Auditer une infrastructure Microsoft

I. Introduction :

A. Où trouver ce document :

Ce document a été écrit par M. Guillaume MATHIEU. Une version électronique est disponible sur http://msreport.free.fr.
Une version au format PDF peut être téléchargée à l'adresse suivante :
http://msreport.free.fr/articles/Audit_infrastructure_Microsoft.pdf

B. Objectifs du document :

Ce document a pour but de vous permettre de déterminer les éléments qui doivent entrer dans le cadre d'un audit et les outils que l'on peut utiliser dans le cadre de cet audit (gratuit de préférence).
Il s'adresse de préférence à ces entreprises qui utilisent une architecture à base de serveurs Microsoft.

II. Audit de l'infrastructure informatique :

Les tâches ci-dessous doivent être effectuées dans l'ordre.

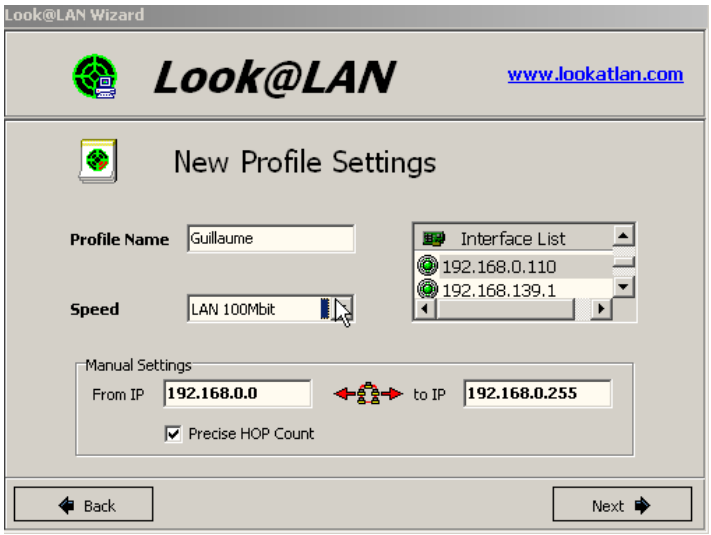
A. Audit du réseau:

L'audit du réseau est a effectué en premier. En effet nous allons pouvoir détecter tous les équipements réseaux (poste de travail, serveur, imprimante réseau, routeur…). Ces éléments feront ensuite l'objet d'une analyse plus approfondie.

Pour cela nous allons utiliser l'application : « Look@Lan que l'on peut télécharger à l'adresse suivante :

http://www.clubic.com/telecharger-fiche14179-look-lan-network-monitor.html

Cette application va nous permettre de générer la liste de toutes les machines sur votre réseau.



Pour cela, choisir d'exporter les résultats sous forme de fichier (dans notre cas Excel).

B. Audit de chaque serveur :

La seconde étape consiste à effectuer un audit de chaque machine que l'on a détecté à l'étape A.

Cet audit devra permettre d'évaluer les performances de la machine, de lister l'ensemble des logiciels et d'évaluer la configuration générale de la machine (mise à jour…).

1. Configurer l'audit des performances :

Sur les serveurs Windows, nous allons utiliser la console MMC « Performances ».

Aller dans le nœud « Journaux et alertes de Performances » puis sélectionner « *Créer nouveaux paramètres de journal* ».

Dans l'onglet Général, il faut ensuite sélectionner les compteurs suivants en cliquant sur « **Ajouter des compteurs** » :

- Sélectionner au niveau de l'objet de Performance « Processeur », le compteur « Temps processeurs »

- Sélectionner au niveau de l'objet de Performance « Disque physique », les compteurs de performance « Lecteur disque, octets par seconde » et Ecriture disque, octets par seconde ». Faire la même chose au niveau de l'onglet « Disque logique ».
- Sélectionner au niveau de l'objet de Performance « *Interface réseau* », les compteurs de performance « *Octets envoyés* » et « *Octets reçus* ». Refaire cette manipulation pour chaque carte réseau.

Configurer l'intervalle de temps sur 1 minute. Vous risquez sinon de créer une charge importante sur le serveur et d'avoir de produire des journaux de logs trop importants.
Il faut ensuite aller dans l'onglet « Fichiers journaux » et sélectionner le format « Fichier texte ». Les fichiers doivent être lisibles.
Aller ensuite dans l'onglet « *Planification* » et configurer l'audit de performances pour s'effectuer pendant 2 heures en heure pleine, c'est-à-dire entre 10 et 12h ou entre 15h et 17h.

2. Obtenir la liste des logiciels installés sur le serveur :

Pour cela utiliser les scripts du Script Center, téléchargeable à l'adresse suivante :

- http://www.microsoft.com/downloads/details.aspx?FamilyID=B4CB2678-DAFB-4E30-B2DA-B8814FE2DA5A&displaylang=en)

Vous pouvez aussi télécharger un de ces logiciels :

- http://www.microsoft.com/France/acheter/entreprises/logiciels/audit-outils.mspx

3. Evaluer la configuration générale de vos serveurs :

Vous pouvez utiliser le mpsreport de Microsoft afin de récupérer automatiquement un certain nombre d'informations sur votre serveur Microsoft :
http://www.microsoft.com/downloads/details.aspx?familyid=cebf3c7c-7ca5-408f-88b7-f9c79b7306c0&displaylang=en
Il existe différentes configurations du mpsreport selon le type de serveurs. Les archives générées par le mpsreport seront ensuite à analyser manuellement.

Pour les paramètres de sécurités de votre serveur Microsoft, utiliser le MBSA de Microsoft (actuellement en version 2.0.1) disponible à cette adresse :
http://www.microsoft.com/downloads/details.aspx?FamilyId=4B4ABA06-B5F9-4DAD-BE9D-7B51EC2E5AC9&displaylang=fr

C. Audit des logiciels :

Un inventaire de tous les logiciels sera réalisé à partir des informations obtenues dans la partie B. Cet inventaire permettra :

- De vérifier que l'on dispose de toutes les licences nécessaires.
- D'étudier les différents modes de licence possible (location, achat ou contrat avec l'éditeur).
- De déterminer les produits qui ne sont plus supportés par l'éditeur ou la date de fin de support des logiciels.
- De déterminer les mises à jour nécessaires pour chaque logiciel.
- D'évaluer le processus de téléchargement, test, validation, installation et de désinstallation des correctifs pour chaque logiciel.

D. Audit de l'infrastructure d'annuaire (Active Directory) :

La quatrième étape consiste à analyser :

- La structure logique (organisation) de votre l'annuaire.
- La structure physique (communication entre serveurs et entre clients et serveurs). C'est toute la partie sur les sites.
- La politique d'administration de votre annuaire (avec un audit des comptes avec des privilèges).
- Le fonctionnement général de votre annuaire.

Pour récupérer les informations générales au niveau d'Active Directory, vous pouvez utiliser les scripts du Script Center, téléchargeable à l'adresse suivante :
http://www.microsoft.com/downloads/details.aspx?FamilyID=B4CB2678-DAFB-4E30-B2DA-B8814FE2DA5A&displaylang=en

Pour analyser le fonctionnement d'Active Directory, télécharger le mpsreport DirSvc à l'adresse suivante :
http://www.microsoft.com/downloads/details.aspx?familyid=cebf3c7c-7ca5-408f-88b7-f9c79b7306c0&displaylang=en

Pour auditer les comptes avec des privilèges administratifs :

- Si vous êtes en mode natif 2003, télécharger le script Audit_AD2003.vbs sur http://msreport.free.fr
- Si vous êtes dans un autre mode de fonctionnement, télécharger le script Audit_AD.vbs sur http://msreport.free.fr.

E. Audit de l'infrastructure de messagerie :

La cinquième étape consiste à vérifier votre environnement de messagerie :

- Si vous utiliser Exchange, Microsoft met à disposition Exchange Best Practice Analyser Tools. Cet utilitaire permet d'analyser la configuration d'Exchange et émet des préconisations. Il est téléchargeable à l'adresse suivante : http://www.microsoft.com/technet/prodtechnol/exchange/downloads/2003/analyzers/sysreqs.mspx
- N'oublier pas aussi d'auditer le fonctionnement des services gérés par vos prestataires de service comme le filtrage anti-spam ou antivirus.

F. Audit connexions Internet :

La sixième étape consiste à vérifier le fonctionnement de votre serveur de messagerie et tout particulièrement :

- La synoptique (type) du trafic entrant et sortant via la liaison Internet.
- Les paramètres de sécurité pour le filtrage du trafic entrant et sortant.
- Le taux d'occupation de la liaison Internet.
- Le coût de la gestion de liaison Internet (location ligne, filtrage des accès, administration de la liaison Internet…).

Vous pouvez utiliser les rapports générés par Isa Server afin de retrouver ces informations.
L'utilitaire Isa Server Best Practice Analyser Tools permet de vérifier si la configuration du serveur Isa Server correspond aux normes établies par Microsoft.

Cet utilitaire est disponible à l'adresse suivant :
http://www.microsoft.com/downloads/details.aspx?FamilyId=D22EC2B9-4CD3-4BB6-91EC-0829E5F84063&displaylang=en

G. Audit de la gestion de vos fichiers :

La septième étape consiste à auditer la gestion de vos fichiers.

- Auditer la sécurité au niveau des emplacements de stockage des fichiers. Et lors du transfert des données.
- Auditer le fonctionnement de d'EFS ou IPSEC si vous avez implémenté ces protocoles.
- Vérifier la configuration de sécurité de votre autorité de certification.

H. Audit des Sauvegarde :

La huitième étape consiste à tester et valider les procédures de sauvegarde de tous les serveurs. Cette étape doit en autre vous permettre :

- De valider votre plan de reprise d'activité (en cas de désastre).
- Vérifier que le processus de sauvegarde/restauration est documenté et connu des équipes en charge.
- Déterminer comment et où sont stockés et gérés les médias de sauvegardes.

I. Audit de votre infrastructure de Patch Management :

La neuvième étape consiste à auditer votre infrastructure de Patch Management, c'est à dire l'ensemble des processus de gestion des mises à jour de vos logiciels et systèmes. Pour cela, vous pouvez télécharger un questionnaire. Il permettra d'évaluer sous forme de graphique radar votre besoin en Patch Management et votre architecture de Patch Management.
Il est téléchargeable à l'adresse suivante :
http://msreport.free.fr/articles/Audit_Patch_Management.xls

III. Audit de l'environnement informatique de l'entreprise:

Un audit de l'environnement informatique de l'entreprise doit être effectué afin de déterminer :

- Les personnes responsables de l'informatique en interne.
- La liste de tous les sous traitant et les modalités d'interventions de chaque sous traitant (niveau d'engagement (SLA), domaines d'intervention, horaires d'interventions, prix).
- La liste de toutes les tâches d'administration informatiques et leurs caractéristiques (la durée, la fréquence, les personnes en charge).
- Le besoin en formation du ou des personnes réalisant ces tâches.
- Le rôle et la criticité de l'environnement informatique pour l'entreprise (prix d'une heure d'arrêt de production).
- Le niveau moyen en informatique des utilisateurs.
- Les attentes des utilisateurs et du responsable de l'informatique au niveau de l'outil informatique.
- Le niveau de documentation actuelle de l'environnement informatique
- Le ou les personnes en charge de la gestion documentaire.
- Le niveau d'aménagements des locaux pour l'informatique.
- Si le matériel est assuré en cas de vols ou de catastrophes naturelles (incendie…).
- S'il existe un plan de reprise de l'activité.

Microsoft propose avec MOF un audit complet du processus de gestion de votre informatique.
Pour plus d'informations sur MOF :
http://technet.microsoft.com/fr-fr/library/bb232042.aspx