BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2021**

ANNEXE 6-1 : Fiche de présentation d'une situation professionnelle (modèle)
E4 Conception et maintenance de solutions informatiques - Coefficient 4

DESCRIPTION D'UNE SITUATION PROFESSIONNELLE

Épreuve ponctuelle ☐ **Contrôle en cours de formation** ☒

OPTION SISR ☒ **OPTION SLAM** ☐

NOM et prénom du candidat : Jaadar Mourad **N° candidat :0110874226**

Contexte de la situation professionnelle[1]:
Suite à une tentative d'intrusion sur l'un des serveurs de la société GSB et un ensemble de dysfonctionnements récurrents, le DSI m'a demandé de trouver l'origine de ces éléments en analysant les fichiers Logs. Mais les LOGS sont présents sur chacun des serveurs. Pour répondre à sa requête j'ai choisi de configurer un serveur Syslog qui centralisera les LOGS des serveurs.

Intitulé de la situation professionnelle :
Mise en place d'un serveur SYSLOG-Loganalyzer

Période de réalisation : Avril-Mai **Lieu : AURILLAC**
Modalité : ☒ Seul ☐ En équipe

Principale(s) activité(s) concernée(s)[2] :
A1.1.1 , Analyse du cahier des charges d'un service à produire , **A1.2.4 , Détermination des tests nécessaires à la validation d'un service** , **A1.2.5 , Définition des niveaux d'habilitation associés à un service** , **A1.3.1 , Test d'intégration et d'acceptation d'un service** , **A1.3.3 , Accompagnement de la mise en place d'un nouveau service** , **A3.2.1 , Installation et configuration d'éléments d'infrastructure** , A3.3.3 Gestion des identités et des habilitations **,**A4.1.3 , Conception ou adaptation d'une base de données

Conditions de réalisation[2] (ressources fournies, résultats attendus)
Infrastructure réseau qui comprend un SRV AD, un SRV DHCP, une DMZ avec SRV IIS et un routeur PAREFEU NetFilter. L'ensemble des serveurs sont sous Windows 2016 R2. Un SRV Syslog sous Debian 10
Redondance au niveau des commutateurs de niveau 2, Redondance au niveau des commutateurs de niveau 3. Clients, logiciel capture trame, tests …

Productions associées
Mode opératoire de la configuration du Serveur Syslog-Loganalyzer
Présentation de la technologie par l'intermédiaire d'un diaporama.

Modalités d'accès aux productions [3]
https://portfolio.mouradjaadar.fr/index.php/deuxieme-activite
Modalités d'accès à la documentation des productions [4]
https://portfolio.mouradjaadar.fr/index.php/deuxieme-activite

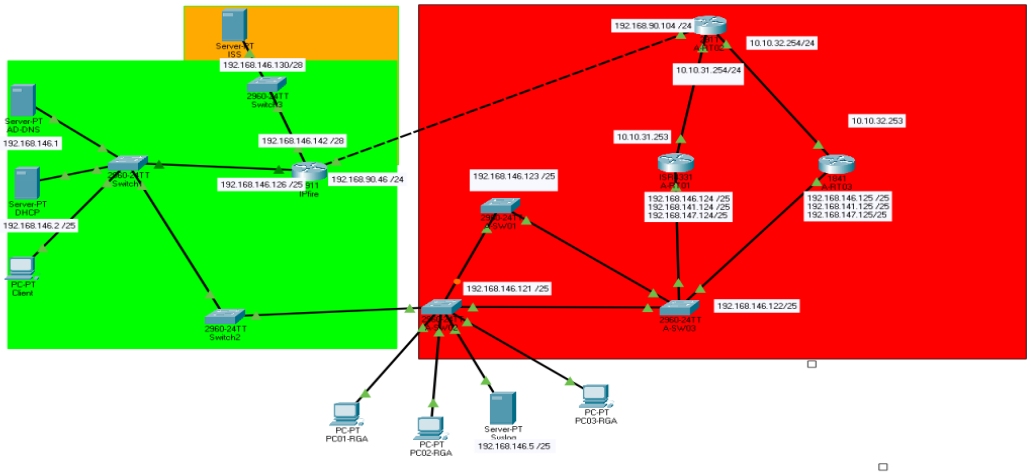
Au verso de cette page, le candidat présente un descriptif détaillé de la situation professionnelle et des productions réalisées sous forme d'un rapport d'activité permettant notamment de mettre en évidence la démarche suivie et les méthodes retenues.

[1] Conformément au référentiel du BTS SIO, le contexte doit être conforme au cahier des charges national en matière d'environnement technologique dans le domaine de spécialité correspondant à l'option du candidat.
[2] En référence à la description des activités des processus prévue dans le référentiel de certification.
[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. Les candidats qui n'en sont pas munis sont pénalisés dans les limites prévues par la grille d'aide à l'évaluation proposée par la circulaire nationale d'organisation. ». Il s'agit par exemple des identifiant, mot de passe, URL d'un espace de stockage et de la présentation de l'organisation du stockage.
[4] Lien vers le document décrivant la situation professionnelle tant au niveau logiciel (par exemple service fourni par la situation, interfaces utilisateurs, description des classes, de la base de données…) que matériel (par exemple schéma complet de réseau mis en place et configurations des services).

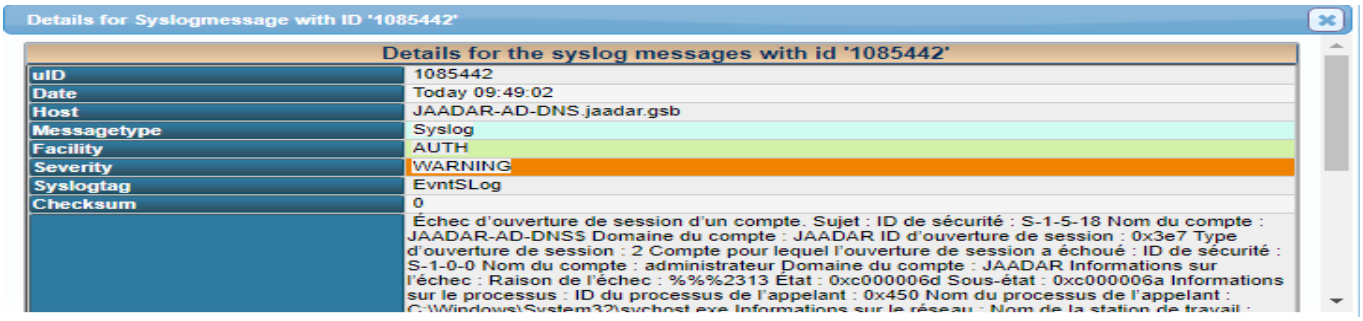
Descriptif détaillé de la situation professionnelle

Afin de mettre en place un serveur Syslog nous disposons d'un Serveur Debian10 ayant les rôles Syslog, Base de données, PHP, Apache2 installés.

Il faut créer la base de données ou seront stockés les LOG et sécuriser celle-ci. Il faut ensuite paramétrer le serveur Syslog en désignant les informations de la base de données. On procède par la suite à l'installation de LogAnalyzer et la configuration de celui-ci. J'ai par la suite procédé à l'installation de phpmyadmin pour mieux gérer ma base de données. Enfin j'ai installé un agent sur mon serveur AD-DNS pour qu'il puisse remonter les logs du serveur



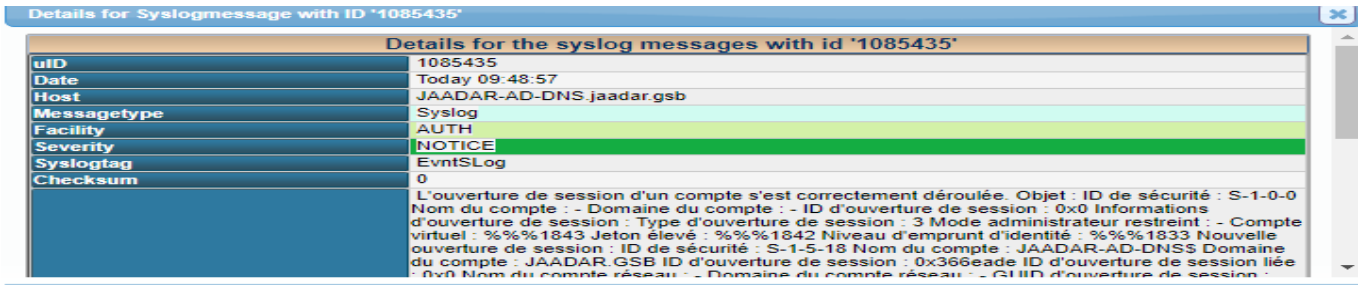
Depuis L'Active directory j'ai essayé de me connecter avec le compte administrateur en saisissant le bon mot de passe puis j'ai réalisé un second test avec un mot de passe erroné.



Details for Syslogmessage with ID '1085442'

Details for the syslog messages with id '1085442'

uID	1085442
Date	Today 09:49:02
Host	JAADAR-AD-DNS.jaadar.gsb
Messagetype	Syslog
Facility	AUTH
Severity	WARNING
Syslogtag	EvntSLog
Checksum	0
	Échec d'ouverture de session d'un compte. Sujet : ID de sécurité : S-1-5-18 Nom du compte : JAADAR-AD-DNSS Domaine du compte : JAADAR ID d'ouverture de session : 0x3e7 Type d'ouverture de session : 2 Compte pour lequel l'ouverture de session a échoué : ID de sécurité : S-1-0-0 Nom du compte : administrateur Domaine du compte : JAADAR Informations sur l'échec : Raison de l'échec : %%%2313 État : 0xc000006d Sous-état : 0xc000006a Informations sur le processus : ID du processus de l'appelant : 0x450 Nom du processus de l'appelant : C:\Windows\System32\svchost.exe Informations sur le réseau : Nom de la station de travail :



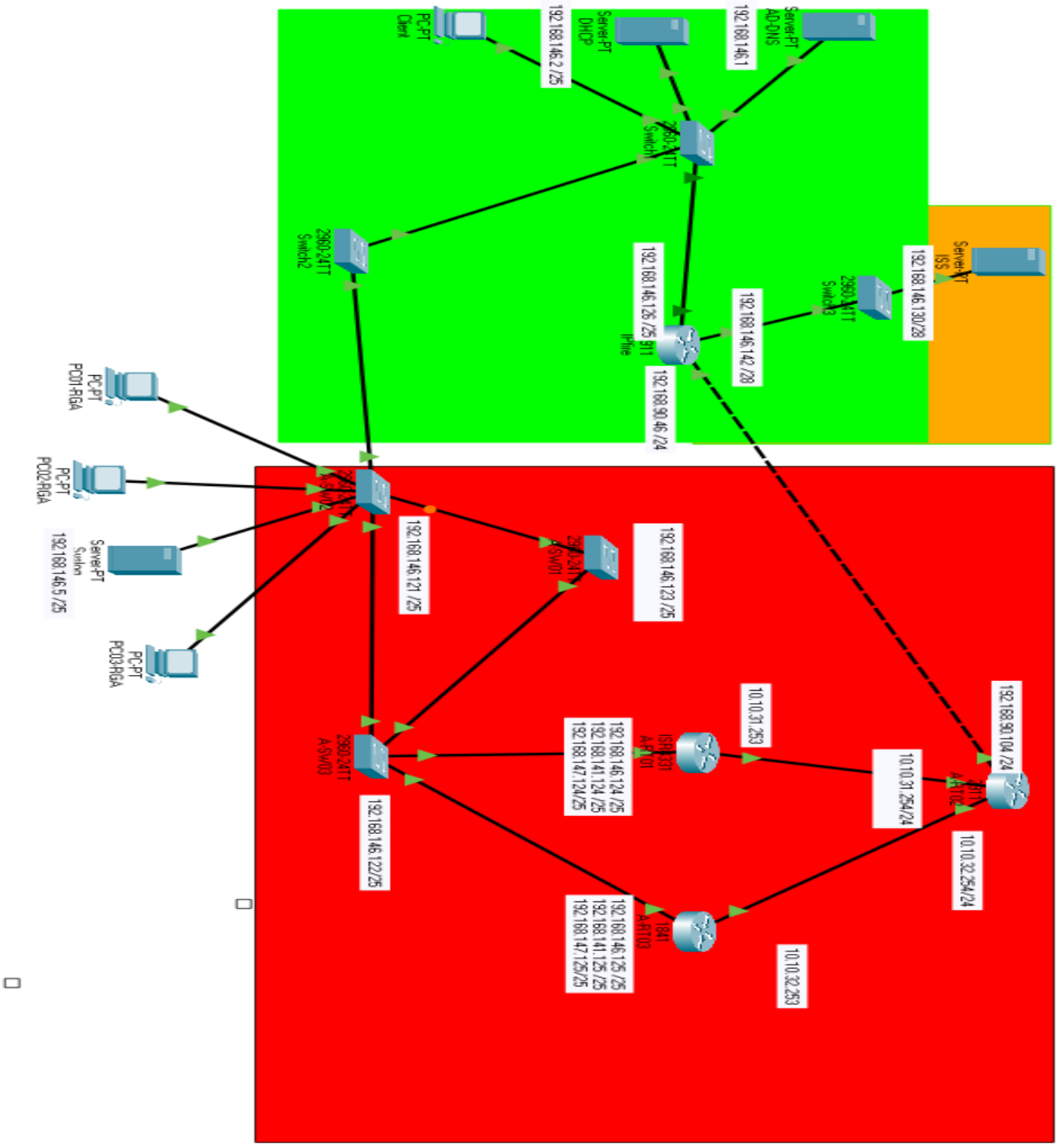
Details for Syslogmessage with ID '1085435'

Details for the syslog messages with id '1085435'

uID	1085435
Date	Today 09:48:57
Host	JAADAR-AD-DNS.jaadar.gsb
Messagetype	Syslog
Facility	AUTH
Severity	NOTICE
Syslogtag	EvntSLog
Checksum	0
	L'ouverture de session d'un compte s'est correctement déroulée. Objet : ID de sécurité : S-1-0-0 Nom du compte : - Domaine du compte : - ID d'ouverture de session : 0x0 Informations d'ouverture de session : Type d'ouverture de session : 3 Mode administrateur restreint : - Compte virtuel : %%%1843 Jeton élevé : %%%1842 Niveau d'emprunt d'identité : %%%1833 Nouvelle ouverture de session : ID de sécurité : S-1-5-18 Nom du compte : JAADAR-AD-DNSS Domaine du compte : JAADAR.GSB ID d'ouverture de session : 0x366eade ID d'ouverture de session liée : 0x0 Nom du compte réseau : - Domaine du compte réseau : - GUID d'ouverture de session :

VM _Debian-10 : Identifiant : Administrateur MDP : gsb$generique,1234	Loganalyzer(192.168.146.5/loganalyzer) : Identifiant : rsyslog MDP : gsb$generique,1234
VM_AD-DNS -DHCP-ISS -Client 2: Identifiant : Administrateur MDP : gsb$generique,1234	Phpmyadmin (192.168.146.5/phpmyadmin) : Identifiant : rsyslog MDP : gsb$generique,1234
Matériel d'interconnexion : Identifiant : cisco MDP : cisco	A-SW01: 192.168.146. 123 A-RT01: 192.168.146.124 A-SW02: 192.168.146.121 A-RT02: 192.168.90.103 A-SW03: 192.168.146.122 A-RT03 : 192.168.146.125

Annexe :


Server-PT
ISS
192.168.146.130/28
2960-24TT
Switch3
192.168.146.142 /28
192.168.146.126 /25
192.168.90.46 /24
2911
IPHte
Server-PT
AD-DNS
192.168.146.1
2960-24TT
Switch
Server-PT
DHCP
192.168.146.2 /25
PC-PT
Client
2960-24TT
Switch2
PC-PT
PC01-RGA
PC-PT
PC02-RGA
Server-PT
Sudren
192.168.146.5 /25
PC-PT
PC03-RGA
192.168.146.121 /25
2960-24TT
A-SW01
192.168.146.123 /25
192.168.90.104 /24
10.10.31.253
ISR4331
A-RT01
192.168.146.124 /25
192.168.141.124 /25
192.168.147.124/25
10.10.31.254/24
10.10.32.254/24
2960-24TT
A-SW03
192.168.146.122/25
192.168.146.125 /25
192.168.141.125 /25
192.168.147.125/25
1841
A-RT03
10.10.32.253