10 comandos a configurar en un dispositivo nuevo

Cada vez que debemos configurar un dispositivo que se incorpora a la red, gran parte de la configuración depende tanto del dispositivo como del diseño de la red en la que ese dispositivo va a incorporarse. Sin embargo, hay también un conjunto de features que siempre podemos o debemos tener en cuenta, independientemente del dispositivo y la red.

Dependiendo de las implementaciones y del mismo Administrador, siempre hay una lista de cosas que "siempre hay que hacer": claves, nombres de dispositivos... etc. Esta es una lista posible de "10 cosas que siempre hay que configurar" en los dispositivos de una red:

1. Configurar cuentas de acceso a los dispositivos.
2. Configurar un hostname que lo identifique.
3. Configurar una clave de acceso al modo privilegiado.
4. Encriptar las claves.
5. Deshabilitar el acceso vía http.
6. Configurar un servicio de traducción de nombres.
7. Configurar commandos alias.
8. Configurar el reloj de los dispositivos.
9. Evitar que los mensajes logging molesten durante las tareas de configuración.
10. Configurar el servicio de logs.

Algunas de estas tareas ya las consideré en otros artículos, a los que procuraré referir en cada cado. Si tenés tu propia lista de "cosas que siempre hay que hacer" o algún elemento más para agregar, por favor, incorporalo como comentario a esta nota.

Configuración de cuentas de acceso a los dispositivos

Es altamente recomendable que los accesos a los dispositivos estén asegurados requiriendo la identificación de usuario y clave. No estamos hablando de una simple clave de acceso a modo usuario para la conexión a través de telnet o consola. La sugerencia es que ese acceso requiera del ingreso de usuario y clave.

Adicionalmente, Cisco IOS nos brinda la posibilidad de que esa clave se encripte utilizando MD5, como un forma adicional de segurizar nuestros dispositivos. El comando de configuración para realizar esta tarea es:

Router(config)#username [usuario] secret [clave]

Luego de configurado usuario y clave, es necesario aplicarlo a cada una de las líneas de acceso:

Router(config)#line con 0

Router(config-line)#login local

Router(config)#line aux 0

Router(config-line)#login local

Router(config)# line vty 0 4

Router(config-line)# login local

Obsérvese, para los que están acostumbrados a configurar una clave de acceso a modo usuario, que espre procedimiento reemplaza aquel.

Configurar un hostname

Todos los dispositivos Cisco tienen un nombre configurado por defecto: Router ó Switch, según corresponda. La configuración de un nombre que identifique claramente al dispositivo es de gran utilidad para el desarrollo de tareas de administración y monitoreo de los dispositivos y en términos generales debe responder a una acción planificada y parametrizada por el Administrador de la red.

La modificación de este nombre por defecto es extremadamente sencilla:

Router(config)#hostname [nombre]

Adicionalmente, Cisco IOS permite configurar un nombre de dominio de modo que el dispositivo "conozca" en qué dominio DNS se encuentra:

Router(config)#ip domain name [dominio]

Configurar una clave de acceso al modo privilegiado

Un elemento de seguridad muy importante es bloquear el acceso al modo privilegiado de los dispositivos (desde el que se accede al modo configuración) utilizando una clave de acceso. Adicionalmente Cisco IOS brinda la posibilidad de que la clave configurada sea encriptada utilizando MD5.

Esta es una tarea extremadamente sencilla:

Router(config)#enable secret [clave]

Encriptar todas las claves no encriptadas

No todas las claves configuradas en dispositivos Cisco IOS están encriptadas por defecto. Esto se puede solucionar fácilmente activando el servicio de encipción de claves que ofrece IOS:

Router(config)#service password-encryption

Deshabilitar el acceso vía http

Acceder a interfaces de administración a través de un web browser es una facilidad buscada por muchos Administradores. Todos sabemos que la configuración por CLI es más tediosa; pero también es más precisa y flexible... y más segura. De aquí que se recomiende fuertemente que, por seguridad, se desactive el acceso vía http (o web broser) a los dispositivos.

Los dispositivos Cisco permiten por defecto el acceso utilizando navegadores web. Si este acceso no va a ser utilizado, es más seguro desactivarlo. Es otra tarea simple:

Router(config)#no ip http server

Configurar un servicio de traducción de nombres

Cuando se ingresa una cadena de caracteres en la CLI de Cisco IOS, por defecto, IOS la interpreta como si se tratara de un comando. Si no puede asociar un comando a esa cadena de caracteres, entonces interpreta que el operador está requiriendo hacer telnet a un dispositivo al que identifica con un nombre, y por lo tanto procura traducir ese nombre a una dirección IP.

Esto suele provocar inconvenientes durante el proceso de configuración ya que, ante un error de tipeo al ingresar un comando el dispositivo comienza inmediatamente a intentar una traducción de nombres hasta que falla (dns lookup en inglés).

Esto tiene 2 soluciones posibles. La primera solución es desactivar el servicio de traducción de nombres que Cisco IOS tiene activado por defecto:

Router(config)#no ip domain-lookup

La otra opción, es configurar un servidor DNS real para que el dispositivo pueda hacer las búsquedas que sean necesarias:

Router(config)#ip name-server [IP]

Configurar comandos alias

El comando alias es un recurso interesante que permite a los Administradores generar su propio conjunto de comandos abreviados para realizar aquellas tareas más repetitivas.

Un ejemplo de las posibilidades que brinda:

Router(config)#alias [modo] [abreviado] [comando]

Router(config)#alias exec s show running-config

De este modo, ingresando una sola letra se ejecuta un comando más complejo.

El comando alias: un modo abreviado de realizar tareas repetitivas.

Configurar el reloj de los dispositivos

La mayoría de los dispositivos Cisco están dotados de un reloj interno que requieren de configuración. Esta tarea es de suma importancia al momento de revisar archivos logs, ya que es la base de información para estampar fecha y hora en los registros del log.

En principio este requisito se puede cubrir configurando, además de fecha y hora en el reloj, el uso horario:

Router#clock set [hh]:[mm]:[ss] [mmm] [dd] [aaaa]

Router#configure terminal

Router(config)#clock timezone [huso] [GMT]

En el caso de países o regiones que modifican el uso horario de acuerdo a la estación:

Router(config)#clock summer-time [huso] recurring

Ahora bien, en redes con numerosos dispositivos, es conveniente configurar el acceso a un servidor NTP a fin de asegurarnos que el reloj de todos los dispositivos se encuentre debidamente sincronizado, de modo que se facilite la tarea de diagnóstico y monitoreo. De este modo el dispositivo siempre buscará la información en el servidor al momento de inicializarse:

Router(config)#ntp server [IP]

Configuración de hora y zona horaria en dispositivos.

Evitar que los mensajes logging molesten

Cuando se está configurando o revisando el resultado de un comando show resulta muy molesta la interrupción que provocan los mensajes de logging de algunos sucesos estándar (p.e. el estado de las interfaces) o de un debug.

Esto es fácilmente solucionable, con una mínima previsión al momento de realizar la configuración. Un modo, no aconsejable, es eliminar sencillamente estos mensajes:

Router(config)#no logging console

El que quizás es el mejor modo (porque nos permite seguir recibiendo estos mensajes de estado, que son de gran importancia), es sincronizar estoa mensajes con el ingreso de comandos en el prompt del sistema operativo:

Router(config)#line con 0

Router(config-line)#logging synchronous

Router(config)#line aux 0

Router(config-line)#logging synchronous

Router(config)#line vty 0 4

Router(config-line)#logging synchronous

Configurar el servicio de log

Los mensajes de estado por defecto son enviados a la consola y no se almacenan. Sin embargo, es muy probable que los eventos que nos preocupan (fallos, actualizaciones de rutas, etc.) ocurran mientras no hay un operador conectado al puerto consola que pueda evaluarlos.

Es por esto de gran utilida indicarle al dispositivo que se desea enviar esta información a un servidor de syslog, o al menos, almacenarlos en un buffer de memoria en el mismo dispositivo:

Router(config)# logging buffered [tamaño]