Supervision

Bruno BEAUFILS

2021/2022

Bruno BEAUFILS

- Maître de conférences en informatique
- Université de Lille
  - IUT / Département informatique
    - Systèmes d'exploitation
    - Réseaux
  - CRIStAL (*Centre de Recherche en Informatique, Signal et Automatique de Lille*)
    - Systèmes Multi-Agents (Théorie des jeux, Finance computationnelle)
    - Intelligence artificielle distribuée / Vie artificielle
    - Réseaux de co-auteurs
    - Médiation scientifique
- Contacts
  - bureau : IUTA-4A49
  - email : `bruno.beaufils@univ-lille.fr`
  - web : `http://beaufils.u-lille.fr`
  - twitter : @brunobeaufils
  - mastodon : @beaufils@mastodon.social
  - téléphone : `03 59 63 21 57`

Objectifs du cours

- Comprendre les principes de la supervision (système et réseau)
  - collecte
  - détection
  - alertes
  - prévision
- Connaître les outils utiles à la supervision
  - journaux
  - planificateur
  - SNMP
  - RRDtool
- Être capable de mettre en œuvre des solutions de supervision

Fonctionnement

- Prérequis
  - *programmation* **shell** de base (Bourne)
  - infrastructure **TCP/IP**
- Déroulement : cours et TP
  - 11/01 (13h30 à 17h30)
  - 18/01 (13h30 à 17h30)
  - 25/01 (13h30 à 17h30)
  - 01/02 (13h30 à 17h30)
  - 08/02 (13h30 à 17h30)
  - 22/02 (13h30 à 17h30)
  - 01/03 (13h30 à 17h30)
- Évaluation : lors de la dernière séance
  - **1 DS** (1 heure) ..... *coefficient 0,5*
  - **TPs** ..... *coefficient 0,5*
- Ressources

`http://supervision.iutinfo.fr`

Références

Administration système

- **Cours CS615 – Aspects of System Administration**,
  - supports de cours par *Jan SCHAUMAN*, Stevens Institute of Technology
  - Vidéos : `https://invidious.fdn.fr/c/cs615asa/playlists`
- **Principles of System Administration**
  - livre par *Jan SCHAUMAN*, Stevens Institute of Technology
  - `https://www.netmeister.org/book`
  - livre en cours de rédaction *permanente*
- **The Debian Administrator's Handbook**
  - livre par *Raphaël HERTZOG* et *Roland MAS*
  - disponible librement (et gratuitement) en ligne et en français
  - basé sur la version *Buster* (10) de Debian pour l'instant
- **Les cahiers de l'Admin BSD, les dessous d'UNIX**
  - livre par *Emmanuel DREYFUSS*

Références (suite)

Supervision

- **Essential SNMP**
  - livre par *Douglas MAURO* et *Kevin SCHMIDT*
- **Syslog : The Complete System Administrator Guide**
  - article par *SCHKN*
- **Supervision - Monitoring**
  - supports de cours par *Lucas NUSSBAUM*, Université de Lorraine
  - Licence professionnelle *Administration de systèmes, réseaux et applications à base de logiciels libres* (ASRALL)

Divers

- **Cyberstructure : l'Internet, un espace politique**
  - livre par *Stéphane BORTZMEYER*
  - la lecture régulière de son blog est saine : `https://www.bortzmeyer.org`
- **How the internet really works**
  - livre par *ARTICLE 19*
- **Les cahiers du débutant sur Debian GNU/Linux Bullseye**
  - livre par *ARPINUX*
  - disponible librement (et gratuitement) en ligne
  - vraiment pour les grands débutants mais utile à lire

Le métier d'adminsys

Aucune définition absolue mais quelques caractéristiques :

- au service **d'autres humains**
  - importance des relations avec les utilisateurs
  - savoir s'adapter et rester calme
- **ingrat**
  - invisible quand tout va bien
  - très visible quand il y a un problème
- difficile à apprendre juste avec un cours
  - importance de l'**expérience**

Une plus longue introduction en vidéo

- **CS615 - Week 01 - Segment 02 - The job of a System Administrator**

Tâches d'un adminsys (objectifs)

Faire fonctionner les ordinateurs (le réseau/le système informatique)

Par exemple :

- Gérer un ensemble de machines/services et son utilisation
  - Installation/Configuration de machines *(ordiphones, stations, **serveurs**, VM)*
  - Gestion de comptes utilisateurs *authentification, autorisation, accès*
  - **Déploiement** de logiciels *(installation, configuration, mise à jour)*
  - **Résolution problèmes** des utilisateurs *(incidents, formation, documentations)*
- Assurer la **sécurité des données et services** ***CIA***
  1. Confidentialité
  2. Intégrité
  3. disponibilité (*Availability*)
- **Surveiller le fonctionnement**
  - des équipements *(serveurs, poste de travail, éléments de réseau, téléphone, etc.)*
  - des systèmes *(mémoire, CPU, système de fichiers, etc.)*
  - des services *(serveur web, BDD, emails, etc.)*
  - du réseau *(lattence, congestion, etc.)*

AUTOMATISER!

Tâches d'un adminsys (objectifs)

Faire fonctionner les ordinateurs (le réseau/le système informatique)

Par exemple :

- Gérer un ensemble de machines/services et son utilisation
  - Installation/Configuration de machines *(ordiphones, stations, **serveurs**, VM)*
  - Gestion de comptes utilisateurs *authentification, autorisation, accès*
  - **Déploiement** de logiciels *(installation, configuration, mise à jour)*
  - **Résolution problèmes** des utilisateurs *(incidents, formation, documentations)*
- Assurer la **sécurité des données et services** *CIA*
  1. Confidentialité
  2. Intégrité
  3. disponibilité (*Availability*)
- **Surveiller le fonctionnement**
  - des équipements *(serveurs, poste de travail, éléments de réseau, téléphone, etc.)*
  - des systèmes *(mémoire, CPU, système de fichiers, etc.)*
  - des services *(serveur web, BDD, emails, etc.)*
  - du réseau *(lattence, congestion, etc.)*

AUTOMATISER!

Tâches d'un adminsys (objectifs)

Faire fonctionner les ordinateurs (le réseau/le système informatique)

Par exemple :

- Gérer un ensemble de machines/services et son utilisation
  - Installation/Configuration de machines *(ordiphones, stations, **serveurs**, VM)*
  - Gestion de comptes utilisateurs *authentification, autorisation, accès*
  - **Déploiement** de logiciels *(installation, configuration, mise à jour)*
  - **Résolution problèmes** des utilisateurs *(incidents, formation, documentations)*
- Assurer la **sécurité des données et services** ***CIA***
  1. Confidentialité
  2. Intégrité
  3. disponibilité (*Availability*)
- **Surveiller le fonctionnement**
  - des équipements *(serveurs, poste de travail, éléments de réseau, téléphone, etc.)*
  - des systèmes *(mémoire, CPU, système de fichiers, etc.)*
  - des services *(serveur web, BDD, emails, etc.)*
  - du réseau *(lattence, congestion, etc.)*

AUTOMATISER!

Tâches d'un adminsys (objectifs)

Faire fonctionner les ordinateurs (le réseau/le système informatique)

Par exemple :

- Gérer un ensemble de machines/services et son utilisation
  - Installation/Configuration de machines *(ordiphones, stations, **serveurs**, VM)*
  - Gestion de comptes utilisateurs *authentification, autorisation, accès*
  - **Déploiement** de logiciels *(installation, configuration, mise à jour)*
  - **Résolution problèmes** des utilisateurs *(incidents, formation, documentations)*
- Assurer la **sécurité des données et services** ***CIA***
  1. Confidentialité
  2. Intégrité
  3. disponibilité (*Availability*)
- **Surveiller le fonctionnement**
  - des équipements *(serveurs, poste de travail, éléments de réseau, téléphone, etc.)*
  - des systèmes *(mémoire, CPU, système de fichiers, etc.)*
  - des services *(serveur web, BDD, emails, etc.)*
  - du réseau *(lattence, congestion, etc.)*

AUTOMATISER!

Tâches d'un adminsys (objectifs)

Faire fonctionner les ordinateurs (le réseau/le système informatique)

Par exemple :

- Gérer un ensemble de machines/services et son utilisation
  - Installation/Configuration de machines *(ordiphones, stations, **serveurs**, VM)*
  - Gestion de comptes utilisateurs *authentification, autorisation, accès*
  - **Déploiement** de logiciels *(installation, configuration, mise à jour)*
  - **Résolution problèmes** des utilisateurs *(incidents, formation, documentations)*
- Assurer la **sécurité des données et services** ***CIA***
  1. Confidentialité
  2. Intégrité
  3. disponibilité (*Availability*)
- **Surveiller le fonctionnement**
  - des équipements *(serveurs, poste de travail, éléments de réseau, téléphone, etc.)*
  - des systèmes *(mémoire, CPU, système de fichiers, etc.)*
  - des services *(serveur web, BDD, emails, etc.)*
  - du réseau *(lattence, congestion, etc.)*

AUTOMATISER!

Tâches d'un adminsys (moyens)

- **Gérer l'hétérogénéité** mais donner une interface standard
  - inventorier
  - outiller
  - interfacer
- **Ne pas trop s'épuiser** pour **rester calme** face aux situations/utilisateurs
  - mettre en place des procédures
  - documentations
  - automatiser (scripts, etc.)
- **Faire de la veille**, *i.e.* suivre les évolutions des techniques/technologies
  - prototyper
  - maquetter
- Utiliser une **méthode scientifique**, *i.e.* connaître et utiliser :
  - les rasoirs (Ockam et Hanlon)
  - les lois (Murphy et Causalité)
  - des règles (**KISS** : *Keep It Simple, Stupid!*)

Une plus longue introduction en vidéo :

- **CS615 - Week 01 - Segment 03 - SysAdmin Core Principles and Rules**

Tâches d'un adminsys (moyens)

- **Gérer l'hétérogénéité** mais donner une interface standard
  - inventorier
  - outiller
  - interfacer
- **Ne pas trop s'épuiser** pour **rester calme** face aux situations/utilisateurs
  - mettre en place des procédures
  - documentations
  - automatiser (scripts, etc.)
- **Faire de la veille**, *i.e.* suivre les évolutions des techniques/technologies
  - prototyper
  - maquetter
- Utiliser une **méthode scientifique**, *i.e.* connaître et utiliser :
  - les rasoirs (Ockam et Hanlon)
  - les lois (Murphy et Causalité)
  - des règles (**KISS** : *Keep It Simple, Stupid!*)

Une plus longue introduction en vidéo :

- **CS615 - Week 01 - Segment 03 - SysAdmin Core Principles and Rules**

Tâches d'un adminsys (moyens)

- **Gérer l'hétérogénéité** mais donner une interface standard
  - inventorier
  - outiller
  - interfacer
- **Ne pas trop s'épuiser** pour **rester calme** face aux situations/utilisateurs
  - mettre en place des procédures
  - documentations
  - automatiser (scripts, etc.)
- **Faire de la veille**, *i.e.* suivre les évolutions des techniques/technologies
  - prototyper
  - maquetter
- Utiliser une **méthode scientifique**, *i.e.* connaître et utiliser :
  - les rasoirs (Ockam et Hanlon)
  - les lois (Murphy et Causalité)
  - des règles (**KISS** : *Keep It Simple, Stupid!*)

Une plus longue introduction en vidéo :

- **CS615 - Week 01 - Segment 03 - SysAdmin Core Principles and Rules**

Tâches d'un adminsys (moyens)

- **Gérer l'hétérogénéité** mais donner une interface standard
  - inventorier
  - outiller
  - interfacer
- **Ne pas trop s'épuiser** pour **rester calme** face aux situations/utilisateurs
  - mettre en place des procédures
  - documentations
  - automatiser (scripts, etc.)
- **Faire de la veille**, *i.e.* suivre les évolutions des techniques/technologies
  - prototyper
  - maquetter
- Utiliser une **méthode scientifique**, *i.e.* connaître et utiliser :
  - les rasoirs (Ockam et Hanlon)
  - les lois (Murphy et Causalité)
  - des règles (**KISS** : *Keep It Simple, Stupid!*)

Une plus longue introduction en vidéo :

- CS615 - Week 01 - Segment 03 - SysAdmin Core Principles and Rules

Tâches d'un adminsys (moyens)

- **Gérer l'hétérogénéité** mais donner une interface standard
  - inventorier
  - outiller
  - interfacer
- **Ne pas trop s'épuiser** pour **rester calme** face aux situations/utilisateurs
  - mettre en place des procédures
  - documentations
  - automatiser (scripts, etc.)
- **Faire de la veille**, *i.e.* suivre les évolutions des techniques/technologies
  - prototyper
  - maquetter
- Utiliser une **méthode scientifique**, *i.e.* connaître et utiliser :
  - les rasoirs (Ockam et Hanlon)
  - les lois (Murphy et Causalité)
  - des règles (**KISS** : *Keep It Simple, Stupid!*)

Une plus longue introduction en vidéo :

- **CS615 - Week 01 - Segment 03 - SysAdmin Core Principles and Rules**

Documentation

L'administrateur doit **produire** de l'information *(cf cours sur les outils)*

- procédures
- documentation (des configurations, des installations)
- base de connaissances

L'administrateur système doit savoir **trouver** l'information :

1. grâce à son savoir
2. grâce aux documentations :
   1. documentations, standards `man`, `RFC`
   2. livres
3. via les gens qui savent :
   - collègues
   - bases de connaissances
     - forum de discussions
     - liste de diffusions de mails
     - moteurs de recherche (stackexchange, etc.)

RTFM = Read The *Fantastic* Manual

Documentation

L'administrateur doit **produire** de l'information *(cf cours sur les outils)*

- procédures
- documentation (des configurations, des installations)
- base de connaissances

L'administrateur système doit savoir **trouver** l'information :

1. grâce à son savoir
2. grâce aux documentations :
   1. documentations, standards `man`, `RFC`
   2. livres
3. via les gens qui savent :
   - collègues
   - bases de connaissances
     - forum de discussions
     - liste de diffusions de mails
     - moteurs de recherche (stackexchange, etc.)

RTFM = Read The *Fantastic* Manual

Documentation

L'administrateur doit **produire** de l'information *(cf cours sur les outils)*

- procédures
- documentation (des configurations, des installations)
- base de connaissances

L'administrateur système doit savoir **trouver** l'information :

1. grâce à son savoir
2. grâce aux documentations :
   1. documentations, standards `man`, RFC
   2. livres
3. via les gens qui savent :
   - collègues
   - bases de connaissances
     - forum de discussions
     - liste de diffusions de mails
     - moteurs de recherche (stackexchange, etc.)

RTFM = Read The *Fantastic* Manual

Documentation

L'administrateur doit **produire** de l'information *(cf cours sur les outils)*

- procédures
- documentation (des configurations, des installations)
- base de connaissances

L'administrateur système doit savoir **trouver** l'information :

1. grâce à son savoir
2. grâce aux documentations :
   1. documentations, standards `man`, RFC
   2. livres
3. via les gens qui savent :
   - collègues
   - bases de connaissances
     - forum de discussions
     - liste de diffusions de mails
     - moteurs de recherche (stackexchange, etc.)

RTFM = Read The *Fantastic* Manual

Documentation

L'administrateur doit **produire** de l'information *(cf cours sur les outils)*

- procédures
- documentation (des configurations, des installations)
- base de connaissances

L'administrateur système doit savoir **trouver** l'information :

1. grâce à son savoir
2. grâce aux documentations :
   1. documentations, standards `man`, RFC
   2. livres
3. via les gens qui savent :
   - collègues
   - bases de connaissances
     - forum de discussions
     - liste de diffusions de mails
     - moteurs de recherche (stackexchange, etc.)

RTFM = Read The *Fantastic* Manual

Savoir être et savoir faire

- Comportement
  - **savoir lire**
  - être **patient**
  - être **curieux**
  - se méfier des modes

- Résoudre les problèmes avec **méthode**
  - détection
  - élimination des causes possibles
    - remonter les couches

Savoir être et savoir faire

- Comportement
  - **savoir lire**
  - être **patient**
  - être **curieux**
  - se méfier des modes

- Résoudre les problèmes avec **méthode**
  - détection
  - élimination des causes possibles
    - remonter les couches

Quelques commandes à maîtriser

- Systèmes
  - shell (*bash*)
  - filtres standards (`grep`, `cut`, `tr`, `head`, `tail`, `sort`, `uniq`, `tee`)
  - `vi`, `sed`
  - expressions régulières
  - `ssh`
  - `cron`
  - `watch`

- Réseaux
  - `ping` tester la présence/réponse d'une machine
  - `ip` (ou `ifconfig`, `route`) obtenir la configuration réseau
  - `netstat` obtenir des informations réseaux et noyau
  - `traceroute` tracer le chemin des paquets
  - `dig` (ou `nslookup`) interroger le DNS
  - `whois` interroger les bureaux d'enregistrements
  - `tcpdump` / `wireshark` capturer les paquets réseaux (inspecter)

Quelques commandes à maîtriser

- Systèmes
  - shell (*bash*)
  - filtres standards (`grep`, `cut`, `tr`, `head`, `tail`, `sort`, `uniq`, `tee`)
  - `vi`, `sed`
  - expressions régulières
  - `ssh`
  - `cron`
  - `watch`

- Réseaux
  - `ping` — tester la présence/réponse d'une machine
  - `ip` (ou `ifconfig`, `route`) — obtenir la configuration réseau
  - `netstat` — obtenir des informations réseaux et noyau
  - `traceroute` — tracer le chemin des paquets
  - `dig` (ou `nslookup`) — interroger le DNS
  - `whois` — interroger les bureaux d'enregistrements
  - `tcpdump` / `wireshark` — capturer les paquets réseaux (inspecter)

Généralités

- **Gestion** et **Surveillance**
  - services primordiaux
  - complexité et hétérogénéité
  - **les méthode ad-hoc (cf rappels) passent difficilement à l'échelle**
- Cadre général de gestion du modèle OSI (ISO/IEC 7498-4)
  - gestion des **performances**
  - gestion des **configurations**
  - gestion de la **comptabilité**
  - gestion des **anomalies**
  - gestion de la **sécurité**
- **Types de supervision**
  - matérielle
  - réseau
  - système
  - applicative
  - procédurale

Généralités

- **Gestion** et **Surveillance**
  - services primordiaux
  - complexité et hétérogénéité
  - **les méthode ad-hoc (cf rappels) passent difficilement à l'échelle**
- Cadre général de gestion du modèle OSI (ISO/IEC 7498-4)
  - gestion des **performances**
  - gestion des **configurations**
  - gestion de la **comptabilité**
  - gestion des **anomalies**
  - gestion de la **sécurité**
- Types de supervision
  - matérielle
  - réseau
  - système
  - applicative
  - procédurale

Généralités

- **Gestion** et **Surveillance**
  - services primordiaux
  - complexité et hétérogénéité
  - **les méthode ad-hoc (cf rappels) passent difficilement à l'échelle**
- Cadre général de gestion du modèle OSI (ISO/IEC 7498-4)
  - gestion des **performances**
  - gestion des **configurations**
  - gestion de la **comptabilité**
  - gestion des **anomalies**
  - gestion de la **sécurité**
- **Types de supervision**
  - matérielle
  - réseau
  - système
  - applicative
  - procédurale

Plusieurs approches

Standards et normes

- ISO/IEC - OSI - **CMIP**
  - Common Management Information Protocol
  - Histoire : Norme ISO/IEC 7498-4 (cadre de gestion du modèle OSI) puis CMIP
  - protocole de gestion de réseau
  - peu utilisé parce que lourd à mettre en place
- Internet - IETF - **SNMP**
  - **Simple** Network Management Protocol
  - Histoire :
    - SGMP (Simple Gateway Monitoring Protocol) pas implémenté
    - puis SNMP (v1, v2c, v2p, v2u, v3)
  - Très répandu parce que facile à implémenter/mettre en place
  - Objectifs
    - disponibilité (sur tout type de matériels)
    - extensibilité
    - robustesse (utilise UDP)

Autres outils

- **ICMP** réseau niveau 3 seulement
- IPMI (Intel)
- **Bonnes pratiques** (BCP RFC, ITIL, etc.)

Plusieurs approches

Standards et normes

- ISO/IEC - OSI - **CMIP**
  - Common Management Information Protocol
  - Histoire : Norme ISO/IEC 7498-4 (cadre de gestion du modèle OSI) puis CMIP
  - protocole de gestion de réseau
  - peu utilisé parce que lourd à mettre en place
- Internet - IETF - **SNMP**
  - **Simple** Network Management Protocol
  - Histoire :
    - SGMP (Simple Gateway Monitoring Protocol) pas implémenté
    - puis SNMP (v1, v2c, v2p, v2u, v3)
  - Très répandu parce que facile à implémenter/mettre en place
  - Objectifs
    - disponibilité (sur tout type de matériels)
    - extensibilité
    - robustesse (utilise UDP)

Autres outils

- **ICMP** réseau niveau 3 seulement
- IPMI (Intel)
- **Bonnes pratiques** (BCP RFC, ITIL, etc.)

Plusieurs approches

Standards et normes

- ISO/IEC - OSI - **CMIP**
  - Common Management Information Protocol
  - Histoire : Norme ISO/IEC 7498-4 (cadre de gestion du modèle OSI) puis CMIP
  - protocole de gestion de réseau
  - peu utilisé parce que lourd à mettre en place
- Internet - IETF - **SNMP**
  - **Simple** Network Management Protocol
  - Histoire :
    - SGMP (Simple Gateway Monitoring Protocol) pas implémenté
    - puis SNMP (v1, v2c, v2p, v2u, v3)
  - Très répandu parce que facile à implémenter/mettre en place
  - Objectifs
    - disponibilité (sur tout type de matériels)
    - extensibilité
    - robustesse (utilise UDP)

Autres outils

- **ICMP** réseau niveau 3 seulement
- IPMI (Intel)
- **Bonnes pratiques** (BCP RFC, ITIL, etc.)

Objectifs

- **connaître l'état global d'un équipement**
  - actif,
  - inactif,
  - partiellement opérationnel
- **gérer les évènements exceptionnels**
  - perte d'un lien réseau
  - arrêt brutal d'un équipement
- **analyser différents métriques afin d'anticiper les problèmes futurs**
  - engorgement réseau...
- **agir sur certains éléments de la configuration des équipements**

Objectifs

- **connaître l'état global d'un équipement**
  - actif,
  - inactif,
  - partiellement opérationnel
- **gérer les évènements exceptionnels**
  - perte d'un lien réseau
  - arrêt brutal d'un équipement
- **analyser différents métriques afin d'anticiper les problèmes futurs**
  - engorgement réseau...
- **agir sur certains éléments de la configuration des équipements**

Objectifs

- **connaître l'état global d'un équipement**
  - actif,
  - inactif,
  - partiellement opérationnel
- **gérer les évènements exceptionnels**
  - perte d'un lien réseau
  - arrêt brutal d'un équipement
- **analyser différents métriques afin d'anticiper les problèmes futurs**
  - engorgement réseau...
- **agir sur certains éléments de la configuration des équipements**

Objectifs

- **connaître l'état global d'un équipement**
  - actif,
  - inactif,
  - partiellement opérationnel
- **gérer les évènements exceptionnels**
  - perte d'un lien réseau
  - arrêt brutal d'un équipement
- **analyser différents métriques afin d'anticiper les problèmes futurs**
  - engorgement réseau...
- **agir sur certains éléments de la configuration des équipements**

Journaux (*logs*)

- Garder une trace de chaque action produite sur un système
  - débogage
  - surveillance
  - comptabilité
  - analyse
- Solution la plus simple
  - chaque **service**
    - enregistre un **message**
    - avant (après) de faire une **action**
  - dans des fichiers **textes** simples
- Sous UNIX il existe un système pour enregistrer ce genre de message
  - `syslog`
  - Linux avec `systemd` : `journalctl(1)`

Syslog (généralités)

- Protocole de communication de message de journalisation RFC 5424
  - produire
  - transmettre
  - collecter
- Objectifs initiaux
  - Architecture de communication
  - Format de message
  - Gestion de la fiabilité et de l'authenticité des messages

- Références
  - Syslog : The Complete System Administrator Guide

Syslog (détails)

- Message **horodaté** défini selon
  - **priority**
    - emerg, alert, crit, err, warning, notice, info, debug
  - **facility**
    - kern, user, mail, daemon, auth, syslog, etc.
- Stockage
  - généralement dans `/var/log`
  - serveur centralisé
  - rotation des fichiers
    - `logrotate(8)`
- API et commande
  - `syslog(3)`
  - `logger(1)`