1002

CONCOURS ~~EXTERNE~~ - INTERNE*

CONCOURS ~~DE~~ INTERNE DE TSIC CN

ÉPREUVE ~~DE~~ ECRITE D'ADMISSIBILITÉ

Solutions logicielles et systèmes d'information

*Rayez la mention inutile :

13/20

N.B. Il est interdit aux candidats de signer leur composition ou d'y mettre un signe quelconque pouvant indiquer la provenance de la copie.

IMPRIMERIE NATIONALE 135 011

NOMBRE D'INTERCALAIRES : 1

1) Pour sécuriser une flotte de téléphones mobiles, la DSI doit pouvoir :
- prévoir un système d'authentification (mot de passe, biométrique, token RSA etc)
- chiffrer les données locales
- chiffrer le traffic radio
- prévoir un système de suppression des données à distance en cas de vol ou de perte
- déployer un logiciel de protection contre les logiciels malveillants et au besoin interdire l'installation d'applications tierces ou non-autorisées par l'utilisateur dans le cas d'un "smartphone"

2) Une Unité Organisationnelle ou OU est un élément logique de classement et d'adressage au sein d'un annuaire de type Active Directory ou LDAP.

3) —

4) Après identification, deux modes d'authentification courants sont
- l'authentification par mot de passe
- l'authentification biométrique

5) Le terme anglosaxon "Cloud Computing" définit les technologies permettant de déporter les usages (traitement et/ou stockage) d'un appareil connecté vers des ressources distantes via le réseau.
Un exemple omniprésent est Amazon S3, qui permet d'effectuer ces deux usages via une API

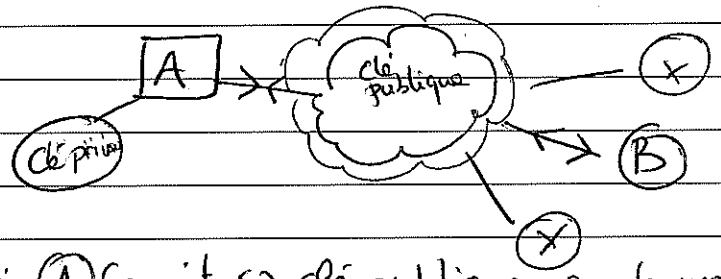
6) Le protocole standard d'administration des réseaux est LDAP (Lightweight Directory Access Protocol)

7) —

8) Un serveur proxy ou "serveur de rebond" est un équipement réseau dont le rôle est de relayer des requêtes ou de les bloquer.

9) Dans un système de chiffrement asymétrique, une "clé publique" ~~est un algorithme de chiffrement [illegible] correspondante~~ sert à chiffrer des données que seules les personnes munies de la "clé privée" peuvent déchiffrer.

Dans l'exemple traditionnel d'échange entre deux personnes "A" et "B":



Ici, (A) fournit sa clé publique sur le web, elle ne servira qu'à chiffrer le message allant de (B) vers (A). Toute personne x ou y n'ayant que la "clé publique" ne pourra pas lire la communication, seul le possesseur de la "clé privée" peut le faire.
En faisant l'opération inverse, les deux personnes (A) et (B) peuvent s'échanger une "clé secrète" et continuer leur ~~[illegible]~~ échange via un système de chiffrement symétrique, moins coûteux.

10) Un serveur DNS (Domain Name Server) étant un annuaire permettant de faire un lien entre un nom de domaine et une adresse IP, la conséquence immédiate d'une panne DNS est que la résolution des noms de domaine ne pourra plus se faire. Ainsi, l'adresse www.linux.org sera inaccessible pour l'utilisateur alors que le serveur distant est bien en ligne.
Il restera d'ailleurs encore accessible si l'utilisateur essayera de contacter directement son IP (ping, netstat ou en saisissant l'IP dans la barre d'URL du navigateur dans le cas de cet exemple)

Cas pratiques => voir intercalaires sup

INTERCALAIRE N° 1

Cas Pratique

1) Les différentes solutions sont

- OSD, qui permet de provoquer une mise à jour de l'OS via Windows Update (MS ou WSUS)
L'avantage est que la mise à jour via le réseau est paramétrable dans le temps pour s'assurer que l'utilisateur donne son accord et puisse s'y préparer.

- WDS qui permet au contraire de déployer une image de Windows 10.
L'avantage est une granularité plus fine pour définir les applications qui seront migrées, et la possibilité de gérer les ressources réseau allouées pour charger l'image sur le poste distant.

Ces deux méthodes sont utilisables via les ~~outils~~ outils de Microsoft MDT 2013 ou ConfigMgr2012, intégrés dans le Windows Assessment and Deployment Kit (ADK)

Enfin, il est possible de migrer les postes au fur et à mesure de leur remplacement.

J'opterai pour la solution ConfigMgr2012 + WDS, qui donne un plus grand contrôle et surtout qui correspond à l'approche que je suggère en effectuant la migration par paliers (mise à jour fractionnée).
Mode opératoire :
Pour un parc moyen/petit de 200 postes, il conviendra dans un premier temps d'effectuer un recueil des besoins, par une analyse de l'organigramme et en effectuant un inventaire complet matériel et applicatif.
Les éventuels problèmes de compatibilité devront être anticipés en amont.
Les utilisateurs seront également sollicités.
Il faudra ensuite prioriser les services, les éléments névralgiques seront migrés en dernier (RH, FINANCIERS, SECURITÉ) afin de bénéficier des retours des migrations précédentes.

Une phase de test sera entreprise, normalement sur des postes non critiques, au sein de la DSI. Une fois cette phase achevée, un calendrier sera établi et communiqué à l'ensemble de l'organisme.

Les premières mises à jour seront accompagnées de PROCEDURES établies au préalable pour répondre aux questions évidentes (changements de l'interface, termes modifiés, etc)

Les premiers retours du service pilote alimenteront une base de connaissances qui servira au Helpdesk ainsi qu'aux autres utilisateurs.

Le déploiement s'achèvera par les postes critiques cités plus haut (+éventuels VIP pour un suivi personnalisé)

Si l'établissement dispose d'un budget et/ou d'un service formation, il faudra prévoir des dispositions si des applications précises doivent être imposées (Navigateur EDGE ou autre)

Une assistance téléphonique ou via un portail INTRANET peut être envisagée.

Dans le cas des applications non conformes avec Windows 10, la solution sécurisée sera, au choix :
- Une solution de virtualisation, avec exécution de l'application dans un environnement "sandboxé"

- Déporter les applications posant un problème sur des ressources cloisonnées distantes via TSE

(25) (2)

Les logiciels libres à mettre en œuvre sont ceux qui ont le statut "R" c'est à dire recommandés.
Ils doivent émaner d'une communauté active et permettre l'interopérabilité des données (format ouvert)
Les plus utiles à l'administration en général sont ceux du secteur SÉCURITÉ (Keepass, éventuellement Veracrypt), les logiciels bureautiques (messagerie Thunderbird, LibreOffice) catégorie Consultation & édition de documents.
D'autres utilitaires devront s'y ajouter au besoin (compression/décompression, éditeur de texte, navigateur libre)

Ces installations devront s'accompagner d'une documentation en Français, de ressources didactiques (didacticiels), d'une assistance sur place ou d'une répartition de l'aide en fonction des ressources humaines (désignation de correspondants informatiques dans chaque service en cas de manque de personnel / budget)

Un exemple utile de migration réussie pourra servir de modèle. Ainsi, le personnel de la gendarmerie nationale a dû passer de Windows XP à GNU/Linux. Pour faciliter la transition, la DSI a dans un premier temps habitué les utilisateurs à des applications libres existantes sur les deux OS pour permettre une transition fluide (passage de MSOffice à OpenOffice, Internet Explorer vers Mozilla firefox, windows Media Player vers VLC etc)