PRIMER EJERCICIO PARTE PRÁCTICA DEL PROCESO SELECTIVO DE

B2 ANALISTA PROGRAMADOR SSII, SISTEMAS, REDES, SEG. RED, SEG. INFORMA, (ORDEN 2)

DE LA UNIVERSIDAD COMPLUTENSE DE MADRID

Concurso-Oposición Libre
Resolución de fecha 20-11-2024

9 de junio de 2025

SUPUESTO 1

En el contexto de la monitorización de infraestructuras y servicios, contar con información externa puede aportar un valor añadido al análisis y a la toma de decisiones.

Una de las fuentes más consultadas es la información meteorológica, especialmente en sistemas sensibles a condiciones climáticas.

El script que se detalla a continuación es un ejemplo de cómo recoger información desde una API externa y enviarla a un servidor de monitorización.

Este script debe ejecutarse automáticamente cada 2 horas utilizando el programador de tareas crontab, una herramienta fundamental en sistemas Unix/Linux que permite planificar la ejecución periódica de comandos y scripts.

Crontab garantiza que esta tarea de recogida y envío de datos se realice de forma constante y sin intervención manual, para mantener la coherencia en los datos recopilados y asegurar la continuidad del monitoreo.

```
#!/bin/bash

API_KEY="as234f****adopiua4"

CITY="Madrid"

MONITOR_SERVER="https://servidor.monitorizacion.ucm.es"

HOSTNAME="WeatherHost"

MONITOR_KEY="weather.data"

response=$(curl -s
"http://api.openweathermap.org/data/2.5/weather?q=${CITY}&appid=${API_
KEY}&units=metric")

temperature=$(echo "$response" | jq '.main.temp')

humidity=$(echo "$response" | jq '.main.humidity')

pressure=$(echo "$response" | jq '.main.pressure')

wind_speed=$(echo "$response" | jq '.main.wind_speed')

weather_data=$(jq -n \

  --arg temp "$temperature" \

  --arg humidity "$humidity" \

  --arg pressure "$pressure" \

  --arg wind_speed "$wind_speed" \

  '{

    temperature: $temp,
```

```
    humidity: $humidity,
    pressure: $pressure,
    wind_speed: $wind_speed
  }')
#pseudo instrucción que dependerá de cada herramienta de
monitorización
curl -X POST -d "host=$HOSTNAME&key=$MONITOR_KEY&value=$weather_data"
$MONITOR_SERVER
```

Preguntas:

1. ¿Qué herramienta se usa en el script para obtener la información del tiempo?

a) curl

b) netcat

c) MONITOR_sender

d) wget

2. ¿Qué método de autenticación/autorización se utiliza al acceder a la API de OpenWeatherMap?

a) OAuth2

b) La api key se pasa por URL

c) Token JWT en el header

d) No hay autenticación

3. Cuando se realiza la petición a la API de OpenWeatherMap, ¿en qué formato se obtiene la información?

a) YAML

b) jQuery

c) XML

d) JSON

4. ¿Cuál es el propósito del parámetro -s en el comando curl usado en el script?

a) Suprime la barra de progreso y mensajes de error

b) Especifica el tamaño del buffer

c) Indica el servidor de destino

d) Activa la salida segura en HTTPS

5. El parámetro -s en el comando curl es una simplificación de:

a) --session

b) --secure

c) --size-buffer

d) --silent

6. ¿En qué formato se envía la información al servidor de monitorización?

a) YAML

b) CSV

c) jQuery

d) JSON

7. ¿Cuál de los siguientes parámetros de jq se utiliza correctamente para leer desde un archivo JSON?

a) jq --execute archivo.json

b) jq --run archivo.json

c) jq '.' archivo.json

d) jq -file archivo.json

8. ¿Qué expresión utilizarías en crontab para ejecutar el script cada 2 horas empezando en un minuto determinado?

a) 0 */2 * * *

b) 0 2 * * *

c) */2 0 1 * *

d) * * * * 2

9. ¿Qué comando se utiliza en la shell Bash para editar las tareas programadas en crontab?

a) cronedit

b) crontab -e

c) cron -edit

d) schedule -edit

10. ¿Qué significa la expresión "0 0 * * 0" en un crontab?

a) Ejecutar la tarea a las 00:00 los domingos

b) Ejecutar la tarea en el minuto 0 y hora 0 todos los días del mes

c) Ejecutar la tarea cada hora

d) Ejecutar la tarea a las 00:00 todos los días de la semana

11. Si nos encontramos en un entorno de sistemas Windows, ¿qué comando debemos ejecutar para abrir el Programador de Tareas?

a) tasksplanner.mcs

b) taskstimer.msc

c) tasksmgr.msc

d) taskschd.msc

12. ¿Qué extensión tiene el archivo que guarda las tareas programadas en un sistema Windows?

a) .ini

b) .bat

c) .xml

d) .task

SUPUESTO 2

La monitorización del rendimiento en sistemas Unix/Linux es fundamental para garantizar la estabilidad, disponibilidad y eficiencia de los servicios.

Las herramientas como ***top*** y ***vmstat*** permiten a los administradores del sistema obtener una vista en tiempo real del uso de recursos como CPU, memoria, procesos activos y carga del sistema.

Una monitorización proactiva permite detectar cuellos de botella, procesos problemáticos o consumo excesivo de recursos antes de que afecten a los usuarios o provoquen caídas del sistema.

Preguntas:

13. ¿Qué muestra la herramienta top por defecto al ejecutarse sin opciones?

a) El historial de acceso al sistema

b) Una vista en tiempo real de los procesos del sistema y su uso de recursos

c) Solo los procesos en espera

d) Información sobre dispositivos conectados

14. ¿Qué tecla permite ordenar los procesos por uso de CPU en la interfaz interactiva de *top*?

a) m

b) u

c) p

d) k

15. ¿Qué significa el campo %CPU en la salida de top?

a) La prioridad del proceso

b) El tiempo total de CPU usado desde el arranque

c) El porcentaje de CPU usado por el proceso en el momento actual

d) El uso de CPU en los últimos 10 minutos

16. ¿Qué tecla permite terminar (kill) un proceso directamente desde top?

a) x

b) z

c) q

d) k

17. ¿Qué tecla permite cambiar el intervalo de actualización en top?

a) d

b) s

c) r

d) i

18. ¿Cuál de las siguientes afirmaciones sobre la tecla u en top es correcta?

a) Muestra solo procesos de sistema

b) Permite filtrar por un usuario específico

c) Cambia el color de la salida

d) Ordena los procesos por ID de usuario

19. ¿Cuál es el formato básico para usar vmstat con intervalos y repeticiones?

a) vmstat -m

b) vmstat -i <veces>

c) vmstat -t <segundos>

d) vmstat <intervalo> <repeticiones>

20. ¿Qué significan los valores en la columna si y so en la salida de vmstat?

a) Entrada/salida de disco

b) Entrada/salida de red

c) Interrupciones del sistema

d) Entrada/salida de la swap

21. En la salida de vmstat, ¿qué representa la columna free dentro del bloque de memoria?

a) Memoria usada por el sistema de archivos

b) Memoria libre en RAM

c) Memoria libre en disco

d) Memoria en uso por el swap

22. ¿Qué muestra el comando vmstat -s?

a) Muestra estadísticas extendidas por segundo

b) Muestra estadísticas por CPU individual

c) Muestra una tabla resumen con el acumulativo de estadísticas desde el arranque

d) Muestra sólo procesos en espera

23. En el entorno de sistemas Windows, ¿qué comando debemos ejecutar para abrir el Monitor de Recursos?

a) taskmgr

b) perfmon.msc

c) resmon

d) monperf

24. En el entorno de sistemas Windows, ¿cómo puedes obtener mediante PowerShell los 10 procesos que más CPU consumen empezando por el que más consume?

a) Get-Process | Sort-Object -Ascending CPU | Select-Object -First 10

b) Get-Process | Sort-Object -Descending CPU | Select-Object -First 10

c) Get-Process | Select-Object -Property CPU | Sort-Object -First 10

d) Get-Process | Select-Object -Property CPU | Sort-Object -Last 10

SUPUESTO 3

En entornos de servidores UNIX-LINUX, la seguridad y la auditoría son fundamentales para garantizar que el sistema esté protegido frente a accesos no autorizados y modificaciones no deseadas.

La implementación de una solución de auditoría permite rastrear y registrar las acciones realizadas en el sistema, lo que facilita la detección de comportamientos anómalos y la identificación de posibles vulnerabilidades.

En este ejercicio, se busca implementar una solución de auditoría enfocada en dos aspectos clave:

*Auditar el acceso de los usuarios: Es fundamental saber quién puede acceder al sistema y bajo qué condiciones. Esto ayuda a prevenir accesos no autorizados y garantiza que los usuarios solo tengan acceso a las áreas del sistema que necesitan para su trabajo.

*Controlar los accesos y modificaciones a ficheros críticos: Algunos ficheros del sistema, como los archivos de configuración de Apache y PHP (/etc/apache2/apache.conf y /etc/php-fpm/php.conf), son fundamentales para el correcto funcionamiento del servidor.

Si estos ficheros se modifican de manera no autorizada, podrían comprometer la seguridad y estabilidad del sistema. Se necesita un control preciso sobre quién accede y modifica estos archivos.

Un ejemplo de esta implementación se muestra en el siguiente fichero de configuración:

```
# This file controls the configuration of the audit daemon

local_events = yes

write_logs = yes

log_file = /var/log/audit/audit.log

log_group = adm

log_format = ENRICHED

flush = INCREMENTAL_ASYNC

freq = 50

max_log_file = 8

num_logs = 5

priority_boost = 4

name_format = NONE

#name = mydomain
```

```
max_log_file_action = ROTATE
space_left = 75
space_left_action = SYSLOG
verify_email = yes
action_mail_acct = root
admin_space_left = 50
admin_space_left_action = SUSPEND
disk_full_action = SUSPEND
disk_error_action = SUSPEND
use_libwrap = yes
#tcp_listen_port = 60
tcp_listen_queue = 5
tcp_max_per_addr = 1
#tcp_client_ports = 1024-65535
tcp_client_max_idle = 0
transport = TCP
krb5_principal = auditd
#krb5_key_file = /etc/audit/audit.key
distribute_network = no
q_depth = 400
overflow_action = SYSLOG
max_restarts = 10
plugin_dir = /etc/audit/plugins.d
```

Preguntas:

25. ¿Qué herramienta de auditoría se utiliza comúnmente en sistemas UNIX-LINUX para rastrear los accesos y actividades de los usuarios?

a) iptables

b) auditd

c) firewalld

d) cron

26. ¿Cuál es la principal diferencia entre los módulos de auditoría de auditd y los controles de acceso de SELinux?

a) auditd registra eventos, mientras que SELinux aplica políticas de seguridad

b) auditd permite el control de acceso, mientras que SELinux se utiliza solo para la auditoría

c) auditd es más eficaz para controlar el acceso físico, mientras que SELinux se usa para aplicaciones web

d) No hay diferencia, ambos realizan las mismas funciones

27. Al configurar auditd, ¿qué significa la opción -F auid=<uid> al crear una regla?

a) Auditar eventos relacionados con una identificación de usuario específica

b) Auditar todos los eventos de acceso de usuario

c) Filtrar eventos de auditoría por tipo de acción

d) Especificar el usuario para el que se realizan las auditorías en tiempo real

28. ¿Qué comando permite ver los logs generados por auditd en Linux?

a) auditctl

b) ausearch

c) logwatch

d) dmesg

29. ¿Cuál es la forma correcta de auditar todos los tipos de acceso al archivo /etc/apache2/apache.conf con auditd?

a) auditctl -w /etc/apache2/apache.conf -p rwxa

b) auditctl -w /etc/apache2/apache.conf -p r

c) auditctl -a always,exit -F path=/etc/apache2/apache.conf

d) auditctl -w /etc/apache2/apache.conf -p -all

30. En un sistema configurado con SELinux, ¿cuál es el principal objetivo de utilizar la política de control de acceso basada en roles (RBAC)?

a) Permitir que los usuarios gestionen sus propios archivos de configuración

b) Proteger el sistema de malware con roles objetivo en tiempo rea

c) Controlar el acceso a las funciones del sistema según el rol del usuario, minimizando privilegios

d) Deshabilitar temporalmente la auditoría de archivos críticos

31. Según la configuración descrita en el fichero de configuración de este supuesto, ¿cuál es el tamaño máximo para el fichero de log?

a) 8 GB

b) 8 MB

c) 8 KB

d) 16 MB siempre que haya 50 libres

32. Según la configuración descrita en el fichero de este supuesto, ¿cuál es el número de ficheros de log que se desea mantener?

a) 8

b) 5

c) 4

d) 50

33. ¿Qué archivo de configuración contiene la lista de los eventos que auditd debe registrar, y qué tipo de información se guarda?

a) /etc/audit/auditd.conf

b) /etc/audit/rules.d/audit.rules

c) /etc/audit/sudoers

d) /etc/auditd.conf

34. En el entorno de sistemas Windows, ¿cómo se llama el proceso de auditoría y dónde se pueden visualizar los registros generados?

a) Windows Security Event Management, accesible desde el "Administrador de Directivas de Grupo"

c) Windows Logging Service, accesible desde la "Herramienta de Seguridad de Windows"

b) Windows Audit Manager, accesible desde "Política de Seguridad Local

d) Windows Security Auditing, accesible desde el "Visor de eventos de Windows"

35. Si se tratara de un entorno de sistemas Windows, ¿qué identificador de evento, visualizable en el Visor de eventos, indica que ha habido acceso a archivos auditados?

a) ID 4663

b) ID 4624

c) ID 4720

d) ID 5038

36. En el entorno de sistemas Windows, ¿qué comando se utiliza para abrir el Editor de directivas de seguridad local?

a) gpedit.msc

b) secpol.msc

c) eventvwr.msc

d) rsop.msc

SUPUESTO 4

En la administración de sistemas y redes, la capacidad de diagnosticar problemas de conectividad es fundamental. Las redes modernas son complejas, y los fallos pueden surgir en cualquier punto: desde una mala configuración de interfaces locales hasta una alta latencia en un enlace remoto.

Para enfrentar estos desafíos, los sistemas Unix/Linux ofrecen un conjunto de herramientas que permiten verificar la conectividad, investigar problemas de red y analizar el estado de las conexiones. Entre las más utilizadas se encuentran: ping, traceroute, netstat, ss, etc.

El dominio de estas utilidades permite detectar problemas como caídas de red, puertos abiertos no deseados, pérdida de paquetes o fallos en la resolución DNS.

Preguntas:

37. ¿Cuál es la función principal del comando ping?

a) Configurar interfaces de red

b) Medir latencia y comprobar la conectividad entre mi dispositivo y otro en la red

c) Analizar tráfico en tiempo real

d) Establecer conexiones TCP

38. ¿Qué protocolo utiliza ping por defecto para enviar sus paquetes?

a) ARP

b) TCP

c) UDP

d) ICMP

39. ¿Qué significa un alto valor en el tiempo de respuesta (time) en ping?

a) El host está desconectado

b) El host no responde con ICMP

c) Hay latencia en la conexión

d) Es un error de redirección DNS

40. ¿Qué opción de ping permite definir el número de paquetes a enviar?

a) -s

b) -c

c) -n

d) -l

41. ¿Cuál es el propósito principal del comando ss?

a) Analizar tráfico de red en tiempo real

b) Mostrar estadísticas de uso de disco

c) Mostrar información sobre sockets y conexiones de red

d) Resolver nombres de dominio

42. ¿Qué significa la opción l en ss -tuln?

a) Muestra sockets en estado de escucha

b) Muestra solo sockets en estado cerrado

c) Lista solo sockets locales

d) Limita la salida a 10 líneas

43. ¿Qué opción de ss se utiliza para mostrar todos los sockets, incluyendo los inactivos y cerrados?

a) -A

b) -a

c) -e

d) -t

44. ¿Cuál es el propósito principal del comando traceroute?

a) Determinar la dirección IP de un dominio

b) Medir el uso de CPU de un proceso

c) Mostrar la ruta que toma un paquete para llegar a su destino

d) Ver las conexiones TCP activas

45. ¿Qué protocolo utiliza traceroute por defecto en Linux?

a) TCP

b) ICMP

c) HTTP

d) UDP

46. ¿Qué opción se puede usar con traceroute para especificar el número máximo de saltos?

a) -n

b) -m

c) -t

d) -h

47. En el entorno de sistemas Windows, ¿qué comando de netstat muestra todas las conexiones activas, incluyendo los IDs de proceso (PID) y las direcciones en formato numérico?

a) netstat -a

b) netstat -n

c) netstat -ano

d) netstat -apn

48. netsh es una herramienta avanzada de sistemas Windows que permite configurar, diagnosticar y administrar la red. ¿Cuál de los siguientes comandos permite habilitar el firewall con dicha herramienta y que esté activo en todas las conexiones?

a) netsh advfirewall set allprofiles state on

b) netsh advfirewall state on

c) netsh advfirewall set domain state enable

d) netsh advfirewall state enable