Ejecutar comandos remotos desde Zabbix

http://www.elmundoenbits.com/2013/03/zabbix-remote-command.html

Ejecutar comandos remotos mediante IPMI

Desde zabbix podemos crear scripts que ejecuten comandos en equipos remotos mediante IPMI, por ejemplo podemos apagar o encender un equipo en caso de ocurrir un evento sin que nadie deba estar físicamente para hacerlo.

Suponemos que ya tenemos configurada la tarjeta BMC y que ya tenemos creado un host, configurado con IPMI y que las "ipmitools" está instalado en nuestro servidor de zabbix, podemos crear los scripts que darán instrucciones al servidor.

Crear el script

Administración → scripts → créate script

- Name: nombre del script.
- Type: el tipo de script, si es normal será "script" de lo contrario será "IPMI" (en nuestro caso elegiremos "script").
- Execute on: podemos elegir entre "zabbix agent" (el comando se ejecuta mediante el agente zabbix en la maquina remota) o "zabbix server" (el comando se ejecuta desde el propio servidor zabbix). En nuestro caso seleccionaremos "zabbix server".
- Commands: el comando que queremos ejecutar:

```
ipmitool -I lan -H {HOST.CONN} -U root -P {$PASSWD} [power soft | power off | power on | chassis status] 2>&1
```

- En el comando anterior Ipmitool es el comando con el cual podemos controlar la placa BMC.
- El parámetro "-I lan" significa que nos conectaremos a través de LAN con la controladora BMC.
- Con "-H {HOST.CONN}" indicamos la ip de la BMC, {HOST.CONN} es una macro de zabbix que es sustituida por la ip del servidor que cliquemos.
- El parámetro "-U root " indica el usuario con el que vamos a acceder.
- Así mismo debemos ingresar la contraseña con "-P {PASSWD}"
- Comando a ejecutar
    - Power soft: apagado seguro.
    - Power off: apagado forzado.
    - Power on: encendido.
    - Chassis status: muestra información sobre el estado del servidor.
- Por último nos encontramos con " 2>&1" que se usa para mostrar el resultado del comando.
- Require host permissions: premiso de escritura o lectura a la hora de ejecutar el comando (en nuestro caso usaremos read)
- Enable confirmation: mensaje que se muestra antes de ejecutar el comando para saber si el usuario esta seguro de realizar la acción.



este comando deberíamos crearlo en una macro en ” Administración > general > macros” . Cuando queramos usar algún script le daremos el valor de la contraseña y cuando acabemos la quitamos, así evitaremos que aparezca explícitamente en el script.

Podemos utilizar utilizar estos comandos manualmente desde **Monitoring → Latest data** o en el caso en el que se dispare algún trigger del equipo podemos ejecutar los comandos desde su nombre en la información de la incidencia.



Si tenemos varios “hosts” y tienen diferentes contraseñas podemos, en lugar de definir variables globales (Administración > genera > script), definir una macro en una template para un grupo de hosts que la compartan o incluso en el propio host se puede definir una para sí mismo.

Una vez hayamos terminado de usar los comandos es recomendable dejar el valor de la macro en blanco para que no aparezca en la base de datos de mysql.



Además deberíamos verificar las contraseñas de los usuarios root (root@localhost, root@dominioDeLaEmpresa y root@127.0.0.1) que tengamos en nuestro mysql para que no se pueda acceder al valor de la macro en caso de que nos olvidemos de dejarla en blanco.

Así mismo, modificaremos el usuario de zabbix en la base de datos cambiando nombre y contraseña. También deberemos modificar el fichero “/etc/zabbix/web/zabbix.conf.php” modificando el usuario y contraseña.

From:
https://wiki.intrusos.info/ - **LCWIKI**

Permanent link:
https://wiki.intrusos.info/doku.php?id=seguridad:monitorizacion:zabbix2:ipmiscripts

Last update: **182023/01/ 13:46**