

Séminaire de 2 jour(s)
Réf : AUR

Participants

Ce cours s'adresse aux architectes de réseaux, aux chefs de projets, aux responsables de systèmes d'information, aux ingénieurs réseaux.

Pré-requis

Connaissances de base dans le domaine des réseaux.

Prix 2012 : 1775€ HT

Dates des sessions

Paris

5 avr. 2012, 7 juin 2012
4 oct. 2012, 6 déc. 2012

Audit et analyse des réseaux

OBJECTIFS

Le trafic sur les réseaux de données est composé de nombreuses applications dont les volumes sont en général inversement proportionnels à l'importance qu'ils revêtent pour l'entreprise. Ce cours se propose de donner les clés, techniques et pratiques, de l'analyse des réseaux. Les différents types d'outils disponibles aujourd'hui seront présentés et analysés. Des exemples concrets illustreront comment, à travers une méthodologie précise, un système de communication multi-applications peut être contrôlé efficacement pour apporter aux applications le niveau de service indispensable.

1) Le contexte technique

2) La gestion du trafic

3) Sécurité

4) La méthodologie

5) La qualité de service

6) Les outils d'audit et de Qos

1) Le contexte technique

Les architectures de réseaux

- Rappels sur les architectures de protocoles.
- Le réseau d'entreprise, les réseaux virtuels, les techniques de VPN.
- Le réseau longue distance, les services des ISP.
- Les réseaux d'accès : xDSL, WiFi, WiMax.

Les paramètres clés du réseau

- Notion d'échantillonnage, problématiques de la mesure.
- Les débits, valeurs moyennes, rafales.
- Le nombre de paquets par seconde (PPS).
- La distribution de la taille des paquets.
- Le volume des données, les taux de perte.
- Les temps de réponse (RTT) au niveau réseau, au niveau des applications.

L'analyse des goulets d'étranglement

- Le terminal.
- Le réseau d'accès.
- Le cœur de réseaux.
- La performance des équipements (pps, statefull context...).
- Les serveurs.

Métriologie active vs métriologie passive

- Que peut-on mesurer avec des éléments passifs ?
- Qu'apportent les mesures actives ?
- La limite des méthodes de collecte.
- Le passage à l'échelle.

Métriologie : l'impact des couches du modèle en couches

- Les approches purement réseau (niveau 2-3-4*).
- Les approches applicatives (niveau 7) : la classification applicative.
- L'impact applicatif sur le réseau.

L'état de la normalisation

- Les groupes de l'IETF : IPSAMP, IPPM, IPFIX...
- Pourquoi tant d'efforts différents.
- Les approches SNMP.
- Les sondes RMON.

La notion de ticket

- Garder une trace des échanges.
- La sécurité et ses obligations légales.
- Le cas de la téléphonie sur IP et de la messagerie.
- La réglementation française.

Les pistes de recherche

- Packet pair.
- Corrélations statistiques.

2) La gestion du trafic

Les outils

- Les méthodes de contrôle d'admission.
- RED, WFQ, leaky bucket, token bucket, etc.
- Impact des technologies sur les comportements.

Capacity planning

- Prévoir les évolutions.
- Garantir les performances.

- Contrôler les engagements de service.

Des outils pour la gestion de parcs informatiques

- Analyse des systèmes d'exploitation.
- Analyse des applications.
- Découverte de topologies.

3) Sécurité

- Les principes de sécurité liés au trafic : les firewalls.
- Les approches Statefull et Stateless.
- Les limites des systèmes actuels.
- La détection d'intrusion : un audit en temps réel.
- La conformité du trafic aux règles du firewall.

4) La méthodologie

- Les étapes importantes.
- Pourquoi une méthodologie ?
- L'audit permanent.

5) La qualité de service

- Notions de SLA.
- QoS vs CoS.
- Le modèle de bout en bout.

6) Les outils d'audit et de Qos

Audits ponctuels

- Pour quoi faire ? Exemple.
- La qualification d'un réseau pour des usages.

Audits structurels

- Le réseau est un système qui doit être géré et contrôlé.
- Les performances et l'impact financier.

Analyseurs, systèmes de gestion, Traffic Shapers, un état du marché

- Acterna/Sniffer Pro.
- Ethereal/TCPDUMP.
- RMON.
- MRTG.
- Infovista/Concord/Qualaby.
- Qosmos.
- Qosmetrix.
- NetFlow v5, v7, v8, v9.
- Ntop.
- Packeteer.
- Ipanéma.
- Streamcore.

Bilan et comparaison synthétique