Instituto Politécnico Nacional

Escuela Superior de Cómputo

Diseño de una Red de Cómputo a partir del modelo de Administración OSI

- **Alumnos:**
  - Hernández Escobedo Fernando
  - Miranda Sandoval Mario Alberto
  - Rojas Alvarado Luis Enrique

- **Fecha:** domingo 11 de octubre de 2020
- **Grupo:** 4CM1
- **Materia:** Administración de Servicios en Red

Objetivo

1. Diseñar una red de cómputo que contenga un servidor Moodle y que considere los elementos de la administración de servicios en red del modelo OSI y especialmente que considere los submodelos de las FCAPS.

Instrucciones

2. Desarrollar un documento donde se especifiquen las características que deberá de cumplir el diseño de una red de cómputo que dará servicio a la ESCOM y que tenga como elemento principal un servidor Moodle para las clases a distancia de los profesores.

3. No se pide una topología específica, sino que se deben de definir todos los elementos que dicha red deberá de cumplir. Para esto, se proponen una serie de preguntas que deberá de considerar el sistema para cada una de las FCAPS y que definirán los requisitos del sistema. Se deberán de investigar aquellos términos que se desconozcan e incluirlos en el documento de diseño.

4. El reporte deberá de numerar cada uno de los párrafos, tal como se muestra en este documento, ya que se realizará un cuestionario donde se presentarán ciertas situaciones y deberá de indicar en qué parte de su documento está considerada la eventualidad. Por ejemplo, si en su documento se considera un monitoreo de cuentas y en la evacuación se presenta un caso de ese tipo usted indicará en qué párrafo y en qué líneas se explica cómo proceder, ejemplo: Párrafo 4, líneas 3 a 6.

Desarrollo

5.Gestión de fallos

Para tener una buena gestión de fallos se contará con un ping poller para pues es un sistema automático que interroga a todos los dispositivos de la organización haciendo ping y que garantiza que toda la topología funciona y tienen un rendimiento óptimo, detectando paquetes perdidos o latencia en la comunicación de los dispositivos.

Se debe usar el Protocolo Simple de Administración de Red o SNMP (en inglés Simple Network Management Protocol) que es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Los dispositivos que normalmente soportan SNMP incluyen routers, switches, servidores, estaciones de trabajo, impresoras, bastidores de módem y muchos más. Nos permitirá supervisar el funcionamiento de la red, buscar y resolver sus problemas.

Para realizar las operaciones básicas de administración anteriormente nombradas, el protocolo SNMP utiliza un servicio no orientado a la conexión (UDP) para enviar un pequeño grupo de mensajes (PDUs) entre los administradores y agentes. La utilización de un mecanismo de este tipo asegura que las tareas de administración de red no afectarán al rendimiento global de la misma, ya que se evita la utilización de mecanismos de control y recuperación como los de un servicio orientado a la conexión, por ejemplo TCP.

Los paquetes utilizados para enviar consultas y respuestas SNMP poseen el siguiente formato:

- Versión: Número de versión de protocolo que se está utilizando (por ejemplo 0 para SNMPv1, 1 para SNMPv2c, 2 para SNMPv2p y SNMPv2u, 3 para SNMPv3, ...).
- Comunidad: Nombre o palabra clave que se usa para la autenticación. Generalmente existe una comunidad de lectura llamada "public" y una comunidad de escritura llamada "private".
- SNMP PDU: Contenido de la Unidad de Datos de Protocolo, el que depende de la operación que se ejecute.

Hay que tomar en cuenta que los mensajes GetRequest, GetNextRequest, SetRequest y GetResponse utilizan la siguiente estructura en el campo SNMP PDU:

- Identificador: Es un número utilizado por el NMS y el agente para enviar solicitudes y respuesta diferentes en forma simultánea;
- Estado e índice de error: Sólo se usan en los mensajes GetResponse´(en las consultas siempre se utiliza cero). El campo "índice de error" sólo se usa cuando "estado de error" es distinto de 0 y posee el objetivo de proporcionar información adicional sobre la causa del problema. El campo "estado de error" puede tener los siguientes valores:
  - 0: No hay error;
  - 1: Demasiado grande;
  - 2: No existe esa variable;
  - 3: Valor incorrecto;
  - 4: El valor es de solo lectura;
  - 5: Error genérico.
- Enlazado de variables: Es una serie de nombres de variables con sus valores correspondientes (codificados en ASN.1).

Podremos utilizar:

⇒ GetRequest: A través de este mensaje el NMS solicita al agente retornar el valor de un objeto de interés mediante su nombre. En respuesta el agente envía una respuesta indicando el éxito o fracaso de la petición. Si la petición fue correcta, el mensaje resultante también contendrá el valor del objeto solicitado. Este mensaje puede ser usado para recoger un valor de un objeto, o varios valores de varios objetos, a través del uso de listas.

⇒ GetNextRequest: Este mensaje es usado para recorrer una tabla de objetos. Una vez que se ha usado un mensaje GetRequest para recoger el valor de un objeto, puede ser utilizado el mensaje GetNextRequest para repetir la operación con el siguiente objeto de la tabla. Siempre el resultado de la operación anterior será utilizado para la nueva consulta. De esta forma un NMS puede recorrer una tabla de longitud variable hasta que haya extraído toda la información para cada fila existente.

⇒ SetRequest: Este tipo de mensaje es utilizado por el NMS para solicitar a un agente modificar valores de objetos. Para realizar esta operación el NMS envía al agente una lista de nombres de objetos con sus correspondientes valores.

⇒ GetResponse: Este mensaje es usado por el agente para responder un mensaje GetRequest, GetNextRequest, o SetRequest. En el campo

"Identificador de Request" lleva el mismo identificador que el "request" al que está respondiendo.

⇒ Trap: Una trap es generado por el agente para reportar ciertas condiciones y cambios de estado a un proceso de administración. El formato de la PDU es diferente:

- Enterprise: Identificación del subsistema de gestión que ha emitido el trap;
- Dirección del agente: Dirección IP del agente que ha emitido el trap;
- Tipo genérico de trap:
    - Cold start (0): Indica que el agente ha sido inicializado o reinicializado;
    - Warm start (1): Indica que la configuración del agente ha cambiado;
    - Link down (2): Indica que una interfaz de comunicación se encuentra fuera de servicio (inactiva);
    - Link up (3): Indica que una interfaz de comunicación se encuentra en servicio (activa);
    - Authentication failure (4): Indica que el agente ha recibido un requerimiento de un NMS no autorizado (normalmente controlado por una comunidad);
    - EGP neighbor loss (5): Indica que en sistemas en que los routers están utilizando el protocolo EGP, un equipo colindante se encuentra fuera de servicio;
    - Enterprise (6): En esta categoría se encuentran todos los nuevos traps incluidos por los vendedores.
- Tipo específico de trap: Es usado para traps privados (de fabricantes), así como para precisar la información de un determinado trap genérico;
- Timestamp: Indica el tiempo que ha transcurrido entre la reinicialización del agente y la generación del trap;
- Enlazado de variables: Se utiliza para proporcionar información adicional sobre la causa del mensaje.

⇒ GetBulkRequest: Este mensaje es usado por un NMS que utiliza la versión 2 o 3 del protocolo SNMP típicamente cuando es requerida una larga transmisión de datos, tal como la recuperación de largas tablas. En este sentido es similar al mensaje GetNextRequest usado en la versión 1 del protocolo, sin embargo, GetBulkRequest es un mensaje que implica un método mucho más rápido y eficiente, ya que a través de un solo mensaje es posible solicitar la totalidad de la tabla.

⇒ InformRequest: Un NMS que utiliza la versión 2 o 3 del protocolo SNMP transmite un mensaje de este tipo a otro NMS con las mismas características, para notificar información sobre objetos administrados, utilizando el protocolo de nivel 4(OSI) TCP, y enviara el InformRequest hasta que tenga un acuse de recibo. [1]

Se deben monitorizar los registros del sistema Syslog, el cuál es el acrónimo de System Logging Protocol, que significa protocolo de registro del sistema. Se trata de un protocolo estándar utilizado para enviar mensajes de registro o eventos del sistema a un servidor específico, llamado servidor de syslog. El syslog se utiliza principalmente para recopilar varios registros de dispositivos de diversas máquinas diferentes en una ubicación central para la supervisión y su análisis.

El protocolo está habilitado en la mayoría de equipos de red, como routers, switches, cortafuegos e incluso en algunas impresoras y escáneres. Además, syslog está disponible en sistemas basados en Linux/Unix y en muchos servidores web como Apache. Syslog no está instalado de manera predeterminada en los sistemas Windows, que usan su propio registro de eventos; si bien es capaz de reenviarlos a través de herramientas de terceros u otras configuraciones utilizando el protocolo Syslog.

El protocolo está habilitado en la mayoría de equipos de red, como routers, switches, cortafuegos e incluso en algunas impresoras y escáneres. Además, syslog está disponible en sistemas basados en Linux/Unix y en muchos servidores web como Apache. Syslog no está instalado de manera predeterminada en los sistemas Windows, que usan su propio registro de eventos; si bien es capaz de reenviarlos a través de herramientas de terceros u otras configuraciones utilizando el protocolo Syslog.

Para supervisar el estado del hardware del dispositivo para detectar fallas por eventos como fallo en el suministro de energía, falla del sistema redundante, temperatura del dispositivo, entre otras, se puede usar Free Windows Admin Tools que ofrece tres herramientas: Remote Task Manager, Remote Device Manager y Remote Desktop Connection. Remote Device Manager te muestra información sobre los componentes de hardware de cada computadora. Te servirá para hacer un inventario del hardware disponible sin desplazarte físicamente. Pruebas de Diagnóstico.- Diseñar y realizar pruebas que apoyen la localización de una falla (Pruebas de conectividad física, pruebas de conectividad lógica, pruebas de medición).

Se debe de tener un proceso de gestión de incidentes para administrar los fallos de servicio de atención. Esto mediante:

- Administración de Reportes.- Registrar y dar seguimiento a todos los reportes generados por los usuarios o por el mismo administrador de la red.

  El ciclo de vida de la administración de reportes se divide en 4 áreas:

  - Creación de Reportes.- Un reporte es creado después de haber recibido una notificación sobre la existencia de un problema en la red.
  - Seguimiento a Reporte.- La administración de reportes debe permitir al administrador dar seguimiento de cada acción tomada para solucionar el problema, y conocer el estado histórico y actual del reporte.
  - Manejo de Reportes.- El administrador debe ser capaz de tomar ciertas acciones cuando un reporte está en curso.
  - Finalización de Reportes.- Una vez que el problema reportado ha sido solucionado, el administrador del sistema de reportes, debe dar por cerrado el reporte.

6.Gestión de configuración

Para poder recopilar la información de inventario se debe de utilizar algún software que pueda recopilar de la red todos los chasis, módulos y números seriales, etc. En este caso podríamos probar con Network Inventory Advisor.[8]

A continuación, se menciona en general de lo que puede hacer el Inventario de red:

El Inventario de red se encarga de la recopilación de todos los activos de hardware y software de una red.

Si se hace usa el inventario se puede tener una lista actualizada de todos los activos de la red de la empresa, informes, seguimiento automático de activos de hardware y software, puede enviar alertas cuando detecta cambios de software y hardware, pude rastrear fácilmente las instalaciones tanto de software como de hardware, las versiones de software, licencias y servicios en todos los ordenadores, es capaz de detectar automáticamente todos los dispositivos Windows, MacOS, Linux y SNMP en la red. Inclusive se puede hacer el seguimiento

de los activos independientes, como impresoras, teclados, dispositivos de sonido e incluso mobiliario de oficina.

Para recopilar las configuraciones de los dispositivos, se puede tener una base de datos del inventario que proporciona la información de la configuración detallada en los dispositivos de red. La información común incluye los modelos de la dotación física, los módulos instalados, las imágenes del software, los niveles del microcódigo, etc.

Para detectar, informar e investigar los cambios en la configuración de los dispositivos, el inventarios se pueden automatizar completamente para estar al tanto de cualquier cambio que se produzca en la red.

**Cabe mencionarse que por ejemplo, el CiscoWorks2000 Essentials se puede utilizar para realizar la autenticación en los cambios de configuración. Un registro de la auditoría de cambio está disponible para seguir los cambios y el Nombre de usuario de los individuos que publican los cambios de configuración en los dispositivos múltiples.

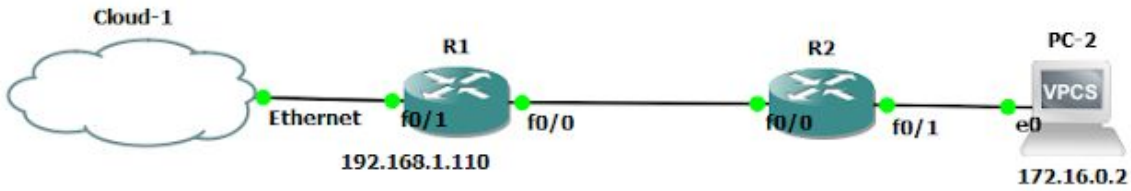
Es viable utilizar una plantilla de configuración básica bien documentada, Cisco tiene algunas en sus paquetes de paga. Por ejemplo: SDM(Switch Database Manager) templates. Las SDM Templates son plantillas propietarias de Cisco, que nos permiten configurar los switches de forma que se les saque un mayor rendimiento, en función de lo que vayan a trabajar.

Las configuraciones en ejecución podrían ser auditadas contra las plantillas de configuración.

7.Gestión contable

Para tener la administración de contabilidad apropiada se medirá la utilización de los recursos de red importantísimos. La utilización de los recursos de red se puede medir usando las características de contabilidad IP NetFlow de Cisco y de Cisco.

Estará habilitada la exportación NetFlow (flujo de red) , que es una tecnología de medición de lado de entrada que permite capturar los datos requeridos para aplicaciones de planificación, supervisión y contabilidad de redes, y así poder ser clasificados según el tipo de servicio o aplicación. Los datos recopilados podrán ser atribuidos a los usuarios o grupos de usuarios específicos, pues el Netflow se debe desplegar en los interfaces del borde/del router de la agregación para los proveedores de servicio o los interfaces del router de acceso a WAN para los clientes de la empresa.




```
configure terminal
  interface FastEthernet0/1
    ip route-cache flow
    exit
ip flow-export destination 192.168.1.111 9999
ip flow-export source FastEthernet0/1
ip flow-export version 9
ip flow-cache timeout active 1
ip flow-cache timeout inactive 15
exit
write
```

Se harán ajustes contables por violaciones de SLA, porque un incumplimiento de contrato puede alterar el ancho de banda de red o ciertos parámetros que realmente debería tener otro precio.

*Un Service Level Agreement (SLA) es un contrato que describe el nivel de servicio que un cliente espera de su proveedor.

8.Gestión de rendimiento

Para la administración de rendimiento es importante contar con las sondas RMON ya que estas nos permitirán capturar el tráfico de la red, si se usan routers de Cisco existe una característica llamada Netflow que sirve para detallar información del tráfico como lo son:

- Direcciones IP de origen y destino.

- Interfaces de entrada y salida.
- Puertos de origen y destino UDP/TCP.
- Número de bytes y paquetes en el flujo.
- Números del sistema autónomo de origen y destino.
- Tipo de servicio.

Los datos de NetFlow recopilados en los dispositivos de red se exportan a una máquina del colector. El colector realiza las funciones tales como reducción del volumen de datos (filtración y agregación), del almacenamiento de datos jerárquico, y de la Administración del sistema de archivos.

Una vez obtenidos estos datos, para almacenarlos se puede usar el software SAS, este al ser un software estadístico nos permitirá guardar una gran cantidad de información además de poder manipularla.

Otros puntos para considerar son que la CPU debe constar de un buen backplane para tener un mejor procesamiento de tráfico, el tamaño de la interfaz y el tubo deben ser amplios para tener una mayor cantidad de datos a enviar de manera simultánea.

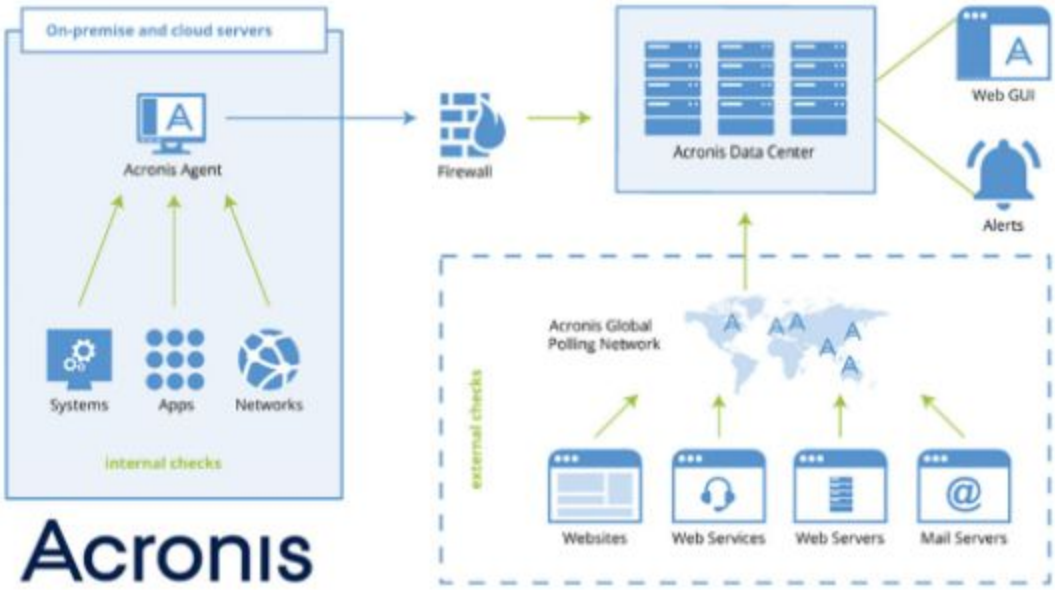
9.Gestión de la seguridad

Se utiliza TACACS, RADIUS o equivalente para la administración de dispositivos, autorización, acceso, ¿y contabilidad? ¿Existen diferentes niveles de acceso y autorización para la mesa de servicio, los operativos y el personal de apoyo de tercer nivel? ¿Los syslog de los dispositivos se alimentan en un servidor syslog común? ¿Se monitorizan o revisan los registros de servidores, enrutadores, conmutadores, cortafuegos y aplicaciones? Ya sea manualmente o empleando algún software para este fin. ¿Se puede implementar un cambio de configuración global en todos los dispositivos en menos de 24 horas? (Como la solución de configuración de CERT o PSIRT).

> Para la parte de seguridad de manera preferente se usarán routers Cisco, ya que estos nos permiten usar el protocolo TACACS pero mejorado por ellos mismos con el fin de tener un control más fino, esta mejora la han llamado TACACS+, que al igual que su base cumple con la arquitectura de las AAA, además se puede usar el modo sin privilegios o privilegiado, se pueden configurar para la tolerancia a incidentes, además que una vez que TACACS+ ha sido iniciado se puede pedir el usuario y contraseña para una sesión o para comandos individuales incluyendo la autenticación y la autorización que entre más privilegios tenga más fuerte será.

Además, para la contabilidad el uso de TACACS+ permite usar comandos para administrar la autenticación, autorización y contabilidad.

Para monitorear la red, el servidor o cortafuegos se puede usar un programa llamado “Acronis Monitoring System”



Esta herramienta tiene la capacidad de monitorizar todos los elementos: redes, rendimiento de los servidores y sistema operativo, aplicaciones y servicios y comprobaciones web sintéticas, además Acronis es compatible tanto para comprobaciones externas como para internas. La monitorización externa recurre a agentes públicos de Acronis que comprueban la red remotamente a través de la red mundial de sondeos. Así determina la disponibilidad y la actividad en los servicios web, cuando se accede a ellos desde el exterior, desde diversas ubicaciones. Cuando se quiere comprobar los sistemas, la aplicación y los parámetros de red en la infraestructura TIC, la monitorización interna recurre a agentes privados instalados en un servidor basado en la nube o in-situ, ambos disponibles tras un cortafuegos.

Referencias

[1]

L. T. Rocamora, «Servicios de Red e Internet,» 2 Febrero 2015. [En línea]. Available: https://es.slideshare.net/Lord_LT/prctica-snmp-servicios-de-red. [Último acceso: 2 Noviembre 2020].

[2]

A. Telesis, «Ping Polling,» [En línea]. Available: https://www.alliedtelesis.com/sites/default/files/documents/feature-guides/ping_polling_feature_overview_guide_revb.pdf. [Último acceso: 2 Noviembre 2020].

[3]

PAESSLER, «It Explained: Syslog,» [En línea]. Available: https://www.es.paessler.com/it-explained/syslog. [Último acceso: 2 Noviembre 2020].

[4]

B. It, «Blue It,» 6 Abril 2017. [En línea]. Available: https://blueit.com.ec/blog/item/225-administrar_hadware_software.html. [Último acceso: 2 Noviembre 2020].

[5]

S. O. V. Manuel, «Mi sitio personal,» [En línea]. Available: https://sites.google.com/a/itdurango.edu.mx/10040372/home/administracion-de-redes/unidad-i. [Último acceso: 2 Noviembre 2020].

[6]

Anonimous, «Desde otra perspectiva,» 27 Mayo 2018. [En línea]. Available:

http://solarisdmt.blogspot.com/2018/05/gns3-configuracion-basica-de-netflow-y.html. [Último acceso: 2 Noviembre 2020].

[7]

Cisco, «Sistema de administración de red: Informe oficial de Mejores Prácticas,» 10 Agosto 2018. [En línea]. Available: https://www.cisco.com/c/es_mx/support/docs/availability/high-availability/15114-NMS-bestpractice.html. [Último acceso: 2 Noviembre 2020].

[8]

Network Inventory Advisor, «Asequible y Rentable Sofware de Inventario de la Red» 2020. [En línea]. Available: https://www.network-inventory-advisor.com/es/

[9]

C. D. Antonio, «Cisco: Configuración de SDM Templates» 26 de abril del 2019. [En línea]. Available: https://openwebinars.net/blog/cisco-sdm-templates/