Agosto 2019

Manual para la implementación de sistemas de monitoreo con sistemas operativos Linux

Versión 1.0

Índice

1. Introducción

La implementación de un sistema de monitoreo confiable que sirva como referencia para la obtención de datos fiables sobre la operación de una red de datos siempre tiene muchos consideraciones específicas que normalmente no son tomadas en cuenta al momento de la implementación, muchas de las cuales provocan falsos positivos, problemas en la operación de los servidores y en casos extremos se vuelven un punto de preocupación en la seguridad de nuestra red, ya que estos tienen acceso a todos los rincones de la red y en teoría están bajo control estricto de seguridad.

El presente manual pretende servir de guía para la implementación de un sistema de monitoreo en la UNAM de forma estándar que permita a otros tener un punto de partida en la implementación de los sistemas de monitoreo que se utilizan con apoyo de servidores que los mismos administradores de redes locales de una unidad académica puedan utilizar en pro de la operación de las aplicaciones de monitoreo que utilizan.

2. Objetivo

Ofrecer una guía práctica a forma de manual de las consideraciones necesarias para que los administradores que tengan a su cargo infraestructura de telecomunicaciones, puedan utilizar como línea base en la implementación de servidores de monitoreo, las cuales permitan garantizar la fiabilidad de la operación de las aplicaciones de monitoreo y la seguridad en la operación de las plataformas que lo soportan.

3. Alcance

Ofrecer una serie de pasos a seguir para la implementación de un sistema de monitoreo sobre servidores Linux que permitan a los encargados controlar el sistema operativo donde se encuentran las aplicaciones de monitoreo.

Ofrecer un serie de requisitos que sirvan como plantilla o para que todos los servidores encargados del monitoreo de la red cumplan para mantenerlo bajo control

Servir de punto de partida para buenas prácticas de implementación y para que en caso de que se requiera el soporte para la revisión de los mismos, se sepa dónde se encuentra implementado cada módulo/aplicación o complemento dentro del sistema operativo.

Generar buenas prácticas en la operación durante la actualización de las aplicaciones para que estas requieran el menor mantenimiento y aprovechen al máximo los recursos de las plataformas sin afectar su funcionamiento.

4. Establecimiento de políticas locales de implementación de los servidores de monitoreo en las redes académicas

En todas las organizaciones se generan políticas sobre el aprovechamiento y operación de los sistemas y servicios institucionales, al interior de los departamentos de cómputo de la misma forma deben existir estas mismas políticas alineadas a las políticas principales.

Con ello se garantiza que la las acciones y decisiones que se tomen acerca de la implementación de sistemas y aplicaciones se lleven a cabo en concordancia con los objetivos organizacionales.

Así mismo el tratamiento y operación de los sistemas debe considerar el establecimiento de políticas locales que permitan mantener el control de la infraestructura bajo responsabilidad de los encargados de TI en cada una dependencia académica.

Para ello lo primero que se recomienda es la consulta de las normas y regulaciones a partir de las cuales generaríamos las políticas.

Al interior de la UNAM se puede considerar como punto de partida la Normateca:

https://www.tic.unam.mx/normateca.html

De donde podemos obtener las regulaciones para el uso del direccionamiento y la administración de sitios web, o apoyarnos de normas existentes como la de la facultad de Ingeniería:

http://www.ingenieria.unam.mx/cacfi/documentos/PoliticasSeguridad.pdf

Ejemplo de relación de una política particular con la política general de la empresa

Para el manejo de las políticas se sugiere lo siguiente durante el ciclo de vida de la misma:

- Etapa 1: Diseño, en la cual se contemplé las necesidades, definición y su redacción.
- Etapa 2: Validación y aprobación de la política por los superiores, se procede a realizar las revisiones y ajustes requeridos, para su posterior aprobación para que esta tenga sustento.
- Etapa 3: Publicación al interior de los involucrados a todos los niveles de la organización, esto formaliza y permite la vigencia y aplicación de la misma.
- Etapa 4: Mantenimiento de la política, se vigila el cumplimiento y vigencia, se refiere a los ajustes o actualizaciones que requiera el instrumento, el periodo de revisión depende de los cambios en la organización.

5. Preparación de la plataforma

Alojamiento físico:
Es común que se utilize el nodo más alejado que se no se usa o la computadora más cercana a la persona encargada del sistema de monitoreo por practicidad en la administración, sin embargo se recomienda lo siguiente para la ubicación de un equipo que alojará el sistema de monitoreo:

En caso de que el objetivo sea monitorear los servicios internos de una organización:

- El servidor debe estar alojado dentro del cuarto de comunicaciones donde se encuentran la infraestructura a monitorear, esto evitará falsos positivos.
- Si se requiere monitorear desde la perspectiva de los usuarios es común emplear agentes de monitoreo, en los segmentos de red local.

- Si interesa el monitoreo desde el exterior, el alojar un equipo físico dentro de la infraestructura de un tercero no es una buena alternativa ya que esto provoca pérdida de control del equipo y la infraestructura que lo rodea, más recomendable es la adquisición de un servicio de monitoreo o máquina virtual para implementar los servicios necesarios.

Sistema operativo

La implementación de sistemas operativos tipo Linux para servir de plataforma en un servidor de monitoreo es muy útil, pero es importante tener las siguientes consideraciones:

Emplear plataformas LTS o de largo tiempo de soporte, como ejemplo un servidor de monitoreo que se implemente sobre un SO como *kubuntu*, *fedora* o *mandriva*, tendrá la necesidad de actualizarse con mayor frecuencia y el riesgo de que ocurran bugs que afecten los servicios.

Implementar solo las aplicaciones necesarias para la implementación, cualquier aplicación extra puede provocar una falla de seguridad, una carga en el procesamiento y desperdicio de recursos o una incompatibilidad con las aplicaciones que se desean instalar.

Las plataformas Linux recomendadas por su estabilidad y la experiencia en ellas son:

- Debian, por su estabilidad y gran comunidad, a pesar de que hay que poner atención en la seguridad
- Centos, por su seguridad y estabilidad y a pesar de no ser la rama principal cuenta con gran soporte
- Suse, por su alta implementación para servicios y porque se incluye el soporte en muchos servidores

Aplicaciones base / presentes siempre:

Es conveniente indicar que la implementación de ciertas herramientas para diagnóstico y monitoreo del propio servidor de monitoreo son de bastante utilidad y se recomiendan tener siempre instaladas ya que no entran en conflicto con otras aplicaciones y pueden apoyar en la operación diaria de los servidores, a continuación se listan las consideradas más útiles y que en su mayoría son comandos y se ejecutan en una terminal:

a) fdisk	j) wget	r) ssh
b) lshw	k) dig	s) ftrace
c) du	l) route	t) iotop
d) netstat	m) iptables	u) iptraf
e) ethtool	n) tcptraceroute	v) tiptop
f) iftop	ñ) tcpflow	w) ltrace
g) top	o) strace	v) sysdiag

h) htop i) curl	p) ld q) apt/rpm	x) dmesg y) ss z) snmp utils

6. Convenciones sobre la implementación de las aplicaciones en el servidor

Aspectos importantes en la implementación del hardware

Es importante contar con un almacenamiento aislado entre aplicaciones y sistemas base, por lo que se recomienda que:

- En caso de implementar un servidor físico:
  - Implementar un disco duro para el sistema y otro para las aplicaciones
  - En caso de tener solo un disco particionarlo
  - La conexión de red se prefiere redundante, pero en caso de no tenerla procurar conectarla lo más cercano a los servicios a monitorear
  - El servidor es prioritario por lo que vale la pena estar en alta disponibilidad

- En caso de implementar un servidor virtual
  - Esto sugiere que hay un respaldo de almacenamiento en RAID, por tanto no es necesario particionar.
  - La conexión virtual debe tener la misma conexión que los servicios

- En caso de tratarse de una aplicación con docker o plataforma similar
  - Contempla un arreglo de almacenamiento por tanto no es necesario particionar
  - La conexión virtual debe tener la misma conexión que los servicios para compartir las características de conexión y una prueba real

Aspectos importantes en la implementación de software

Las implementaciones de las soluciones más complejas por lo regular se implementan en el directorio:

- /usr/local ➔ Soluciones completas
- /usr/local/src ➔ Archivos fuente
- /etc/ ➔ Archivos de configuración para inicio y detención de las aplicaciones

Esto garantiza que ante una falla solo hay que revisar un directorio.

Si se cuenta con bases de datos sin embargo estas deberán ser alojadas en particiones diferentes ya que la lectura y escritura representa un riesgo para el almacenamiento de las demás aplicaciones a menos que estas tengan un esquema virtualizados o de contenedores.

7. Consideraciones de operación físicas y lógicas

Consideraciones lógicas:

- La estructura de distribución de archivos y directorios dentro de los sistemas por lo regular se basa en el Filesystem Hierarchy Standard (FHS) mantenido por el grupo de estándares libres FEG de Linux Fundation por lo que si se tiene alguna duda de la ubicación de los archivos debe referirse a este.

- Otra característica a considerar es que las aplicaciones abren puertos de escucha, estos deben ser correctamente gestionados por los firewalls, así como las peticiones que estos realizan para garantizar la operación de los mismos servidores.

- Se dice que el equipo de cómputo apagado, es la única forma de garantizar su seguridad lógica, por lo que un diagnostico e inclusive una auditoria es importante para verificar la operación.

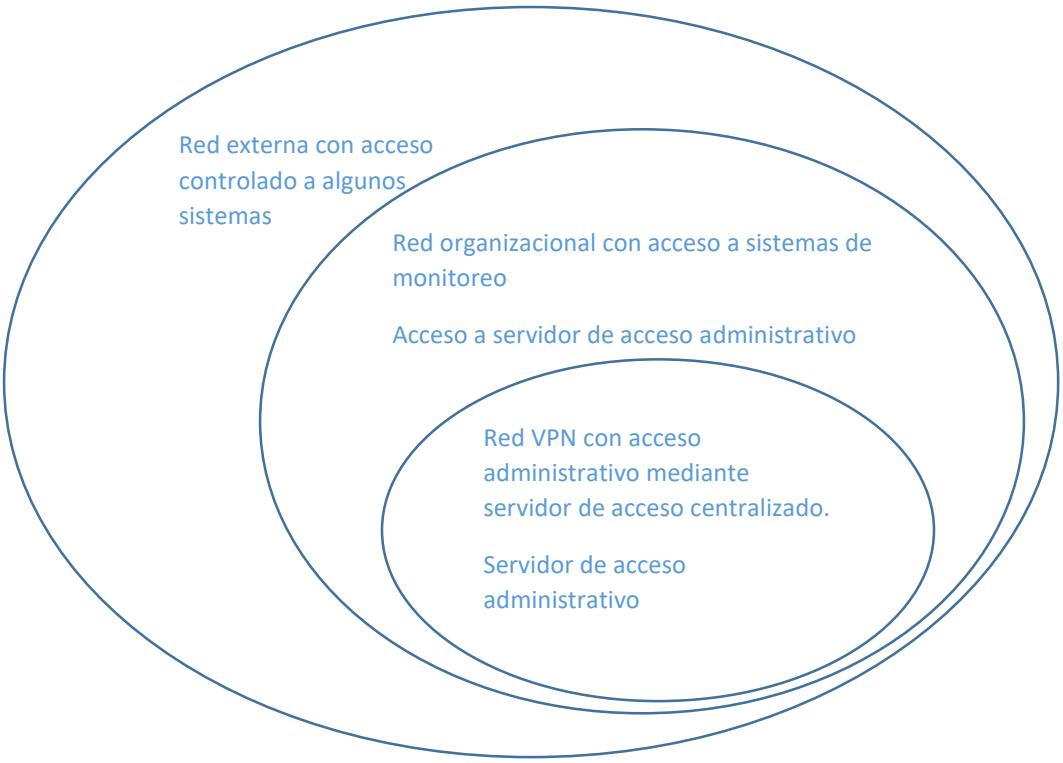
- Etiquetado físico de los servidores para ubicar siempre donde se encuentra cada equipo y que es lo que contiene.

- Registro de aplicaciones e inventarios

- Es importante tener el inventario de las aplicaciones instaladas y ubicaciones, deseable que se cuente con manejo de versiones y fechas de actualización.

8. Control de acceso y puesta en operación

- Como todo servidor es necesario contar con el control de acceso seguro a las plataformas, en este caso se sugiere utilizar un gestor de contraseñas que cifre las mismas para un mejor manejo de ellas.
- Se recomienda que solo una persona cuente con el acceso al servidor de forma administrativa, pero de ser necesario generar cuentas para mantener el control del acceso
- La información es útil en cualquiera de las formas que se obtenga, por lo que es importante que la información de monitoreo sea accedida solo por la personas que deban tener acceso, es por esto que todos los sistemas de monitoreo con acceso web deben tener un control de acceso de preferencia con HTTPS pero mínimamente con usuario y password.
- Así mismo si es importante solo las redes de operación deben tener acceso a los sistemas de monitoreo, agregando un nivel de seguridad
- Es ideal contar con un sistema de acceso administrativo centralizado como el que se propone a continuación:



Cada ovalo indica los límites de acceso de la organización a los servicios de monitoreo implementados.

9. Actualización y mantenimiento

Se recomienda tener un calendario y estrategia de mantenimiento para todos los servidores, por tanto para la implementación de este tipo de servidores de monitoreo se recomienda lo siguiente:

Implementación	Observaciones	Actualización de hardware	Actualización de software
Fecha de instalación	Realizdo/pendiente	Fecha planificada	Fecha planificada
Fecha de actualización	Realizdo/pendiente	Fecha planificada	Fecha limite
Fecha de mantenimiento físico	Realizdo/pendiente	Fecha planificada	Fecha límite

Permitiendo contar con un control y tomar decisiones sobre las soluciones de monitoreo.

Las fechas límite por lo regular se estableces a partir de los siguientes criterios sugeridos:

- Tiempo de vida del sistema operativo, en caso de ser LTS si se trata de Linux, hay una fecha en la que se termina el soporte de actualizaciones.
- Nueva versión de aplicación
- Mantenimientos programados de acuerdo a soporte de proveedor de hardware o recomendaciones internas del centro de datos donde se encuentre
- Tiempo de vida de elementos internos (Discos duros)

10. Anexo de documentos de apoyo y repositorios de descarga

Los siguientes enlaces se adjuntan como apoyo para implementación de cada una de las recomendaciones que en el presente manual se enumeran:

4. Como se elabora un sistema de políticas, with paper KPMG:
https://assets.kpmg/content/dam/kpmg/es/pdf/2016/12/Cuadernos_Legales_N5.pdf

Políticas de Seguridad en cómputo para la facultad de Ingeniería:
http://www.ingenieria.unam.mx/~unica/pdf/seguridad_computo.pdf

5. Descripción rápida de comandos en Linux, Facultad de Ingeniería República de Uruguay:
https://www.fing.edu.uy/inco/cursos/sistoper/recursosLaboratorio/tutorial0.pdf

6. Estándar completo sobre la distribución jerarquica de los archivos en Linux
http://www.pathname.com/fhs/

7. RFC IETF, well kown ports (puertos conocidos)
https://tools.ietf.org/html/rfc1340

8. Documentación oficial sobre la administración de la aplicación OpenVPN:
https://openvpn.net/images/pdf/OpenVPN_Access_Server_Sysadmin_Guide_Rev.pdf

Referencias:

Manual de administración por la LinuxFundation:
http://linux-training.be/linuxfun.pdf

Control de Versiones al Documento

Versión	Descripción	Autor	Fecha
1.0	Creación del documento	Esteban Roberto Ramírez Fernández	25/08/2019

Revisión del Documento

Puesto/Rol	Nombre	Revisó
Jefe del Centro de Monitoreo del NOC UNAM	Hugo Rivera Martínez	Contenido
Staff NOC UNAM	Erika Hernández Valverde	Estructura del documento

Aprobación del documento

Puesto/Rol	Nombre y Firma	Fecha de aprobación
Jefe del Centro de Operación de RedUNAM (NOC-RedUNAM	Hugo Rivera Martínez	20/10/2019

Repositorio y publicación

Medio	Ubicación
Sitio Web del NOC www.noc.unam.mx	http://www.noc.unam.mx/conocimiento/
Repositorio Nube NOC	www.nocloud.noc.unam.mx/NOC/ProductosyPublicaciones

Control de Cambios

Revisión	Fecha	Motivo del Cambio
Primera versión	20/10/2019	Documento en primer versión