

CESI

Livrable 1

Projet Administration du Système d'Information

Groupe 1 : Hugo Breniaux – Arnaud Hittinger – Arthur
Lambert
05/10/2021

Table des matières

Contexte	2
Etat actuel de l'Infrastructure	3
Schéma actuel de l'infrastructure	3
Description.....	3
Serveur Windows.....	4
Serveur IPBX	12
Serveur Web	16
Analyse de sécurité DCIP	18
Hypothèses.....	19
Schéma de la nouvelle Infrastructure	20
Schéma.....	20
Explication des choix.....	20
Procédure de migration	21
Préparer la fusion des deux AD	26

Contexte

La société ANIMUS, leader mondial dans les télécommunications multi-niveaux, ne cesse de s'accroître du fait des besoins croissants sur ce marché.

Elle procède régulièrement à des rachats d'entreprises et notamment des PME. Elle avait entendu parler récemment des difficultés d'une entreprise nommée ABSTERGO qui s'est spécialisée dans les protocoles Bluetooth nouvelle génération.

Cette opportunité n'était pas à rater et, rapidement, la vente de la société s'était conclue.

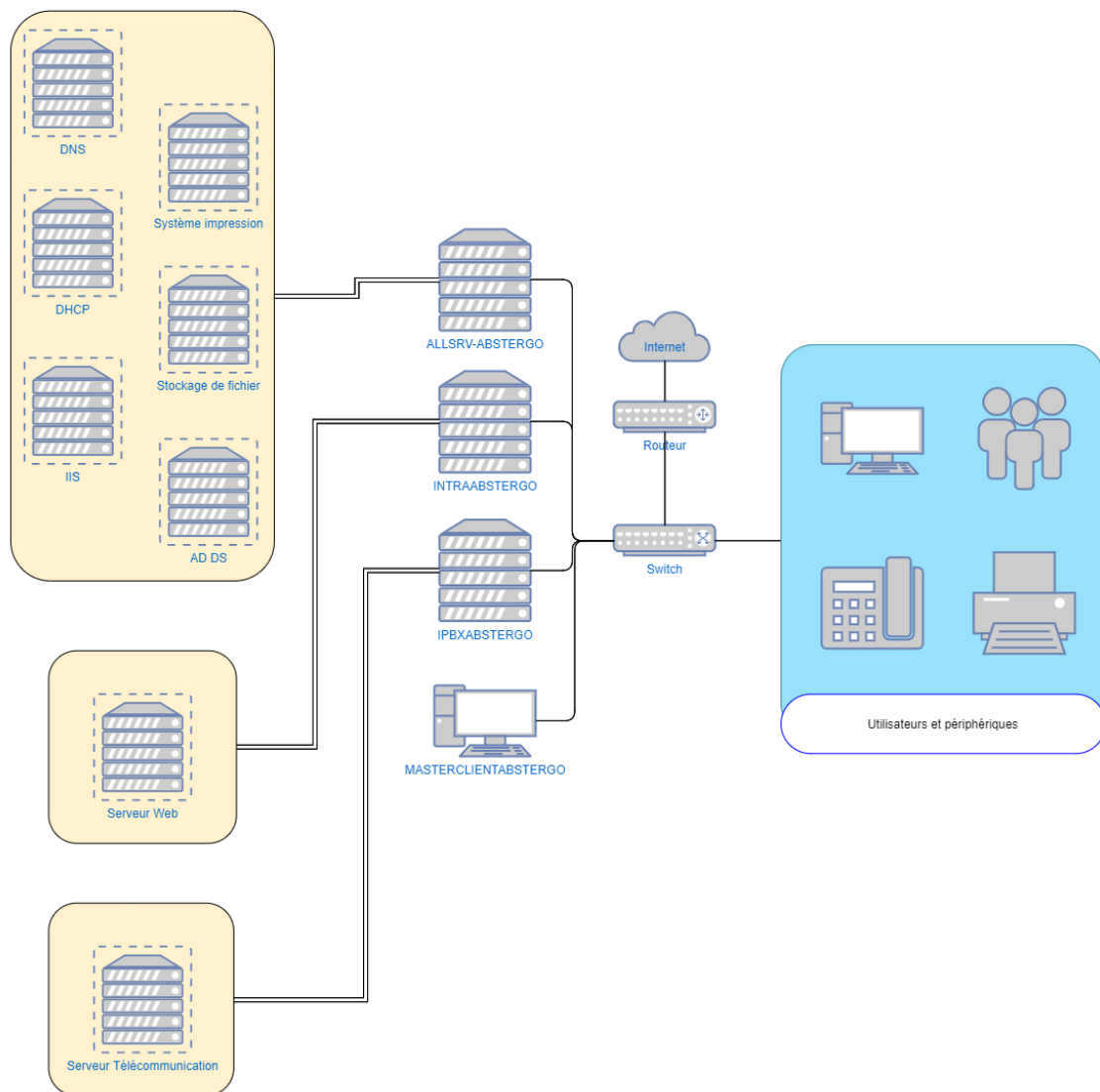
Comme à chaque fois, il est prévu d'intégrer le Système d'Information de l'entreprise rachetée dans celui d'ANIMUS.

ANIMUS nous a donc chargé d'effectuer le travail préparatif pour effectuer cette intégration de Système d'Information.

Nous allons commencer par déterminer la future infrastructure de l'entreprise ABSTERGO avant de l'intégrer dans le Système d'Information de l'entreprise ANIMUS.

Etat actuel de l'Infrastructure

Schéma actuel de l'infrastructure



Description

Dans un premier temps nous avons cartographié la SI actuelle qui est composée d'un routeur et d'un switch, de trois serveurs ainsi que le matériel informatique de l'entreprise. Sur ces serveurs, nous retrouvons un serveur Windows, sur lequel on retrouve un DNS, un DHCP, un IIS, un système d'impression, un partage de fichiers et un AD. Ainsi que deux serveurs Linux un pour héberger un site WEB et un IPBX pour la télécommunication.

Serveur Windows

Le serveur ALLSRV-ABTERGO possède plusieurs services :

Active Directory Domain Services : Fournit les méthodes de stockage des données d'annuaire et de mise à disposition de ces données pour les utilisateurs et administrateurs du réseau.

Active Directory Web Services : est un nouveau service Windows qui fournit une interface de service Web aux domaines Active Directory, aux instances d'Active Directory Lightweight Directory Services (AD LDS) et aux instances de l'outil de montage de base de données Active Directory qui s'exécutent sur le même serveur qu'ADWS.

Application Host Service : Le service d'assistance d'hôte d'application (AppHostSvc) fournit des services administratifs pour IIS, par exemple l'historique de configuration et le mappage de compte de pool d'applications.

AppX Deployment Services (AppXSVC) : Assure la prise en charge de l'infrastructure pour le déploiement d'applications du Store. Ce service démarre à la demande. S'il est désactivé, les applications du Store ne sont pas déployées sur le système et peuvent ne pas fonctionner correctement.

AVCTP service : service de protocole de transport de contrôle audio vidéo

Background Tasks Infrastructure Service : est un service Windows Server 2012 qui contrôle les tâches en arrière-plan pouvant être exécutées sur le système.

Base Filtering Engine : gère les stratégies de pare-feu et IPsec et implémente le filtrage en mode utilisateur. L'arrêt ou la désactivation du service BFE réduit considérablement la sécurité du système et entraîne un comportement imprévisible dans la gestion IPsec et les applications de pare-feu.

Capability Access Manager Services : Service Windows 10. Il fournit des fonctionnalités pour gérer l'accès des applications UWP aux fonctionnalités de l'application, ainsi que pour vérifier l'accès d'une application à des fonctionnalités d'application spécifiques. Ce service existe uniquement sous Windows 10.

Certificate Propagation : Le service de propagation des certificats s'active lorsqu'un utilisateur connecté insère une carte à puce dans un lecteur attaché à l'ordinateur. Cette action entraîne la lecture du certificat à partir de la carte à puce. Les certificats sont ensuite ajoutés au magasin personnel de l'utilisateur. Les actions du service de propagation des certificats sont contrôlées à l'aide de la stratégie de groupe.

Client License Service (ClipSVC) : Permet la prise en charge de l'infrastructure de Microsoft Store. Ce service démarre à la demande. S'il est désactivé, les applications achetées via le Windows Store ne se comportent pas correctement.

CNG Key Isolation : Le service fournit l'isolation du processus de clé aux clés privées et aux opérations cryptographiques associées, comme requis par les Critères communs pour l'évaluation de la sécurité des technologies de l'information

COM+ Event System : Il fournit une distribution automatique des événements aux composants COM qui y sont abonnés. Les événements COM+ étendent le modèle de programmation COM+ pour prendre en charge les événements à liaison tardive ou les appels de méthode entre l'éditeur ou l'abonné et le système d'événements. Le système d'événements avertit les consommateurs d'événements lorsque des informations deviennent disponibles et il n'interroge pas le serveur à plusieurs reprises.

Connected Devices Platforme Service : Ce service est utilisé pour les scénarios de plate-forme d'appareils connectés

Connected Devices Platforme User Service_65573

Connected User Expériences and Telemetry : active des fonctionnalités qui prennent en charge les expériences utilisateur intégrées et connectées. De plus, ce service gère la collecte et la transmission d'informations de diagnostic et d'utilisation basées sur les événements (utilisées pour améliorer l'expérience et la qualité de la plate-forme Windows) lorsque les paramètres des options de diagnostic et de confidentialité de l'utilisation sont activés sous Commentaires.

CoreMessaging : Gère la communication entre les composants du système.

Cryptographique Services : crypte et décrypte les données sur les périphériques de stockage lorsqu'ils y accèdent. Il peut être utilisé pour l'authentification des utilisateurs afin d'archiver le cryptage ou le décryptage.

DCOM Server Process Launcher : Le service DcomLaunch implémente les technologies Component Object Model (COM) et Distributed Component Object Model (DCOM) de Microsoft , qui facilitent respectivement la communication entre les applications et la communication entre les ordinateurs.

Device Setup Manager : Permet la détection, le téléchargement et l'installation des logiciel du Software.

DFS Namespace : service de rôle dans Windows Server qui vous permet de regrouper des dossiers partagés situés sur différents serveurs dans un ou plusieurs espaces de noms logiquement structurés. Cela permet de donner aux utilisateurs une vue virtuelle des dossiers partagés, où un seul chemin mène à des fichiers situés sur plusieurs serveurs

DFS Replication : service de rôle de Windows Server qui permet de répliquer des dossiers de manière efficace (notamment les dossiers désignés par un chemin d'espace de noms DFS) sur plusieurs serveurs et sites.

DHCP Client : Enregistre et met à jour les adresses IP et les enregistrements DNS de votre ordinateur. Si ce service est arrêté, votre ordinateur ne recevra pas les adresses IP dynamiques et les mises à jour DNS. Si ce service est désactivé, tous les services qui en dépendent explicitement ne pourront pas démarrer.

DHCP Server : Ce service attribue des adresses IP aux ordinateurs clients. Ceci est très souvent utilisé dans les réseaux d'entreprise pour réduire les efforts de configuration. Toutes

les adresses IP de tous les ordinateurs sont stockées dans une base de données qui réside sur une machine serveur.

Diagnostic Policy Service : Ce service a pour but de détecter et de dépanner les problèmes potentiels des composants de votre Windows. Il initiera une action corrective automatique ou consignera les informations de diagnostic appropriées pour l'analyse des causes des problèmes, puis informera l'utilisateur du problème potentiel.

Distributed Transaction Coordinator : permet de coordonner des opérations qui s'étendent sur plusieurs gestionnaires de ressources, telles que les bases de données, les files d'attente de messages et les systèmes de fichiers.

DNS Client : Le service client DNS (dnscache) met en cache les noms DNS (Domain Name System) et inscrit le nom complet de cet ordinateur. Si le service est arrêté, les noms DNS continuent d'être résolus. Toutefois, les résultats des requêtes de noms DNS ne sont pas mis en cache et le nom de l'ordinateur n'est pas inscrit. Si le service est désactivé, les services qui en dépendent explicitement ne peuvent pas démarrer.

DNS Server :

Filezilla Server FTP Server : permet de partager et transférer des fichiers entre des PC de votre réseau local LAN ou par internet.

Function Discovery Provider Host : fournit une interface de programmation uniforme pour l'énumération des ressources système, telles que les périphériques matériels, qu'ils soient connectés localement ou via un réseau. Il permet aux applications de découvrir et de gérer des listes de périphériques ou d'objets triés par fonctionnalité ou classe. Les applications et les utilisateurs peuvent utiliser le service hôte du fournisseur de découverte de fonctions pour découvrir les fonctions que leur système peut exécuter, quel que soit le périphérique ou l'architecture logicielle sous-jacente.

Function Discovery Resource Publication : publie des informations sur un ordinateur et les ressources qui sont attachées à cet ordinateur afin qu'elles puissent être découvertes sur le réseau. Si ce service est arrêté, ces ressources ne peuvent pas être publiées et elles ne peuvent pas être découvertes par d'autres ordinateurs sur le réseau.

Group Policy Client : chargé d'appliquer les paramètres configurés par les administrateurs pour l'ordinateur et les utilisateurs via la stratégie de groupe. Si le service est arrêté ou désactivé, les paramètres ne sont pas appliqués et les applications et les composants ne peuvent pas être gérés via la stratégie de groupe. Les composants ou les applications qui dépendent de la stratégie de groupe peuvent ne pas fonctionner si ce service est arrêté ou désactivé.

Hyper-V Data Exchange Service : un des services d'intégration sur Hyper-V qui fournit un mécanisme pour échanger des métadonnées de base entre la machine virtuelle et l'hôte.

Hyper-V Guest Shutdown Service : Fournit un mécanisme pour arrêter le système d'exploitation de cette machine virtuelle à partir des interfaces de gestion sur l'ordinateur physique.

Hyper-V Heartbeat Service : Surveille l'état de machine virtuelle en récupérant à intervalles réguliers des informations.

Hyper-V Remote Desktop Virtualization Service : Fournit une plate-forme pour la communication entre la machine virtuelle et le système d'exploitation s'exécutant sur l'ordinateur physique.

Hyper-V Time Synchronization Service : Synchronise l'heure système de cette machine virtuelle avec l'heure système de l'ordinateur physique.

Hyper-V Volume Shadow Copy Requestor : Coordonne les communications requises pour utiliser le service de cliché instantané de volume pour sauvegarder des applications et des données sur cette machine virtuelle à partir du système d'exploitation sur l'ordinateur physique.

IKE and AuthIP IPsec Keying Modules : Ces modules de clé sont utilisés pour l'authentification et l'échange de clés dans la sécurité du protocole Internet (IPsec). L'arrêt ou la désactivation du service IKEEXT désactivera l'échange de clés IKE et AuthIP avec les ordinateurs homologues. IPsec est généralement configuré pour utiliser IKE ou AuthIP, par conséquent, l'arrêt ou la désactivation du service IKEEXT peut entraîner une défaillance IPsec.

Intersite Messaging : permet des échanges de messages entre les ordinateurs dans un environnement avec des serveurs qui exécutent le système d'exploitation Windows Server. Ce service est utilisé pour la réplication basée sur la messagerie entre les sites. AD DS inclut la prise en charge de la réplication entre les sites via le transport SMTP sur IP. La prise en charge SMTP est fournie par le service SMTP, qui est un composant d'IIS.

IP Helper : Fournit une connectivité de tunnel à l'aide des technologies de transition IPv6 et IP-HTTPS. Si ce service est arrêté, l'ordinateur ne bénéficiera pas des avantages de connectivité améliorés offerts par ces technologies.

IPsec Policy Agent : L'écureuil du protocole Internet(IPsec) prend en charge l'authentification par les pairs au niveau du réseau, l'authentification de l'origine des données, l'intégrité des données, la confidentialité des données (cryptage) et la protection contre la relecture. Ce service applique les stratégies IPsec créées en pensant au composant logiciel enfichable Stratégies de sécurité IP ou à l'outil de ligne de commande « netsh ipsec ».

Kerberos Key Distribution Center : Le protocole Kerberos est un protocole sécurisé et il fournit une authentification mutuelle entre un client et un serveur. Dans le protocole Kerberos, le client s'authentifie auprès du serveur et le serveur s'authentifie également auprès du client. Avec l'authentification mutuelle, chaque ordinateur ou un utilisateur et un ordinateur peuvent vérifier l'identité de l'autre. Kerberos est extrêmement efficace pour authentifier les clients dans les environnements réseau des grandes entreprises. Kerberos utilise le chiffrement par clé secrète pour le trafic d'authentification du client.

La même clé secrète est également utilisée par le protocole Kerberos sur le serveur pour déchiffrer le trafic d'authentification.

Local Session Manager :

Microsoft Account Sign-in Assistant : Activez la connexion utilisateur via les services d'identité de compte Microsoft.

Netlogon : Maintient un canal sécurisé entre cet ordinateur et le contrôleur de domaine pour authentifier les utilisateurs et les services. Si ce service est arrêté, l'ordinateur peut ne pas authentifier les utilisateurs et les services et le contrôleur de domaine ne peut pas enregistrer les enregistrements DNS. Si ce service est désactivé, tous les services qui dépendent fortement de ne pouvoir.

Network Connection Broker : une application logicielle qui sert de liaison entre un client et un serveur ou entre deux ou plusieurs clients homologues.

Network List Service : identifie les réseaux auxquels l'ordinateur s'est connecté, collecte et stocke les propriétés de ces réseaux et avertit les applications lorsque ces propriétés changent. Ce service, associé au service Network Location Awareness, permet d'afficher l'état des connexions réseau dans la zone de notification. Ce service fait partie de Network Diagnostics Framework.

Network Location Awareness : Permet aux applications Windows Sockets 2 d'identifier le réseau logique auquel un ordinateur Windows est connecté.

Network Store Interface Service : Ce service fournit des notifications réseau (par exemple, ajout/suppression d'interface, etc.) aux clients en mode utilisateur. L'arrêt de ce service entraînera une perte de connectivité réseau. Si ce service est désactivé, tous les autres services qui dépendent explicitement de ce service ne pourront pas démarrer.

Plug and Play : Permettez à un ordinateur de reconnaître et de s'adapter aux modifications matérielles avec peu ou pas d'intervention de l'utilisateur. L'arrêt ou la désactivation de ce service entraînera une instabilité du système.

Power : Le service Power implémente les schémas d'alimentation, les stratégies et les notifications de votre ordinateur

Print Spooler : application qui gère les travaux d'impression papier envoyés de l'ordinateur à l'imprimante ou au serveur d'impression.

Remote Access Connection Manager : gère les connexions d'accès à distance et VPN de l'ordinateur à Internet ou à d'autres réseaux distants.

Remote Desktop Configuration : permet à un utilisateur de se connecter à un serveur Windows depuis son poste client.

Remote Desktop Services : Architecture centralisée qui permet à un utilisateur de se connecter sur un ordinateur distant utilisant Microsoft Terminal Services.

Remote Desktop Services UserMode Port Redirector : Remote Desktop Services UserMode Port Redirector

Remote Procedure Call (RPC) : Protocole réseau permettant de faire des appels de procédures sur un ordinateur distant à l'aide d'un serveur d'applications.

RPC Endpoint Mapper : résout les identificateurs d'interface RPC pour transporter les points de terminaison.

Secure Socket Tunneling Protocol Service : un type de tunnel VPN qui fournit un mécanisme pour transporter PPP ou L2TP à travers un canal SSL 3.0. SSL fournit une sécurité au niveau transport avec une négociation de clés, le chiffrement, et le contrôle de l'intégrité des données.

Security Accounts Manager : Il authentifie les ouvertures de session des utilisateurs locaux. Sur un contrôleur de domaine, il stocke simplement le compte administrateur à partir du moment où il était un serveur, qui sert de compte de récupération DSRM (Directory Services Restore Mode).

Server : composant des systèmes d'exploitation Microsoft Windows Server qui permet à un serveur de partager des fichiers et des ressources d'impression avec des clients sur le réseau. Lorsqu'un redirecteur sur un client demande une ressource partagée à partir d'un serveur, le service Serveur sur le serveur répond et achemine la ressource vers le client.

Shell Hardware Detection : surveille et fournit une notification pour les événements matériels de lecture automatique. La lecture automatique est une fonctionnalité qui détecte le contenu tel que des images, de la musique ou des fichiers vidéo sur un périphérique de stockage amovible.

State Repository Service : un service basé sur un navigateur, vous aide à capturer et à stocker des instantanés des sessions de navigation sur le navigateur Web. Cela signifie qu'il peut enregistrer vos informations de navigation, y compris l'historique de navigation, la dernière page affichée dans le navigateur, l'état des objets de script et de document, les informations saisies dans le formulaire sur la dernière page consultée et les cookies.

SysMain : maintient et améliore les performances du système au fil du temps

System Event Notification Service :

System Events Broker

Task Scheduler : un logiciel qui permet de programmer le démarrage de programmes ou de scripts à des temps prédéfinis ou après certains intervalles prédéfinis.

TCP / IP NetBIOS Helper : prend en charge le service NetBIOS sur TCP/IP (NetBT) et fournit la résolution de noms NetBIOS pour les clients de votre réseau. Il permet aux utilisateurs de partager des fichiers, d'imprimer et de se connecter au réseau.

Themes

Time Broker : Coordonne l'exécution du travail en arrière-plan pour l'application WinRT

Touch Keyboard and Handwriting Panel Service :

Update Orchestrator Service : organise les mises à jour pour votre PC. Il fonctionne en arrière-plan et facilite un processus de mise à jour sûr, sécurisé et optimal pour votre PC.

User Access Logging Service : Le service peut collecter les données d'utilisation des clients par rôles de serveur (par exemple : Certificate Services, RMS, Hyper-V, IIS...) et par les produits logiciels installés sur un serveur Windows.

User Manager :

User Profile Service

Volume Shadow Copy : permet d'effectuer des sauvegardes automatiques ou manuelles de fichiers ou de disques, même s'ils sont en cours d'utilisation.

Web Account Manager

Windows Biometric Service : Permet aux applications clientes la possibilité de capturer, comparer, manipuler et stocker des données biométriques sans accéder directement à du matériel ou à un échantillon biométrique.

Windows Connection Manager : Prend des décisions de connexion/déconnexion automatiques en fonction des options de connectivité réseau actuellement disponibles sur le PC et permet la gestion de la connectivité réseau en fonction des paramètres de la stratégie du groupe

Windows Defender Antivirus Network Inspection Service : Composant antivirus de Microsoft Windows.

Windows Defender Antivirus Service : Composant antivirus de Microsoft Windows.

Windows Defender Firewall : Composant antivirus de Microsoft Windows.

Windows Event Log : permet aux utilisateurs et aux administrateurs de voir le journal des événements d'un ordinateur sur cet ordinateur ou sur une machine distante.

Windows Font Cache Service : Optimise les performances des applications en mettant en cache les données de police couramment utilisées.

Windows Management Instrumentation : prend en charge le modèle de données CIM (Common Information Model), qui décrit les objets d'un environnement de gestion.

Windows Process Activation Service : le composant clé qui fournit le modèle de processus et les fonctionnalités de configuration aux applications Web et aux services Web.

Windows Push Notifications System Service : permettre aux développeurs tiers d'envoyer des toasts, des vignettes, des badges et des mises à jour brutes à partir de leur propre service cloud. Cela fournit un mécanisme pour fournir de nouvelles mises à jour à vos utilisateurs de manière économe en énergie et fiable.

Windows Remote Management (WS-Management) : protocole standard soap (Simple Object Access Protocol) pour les pare-feu qui permet au matériel et aux systèmes d'exploitation, de différents fournisseurs, d'interagir.

Windows Security Service : Composant antivirus de Microsoft Windows.

Windows Time : utilise la suite complexe d'algorithmes définie dans les spécifications NTP pour faire en sorte que les horloges des ordinateurs d'un réseau soient aussi précises que possible.

Windows Update : Gère automatiquement les mise à jour du Système.

Windows Update Medic Service : le service Windows Update peut être la cible d'erreurs et d'incohérences de fichiers. Lorsque cela se produit, plusieurs services commencent à s'exécuter en arrière-plan, cherchant à réparer Windows Update. Par conséquent, l'un des composants est le service Windows Update Medic.

WinHTTP Web Proxy Auto-Discovery Service : protocole qui permet à un client HTTP de découvrir automatiquement une configuration de proxy.

Workstation : Composant des systèmes d'exploitation Microsoft Windows Server qui permet à un client de demander des ressources de fichiers et d'impression aux serveurs sur le réseau.

World Wide Web Publishing Service : composant des services Internet (IIS) sur les systèmes d'exploitation Microsoft Windows Server qui permet aux utilisateurs de publier du contenu Web à utiliser sur Internet.

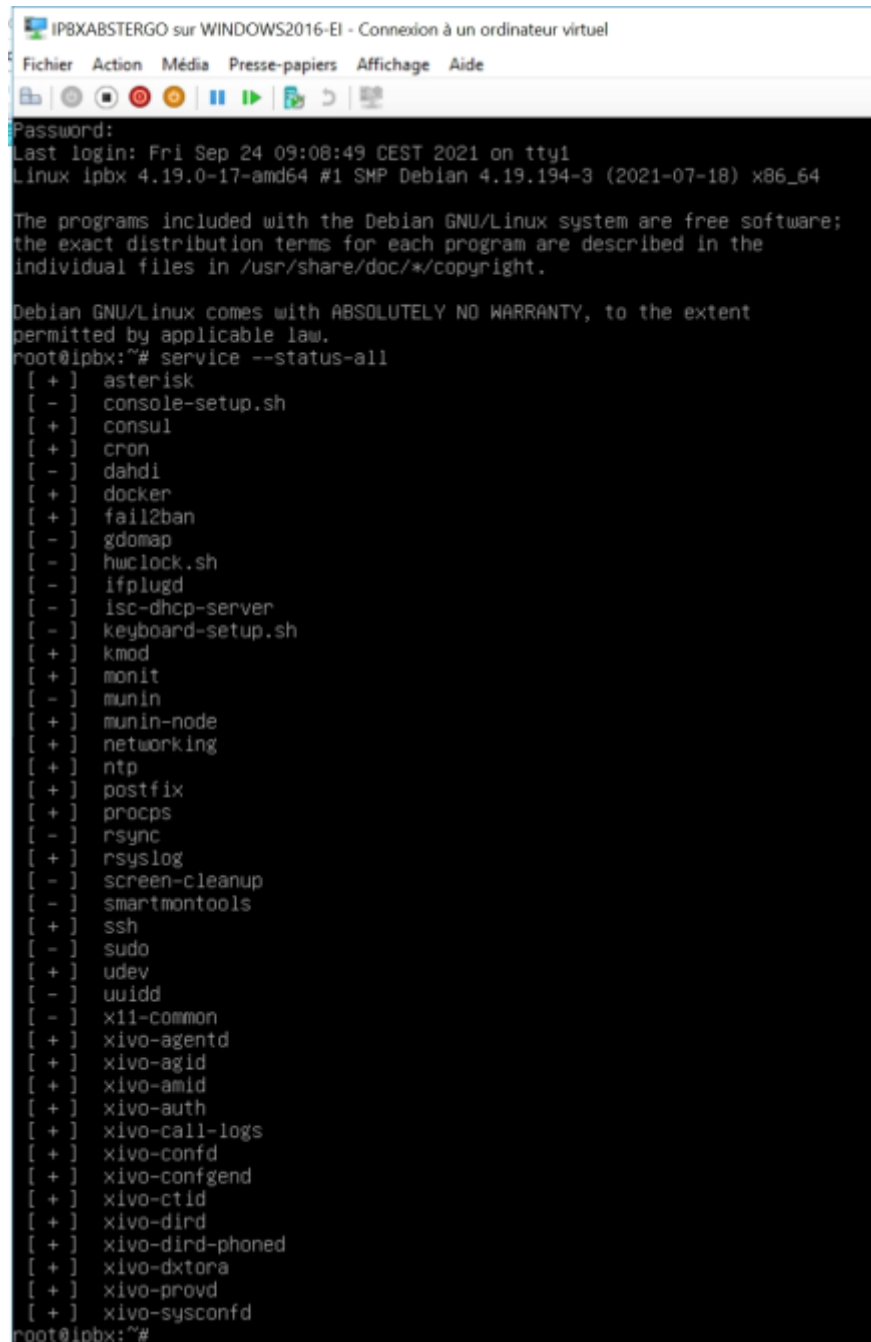
Serveur IPBX

La liste des services sur IPBXABSTERGO sont les suivants :

Nous avons un serveur Linux nommée IPBX cela signifie Internet Protocol Private Branch eXchange.

C'est donc un serveur qui permet de faire de la télécommunication.

Voici les services qui se trouve sur ce serveur :



```
IPBXABSTERGO sur WINDOWS2016-EI - Connexion à un ordinateur virtuel
Fichier Action Média Presse-papiers Affichage Aide
Password:
Last login: Fri Sep 24 09:08:49 CEST 2021 on tty1
Linux ipbx 4.19.0-17-amd64 #1 SMP Debian 4.19.194-3 (2021-07-18) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@ipbx:~# service --status-all
[ + ] asterisk
[ - ] console-setup.sh
[ + ] consul
[ + ] cron
[ - ] dahdi
[ + ] docker
[ + ] fail2ban
[ - ] gdomap
[ - ] hwclock.sh
[ - ] ifplugd
[ - ] isc-dhcp-server
[ - ] keyboard-setup.sh
[ + ] kmod
[ + ] monit
[ - ] munin
[ + ] munin-node
[ + ] networking
[ + ] ntp
[ + ] postfix
[ + ] procps
[ - ] rsync
[ + ] rsyslog
[ - ] screen-cleanup
[ - ] smartmontools
[ + ] ssh
[ - ] sudo
[ + ] udev
[ - ] uidd
[ - ] x11-common
[ + ] xivo-agentd
[ + ] xivo-agid
[ + ] xivo-amid
[ + ] xivo-auth
[ + ] xivo-call-logs
[ + ] xivo-confd
[ + ] xivo-confgend
[ + ] xivo-ctid
[ + ] xivo-dird
[ + ] xivo-dird-phoned
[ + ] xivo-dxtora
[ + ] xivo-provd
[ + ] xivo-sysconfd
root@ipbx:~#
```

Le [+] indique que le service est utilisé, et le [-] indique que le service est inutilisé :

Dans l'industrie des télécommunications, on désigne par PABX IP (PBX IP ou encore IPBX; de l'anglais Internet Protocol Private Branch eXchange) un autocommutateur téléphonique privé utilisant le protocole internet (IP) pour gérer les appels téléphoniques

d'une entreprise, en interne sur son réseau local (LAN). Couplé à des technologies de voix sur IP, les communications téléphoniques peuvent ainsi être acheminées sur le réseau étendu (WAN) de l'entreprise.

- **Asterisk** : dépendance xivo
- **Console-setup.sh** : Ce paquet fournit à la console le même modèle de configuration du clavier que celui du système X Window.
- **Consul** est une solution de mise en réseau de services qui permet d'automatiser les configurations de réseau, de découvrir des services et d'activer une connectivité sécurisée dans n'importe quel cloud ou runtime.
- **Cron** service Cron (crond) est utilisé pour exécuter des commandes ou des scripts planifiés. cron se réveille toutes les minutes, examine tous les crontabs stockés, vérifie chaque commande pour voir si elle doit être exécutée dans la minute en cours.
- **Dahdi** DAHDI is a collection of open source drivers, for linux, that are used to interface with a variety of telephony related hardware. It consists of two parts.

The DAHDI-Linux project contains the individual board drivers for the supported hardware.

The DAHDI-Tools project contains an assortment of user space utilities that are used to setup and test the drivers.

- **Docker** : Docker est un ensemble de produits "platform as a service" qui utilisent la virtualisation au niveau du système d'exploitation pour fournir des logiciels dans des paquets appelés conteneurs. Les conteneurs sont isolés les uns des autres et regroupent leurs propres logiciels, bibliothèques et fichiers de configuration ; ils peuvent communiquer entre eux par des canaux bien définis.

```
root@lpxb:~# docker ps
```

CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS	PORTS
3d2ec6a60448	xivoxc/xivo-switchboard-reports:2021.07.latest	"bin/xivo-switchboar..."	10 days ago	Up About an hour	127.0.0.1
9510->9510/tcp	xivo_switchboard_reports_1				
82c726a54dcf	xivoxc/xivo-outcall:2021.07.latest	"bin/xivo-outcall-do..."	10 days ago	Up About an hour	
	xivo_outcall_1				
bd6d2a64242f	xivoxc/config-mgt:2021.07.latest	"bin/config-mgt-dock..."	10 days ago	Up About an hour	0.0.0.0:3
00->9000/tcp	xivo_config_mgt_1				
2c1e2b76b272	xivoxc/xivo-webi:2021.07.latest	"docker-php-entrypoi..."	4 weeks ago	Up About an hour	
	xivo_webi_1				
6fe7d033609a	xivoxc/xivo-nginx:2021.07.latest	"/usr/local/bin/dock..."	4 weeks ago	Up About an hour	
	xivo_nginx_1				
2744b315dffa	xivoxc/xivo-db:2021.07.latest	"docker-entrypoint.s..."	4 weeks ago	Up About an hour	0.0.0.0:3
32->5432/tcp	xivo_db_1				
6dea716c69f7	xivoxc/rabbitmq:2021.07.latest	"docker-entrypoint.s..."	4 weeks ago	Up About an hour	
	xivo_rabbitmq_1				

- **Fail2ban** : Fail2Ban est un cadre logiciel de prévention des intrusions qui protège les serveurs informatiques contre les attaques par force brute.
- **Gdomap** : gdomap est utilisé par les programmes GNUstep pour rechercher des objets distribués de processus s'exécutant sur le réseau (et entre différents comptes d'utilisateurs sur une seule machine).
- **Hwclock.sh** : Régler l'horloge du système sur l'horloge matérielle, selon le # paramètre UTC.

- **Ifplugd** : un démon qui configurera automatiquement votre périphérique Ethernet lorsqu'un câble est branché et le déconfigurera automatiquement si le câble est retiré.
- **Isch-dhcp-server**: ISC DHCP offre une solution open source complète pour la mise en œuvre de serveurs DHCP : Dynamic Host Configuration Protocol
- **Keyboard-setup.sh(en fait, les scripts mis en cache)**
- **Kmod** : kmod est un binaire multi-appels qui implémente les programmes utilisés pour contrôler les modules du noyau Linux
- **Monit** : Monit est un outil gratuit et open-source de supervision de processus pour Unix et Linux.
- **Munin** : Munin est une application logicielle libre et gratuite de surveillance de systèmes informatiques, de réseaux et d'infrastructures.
- **Munin-node** -----
- **Networking** Les services réseau sous Linux sont définis comme le groupe d'applications qui s'exécutent en arrière-plan et permettent des activités basées sur le réseau, comme la connexion à Internet, le transfert de fichiers, etc.
- **Ntp** : Le protocole de temps réseau (NTP) synchronise l'heure d'un client ou d'un serveur informatique avec un autre serveur ou à quelques millisecondes près du temps universel coordonné (UTC).
- **Postfix** : Postfix est un agent de transfert de courrier libre et gratuit qui achemine et distribue le courrier électronique. Il est publié sous la licence publique IBM 1.0 qui est une licence de logiciel libre.
- **procps** : le service procps n'est pas vraiment un démon qui tourne longtemps. service procps start invoque simplement le script dans /etc/init/procps, qui fait en sorte que tout le contenu de /etc/sysctl.d/*.conf et /etc/sysctl.conf soit envoyé à sysctl -e -p -.
- **rsync** : est un utilitaire permettant de transférer et de synchroniser efficacement des fichiers entre un ordinateur et un disque dur externe, ainsi qu'entre des ordinateurs en réseau, en comparant les temps de modification et les tailles des fichiers
- **rsyslog** fournit des facilités à la fois pour exécuter un serveur de journalisation et pour configurer les systèmes individuels afin qu'ils envoient leurs fichiers journaux au serveur de journalisation.
- **screen-cleanup** : script pour supprimer l'écran périmé nommé pipes au démarrage
- **smartmontools** : est un ensemble d'applications qui permettent de tester les disques durs et de lire les statistiques SMART de leur matériel.
- **ssh** : SSH ou Secure Shell est un protocole de communication réseau qui permet à deux ordinateurs de communiquer
- **sudo** : Le fichier de service sudo existe pour s'assurer que les privilèges demandés ne restent pas après un redémarrage. En gros, il garantit qu'après le redémarrage, les utilisateurs normaux qui ont demandé les droits root resteront des utilisateurs normaux.
- **udev** udev est un gestionnaire de périphériques pour le noyau Linux. En tant que successeur de devfsd et hotplug, udev gère principalement les nœuds de périphériques dans le répertoire /dev.
- **uuid** Le démon uuid est utilisé par la bibliothèque UUID pour générer des identifiants universellement uniques (UUID), en particulier des UUID basés sur le

temps, de manière sécurisée et garantie, même face à un grand nombre de threads fonctionnant sur différents CPUs et essayant de saisir des UUID.

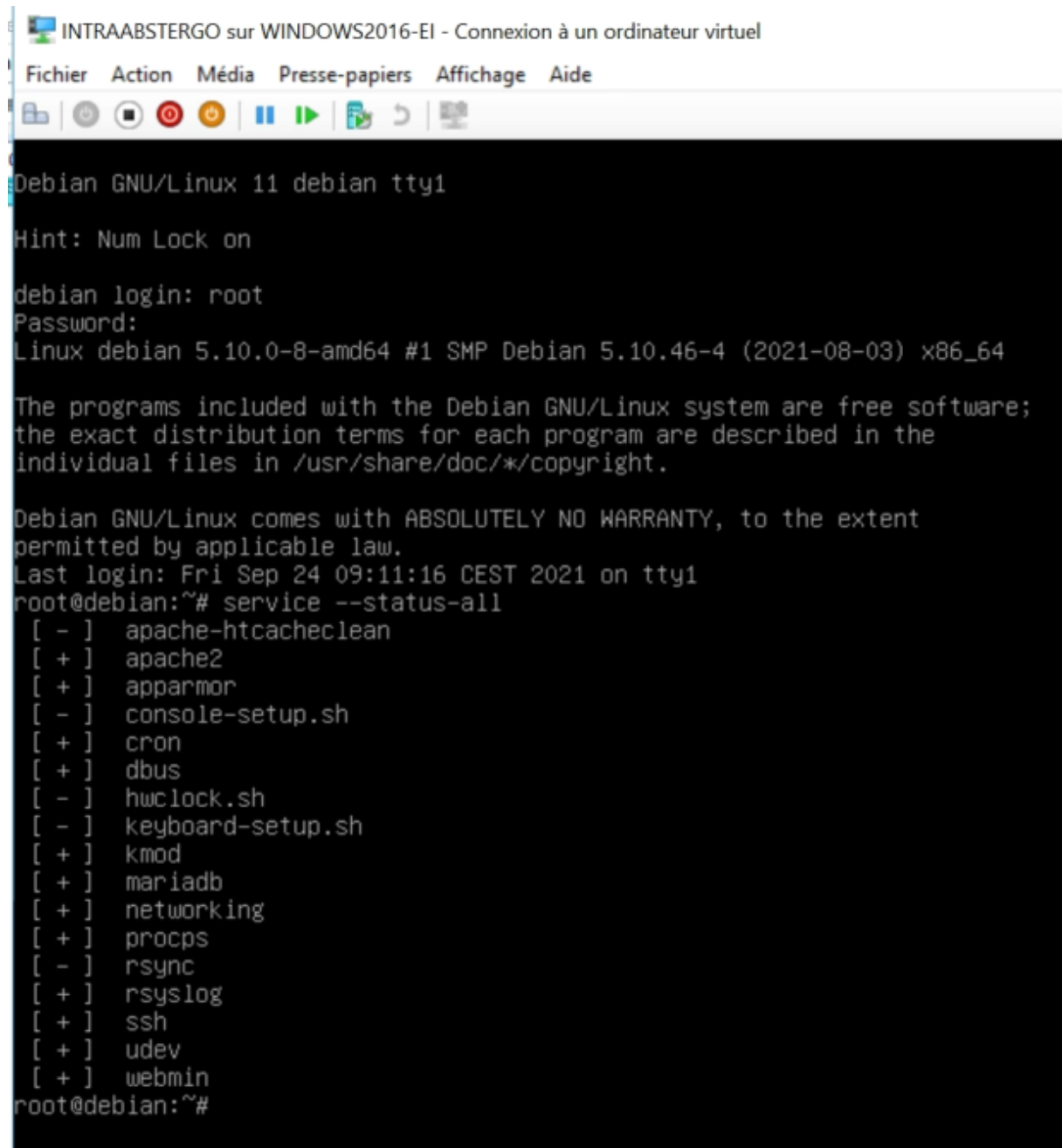
- **x11-common** : x11-common contient l'infrastructure des fichiers requise pour installer le système X Window dans n'importe quelle configuration.

xivo-agentd
xivo-agid
xivo-amid
xivo-auth
xivo-call-logs
xivo-confd
xivo-confgend
xivo-ctid
xivo-dird
xivo-dird-phoned
xivo-dxtora
xivo-provd
xivo-sysconfd

XiVO est une suite applicative basée sur plusieurs composants libres existants dont Asterisk, et nos propres développements pour fournir des services de communication (IPBX, Messagerie unifiée, ...) aux entreprises. XiVO est un logiciel libre. La plupart de ses composants distinctifs, et XiVO dans son ensemble, sont distribués sous la licence GPLv3.

Serveur Web

Nous avons un serveur Web qui héberge un site web qui n'est pas encore fini . Il semble que tous les servies pour faire fonctionner ce site soient opérationnels :



```
INTRAABSTERGO sur WINDOWS2016-EI - Connexion à un ordinateur virtuel
Fichier Action Média Presse-papiers Affichage Aide

Debian GNU/Linux 11 debian tty1

Hint: Num Lock on

debian login: root
Password:
Linux debian 5.10.0-8-amd64 #1 SMP Debian 5.10.46-4 (2021-08-03) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Sep 24 09:11:16 CEST 2021 on tty1
root@debian:~# service --status-all
[ - ] apache-htcacheclean
[ + ] apache2
[ + ] apparmor
[ - ] console-setup.sh
[ + ] cron
[ + ] dbus
[ - ] hwclock.sh
[ - ] keyboard-setup.sh
[ + ] kmod
[ + ] mariadb
[ + ] networking
[ + ] procps
[ - ] rsync
[ + ] rsyslog
[ + ] ssh
[ + ] udev
[ + ] webmin
root@debian:~#
```

- **apache-htcacheclean** : htcacheclean permet de maintenir la taille de l'espace de stockage réservé à mod_disk_cache en dessous d'une limite de taille donnée ou d'inodes utilisés.
- **apache2** : Le serveur HTTP Apache, familièrement appelé Apache, est un logiciel de serveur web multiplateforme gratuit et ouvert, publié selon les termes de la licence Apache 2.0. Apache est développé et maintenu par une communauté ouverte de développeurs sous les auspices de l'Apache Software Foundation.

- **apparmor** Apparmor est un système de contrôle d'accès obligatoire (ou MAC)
- **console-setup.sh** : Ce paquet fournit à la console le même modèle de configuration du clavier que celui du système X Window
- **cron** service Cron (crond) est utilisé pour exécuter des commandes ou des scripts planifiés. cron se réveille toutes les minutes, examine tous les crontabs stockés, vérifie chaque commande pour voir si elle doit être exécutée dans la minute en cours.
- **dbus**
- **hwclock.sh** Régler l'horloge du système sur l'horloge matérielle, selon le # paramètre UTC
- **keyboard-setup.sh** (en fait, les scripts mis en cache)
- **kmod** kmod est un binaire multi-appels qui implémente les programmes utilisés pour contrôler les modules du noyau Linux
- **mariadb**
- **Networking** Les services réseau sous Linux sont définis comme le groupe d'applications qui s'exécutent en arrière-plan et permettent des activités basées sur le réseau, comme la connexion à Internet, le transfert de fichiers, etc.
- **procps** le service procps n'est pas vraiment un démon qui tourne longtemps. Service procps start invoque simplement le script dans /etc/init/procps, qui fait en sorte que tout le contenu de /etc/sysctl.d/*.conf et /etc/sysctl.conf soit envoyé à sysctl -e -p -.
- **rsync** st un utilitaire permettant de transférer et de synchroniser efficacement des fichiers entre un ordinateur et un disque dur externe, ainsi qu'entre des ordinateurs en réseau, en comparant les temps de modification et les tailles des fichiers
- **rsyslog** fournit des facilités à la fois pour exécuter un serveur de journalisation et pour configurer les systèmes individuels afin qu'ils envoient leurs fichiers journaux au serveur de journalisation.
- **ssh** SSH ou Secure Shell est un protocole de communication réseau qui permet à deux ordinateurs de communiquer
- **udev** udev est un gestionnaire de périphériques pour le noyau Linux. En tant que successeur de devfsd et hotplug, udev gère principalement les nœuds de périphériques dans le répertoire /dev.
- **Webmin** : Webmin est un outil de configuration système basé sur le Web pour les systèmes de type Unix, bien que les versions récentes puissent également être installées et exécutées sur Microsoft Windows.

Nous avons trouvé un seul fichier pour ce site :

```

root@debian:/var/www/html# ls
index.html
root@debian:/var/www/html# less index.html
Ici sera mis le site web abstergo quand le d veloppeur nous aura envoy  les fichiers.
index.html (END)
<

```

État : Exécution

Analyse de sécurité DCIP

À la suite de l'étude du Système d'information, nous avons déterminé que le système pose des risques en termes de sécurité :

Disponibilité : l'information est effectivement atteignable

Confidentialité : la présence de mots de passe identiques et simples entre les différentes machines, surtout le serveur de partage de fichier, et le fait que certaines personnes soit capable de rentrer leur poste personnel dans l'Active Directory montre de gros problèmes.

Intégrité : Pour les raisons précédemment citées, l'intégrité des données ne peut être garantie pour les utilisateurs.

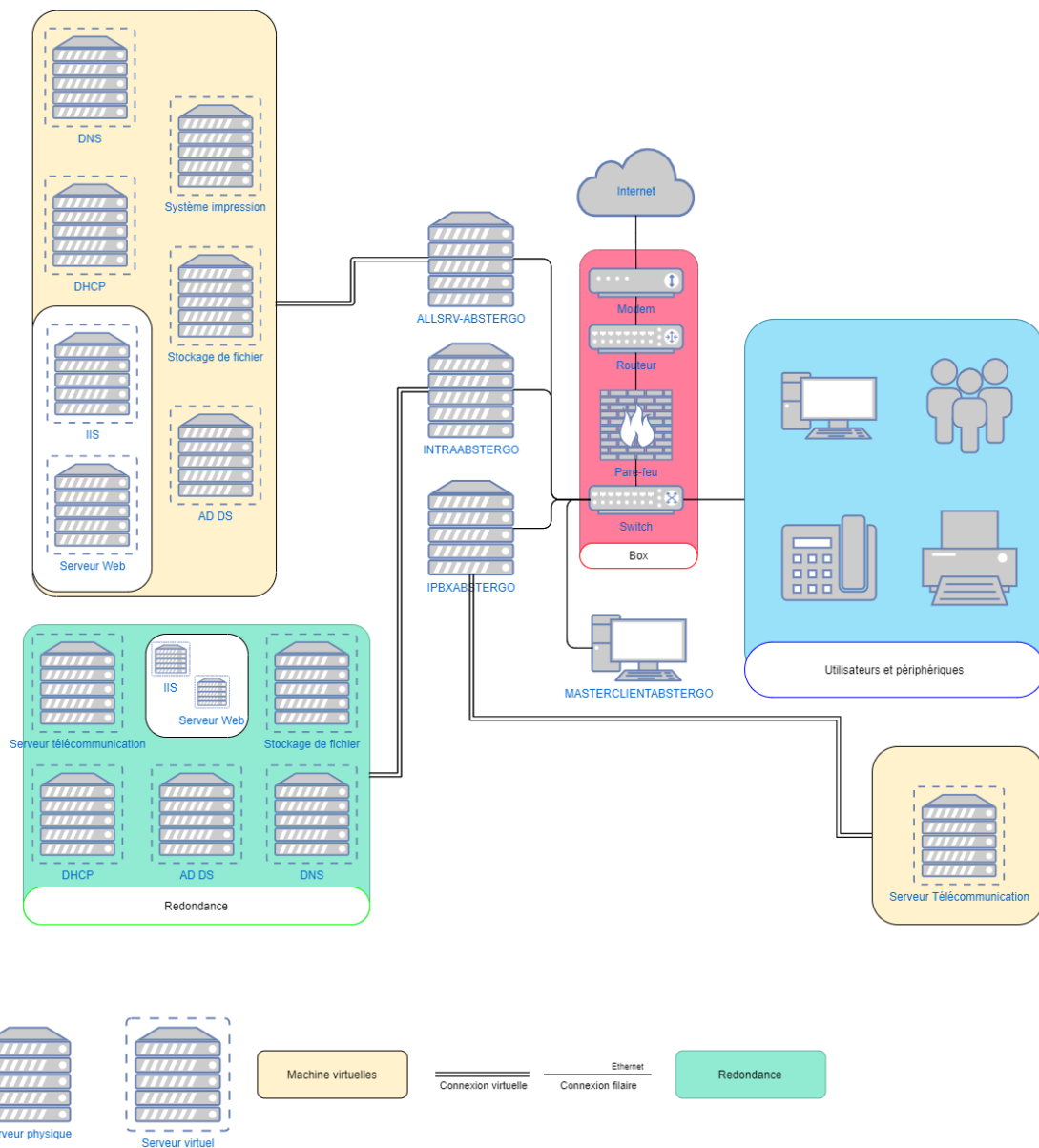
Preuve : Nous disposons de traçabilité sur le Système grâce aux logs d'Active Directory. Cependant, ces failles ne peuvent être tolérées et des mesures doivent être prises avant la migration vers l'AD mère.

Hypothèses

- Pour économiser un serveur, on ne va conserver qu'un service d'application Web (entre IIS et serveur WEB).
- Il est possible d'utiliser le serveur INTRAABTERGO comme serveur de redondance.

Schéma de la nouvelle Infrastructure

Schéma



Explication des choix

Après étude du SI actuel de l'entreprise ABSTERGO, nous avons apporté quelques modifications à l'infrastructure.

- Nous avons commencé par ajouter une Box qui contiendrait un modem, un routeur, un pare-feu et un switch.
- Nous avons ensuite mis en place une redondance des services en passant le serveur web sur le serveur Windows pour pouvoir le réutiliser pour la redondance du serveur Windows ainsi que du serveur IPBX. De cette façon, si un de ces deux serveurs venait à tomber, ce serveur pourra prendre le relais.

Procédure de migration

Procédure de migration :

Informations :

- Active directory Animus :
 - Mono forêt / multi domaine
 - Windows server 2016
- Active directory Abstergo :
 - Mono forêt / multi domaine
 - Windows server 2019
- Pas de relation d'approbation dans l'Active directory d'Animus

Prérequis :

Le design du document :

La documentation est cruciale dans toutes les implémentations système. Avant de démarrer, il est nécessaire de produire un document comprenant la topologie physique, logique d'Active directory ainsi que les risques et les technologies utilisées. Il est recommandé de valider la documentation auprès du personnel autorisés avant le déploiement.

Domaine et forêts

Dans une organisation il est important de se mettre d'accord sur un nom de domaine et de forêt. Ici nous allons garder les domaines assignés de base.

Adresse IP dédiée

Les contrôleurs de domaine sont recommandés pour gérer les adresses IP statiques. Il faut assigner au contrôleur de domaine une adresse IP statique. L'adresse IP du contrôleur de domaine de l'active directory peut être modifié mais c'est à éviter le plus possible.

Gestion

La gestion des performances système, de la santé, des composants et des services d'intégrités permettent l'identification de potentiels étranglements (bottlenecks du réseau) et impacts serveurs. Microsoft System Center Operation Manager (SCOM) et Microsoft Operation Management Suite (OMS) sont les outils de gestion recommandés. Ils incluent des modules spéciaux conçus pour identifier le niveau de service et les problèmes de sécurités.

Système de restauration

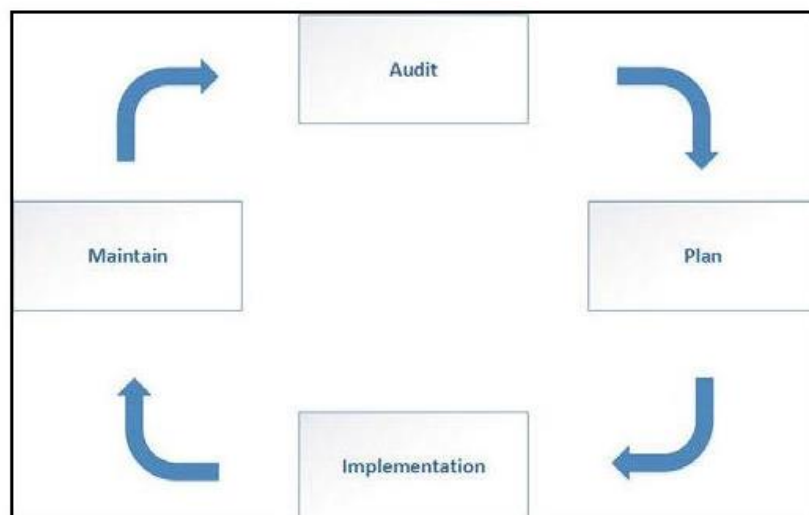
Il est important de garder fonctionnel l'identité d'une infrastructure pendant un imprévu avec le minimum d'opérations. Il y a plusieurs services permettant le backup des contrôleurs de domaine active directory. Une fois la solution définie il faut planifier des tests périodiques pour vérifier la validité de la solution.

Protection des virus et contrôleur de domaine

Les contrôleurs de domaine peuvent être eux aussi infectés par du code malveillant. Il y a des débats portant sur si oui ou non le contrôleur de domaine de l'active directory doit posséder un antivirus. Dans la documentation Microsoft il n'y a pas de passage notifiant le fait de ne pas installer d'antivirus. Il faut donc vérifier si l'antivirus est compatible avec le contrôleur de domaine active directory et pour le protéger.

Les étapes de migration :

Etapes de migration (cycle de vie de la migration)



Audit

Préparer et auditer sont les étapes les plus importantes du processus de migration. Lorsqu'il y a un audit et un plan acceptable, le processus d'implémentation devient simple (cela évite de futurs problèmes (post-processus)). Dans l'audit il faut revoir l'actuelle infrastructure de l'active directory, comprendre la topologie physique et logique, l'état de santé et identifier les potentiels risques de migration.

Topologie logique et physique d'active directory

Il est nécessaire de recueillir des informations précises sur le système en place, cela permet de mettre en place un nouvel AD plus efficacement.

Health check

Si l'active directory possède des problèmes liés à ses principales opérations (comme le DNS, la réplication, les liaisons entre différents sites...), ils ont besoins d'être identifiés et fixés avant la migration. Dans le cas contraire ils ne permettront pas la migration.

Il n'y a pas de liste définie/imposée pour la vérification de l'active directory, on peut créer sa propre liste et ses étapes de vérification de l'active directory.

Différents outils permettent de vérifier l'état de l'active directory et de ses contrôleurs de domaine (état de réplication entre contrôleur de domaine) tel que Repadmin.exe

Exemples de checklist:

1. Revue du statut de connexion entre les contrôleurs de domaine
2. Si l'organisation possède un système de gestion, revoir les rapports et derniers événements autour des contrôleurs de domaine, des rôle de l'active directory, de la santé de réplication et des services DNS
3. Revue du dernier rapport de backup
4. Revue des problèmes DNS et événements
5. Revue de l'état du contrôleur de domaine de l'active directory
6. Test de la réplication de l'active directory
7. Revue de logs active directory pour les problèmes de ré-occurrence
8. Revue des performances du contrôleur de domaine actuel
9. Revue de l'utilisation de la bande réseau entre les différents sites

Évaluation de l'impact de la migration

Avant le processus d'implémentation, il est important de reconnaître les applications intégrées dans active directory et d'évaluer leurs impacts pendant la migration.

LDAP Connection

Dans le cas du SSO (single sign-on) avec des applications, il doit être utilisé la connexion LDAP au contrôleur de domaine. Parfois, des applications utilisent des noms d'hôtes ou des adresses IP des contrôleurs de domaine codé en dur pour définir la connexion. Si la migration comprend la modification des adresses IP et de nom d'hôte, alors l'altération de ces informations devront être pris en compte.

Changement de la version du schéma

Il faut vérifier que les applications utilisées supportent le nouveau schéma de l'AD.

Migration d'application

Il y a certaines organisations qui possèdent des applications non maintenues. Mais parfois cela ralentit, étrangle la migration de l'AD. Pour y remédier il faut soit changer d'application, soit de système.

Rôle/applications d'un serveur installé sur un contrôleur de domaine.

Dans la majorité des cas, une fois les rôles FSMO migrés vers un nouveau contrôleur de domaine, l'ancien contrôleur de domaine est décommissionné. Même si Microsoft recommande de ne pas installer des applications ou des rôles serveurs dans le contrôleur de domaine, des gens le font quand même. Les plus fréquents sont un DHCP, un serveur de fichier, et un serveur de License.

Dans le cas d'un serveur décommissionné, ces applications et rôles serveur doivent être migrés vers le nouveau serveur. Mais parfois ces applications ne sont plus disponibles, dans ce cas il faut prévoir un plan pour mettre à jour l'application ou la remplacer par un équivalent.

Plan :

DONNÉE	DESCRIPTION
Vue d'ensemble d'infrastructure de l'active directory actuel	Informations à propos de la topologie physique et logique de l'active directory
Vue d'ensemble de la solution proposée	Inclus des données à propos des changements de la topologie, le placement du nouveau contrôleur de domaine, le placement des rôles FSMO, les nouvelles liaisons aux sites, les adresses IP, les nom d'hôtes, des ressources informatiques (machines virtuelle / machines informatique), les règles de changement du firewall, ...
Risques	Potentiels risques pouvant impacter la migration de l'AD. A cause de mauvais design, mauvais état des services de l'AD, ou d'autres problèmes. Ils peuvent être catégorisés en se basant sur l'impact (faible, moyen, fort)

Plan d'atténuation des risques	Plan décrivant les actions pouvant être prises pour résoudre les risques. Si possible y inclure une liste de tâches, une estimation de temps et le budget du plan
Interruptions des services	Peut être causé par la migration des applications, ou du changement de l'IP du serveur. Faire une liste de ces interruptions, avec une fourchette de temps.
Recommandations	Manière d'améliorer la sécurité, performance ou manageabilité de l'AD DS. Cela ne doit pas impacter la migration de l'AD.
Liste de tâches et planning	Liste détaillée et planning pour la migration de l'AD. Comprenant les rôles et responsabilités pour compléter chaque tâche.
Plan de test	Plan détaillé des tests pour tester les fonctions de l'active directory après la migration. Vérifie l'intégrité et l'état du système. Il doit contenir les preuves de succès d'exécutions des différentes tâches (screen, événements, rapport ...)
Plan de relance	Un plan de relance, récupération dans le cas d'une erreur. Il doit contenir une solution backup.

Liste des étapes de migration

- Evaluer les besoins pour la migration d'active directory
- Faire un audit sur l'infrastructure de l'AD actuel
- Fournir un plan pour l'implémentation
- Préparer les ressources physique/virtuelle pour le contrôleur de domaine
- Patcher les serveurs avec la dernière update
- Assigner une IP dédiée au contrôleur de domaine
- Installer les rôles de l'AD
- Migrer les applications et les rôles serveur depuis le contrôleur de domaine existant
- Migrer les rôles FSMO
- Ajouter un nouveau contrôleur de domaine
- Décommissionner l'ancien contrôleur de domaine
- Améliorer le niveau fonctionnel du domaine et de la forêt
- Mettre en place une maintenance

Préparer la fusion des deux AD

En vue de la migration du SI vers l'AD d'ANIMUS, certaines préparations seront à effectuer pour garantir le bon déroulement du transfert :

- La version du serveur d'ABSTERGO (Windows Serveur 2016) ne posera pas de problème dans son intégration vers l'AD d'ANIMUS (Windows Serveur 2019) car ultérieure, donc pas de modification à ce niveau.
- Un serveur équipé d'ADMT ainsi que de SQL Serveur sera nécessaire
- Une relation d'approbation et un compte présent dans BUILTIN\Administrateurs dans les deux AD. Le compte doit aussi être admin sur le poste.
- Facultatif : Password Export Server, qui permet de transférer les mots de passe en plus des utilisateurs.
- Créer un OU servant à accueillir les objets transférés sur le SI d'ANIMUS.
- Evidemment une modification du SI d'ABSTERGO pour remplir les contraintes en matière de DICP

Conclusion

En conclusion, nous avons identifié plusieurs faiblesses dans le SI d'ABSTERGO qui devront être comblé avant d'être intégré au SI d'ANIMUS.

Pour pouvoir intégrer ce SI, nous allons devoir suivre une procédure de migration précise permettant le bon déroulement de celle-ci.

Nous avons donc dû répartir la charge de travail au sein du groupe pour pouvoir élaborer une analyse complète et détaillée ainsi qu'une méthode de migration respectant les besoins et les contraintes imposées par notre client, ANIMUS.