The bridge to possible

Le Projet d'AUDIT en environnement Cisco

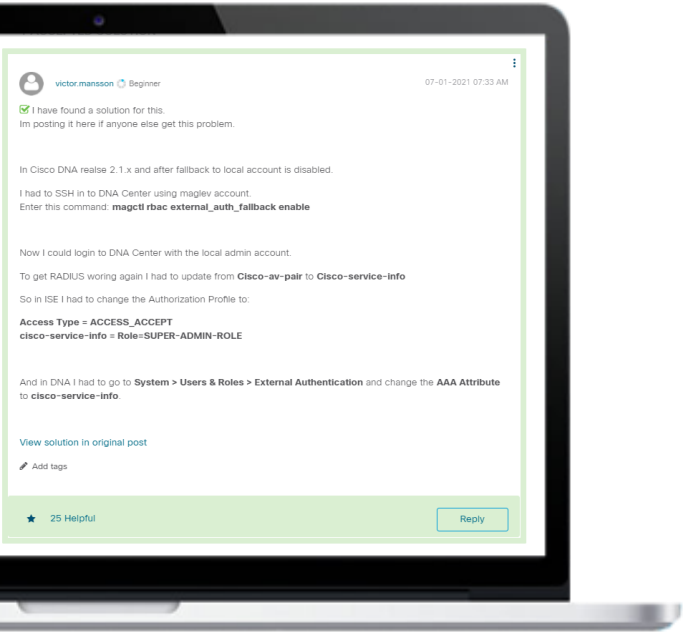
Appréhender les aspects techniques, humains et organisationnels.

Community Live – Général

Alain Faure– CCIE #8935 R&S

18 Novembre 2021

Connect, Engage, Collaborate!



Lorsque vous recevez une réponse correcte, **acceptez-la comme solution !**

Cela aide les autres utilisateurs à trouver des réponses correctes

Mettez en évidence les autres membres

Les votes utiles motivent les membres enthousiastes en leur offrant **un signe de reconnaissance !**

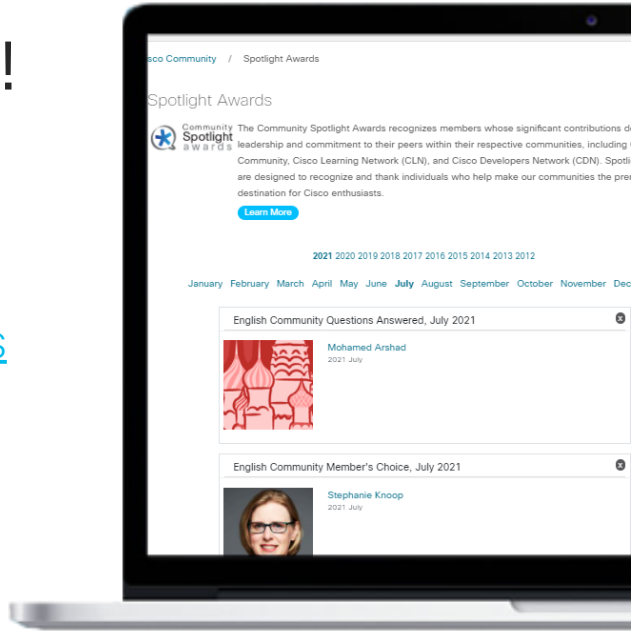
Spotlight Awards

De nouveaux lauréats chaque mois !

Gagnant du mois d'Octobre : **Youssouf Diallo**

Démarquez-vous par vos efforts et votre engagement à améliorer la communauté et à aider les autres membres. Les Spotlight Awards sont distribués chaque mois pour mettre en valeur les membres les plus remarquables.

Maintenant vous pouvez aussi désigner un candidat ! Cliquez ici



Notre Expert

Alain Faure
Présentateur

Jimena Saez
Modérateur

[Téléchargez la présentation !]

Agenda

1. Introduction
2. Livrables
3. Plan de travail
4. Relations humaines
5. Protocoles de l’information
6. Projet d’Audit

1. Introduction

Cette présentation

Dans tout réseau on se retrouve à faire ou à demander des audits techniques.

Nous allons voir en parallèle, les aspects :

- Techniques
- Relationnels
- d'Organisation

La philosophie de management derrière cette présentation est le **gain de vitesse** et de **maîtrise de l'infrastructure**.

Les bénéfices de l'audit

- Enlève le stress & évite le burn-out
- Permet de nombreuses économies
- Vous donne une connaissance complète et exhaustive de l'infrastructure
- Vous donne de bonnes relations avec la plupart de vos collègues
- Bref, Il guéri tous les maux.
  Par la prévention ! -> Sans douleur !

Ce que n’est PAS un audit

Abus de langage trop courant :
« il faut un audit qui solutionnera des problèmes »

Auditus (latin) -> <u>écouter</u> !

Un audit sert uniquement à écouter, à regarder, à comprendre. A recueillir l’information. C’est du renseignement.

Avertissement pour la MOE

- Evitez d'amener des virus, utilisez: LINUX
- N'essayez pas de « réparer » quoi que ce soit ! Facturez (contrat/assurance pro.) !
- Interrogez les utilisateurs, toujours !
- Soyez neutre à tout prix : personne n'a besoin d'un résultat biaisé.
- Quels sont les types d'équipements déployés ? Ayez la procédure de récupération des mots de passe au « cas où ».

Avertissement pour la MOA

- Ayez des rendez-vous réguliers 2j/sem.
- Ne demandez pas une réparation immédiate. L'audit doit d'abord être fini avant la phase intervention/changement.
- Assurez-vous de l'expérience de la MOE dans le domaine pro. > 10 ans (tech. et humains voir réglementaires)
- Rassemblez le maximum d'éléments techniques pour les tenir à disposition.
- Si vous avez un pbm de confidentialité demandez une clause NDA.

L’audit : une photo vitale

Quand on parle d’outils et de méthode, il faut savoir à quoi cela correspond : réaliser un audit c’est faire une photo d’un état à un instant T.

À partir de cette photo, on peut réaliser divers services :

- ✓ Recherche de panne
- ✓ Préparation à une évolution
- ✓ Préparation à la gestion quotidienne
- ✓ Etc.

L’audit : une organisation

Séparer la « photo » du « film » :

Photo : le résultat de l’audit

Film : le projet, la façon dont ont réalise l’audit

L’audit : le résultat

Etat actuel : la « photo »

- Plans, configurations, schémas
- Normes de nommage (étiquettes)
- Description texte du détail de l’architecture IT

En pratique : *chapitre* « Livrables »

- Répertoire par couche OSI
- Repérage par date et par périmètre
- Maintenir à jour et archiver ce qui est périmé

L’audit : le projet, la façon de le réaliser

Documentation du changement : « Film » de la modification et de l’évolution du réseau

Façon dont ce sont déroulé les projets, installations ou modifications

Mémoire de l’équipe infrastructure

En pratique : *chapitre* « Projet d’audit »

Répertoire par projet et par type d’évolution (audit : fait évoluer la partie documentaire)

Repérage par date et par périmètre

Polling Question 1

Lors de votre dernier audit vous étiez plutôt ?

1) MOA (maîtrise d'Ouvrage) : demandeur de l'audit
2) MOE (maîtrise d'Œuvre) : réalisateur de l'audit

2. Les livrables

Présentation du template

- Pour ma part j'utilise un template qui me sert pour la plupart de mes audits.
- Je vais vous décrire ce template en mettant l'accent sur la partie schéma.

SCHEMAS :

- Importance des schéma : GAGNER du temps -> Rapidité d'action
- Transfert de compétence plus rapide
- Facilite grandement les interventions des externes
- Mais ne remplace pas un document

ATTENTION : Ne pas doubler les informations. Une information ne doit se trouver qu'à un et un seul endroit !

Couche 1 OSI

- Types de câblage -Ex : cat6-
- Vérification du câblage (état des câbles, certification électronique)
- Les Points de raccordement (prises, patch-panels, interfaces)

Le LTE :

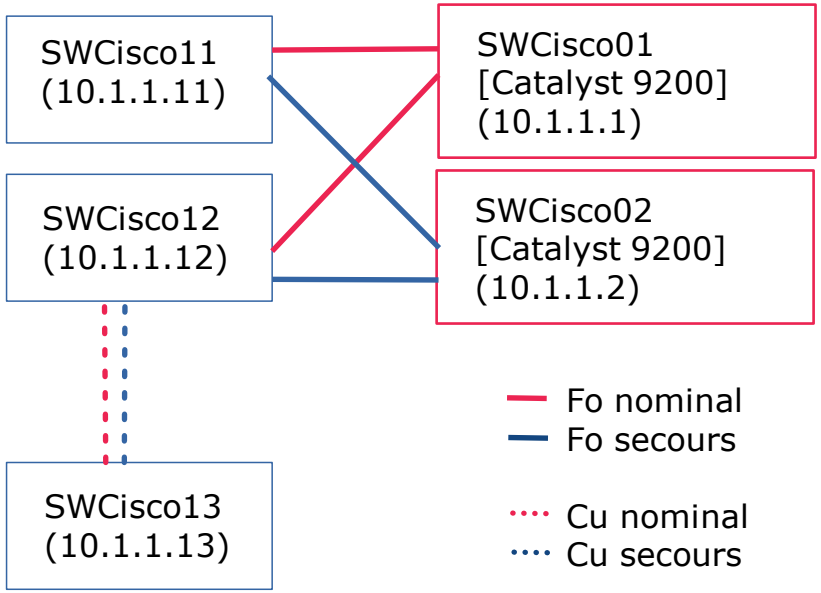
- Arrivées électriques et climatisation
- Mesures de sécurité et contrôle d'accès
- Racks, et Pach-panels et position des équipements
- Utilisation de protocoles comme CDP 'Cisco Discovery Protocol'
- Vérification de l'étiquetage

Couche 1 OSI - Schéma

Repérage:

- Nom, Adresse IP de management, type d'équipement
- Titre : Nom de site

- Pas toutes les liaisons : juste des trunks ou les liaisons vers un équipement commun -Ex: Routeur, FW-. Un fichier Excel est là pour ça.



Couche 2 OSI

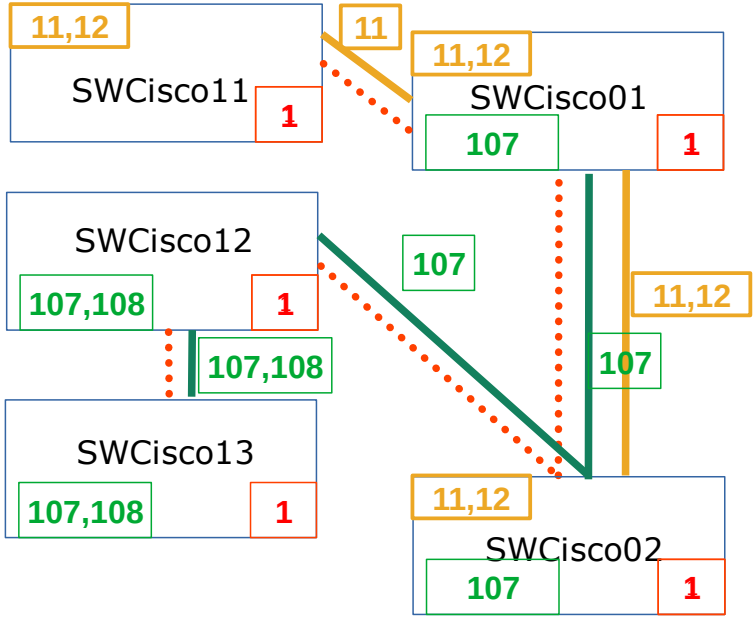
- Il est facile de représenter les liaisons de Niveau 2 du modèle OSI (VLANs, WANs) sur les schémas.
- Ce plan est indispensable pour les interventions sur le réseau. Il a une vraie utilité dans le travail quotidien et cela vaut le coup de le réaliser en couleur et de l'afficher en poster format A2 ou A1.
- Même si les plans existent sous forme électronique, une coupure de courant ou de réseau est vite arrivée, alors les plans papier peuvent sauver la situation. Il sont aussi beaucoup plus rapide à consulter.

Couche 2 OSI - Schéma

Repérage:

- Nom, liste des VLANs et les regrouper par couleur (data, Voip, wifi) . Indiquez le vlan par défaut (ici 1).
- Titre : Nom de site

- Les VLANs et leurs caractéristiques seront listées dans un fichier excel approprié.



Couche 3 OSI (1)

- Le schéma des domaines de routage.
- Une liste des sous-réseaux et leurs caractéristiques avec une description de leur utilité.
- Un schéma des réseaux avec représentation des équipements de traitement du niveau 3 comme :
  - ✓ Les routeurs
  - ✓ Les firewalls
  - ✓ Les répartiteurs de charge

Couche 3 OSI (2)

Un schéma des réseaux de niveau 3 avec représentation des éléments de niveau 2 comme support des réseaux:

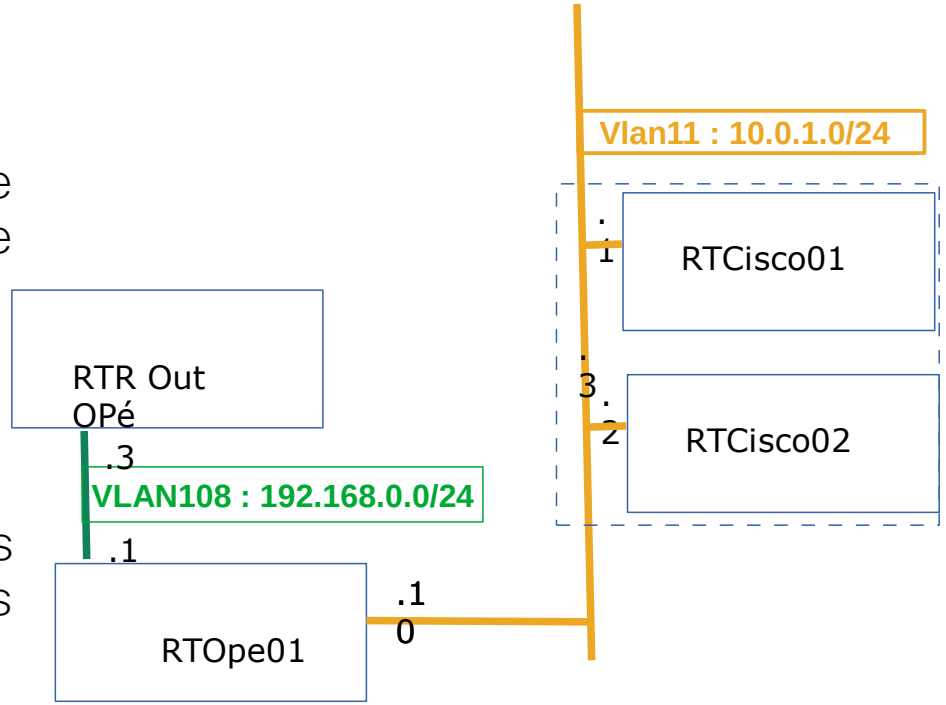
- Les VLANs
- Les liaisons WAN comme les liaisons MPLS, SDSL, frame-relay
- Les liaisons VLL comme des liaisons Ethernet longue distance

Avoir tous les schémas de la couche 3 sous forme papier est indispensable au travail quotidien.

Couche 3 OSI – Schéma adressage

Repérage:

- Nom, adresses IP, numéro de réseau avec masque, adresse passerelle par défaut.
- Titre : Nom de site
- Les réseaux IPs et leurs caractéristiques seront listées dans un fichier excel approprié.

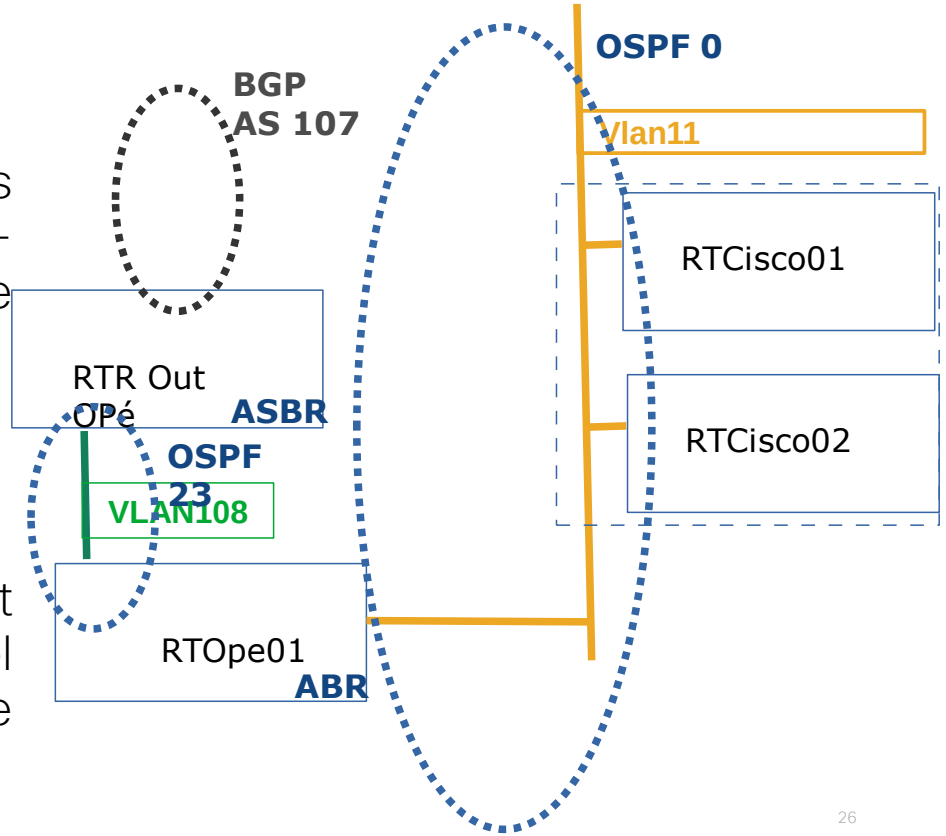


Couche 3 OSI – Schéma routage

Repérage:

- Nom, ID des routeurs, ID des zones, repérage des niveau 2 – Ex :VLANs-, points de redistribution.
- Titre : Nom de site

- Les réseaux et adresses IPs seront listées dans un fichier excel approprié. Ceci est susceptible de modification.



Livrables WiFi

- Document d'implémentation des points d'accès (AP).
- Un document descriptif des caractéristiques purement WiFi (intégration et caractéristiques WiFi). A faire par groupement d'AP WiFi similaires et par WLAN.

Finalisation de l’audit

Une fois les livrables réalisés et présentés il faut les classer dans une arborescence de répertoire.

Au delà du strict recueil d'information, la MOA attend aussi une expertise et une aide sur :

- Les points qui posent problèmes
- Les points à améliorer
- La prévision d'actions futures -Ex : achat d'équipement -

Arborescence typique

0_Géographie

1_Câblage

2_VLANs-SDACCESS

3_IPs-SDWAN

4_PortsTcpUdpFW

5_

6_

7_Applications

8_Utilisateurs

9_Archives

Polling Question 2

Pour quelle raison étiez-vous impliqués dans le dernier audit ?

1) Détection panne ponctuelle
2) Détection problème récurrent
3) Préparation de changement
4) Mise à jour documentation

3. Plan de travail

5 niveaux d’audit

1) Situation géographique, locaux techniques et racks
2) (Couche 1 OSI) Câblage, inventaire du câblage, Schémas
3) (Couche 2+ OSI) Configuration, Récupération des configurations et explications des particularités
4) Analyse des logs et des fichiers produits du système
5) Utilisateurs et équipements du poste client

Niveau 1

Réaliser un Inventaire matériel et Géographique.

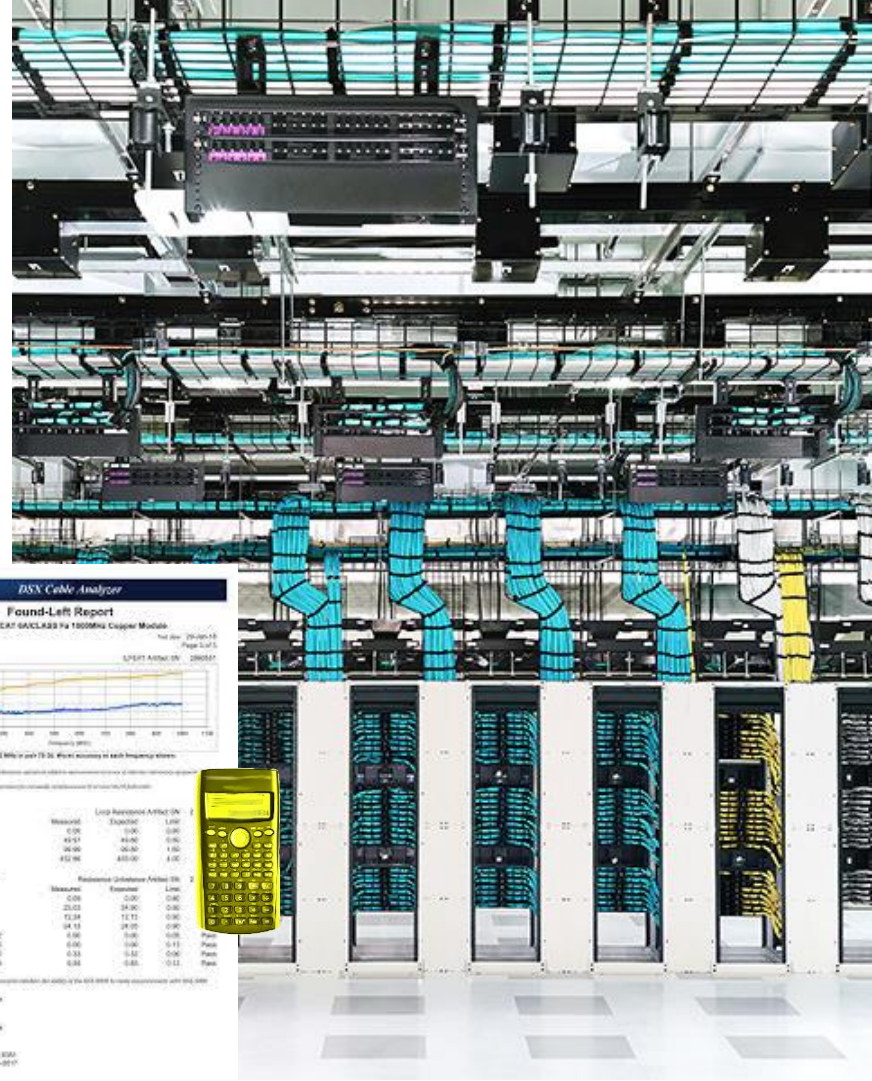
C'est l'occasion de faire une Visite de site et de discussion avec les responsables de la gestion des locaux (bâtiment).

Certification de câblage

Chaque bâtiment livré doit comporter un carnet de certification du câblage !
(une à 4 pages A4 par câble !)

Equipements pour le cuivre et la fibre optique sont disponibles.

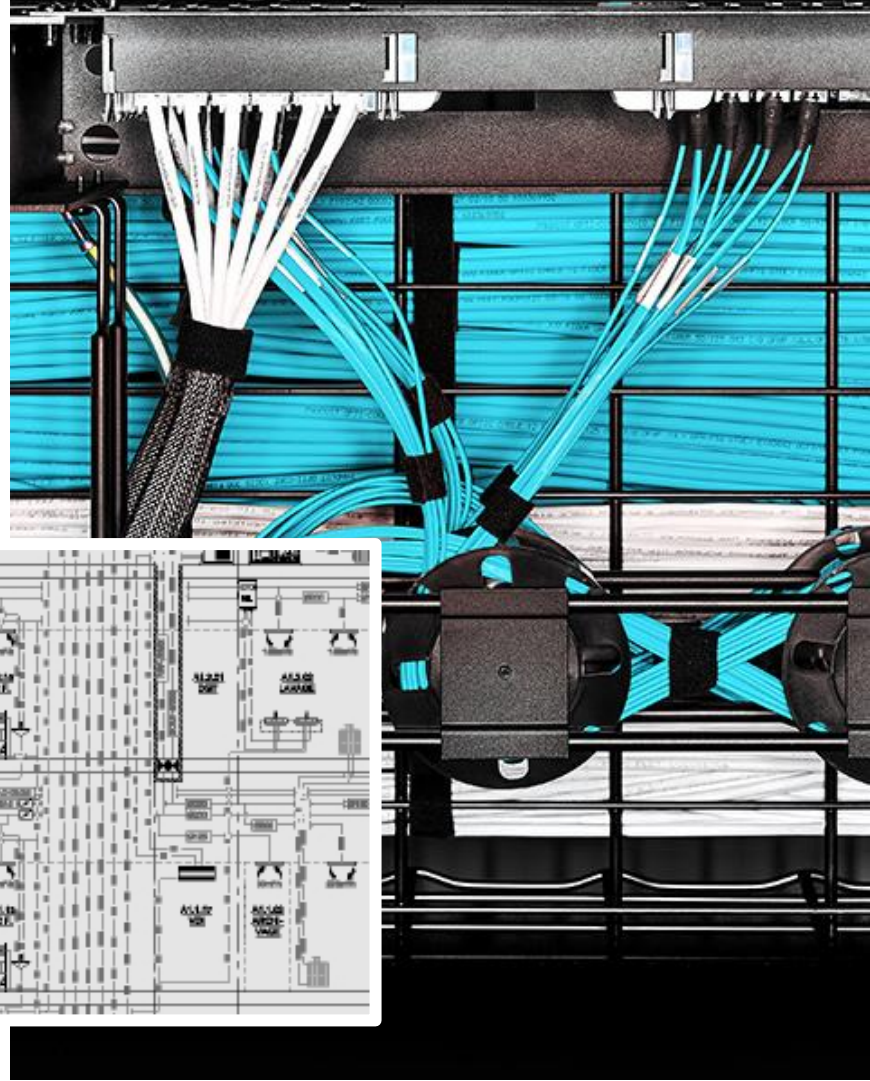
Ce travail doit être fait à la livraison où quand les problèmes erratiques commencent immanquablement.



Plan du câblage bâtiment

Avec chaque certification de câblage ou livraison d'un câblage il doit y avoir un plan du câblage qui se situe dans les faux planchers, les dalles, les gaines techniques et les LTE (Locaux Techniques d'Etage).

Les gens en charge du bâtiment peuvent l'avoir.



Niveau 2

Faire l'inventaire de toutes les liaisons physiques entre les équipements.

Les sources d'informations sont :

- Les schémas existants
- Le rapport de visite des locaux
- Éventuellement l'interview d'un employé réalisant le câblage

Dans ce genre d'exercice l'appareil photo est indispensable pour certains relevés fastidieux (surtout quand il y a des étiquettes. Chance !)

Niveau 3

La récupération puis l'analyse des configurations des équipements va permettre d'expliquer le fonctionnement des différentes parties de l'infrastructure.

On a besoin de recueillir les configurations et de les archiver dans un endroit de stockage.

Niveau 4

C'est le type d'audit classique quand il y a un problème à résoudre. Il faut vérifier les logs.

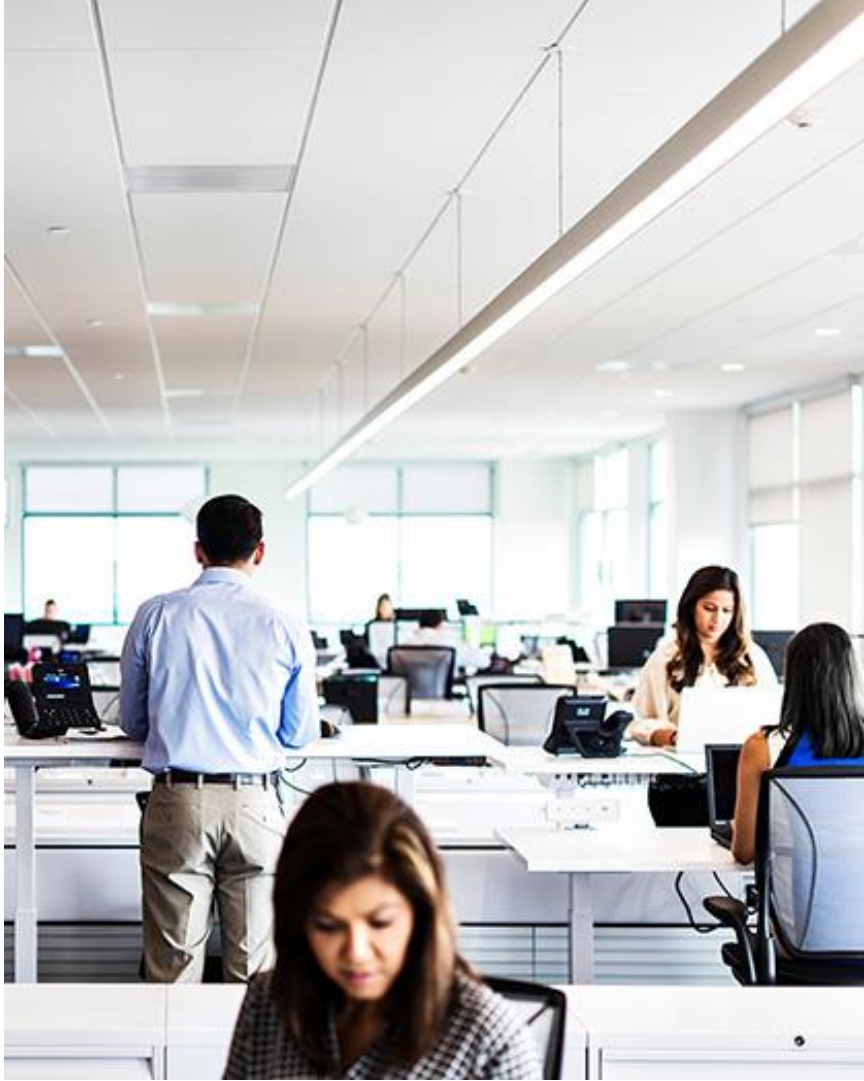
- Le temps (utilisation d'un serv. NTP)
- La précision du temps (à la ms près)
- Le fuseau horaire (en Europe GMT+1)
- La capacité de stockage

Mettre en relation les événements des logs avec les événements externes obtenus grâce aux relations humaines.

Niveau 5

Un système informatique n'a de valeur qu'en fonction du service rendu aux utilisateurs. Il faut donc les considérer avec un maximum d'attention.

- Liste des utilisateurs (un annuaire)
- Liste des postes clients et équipements dédiés aux utilisateurs
- Interviews avec des utilisateurs types et des responsables de groupes



5 sujets d’audit typiques

Sur une infrastructure d’entreprise, on peut avoir 5 sujets fréquents:

1) Le câblage et ce qui concerne la couche 1 du modèle OSI
2) Les VLANs, les liaisons inter-équipement et ce qui concerne la couche 2 du modèle OSI / SD ACCESS
3) Les réseaux IP, le routage et ce qui concerne la couche 3 du modèle OSI / SD-WAN
4) Le WiFi (WLAN)
5) La Sécurité

Câblage et couche 1 OSI

Collectez :

- Les plans d'architecte du bâtiment
- Les plans du câblage électrique
- Les plans du câblage réseau

Repérages :

- Localisations et identifier les lieux d'intervention
- Racks et LTE 'Locaux Techniques d'Etage'
- Les salles serveurs ou Datacenter
- Points de raccordement (prises, patch-panels, interfaces)

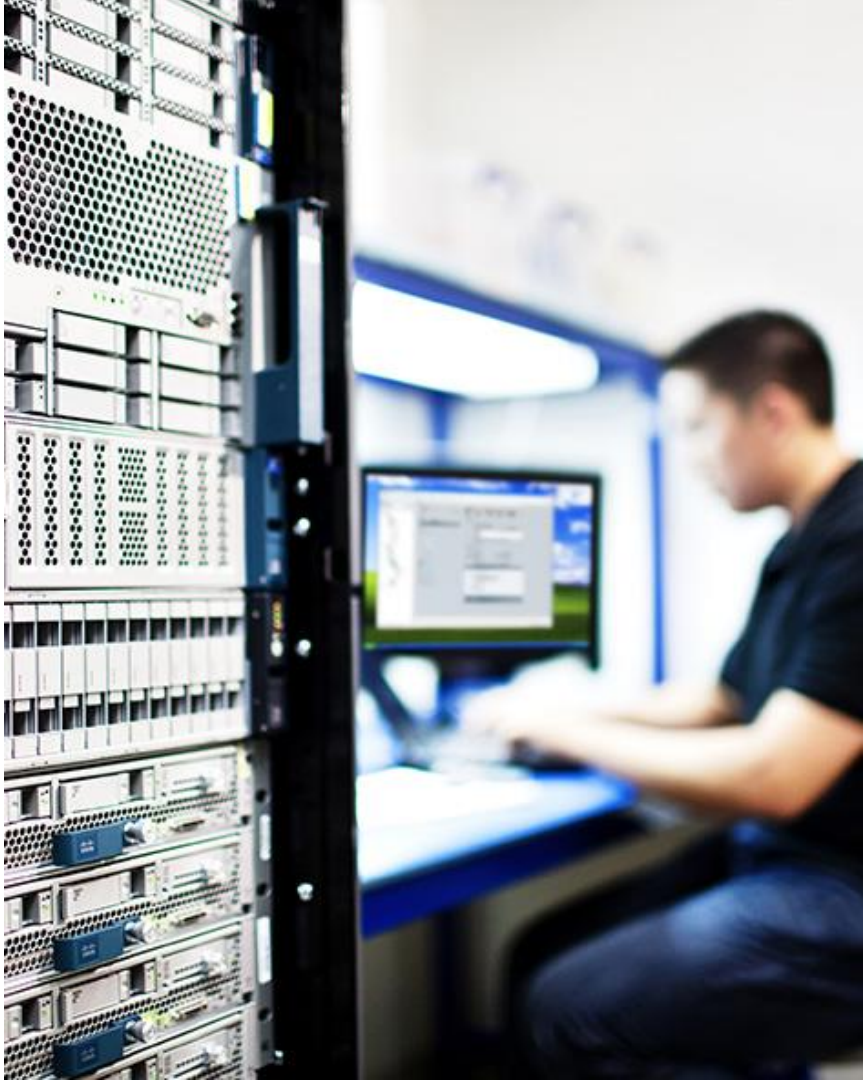
VLANs, liaisons, couche 2 OSI / SD ACCESS

Collectez :

- Les plans du câblage réseau
- La liste des VLANs si elle existe
- Les configurations de couche 2 -Ex: switchs, trunk sur FW ou routeurs-
- Recherchez les équipements inconnus !
- Pensez aux services réseaux -Ex: DHCP, ISE-

Repérages :

- Les étiquettes s'il y en a
- Utilisez CDP ou LLDP pour cartographier le réseau



Réseaux IP, routage, couche 3 OSI / SD-WAN

Collectez :

- Les plans et l'information de niveau 2
- Les plans de routage, les liste des réseaux
- Les configurations des routeurs
- Etudiez la configuration des services réseaux -Ex: DNS, DHCP, RADIUS, LDAP, AD- si nécessaire

Repérages :

- Cartographiez le réseau avec les tables de routage
- Listez les services réseau
- Lister les connexions opérateur

WiFi (1)

Un audit WiFi est comme un audit aux Niveaux 2 et 3 du modèle OSI.

- Il y a une problématique d'accès et une problématique d'adressage.
- Le site peut être audité pour les différents types de WiFi présents : 802.11a,b,g,n,ac par exemple
- Il faut aussi établir la liste des SSIDs et des zones WiFi d’utilisation.

WiFi (2)

Dans une architecture WiFi un gros travail de positionnement du matériel est normalement réalisé avant l'installation.

Repérez le(s) document(s) de référence à ce sujet. Si le document existe, il y contient les références et la localisation des équipements.

WiFi (3)

Liste à établir, par AP :

- Numéro d'AP trouvé / bâtiment / étage
- Nom d'AP / type d'AP
- Mode de travail
- Canaux et puissance (dbm) 2.4ghz, 5.1ghz

Il peut y avoir des remarques sur des problèmes localisés.

Il faut établir aussi une liste des sources d’interférence.

WiFi (4)

Collectez :

- Connectivité (éventuellement présence dans un VLAN) et alimentation (POE ou classique)
- Localisation des contrôleurs WiFi
- Description des APs et des contrôleurs WiFi
- SSID spécifiques

Polling Question 3

Votre audit s'étale sur 1 mois. Quelle périodicité pour les réunions avec la MOA ?

1) 2 réunions par semaine
2) 1 réunion par semaine
3) 1 réunion toutes les 2 semaines
4) 1 réunion au début et à la fin

4. Relations humaines

Les relations humaines (1)

Sans qualité pour créer de bonnes relations humaines, il n'y a pas d'audit efficace.

Audit efficace : rapide et exhaustif.

La gestion des relations humaines en fonction des profils rencontrés et des situations est déterminante dans la facilité à obtenir des informations.

Un audit intervient surtout en période de changement quand les esprits ne sont pas nécessairement très constructifs.

Les relations humaines (2)

Pour vous, la pyramide hiérarchique est en quelque sorte inversée : Les gens qui vont vous apprendre le plus de chose sont ceux qui se situent en bas de l'échelle hiérarchique. Veuillez donc à engager le dialogue dès que possible.

Grâce à eux vous pouvez obtenir de manière informelle des infos comme :

- ✓ Problèmes récurrents sur des périmètres oubliés
- ✓ Infos sur la survenue d'événement perturbants
- ✓ Infos sur les blocages humains (pouvant expliquer des problèmes)
- ✓ Infos sur des détails techniques d'importance, plans, etc.

Les relations humaines (3)

Il faut documenter (et donc rechercher *ceux qui savent*) les installations que « tout le monde à oublié » :

- Badgeuses
- Alarmes
- PCs/serveurs « historiques »
- Modem ! PABX !
- Imprimantes spéciales
- Protocoles fossiles -Ex : IPX, X25, XoT, LU6.2, Appletalk- (Oldies)

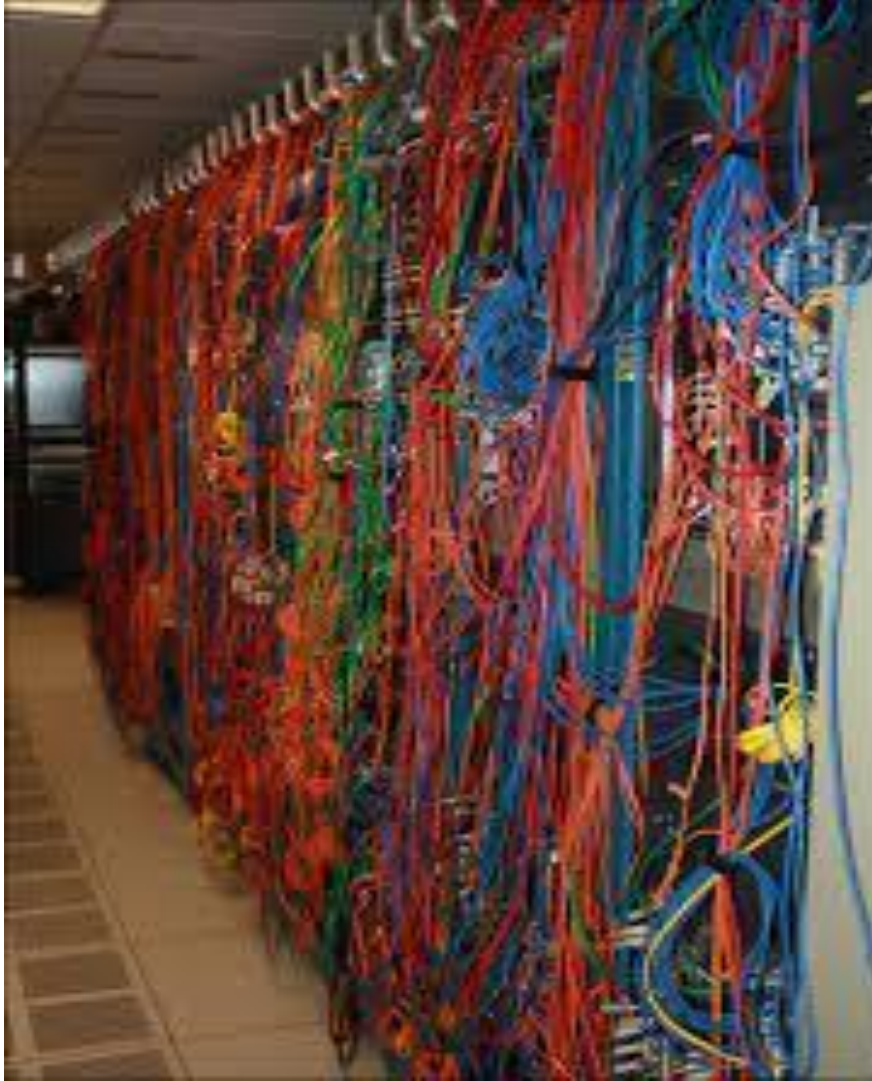
Les relations humaines (4)

Quand l'infrastructure sur un bâtiment commence à dépasser la cinquantaine de poste utilisateurs, soyez très attentif au câblage et à l'électricité.

Couche 1 OSI

- Câblage
- Etiquettes
- Alimentation électrique (donc mise à la terre)

C'est une prise de conscience que vous devez amener dans la structure !



Les relations humaines (5)

Quand les relations sont difficiles, nous allons voir différentes possibilités et des solutions, mais tout d'abord n'oubliez pas que vous avez une carte en main qui est importante : vous avez la connaissance et vos interlocuteurs vous voient comme un expert.

Les relations humaines (6)

Les limites : à découvrir avant d'accepter la mission d'audit :

- Le donneur d'ordre est t-il vraiment convaincu par le fait de faire un audit ?
- Le donneur d'ordre a t-il l'organisation propre à ce que l'audit lui soit utile ?
- Est-ce que vos méthodes sont compatibles avec celles de votre donneur d'ordre ?

Les relations humaines (7)

Partez sur un audit avec la conviction que l'on ne vous a pas tout dit sur la situation de l'entreprise :

- Y a t-il un problème particulier dans un service, avec des ou une personne spécifiquement ?
- L'entreprise a t'elle des projets quelle ne souhaite pas dévoiler, mais qui créent des tensions ?
- Des employés ont-ils des attentes particulières (déraisonnables ?) sur le résultat de votre audit ?

Les relations humaines (8)

Créez tant que faire se peu une relation intime avec les personnes que vous interrogez. Intime, mais professionnelle:

- Votre expérience professionnelle doit vous permettre de comprendre les points difficiles du métier de l'autre.
- Votre expérience de la vie doit vous permettre de comprendre la situation personnelle de votre interlocuteur.

Les relations humaines (9)

Recherchez et liez des contacts amicaux avec un ou deux employés relativement anciens dans la structure. Instaurez absolument un échange tacite:

- Ils vous donnent de l'info, donnez leur de la formation sur votre expertise. Faites un transfert de compétence.
- En présentiel, ayez un budget « café » pour offrir des cafés, cela passe souvent bien, selon les cultures locales.
- En télétravail, ayez un très bon son. Donc un super micro haute qualité.

Les relations humaines (10)

Apprenez à gérer les crises :

- Les employés réfractaires à l'organisation. Soyez humble et dans le contrôle, montrez dès que possible votre compréhension du métier de l'autre (c'est ce qui manque).
- Les employés en opposition à leur hiérarchie (personne) ou collègues. Ne pas de jouer les justiciers ou au contraire le relais de la direction. Alliés possibles.
- Les employés en opposition avec vous. Soyez un expert et professionnel, mais ne vous laissez pas marcher sur les pieds. Jamais.

Les relations humaines (11)

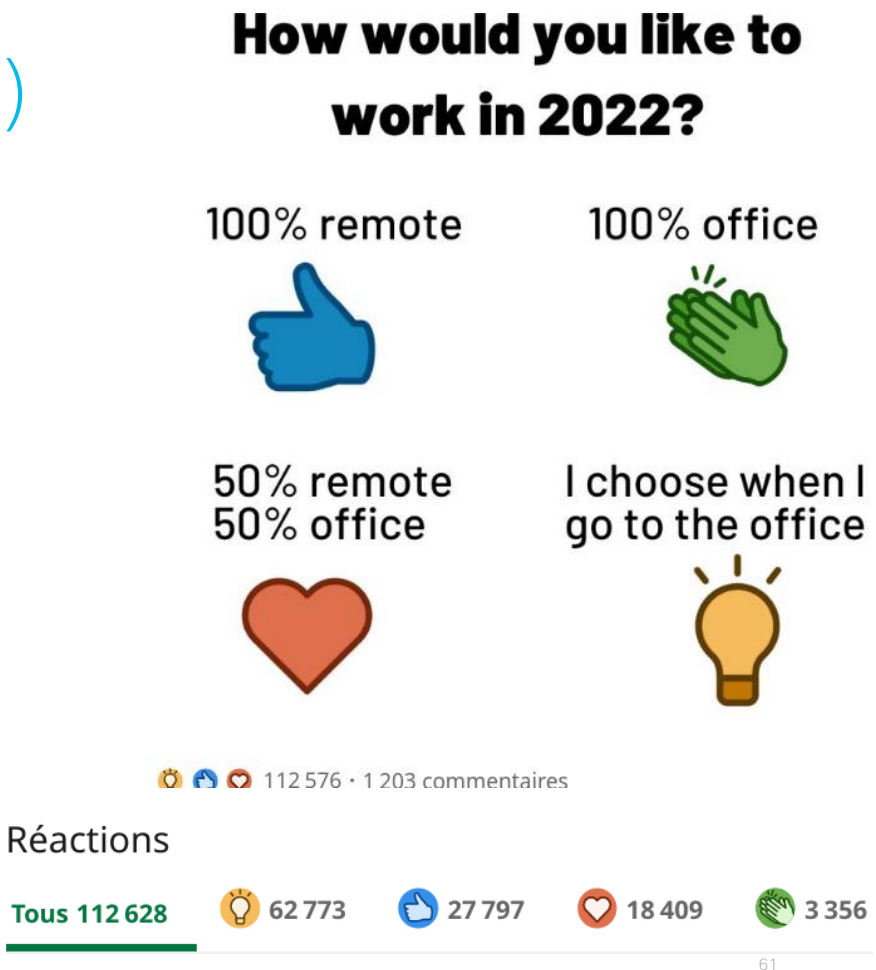
Formez vous aux relations humaines, cela s'apprend aussi :

- PNL
- Caractériologie
- Analyse transactionnelle
- Il existe différents systèmes qui vous donneront un référentiel pratique pour mieux comprendre les ressorts psychologiques de vos interlocuteurs. L'expérience de la vie fera le reste.

Les relations humaines (12)

L'apport du télétravail :

- Tous les avantages de la vidéoconférence : La communication non verbale !
- Oui il est possible des relations de confiance en vidéoconférence
- Ayez du matériel de très bonne qualité surtout au niveau sonore.



Polling Question 4

Qu’est ce qu’un réflectomètre mesure ?

1) L’écho
2) Les reflets dans la fibre
3) L’onde réfléchie
4) L’intelligence

5. Protocoles de l’information

SSH (rfc4253)

Maintenant utilisé partout pour la connexion à l'administration des machines. Il peut rester des machines en telnet (TCP port 23).

Vérifiez :

```
show version - > K9
show ip ssh - > SSH Enabled - version 2.0
hostname routeur1
ip domain masociete
crypto key generate rsa general-keys modulus 1024
ip ssh version 2
aaa new-model
aaa authentication login default local
username admin secret Mot2Passe
line vty 0 15
login local
transport input ssh
```

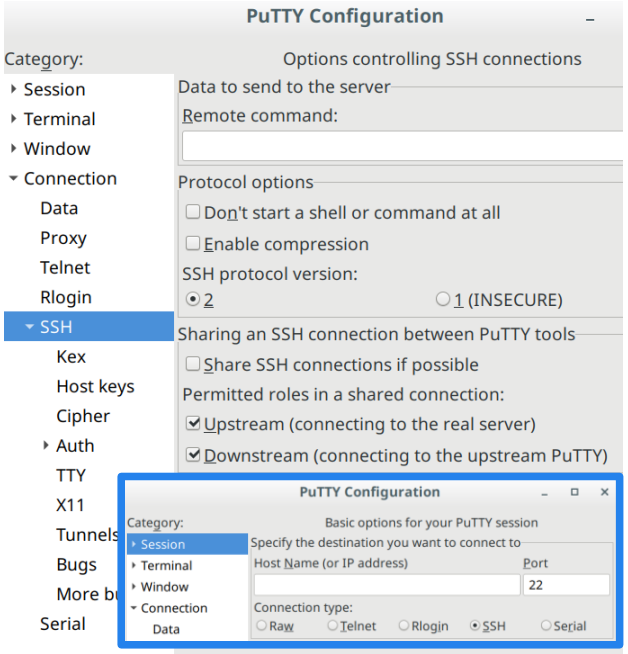
Côté MOA: pensez à changer ces mots de passe juste après l'audit ! Ou utilisez des mots de passe temporaires.

SSH PuTTY (1)

Un bon moyen de tester un accès SSH c'est d'utiliser PuTTY.

Notez que vous pouvez aussi tester à partir d'un autre routeur Cisco simplement avec la commande :

```
ssh 192.168.0.1
```



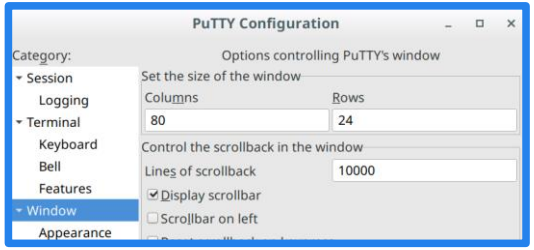
Côté MOA: exigez l'utilisation de postes clients Linux avec bcp moins de risque !

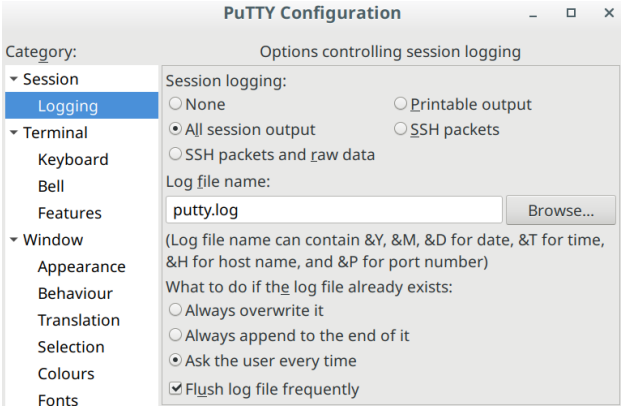
SSH PuTTY (2)

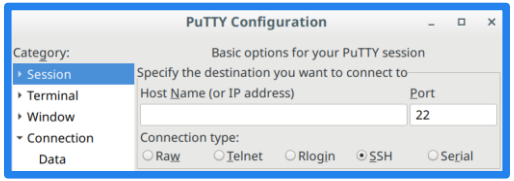
Utilisez une longueur maximale de scrollback, ayez un fichier de log.

Si possible rendre la longueur de terminal = 0 sur l'équipement

```
terminal length 0
```





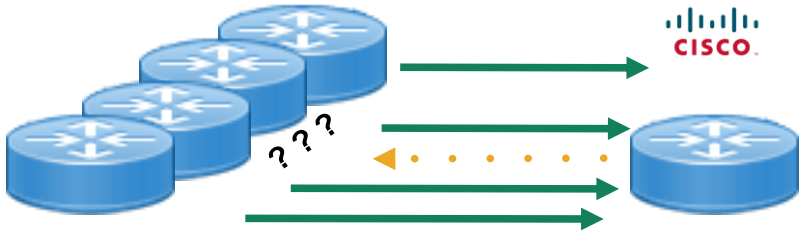


Côté MOA: pensez à demander et sauvegarder une copie des fichiers de log !

CDP (1)

CDP : Cisco Discovery Protocol

Pas de RFC : pas de norme, mais se retrouve chez d'autres éditeurs/constructeurs -Ex : HPE, VMware-.




```
IEEE 802.3 Ethernet
    Destination: CDP/VTP (01:00:0c:cc:cc:cc)
    Source: Cisco_12:34:56 (00:07:85:12:34:56)
    Length: 372
```

Côté MOA: pensez à vérifier que des trames CDP ne sortent pas de votre réseau !

CDP (2)

Côté MOA: Voici toutes les informations communiquées.

Trame CDP

```
Cisco Discovery Protocol
    Version: 2
    TTL: 180 seconds
    Checksum: 0xc2c3
    Device ID: LAN354802
        Type: Device ID (0x0001)
        Length: 13
        Device ID: LAN354802
    Addresses
        Type: Addresses (0x0002)
        Length: 17
        Number of addresses: 1
        IP address: 192.168.2.62
            Protocol type: NLPID
            Protocol length: 1
            Protocol: IP
            Address length: 4
            IP address: 192.168.2.62
```

```
Port ID: FastEthernet0/7
    Type: Port ID (0x0003)
    Length: 19
    Sent through Interface: FastEthernet0/7
Capabilities
    Type: Capabilities (0x0004)
    Length: 8
    Capabilities: 0x0000000a
        .... .... .... .... .... .... .... ...0 = Not a Router
        .... .... .... .... .... .... .... ..1. = Is  a Transparent Bridge
        .... .... .... .... .... .... .... .0.. = Not a Source Route Bridge
        .... .... .... .... .... .... .... 1... = Is  a Switch
        .... .... .... .... .... .... ...0 .... = Not a Host
        .... .... .... .... .... .... ..0. .... = Not IGMP capable
        .... .... .... .... .... .... .0.. .... = Not a Repeater
```

CDP (3)

Trame CDP (suite)

```
    Software Version
        Type: Software version (0x0005)
        Length: 225
        Software Version: Cisco Internetwork Operating System Software
                          IOS (tm) C3500XL Software (C3500XL-C3H2S-M), Version 12.0(5)WC8, RELEASE
SOFTWARE (fc1)
                          Copyright (c) 1986-2003 by cisco Systems, Inc.
                          Compiled Thu 19-Jun-03 12:37 by antonino
    Platform: cisco WS-C3548-XL
        Type: Platform (0x0006)
        Length: 21
        Platform: cisco WS-C3548-XL
    Protocol Hello: Cluster Management
        Type: Protocol Hello (0x0008)
        Length: 36
        OUI: 0x00000C (Cisco)
        Protocol ID: 0x0112 (Cluster Management)
        Cluster Master IP: 0.0.0.0
        UNKNOWN (IP?): 0xFFFFFFFF (255.255.255.255)
        Version?: 0x01
        Sub Version?: 0x01
        Status?: 0x21
        UNKNOWN: 0xFF
        Cluster Commander MAC: 00:00:00:00:00:00
        Switch's MAC: 00:07:85:12:34:56
        UNKNOWN: 0xFF
        Management VLAN: 100
```

CDP (4)

Trame CDP

(suite – fin)

```
VTP Management Domain: mynet
    Type: VTP Management Domain (0x0009)
    Length: 10
    VTP Management Domain: mynet
Native VLAN: 105
    Type: Native VLAN (0x000a)
    Length: 6
    Native VLAN: 105
Duplex: Full
    Type: Duplex (0x000b)
    Length: 5
    Duplex: Full
```

LLDP
(Link Layer Discovery Protocol)

Côté MOA: LLDP peut être aussi problématique que CDP !

Voir : https://wiki.wireshark.org/LLDP

~~RFC~~ . IEEE 802.1AB et IEEE 802.3 section 6 clause 79

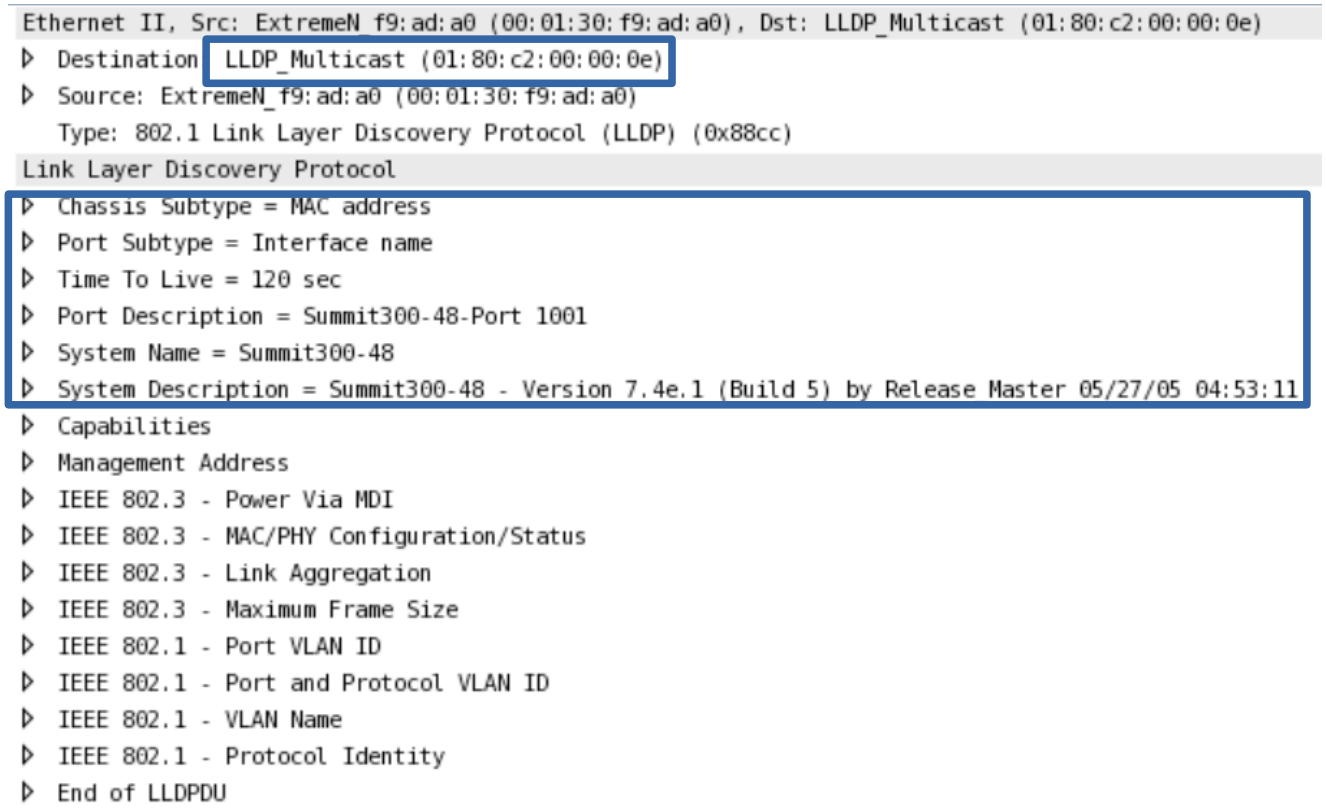
Couche 2 modèle OSI

LLDP-MED

LLDP-MED : Link Layer Discovery Protocol-Media Endpoint Devices

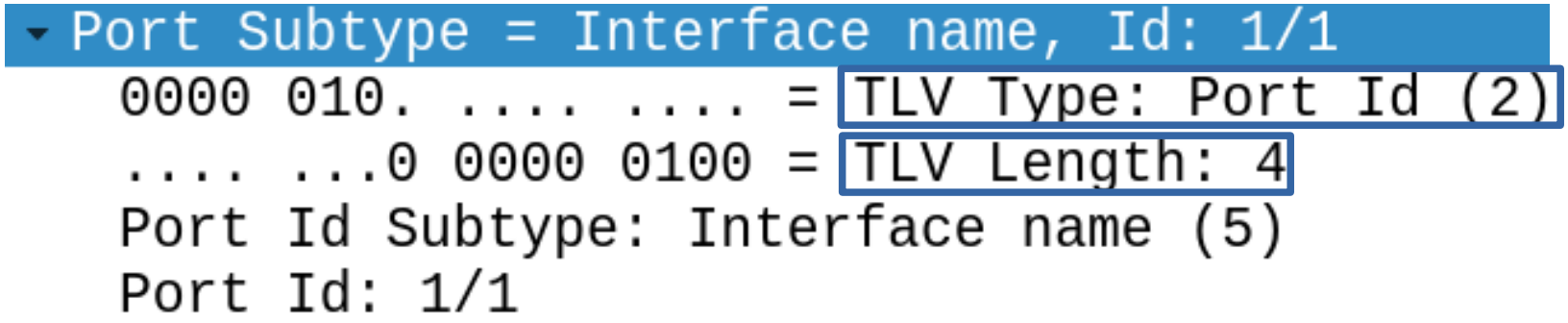
Extension du LLDP - Couche 2 modèle OSI

LLDP



LLDP

Avec LLDP, on a un concept de normalisation de l'information : TLV : (Type, Longueur, valeur)



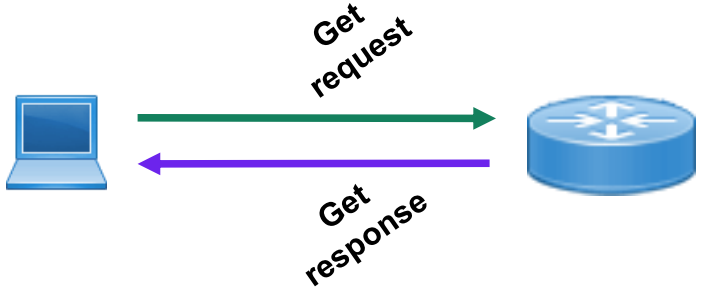
SNMP

Côté MOA: préférez snmpv3 plus sécurisé !

Simple Network Management Protocol RFC 1157 (rfc historique).

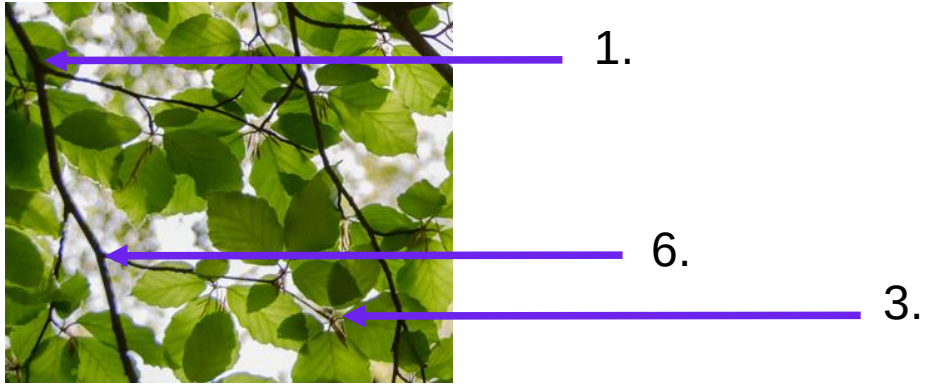
Il existe plusieurs versions, mais la v3 est préférable pour des raisons de sécurité.

UDP 161 & 162 voir Wikipédia : https://fr.wikipedia.org/wiki/Simple_Network_Management_Protocol



SNMP

L’organisation des informations influe sur la façon dont l’équipement est interrogé ! Avec SNMP on a affaire à une organisation en arbre. Chaque feuille de l’arbre contient une information. Pour faire la requête il faut donner le chemin vers la feuille.



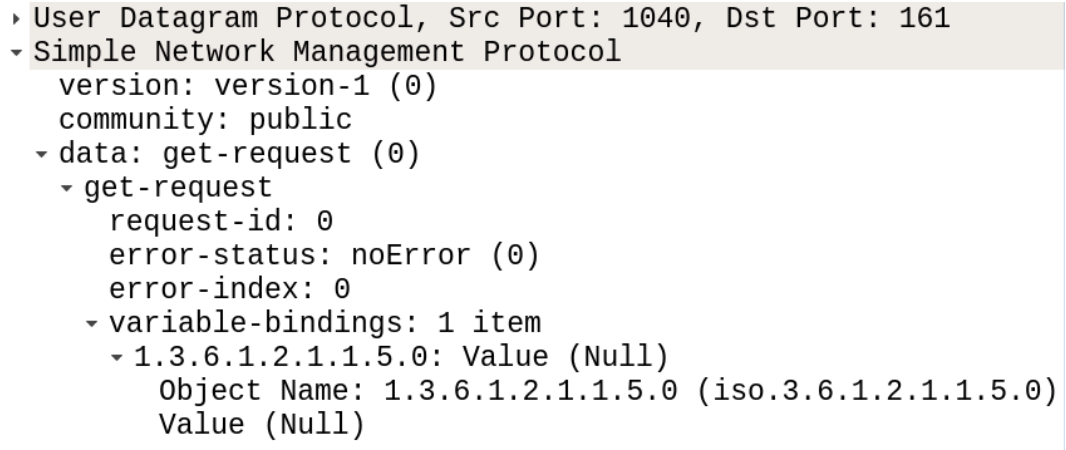
1 . 6 . 3

C’est la M.I.B.

(Management Information Base)

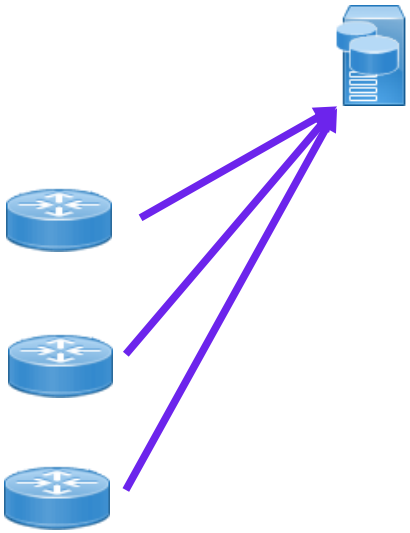
SNMP

Pour plus d'informations sur le protocole :
https://wiki.wireshark.org/SNMP



Les logs (Syslog)

RFC 5424



[Search] [txt|html|pdf|bibtex] [Tracker] [WG] [Email] [Diff1] [Diff2] [Nits]

From: draft-ietf-syslog-protocol-23 — Proposed Standard
Errata exist

Network Working Group — R. Gerhards
Request for Comments: 5424 — Adiscon GmbH
Obsoletes: 3164 — March 2009
Category: Standards Track

The Syslog Protocol

Status of This Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

CDP

Autorisation globale :

```
cdp run
cdp advertise-v2
cdp timer seconds
cdp holdtime seconds
```

Vérification :

```
clear cdp counters
clear cdp table
show cdp
show cdp entry device-name
show cdp interface [type number]
show cdp neighbors detail
show cdp traffic
```

LLDP

Autorisation globale :

```
lldp run
lldp holdtime seconds
lldp reinit seconds
lldp timer seconds

lldp receive
Lldp transmit
```

Vérification :

```
clear lldp counters
clear lldp table
show lldp
show lldp entry device-name
show lldp interface [type number]
show lldp neighbors detail
show lldp traffic
```

SNMP

Autorisation globale :

```
snmp-server community
pourtous RO

snmp-server community pourmoi
RW
```

Vérification :

show snmp

SYSLOG

Autorisation globale :

```
logging 192.168.1.100
logging on
```

Vérification :

show logging

Polling Question 5

Qu’est ce qu’un modèle en «V» ?

1) Le modèle de la victoire
2) Le modèle au 5 phases
3) On dit le cycle en « V »
4) C’est ISO 9001

6. Projet d’audit

Le projet d’audit type

Découpage en 6 phases :

0) Avant vente

1) Préparation

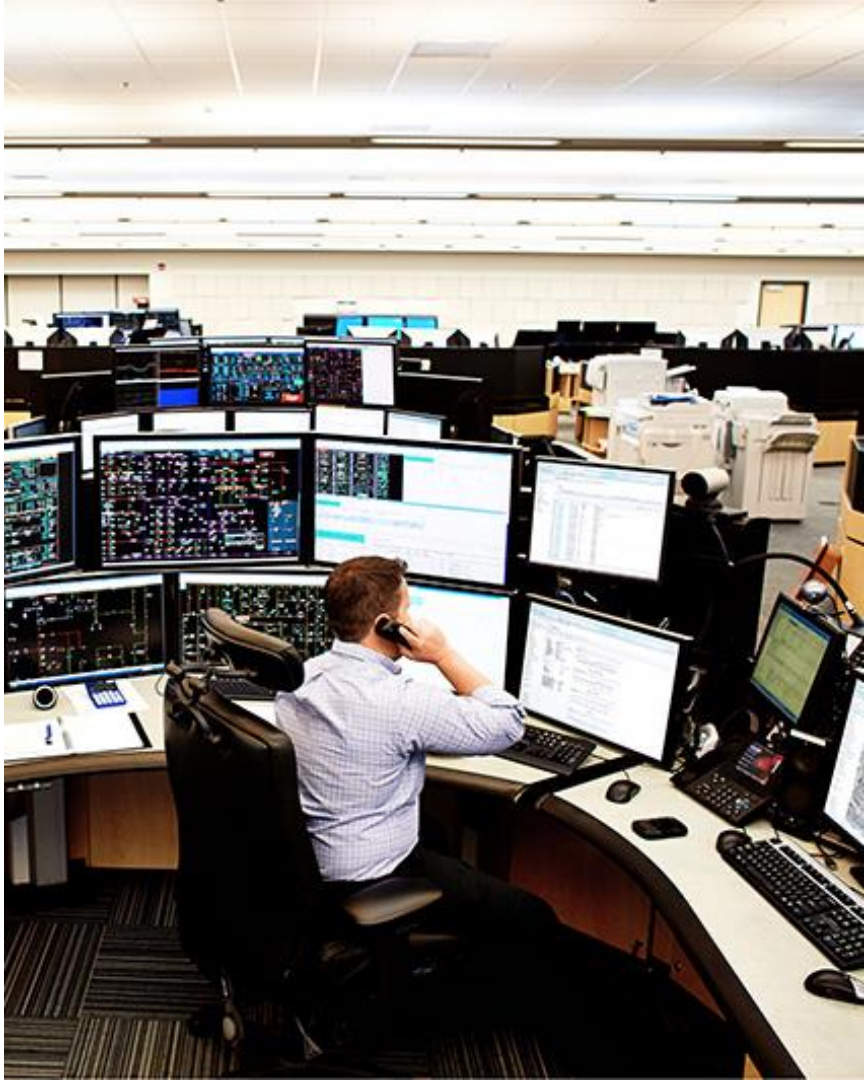
2) Réunion préparatoire

3) Recueil

4) Finalisation d’audit

5) Analyse

6) Présentation finale des résultats



Avant vente

C'est la phase de l'entretien d'avant vente pour voir le type d'audit demandé par la MOA et les particularités techniques et organisationnelles.

Le résultat de cet entretient est consigné dans une note : **REN (Rapport d'entretien)**

(Les Documents vus ici sont différents des livrables vu précédemment. Ils sont donnés à titre indicatif)

Documents:

REN (Rapport d'entretien) *base documentaire en phase 0*

Préparation

Le chef de projet MOE prépare (ou s'assure) que toutes les ressources nécessaires pour les experts sont présentes :

- matériel
- formation de l’équipe
- logiciel
- documentation
- Planning envisagé

Documents:

LDC (Liste des contacts) *base documentaire en phase 1*

Réunion préparatoire

Le chef de projet MOE qui va chez la MOA pour se mettre d'accord sur l'organisation et mettre en place les moyens matériels, logiciels, les autorisations et les procédures nécessaire pour que l'expert puisse intervenir à distance.

La réunion est prévue pour s'assurer que tout est bien compris, lors de cette réunion, doit être complété un document de préparation d'audit (DPA).

Documents:

DPA (Document de Préparation d'Audit) *base documentaire en phase 2*.

- Listes des matériel, logiciels et ressources nécessaire
- But de l'audit et feuille de résultat de l'audit
- Liste exhaustive des points à auditer (matériel, logiciel, système, réseau etc.)

Recueil

Lors de ces recueils d'information, une liste précise des informations recueillies devra être établie. Les informations sensibles appartenant à l'organisation de la MOA ne pourront pas être "sorties" de l'organisation.

La MOA s'engage à fournir à notre équipe des mots de passe qui doivent être révoqués juste après l'audit.

Documents:

Les recueils *base documentaire en phase 3*

Finalisation d’audit

Une fois la phase de recueil terminée, le document de préparation d'audit est complété pour montrer les points effectivement réalisés.

Documents:

DPA *base documentaire en phase 4*

Analyse

La phase d'analyse va permettre de réaliser un document d'analyse et/ou de synthèse d'audit qui sera versé dans la base de connaissance **AA(Analyse d'Audit)**.

Documents:

AA (Analyse d'Audit) *base documentaire en phase 5.*

Ce document va faire une synthèse de tous les points découverts dans l'audit et qui méritent une mise en lumière ou une explication.

Présentation finale des résultats

Une synthèse des documents ER/ DPA et **AA** doit être réalisée par le chef de projet et présentée au client. La synthèse comporte tous les documents produits pour le client.

Suite à cette présentation, un document de recette doit être signé.

Documents:

Recette *base documentaire en phase 6.*

Ce document récapitule le sujet de l'audit et permet de valider par la MOA le travail de la MOE.

Arborescence typique

0_Avant-vente

1_Préparation

2_Réunion_Préparatoire

3_Recueil

4_Finalisation_Audit

5_Analyse

6_Recette_Final

9_Archives

Avez-vous encore des questions ?
Utilisez le panneau « Q&R »

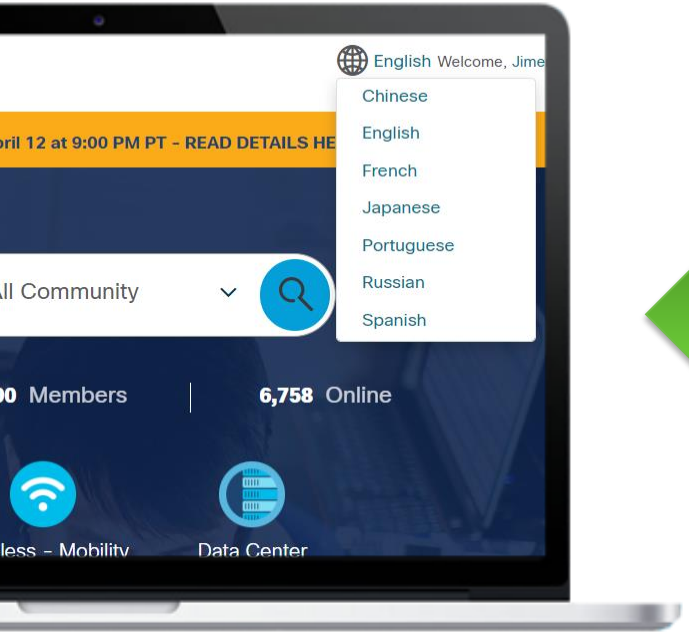
Forum Ask Me Anything

Retrouvez notre expert sur la page de Discussion

Toutes les nouvelles questions sur le sujet de ce webinaire seront répondues par la suite jusqu'à la semaine prochaine: 26 Nov.

Postez une question ici
https://bit.ly/AMAd-nov21

Où que vous soyez restez connecté…



- Facebook CiscoSupportCommunity
- Twitter @cisco_support
- YouTube CiscoSupportChannel
- LinkedIn Cisco Community
- Instagram CiscoSupportCommunity


Avez-vous des commentaires ?
Répondez à notre enquête !

The bridge to possible