

Projets LPRS 2020

Sujet 1 : l'IoT aujourd'hui, le temps de la démocratisation : quelle(s) technologie(s) avec quel niveau de sécurité pour quel(s) impact(s) ?

Tuteur : Jean-Luc BOURDON (jean-luc.bourdon@u-cergy.fr)

Objectif : Définir un benchmark des technologies actuelles utilisées dans les objets de l'IoT et de leur niveau de sécurité

Contexte : Le développement de l'IoT depuis quelques années va croître encore de manière exponentielle pour les 20 prochaines années...

- Qu'en est-il des technologies utilisées ? De leur sécurité ?
- Quid des normes américaines vs les normes européennes ?
- Quid de leur impact environnemental ?
- Quid de leur impact économique ?
- Quid de leur impact sur la vie citoyenne ?

Ce projet a pour objectif un état de l'art de la situation actuelle et des prévisions à court, moyen et long terme.

Sujets 2 / 3: Energy Aware Live Migration and Dynamic Load Balancing of Virtual Machines in VM-Ware / Microsoft Azure Environment(s)

Tuteur : Iryna Andriyanova

ATTENTION : les deux sujets sont identiques mais le travail est à effectuer dans deux contextes techniques différents. Le sujet est en anglais mais la réalisation se fera et sera évaluée en français !

Objectif :

- To purpose an algorithm for “Energy Aware Live Migration and Dynamic Load Balancing of Virtual Machines in Data Centers”
- Verify the algorithm by testing it on a real physical servers
- Present the results

Contexte : In data centers hardware resources are shared using virtual machines. These virtual machines are a source to optimize resource allocation and utilization, reduce job processing time and efficient use of data storage. Other key benefits of virtual machines in data centers includes multiplexing of resources, saving on power by consolidating various virtual machines on a single physical server and migration of virtual machines for load balancing. Recently, virtual machines are used for another big advantage and that is live migration of virtual machines. Live migration of virtual machines enable data centers to better distribute the work load across physical servers when resources are not sufficient for virtual machines.

The energy aware live migration and load balancing of virtual machine problem determines how to distribute work evenly between available resources in a way that achieves performance goals. In our scenario the performance goals are Energy Consumption and Load Balancing.

Available Equipment

Power Edge 6415 AMD EPYC 7551P - 32 Core Processor
Power Edge R630 Intel(R) Xeon(R) CPU E5-2620 V4 - 8 Core Processor

After completing this project students will be able

1. To develop hands-on skills on configuring virtual machines on real servers
2. To deploy virtual machines that achieves high performance and low energy consumption
3. To improve analytical skills by reading several research papers

Sujet 4 : Sécurisation d'un hébergement web mutualisé pour un intranet

Tuteur : Marc Lemaire

Objectif : proposer une solution complète d'hébergement web mutualisé robuste dans le cadre d'un intranet pour les enseignements.

Contexte : les enseignements de développement web s'appuient sur des serveurs dédiés avec un hébergement mutualisé à finalité pédagogique dans une architecture 3 tiers.

Réalisation : le but de ce projet est de mettre en œuvre une infrastructure intranet complète (DNS, serveurs web et sftp, certificats https auto-signé, serveur mail interne, serveur SGBD mysql et postgresql, etc.) dédiée aux enseignements tout en assurant une qualité de service de niveau élevé et en sécurisant la solution proposée : automatisation de la gestion des comptes, droit restreints de type « chroot », isolation des scripts PHP de type « jail », limitation via adresses IP et numéro ports, rôle du DBA, etc..

Livrables : Une procédure complète de mise en œuvre de l'infrastructure retenue avec l'ensemble des paramètres et configurations permettant de reproduire la solution.

Environnement technique : Solutions Open Source ; distribution Debian ou Ubuntu Server.

Sujet 5 : Audit de sécurité d'un site web.

Tuteur : Marc Lemaire

Objectif : définir une procédure permettant un audit de sécurité d'un site web.

Contexte : on considère dans un premier temps un site web (à créer) d'un intranet mais idéalement une validation sur un site web (à créer) en ligne sur internet est à prévoir, car il constitue une cible de choix pour les pirates...

Réalisation : le but de ce projet est de mettre en place un site web simple en architecture 3

tiers à base de PHP / MySQL (l'utilisation d'un CMS est envisageable partiellement mais des développements spécifiques même simples sont à utiliser dans tous les cas). Une fois le site web mis en place, il faut identifier les principales attaques et donc les parades qu'il est possible de mettre en œuvre.

Livrables : Un manuel de type "howto" orienté sur les paramètres de configuration (Apache / PHP / MySQL – Postgres / scripts php) associés aux principales préconisations permettant d'aboutir à une liste détaillée des précautions à prendre ainsi qu'à l'ensemble des outils / scripts permettant l'audit.

Projet 6 : sécurisation réseau d'entreprise

Tuteur : N. Ouassini

Description Une entreprise souhaite sécuriser son réseau dont l'architecture est décrite comme suit :

- Un réseau local avec l'adressage 192.168.1.0/24
- Un accès WAN avec l'@ IP de sortie 193.95.66.1
- Deux serveurs FTP et HTTP publics ayant des @ dans le réseau 10.1.1.0/24 (à placer dans une zone DMZ).

Les clients dans le réseau local sont autorisés à naviguer sur le web (le protocole http est autorisé dans le sens LAN_ WAN). Parfois des clients distants doivent se connecter sur le réseau local pour faire des transactions sécurisées et ceci en utilisant une connexion à travers un VPN.

L'administrateur réseau doit accéder depuis la machine LAN vers la zone DMZ moyennant le protocole SSH. L'authentification entre le serveur SSH et son client doit se faire avec des clés, pas avec des mots de passe.

Travail demandé

1. Reproduire l'architecture de réseau en utilisant des machines virtuelles sous Linux. On vous demande de faire la connectique physique nécessaire ainsi que la configuration du routage pour tester la connectivité entre les trois zones (LAN, WAN et DMZ). Vérifier la création d'un segment LAN différent pour chaque zone de la maquette.
2. Etablir la politique de filtrage à adoptée pour contrôler l'accès vers les différentes zones de cette maquette.
3. Rendre le serveur http en HTTPS.
4. Installer et configurer IPFIRE comme firewall pour sécuriser l'accès à travers les différentes zones.
5. Installer et configurer snort comme sonde IDS sur la machine LAN avec l'interface graphique BASE.
6. Installer et configurer openvpn sur les deux machines LAN et WAN. Voici la configuration
Type d'encapsulation udp
Type du tunnel ethernet tunnel
Sous réseau du tunnel VPN
172.16.10.0/24
7. Installer et configurer openssh sur la machine DMZ et un client SSH sur la machine LAN et configurer une authentification par clé.
8. Réaliser une cartographie de la maquette réseau avec les adresses IP, les services, Toute la

plateforme est à base de Linux.

Tests :

- HTTPS: Tester l'accessibilité au service HTTPS à partir du LAN et du WAN.
- IPFIRE : Test d'accès aux différents services suivant à partir des différentes zones :
 - Accès vers le web à partir du LAN.
 - Accès vers les serveurs publics à partir du LAN et du WAN.
- Openvpn :
 - Test d'établissement du tunnel VPN entre les deux machines LAN et WAN.
 - Visualiser avec wireshark le trafic échangé entre ces deux machines pour l'établissement du tunnel VPN.
- Snort : lancer deux attaques arpspoofing et synflooding sur le réseau et visualiser les deux alertes sur l'interface graphique de snort.
- SSH : Test de l'ouverture d'un accès à distance à travers SSH depuis la machine LAN vers la DMZ.

Projet 7 : Mise à niveau d'une chaîne de production automatisée

Tuteur : N. Ouassini

Un administrateur réseaux d'une entreprise rencontre beaucoup de problème sur une chaîne de production automatisée.

Cette chaîne de production est gérée par un serveur avec un système d'exploitation Windows 2000NT avec beaucoup de problèmes listés ci-dessous :

1. Aucune mise à jours ni sécurité
2. Système d'exploitation obsolète
3. Machine avec carte mère processeur obsolète
4. Logiciel de gestion de la machine de production perdu

Quelles solutions pouvez-vous lui proposer pour sécuriser son système et lui venir en aide, sachant que l'administrateur cherche à mettre en place une stratégie de virtualisation et de redondance entre 2 machines virtuelles.

Projet 8 : Amélioration d'un réseau local

Tuteur : N. Ouassini

Une petite structure cherche à améliorer son infrastructure et perfectionner son réseau local, avec des protocoles pour faciliter le quotidien de ces employés

La mission qui attend l'administrateur est d'assurer aux utilisateurs

1. une continuité de service
2. la mise en place d'un serveur VPN
3. la configuration d'un wifi
4. une sécurité totale avec une authentification unique sur le réseau (vous avez le choix entre AD ou LDAP).

Projet 9 : Configuration automatisée de postes de travail

Tuteur : N. Ouassini

SOFTIN est un grossiste en solutions logicielles répondant aux besoins des PME/PMI en matière de gestion des systèmes d'information. Ces solutions sont vendues exclusivement sous forme électronique et offrent un bon compromis entre logiciels open source et grandes marques. Sur son site, à PARIS, SOFTIN organise des formations dédiées à certains produits de son catalogue, permettant ainsi à ses clients de mieux maîtriser les solutions logicielles proposées. Pour cela, l'entreprise met à disposition une dizaine de postes. Pour chaque nouvelle formation, la société veut remettre à neuf les postes de travail sans devoir se servir d'un support matériel. C'est dans ce cadre que SOFTIN a sollicité vos services.

La solution proposée consiste à implémenter, dans l'infrastructure existante, un rôle de déploiement de distributions Microsoft. Pour cela j'ai choisi d'utiliser le rôle WDS (Windows Deployment Services). L'objectif de ce projet est d'implémenter, sur le serveur dédié à la salle de formation, le rôle WDS et de déployer des systèmes d'exploitation sur les postes de formation. Du côté du serveur injectez 2 versions de Windows : Windows 7 Entreprise et Windows 10 Professionnel. Pour ce projet, vous n'allez vous servir que de deux postes utilisateurs. Sur le premier vous déployez Windows 7, et Windows 10 sur le second.

Quelles sont les exigences à respecter ? Les postes doivent être paramétrés pour démarrer sur la carte réseau par défaut afin de simplifier la tâche de l'administrateur lorsqu'il souhaitera déployer une image sur ceux-ci. En outre, ils doivent être joints au domaine de formation pendant l'installation du système d'exploitation. Quelles solutions sont disponibles ? Description de la solution retenue : Avantages, Inconvénients ?

Projet 10 : continuité de service

Tuteur : N. Ouassini

Aujourd'hui, que ce soit dans une petite ou une grande entreprise, une coupure internet peut vite coûter cher à la structure professionnelle qui la subit. En effet, le coût potentiel d'une panne due à la défaillance d'un serveur web clé est significatif ; le coût horaire d'une telle panne, même pour une petite entreprise se chiffre en milliers d'euros.

Le coût général d'une telle panne dépend beaucoup de l'organisation (son utilisation d'internet, sa dépendance à certaines applications web...) mais ces pannes poussent les clients à aller ailleurs, laissent les employés inactifs et frustrés et peuvent être extrêmement préjudiciables à la réputation d'une entreprise. Il est impératif que les entreprises évaluent l'impact d'une défaillance et prennent les mesures appropriées pour minimiser le risque de défaillance d'un serveur.

Étant administrateur système d'une de ces entreprise, votre rôle est de mettre en place le load balancing pour assurer une continuité de service.