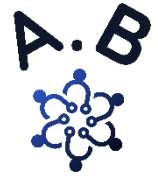


Épreuve du BTS SIO



Umbrella Corp

Dossier Technique

Situation N°1

BARROS ADRIEN

BTS SIO SISR : 2025-2026

VERSION 1.0



DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE		N° réalisation : 1
Nom, prénom : Barros Adrien		N° candidat :02313980410
Épreuve ponctuelle <input type="checkbox"/>	Contrôle en cours de formation <input checked="" type="checkbox"/>	Date : 03 / 06 / 2026
Organisation support de la réalisation professionnelle : Lycée Saint-John Perse		
Intitulé de la réalisation professionnelle : Umbrella Corp		
Période de réalisation : Seconde année Lieu : Lycée Saint-John Perse		
Modalité : <input checked="" type="checkbox"/> Seul(e) <input type="checkbox"/> En équipe		
Compétences travaillées <input checked="" type="checkbox"/> Concevoir une solution d'infrastructure réseau <input checked="" type="checkbox"/> Installer, tester et déployer une solution d'infrastructure réseau <input type="checkbox"/> Exploiter, dépanner et superviser une solution d'infrastructure réseau		
Conditions de réalisation¹ (ressources fournies, résultats attendus) Infrastructure fonctionnelle avec tests de validation effectués sur l'ensemble des services déployés.		
Description des ressources documentaires, matérielles et logicielles utilisées² L'ensemble des ressources documentaires, matérielles et logicielles utilisées est présenté dans ce dossier.		
Modalités d'accès aux productions³ et à leur documentation⁴ Toute la documentation ainsi que les productions réalisées sont présentes et accessibles dans ce document joint.		

¹ En référence aux *conditions de réalisation et ressources nécessaires* du bloc « Administration des systèmes et des réseaux » prévues dans le référentiel de certification du BTS SIO.

² Les réalisations professionnelles sont élaborées dans un environnement technologique conforme à l'annexe II.E du référentiel du BTS SIO.

³ Conformément au référentiel du BTS SIO « *Dans tous les cas, les candidats doivent se munir des outils et ressources techniques nécessaires au déroulement de l'épreuve. Ils sont seuls responsables de la disponibilité et de la mise en œuvre de ces outils et ressources. La circulaire nationale d'organisation précise les conditions matérielles de déroulement des interrogations et les pénalités à appliquer aux candidats qui ne se seraient pas munis des éléments nécessaires au déroulement de l'épreuve.* ». Les éléments nécessaires peuvent être un identifiant, un mot de passe, une adresse réticulaire (URL) d'un espace de stockage et de la présentation de l'organisation du stockage.

⁴ Lien vers la documentation complète, précisant et décrivant, si cela n'a été fait au verso de la fiche, la réalisation, par exemples schéma complet de réseau mis en place et configurations des services.

Sommaire :

SOMMAIRE

1.	Contexte et presentation	3
1.1	Contexte et mission.....	3
1.2	Présentation de l'organisation Umbrella Corp	3
1.3	Besoins.....	3
2.	Schéma réseau.....	4
3.	Informations d'accès aux services de l'infrastructure	5
4.	TABLEAU D'ADRESSAGE.....	6
5.	Spécification technique.....	7
6.	CONFIGURATION DU ROUTEUR.....	8
6.1	Règles Umbrella-pfINT	8
6.2	Règles Umbrella-pfEXT.....	9
6.3	Configuration des routeurs / pare-feux	10
7.	Présentation technique des services déployés par machine.....	11
7.1	Umbrella-sweb.....	11
7.2	Umbrella-sprive.....	12
7.3	Umbrella-mail.....	13
7.4	Umbrella-asterisk.....	14
7.5	Umbrella-pc1 / Umbrella-pc2.....	15
8.	Umbrella-AD.....	16
8.1	Présentation du serveur Active Directory	16
8.2	Organisation Active Directory (OU).....	17
8.3	Serveur de partage de fichiers	19
8.4	Stratégies de groupe (GPO).....	20
8.5	Audit de sécurité Active Directory — PingCastle.....	22

1. CONTEXTE ET PRESENTATION

1.1 Contexte et mission

Dans le cadre de la modernisation de son système d'information, l'entreprise **Umbrella** souhaite restructurer son infrastructure réseau afin d'améliorer la sécurité, la disponibilité et la segmentation de ses services internes et externes.

La mission consiste à concevoir et déployer une infrastructure sécurisée intégrant une DMZ, une messagerie d'entreprise, un système de téléphonie IP et une gestion centralisée des utilisateurs.

1.2 Présentation de l'organisation Umbrella Corp

Umbrella est une entreprise française basée à **Bordeaux**, spécialisée dans la conception, la fabrication et la distribution de parapluies et équipements de protection contre les intempéries.

L'entreprise dispose de plusieurs services internes tels que la direction, l'administration, la logistique, le service commercial et le support client, tous dépendants du système d'information pour assurer le bon fonctionnement de l'activité.

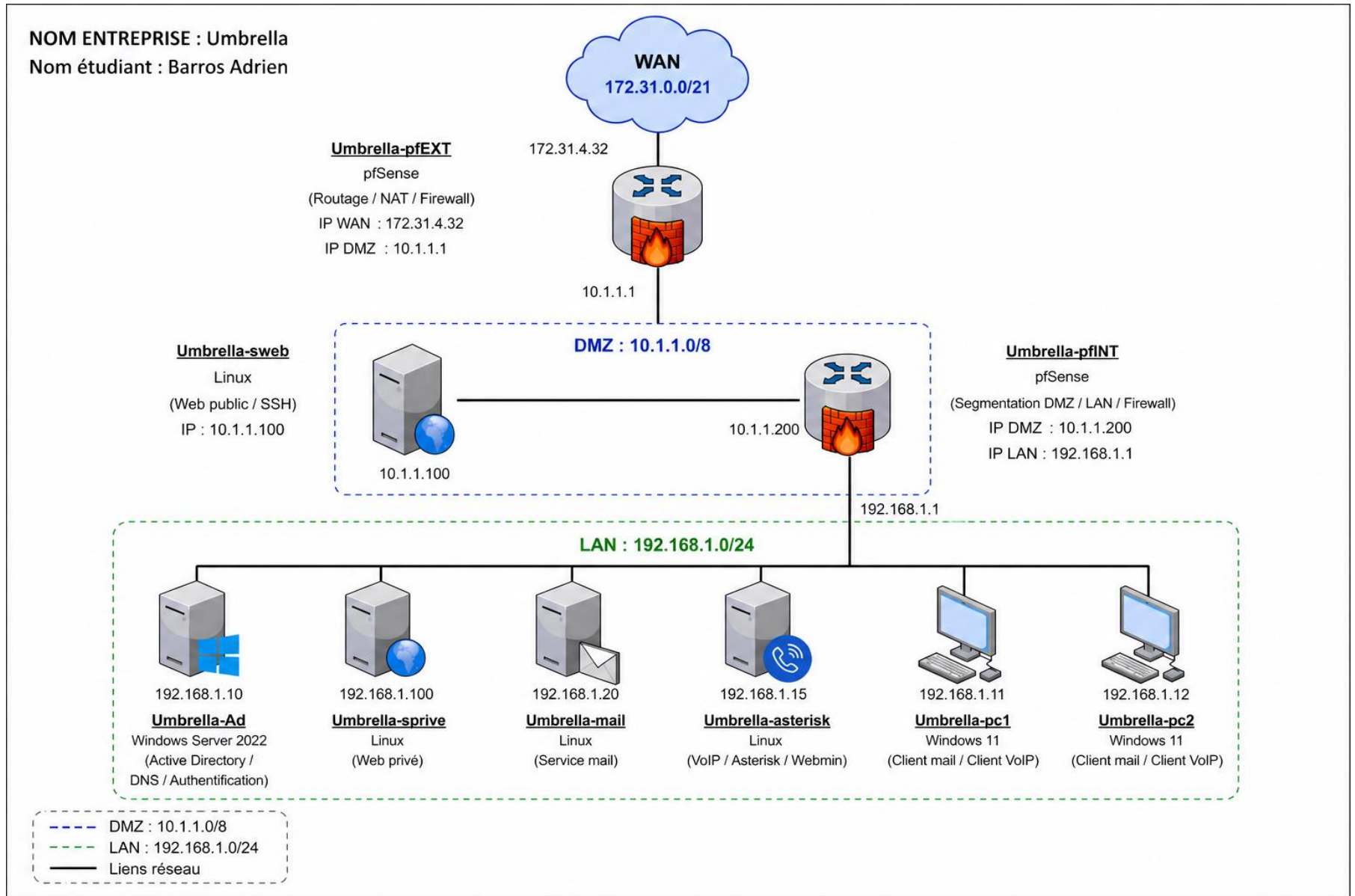
Dans le cadre de son développement, Umbrella souhaite professionnaliser et sécuriser son infrastructure informatique.

1.3 Besoins

Afin d'accompagner sa croissance et sécuriser son système d'information, Umbrella souhaite :

- Isoler les services exposés sur Internet dans une DMZ dédiée
- Mettre en place une authentification centralisée via Active Directory
- Déployer une solution de messagerie professionnelle interne
- Intégrer une infrastructure VoIP pour la téléphonie d'entreprise
- Héberger un site web public et un portail web privé
- Sécuriser les échanges réseau entre WAN, DMZ et LAN via pare-feu pfSense

2. SCHÉMA RÉSEAU



3. INFORMATIONS D'ACCES AUX SERVICES DE L'INFRASTRUCTURE

Service / Accès	Lien / Adresse	Identifiant	Mot de passe	Description
pfSense externe (pfEXT)	http://172.31.4.32/	admin	pfsense	Pare-feu principal assurant le routage WAN ↔ DMZ
pfSense interne (pfINT)	http://10.1.1.200/	admin	pfsense	Pare-feu assurant la segmentation DMZ ↔ LAN
Active Directory — Administrateur	Domaine : umbrella.corp	Administrateur	sio	Compte administrateur du domaine
Active Directory — Administrateur secondaire	Domaine : umbrella.corp	a.wesker	Cochondinde642!	Compte administrateur de démonstration
Active Directory — Utilisateur	Domaine : umbrella.corp	l.kennedy	Cochondinde642!	Compte utilisateur standard du domaine
Webmail Roundcube	https://mail.umbrella.corp/mail/	a.wesker@umbrella.mail	Cochondinde642!	Compte utilisateur de messagerie
Webmail Roundcube	https://mail.umbrella.corp/mail/	l.kennedy@umbrella.mail	Cochondinde642!	Deuxième compte utilisateur de messagerie
Administration iRedMail	https://192.168.1.20/ired-admin/login	postmaster@umbrella.mail	sio	Administration du serveur mail
Asterisk / MicroSIP	Serveur SIP : 192.168.1.15	1001	MotDePasse1001	Compte VoIP utilisateur
Asterisk / MicroSIP	Serveur SIP : 192.168.1.15	1002	MotDePasse1002	Deuxième compte VoIP utilisateur

4. TABLEAU D'ADRESSAGE

Réseau / Postes	IP	CIDR	Gateway	DNS
WAN		21		
Umbrella-pfEXT	172.31.4.32	21	172.31.0.245	
DMZ	10.1.1.0	8		
Umbrella-pfEXT	10.1.1.1	8		
Umbrella-pfINT	10.1.1.200	8		
Umbrella-sweb	10.1.1.100	8	10.1.1.1	192.168.1.10
LAN	192.168.1.0	24		
Umbrella-pfINT	192.168.1.1	24		
Umbrella-Ad	192.168.1.10	24	192.168.1.1	127.0.0.1
Umbrella-sprive	192.168.1.100	24	192.168.1.1	192.168.1.10
Umbrella-mail	192.168.1.20	24	192.168.1.1	192.168.1.10

Umbrella-asterisk	192.168.1.15	24	192.168.1.1	192.168.1.10
Umbrella-pc1	192.168.1.11	24	192.168.1.1	192.168.1.10
Umbrella-pc2	192.168.1.12	24	192.168.1.1	192.168.1.10

5. SPÉCIFICATION TECHNIQUE

Spécifications techniques

Vous trouverez ci-dessous l'ensemble des caractéristiques techniques de chaque machine utilisée dans le cadre du projet :

Machine	Nom	OS	CPU	RAM	Stockage
Routeur	Umbrella-pfEXT	pfSense	1 Coeurs	1Go	16Go
Routeur	Umbrella-pfINT	pfSense	1 Coeurs	1Go	16Go
Serveur Web Public	Umbrella-sweb	Debian 12	2 Coeurs	2Go	20Go
Serveur Active Directory	Umbrella-Ad	Windows Server 2022	4 Coeurs	4Go	80go

Serveur Web Privé	Umbrella-sprive	Debian 12	2 Cœurs	2 Go	20 Go
Serveur Mail	Umbrella-mail	Debian 12	2 Cœurs	2 Go	20 Go
Serveur VoIP	Umbrella-asterisk	Debian 12	2 Cœurs	2 Go	20 Go
Poste Client	Umbrella-pc1	Windows 11	2 Cœurs	4 Go	80 Go
Poste Client	Umbrella-pc2	Windows 11	2 Cœurs	4 Go	80 Go

6. CONFIGURATION DU ROUTEUR

6.1 Règles Umbrella-pfINT

Floating DMZ LAN

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	7/1.33 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0/0 B	IPv4 *	LAN subnets	*	*	*	*	none			
<input type="checkbox"/>	3/43 KiB	IPv4 UDP	*	*	*	53 (DNS)	*	none			
<input type="checkbox"/>	5/7.73 MiB	IPv4 TCP	*	*	*	80 - 443	*	none			
<input type="checkbox"/>	0/0 B	IPv4 ICMP any	*	*	*	*	*	none			
<input type="checkbox"/>	0/23 KiB	IPv4 *	*	*	*	*	*	none			











Add
 Add
 Delete
 Toggle
 Copy
 Save
 Separator

6.2 Règles Umbrella-pfEXT

WAN :

Floating **WAN** DMZ

















































Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	*	*	10.1.1.100	80 (HTTP)	*	none		NAT	    
<input type="checkbox"/>	✗ 0/12 KiB	IPv4 *	*	*	*	*	*	none			    

DMZ :

Floating WAN **DMZ**

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 4/1.05 MiB	*	*	*	DMZ Address	80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	10.1.1.100	*	*	80 (HTTP)	*	none			     
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	10.1.1.100	*	*	443 (HTTPS)	*	none			     
<input type="checkbox"/>	✓ 0/0 B	IPv4 UDP	10.1.1.100	*	*	53 (DNS)	*	none			     
<input type="checkbox"/>	✓ 0/1.80 MiB	IPv4 TCP	10.1.1.200	*	*	80 (HTTP)	*	none			     
<input type="checkbox"/>	✓ 6/4.68 MiB	IPv4 TCP	10.1.1.200	*	*	443 (HTTPS)	*	none			     
<input type="checkbox"/>	✓ 11/83 KiB	IPv4 UDP	10.1.1.200	*	*	53 (DNS)	*	none			     
<input type="checkbox"/>	✓ 0/1 KiB	IPv4 ICMP any.	*	*	*	*	*	none			     
<input type="checkbox"/>	✗ 0/26 KiB	IPv4 *	*	*	*	*	*	none			    

6.3 Configuration des routeurs / pare-feux

L'infrastructure réseau repose sur deux routeurs/pare-feux **pfSense**, assurant la segmentation et la sécurisation des flux entre le WAN, la DMZ et le LAN.

pfSense externe – Umbrella-pfEXT

Le routeur externe est configuré avec deux interfaces réseau, chacune disposant d'une adresse IP statique :

- **em0** correspond à l'interface **WAN**, configurée avec l'adresse IP **172.31.4.32/21**.
- **em1** correspond à l'interface **DMZ**, configurée avec l'adresse IP **10.1.1.1/8**.

Ce pare-feu assure le routage entre Internet et la zone DMZ ainsi que le filtrage des flux entrants/sortants.

pfSense interne – Umbrella-pfINT

Le routeur interne est configuré avec deux interfaces réseau, chacune disposant d'une adresse IP statique :

- **em0** correspond à l'interface **DMZ**, configurée avec l'adresse IP **10.1.1.200/8**.
- **em1** correspond à l'interface **LAN**, configurée avec l'adresse IP **192.168.1.1/24**.

Ce pare-feu assure la segmentation entre la DMZ et le réseau interne de l'entreprise.

Configuration IP

Toutes les adresses IP des interfaces réseau sont définies de manière **statique** (pas de DHCP).

7. PRESENTATION TECHNIQUE DES SERVICES DEPLOYES PAR MACHINE

7.1 Umbrella-sweb

Service : Apache2

Rôle : Serveur web public hébergé dans la DMZ permettant l'accès au site Internet de l'entreprise depuis le WAN.)

Fichier de configuration principal : `/etc/apache2/sites-available/000-default.conf`

Rôle du fichier : Configure le site web principal hébergé sur le serveur Apache.

Répertoire du site web : `/var/www/html`.

Publication du service :

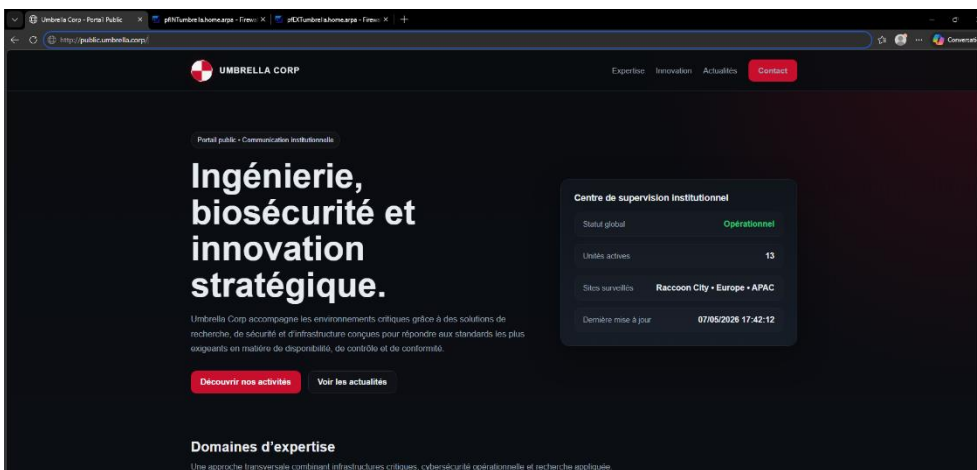
- Redirection NAT configurée sur pfSense externe
- WAN TCP 80 → 10.1.1.100:80

Enregistrement DNS : Un enregistrement DNS nommé `public.umbrella.corp` est configuré sur le serveur Active Directory afin de permettre la résolution du nom vers le serveur web public.

Adresse d'accès : <http://public.umbrella.corp/>

Configuration réseau : Serveur positionné dans la DMZ afin d'isoler le service web du réseau interne.

Validation du service web public Apache2 :



7.2 Umbrella-privé

Service : Apache2

Rôle : Serveur web privé hébergé sur le réseau LAN permettant l'accès à une interface interne réservée aux employés de l'entreprise.

Fichier de configuration principal : /etc/apache2/sites-available/000-default.conf

Rôle du fichier : Configure le site web privé hébergé sur le serveur Apache.

Répertoire du site web : /var/www/html.

Publication du service :

- Service accessible uniquement depuis le réseau interne LAN
- Aucune publication WAN configure

Enregistrement DNS : Un enregistrement DNS nommé `privé.umbrella.corp` est configuré sur le serveur Active Directory afin de permettre la résolution du nom vers le serveur web privé.

Adresse d'accès : <http://privé.umbrella.corp/>

Configuration réseau : Serveur positionné sur le réseau LAN afin de limiter l'accès aux utilisateurs internes de l'entreprise.

Validation du service web privé Apache2 :

The screenshot displays the 'Portail interne Umbrella' interface. The top navigation bar includes the Umbrella Corp logo and the text 'Portail interne Umbrella' with a subtitle 'Accès centralisé aux ressources métiers, à la communication interne et aux services techniques.' A 'Session active' indicator shows the user 'a.barros' is logged in at '07/05/2020 17:52:13'.

The main content area is divided into several sections:

- Tableau de bord:** A sidebar on the left with links for 'Messagerie', 'Téléphonie', 'Ressources RH', 'Documentation IT', 'Support interne', and 'Supervision'.
- Services Internes:** A central section with four status cards:
 - Webmail entreprise:** 'Disponible' (green)
 - Serveur VoIP:** 'Disponible' (green)
 - Supervision Zabbix:** 'Supervisé' (green)
 - Partages réseau:** 'Disponible' (green)
- Notes Internes:** A section on the right with three items:
 - Maintenance planifiée:** 'Une opération de vérification des services internes est prévue ce soir à 22h00.'
 - Politique de sécurité:** 'Le changement de mot de passe est obligatoire à la première ouverture de session.'
 - Support utilisateurs:** 'Pour toute anomalie, contactez le support interne ou ouvrir un ticket via le portail IT.'

At the bottom, there are three red buttons: 'Ouvrir le webmail', 'Accéder à la supervision', and 'Consulter la documentation'.

7.3 Umbrella-mail

Service : iRedMail / Postfix / Dovecot / iRedAdmin

Rôle : Serveur de messagerie permettant l'envoi et la réception des emails au sein de l'entreprise.

Interface administration : IredAdmin

Adresse iRedAdmin : <http://192.168.1.20/iredadmin>

Enregistrement DNS : Un enregistrement DNS nommé mail.umbrella.corp est configuré sur le serveur Active Directory afin de permettre la résolution du serveur de messagerie.

Interface Webmail : Roundcube Webmail

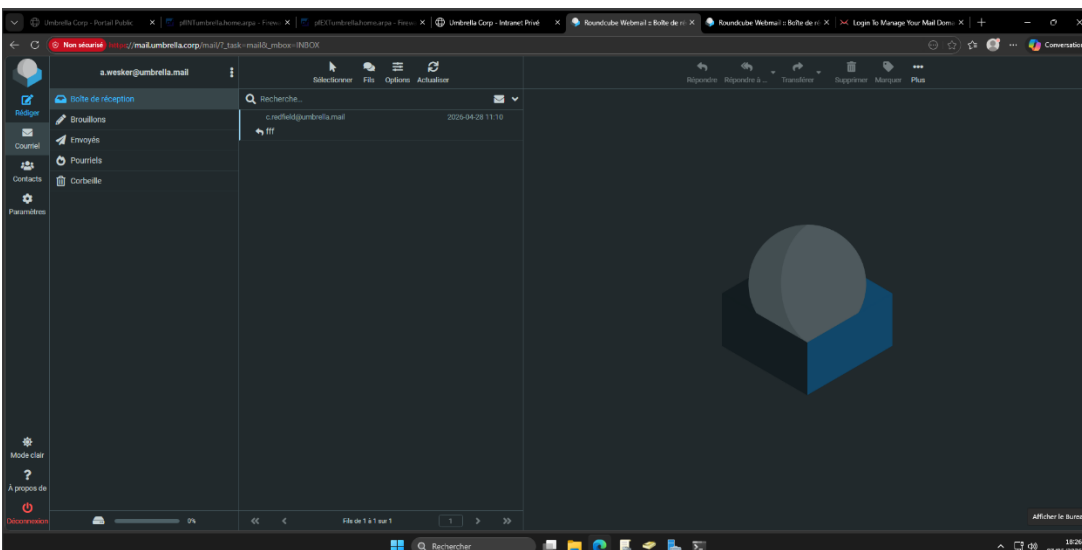
Adresse Webmail : <https://mail.umbrella.corp/mail/>

Protocoles utilisés :

- SMTP (envoi des mails)
- IMAP (consultation des mails)

Configuration réseau : Serveur positionné sur le réseau LAN afin de sécuriser les échanges de messagerie internes.

Validation de l'interface Webmail Roundcube :



7.4 Umbrella-asterisk

Service : Asterisk / Webmin / MicroSIP

Rôle : Serveur de téléphonie IP permettant la communication VoIP entre les utilisateurs de l'entreprise.

Interface d'administration : Webmin

Adresse Webmin : <https://192.168.1.15:10000>

Logiciel client utilisé :

- MicroSIP

Fichier de configuration principal : /etc/asterisk/pjsip.conf

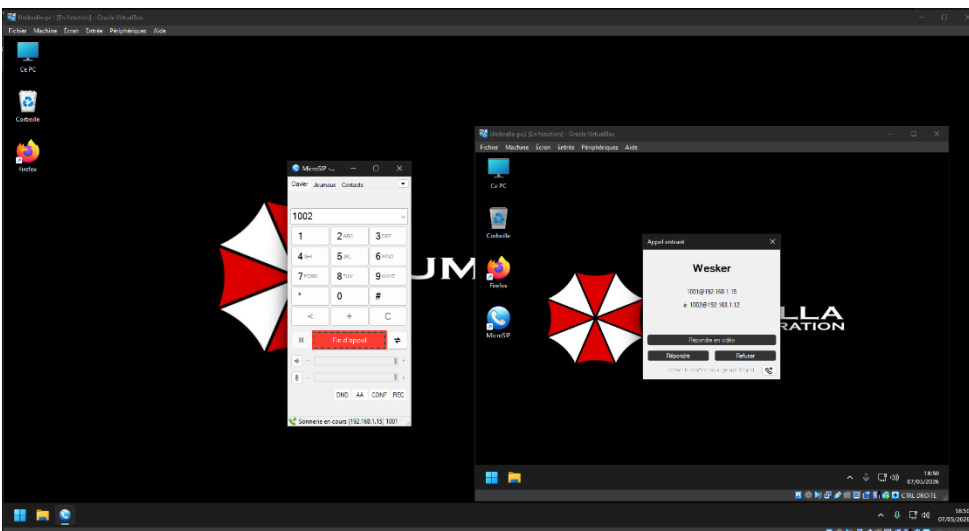
Rôle du fichier : Configure les utilisateurs SIP ainsi que les paramètres principaux du serveur de téléphonie Asterisk.

Fichier de gestion des extensions : /etc/asterisk/extensions.conf

Rôle du fichier : Configure le plan de numérotation ainsi que les appels entre les différentes extensions téléphoniques.

Configuration réseau : Serveur positionné sur le réseau LAN afin de limiter l'accès aux utilisateurs internes de l'entreprise.

Validation de la communication VoIP entre extensions SIP :



7.5 Umbrella-pc1 / Umbrella-pc2

Service : Postes clients utilisateurs

Rôle : Postes clients permettant aux utilisateurs de l'entreprise d'accéder aux différents services du système d'information.

Système d'exploitation : Windows 11

Logiciels installés :

- Firefox
- MicroSIP

Configuration réseau :

- Postes intégrés au réseau LAN
- Adressage IP statique
- Utilisation du serveur Active Directory comme serveur DNS

Adresses IP :

- Umbrella-pc1 : 192.168.1.11
- Umbrella-pc2 : 192.168.1.12

Services accessibles :

- <http://public.umbrella.corp>
- <http://prive.umbrella.corp>
- <https://mail.umbrella.corp/mail/>

Fonctionnalités :

- Navigation web
- Consultation des emails
- Communication VoIP via MicroSIP
- Résolution DNS via le serveur Active Directory

Rôle dans l'infrastructure :

- Validation des services utilisateurs
- Test des communications VoIP
- Vérification des accès réseau internes et externes

8. UMBRELLA-AD

8.1 Présentation du serveur Active Directory

Service : Active Directory / DNS

Système d'exploitation: Windows Server 2022

Rôle : Serveur principal de l'infrastructure assurant l'authentification centralisée des utilisateurs ainsi que la gestion du domaine de l'entreprise.

Nom du domaine : umbrella.corp

Fonctionnalités mises en place :

- Authentification centralisée des utilisateurs
- Gestion des comptes utilisateurs et groupes
- Gestion des ordinateurs du domaine
- Résolution DNS interne
- Application des stratégies de groupe (GPO)
- Gestion des partages réseau

Services installés :

- Active Directory Domain Services (AD DS)
- DNS Server
- Group Policy Management

Configuration réseau :

- Adresse IP statique : 192.168.1.10
- Serveur positionné sur le réseau LAN
- Serveur DNS principal de l'infrastructure

Intégration dans l'infrastructure : Le serveur Active Directory centralise l'administration du système d'information Umbrella et permet aux utilisateurs d'accéder aux ressources réseau via une authentification unique.

Validation du serveur Active Directory Windows Server 2022 :

Gestionnaire de serveur

Gestionnaire de serveur > Tableau de bord

Tableau de bord

- Serveur local
- Tous les serveurs
- AD DS
- DNS
- Services de fichiers et d...

BIENVENUE DANS GESTIONNAIRE DE SERVEUR

1 Configurer ce serveur local

- Ajouter des rôles et des fonctionnalités
- Ajouter d'autres serveurs à gérer
- Créer un groupe de serveurs
- Connecter ce serveur aux services cloud

Rôles et groupes de serveurs

Rôles : 3 | Groupes de serveurs : 1 | Nombre total de serveurs : 1

Rôle	Facilité de gestion	Événements	Services	Performances	Résultats BPA
AD DS	1	1	1	1	1
DNS	1	1	1	1	1
Services de fichiers et de stockage	1	1	1	1	1
Serveur local	1	1	1	1	1
Tous les serveurs	1	1	1	1	1

8.2 Organisation Active Directory (OU)

Service : Organisation des unités d'organisation Active Directory

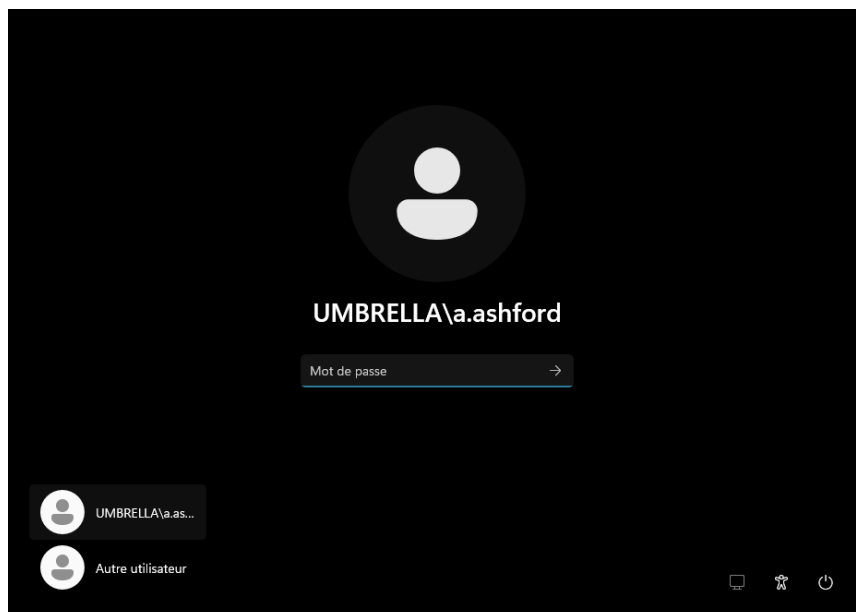
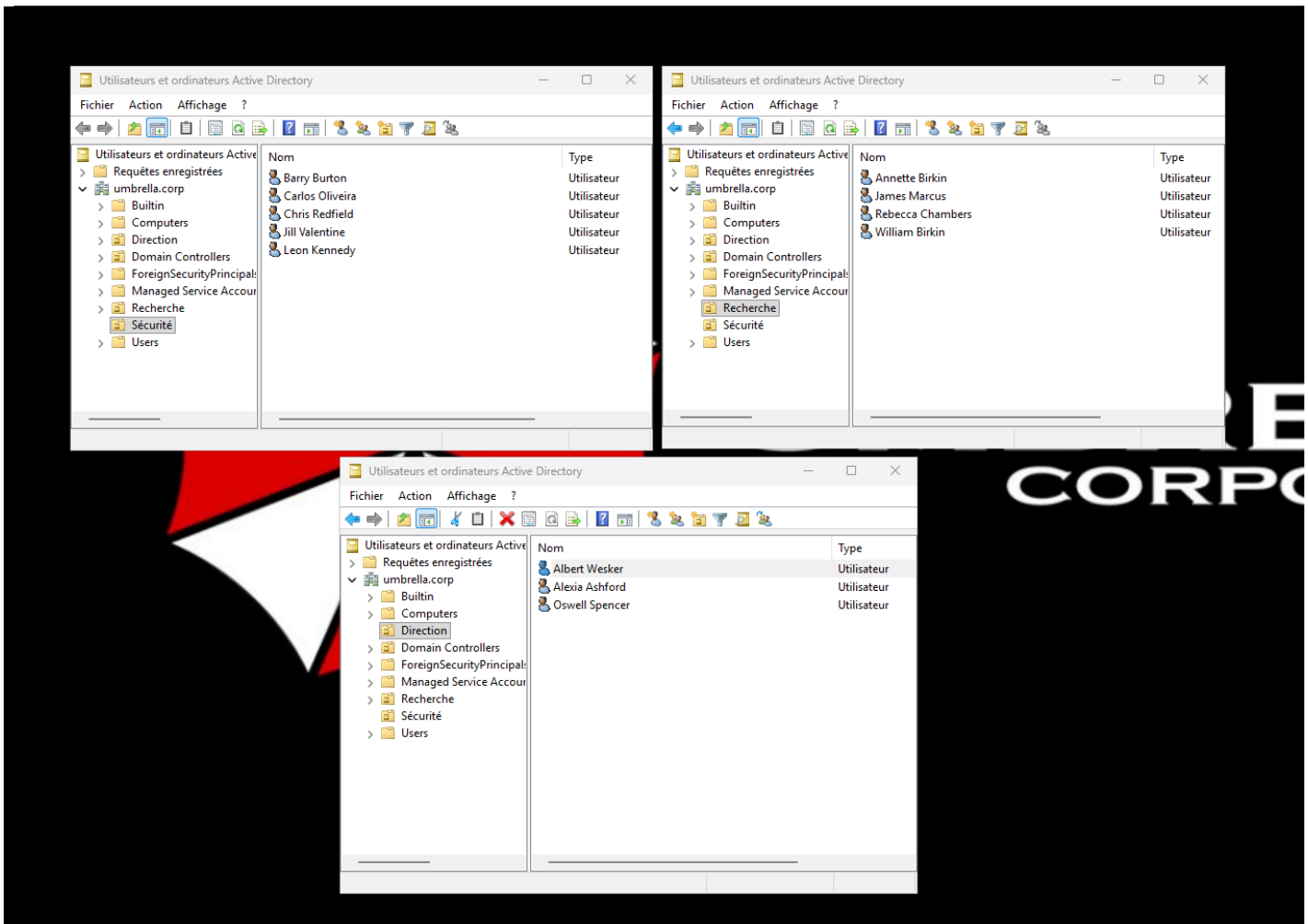
Rôle : Structurer les utilisateurs et les ressources du domaine afin de simplifier l'administration du système d'information.

Organisation mise en place :

- Direction (Albert Wesker, Alexia Ashford, Oswald Spencer)
- Recherche (Annette Birkin, James Marcus, Rebecca Chambers, William Birkin)
- Sécurité (Barry Burton, Carlos Oliveira, Chris Redfield, Jill Valentine, Leon Kennedy)

Fonctionnalités mises en place :

- Séparation logique des utilisateurs par service
- Administration simplifiée des comptes utilisateurs
- Application ciblée des stratégies de groupe (GPO)
- Gestion centralisée des droits et permissions

Validation de l'organisation des utilisateurs dans les unités d'organisation Active Directory :

8.3 Serveur de partage de fichiers

Service : Partages réseau SMB

Rôle : Serveur de fichiers permettant le stockage et le partage des ressources de l'entreprise entre les utilisateurs du domaine.

Partages réseau mis en place :

- Personnel (H:)
- Commun (Z:)

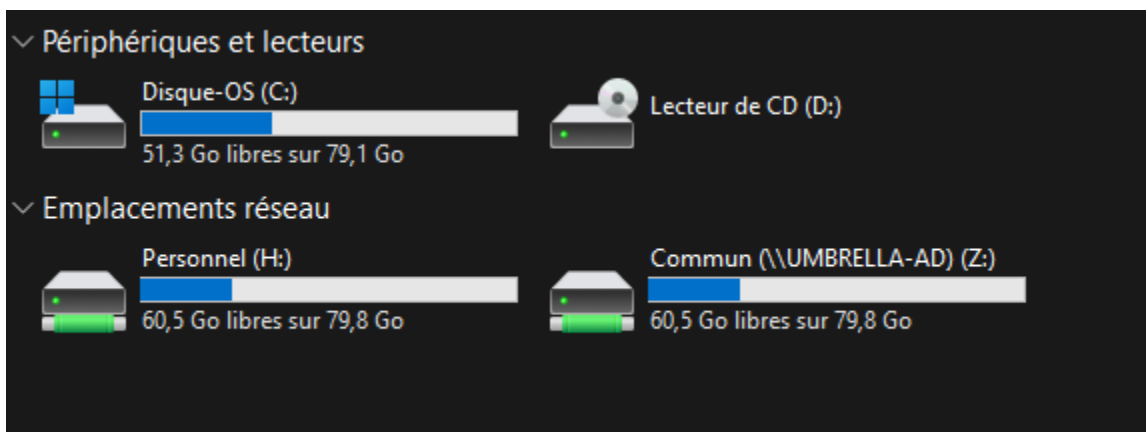
Fonctionnalités mises en place :

- Dossier personnel propre à chaque utilisateur
- Partage commun accessible selon les permissions définies
- Attribution automatique des lecteurs réseau via GPO
- Gestion centralisée des accès utilisateurs

Gestion des permissions : Les accès aux partages réseau sont contrôlés via les groupes et utilisateurs Active Directory afin de sécuriser les données de l'entreprise.

Déploiement automatique : Les lecteurs réseau sont automatiquement montés sur les postes clients via une stratégie de groupe (GPO).

Validation des lecteurs réseau déployés via les stratégies de groupe :



8.4 Stratégies de groupe (GPO)

Service : Group Policy Objects (GPO)

Rôle : Les stratégies de groupe permettent l'administration centralisée des postes et des utilisateurs du domaine umbrella.corp.

Stratégies mises en place :

- GPO_Lecteurs_Reseau
- GPO_Navigateur_Default
- GPO_Sécurité_Poste
- GPO_Sécurité_USB
- GPO_Wallpaper_Umbrella

Configuration des lecteurs réseau : Les lecteurs réseau H: et Z: sont automatiquement montés lors de la connexion des utilisateurs au domaine.

Configuration du navigateur :

Une stratégie de groupe configure automatiquement Firefox afin d'ouvrir par défaut le site web public de l'entreprise : <http://public.umbrella.corp/>

Sécurisation des postes :

Des stratégies de sécurité ont été appliquées afin de limiter certaines actions utilisateurs sur les postes clients :

- Blocage de l'accès au panneau de configuration
- Blocage de l'invite de commandes (CMD)
- Restriction de l'utilisation des périphériques USB via la GPO_Sécurité_USB

Déploiement du fond d'écran : Un fond d'écran personnalisé Umbrella est automatiquement appliqué sur les postes du domaine via une stratégie de groupe.

Politique de mot de passe : Une stratégie de mot de passe est configurée dans la Default Domain Policy afin de renforcer la sécurité des comptes utilisateurs du domaine umbrella.corp.

Paramètres appliqués :

- Complexité des mots de passe activée
- Longueur minimale de 12 caractères
- Historique de 5 mots de passe mémorisés
- Durée maximale des mots de passe fixée à 90 jours
- Durée minimale des mots de passe fixée à 1 jour

Objectif de la stratégie : Cette configuration permet de limiter les risques liés aux mots de passe faibles et d'améliorer la sécurité globale de l'infrastructure Active Directory.

Conformité : Les paramètres appliqués se rapprochent des recommandations de sécurité de la CNIL et de l'ANSSI concernant la gestion des mots de passe en environnement professionnel.

Validation des stratégies de groupe déployées sur le domaine Active Directory

Objets de stratégie de groupe dans umbrella.corp					
Contenu					
Nom	État GPO	Filtre WMI	Modifié le	Propriétaire	
Default Domain Controllers Policy	Activé	Aucun(e)	02/04/2026 14:44:26	Admins du domaine (UMBRELL...	
Default Domain Policy	Activé	Aucun(e)	08/04/2026 20:05:32	Admins du domaine (UMBRELL...	
GPO_Lecteurs_Reseau	Activé	Aucun(e)	09/04/2026 18:39:10	Admins du domaine (UMBRELL...	
GPO_Navigateur_Default	Activé	Aucun(e)	09/04/2026 18:55:02	Admins du domaine (UMBRELL...	
GPO_Sécurité_Poste	Activé	Aucun(e)	09/04/2026 17:21:24	Admins du domaine (UMBRELL...	
GPO_Sécurité_USB	Activé	Aucun(e)	09/04/2026 17:23:32	Admins du domaine (UMBRELL...	
GPO_Wallpaper_Umbrella	Activé	Aucun(e)	09/04/2026 19:07:12	Admins du domaine (UMBRELL...	

Validation de la stratégie de mot de passe du domaine Active Directory

Stratégie	Paramètres de stratégie
Assouplir les limites de longueur minimale du mot de passe	Non défini
Audit de la longueur minimale du mot de passe	Non défini
Conservier l'historique des mots de passe	5 mots de passe mémorisés
Durée de vie maximale du mot de passe	90 jours
Durée de vie minimale du mot de passe	1 jours
Enregistrer les mots de passe en utilisant un chiffrement rév...	Désactivé
Le mot de passe doit respecter des exigences de complexité	Activé
Longueur minimale du mot de passe	12 caractère(s)

8.5 Audit de sécurité Active Directory — PingCastle

Service : PingCastle

Rôle : Outil d'audit de sécurité permettant d'analyser la configuration et le niveau de sécurité de l'infrastructure Active Directory.

Fonctionnalités :

- Analyse des vulnérabilités Active Directory
- Détection des mauvaises pratiques de sécurité
- Vérification des comptes privilégiés
- Analyse des objets obsolètes du domaine
- Génération d'un rapport de sécurité détaillé

Résultat de l'analyse : Un audit de sécurité a été réalisé sur le domaine umbrella.corp afin d'évaluer le niveau global de sécurité de l'infrastructure Active Directory.

Score obtenu :

- Domain Risk Level : 70 / 100

Analyse : Le rapport met en évidence plusieurs points de vigilance concernant les comptes privilégiés ainsi que certaines anomalies de configuration présentes dans le domaine Active Directory.

Objectif de l'audit : Cet audit permet d'identifier les faiblesses de sécurité de l'infrastructure afin d'améliorer progressivement la protection du domaine et des utilisateurs.

Validation de l'audit de sécurité Active Directory avec PingCastle

