Administración de redes y sistemas
CASO 2006/2007

Author: Sergio Talens-Oliag
Contact: sto@uv.es
Date: 17 de enero de 2007

1. Resumen

En esta presentación introduciremos qué entendemos por administración de redes y sistemas, qué tareas lleva aparejadas y que técnicas podemos emplear para realizarlas de modo más eficiente.

Los contenidos de la presentación se han extraído del libro *Principles of Network and System Administration, Second Edition*. Mark Burgess. John Willey and Sons Ltd., 2004.

2. Administración de redes y sistemas (1)

- Es una rama de la ingeniería que se ocupa de la gestión de sistemas formados por computadoras y usuarios; trata de organizar redes de ordenadores, hacer que funcionen y mantenerlos en marcha a pesar de lo que hagan sus usuarios.
- El objetivo del administrador de sistemas es que sus usuarios puedan realizar sus tareas sin problemas; al definir las políticas a implantar en sus sistemas debe pensar en las necesidades de todos ellos, no solo en las de unos pocos.

3. Administración de redes y sistemas (2)

- El trabajo de un administrador implica tratar con hardware, software, soporte a usuarios y realizar tareas de diagnostico, prevención y reparación de problemas.
- Podemos decir que el termino administración de sistemas se refiere a la gestión de computadoras estén o no conectadas en red, mientras que el de administración de redes se refiere a la gestión de dispositivos de la infraestructura de red (*routers* y *switches*).

4. Desafíos del administrador de sistemas

- Diseño de redes lógicas y eficientes.
- Gestión de instalaciones de gran numero de equipos de modo que se puedan actualizar fácilmente.
- Decidir que servicios y configuraciones se precisan.
- Planear e implantar medidas de seguridad adecuadas.
- Proporcionar un entorno agradable a los usuarios.
- Disponer de estrategias para resolver los problemas que se plantean.

- Mantenerse al día y usar el conocimiento que se adquiere.

5. Principios de la administración de sistemas

- Definición de políticas: especifican lo que queremos conseguir y que vamos a permitir.
- Previsibilidad: los sistemas deben ser previsibles, ya que esto es la base para sean fiables y nos den confianza y seguridad.
- Escalabilidad: un sistema escalable es el que crece de acuerdo con la política y continua funcionando de modo previsible incluso cuando aumenta de tamaño.

6. Elementos de un sistema

- Los principales elementos de un sistema en red son los usuarios, los ordenadores y el hardware de red (routers, switches, cables, ...).
- Los ordenadores tienen componentes hardware (discos, memoria, fuente de alimentación, ...) y software (sistemas operativos y aplicaciones de usuario).
- La red puede ser solo de área local o conectarse con resto del mundo a través de Internet.

7. Gestión de equipos

- Sistemas Operativos a instalar y dar soporte.
- ¿Cómo mantenemos los sistemas? ¿Usamos el modelo y las herramientas del fabricante o definimos un modelo propio? ¿Configuramos todos los equipos igual o permitimos diferencias?
- Automatización de la instalación y actualización de software.
- Uso de herramientas de catalogación y auditoría del software instalado en los sistemas.

8. Gestión de usuarios

- Uso de sistemas de directorio para tener los mismos usuarios en todos los equipos. Se debe controlar el uso de usuarios locales y si se permite o no a los usuarios gestionar sus propios equipos.
- Tareas del administrador:
  - altas, bajas y modificaciones de la información de los usuarios; control de permisos y niveles de acceso
  - soporte técnico: formación, documentación y gestión de incidencias.

9. Gestión de red

- Diseño de la topología de la red teniendo en consideración aspectos de seguridad (red privada vs. DMZ) y de hardware (switches, cables, ...).
- Uso de sistemas de monitorización para el hardware de red (SMTP).
- A nivel de aplicación, uso de sistemas de directorio para control de usuarios, asignación de nombres y direcciones, etc.

10. Configuración y mantenimiento

- Uso de recursos compartidos para simplificar el mantenimiento (sistemas de archivos de red, servidores de impresión, etc.)
- Gestión configuraciones: manual vs. automática, control de versiones para mantener históricos.
- Uso de sistemas de programación de tareas y/o agentes para automatizar monitorización (los datos se pueden emplear para ajustar el rendimiento de los sistemas) y los cambios.

11. Gestión de cambios

- Documentación de los cambios: ¿qué?, ¿cómo? y ¿por qué se cambia?
- Diseño de casos de prueba para validar los cambios a realizar.
- Pruebas de actualización (si es posible) y definición de un sistema de vuelta atrás en caso de problemas al aplicarlos (deshacer cambios en ficheros, recuperar datos y programas de un backup, etc.).

12. Tolerancia a fallos y alta disponibilidad

- Sistemas de monitorización que detectan y avisan de los fallos, poniendo en marcha sistemas alternativos si es posible (sistemas de HA).
- Uso de sistemas redundantes a todos los niveles posibles: RAID (discos), servidores primarios y secundarios (DNS, LDAP, ...), sistemas de balanceo de carga automáticos, ...
- Problemas: la alta disponibilidad y la tolerancia a fallos son caras.

13. Seguridad: Objetivos

- Los tres objetivos fundamentales de la seguridad informática son:
  - Confidencialidad; el acceso a los activos del sistema debe estar limitado a usuarios autorizados.
  - Integridad; los activos del sistema solo pueden ser borrados o modificados por usuarios autorizados.
  - Disponibilidad; el acceso a los activos en un tiempo razonable esta garantizado para usuarios autorizados.
- Para conseguir esos objetivos deberemos definir e implantar políticas de seguridad.

14. Seguridad: tareas para definir e implantar políticas

- Identificar los activos a proteger e implantar medidas para protegerlos.
- Evaluar riesgos y determinar niveles de confianza; uso de sistemas de control de acceso y de detección y corrección de errores redundantes.
- Respuesta ante ataques preventivas y reactivas; sistemas monitorización y regulación.
- Validar supuestos y evitar dependencias e inconsistencias innecesarias.

15. Seguridad: aspectos a estudiar

- Seguridad física.
- Autentificaron: Criptografía y PKI.
- Seguridad de los datos: backups.
- Seguridad a nivel de red: firewalls.
- Seguridad a nivel de transporte: SSH, TLS, ...
- Seguridad a nivel de aplicación: auditoría.
- Monitorización : IDS de host y de red.