BTS SERVICES INFORMATIQUES AUX ORGANISATIONS

E5 : Production et fourniture de services informatiques

SESSION 2017

Durée : 4h00 Coefficient : 5

CAS ARMATIS-LC

Ce sujet comporte 16 pages dont 11 pages de documentation.
Il est constitué de deux parties qui peuvent être traitées de façon indépendante.
La candidate ou le candidat doit vérifier que le sujet qui lui est remis est complet.

Aucun matériel ni document n'est autorisé

Barème :

Partie A	***Gestion des serveurs DNS et web hébergés chez le prestataire BDN***	*50 points*
Partie B	***Gestion des éléments d'infrastructure***	*50 points*
	Total	**100 points**

Liste de la documentation jointe :

Conformément aux recommandations du Haut Conseil à l'Égalité entre les femmes et les hommes dans son guide publié en novembre 2015, l'expression du féminin et du masculin s'effectue en utilisant le point, par exemple, employé.e.

Présentation du contexte

Créée en 1989, la société Armatis-LC est un acteur majeur des centres de contacts et d'appels en France, spécialisé notamment dans la gestion de la relation client, le marketing direct, la prospection et la fidélisation. Elle compte plus de 6 500 salariés travaillant sur quinze sites indépendants les uns des autres, implantés en France métropolitaine et à l'étranger.

Armatis-LC se structure autour de douze sites en France, trois sites à l'étranger, et plus de 5 000 positions de travail afin de répondre au mieux aux besoins de ses différents clients.

Le service informatique est réparti entre divers sites dont celui de Châteauroux dans l'Indre. Il repose sur une organisation divisée en trois niveaux d'intervention :

- Le niveau 1 correspond aux techniciens intervenant essentiellement pour aider les utilisateurs du système informatique ;
- Le niveau 2 correspond aux techniciens systèmes et réseaux capables d'intervenir sur l'infrastructure ainsi que sur les serveurs de l'entreprise ;
- Le niveau 3 regroupe les ingénieurs et les administrateurs systèmes et réseaux qui conçoivent, organisent et sécurisent l'ensemble de l'infrastructure système et réseau de l'entreprise à l'échelle nationale et internationale.

L'infrastructure informatique d'Armatis-LC est structurée de la manière suivante :

- L'ensemble des sites est interconnecté en utilisant le protocole MPLS (*MultiProtocol Label Switching*) fourni par la société OBS *(Orange Business Services*) ;
- Armatis-LC dispose d'un hébergement externalisé de type IaaS[1] souscrit auprès de l'entreprise BDN (*Business Data Network*). Cet hébergement comprend notamment les serveurs *web* et serveurs DNS (*Domaine Name System*) de l'entreprise ;
- L'accès internet se fait uniquement par le réseau et le centre de données de l'entreprise BDN ;
- Certains serveurs, comme le serveur de gestion de configuration GLPI et le serveur abritant le progiciel de gestion intégré, sont hébergés dans les centres de données (*datacenter*) appartenant à la société Armatis-LC à Châteauroux et Bordeaux ;
- La plupart des serveurs sont virtualisés grâce à une infrastructure reposant sur le logiciel de virtualisation *VMware vSphere* ;
- La gestion de la partie téléphonie est réalisée à l'aide d'un système de voix sur IP (VoIP) reposant sur des téléphones et des autocommutateurs adaptés ainsi que sur des protocoles et des logiciels libres ou propriétaires.

Vous travaillez en tant que technicien.ne systèmes et réseaux de niveau 2 sur le site de Châteauroux. Le responsable de ce site, monsieur Ricot, décide de vous confier un certain nombre de missions pour :

- assurer une meilleure tolérance aux pannes ;
- améliorer la sécurisation ;
- choisir un élément d'infrastructure (onduleur) et l'intégrer dans le système de supervision ;
- participer à l'intégration d'un nouveau plateau technique pour gérer l'activité d'un nouveau client.

[1] ***Infrastructure As A Service*** est un modèle d'informatique dans les nuages (*cloud computing*) destiné aux entreprises où le fournisseur met à disposition les serveurs, les réseaux et le stockage des données et où le client est responsable de ses applications, de ses données et du système d'exploitation.

Dossier A : Gestion des serveurs DNS et web hébergés chez le prestataire BDN

Documents nécessaires à la réalisation du dossier A : A.1 à A.5.

Mission 1 - Gestion du domaine *armatis-lc.com*

À l'heure actuelle, les serveurs DNS et *web* sont hébergés dans le centre de données de l'entreprise BDN. En tant que technicien.ne systèmes et réseaux, vous êtes en charge de l'administration et de la gestion du domaine *armatis-lc.com*.

L'attaque du 21 octobre 2016 par déni de service distribué (DDoS), qui a touché les serveurs DNS de *Dyn* et a de ce fait grandement perturbé l'accessibilité des grands sites *web* comme *Netflix, Twitter, Spotify, Amazon* ou le *New York Times*, a été le déclencheur d'une réflexion au sein de l'équipe du site de Châteauroux.

La non disponibilité du site *web* de Armatis-LC pourrait avoir des conséquences économiques très graves. M. Ricot désire connaître précisément les risques encourus, compte tenu de l'architecture existante, tant au niveau des serveurs DNS que des serveurs *web*.

Afin d'assurer une résilience optimale du service DNS, c'est-à-dire s'assurer de sa capacité à demeurer disponible, M. Ricot souhaite mettre en œuvre les bonnes pratiques recommandées dans les RFC (*requests for comments*). Un résumé de ces RFC figure dans le dossier documentaire.

A.1.1 : Rédiger un état des lieux argumenté et justifié concernant le service DNS, en distinguant :

a) la ou les recommandations déjà mises en œuvre ;

b) la ou les recommandations qu'il faut implémenter et pourquoi.

Vous vous intéressez maintenant plus spécifiquement au service web et vous constatez dans le fichier de zone DNS la présence de deux adresses IPv4 distinctes qui correspondent à deux serveurs distincts mais pour un seul et même nom de domaine pleinement qualifié (FQDN) *www.armatis-lc.com*.

A.1.2 : Expliquer à M. Ricot l'intérêt de l'inscription de ces deux lignes dans le fichier de zone DNS.

L'objectif à atteindre est une meilleure tolérance aux pannes pour une disponibilité maximum du site *web*.

A1.3 : Proposer deux évolutions, tant matérielles que logicielles, permettant d'atteindre l'objectif visé. Vos propositions seront argumentées et justifiées.

Par ailleurs, lorsqu'ils sont sollicités par leur nom de domaine pleinement qualifié (FQDN), les deux serveurs *web* d'Armatis-LC doivent être en mesure de répondre aux requêtes émises à l'aide du protocole IPv6.

A.1.4 : Définir les entrées à ajouter dans le fichier de zone `db.armatis-lc.com` pour prendre en compte le protocole IPv6.

Mission 2 – Administration à distance des serveurs *web*

Pour administrer les serveurs *web* dédiés hébergés au sein de l'infrastructure BDN, l'équipe systèmes et réseaux d'Armatis-LC utilise le protocole SSH. Votre responsable vous demande de rédiger une procédure « Connexion aux serveurs en SSH » décrivant la connexion au service SSH de chaque serveur. Cette procédure sera intégrée à la base de connaissance dans la rubrique « Bonnes pratiques techniciens ».

Pour cela, vous testez la connexion au serveur « Web 2 » à partir de votre compte nouvellement créé (*techsys*) et vous tracez les événements survenus lors des connexions SSH dans un document.

A.2.1 : Rédiger la procédure en fournissant toutes les explications nécessaires concernant :

a) **L'impossibilité de se connecter avec le compte administrateur *root* ;**

b) **L'apparition du message d'avertissement lors d'une première connexion depuis un client SSH en justifiant l'attitude à adopter.**

Le serveur « Web 2 » a subi une panne physique. Le temps de la réparation, l'hébergeur vous met à disposition, sur la même adresse IP, un autre serveur. Un message d'erreur est affiché lors de la tentative de connexion au serveur de secours qui a les mêmes configurations IP que l'ancien serveur Web 2

A.2.2 : Expliquer la raison du message d'erreur lors de la tentative de connexion sur le nouveau serveur de secours.

A.2.3 : Proposer une solution afin de pouvoir se connecter à distance avec le protocole SSH sur le serveur de secours.

Votre responsable vous demande d'analyser les fichiers journaux concernant l'authentification au service SSH sur le serveur « Web 2 ». Vous constatez que de nombreuses tentatives de connexion illégitimes depuis internet ont été tentées.

A.2.4 : Définir le principe des attaques de type force brute.

A.2.5 : Proposer trois recommandations non encore implémentées afin de minimiser les risques liés à ce type d'attaque sur le service SSH de vos serveurs.

Dossier B : Gestion des éléments d'infrastructure

Documents nécessaires à la réalisation du dossier B : B.1 à B.6.

Mission 1 - Élaboration et présentation d'un dossier de choix de solution technique

Un incident sur le réseau électrique a montré la nécessité de renouveler l'onduleur du site de Châteauroux. M. Ricot vous a envoyé un courrier électronique dans lequel il précise un certain nombre d'éléments techniques utiles afin de préparer une décision d'achat.

B.1.1 : Établir une liste des critères à étudier pour choisir l'onduleur en respectant les besoins exprimés par M. Ricot.

B.1.2 : Calculer la puissance en VA (voltampères) que devra fournir l'onduleur pour couvrir les besoins des éléments à protéger sur le site de Châteauroux.

B.1.3 : Rédiger la réponse au courrier électronique de M. Ricot dans laquelle vous justifierez le modèle d'onduleur que vous préconisez.

Mission 2 - Supervision des services et éléments d'infrastructure

Le nouvel onduleur vient d'être installé et intégré au logiciel de supervision en tant que nouvel hôte supervisé.

Vous avez en charge la préparation du paramétrage des deux nouveaux services à créer permettant le déclenchement d'une alerte lorsque que :

a) le niveau de batterie passe à « faible » puis à « déchargé » ;
b) le temps restant de fourniture d'électricité par l'onduleur passe d'un niveau normal à un niveau d'alerte, puis à un niveau d'alarme critique.

B.2.1 : Indiquer, pour chaque service, les valeurs ou intervalles de valeurs des trois arguments nommés « OID », « warning » et « critical ».

Mission 3 : Intégration d'un nouveau plateau technique pour gérer l'activité d'un nouveau client

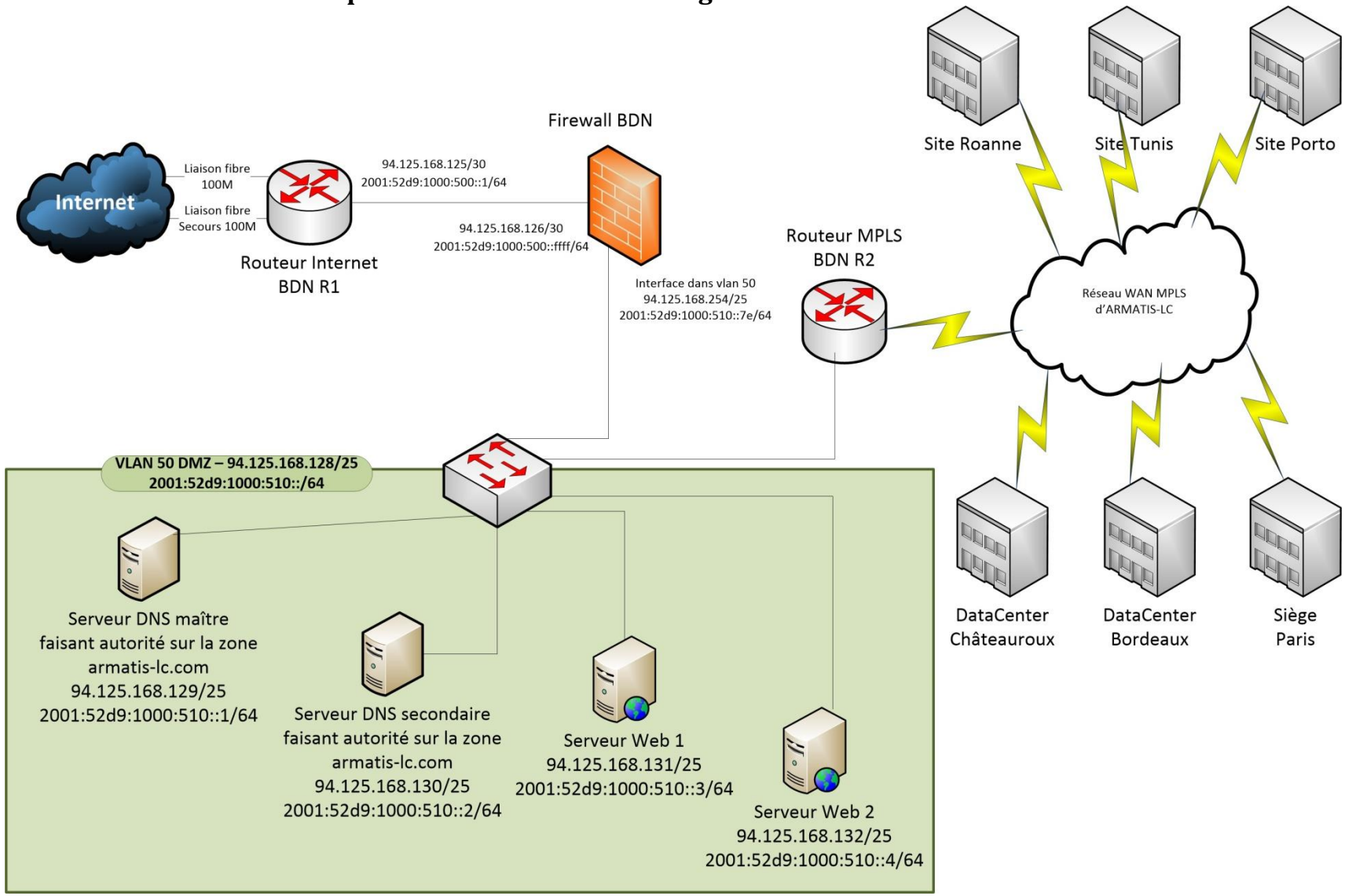
Armatis-LC ayant remporté un important marché auprès du client Engie, un nouveau plateau technique de télémarketing (C2) a été monté en urgence dans le bâtiment A du site de Châteauroux afin de démarrer au plus vite l'activité. Alors que le brassage dans les baies du plateau C2 est conforme à la situation décrite par le document B.6, les tests ont montré que toute communication entre ordinateurs est impossible. Il ne fait aucun doute que le réseau du plateau C2 est victime d'une tempête de diffusion.

B.3.1 : Identifier, à partir du tableau décrivant le câblage réel, quelle est la raison de cet incident et quelle intervention précise sur le câblage va permettre un retour instantané à la normale.

Après la mise en exploitation et en réétudiant le document B.5, il a finalement été décidé d'améliorer la tolérance aux pannes sur les liens montants des deux ailes Nord-Sud vers le commutateur SwCHTX20.

B.3.2 : Proposer les modifications à effectuer pour atteindre cet objectif en prenant soin de différencier les modifications à effectuer au niveau du câblage et celles à effectuer au niveau du paramétrage logiciel des équipements d'interconnexion.

Document A.1 : Schéma simplifié du réseau chez l'hébergeur BDN



Document A.2 : Configuration des serveurs hébergés chez le prestataire BDN

Tableau de synthèse de la configuration réseau des serveurs :

	Nom de domaine FQDN	Adresses IPv4	Adresses IPv6
Serveur DNS faisant autorité	ns1.armatis-lc.com	94.125.168.129/25 127.0.0.1/8	2001:52d9:1000:510::1/64 fe80::ca0a:a9ff:fec8:e8b4/64 ::1/128
Serveur DNS secondaire faisant autorité	ns2.armatis-lc.com	94.125.168.130/25 127.0.0.1/8	2001:52d9:1000:510::2/64 fe80::ca0a:a9ff:fec8:e8b5/64 ::1/128
Serveur Web 1	www.armatis-lc.com	94.125.168.131/25 127.0.0.1/8	2001:52d9:1000:510::3/64 fe80::ca0a:a9ff:fec8:e9b6/64 ::1/128
Serveur Web 2	www.armatis-lc.com	94.125.168.132/25 127.0.0.1/8	2001:52d9:1000:510::4/64 fe80::ca0a:a9ff:fec8:eab7/64 ::1/128

Extraits des fichiers de configuration d'un des serveurs DNS faisant autorité

adminsys@ns1:~$ **sudo cat /etc/bind/db.armatis-lc.com**

```
; La durée de vie des enregistrements est de 12 heures. Les serveurs DNS récursifs
; stockeront les informations sur cette zone dans leur cache pendant ce laps de temps
$TTL 43200   ; 12 heures

; l'adresse du contact technique est postmaster@armatis-lc.com
armatis-lc.com.  IN   SOA  ns1.armatis-lc.com.  postmaster.armatis-lc.com. (
             2017060101   ; Serial
             1D     ; Refresh
             1H     ; Retry
             1W     ; Expire
             3H )   ; Negative Cache TTL


; Déclaration des serveurs DNS

armatis-lc.com.           IN     NS     ns1.armatis-lc.com.
ns1.armatis-lc.com.       IN     A      94.125.168.129

armatis-lc.com.           IN     NS     ns2.armatis-lc.com.
ns2.armatis-lc.com.       IN     A      94.125.168.130

; Déclaration des serveurs Web (round-robin)

www.armatis-lc.com.       IN     A      94.125.168.131
www.armatis-lc.com.       IN     A      94.125.168.132
extranet.armatis-lc.com.  IN     CNAME  www.armatis-lc.com.


...
```

Document A.3 : DNS - principes, fonctionnement global et recommandations

La résolution de noms de domaine DNS est le mécanisme qui permet de récupérer les enregistrements associés à un nom de domaine et à un type donnés. Les serveurs DNS hébergés au sein du centre de données de l'hébergeur BDN sont des serveurs faisant autorité sur le domaine *armatis-lc.com*.

Les principaux types d'enregistrement

Les différents types d'enregistrement DNS sont publiés et maintenus par l'*Internet Assigned Numbers Authority* (l'IANA) dans un registre dédié aux paramètres du DNS :

- A : une adresse IPv4 ;
- AAAA : une adresse IPv6 ;
- MX : le nom d'un relais de messagerie électronique entrant ;
- NS : le nom d'un serveur DNS ;
- CNAME : type d'enregistrement DNS qui permet de signifier qu'un nom de domaine est un alias correspondant à un autre nom de domaine.

Résilience du service DNS selon les RFC

La résilience est définie comme la capacité à fonctionner pendant un incident et à revenir à l'état nominal. Les *requests for comments* (littéralement demande de commentaires (ou RFC)), normes de fait et développées par *l'Internet Engineering Task Force* (IETF) - l'entité qui élabore les standards de l'Internet - recommandent l'utilisation d'au moins deux serveurs de noms distincts.
Ainsi, la localisation des différents serveurs devrait être prise en considération afin de limiter l'impact d'incidents environnementaux, comme les coupures électriques, les coupures de fibres optiques, les inondations ou encore les tremblements de terre.
Les serveurs de noms doivent être physiquement dispersés. Il faut prévoir au minimum un second site d'hébergement. Cette précaution reste valable au niveau de l'architecture du réseau. Il faut s'assurer que tous les serveurs de noms ne dépendent pas d'un même élément physique (routeur, commutateur, etc.), ne soient pas dans le même sous-réseau et ne soient pas sur une même ligne dédiée.

Répartition de charge à l'aide de la technologie DNS *round-robin*

Le DNS tourniquet ou *round-robin* est une des techniques de répartition de charge consistant à associer plusieurs adresses IP à un nom de domaine pleinement qualifié (FQDN) afin de répartir les réponses à un service sur plusieurs serveurs, suivant un algorithme d'ordonnancement de type égalitaire.
L'avantage de ce système de répartition de charge est qu'il ne nécessite pas d'outil logiciel spécifique ou de boitier spécialisé. De plus, les serveurs n'ont pas à être sur le même réseau, ni gérés par le même prestataire.
Un des inconvénients de cette technologie est que lorsque le serveur DNS faisant autorité sur une ou plusieurs zones est modifié, il faut attendre un certain délai nommé *Time to live* pour que l'ancienne adresse IP ne soit plus utilisée par les clients ou les serveurs récursifs qui l'avaient placée en cache.

Sources :

- Extrait du rapport *Résilience de l'Internet français 2014* publié par l'Agence Nationale de la sécurité des systèmes d'information (ANSSI) et l'Association française pour le nommage Internet en coopération (Afnic).
- Extrait du guide *Bonne pratique pour l'acquisition et l'exploitation d'un nom de domaine* publié par l'ANSSI en 2015.
- Extrait de l'article *DNS Round-Robin* publié sur le site Wikipédia.

Document A.4 : Le protocole SSH - principes, fonctionnement global et recommandations

SSH, ou *Secure Shell*, crée un canal chiffré et authentifié entre un client et un serveur. Le service écoute sur le port 22 et fonctionne à l'aide du protocole de transport TCP. L'administration à distance en ligne de commande est le cas d'usage le plus répandu de SSH.

L'approche *Trust on the first use* (TOFU)
Le principe général est de considérer, par un acte de foi (TOFU est également appelé, en anglais, "*leap of faith*"), que la première fois que l'on reçoit une empreinte de clef publique, celle-ci n'a pas été émise par un attaquant. Une fois cette empreinte de clef acceptée une première fois, il est admissible que toute communication future impliquant cette clef publique soit avec le même correspondant. Le client n'émettra ensuite un avertissement qu'à la réception d'une nouvelle clef pour un serveur sur lequel il ne s'est encore jamais connecté.

Configurations
Sur un serveur :
1. */etc/ssh/sshd_config* est le fichier de configuration du service SSH ;
2. */etc/ssh/ssh_host_ecdsa_key.pub* est la clef publique sur serveur SSH ;
3. */etc/ssh/ssh_host_ecdsa_key* est la clef privée du serveur SSH ;

Sur un client :
1. */etc/ssh/ssh_config* est le fichier de configuration générique du client SSH ;
2. *~/.ssh/known_hosts* est le fichier où sont enregistrées les empreintes des clefs publiques des serveurs proposées lors d'une première connexion avec un utilisateur particulier. Chaque utilisateur dispose de son propre fichier *known_hosts*.

Note : « ~» est une variable d'environnement prenant pour valeur le répertoire personnel de l'utilisateur connecté.

Bonnes pratiques (non exhaustives) à respecter dans l'utilisation du protocole SSH
- Il faut s'assurer de la légitimité du serveur contacté avant de poursuivre l'accès. Cela passe par l'authentification préalable de la machine au travers de l'empreinte de sa clé publique.
- La clé privée ne doit être connue que de l'entité qui cherche à prouver son identité à un tiers. Cette clé privée doit être dument protégée pour en éviter la diffusion à une personne non autorisée.
- La possession d'un compte dédié pour chaque utilisateur permet une gestion plus fine des accès et une meilleure traçabilité. Le compte *root* est un compte générique sur les systèmes Unix et GNU/Linux qui dispose de tous les droits sur le système. Ainsi, le compte *root* ne doit pas être accessible directement à un utilisateur distant.
- Il faut privilégier l'authentification par clefs cryptographiques plutôt que par simple mot de passe. Cela limite les risques d'attaques par dictionnaire et par force brute.
- L'utilisation d'outils spécialisés comme *Fail2ban* permettent de bloquer temporairement les adresses IP qui émettent des attaques de type force brute sur le service SSH à partir de l'observation en temps réel des journaux systèmes. Leur principe de fonctionnement est relativement simple, il s'agit de bloquer les adresses IP qui ont tenté un certain nombre de connexions infructueuses dans un laps de temps donné.

Sources
- Extraits du guide *des recommandations pour un usage sécurisé d'(Open)SSH* publié par l'ANSSI en 2011.
- Extrait de *La fin annoncée des autorités de certification, alternatives : TOFU, Convergence, CATA, Clés souveraines, DANE* publié en 2011 par Florian Maury, spécialiste sécurité des services et des réseaux à l'ANSSI.

Document A.5 : Événements survenus lors des connexions SSH vers le serveur Web 2

Première connexion sur le serveur Web 2 en SSH

```
techsys@pc-client:~$ ssh techsys@94.125.168.132
The authenticity of host '94.125.168.132' can't be established
ECDSA key fingerprint is SHA256:QybjOXjdyDj7yg7T+cV3cyPqWpsGkZGvqtg44W8xtM0.
Are you sure you want to continue connecting (yes/no)? yes
techsys@94.125.168.132's password:
Linux www2 3.2.0-4-amd64 #1 SMP Debian 3.2.68-1+deb7u2 x86_64
Last login: Wed May 03 17:55:04 2017 from 198.51.100.57
techsys@www2:~$
```

Échec de la connexion SSH au serveur Web 2 avec le compte et le mot de passe de l'administrateur *root*

```
techsys@pc-client:~$ ssh root@94.125.168.132
root@94.125.168.132's password:
Permission denied, please try again.
root@94.125.168.132's password:
Permission denied, please try again.
root@94.125.168.132's password:
Permission denied (publickey,password).
```

Analyse des fichiers journaux d'authentification concernant le service SSH (extrait)

techsys@www2:~$ **sudo cat /var/log/auth.log | grep sshd | grep Failed**

```
May 5 08:25:44 www2 sshd: Failed password for invalid user admin from
91.224.160.131 port 41120 ssh2
May 5 08:26:00 www2 sshd: Failed password for invalid user adm from
91.224.160.131 port 41120 ssh2
May 5 08:26:05 www2 sshd: Failed password for invalid user postgres from
91.224.160.131 port 41120 ssh2
May 5 14:22:28 www2 sshd: Failed password for root from 198.51.100.57 port 51495
ssh2
```

Message d'erreur lors de la tentative de connexion au serveur de secours à qui il a été attribué les mêmes configurations IP que l'ancien serveur Web 2

```
techsys@pc-client:~$ ssh techsys@94.125.168.132
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!       @
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)! It
is also possible that a host key has just been changed. The fingerprint for the
ECDSA key sent by the remote host is
SHA256:9lfA9ctGHx/EXi4JefeBmiI0Tw6MAKYQ3/Lki+vDviQ.
Please contact your system administrator.
Add correct host key in ~/.ssh/known_hosts to get rid of this message.
Offending ECDSA key in ~/.ssh/known_hosts:9
ECDSA host key for 94.125.168.132 has changed and you have requested strict
checking.
Host key verification failed.
```

Document B.1 : Courrier électronique envoyé par M. Ricot

De : a.ricot@armatis-lc.com

À : techsys@armatis-lc.com

Objet : choix pour renouvellement de l'onduleur Salle 2 – Baie R3

Bonjour,

Lors des dernières intempéries, le réseau électrique a été coupé et notre onduleur du site de Châteauroux n'a pas été en mesure de tenir la charge nécessaire le temps théoriquement prévu (on souhaite que les éléments de notre salle serveurs soient encore opérationnels au moins 1 heure 30 en cas de panne électrique du secteur). J'ai déjà commencé à sélectionner quelques modèles qui me paraissaient plus ou moins intéressants, mais je n'ai pas eu le temps de pousser plus loin les recherches.

Chez Armatis-LC - site de Châteauroux, les éléments à protéger impérativement à ce jour de toute coupure électrique durant la durée fixée sont les suivants :

Éléments	Nombre	Puissance approximative consommée par élément (**en Watts**)
Serveurs dédiés aux activités de nos clients	5	300
Moniteurs de contrôle	2	100
Commutateurs	10	400
Routeurs	10	200
Serveurs physiques équipés des ESXi	3	300
Routeurs pour connexions WAN Armatis-LC et clients	5	100
Robot de sauvegardes	1	500
Baie SAN	1	400

Pour rappel : **Puissance (VA) ≈ Puissance (W) x 1,5.**

Exemple : 100 W ≈ 150 VA (Voltampères).

Les contraintes environnementales dont Armatis-LC s'est emparée nous conduisent aussi à envisager un objectif de réduction de 20 % des consommations électriques d'ici 2022. En effet, Armatis-LC souhaite respecter la norme ISO 50001 qui fixe les lignes directrices pour développer une gestion méthodique de l'énergie afin de privilégier la performance énergétique.

Il est également fondamental que le nouvel onduleur envisagé puisse être supervisé afin de pouvoir être informé au plus tôt dès que l'un des paramètres critiques n'est plus conforme (niveau de charge restant, durée restante, …).

J'ai placé en pièces jointes quelques extraits issus d'une première sélection de sites marchands présentant différents modèles d'onduleurs qui pourraient s'avérer intéressants, mais une analyse plus complète reste à opérer. Je n'ai pas pris le temps de m'assurer que toutes les caractéristiques étaient conformes à nos attentes.

Cordialement,
A. Ricot.

Pièce 1 jointe au courriel de M. Ricot

SOCOMEC Masterys-BC

de 8 à 12 kVA : Protection de l'alimentation fiable, simple et prête à l'emploi

La solution pour : • Salle serveurs • Secteur tertiaire • Infrastructure • Secteur de la santé

Avantages : La protection idéale

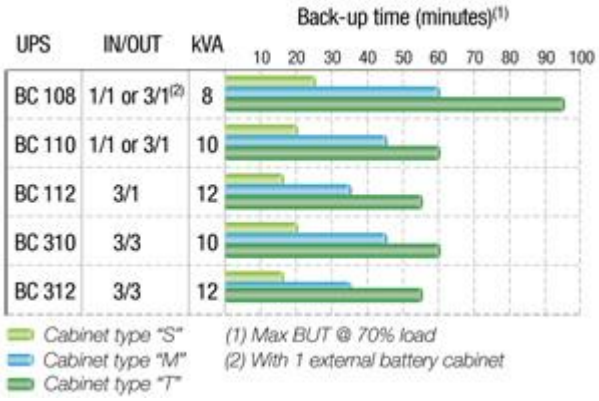
• Adaptée aux entreprises de taille moyenne.
• Les avantages d'une technologie de pointe.

Excellent rapport dimensions / puissance / autonomie

• Bien adapté aux applications professionnelles sensibles.
• Recommandé pour la protection des environnements informatiques en raison de l'intégration des batteries et de sa possibilité de montage dans des armoires rack 19".

Adapté à votre environnement

• Choix des autonomies ;
• Différentes config. sont disponibles : soit intégrées dans l'armoire standard de l'onduleur, soit en utilisant des armoires onduleurs plus hautes, sans augmenter la surface au sol
• Extensible en puissance ou en disponibilité (redondance) par la mise en parallèle jusqu'à 2 unités.



Options de communication

• Coffret synoptique de télésignalisation.
• NET VISION : interface professionnelle WEB/SNMP pour la supervision de l'onduleur et la gestion d'arrêt de différents O/S.

Caractéristiques techniques MASTERYS-BC

Sn [kVa]	8	10	12
Pn [kW]	5,6	7	8,4
Masse	155 kg	160 kg	175 kg
Configuration parallèle	jusqu'à 2 unités		
Entrée	Tension nominale : 230 V ou 400 V		
Sortie	Tension nominale **:** 230 V ou 400 V		
Rendt (certification ISO 50001)	ECO MODE **:** jusqu'à 98 %		
Dim. type S (courte) L x P x H	444 x 795 x 800 mm		
Dim. type M (médium) LxPxH	444 x 795 x 1000 mm		
Dim. type T (haute) L x P x H	444 x 795 x 1400 mm		
Normes Sécurité	CEI/EN 62040-1, EN 60950-1-1, AS 62040.1.1, AS 62040.1.2		
Normes Perf.	VFI-SS-111 - CEI/EN 62040-3, AS 62040.3		

Pièce 2 jointe au courriel de M. Ricot

APC Symmetra LX 16kVa

Tensions : 220/230/240V ou 380/400/415V

Durée de fonctionnement: **180 minutes**

Équipements standards :

- Interface Port DB-9 RS-232
- RJ-45 10/100 Base-T
- Smart-Slot,
- Comprend: CD avec logiciel et documentation, Carte de gestion web/SNMP

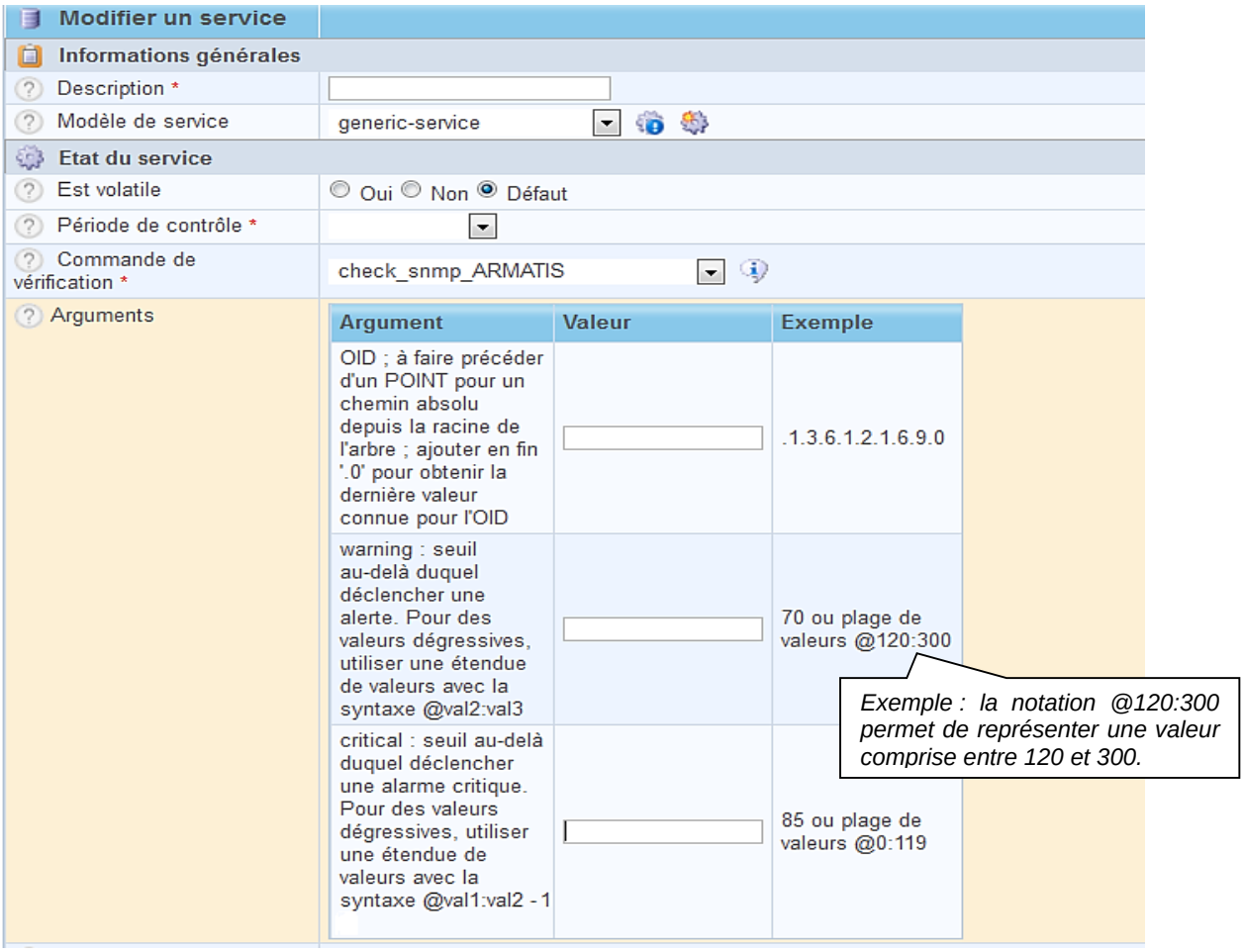
Principales fonctionnalités

- Puissance de 16 kVa
- Alarmes sonores
- Redémarrage automatique des charges après extinction de l'onduleur
- Autotest automatique
- Modules de batteries connectés en parallèle
- Configurable pour redondance interne N+1
- Notification de batterie déconnectée
- Compatible avec le générateur
- Batteries échangeables à chaud
- Modules de renseignement échangeables à chaud
- Modules de distribution échangeables à chaud
- Gestion intelligente des batteries
- Écran LCD
- Batteries externes gérables
- Gérable par réseau
- Batteries externes Plug-and-Play
- Notification prédictive de panne
- Modules de renseignements redondants
- Plateau amovible de câblage d'entrée/sortie
- Coupe-circuits réarmables
- Homologué par un Bureau de sécurité
- Certification ISO 50001
- Capacité électrique évolutive
- Durée de fonctionnement évolutive
- SmartSlot
- Batteries, modules de renseignements et modules d'alimentation remplaçables par l'utilisateur

Document B.2 : Le système de supervision par hôte

L'outil de supervision employé au quotidien chez Armatis-LC est *Centreon*, logiciel libre édité par la société française *Merethis* permettant de surveiller des éléments actifs (commutateurs, routeurs, etc.), des hôtes (PC, imprimantes, caméras, etc.) et les services spécifiés. Basé historiquement sur l'application Nagios, il intègre depuis 2012 ses propres moteur de collecte (*Centreon Engine*) et gestionnaire d'événements (*Centreon Broker).*

Typiquement, la surveillance d'un service (sur un élément) et la génération automatique d'alerte SNMP (*Simple Network Management Protocol*) se réalise via le formulaire suivant (extrait) :



Document B.3 : Supervision des services inhérents au nouvel onduleur

Les besoins immédiats concernent, d'une part, le niveau de batterie et, d'autre part, le temps restant à l'onduleur dans sa capacité à fournir de l'électricité.

M. Ricot souhaite que les états de type « Warning » et « Critical » se déclenchent automatiquement et qu'il soit informé immédiatement par courrier électronique et SMS pour deux services :

- **le service « Etat_batterie_onduleur »** : le système doit déclencher une alerte lorsque la batterie passe à l'état « faible » et une alarme critique lorsqu'elle présente une charge insuffisante (état « déchargée ») ;
- **le service « Temps_restant_batteries_onduleur »** : l'arrêt d'urgence des serveurs prend au maximum huit minutes. Durant une période couvrant le double de ce temps, l'onduleur doit déclencher une alarme critique. Par précaution, le niveau d'alerte doit, lui, couvrir la période allant jusqu'à quatre fois le temps d'arrêt d'urgence.

Document B.4 : Description d'OID (Object Identifier) de la MIB (Management Information Base) UPS (Uninterruptible Power Supply) – extrait

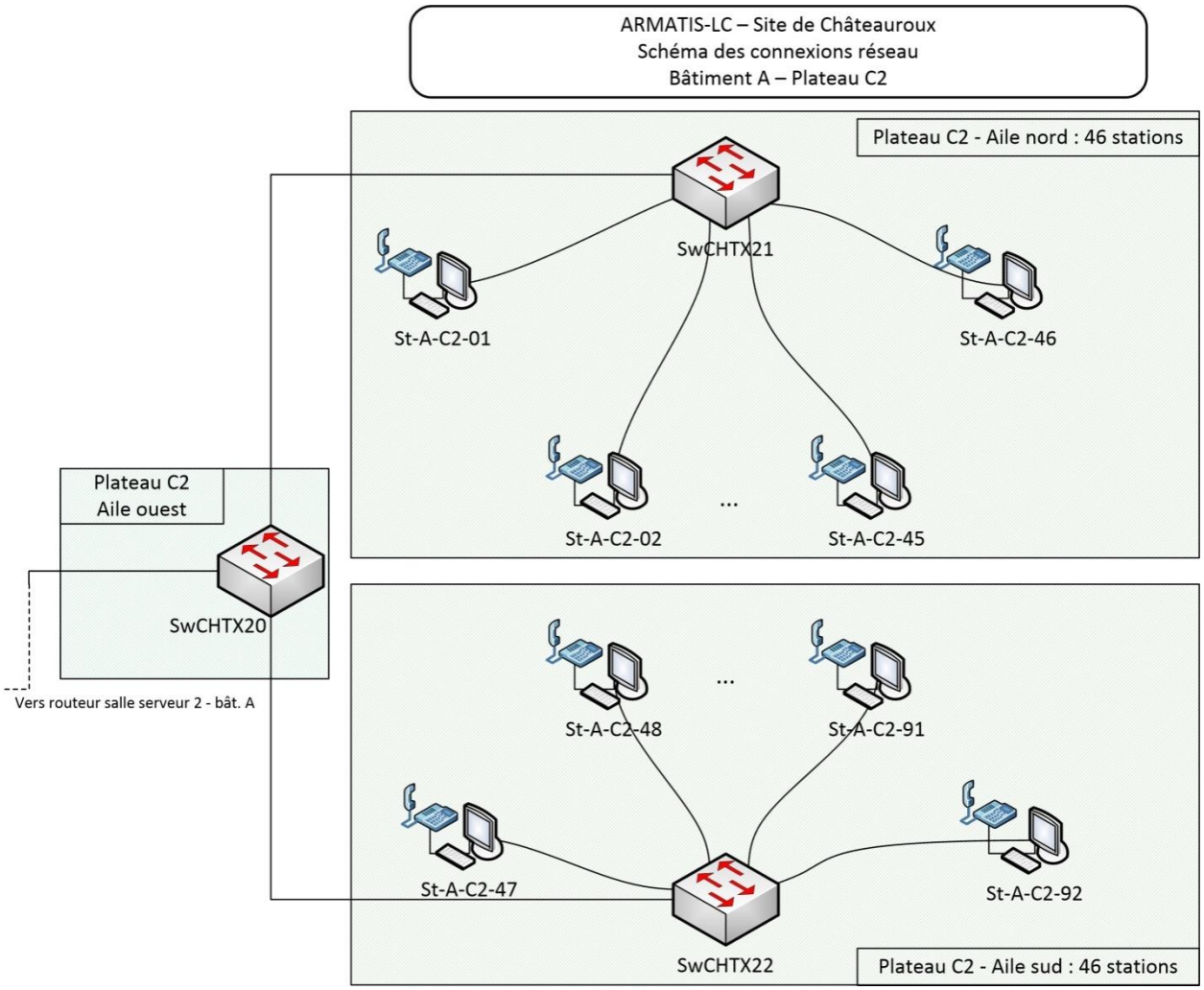
Source : IETF (Internet Engineering Task Force)

OID	Nom	Description	Unité	Syntaxe
1.3.6.1.2.1.33.1.1.1	upsIdentManufacturer	Nom du fabricant de l'UPS.		OctetString (0...31)
1.3.6.1.2.1.33.1.1.2	upsIdentModel	Libellé du modèle de l'UPS.		OctetString (0...63)
1.3.6.1.2.1.33.1.1.3	upsIdentUPSSoftwareVersion	Version(s) logicielle(s) de l'UPS.		OctetString (0...63)
1.3.6.1.2.1.33.1.2.1	upsBatteryStatus	Indication de la capacité restante dans les accumulateurs de l'UPS. La valeur *batteryNormal* indique que le temps d'exécution restant est supérieur à *upsConfigLowBattTime*. La valeur *batteryLow* indique que le temps de fonctionnement restant sur accumulateur est inférieur ou égal à *upsConfigLowBattTime*. La valeur *batteryDepleted* indique que l'UPS sera ou serait incapable de soutenir la charge actuelle si la source d'alimentation est ou était perdue.		Enumeration (1-unknown, 2-batteryNormal, 3-batteryLow, 4-batteryDepleted)
1.3.6.1.2.1.33.1.2.2	upsSecondsOnBattery	Lorsque l'équipement fonctionne sur accumulateur : temps écoulé depuis la dernière commutation sur accumulateur ou depuis le dernier redémarrage du sous-système de gestion du réseau (plus petite des deux valeurs). La valeur zéro est retournée si l'équipement ne fonctionne pas sur accumulateur.	Secondes	NonNegativeInteger
1.3.6.1.2.1.33.1.2.3	upsEstimatedMinutesRemaining	Estimation du temps restant avant épuisement des accumulateurs dans les conditions actuelles de charge si la source d'alimentation est coupée et le reste, ou si elle devait être coupée et le rester.	Minutes	PositiveInteger
1.3.6.1.2.1.33.1.2.4	upsEstimatedChargeRemaining	Estimation de la charge restante des accumulateurs exprimée en pourcentage de la charge maximale.	Pourcentage	Integer32 (0...100)
1.3.6.1.2.1.33.1.2.5	upsBatteryVoltage	Tension actuelle des accumulateurs.	0,1 Volt	NonNegativeInteger
1.3.6.1.2.1.33.1.2.6	upsBatteryCurrent	Intensité actuelle des accumulateurs.	0,1 Ampère	Integer32
1.3.6.1.2.1.33.1.2.7	upsBatteryTemperature	Température ambiante dans ou à proximité du boîtier de l'*UPS*.	Degrés C	Integer32
1.3.6.1.2.1.33.1.3.3.1.2	upsInputFrequency	Fréquence actuelle en entrée.	0,1 Hertz	NonNegativeInteger
1.3.6.1.2.1.33.1.3.3.1.3	upsInputVoltage	Tension actuelle en entrée.	Volts	NonNegativeInteger
1.3.6.1.2.1.33.1.4.4.1.2	upsOutputVoltage	Tension actuelle en sortie.	Volts	NonNegativeInteger
1.3.6.1.2.1.33.1.4.4.1.4	upsOutputPower	Puissance actuelle en sortie.	Watts	NonNegativeInteger
1.3.6.1.2.1.33.1.4.4.1.5	upsOutputPercentLoad	Pourcentage de la capacité de l'UPS couramment exploité en sortie.	Pourcentage	Integer32 (0...200)
1.3.6.1.2.1.33.1.6.3.1	upsAlarmBatteryBad	Un accumulateur doit être remplacé.		
1.3.6.1.2.1.33.1.6.3.13	upsAlarmChargerFailed	Un problème irrécupérable a été détecté dans le sous-système de recharge de l'*UPS*.		
1.3.6.1.2.1.33.1.6.3.14	upsAlarmUpsOutputOff	La sortie de l'UPS est désactivée.		

Document B.5 : Schéma simplifié de connexions réseau

Plateau C2 du bâtiment A : projet de câblage

Ce schéma, fourni dans le cahier des charges, présente les besoins du service de télémarketing nécessaires au traitement du client Engie.



Quatre-vingt-douze stations mixtes de travail (PC de bureau + téléphone IP avec micro-casque) doivent être installées afin de répondre aux besoins du nouveau client Engie, ainsi que trois baies de brassage équipées de bandeaux d'interconnexion et de commutateurs de niveau 2.

Document B.6 : Description du câblage réalisé dans les baies de brassage du plateau C2

Bâtiment A / Plateau C2 / Baie de brassage A-C2-Nord

Panneau de distribution « bandeau A » : 24 connecteurs

Numéro du connecteur	***Numéro de la prise raccordée***	***Commutateur et port reliés***
A1 à A24	(vers St-A-C2-01 à St-A-C2-24)	SwCHTX21 ports 0/1 à 0/24

Panneau de distribution « bandeau B » : 24 connecteurs

Numéro du connecteur	***Numéro de la prise raccordée***	***Commutateur et port reliés***
B1 à B22	(vers St-A-C2-25 à St-A-C2-46)	SwCHTX21 ports 0/25 à 0/46
B23	(vers Baie-A-C2-Sud-B23)	SwCHTX21 port 0/47
B24	(vers Baie-A-C2-Ouest-A21)	SwCHTX21 port 0/48

Commutateur « SwCHTX21 » : 48 ports (tous exploités)

Numéro du port	***Configuration VLAN***	***Numéro de VLAN***
0/1 à 0/46	Mode assigné (*access mode*)	20
0/47 à 0/48	Étiqueté 802.1Q	Tous

Bâtiment A / Plateau C2 / Baie de brassage A-C2-Sud

Panneau de distribution « bandeau A » : 24 connecteurs

Numéro du connecteur	***Numéro de la prise raccordée***	***Commutateur et port reliés***
A1 à A24	(vers St-A-C2-47 à St-A-C2-70)	SwCHTX22 ports 0/1 à 0/24

Panneau de distribution « bandeau B » : 24 connecteurs

Numéro du connecteur	***Numéro de la prise raccordée***	***Commutateur et port reliés***
B1 à B22	(vers St-A-C2-71 à St-A-C2-92)	SwCHTX22 ports 0/25 à 0/46
B23	(vers Baie-A-C2-Nord-B23)	SwCHTX22 port 0/47
B24	(vers Baie-A-C2-Ouest-A22)	SwCHTX22 port 0/48

Commutateur « SwCHTX22 » : 48 ports (tous exploités)

Numéro de l'port	***Configuration VLAN***	***Numéro de VLAN***
0/1 à 0/46	Mode assigné (*access mode*)	20
0/47 à 0/48	Étiqueté 802.1Q	Tous

Bâtiment A / Plateau C2 / Baie de brassage A-C2-Ouest

Panneau de distribution « bandeau A » : 24 connecteurs

Numéro du connecteur	***Numéro de la prise raccordée***	***Commutateur et port reliés***
A1	(vers Routeur – Bât. A – Serveurs 2)	SwCHTX20 port 0/1
A21	(vers Baie-A-C2-Nord-B24)	SwCHTX20 port 0/21
A22	(vers Baie-A-C2-Sud-B24)	SwCHTX20 port 0/22

Commutateur « SwCHTX20 » : 48 ports (3 exploités ; 45 libres)

Numéro de l'port	***Configuration VLAN***	***Numéro de VLAN***
0/1 à 0/48	Étiqueté 802.1Q	Tous

Note : le VLAN 20 est le VLAN attribué au client Engie.