MASSyS

Méthode d'**A**udit

Simplifié du **Sy**stème de

Sauvegarde

Version 1.0 – Avril 2006

Master Management de la Sécurité des Systèmes Industriels et des Systèmes d'Information

Didier BERNAUDEAU Julien VEHENT

PRÉAMBULE

Dans le courant de l'année 2000, 49% des entreprises Européennes étaient incapables d'estimer la valeur de leurs données informatiques. En 2003, le *Clusif* publie des rapports éloquents : 84% des entreprises françaises ne possèdent aucun plan de secours pour maintenir leur activité en cas de perte des ressources informatiques. Un dernier chiffre, enfin, pour relier les précédents : 50% des entreprises qui subissent un sinistre important sans être équipées d'un système de sauvegarde pertinent meurent dans les deux ans qui suivent ledit sinistre.

Nous avons réalisé la première version de la méthode MASSyS dans le cadre du *Master « Sécurité des Systèmes Industriels et des Systèmes d'Information » à l'IRIAF* de Niort alors que nous travaillions à l'élaboration d'un forum sur la Gestion de Crise. Si l'objectif initial de notre travail était de mettre au point un guide des bonnes pratiques en matière de systèmes de sauvegarde, il nous est rapidement apparu qu'il n'existait aucune méthode permettant d'évaluer la qualité de ces derniers.
Lors de l'élaboration de MASSyS, nous nous sommes aperçus que ce manque de formalisation conduisait les responsables informatiques à évaluer très grossièrement leurs systèmes de sauvegarde. Souvent, cette évaluation est bien trop optimiste et les systèmes de sauvegardes concernés deviennent de vrais pièges à informations. Lorsqu'un incident survient (pas forcément un sinistre mais peut-être un vol ou une malveillance), les failles des systèmes de sauvegarde sont alors clairement identifiées, mais à quel prix ?

Toute entreprise aimerait pouvoir se remettre instantanément d'un incident sans aucune perte de données. Si cet objectif est, soyons réaliste, impossible à atteindre, il est toutefois possible de tendre vers un niveau d'efficacité satisfaisant.
C'est en partant de cette idée que nous avons mis au point la méthode MASSyS. Son but est de permettre aux responsables de la sécurité du système d'information de maîtriser leurs systèmes de sauvegarde, et par la même, de préserver les données sensibles de l'entreprise.
MASSyS se déroule en trois étapes :

1. Recensement des données et de leur criticité.
2. Évaluation de l'architecture de sauvegarde existante.
3. Intégrité des données et maîtrise de la restauration.

Chaque étape vous permet d'affiner la vision que vous avez de votre système de sauvegarde. Nous allons d'abord nous intéresser à ce qui doit être sauvegardé, puis nous regarderons comment fonctionne le système actuel ; enfin, nous mettrons en place une structure de contrôle continu des sauvegardes.

Comme toute méthode d'audit, la pertinence d'une étude basée sur MASSyS dépend grandement de l'implication des différents acteurs, à commencer par celle de l'auditeur. Dans l'idéal, cette étude doit être effectuée par un auditeur extérieur au système d'information. Dans le cas contraire, assurez-vous de disposer de l'aval total de votre direction pour effectuer une étude aussi complète et pertinente que possible.

Nous avons mis au point MASSyS en nous basant en partie sur les méthodes d'évaluation des risques industriels que sont MOSAR et AMDEC. Si vous connaissez ces méthodes, vous intégrerez rapidement les différents concepts exposés ici.
Une des caractéristiques de ces méthodes est qu'elles se sont construites sur de nombreuses années. À ce titre, MASSyS est une méthode très jeune qui à besoin d'évoluer et de grandir. N'hésitez pas à nous communiquer vos retours d'expériences, propositions d'améliorations ou autres suggestions par mail. Nous y prêterons la plus grande attention (nos contacts sont en fin de document).

Les Auteurs.

Table des matières

1. Recensement des données et de leur criticité

1.1 Le recensement des données

Dans cette première partie, nous allons recenser l'ensemble des données à sauvegarder. Pour cela, il faut non seulement recenser les parcs de stockage identifiés (*baies de disques, serveurs de fichiers, etc...*) mais également les données plus difficilement accessibles qui peuvent être stockées sur les postes clients ou sur les équipements du système d'information (*logs, configuration dynamique, etc..*).

Dans le cas des postes clients, nous nous heurtons à une première difficulté. Chaque utilisateur possède son arborescence propre et, dans bien des cas, ne va pas prendre conscience du risque lié à la perte de ces données. Afin de faciliter le travail de recensement et de sensibilisation, une méthode pertinente consiste à préparer un questionnaire (*typiquement, un formulaire PHP sur l'intranet*) et à demander à chacun de le remplir. Les outils SQL des bases de données vous permettront des recoupements faciles et une identification rapide des données critiques. Voici un exemple de questionnaire sur lequel vous pouvez vous baser :

Questionnaire utilisateur pour la politique de sauvegarde

Nom & Prénom :

Service :

Fonction :

Supérieur hiérarchique :

Type d'ordinateur : ❑ fixe ❑ portable

Utilisez-vous des partages réseau : ❑ oui ❑ non
Si oui, lesquels ? (lettre de lecteur ou nom) :
.....

Stockez-vous des données en local qui sont critiques pour votre travail ? ❑ oui ❑ non

Quel volume (en giga-octets) cela représente t-il ?
.....

Evaluez de 1 à 7 l'importance de ces données :
.....

1 & 2 = données d'information
3 & 4 = données importantes ou vitales pour le fonctionnement d'un service
5 & 6 = données importantes ou vitales pour le fonctionnement de plusieurs services
7 = données vitales pour le métier de l'entreprise

Il est possible qu'un utilisateur ai plusieurs groupes de données de gravités différentes. Adaptez cet exemple de formulaire pour qu'il traite ce cas.

Le questionnaire demande aux utilisateurs d'évaluer l'importance de leurs données (si elles existent). Certains utilisateurs vont remplir ce champ avec le maximum d'objectivité possible, d'autres non. Il vous appartient donc, en tant qu'auditeur, de vérifier ces informations afin de les rendre les plus objectives possible.

Vous allez récupérer une quantité importante d'informations (*dépendant de la taille de votre système*). Afin de traiter ces données le plus efficacement possible, nous allons les regrouper et créer ce que nous appellerons des « *Ensembles* ». Un Ensemble est constitué de données appartenant à différentes entités du système d'information ayant des traits communs. Ce peut être une gravité similaire dans une même zone géographique, le niveau hiérarchique de leurs propriétaires (*les chefs de services, les ingénieurs d'un département R&D, ...*), ou le type de sauvegarde que l'on va appliquer à l'Ensemble (*commerciaux nomades, partenaires, ...*).

1.2 Établissement de la gravité des Ensembles

Une fois vos Ensembles définis, nous allons nous intéresser à leurs volumes (*évalués en giga-octets*) et à la gravité liée à leurs perte.

Pour évaluer la gravité, de nombreuses méthodes sont possibles et vous préférerez certainement établir votre propre échelle. Dans la suite de la méthode, nous nous baserons sur une échelle de gravité allant de 1 à 7 comme le présente le tableau suivant:

Valeur de gravité	*Importance des données*
1	Faible: données d'informations (*inférieur*)
2	Faible: données d'informations (*supérieur*)
3	Moyenne : Ensemble de données essentielles au fonctionnement d'un service de l'entreprise (*inférieur*)
4	Moyenne : Ensemble de données essentielles au fonctionnement d'un service de l'entreprise (*supérieur*)
5	Importante : Ensemble de données essentielles au fonctionnement de plusieurs services de l'entreprise (*inférieur*)
6	Importante : Ensemble de données essentielles au fonctionnement de plusieurs services de l'entreprise (*supérieur*)
7	Vitale : Ensemble de données vitales pour le métier de l'entreprise

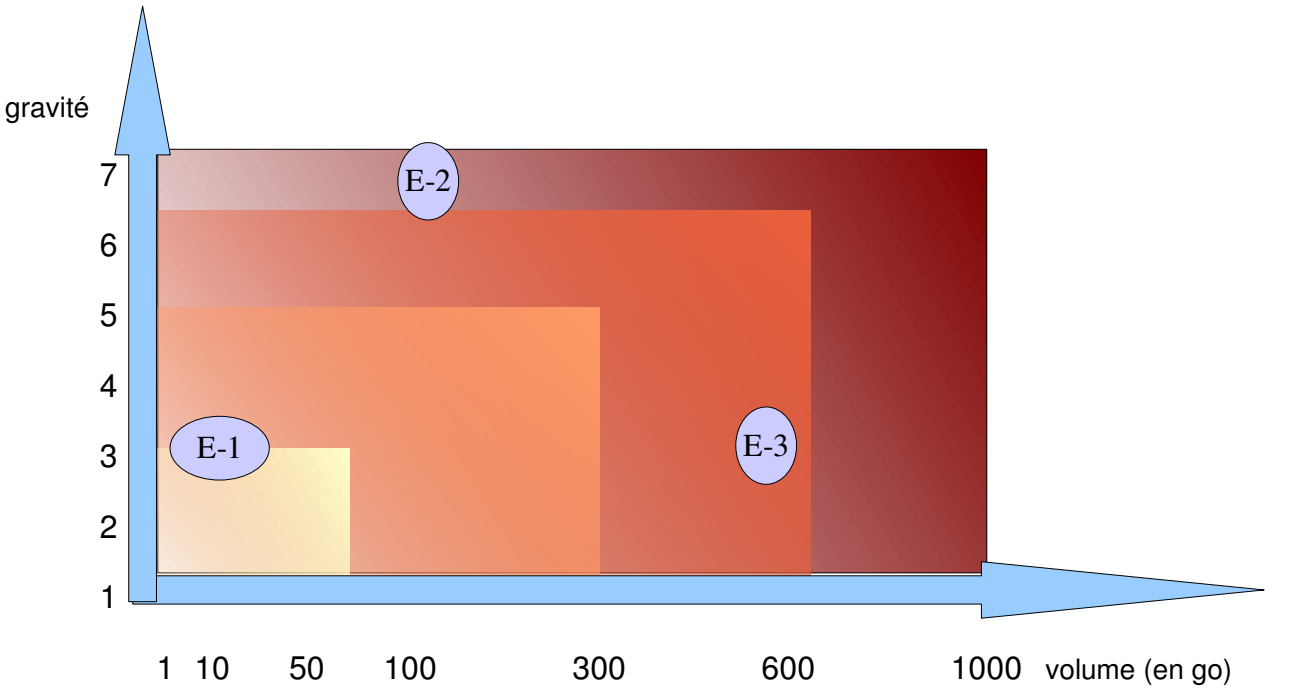
L'évaluation du volume est triviale : c'est la somme de toutes les données de l'Ensemble.

À chaque Ensemble correspondra donc un volume et une gravité ; nous allons utiliser ces informations dans la phase suivante.

1.3 Établissement de la Criticité

L'étape la plus délicate est l'établissement de la criticité des Ensembles de données. Il s'agit (*dans notre système*) d'une valeur indexée de 1 à 100 que nous comparerons plus tard avec un Indice de Sécurité.

Pour établir la criticité d'un Ensemble, placez-le sur la grille ci-dessous. Vous pouvez moduler la taille et la forme d'un Ensemble sur la grille en fonction de la fluctuation des données qui le composent.



criticité environ égale à 20	criticité comprise entre 25 et 40
criticité comprise entre 45 et 60	criticité supérieure à 60

Comme vous pouvez le voir, nous n'avons pas défini de calcul précis de la criticité. Il est en effet difficile, voire illusoire, de retirer une fonction générale de criticité à partir de la gravité et du volume. C'est pourquoi vous devez établir la criticité d'un Ensemble avec souplesse et réalisme.

Dans le graphique précédent, nous avons pris en exemple trois Ensembles, E-1, E-2 et E-3 :
E-1 est l'exemple d'un Ensemble de données à protéger sans pour autant déployer des moyens hors de propos. La perte de cet Ensemble peut s'avérer fortement gênante mais ne compromettra pas la survie de l'entreprise. On lui attribue un Indice de Criticité de 25.

Que dire de E-2 et E-3 ?

Le premier est un Ensemble fortement critique. Il représente des données touchant directement le métier de l'entreprise (*base de données des commandes en cours, fichier clients, etc...*). Il mérite donc un Indice de Criticité élevée : disons 65.

Le second est l'exemple même d'un Ensemble facilement identifiable, du fait de l'importance de son volume. On pourrait le comparer à une sauvegarde des données des postes clients. La gravité liée à sa perte peut sembler faible mais risque de très fortement perturber le fonctionnement de l'entreprise pendant une période de temps de plusieurs semaines. Mettons-lui un indice de Criticité de 52, il n'est pas aussi vital que peut l'être l'Ensemble E-2.

1.4 Globalisation

Répertoriez ces informations dans un tableau global :

Ensemble	***Description***	***Gravité***	***Volume (en go)***	***Criticité***
E-1	*Données d'exploitation de la plate-forme téléphonique*	3	~10	25
...	...	...	...	...

Vous avez ainsi une vision synthétique de votre système d'information à un instant « *t* ». Ces données sont variables, en particulier les volumes : veillez à ré-estimer ces derniers au moins chaque trimestre.Ce tableau global est l'élément final de la partie recensement. Archivez les informations relatives à sa constitution (*vous en aurez besoin pour le maintien de l'audit dans le temps*) et conservez uniquement ce tableau pour l'exploitation.
Maintenant que nous disposons d'informations précises concernant le système d'information, nous allons nous intéresser à l'architecture de sauvegarde existante.

2. Évaluation de l'architecture de sauvegarde existante

La première partie de l'audit nous à fourni des Ensembles possédant chacun un Indice de Criticité. Nous allons, dans cette deuxième partie de l'audit, nous intéresser à l'architecture technique de sauvegarde actuellement en place. Cette étude va nous permettre d'obtenir un Indice de Sécurité pour chaque schéma de sauvegarde existant, que nous comparerons pour évaluer la qualité du système de sauvegarde.

2.1 Évaluation des équipements

Pour effectuer l'évaluation des équipements de sauvegarde des Ensembles, nous mettons à votre disposition trois grilles. Ces grilles présentent des critères d'évaluation pour chacune des trois familles de solutions de sauvegarde : le *DAS* (Directly Attached Storage), le stockage en réseau (*NAS & SAN*) et la télé-sauvegarde. Vous trouverez les informations relatives à ces familles dans le guide « *Maîtrisez votre système de sauvegarde* » disponible sur les sites Internet de MASSyS (voir contacts). Chaque équipement doit être évalué par une grille qui lui est propre. Nous allons décrire le contenu de chacune des grilles.

2.1.1 Directly Attached Storage

Cette grille à pour objectif de mettre en évidence les points forts et les points faibles de votre sauvegarde avec un DAS. L'audit du système se fait en deux étapes : la sauvegarde et la restauration puis le stockage des supports.

A - La sauvegarde

1. Capacité

Le point le plus important est la vitesse de transfert de votre lecteur. Elles doit être adaptée à la quantité d'information que vous devez restaurer.

L'objectif est de restaurer les données le plus rapidement possible. Pour des raisons financières, les

lecteurs sont généralement adaptés à la quantité d'informations sauvegardées. Ainsi, que vous ayez 10 Go ou 400 Go, le choix du support et de son lecteur vous permettra d'optimiser votre système. La durée acceptable pour une restauration est de 3h, quelque soit la quantité de données à restaurer.

Pour effectuer le calcul, vous pouvez vous appuyer soit sur la totalité des données sauvegardées, soit sur un sous-ensemble que vous considérez plus important. Ce dernier choix n'est possible que si votre système de sauvegarde vous permet de regrouper et de retrouver rapidement un sous-ensemble de fichiers (*ex: données d'un serveur particulier stocké sur une bande particulière*).

2. Sauvegarde

Ce point indique la périodicité des sauvegardes. Les sauvegardes différentielles et les sauvegarde complètes sont liées. Par exemple, si vous effectuez une sauvegarde complète par semaine, les sauvegardes différentielles seront effectuées quotidiennement. Ainsi, la périodicité des sauvegardes différentielles est toujours inférieure à la la périodicité des sauvegardes complètes.
L'idéal serait d'effectuer une sauvegarde complète quotidiennement. L'évaluation de la quantité de supports à mettre en œuvre est importante, ainsi que la main d'œuvre nécessaire pour leur manipulation (*externalisation et rotation des supports*).

3. Rotation des supports

La rotation quotidienne doit être faite par un robot la majorité du temps. En effet, le risque d'oubli d'un changement du support est trop élevé pour être acceptable. Par contre, la rotation hebdomadaire est généralement manuelle. Les robots gérant un aussi grand nombre de supports sont rares et chers.

4. Renouvellement des supports

Ce point permet de vérifier si le renouvellement des supports est adapté à leurs utilisation. Les périodes de renouvellement étant très différentes selon la périodicité des sauvegarde et la quantité de supports dont vous disposez, vous devez adapter cette partie de la grille à vos besoins. L'objectif est de s'assurer que les supports ne sont pas utilisés au-delà de leur durée de vie.

B - Stockage

1. Lieu

La solution idéale est généralement un lieu de stockage externe sécurisé à l'accès limité.

2. Période d'accès

Un accès permanent est préférable, mais certains prestataires de service comme les banques imposent des horaires d'ouverture restreints. Un stockage externe appartenant à l'entreprise permet une plus grande souplesse mais un coût plus élevé.

3. Temps de récupération

Le lieu de stockage doit être à proximité de l'entreprise pour optimiser le RTO (*Recovery Time Objective, le temps de récupération acceptable*). N'oubliez pas de prendre en compte la circulation difficile (*heure de pointe, travaux...*) au moment exact de l'audit.

4. Conditions

Les supports sont très sensibles à l'environnement. Il faut donc s'assurer que les taux d'humidité et la température soient inférieurs aux limites supportées. Les valeurs indiquées sur la grille sont des valeurs moyennes constatées. Vous devez connaître ces informations afin de savoir si votre lieu de stockage est adapté. Si ce n'est pas le cas, attribuez une valeur nulle.

Auditez votre système DAS

Auditeur

Date

Sauvegarde

1. Capacité

< 2h	☐ +5
< 3h	☐ +4
< 4h	☐ +3
> 4h	☐ +2

2. Sauvegarde

Complète

Quotidienne	☐ +5
Hedomadaire	☐ +3
Mensuelle	☐ 0

Différentielle

Quotidienne	☐ +3
Hedomadaire	☐ 0
Mensuelle	☐ -2

3. Rotation des supports

Quotidienne

Automatique	☐ +5
Manuelle	☐ -2

Hebdomadaire

Automatique	☐ 0
Manuelle	☐ +2

4. Renouvellement des supports

½ par trimestre	☐ +3
1/3 par trimestre	☐ +1
1/6 par trimestre	☐ 0

Stockage

1. Lieu

Externe et Sécurisé	☐ +5
Externe	☐ +2
Interne et Protégé	☐ +1
Interne	☐ 0

2. Période d'accès

24h/24, 7jours/7	☐ +2
12h/24, 5jours/7	☐ +1

3. Temps de récupération

< 1h	☐ +2
< 3h	☐ +1
> 3h	☐ -2

4. Condition de stockage

Température

< 30 °C	☐ +2
> 30 °C	☐ -2
Inconnu	☐ -5

Humidité

< 60%	☐ +2
> 60%	☐ -2
Inconnu	☐ -5

Personnel

Tâche	Nom	Fonction
Responsable		
Sauvegarde		
Rotation du jeu		
Restauration		

Score: _____/ 36

MASSyS version 1.0 – D. Bernaudeau & J. Vehent – Mars 2006

2.1.2 Stockage en réseau

Les solutions de stockages en réseau se découpent en deux sous-familles : les *Network Attached Storages* (*typiquement, les serveurs de fichiers*) et les *Storage Area Networks* (*des librairies de stockage indépendantes du réseau*). Nous traitons ces deux solutions de façon différente car ces deux sous-familles ne répondent pas aux mêmes besoins et n'ont pas les mêmes coûts.

A – Network Area Storage (NAS)

Ces équipements commencent avec un score de base de 15 car ils permettent par défaut d'obtenir un niveau minimum de sécurité des données. Attention à ne pas faire d'amalgame avec certains produits faussement appelés NAS (*par exemple les disques USB avec un bouton activant la sauvegarde, ces derniers sont des DAS*). Un NAS est un serveur dédié au stockage des données.

1. Charge réseau

Les constructeurs d'équipements réseaux préconisent une charge moyenne inférieure à 30% de la capacité théorique du réseau pour garantir son bon fonctionnement. Étant donné que les NAS dépendent complètement ce la qualité du réseau, vous devez être capable d'en évaluer la charge.

2. Redondance

Les systèmes de sauvegarde sur disques doivent absolument utiliser les technologies RAID afin de garantir qu'un disque défectueux ne va pas compromettre les données. Nous évaluons ici le niveau RAID utilisé ainsi que l'éventuelle présence d'une carte contrôleur secondaire.

3. Monitoring

Ces systèmes étant quasiment indépendants et autonomes, l'intervention de l'homme devient pratiquement nulle. Toutefois, vous devez être informé des dysfonctionnements. Certains systèmes proposent une interface web complète, d'autres un simple envoi de mail en cas d'erreurs et, dans certains cas, ces deux moyens sont proposés.

B – Storage Area Network (SAN)

Les SAN s'adressent à des structures plus exigeantes mais les contraintes générales sont les mêmes que pour les NAS. Les SAN débutent l'étude avec un score de base de 30.

Auditez votre système de sauvegarde réseau

Objectif

RTO _____

RPO _____

NAS *(de base: +15)*

1. charge réseau :
- ☐ <30% (+2)
- ☐ >30% (-2)
- ☐ inconnue ((-5)

2. redondance :

raid :
- ☐ 50 (+5)
- ☐ 10 (+4)
- ☐ 5 (+2)
- ☐ 1 (0)
- ☐ aucun (-5)

☐ contrôleur raid secondaire (+5)

3. monitoring
- ☐ rapports d'erreurs (+2)
- ☐ interface web (+5)

score temporaire: _____/ 17

NAS *(de base: +30)*

1. réseau :
- ☐ Ethernet 100mbps (-2)
- ☐ iSCSI ou Fibre Optique (+2)

2. monitoring :
- ☐ rapports d'erreurs (+2)
- ☐ interface web (+5)

3. redondance :
- ☐ contrôleur raid secondaire (+5)

score temporaire: _____/ 12

Personnel

	Nom	*Fonction*
Responsable		
Personnes en charge de la restauration		

SCORE GLOBAL : _____/___ (sur 32 ou 42 selon l'équipement)

MASSyS version 1.0 – D. Bernaudeau & J. Vehent – mars 2006

2.1.3 Télé-sauvegarde

Les systèmes de télé-sauvegarde permettent d'assurer un très bon niveau de sécurité. La grille suivante vous permet de vérifier la pertinence de votre système de sauvegarde externe. Elle prend en considération votre système interne ainsi que la qualité et la fiabilité de votre prestataire de service.

A – Système interne

1. Liaison avec le prestataire

La perte de la liaison avec votre prestataire de service réduit à néant votre système de sauvegarde. Une redondance de la connexion internet ou un taux de disponibilité garanti sont obligatoires pour assurer la fiabilité du système.

2. La sauvegarde

L'envoi complet des données chaque nuit est la solution idéale. Cependant, une quantité importante d'informations à envoyer impose une planification des sauvegardes sur la semaine. Il est difficile de laisser ce type de sauvegarde à la volonté de l'utilisateur car il vous serait impossible de maîtriser les flux de données, le risque étant d'engendrer une saturation de la liaison.

3. Capacité

Le débit de votre connexion internet doit être adapté à la quantité d'informations que vous devez envoyer. Le temps d'envoi moyen ne doit pas excéder les 10h, temps d'arrêt maximum constaté entre deux journées de travail. Réduire le temps d'envoi vous permet d'effectuer des sauvegardes régulièrement, voire de les segmenter, par exemple pendant la pause du midi, et ainsi améliorer votre RPO (Recovery Point Objective ; le RPO est l'âge maximal acceptable de vos sauvegarde, généralement 24h et parfois 12h).

B – Prestataire de service

1. Sécurité

Le principal danger lié à la télé-sauvegarde est l'espionnage industriel. Le transfert et le stockage de

données doit être cryptés afin de garantir la confidentialité. Les deux solutions proposées dans cette grille peuvent être sélectionnées simultanément.

2. Récupération des données

La télé-sauvegarde est excellente quand il s'agit de restaurer une partie identifiée des données sauvegardées. Mais pour récupérer l'intégralité de vos données, il est préférable de prévoir l'envoi d'un support contenant la totalité de la sauvegarde. Vous devez prévoir le temps de récupération des données via ce support.

C – Confiance

Un point rarement abordé par les prestataire (*on peut aisément comprendre pourquoi*) est la question de la confiance. Lorsque vous externalisez vos sauvegardes dans une entreprise tierce, vous perdez le contrôle sur vos données. Si ces données sont extrêmement importantes pour votre entreprise, vous devez vous demander si ce choix est judicieux.

Auditez votre système de Télé-Sauvegarde

Auditeur

Date

Système Interne		Prestataire de service	
1. Liaison		**1. Sécurité**	
Redondante	☐ +5	Liaison Sécurisée (VPN)	☐ +5
Disponibilité > 99,5%	☐ +3	Stockage Crypté	☐ +3
2. Sauvegarde		**2. Récupération des données**	
Quotidienne	☐ +5	Support DAS en 24h	☐ +5
Planification	☐ +2	Support DAS en 48h	☐ +2
Déclenché par l'utilisateur	☐ -2	Uniquement par Internet	☐ -5
3. Durée de la sauvegarde			
< 2h	☐ +10		
< 5h	☐ +5		
< 10h	☐ +2		
> 10h	☐ -2		

Personnel

	Nom	Fonction
Responsable		
Maintenance		

Confiance

Notez, de 0 à 5, la confiance que vous placez dans le fournisseur de la solution de télé-sauvegarde:

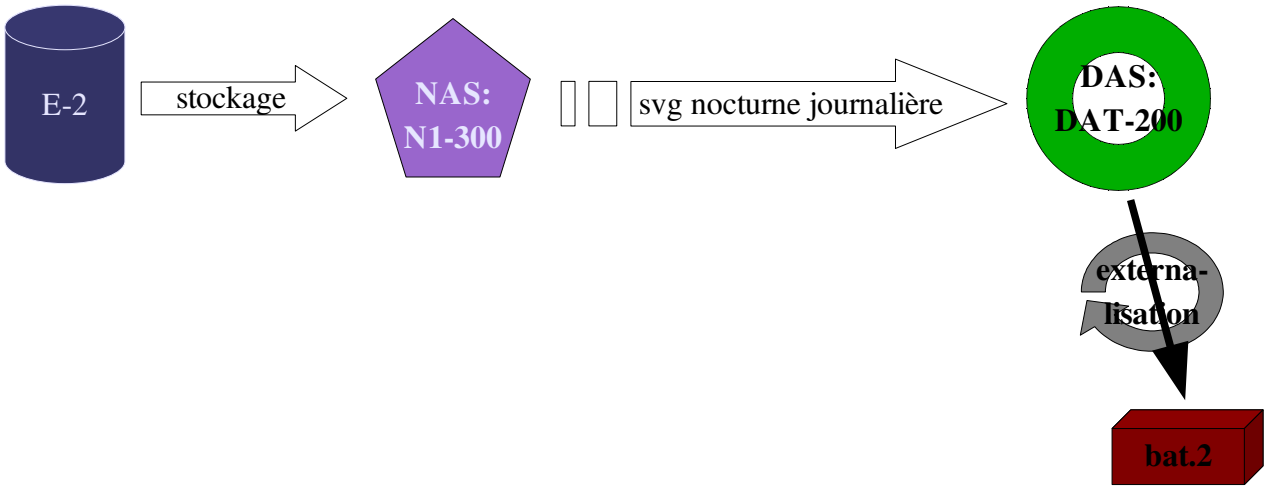
Note: _____/5

Commentaires :

2.2 Schémas de sauvegarde

Dans la partie précédente, nous nous sommes intéressés aux équipements en eux-mêmes. Mais nous n'avons pas considéré le « *chemin* » suivi par un Ensemble de données au cours de sa sauvegarde. Il est donc primordial de définir des schémas de sauvegarde et de placer vos Ensembles dans un schéma particulier.

Un schéma est la liste des équipements que traverse un Ensemble. Prenons comme exemple l'Ensemble E-2 que nous avons vu dans la première partie de l'audit. Nous lui avons attribué un Indice de Criticité valant 65. Regardons maintenant quel schéma de sauvegarde suit cet ensemble:



E-2 est stocké sur le NAS identifié par N1-300 (*conventionner le nommage simplifie la lecture de ce type de schéma*). N1-300 est sauvegardé chaque nuit sur une robot de sauvegarde DAT-200 et les bandes DAT de ce dernier sont emmenées chaque matin dans le bâtiment 2 (*les bandes sont ramenées dans le bâtiment principal à j+2*).

Supposons que les scores de N1-300 et de DAT-200 soient respectivement de 20 et de 23, nous pouvons donc définir pour ce schéma un Indice de Sécurité de 43. Or, nous avons établi un Indice de Criticité valant 65 pour E-2.

Nous avons donc un problème concernant l'Ensemble de données E-2. Soit sa criticité est trop élevée (cas *peu probable*), soit les moyens dédiés à sa sauvegarde ne sont pas suffisants. Il appartient donc à l'auditeur de proposer les améliorations possibles qui permettront de garantir un niveau de sécurité à la hauteur de la criticité de l'Ensemble.

Problème du maillon faible:

L'inconvénient des schémas de sauvegarde est qu'ils ne nous permettent pas de savoir si tous les équipements du schéma sont bons. La régle générale est que le niveau de sécurité d'un système est en fait le niveau de sécurité de son élément le plus mauvais. Pour refléter cet aspect dans le schéma de sauvegarde, nous utilisons le principe de l'écart.

Prenons l'équipement le plus faible et considérons son score: nous l'apellerons « S_{min} ». Considérons maintenant « n » le nombre d'équipement du schéma, « S_T » son score total de sécurité et « C_{E-2} » la criticité de l'ensemble considéré.

Nous avons déjà vu que si $\frac{C_{E-2}}{n} \approx Smin$ $C_{E-2} \approx S_T$, alors notre schéma de sauvegarde répond à nos besoins. Maintenant vérifions que :

Autrement dit, vérifions que la criticité de l'ensemble divisée par le nombre d'équipements est environ équivalente au niveau de sécurité de l'élément le plus faible du schéma. Ainsi, nous pouvons vérifions qu'un schéma de sauvegarde ne comporte pas de maillon faible risquant de mettre en péril tout le système.

Il est également possible de faire cette opération avec le niveau de sécurité de l'équipement le plus fort avant de vérifier que notre schéma est homogène et adapté aux besoins.

3. Intégrité des données et maîtrise de la restauration

Lorsque l'on s'aperçoit que le système de sauvegarde est défaillant, il est souvent trop tard. Il est donc conseillé de tester régulièrement vos sauvegardes.

La grille suivante vous permet de conserver un historique de vos restaurations, que ces dernières soient des restaurations de test ou non. Les informations relevées vous permettront de mieux remplir les grilles d'audit précédentes et plus particulièrement les données sur le temps de restauration. En effet, un test réel est plus fiable que des calculs théoriques.

Pour une utilisation plus aisée, nous vous conseillons d'établir une grille par Ensemble de données. Ainsi, la grille vous permettra d'analyser l'évolution de votre système. Avec le temps, la quantité d'informations augmentera et vous aidera à remettre en question votre système de sauvegarde.

Suivi des restaurations

Date	Ensemble	Quantité d'information (en Go)	Temps nécessaire à l'opération	Observations	Erreur	Intégrité des données	Participants		
							Nom	Fonction	Tache
02/04/06	E-2	104,5 Go	5h45	restauration de test	erreur de lecture à 45 Go, disparue au 2éme essai	OK (test md5)	Bernaudeau	....	resp. test

4. Conclusion

Au terme de cet audit, vous aurez acquis une bonne maîtrise de votre système de sauvegarde et plus globalement de votre système d'information. En effet, les deux sont intimement liés et, au delà des aspects liés à la sauvegarde, les points abordés au cours de MASSyS sontt également très intéressants des points de vue sécurité et reprise d'activité.

Les faiblesses d'un système d'information sont difficiles à mettre en évidence, et il est plus difficile encore d'adapter les moyens liés à sa protection. Si cette méthode souhaite souligner les points sensibles d'un système, il ne faut toutefois pas inverser ses résultats et déployer des protections hors de propos. En cela, le principe du schéma de sauvegarde vous sera certainement très utile si vous l'utilisez dans une optique de conception d'architecture, problème que nous n'avons pas abordé ici.

À ce jour, MASSyS est une méthode jeune qui a besoin d'être testée et améliorée. En la matière, toute contribution est la bienvenue. C'est avec ces différents retours d'expérience que nous voulons faire de MASSyS un outil très performant pour toute Direction Informatique, que ce soit au sein d'une PME comme dans de grands groupes travaillant sur des entrepôts de données à fortes contraintes sécuritaire. Nous souhaitons également conserver notre optique de départ : réaliser un outil simple applicable à des systèmes complexes.

Pour y parvenir, de nombreuses voies restent à explorer et bien que les auteurs restent convaincus de l'intérêt du travail accompli. Il reste à mettre en place une structure permettant à MASSyS de se développer le plus efficacement possible et un logiciel permettant de réaliser l'audit plus simplement, en automatisant certaines tâches. A ce sujet, nous ne le répéterons jamais assez, toutes les contributions sont les bienvenus.

Contacts

MASSyS

La méthode est diffusée sur les sites personnels des auteurs, à savoir :

http://jvehent.free.fr/index.php?Massys

http://www.bernaudeau.net/MASSyS/

Les auteurs :

Didier BERNAUDEAU	Julien VEHENT
mail: didier@bernaudeau.net	mail: julien@linuxwall.info
web: http://www.bernaudeau.net	web: http://jvehent.free.fr