Routeur Cisco 1841	192.168.36.0/24	

IV. Câblage et configuration

Le câblage devra être réalisé en respectant les numéros de port utilisés sur le schéma. Les X sont à remplacer par votre numéro d'établi.

Les ordinateurs clients seront connectés sur le switch d'accès CISCO 2960, nommé S1.

S1 sera relié par un lien trunk vers chaque switch de cœur des réseaux SR1 et SR2. Les switches cœurs de réseaux seront eux-mêmes reliés par un lien trunk.

V. Configuration SSH et sécurité

Vous configurerez la connexion SSH sur chaque switch et routeur du réseau. La mise en œuvre de la sécurité passera par la désactivation des ports non utilisés sur le switch.

De la même manière, la gestion du serveur Ubuntu se fera en SSH depuis le poste administrateur.

VI. Configuration des VLAN

3 VLANs seront créés sur tous les switches du réseau :

- VLAN Data, VLAN ID : 10[1][2][3]
- VLAN Server, VLAN ID : 20
- VLAN Administration, VLAN ID : 100

Vous créerez les interfaces VLAN suivantes :

- sur SR1 :
 - int VLAN 10 192.168.10.252/24
 - int VLAN 20 192.168.20.252/24
 - int VLAN 100 192.168.100.252/24
- et SR2 :
 - int VLAN 10 192.168.10.253/24
 - int VLAN 20 192.168.20.253/24
 - int VLAN 100 192.168.100.253/24

Le tableau suivant synthétise les informations sur les VLANs à gérer.

VLAN	Adresse sur SR1	Adresse sur SR2
VLAN Data, VLAN ID : 10	192.168.10.252/24	192.168.10.253/24
VLAN Server, VLAN ID : 20	192.168.20.252/24	192.168.20.253/24
VLAN Administration, VLAN ID : 100	192.168.100.252/24	192.168.100.253/24
VLAN 36	Géré par le FAI	

VII. Haute disponibilité - niveau 2

Une instance de spanning-tree sera mise en œuvre pour chacun des VLAN. SR2 sera root bridge pour le VLAN Server, SR1 sera root bridge pour les autres VLAN.

VIII. Configuration du routage

Sur le réseau local dont vous avez la charge, vous utiliserez le protocole de routage dynamique OSPF (une seule zone, pas d'annonce OSPF (LSA) en dehors du LAN).

Les routes par défaut seront annoncées avec des métriques de type E1.[4]

IX. Configuration du NAT

Le NAT dynamique sera configuré sur R3 et R4. Seules les machines connectées au réseau d'accès[5] (adresses IP 192.168.XX.YY/24) sont autorisées à accéder à Internet.

X. Haute disponibilité - niveau 3

Afin d'améliorer la haute disponibilité, VRRP est configuré sur les switches L3.

SR1 est routeur maître (priorité de 100) sur les VLAN 20 et 100, et l'adresse IP virtuelle sera 192.168.Y.254/24 (Y sera remplacé par la valeur du VLAN). La priorité du routeur sera décrétementée de 20 si l'interface reliée au routeur R4 est défaillante. Dans ce cas, c'est le routeur SR2 qui deviendra maître.

Le mode VRRP sera préempté et les annonces se feront toutes les 4 secondes.

SR2 sera routeur maître (priorité de 100) sur le VLAN10 et l'adresse IP virtuelle sera 192.168.10.254/24. La priorité du routeur sera décrétementée de 20 si l'interface reliée au routeur R3 est défaillante.

XI. Service DNS:

Ce service sera installé et configuré sur le serveur Windows Server. Votre serveur DNS fera autorité sur le domaine butrtx.lan [6][7][8](X correspond à votre numéro d'établi)[9]. Il contiendra obligatoirement les enregistrements mail.butrtX.lan avec X ∈ [1,8], donc pour votre serveur de messagerie ainsi que pour les serveurs des autres binômes.

Attention aux adresses IP que vous choisirez !!!

XII. Service DHCP:

Un seul serveur DHCP sera activé dans votre entreprise mais ce dernier contiendra plusieurs étendues : une pour chaque Vlan sauf le Vlan serveur qui lui sera en adressage IP statique.

XIII. Service de messagerie :

Ce service sera configuré sur un serveur Ubuntu 20. Chaque binôme aura en charge son nom de domaine butrtX.lan* (X correspond à votre numéro d'établi). Chacun des utilisateurs (bob, phil, max, samir, eli) possède

une boîte aux lettres sur le serveur de messagerie se trouvant dans le Vlan20. Leurs adresses emails seront donc, par exemple, de la forme : bob@butrt4.lan pour l'établi 4. Un utilisateur d'un établi (ex: phil@butrt6.lan) pourra envoyer des emails vers n'importe quel utilisateur (ex: eli@butrt2.lan). Dans un premier temps, l'authentification au serveur de messagerie sera une liste d'utilisateurs contenue dans le serveur Linux/Ubuntu. L'authentification à la boîte aux lettres à partir de l'AD est un Bonus (vous ferez cela en dernier si vous avez du temps). Le serveur de messagerie accèdera à Internet en priorité par le Vlan36[10].[11][12]

Sécurisation d'accès au serveur : L'envoi et la lecture des emails depuis le MUA (Mail User Agent, privilégier l'utilisation de Thunderbird) se fera de façon sécurisée. Dans ce cas, l'authentification du serveur sera effectuée par des certificats numériques auto-signés (Cf ressource R303 Travaux Pratiques).

* le serveur DNS fera autorité sur le domaine butrX.lan

Bonus : Les comptes utilisateurs de la messagerie sont sur le serveur AD.[13]

XIV. Sécurité et ACL

Vous mettrez en œuvre des ACL sur les switchs L3 pour que l'administration des serveurs Ubuntu et AD soit possible depuis le poste de l'administrateur uniquement. Cette ACL ne devra pas entraver l'accès au service de messagerie et d'Active Directory.

XV. Annuaire Active Directory

Les informations concernant la mise en œuvre d'un serveur Active Directory seront données dans le chapitre suivant.

AD DS du Campus de l'Université de Hogwards

I. Configuration de l'architecture AD DS sur le site Hogwards-Ouest

L'Université de Hogwards dispense différentes formations sur 2 sites situés à proximité dans la même ville. Environ 400 étudiants, 80 enseignants. 40 administratifs travaillent sur les 2 sites.

Pour une meilleure gestion de son réseau, on décide de mettre en place l'annuaire AD DS. Cet annuaire doit gérer le parc informatique de l'Université ainsi que l'authentification sécurisée des utilisateurs et des ordinateurs.

Les 2 sites de l'Université hébergent 3 départements qui feront partie du même forest AD.

Site Hogwards-Ouest (le site situé dans la partie ouest de la ville)	Site Hogwards-Nord (le site situé dans la partie nord de la ville)
Département administratif central (appelé ac) Domaine racine : butrtX.lan Où X est le nr de votre établi	Département GEII (appelé geii) Domaine geii.butrtX.lan Où X est le nr de votre établi
Département RT (appelé rt) Domaine butrtX.lan Où X est le nr de votre établi	

Le site **Hogwards-Ouest** héberge 2 départements :

- Département administratif central (appelé AC)
- Département RT (appelé RT)

Le **Département administratif central**, constituera le **domaine racine** appelé **butrtX.lan**. Il gère

- le personnel administratif et
- le parc informatique du réseau du personnel administratif.

Le **département RT (Réseaux et Télécommunications)** sera géré dans le même domaine **butrtX.lan**. Il gère

- le parc informatique des salles de TP,
- les comptes des étudiants du département,
- les comptes des professeurs et leurs ordinateurs (chaque professeur a un ordinateur propre).

Le site **Site Hogwards-Nord** héberge 1 département :

- Département GEII (Génie Electrique et Informatique Industrielle)

Le département GEII (Génie Electrique et Informatique Industrielle) faisant partie du domaine **geii.butrtX.lan**, gère :

- le parc informatique des salles de TP,
- les comptes des étudiants du département,

- les comptes des professeurs et leurs ordinateurs (chaque professeur a un ordinateur propre).

II. A faire dans le domaine hogwards.edu sur le site Hogwards-Ouest

Le rôle AD DS sera installé sur la VMware ESXi, Windows Server, dans le sous-réseau spécifié dans l'architecture.

La mise en place du domaine **butrtX.lan** nécessite de suivre les étapes ci-dessous.

A. Etapes pour la mise en place du domaine hogwards.edu.

Dans **la section III** vous trouverez les descriptions des éléments nécessaires : site, domaine, DC, OUs, Users, groupes, comptes ordinateurs.

La création manuelle de cette structure risque de prendre beaucoup de temps. Le risque d'avoir des erreurs est très important. Pour cette raison, il est préférable d'utiliser **les scripts PowerShell** pour la création des comptes utilisateurs, ordinateurs et groupes.

1. Création du site, du domaine et du DC (Domaine Controller) (voir le chapitre Managing sites and subnets)
2. Créations des OUs, Groups (voire Section III et Annex 2),
3. Création des comptes utilisateurs (voire Section III et Annex 1)
4. Création des comptes ordinateurs (Section III et le chapitre Managing Computer Account)

Une fois le domaine mis en place, valider son bon fonctionnement !

B. Étapes pour la personnalisation de la configuration du domaine butrtX.lan

Une fois le domaine créé intégralement et validé, vous pouvez personnaliser la configuration de votre parc informatique. Vous devez créer des GPOs et des politiques de configuration des mots de passe spécifiques aux groupes d'utilisateurs définis.

Les différentes PSOs et GPO qui doivent être implémentées sont décrites dans la **section IV** (voir aussi le Chapitre Groupe Policy Object).

1. Sécurisation des mots de passe – création des PSOs.
2. Création des GPOs pour les configurations Utilisateur et Ordinateur

III. Description du site **Hogwards-Ouest**

1. Description du site, du domaine et du DC (Domaine Controller)

!!!! X doit être remplacé par le nr de votre établi

Le site Hogwards-Ouest

Nom : HogOuest-SiteX

Location : Hogwards

Description : Université Hogwards – Départements AC et R&T

Sous-réseau : spécifié dans le document d'architecture

!!!! X doit être remplacé par le nr de votre établi

Le DC (Domaine Controller / Contrôleur de Domaine)

Nom : HogOuest-DCX

Type : DC principal (pas de RODC)

Fonctionnalités :

- Il doit avoir la fonctionnalité de Catalogue Global,
- Vous devez changer le répertoire implicite de Sysvol

DNS :

- Le DNS doit être installé lors de l'installation du rôle AD DS.

Définition des sous-réseaux

3 sous-réseaux doivent être définis correspondants aux VLANs 10, 20 et 100. Pour leur description voir l'Annexe Adressage plus loin.

2. Description des OUs, Groups, comptes Users et Ordinateurs

Définition des OUs

!!!! X doit être remplacé par le numéro de votre établi

Nom de l'OU	Description de l'OU	Location de l'OU
HogOuest-ACX	Top Level OU - associé au département AC	Site Hogwards Ouest
Users-ACX	Les utilisateurs du département AC	Site Hogwards Ouest
Ordi-ACX	Les ordinateurs du département AC	Site Hogwards Ouest
Groups-ACX	Les groupes du département AC	Site Hogwards Ouest
HogOuest-RTX	Top Level OU - associé au département RT	Site Hogwards Ouest
Users-RTX	Les utilisateurs du département RT	Site Hogwards Ouest
Ordi-RTX	Les ordinateurs du département RT	Site Hogwards Ouest
Groups-RTX	Les groupes du département RT	Site Hogwards Ouest

Définition des groupes AC

!!!! X doit être remplacé par le nr de votre établi

Nom du groupe	Type	Etendue	Créé dans la OU	Description du groupe
AC-GrO- Comptax	Sécurité	Locale	Groups-ACX	Ordinateurs du personnel travaillant dans la comptabilité
AC-GrO-Adminsx	Sécurité	Locale	Groups-ACX	Ordinateurs des administrateurs réseau
AC-GrO-Othersx	Sécurité	Locale	Groups-ACX	Ordinateurs des employés
AC-GrU- Comptax	Sécurité	Globale	Groups-ACX	Utilisateurs travaillant dans la comptabilité
AC-GrU-Adminsx	Sécurité	Globale	Groups-ACX	Utilisateurs administrateurs du réseau
AC-GrU-Othersx	Sécurité	Locale	Groups-ACX	Les autres employés

Définition des groupes RT

!!!! X doit être remplacé par le nr de votre établi

Nom du groupe	Type	Etendue	Créé dans la OU	Description du groupe
RT-GrO-H33x	Sécurité	Locale	Groups-RTX	Ordinateurs de la salle TP H33
RT-GrO-Prof sx	Sécurité	Locale	Groups-RTX	Ordinateurs des professeurs RT
RT1-GrU-Etudiantx	Sécurité	Locale	Groups-RTX	Utilisateurs Etudiants RT1
RT2-GrU-Etudiantx	Sécurité	Locale	Groups-RTX	Utilisateurs Etudiants RT2
RT-GrU-Prof sx	Sécurité	Globale	Groups-RTX	Utilisateurs Professeurs RT

Définition des comptes utilisateurs et les groupes associés

Rappel des groupes Utilisateurs

!!!! x doit être remplacé par le nr de votre établi

Nom du groupe	Type	Etendue	Créé dans la OU	Description du groupe
AC-GrU- Comptax	Sécurité	Globale	Groups-ACx	Utilisateurs travaillant dans la comptabilité
AC-GrU-Adminsx	Sécurité	Globale	Groups-ACx	Utilisateurs administrateurs du réseau
AC-GrU-Othersx	Sécurité	Locale	Groups-ACx	Les autres employés
RT1-GrU-Etudiantx	Sécurité	Locale	Groups-RTx	Utilisateurs Etudiants RT1
RT2-GrU-Etudiantx	Sécurité	Locale	Groups-RTx	Utilisateurs Etudiants RT2
RT-GrU-Prof sx	Sécurité	Globale	Groups-RTx	Utilisateurs Professeurs RT

Il faut créer les comptes suivants.

Dans le tableau ci-dessous « i » prendra les valeurs de 1 à N (la valeur de la première colonne).

!!!! X doit être remplacé par le nr de votre établi

N (Nbr de comptes)	Prénom	Nom	samAccountName (nom de connexion)	Compte défini dans la OU	Membre du Group
4	Alain-i	Compta-i	Compta-i	Users-ACx	AC-GrU- Comptax
2	Bernard-i	Admin-i	Admin-i	Users-ACx	AC-GrU-Adminsx
8	Quentin-i	Other-i	Other-i	Users-ACx	AC-GrU-Othersx
15	Mathis-i	RT1-Etudiant-i	RT1-Etudiant-i	Users-RTx	RT1-GrU-Etudiantx
10	Justin-i	RT2- Etudiant-i	RT2- Etudiant-i	Users-RTx	RT2-GrU-Etudiantx
4	Anna-i	RT-Prof1-i	RT-Prof1-i	Users-RTx	RT-GrU-Prof sx
6	Thomas-i	RT-Prof2-i	RT-Prof2-i	Users-RTx	RT-GrU-Prof sx

Exemple :

On doit définir 4 comptes utilisateurs :

Prenom	Nom	samAccountName (nom de connexion)	Membre du Group
Alain-1	Compta-1	Compta-1	AC-GrU-Comptax
Alain-2	Compta-2	Compta-2	AC-GrU- Comptax
Alain-3	Compta-3	Compta-3	AC-GrU- Comptax
Alain-4	Compta-4	Compta-4	AC-GrU-Contax

Définition des comptes ordinateurs et les groupes associés

Rappel des groupes Ordinateurs

!!!! X doit être remplacé par le nr de votre établi

Nom du groupe	Type	Etendue	Créé dans la OU	Description du groupe
AC-GrO-Comptax	Sécurité	Locale	Groups-ACx	Ordinateurs du personnel travaillant dans la comptabilité
AC-GrO-Adminsx	Sécurité	Locale	Groups-ACx	Ordinateurs des administrateurs réseau
AC-GrO-Othersx	Sécurité	Locale	Groups-ACx	Ordinateurs des employés
RT-GrO-H33x	Sécurité	Locale	Groups-RTx	Ordinateurs de la salle TP H33
RT-GrO-Prof sx	Sécurité	Locale	Groups-RTx	Ordinateurs des professeurs RT

Il faut créer les comptes suivants

Dans le tableau ci-dessous « i » prendra les valeurs de 1 à N (la valeur de la première colonne).

!!!! X doit être remplacé par le nr de votre établi

N (Nbr de comptes)	Ordinateur	Compte défini dans la OU	Membre du Group
4	OrdiCompta-i	Ordi-ACx	AC-GrO-Comptax
2	OrdiAdmin-i	Ordi-ACx	AC-GrO-Adminsx
8	OrdiOther-i	Ordi-ACx	AC-GrO-Othersx
20	H33-PC-i	Ordi-RTx	RT-GrO-H33x
4	RT-PC-Prof1-i	Ordi-RTx	RT-GrO-Profsx
6	RT-PC-Prof2-i	Ordi-RTx	RT-GrO-Profsx

IV. Description des GPOs et FGPP pour le site Hogwards-Ouest

1. Politique de mot de passe (Fine-Grained Password Policies)

Les 3 politiques de mot de passe suivantes seront créées avec l'interface graphique, à l'aide de la console ADAC.

1. **FGPP AdminPSO** : pour le groupe AC-GrU-Admins (Administrateurs) – Name: AdminPSO
2. **FGPP ComptaPSO** : pour le groupe AC-GrU- Compta (Comptabilité) – Nom: ComptaPSO
3. **FGPP ProfPSO** : pour le groupe RT-GrU-Prof (professeurs) – Nom: ProfPSO

Name	AdminPSO	ComptaPSO	ProfPSO
Description	FGPP Administrateur	FGPP Comptabilité	FGPP Professeur
Group associé	AC-GrU-Admins	AC-GrU- Compta	RT-GrU-Prof
Minimum password length	12	10	8
Number of passwords to remember	3	2	1
Password must meet complexity requirements	A définir	A définir	A définir
Minimum password age			
Maximum password age	15 jours	30 jours	6 mois
Account lockout policy (optional)			
Number of failed logon attempts allowed	2	3	3
Reset failed logon count after n minutes	3	3	3
Account will be locked out for n minutes or until administrator unlocks the account	1	1	1

2. GPO pour la personnalisation des comptes utilisateur des professeurs

Description de la GPOs pour les configurations Utilisateur des comptes professeur.

Créez une GPO pour la configuration utilisateur des comptes professeurs et reliez cette GPO à la OU correspondante. Vous devez configurer :

- le temps d'inactivité (idle time) avant le démarrage du screen saver. L'écran sera bloqué (locked) quand le screen saver se déclenchera. L'utilisateur doit retaper son mdp.
- Configurer le fond d'écran en utilisant une image quelconque

3. Install GPO - Configuration de l'installation d'une application

Cette GPOs doit avoir une configurations Utilisateur et être associé à l'OU des **comptes Users des professeurs**.

La GPO doit installer le logiciel **7-zip File Manager**.

Pour la description détaillée de cette tâche voir **l'Annexe – Convertir un fichier .exe en .msi**, plus loin, ainsi que le chapitre sur les GPOs.

4. logon GPO - Configuration à la connexion

Cette GPOs sera associée à la configuration Utilisateur des « comptes étudiants »

Voir le chapitre sur les GPOs (Assigning Logon Scripts in a GPO).

5. Startup GPO - Configuration démarrage de l'ordinateur

Cette GPOs sera associée à la configuration Ordinateur des « ordinateur des professeurs ».

Voir le chapitre sur les GPOs (Startup Scripts in a GPO).

Bonus – création du site Hogwards-Nord

V. Description du site Hogwards-Nord

VI. A faire dans le domaine **geii.butrtX.lan**

A fournir – En fonction de votre avancement

Annexe - Virtualisation des services

Le serveur HP Proliant possède 2 interfaces Gi1 et Gi2. L'hyperviseur VMware Esxi va gérer les VMs.

Seule l'interface Gi2 (cordon blanc) sera utilisée pour connecter les VM de cette SAE à votre réseau.

L'interface Gi1 sera utilisée pour la gestion de l'ESXi. Elle est raccordée à la prise murale et ne doit jamais être déconnectée.

Les VM seront connectées sur le **vSwitch1** et seront reliées au réseau par **l'interface physique vmnic1** (voir document ressource).

Les adresses IP de **gestion des ESXi** sont **192.168.35.1X/24**, X étant le numéro de votre établi.

Vous possédez un **compte** avec des droits limités mais qui vous permet de créer/supprimer/modifier des VM.

Les **login/Mdp** sont **etudiant/Velizy78!**.

Le datastore de l'hyperviseur contient les fichiers iso des OS à installer.

Les serveurs Windows et Linux Ubuntu seront gérés par l'hyperviseur VMware Esxi.

Annexe - Adressage

Adressage des sous-réseaux

Sous-réseau	Adresse	
Gestion de l'ESXi	192.168.35.1X/24 (X étant le numéro de votre établi)	login/Mdp : etudiant/Velizy78!
AD Windows, Serveur Mail,	VLAN Server, VLAN ID : 20 192.168.20.252/24	
PCs	VLAN Data, VLAN ID : 10 192.168.10.252/24	
SR1 – R4	172.16.14.0/28	
SR2 - R3	172.16.23.0/28	
R4 – Routeur Département RT	sur le réseau du département R&T, l'adresse « Wan » sera attribuée par un serveur DHCP	
R3- Routeur Cisco 1841	192.168.36.0/24	

Configuration des VLANs

VLAN	Adresse sur SR1	Adresse sur SR2
VLAN Data, VLAN ID : 10	192.168.10.252/24	192.168.10.253/24
VLAN Server, VLAN ID : 20	192.168.20.252/24	192.168.20.253/24
VLAN Administration, VLAN ID : 100	192.168.100.252/24	192.168.100.253/24
VLAN 36	?????	

Annexe – Convertir un fichier .exe en .msi

Lien vers le site de l'éditeur Advanced Installer: <https://www.advancedinstaller.com/>

Tutorial pour la conversion .exe => .msi

<https://www.youtube.com/watch?v=uZc37pVy1ww>

Dans l'exemple présenté à l'adresse suivante on converti le le fichier. Exe du programme **7-zip File Manager** dans un fichier .MSI. En utilisant ce tutorial procédez à la conversion et par la suite à l'installation du package obtenu avec la GPO d'installation.

<https://www.advancedinstaller.com/user-guide/tutorial-convert-exe-to-msi.html>