Réalisations possibles de l'outil de gestion des VLAN's sur grid5000

1) Contexte de travail

Grid5000 est un réseau expérimental qui peut être décrit comme une architecture comportant un ensemble de machines interconnectées et réparties sur plusieurs sites géographiques (à terme 5000 processeurs). C'est un réseau hétérogène de machines et d'équipements, ou plus précisément de clusters. Il est assez complexe en raison de sa nature expérimentale. Actuellement il fonctionne comme un ensemble de réseaux interconnectés par des routeurs. Différents outils ont été mis en place et entre autre un outil de réservation de ressources qui est la base de l'accès a grid5000. Cet outil permet de réserver des machines, soit sur un site ou bien sur plusieurs. Le but des réservations peut être différent, il peut être voué à l'exécution de programmes distribués ou bien au déploiement de systèmes d'exploitations pour effectuer différents tests. De manière générale, une réservation se fait par le biais d'une machine que l'on nomme “frontale” qui est l'interface entre l'extérieur et le réseau grid5000. Cette machine permet la réservation sur le site local et à titre expérimental une réservation globale.

L'outil à réaliser va se placer à un niveau sous-jacent du logiciel de réservation et devra permettre l'isolation des machines réservées. Les cas d'utilisations seront présentés pour pouvoir comprendre l'utilisation qui sera faite du logiciel. Le but est de faire un outil de configuration automatique de VLAN's. Cet outil servira à isoler des machines par le biais de la technologie VLAN supportée sur la plupart des switchs et routeurs actuels. Il sera dans un premier temps utilisable au niveau de sites isolés en raison de l'hétérogénéité des équipements mais pourra être porté de manière a supporter des réservations globales que l'on veut isoler. Les équipements réseaux étant différents suivant les sites, l'outil devra prendre en compte cette contrainte et permettre l'ajout d'extensions permettant la configuration de nouveaux équipements. Il devra s'assurer de ne pas perdre de machine du réseau et surtout de garder un état cohérent et permettre la remise initiale de la configuration.

L'architecture réseau au niveau de chacun des sites est différentes mais il y a des choses qui se retrouvent, chaque site contient une machine frontale et un ensemble de serveurs (DHCP, DNS). Il y a un ensemble de switchs permettant d'interconnecter des machines. Ces switchs peuvent être de marque différentes suivant les sites. Les modifications que pourra faire l'outil devront se limiter a la

machine frontale, aux switchs et aux routeurs. L'outil sera lancé à partir de la machine frontale.

Comme présenté précédemment, l'outil se situe dans un contexte de grille. L'interconnexion des équipements présents dans la grille se fait via un réseau. Ce réseau est d'ampleur nationale et est géré au niveau de chaque site différemment. Le routage au niveau inter-sites est statique et une plage d'adresse est réservée pour chaque site.

Dans la configuration actuelle les machines de grid5000 ne font parties d'aucun VLAN.

2) Utilité des vlans dans le cas grid5000

Les VLAN's peuvent avoir plusieurs utilités dans grid5000. Nous allons en lister quelques unes pour comprendre l'intérêt de l'implantation de kavlan au sein de grid5000.

Le premier est d'isoler les machines pour avoir un accès exclusif à celles-ci. Dans la configuration présente, lors de lancement d'exécution sur des machines réservées, celles-ci sont encore accessibles aux connexions extérieures.

Isoler les machines lors de déploiements pour ne pas rentrer en conflit avec les serveurs installés. L'outil devra donc remplir cette contrainte en proposant le maximum de flexibilité.

Limiter le trafic sur le réseau (broadcast).

Avoir une vue logique de l'ensemble des machines réservées.

3) Réalisations possibles et présentations et contraintes

Tout d'abord, voici une brève présentation des VLAN. Différentes techniques de VLAN sont utilisables. Il y en a trois qui se nomment VLAN par port (de niveau 1 de la couche OSI), VLAN par adresse (de niveau 2 de la couche OSI) et VLAN par protocole (de niveau 3 de la couche OSI). Chacun d'entre eux agit à un niveau différent et présente des avantages et inconvénients. Les VLAN par port sont très sûr mais restrictifs car ils nécessitent de connaître le port de connexion de la machine et en cas de déplacement de celle-ci, la reconfiguration des VLAN. Les VLAN de niveau 2 sont déjà plus souples car ils se basent sur l'adresses MAC qui est unique pour chaque interface réseau. Cependant l'usurpation d'adresse MAC étant possible, il y a plus de risque de connexion par un tiers que lors des VLAN par port. Les VLAN par protocoles sont beaucoup plus souples mais plus sensibles car cette fois ci on se base sur l'adresse IP et dans ce cas l'appartenance à un VLAN est faite par le changement d'adresse et non pas lorsque l'on décide de faire appartenir une machine à un VLAN. Cette dernière technologie étant d'ailleurs plus récente, elle est moins présente dans les équipements réseaux que sont les switchs car elle agit au niveau 3.

La technologie VLAN peut donc être utilisée quelque soit le niveau voulu. VLAN est un protocole de niveau 2, c'est à dire que des informations sont insérées au niveau trames. Il y a deux façons de traiter ce protocole, soit se sont les switchs qui voient l'appartenance d'une machine à un VLAN et dans ce cas, ils transmettent une trame ethernet standard à la machine : c'est le mode non tagué. Soit le switch transmet une trame contenant une information sur le VLAN dont la trame provient : c'est le mode tagué. Les deux modes sont utilisables sur les ports des switchs et un port peut utiliser les deux modes en même temps. C'est alors à la machine de différencier les VLAN à l'aide d'une interface virtuelle. Il est également possible de faire appartenir un port à plusieurs VLAN en mode tagué car on peut différencier les trafics. La seule contrainte est qu'un port du switch ne peut appartenir à deux VLAN en mode non tagué car il appartiendrait à deux réseaux à la fois sans pouvoir les distinguer. Pour résumer le traitement se fait au niveau de la machine, soit on reçoit normalement des trames, soit on doit créer une interface particulière pour recevoir des trames, ou bien on couple les deux solutions.

Voici les différentes manières dont pourrait fonctionner l'outil. Chaque solution correspond à

un niveau d'accès différent aux VLAN créés.

- accès via le routeur
- accès direct par le frontal
- accès par machine réservée passerelle

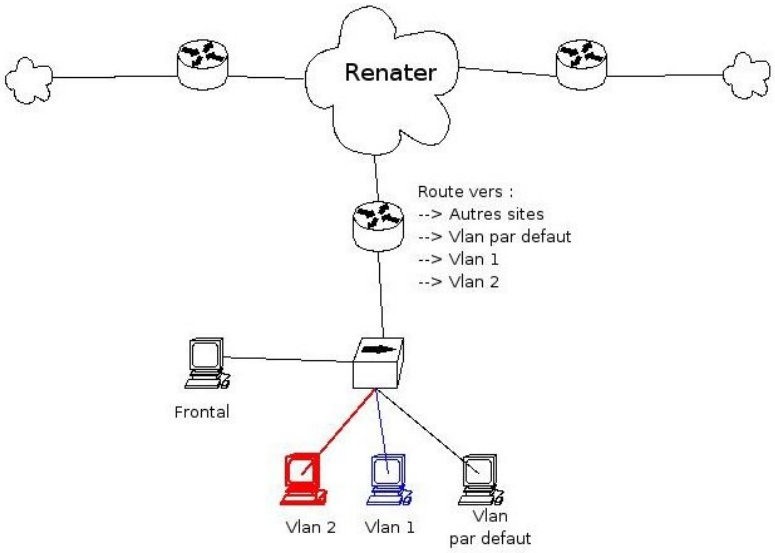
Pour l'accès via le routeur il faudrait créer les VLAN, et créer une interface virtuelle au niveau du routeur avec un sous réseau réservé pour le VLAN nouvellement créé. Cela permettrait d'avoir un accès direct aux machines tout en les isolants. Le routeur connaissant l'adresse de destination du nouveau VLAN pourrait alors de lui même rediriger tout le trafic en destination de celui-ci. La seconde solution qui est l'accès par le frontal nécessite la même opération de création d'interface virtuelle mais il faudrait en plus que le frontal appartienne a tous les VLAN créés. Dans ce cas, un problème intervient au niveau de la transmission des données des VLAN's entre les sites car les sites ne peuvent pas accéder aux VLAN's des autres sites sans passer via la machine frontale de chaque cluster. La dernière solution qui est l'accès par machine passerelle nécessite la création des VLAN seulement au niveau des switchs mais la configuration au niveau utilisateur est plus complexe car elle oblige l'utilisateur à mettre en place par lui même une machine qui a une patte sur les deux réseaux (le VLAN par defaut et celui créé), de plus l'accès aux machines reste plus complexe car il faut passer par cette machine passerelle pour pouvoir se connecter aux autres membres du VLAN.

La solution qui semble la plus facile d'accès pour l'utilisateur et la plus extensible est celle qui passe par la création d'interfaces au niveau du routeur. Dans les trois cas les flux internes aux VLAN's seront isolés mais du point de vue utilisation cette solution reste la plus simple.

La mise en place de kavlan quelque soit la solution nécessitera la création d'un nouveau sous réseau par VLAN. Cela permettra de faciliter la compréhension et l'utilisation de kavlan. L'intérêt de kavlan étant de créer des réseaux distincts, il passe donc par la création de sous réseaux. On peut cependant créer des VLAN sans modifier les adresses IP des machines et avoir le même réseau pour les différents VLAN mais le problème est de pouvoir router l'information vers les machines des VLAN et cela est plus simple lorsque les VLAN's correspondent à des réseaux différents

La question du routage inter vlan et du routage inter site pour les vlan s'est posé. En ce qui

concerne le routage entre les vlan d'un même site, il sera effectué car il est plus intéressant de pouvoir isoler certaines machines et de quand même pouvoir y accéder par des machines qui ne sont pas forcement sur le même VLAN. Les machines des VLAN's restent donc isolées mais accessibles, ce qui est essentiel pour un fonctionnement de kavlan au niveau de l'ensemble de grid5000. En ce qui concerne le routage inter sites, le protocole VLAN n'est pas un protocole routé. Il est dont impossible d'avoir une gestion centralisée des VLAN, cependant on peut créer des VLAN sur chaque site avec les masques de sous réseaux correspondants aux critères des sites. Les VLAN's crées sur chaque sites seront accessibles car les routeurs, connaissant les plages d'adresses de chaque site, pourront routés les informations vers le site destiné et acheminer les informations jusqu'aux machines appartenant à d'autres VLAN's. L'outil permettra des configurations au niveau de chaque site mais fonctionnera au niveau grid5000.



La création des VLAN entraîne certaines contraintes, et l'utilisation peut nécessiter des connaissances de la part de l'utilisateur. Les contraintes les plus importantes sont au niveau des protocoles et des flux réseaux. Après la création d'un VLAN et l'intégration des machines à celui-ci, le réseau sera isolé du réseau grid5000 et n'aura donc plus accès aux services tel que le DHCP. Ce qui signifie que les machines devront être gérées par l'utilisateur et qu'elles devront être configurées correctement avant de les faire appartenir au VLAN crée à moins de déployer un serveur DHCP pour ce nouveau VLAN et de le configurer avec la plage IP réservée. De plus, les machines ne seront plus accessibles via leur nom DNS car leurs adresses ayant changées, le DNS ne sera pas mis a jour et cela nécessitera la mémorisation des adresses IP des machines du VLAN créé. Il est à noter qu'une machine pourra appartenir à plusieurs VLAN mais dans ce cas, la création d'interfaces virtuelles pour traiter les VLAN's sera nécessaire dans le cas d'utilisation du mode tagué.

4) Choix techniques et Configurations nécessaires sur les switchs et routeurs

Pour la réalisation des VLAN, plusieurs choix sont possibles. On peut utiliser différents types de VLAN qui sont : par port, par adresse MAC, par adresse IP. Dans notre cas, les configurations qui sont les plus intéressantes sont les VLAN's par port ou par adresse MAC car on veut pouvoir isoler des machines quelque soient leurs adresses IP's. Le seul problème sera la manière de récupérer les ports de connexions ou bien les adresses MAC des machines que l'on veut réserver.

La configurations des VLAN devra se faire au niveau des switchs. Plusieurs pistes sont exploitables, on peut soit modifier les tables de VLAN sur chaque switch lors de la création et suppression de VLAN, ou bien utiliser le protocole VTP (Vlan Trunking Protocol) ou GVRP (GARP (Generic Attribute Registration Protocol) Vlan Registration Protocol) qui permettent la diffusion des informations concernant les VLAN entre les switchs. La aussi une contrainte technique se pose, c'est l'interopérabilité de ces protocoles car certains switchs ne les supportent pas. La solution de modification sur chaque switch parait donc la plus logique mais nécessite néanmoins de posséder les adresses de tous les équipements réseaux à mettre à jour, ou bien dans le cas ou les équipements sont administrés de façon “stackée” (tous les switchs sont représentés de manière logique comme un switch administrable) l'adresse du switch d'administration.

Pour l'administration des switchs et la configuration, le protocole SNMP est le seul qui soit supporté par tous les matériels. L'avantage est que ce protocole est léger et qu'il apporte une grande flexibilité au niveau de sa manipulation. Certaines options sont dépendantes du matériel et l'outil devra gérer la possibilité d'ajout de ceux-ci. Le principal inconvénient est que ce protocole dans la version la plus présente sur les matériel (v2) ne comporte pas de mécanismes de sécurité fiable.

5) Fonctionnalités de l'outil à réaliser

Après avoir énuméré les utilisations possibles et les contraintes, voici les fonctionnalités qui seront proposées a l'utilisateur pour la gestion des VLAN's. Tout d'abord, l'outil devra limiter les droits de la personne en l'autorisant à modifier seulement les ports qui sont connectés aux machines réservées par la biais d'OAR pour ne pas mettre en péril les autres réservations d'utilisateurs de grid5000.

L'outil d'administration de VLAN's sera accessible via la machine frontale et proposera les artifices dont les conséquences seront réversibles :

- Créer un VLAN avec une plage IP qui sera utilisée dans le VLAN
- Ajouter/Retirer une machine du mode non taggé dans un VLAN (c'est a dire reçoit les trames réseau d'un certain VLAN mais sans l'en tête du VLAN)
- Ajouter/Retirer un machine du mode taggé dans un VLAN (recevoir des trames avec l'en tête du VLAN : nécessite généralement la création d'interfaces virtuelles au niveau de la machine)
- Supprimer un VLAN
- Annuler toutes les manipulations effectuées (sauvegardées dans fichier ou avec configuration actuelle des switchs)
- EXTENSION : Utiliser des fichiers de sauvegarde des VLAN's et des étapes de déploiements (peut permettre de valider chaque étape et d'attendre la réalisations de certaines manipulations avant de passer à l'étape suivante)

Un utilisateur particulier qui sera l'administrateur aura des fonctionnalités supplémentaires qui seront :

- Mise a zéro de la configuration des VLAN pour les utilisateurs ou au niveau site
- Gérer les extensions pour manipuler des équipements d'une certaine marque (MIB's)
- Gérer les adresses des équipements réseaux à configurer
- EXTENSION : L'édition du fichier de configuration global (permet de sauvegarder des topologies d'assignements aux VLAN's)

6) Conclusion

L'outil kavlan pourra s'intégrer et être proposé à l'utilisateur pour gérer des VLAN's au niveau de chaque site sur les machines réservées. Il effectuera la configuration automatique des switchs et routeurs pour permettre à l'utilisateur de pouvoir utiliser cet outil et la fonctionnalité proposé de la manière la plus simple possible. Avec la configuration proposée, il laisse libre choix à l'utilisateur d'effectuer la majeur partie des commandes disponibles pour les VLAN (création, suppression, ajout d'une machine au VLAN dans les différents modes, suppression). La possibilité de rétablissement de configuration initiale ainsi que les commandes disponibles donnerons une souplesse d'utilisation ainsi que la possibilité d'annulation des manipulations ayant coupé l'accès à certaines machines.