INSTITUTO TECNOLOGICO SUPERIOR DE TANTOYUCA

ING. SISTEMAS COMPUTACIONALES

Administración de Redes.

DOCENTE:

Ing. Edgar Medellín Orta

ALUMNO(A):

Arely Alejandra de Jesús Rendon

"ANALISIS Y MONITOREO"

INDICE

Introducción.

En la actualidad es importante contar con un protocolo de administración de red este se compone de un conjunto de normas para la gestión de la red, incluyendo una capa de aplicación del protocolo, una base de datos de esquema, y un conjunto de objetos de datos esto permite a los administradores supervisar el funcionamiento de la red, buscar y resolver sus problemas, y planear su crecimiento, esto con el fin de satisfacer satisfactoriamente las necesidades del usuario, las bitácoras nos funcionaran para poder anotar periodo por periodo de monitoreo de la red como esta su evolución y si este ha presentado un error tener conocimiento de ello, y así poder tener un control mejor.

Contenido.

PROTOCOLOS DE ADMINISTRACIÓN DE RED

Los protocolos de administración de redes funcionan en el ámbito de las redes y por lo tanto son protocolos de red.

Ahora bien, es importante diferenciarlos de aquellos protocolos de red que permiten la transferencia de data entre dos dispositivos, tales como TCP, UDP, SMTP, CSMA/CD, etc.

En una red convivirán tanto los protocolos de transferencia de data como los de administración, compartiendo los recursos como CPU y ancho de banda de enlaces.

Por lo tanto es interesante tener presente que los protocolos de administración de redes también influyen el rendimiento global de la plataforma.

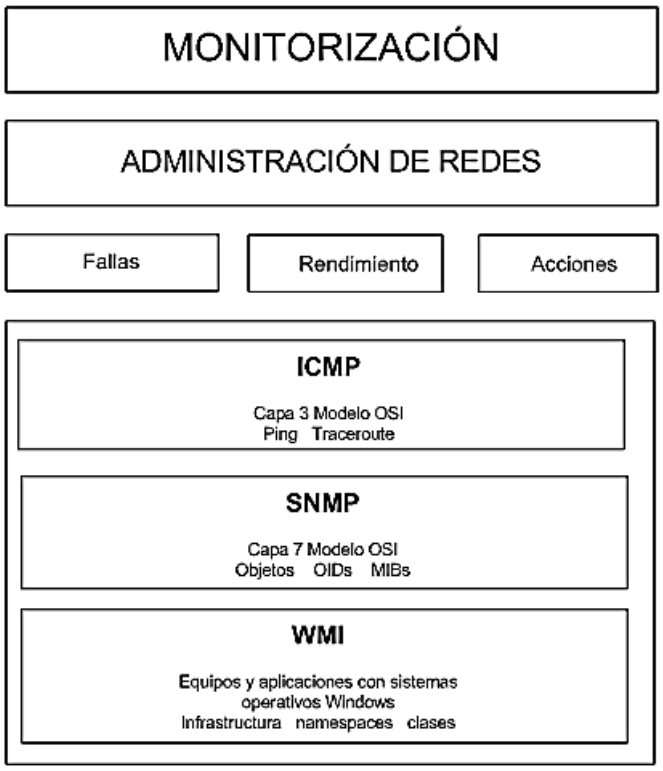

Fig 1. La administración de redes y sus protocolos

ICMP

ICMP (Internet Control Message Protocol) es un protocolo de capa de red que es parte del grupo de subprotocolos asociados con el protocolo IP.

ICMP funciona en el ámbito de la validación de fallas y además permite el cálculo de ciertas métricas de rendimiento.

El lector puede leer sobre las especificaciones detalladas del protocolo en el RFC792.

El procedimiento que propone ICMP parte de la detección de una condición de error y el envío de un mensaje reportando dicha condición.

Así pues, el elemento clave son los mensajes contemplados por ICMP, los cuales suelen clasificarse en dos categorías:

- Mensajes de error: Utilizados para reportar un error en la transmisión de paquete.
- Mensajes de control: Utilizados para informar sobre el estado de los dispositivos.

La arquitectura con la que trabaja ICMP es muy flexible, ya que cualquier dispositivo de la red puede enviar, recibir o procesar mensajes ICMP.

En la práctica se utiliza para que los enrutadores y switches reporten a los host que originan un paquete que dicho paquete no puede ser entregado por un error de la red.

Además, ICMP es utilizado también para realizar cálculos de métricas sobre el rendimiento, como niveles de latencia, tiempo de respuesta o pérdida de paquetes, entre otros.

SNMP

SNMP, Protocolo Simple de Administración de Red (Simple Network Management Protocol) es un estándar de administración de redes basado en el conjunto de protocolos TCP/IP, que permiten la consulta a los diferentes elementos que constituyen la red.

SNMP ofrece un esquema para reunir, organizar y comunicar información de administración entre los dispositivos que conforman una red.

Se utiliza para administrar redes basadas en TCP/IP y IPX.

Permite a los administradores de red:

- Supervisar la operación de la red.
- Configurar equipos.
- Encontrar y resolver fallos.
- Analizar prestaciones de los equipos.

e. Acceder a la información de productos de diferentes fabricantes de una misma manera, desarrollando una herramienta común de monitoreo.

Hoy en día SNMP es el protocolo de administración de red más ampliamente usado y desarrollado.

Componentes de SNMP

El entorno de trabajo del protocolo SNMP se basa en cuatro componentes:

1. SMI, Estructura de Administración de la Información: RFC1155, lenguaje de definición de datos, que especifica los tipos de datos, un modelo de objetos y reglas para escribir y comprobar la información de administración. Los objetos MIB se especifican a partir de este lenguaje.

2. Administración de la Base de Información, MIB: RFC1156, RFC 1213, incluye la definición de los objetos de red, conocida como objetos MIB. La información de administración se representa como un conjunto de objetos que conforman un almacenamiento de información virtual, conocido como Base de Información de Administración. Un objeto MIB, puede ser un contador (por ejemplo el número de datagramas IP que han sido eliminados en el router debido a los errores en la cabecera del datagrama IP o bien el número de errores de detección de la portadora en una tarjeta de interfaz Ethernet). Los objetos MIB definen la información de administración que mantiene un dispositivo y aquéllos que están relacionados, se recogen en un módulo MIB.

3. Protocolo Simple de Administración de Redes, SNMP: RFC 1157, medio de comunicación para transmitir información y comandos entre la Administración de Redes Protocolos de Administración de Red Elaborado por: Ing. Ma. Eugenia Macías Ríos 4 entidad administradora y un agente que se ejecuta en un dispositivo de red en representación de dicha entidad.

4. Capacidad de seguridad y administración de objetos.

WMI

Con WMI (Windows Management Instrumentation) nos moveremos en el universo compuesto por equipos que corren algún sistema operativo Windows y por las aplicaciones que dependen de dicho sistema operativo.

De hecho, WMI propone un modelo para que podamos representar, obtener, almacenar y compartir información de administración sobre el hardware y software basado en Windows, tanto local como remoto.

Por otro lado, además de lo asociado con la información de administración, WMI permite también la ejecución de ciertas acciones.

BITÁCORAS

El nombre bitácora está basado en los cuadernos de bitácora, cuadernos de viaje que se utilizaban en los barcos para relatar el desarrollo del viaje y que se guardaban en la bitácora. Aunque el nombre se ha popularizado en los últimos años a raíz de su utilización en diferentes ámbitos, el cuaderno de trabajo o bitácora ha sido utilizado desde siempre.

Bitácora de red

Proceso esencial de llevar un registro de lo que ocurre en el transcurso del mismo, y más si es algo sobresaliente, de manera que esto nos permita predecir incidentes o resolvernos de una manera rápida en caso de que ya se hayan presentado, para esto existen las bitácoras de sucesos. En el caso de redes algunos de los sucesos pudieran ser: fallas en el sistema, caída de la red, infección de algún virus a la red, etc.

Base de datos de red es una base de datos conformada por una colección o set de registros, los cuales están conectados entre sí por medio de enlaces en una red.

El registro es similar al de una entidad como las empleadas en el modelo relacional. Un registro es una colección o conjunto de campos (atributos), donde cada uno de ellos contiene solamente un único valor almacenado. El enlace es exclusivamente la asociación entre dos registros, así que podemos verla como una relación estrictamente binaria. Una estructura de base de datos de red, llamada algunas veces estructura de plex, abarca más que la estructura de árbol: un nodo hijo en la estructura red puede tener más de un nodo padre. En otras palabras, la restricción de que en un árbol jerárquico cada hijo puede tener sólo un padre, se hace menos severa. Así, la estructura de árbol se puede considerar como un caso especial de la estructura de red.

Monitorización del registro de eventos de seguridad

Monitorización del registro de eventos de Windows de OpManager proporciona varias reglas automáticas para monitorizar los registros de seguridad críticos en todos los servidores y estaciones de trabajo Windows de su red. Puede detectar fácilmente eventos tales como inicios de sesión fallidos, errores de inicio de sesión debidos a contraseñas erróneas, bloqueos de cuentas, intentos de acceso fallido a archivos seguros, intrusión en el registro de seguridad, etc. También puede crear las reglas personalizadas que necesite para reforzar las directivas de seguridad adoptadas por su empresa.

Monitorización del registro del sistema y aplicaciones – Servidores Monitor IIS, Exchange, SQL e ISA

Además de los registros de seguridad, la función de Monitorización del registro de eventos de Windows de OpManager' puede monitorizar los registros de las aplicaciones, del sistema y otros registros de eventos. Hay disponibles varias reglas para monitorizar aplicaciones críticas para la misión como servidores Exchange, IIS, MS-SQL e ISA. También puede añadir reglas personalizadas para monitorizar eventos generados por cualquier aplicación. Además, existen reglas para monitorizar servicios de directorios, servidores DNS y servidores de replicación de archivo.

Monitorización integrada del registro de eventos

En vez de tratar la monitorización del registro de eventos de Windows como una solución autónoma aislada, la función de Monitorización del registro de eventos de Windows de OpManager le permite monitorizar los registros de eventos de Windows como parte de una solución integrada de gestión de la red, las aplicaciones y los servidores. Así sus operadores sólo tienen que aprender una única interfaz para monitorizar los registros de eventos de Windows.

Bibliografía.

http://administracionredesu3.blogspot.com/p/blog-page_14.html

https://es.slideshare.net/laonda601/investigacion-unidad-3

https://prezi.com/erqh0mt_hgap/protocolos-administracion-de-redes/

https://pandorafms.com/blog/es/protocolos-de-administracion-de-redes/