MISSION 8 : SOLUTION DE SUPERVISION

I-) Contexte

a) **Presentation de stadium company**

Stadium Company est une société qui s'occupe de la gestion des stades , qui souhaite moderniser l'infrastructure réseau de son stade , la rendre scalable au fur et à mesure que ses ambitions augmentent . Elle emploie 170 personnes à plein temps et 80 à temps partiels . Elle projette ajouter des fonctions haute technologie afin de pouvoir prendre en charge l'organisation des concerts . La direction de Stadium Company n'étant pas compétente en matière d'Infrastructure réseau décide de faire appel à une entreprise de consultants réseaux qui s'en occupera de la conception à la mise en oeuvre en passant par la gestion du projet . Il sera mis en oeuvre en trois phases à savoir :

- La planification du projet et la préparation de la conception réseau haut niveau
- Le développement de la conception reseau détaillée
- La mise en oeuvre de la conception

b) **Presentation NetworkingCompany**

Le prestataire désigné pour l'exécution de ce projet est la société Networking Company, une firme locale spécialisée dans la conception d'infrastructure réseau et le conseil . C'est une société Cisco Premier Partner qui emploie 20 ingénieurs réseaux certifiés et expérimentée dans ce secteur.

Dans le but de concevoir le nouveau plan de l'infrastructure de haut niveau , Networking Company a décrit un profil de l'organisation et des installations sur la base des études menées par ses experts notamment en interrogeant le personnel.

Mission 8 : Mise en place d’un système de supervision Open source.

Contexte :

StadiumCompagny recherche, l’Implémentation et la configuration d'une solution Open Source qui vise à superviser à distance les différents éléments actifs de l’infrastructure systèmes et réseaux du Stade avec gestion des alertes.

Plan du travail :

Le but principal du projet est de pouvoir établir, choisir et installer une solution de surveillance des serveurs, routeurs, commutateurs, ..., qui remplit les conditions suivantes:

- Coûts financiers les plus réduits possibles.
- Récupération des informations permettant la détection des pannes, l’indisponibilité des serveurs (Windows, Linux), routeurs, commutateurs, les états des imprimantes réseau et leurs services.
- Des renseignements supplémentaires de monitoring sur la charge CPU, espace disque,mémoire disponible, input/output, processus en cours d’exécution, paquet perdu, temps moyen de parcours, information d'état SNMP, trafic, bande passante consommée etc...
- Des renseignements supplémentaires de monitoring sur les services DNS, DHCP, http, SMTP, POP, IMAP, FTP, ...
- Gestion des alertes.
- Notification par mail ou SMS en cas de problème.
- Générer des rapports sur le fonctionnement des serveurs par mois.
- Générer des graphes (cartographie du réseau, ...)
- Une interface graphique claire pour l’interaction utilisateur/Logiciel

Introduction à la supervision

La supervision est un processus informatique qui permet de surveiller l'ensemble du SI d'une organisation. Les outils de supervisions s'appellent des superviseurs qui permettent de surveiller les traitements informatiques. Dès qu'un traitement ne s'est pas exécuté correctement l'outil de supervision déclenche une alerte ; l'alerte est ensuite traitée par l'équipe pilotage. L'équipe de pilotage ont pour mission de surveiller les alertes remontées et d'exécuter des consignes pour résoudre ces alertes.
La supervision consiste à indiquer et à commander l'état d'un appel, d'un système ou d'un réseau. Les solutions de supervision permettent de remonter des informations techniques et fonctionnelles du système d'information.

L'informatique étant devenue l'épine dorsale de l'entreprise quel que soit son secteur d'activité, le système d'information est au centre de l'activité de différentes entités métiers et doit fonctionner pleinement et en permanence pour garantir l'efficacité de l'entreprise. A tous les niveaux, les réseaux, les terminaux utilisateurs, les serveurs d'applications et les données constituent autant de maillons sensibles dont la disponibilité et la qualité de service conditionnent le bon fonctionnement de l'entreprise.

Les problèmes liés à l'informatique doivent donc être réduits au minimum, car une indisponibilité du système d'information a des impacts très préjudiciables sur l'activité et sur la notoriété d'une entreprise.

Il existe deux enjeux majeurs pour les directions informatiques. Le premier est de garantir la disponibilité et les niveaux de service du système en cas de panne ou de dégradation des performances (par des mécanismes de redondance et d'équilibrage…). Le second est de tenter de prévenir en cas de problème et, le cas échéant, garantir une remontée d'information rapide et une durée d'intervention minimale. C'est le rôle de la supervision.

Il existe plusieurs méthodes pour superviser le système d'information :

- Analyser les fichiers de log
- Récupérer des résultats de commandes et de scripts locaux ou distants
- SNMP : Simple Network Management Protocol

Gestion proactive est une démarche de travail qui permet d'agir en avance puisqu'on anticipe les incidents c'est-à-dire on sait à l'avance qu'est-ce qu'on va faire lorsque des incidents surviennent. Prévoir pour mieux gérer c'est à dire agir avant qu'une situation ne devienne une cause de confrontation ou de crise. Donc, anticiper en se posant les bonnes questions est primordial.

Superviser : quoi ?

La supervision informatique permet de superviser l'ensemble du système d'Information de l'entreprise :

- Le réseau et ses équipements
- Les serveurs
- Les périphériques
- Les applications
- Le workflow
- Surveiller les systèmes d'information
- assurer la disponibilité des services.
- prévenir les défaillances.
- détecter les anomalies (sécurité, système).
- fédérer l'information d'équipements hétérogénes en un portail unique.
- Automatiser les téches
- alerter en cas d'interruption d'un service.
- relancer des services interrompus.

Les niveaux de supervision

Supervision environnementale

- température de la pièce
- humidité de la pièce

Supervision réseau et matérielle

- commutateurs et routeurs : disponibilité, interrogation des sondes, alertes.
- serveurs : disponibilité, interrogation des sondes matérielles, alertes.
- onduleurs : disponibilité, charge, état.
- imprimantes : disponibilité, état de l'imprimante et des consommables.

Supervision des systèmes

- commutateurs : utilisation des ressources, métrologie.
- serveurs : utilisation des ressources.

Supervision des applications et services

- disponibilité.
- cohérence des réponses aux interrogations.
- performances.

Superviser : pourquoi ?

L'informatique est au cœur de l'entreprise, quelle que soit son secteur d'activité. On peut facilement comparer la place que joue l'informatique au sein d'une entreprise é celle que joue le système nerveux chez l'être humain. En effet, il est au centre de l'activité, et doit fonctionner pleinement et en permanence pour garantir l'activité.

Certaines ramifications même comme le réseau et les terminaux utilisateurs doivent aussi fonctionner, à l'instar des nerfs du système dans le corps humain.

Les problèmes liés à l'informatique doivent donc être réduits au minimum, car une indisponibilité du système d'information peut être la cause de plusieurs millions d'euros de pertes.

Deux phases sont donc importantes pour les directeurs informatiques : garantir la disponibilité du système en cas de panne (par des mécanismes de redondance…) mais aussi tenter de prévenir en cas de problème et, le cas échéant, garantir une remontée d'information rapide et une durée d'intervention minimale : c'est le rôle de la supervision.

Superviser : comment ?

Il existe plusieurs méthodes pour superviser le système d'information :

- Analyser les fichiers de log
- Récupérer des résultats de commandes et de scripts locaux ou distants
- Supervision en mode actif
- Supervision en mode passif

Nagios

Nagios est un logiciel de supervision destiné à vous informer de problèmes éventuels dans votre système d'informations avant que vos clients, utilisateurs ou managers ne le fassent. Il est prévu pour fonctionner sur système d'exploitation Linux mais fonctionne également sans problème sur la plupart des variantes *NIX. Le démon de supervision effectue des contrôles intermittents sur les hôtes et services que vous spécifiez en utilisant des plugins externes qui retournent un statut d'état à Nagios. Quand des problèmes surviennent, il peut envoyer des notifications à des contacts administratifs de façons différentes (email, SMS, messagerie instantanée, etc…). Les informations d'états courants, les historiques et les rapports peuvent être consultés à partir d'un simple navigateur.

Présentation

Moniteur de supervision :

- vérification des services réseau (SMTP, HTTP, …etc.).
- surveillance des ressources des hôtes (charge CPU, espace disque, …etc.).
- contrôle des équipements réseau (CPU, ventilateurs, …etc.).

Ordonnanceur et analyseur gérant les actions :

- système complet de notification fonction du service, de l'heure et de la date.
- gestion des escalades.
- possibilité de paramétrer des réactions automatisées.
- possibilité de définir des gestionnaires d'événements.
- Système de modules/plugins de vérification
- fonctionne tels des programmes externes.
- permet de développer ses propres modules.
- Possibilité de définir la hiérarchie du réseau en utilisant des hôtes parents.
- Une interface Web avec gestion des droits pour la consultation.
- Génération de rapports de surveillance.
- N'est pas destiné à faire de la métrologie.

Possibilités

Nagios (anciennement appelé Netsaint) est un logiciel qui permet de superviser un système d'information complet. C'est un logiciel libre, il est sous licence GPL.
C'est un programme modulaire qui se décompose en trois parties:

1. Le moteur de l'application qui vient ordonnancer les tâches de supervision.
2. L'interface web, qui permet d'avoir une vue d'ensemble du système d'information et des possibles anomalies.
3. Les plugins, une centaine de mini programmes que l'on peut compléter en fonction de nos besoins pour superviser chaque service ou ressource disponible sur l'ensemble des ordinateurs ou éléments réseaux de notre SI.

- Superviser des services réseaux : (SMTP, POP3, HTTP, NNTP, ICMP, SNMP, LDAP
, etc.)
- Superviser les ressources des serveurs (charge du processeur, occupation du disque dur, utilisation de la mémoire paginée) et ceci sur les systèmes d'exploitations les plus répandus.
- La supervision à distance peut utiliser SSH ou un tunnel SSL.
- Les plugins sont écrits dans les langages de programmation les plus adaptés à leur tâche (Bash, C++, Python, Perl, PHP, C, etc.)
- La vérification des services se fait en parallèle.

- Possibilité de définir une hiérarchie dans le réseau pour pouvoir faire la différence entre un serveur en panne et un serveur injoignable.
- La remontée des alertes est entièrement paramétrable grâce à l'utilisation de plugins (alerte par email, SMS, etc.)
- Chaque test renvoi un état particulier:

1. # OK (tout va bien)
2. # WARNING (le seuil d'alerte est dépassé)
3. # CRITICAL (le service a un problème)
4. # UNKNOWN (impossible de connaître l'état du service)

Architecture

- un ordonnanceur qui gère :
  - l'ordonnancement et les dépendances des vérifications.
  - les actions à entreprendre suite à des incidents (alertes, escalades, corrections automatiques).
- une interface graphique de type client Web.
- des modules/sondes dont un grand nombre sont fournis de base. (ex : check_mailq, check_http, check_imap).
- Nagios est un noyau
- ordonnanceur et analyseur.
- système de modules pour les vérifications.
- rassemblement et analyse d'informations.
- réaction, prévention et réparation.
- souplesse et finesse de configuration.

Avantages

- Reconnu auprès des entreprises, grande communauté
- Plétore de plugins qui permettent d'étendre les possibilités (agents comme zabbix, reporting amélioré, etc...)
- Une solution complète permettant le reporting, la gestion de panne et d'alarmes, gestion utilisateurs, ainsi que la cartographie du réseaux
- Beaucoup de documentations sur le web
- Performances du moteur

Inconvénients

- Interface non ergonomique et peu intuitive
- Configuration fastidieuse via beaucoup de fichiers
- Pour avoir toute les fonctionnalités il faut installer des plugins, de base c'est assez limité.

Centreon

Centreon est LE dérivé français de Nagios de référence développé par la société Merethis. Il s'agit d'une couche applicative Web venant se greffer à Nagios pour offrir une administration moins rudimentaire (évite les fichiers de configuration et les lignes de commandes brute). L'équipe de chez Merethis est avant-gardiste et a inspiré pour certains points les lignes directrices de la communauté. C'est un produit très complet et son interface le rend très professionnel aux yeux des dirigeants.

Schéma Fonctionnel

- Principe de fonctionnement

Le schéma ci-dessous montre comment Centreon et Nagios intéragissent l'un avec l'autre.

- Gestion des flux

Le schéma ci-dessous montre les protocoles et flux utilisés par les différents éléments qui compose une supervision Centreon / Nagios

Avantages

- La robustesse et la renommée de Nagios
- Une interface beaucoup plus sympathique, permettant de tout configurer, de garder un oeil sur tout le réseau en permanence
- Les utilisateurs de Nagios ne seront pas perdus pour autant, l'interface reprenant avantageusement certaines vues Nagios
- Une solution complète permettant le reporting, la gestion de panne et d'alarmes, gestion utilisateurs, ainsi que la cartographie du réseau
- Une entreprise qui pousse le développement
- Peut-être décorelé du serveur Nagios et tourner tout seul sur un autre serveur

Inconvénients

- L'interface peut paraître complexe car il existe beaucoup d'options, de vues....cela nécessite une petite formation
- Un développement qui n'est pas encore en phase avec celui de Nagios : Parfois des problèmes de compatibilité
- Un peu plus lourd que du Nagios pur

Cacti

Présentation de Cacti

Cacti est un logiciel de supervision (dit de « capacity planning ») basé sur RRDtool permettant de surveiller l'activité de son architecture informatique à partir de graphiques quotidiens, hebdomadaires, mensuels et annuels.

Cette solution n'est donc pas destinée à alerter en temps réel sur les dysfonctionnements d'un système mais bien de proposer une vision dans le temps de l'évolution d'indicateurs matériels et logiciels (trafic réseau, occupation des disques, temps de réponse, etc…).

acti est une interface de présentation (frontend) complète à RRDTool, il stocke toute l'information nécessaire pour créer des graphiques et pour les peupler avec des données dans une base de données MySQL. Le frontend est complètement écrit PHP. Il supporte également SNMP et tend à se substituer à MRTG pour créer des graphiques.

Cacti permet d'alimenter les graphiques à partir de n'importe quel script / command externe.

Une fois qu'un ou plusieurs points d'émission de données sont définis, un graphique de RRDTool peut être créé en utilisant les données. Cacti vous permet de créer presque n'importe quel graphique en utilisant tous les types de graphique de RRDTool et fonctions standards de consolidation, mais aussi de présentation. Cacti offre également une gestion d'utilisateurs qui permet à chacun la possibilité de personnaliser l'interface mais aussi de limiter l'accès.

Présentation de RRDtool

Le programme RRDtool a été développé par Tobias Etiker dès 1995. Il est librement téléchargeable sur le site suivant : http://people.ee.ethz.ch/~oetiker/webtools/rrdtool/.

RRD est l'acronyme de Round Robin Database, qui peut se traduire par « base de données cyclique ». Ce mécanisme permet de stocker des données dans des fichiers de taille invariante, définie à la création, par un mécanisme de pile LILO (Last In Last Out). Un fichier RRD peut contenir plusieurs RRA (Round Robin Archive) qui correspondent aux différents cycles de conservation des données (jour, semaine, mois, année, etc.).

Une fois les données collectées, RRDtool fournit des outils permettant de générer des graphiques hautement personnalisables, retraitant les données à la volée.

Avantages

- Interface : Beaucoup plus claire que celle de NetMRG elle permet également beaucoup plus de choses (Plus de modes d'affichages et plus de possibilités de configuration)
- Configuration : Avec l'utilisation des templates pour les machines, les graphiques, et la récupération des données tout se configure aisément et entièrement via l'interface web. Import/ Export très simple des templates au format XML. On peut aussi très facilement utiliser des options poussées de RRDTOOL
- Performance : Avec le choix du moteur de récolte des données, On peut opter pour la performance ou la simplicité
- Gestion des utilisateurs
- Communauté sur le web, présence d'une dizaine de plugins permettant d'étendre les fonctionnalités

Inconvénients

- Pas de gestion d'alarmes, sauf avec un plugin nommé Thold
- Pas de gestion de panne et absence d'une cartographie de réseau
- Un développement lent