Solución de problemas y gestión de un servidor de Cyber Vision Center

Contenido

Introducción

Este documento describe los diversos pasos que se pueden tomar para mantener, resolver problemas y monitorear un Cisco Cyber Vision Server.

Cisco Cyber Vision le ofrece una vista detallada de su estado de seguridad de la tecnología operativa (TO). Cyber Vision proporciona a sus herramientas de seguridad de TI información sobre los activos y eventos de TO, lo que facilita la gestión de riesgos y la aplicación de políticas de seguridad en toda la red.

Actualizaciones de servidor

Mantenga el servidor actualizado para encontrar correcciones de vulnerabilidades, correcciones de errores y nuevas funciones que se integren en el software en función de los escenarios de implementación.

Estado del sistema

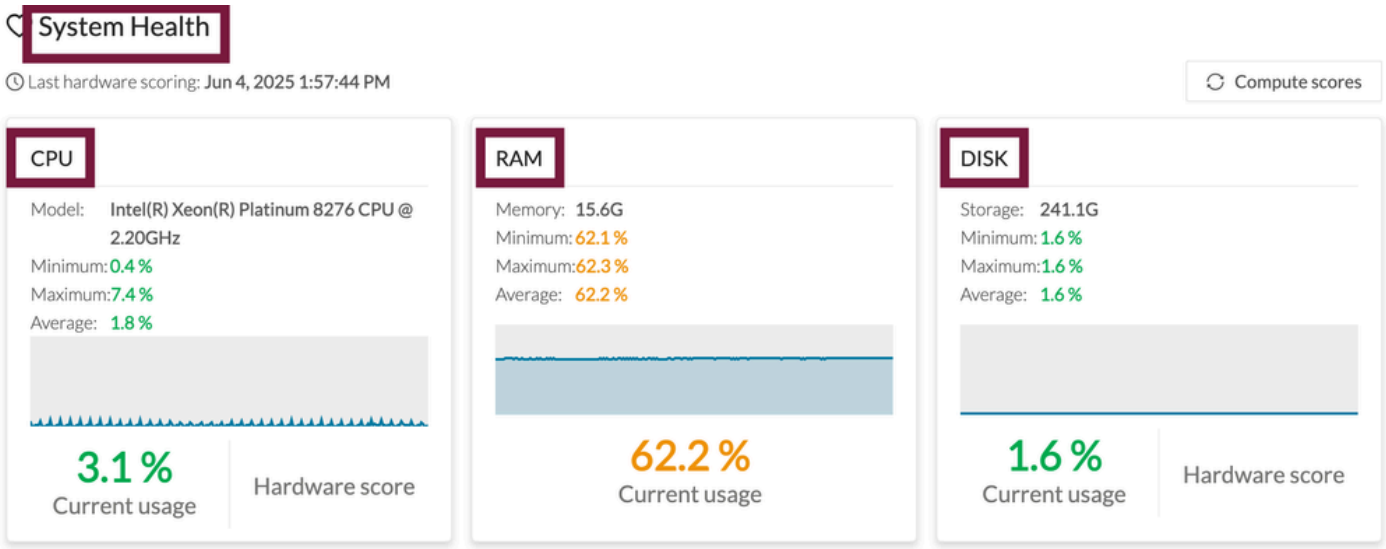
- Configuración de trampas SNMPv3 para enviar alertas de estado del sistema

En la interfaz de usuario (para comprobar el valor histórico):

Desplácese hasta Estadísticas del sistema (centro o sensores) y compruebe el uso de la CPU y la RAM.

- Se espera que los sensores en torno al 60% de la RAM y el 40% de la CPU estén en condiciones normales.
- Se espera que los centros con aproximadamente un 80% de RAM y una CPU con un 50%

se encuentren en condiciones normales.



Estos son valores utilizados como referencia. Estos recursos pueden llegar a porcentajes muy altos, pero se espera que regresen después de la finalización de una tarea específica, pero no permanecerán allí.

Desde la CLI (comprobación en tiempo real):

Utilice el comando top para verificar el uso de la CPU y la RAM para comprender qué procesos están consumiendo los recursos.

Se puede verificar usando el comando:

'top -n 1 -b' | head -n 5

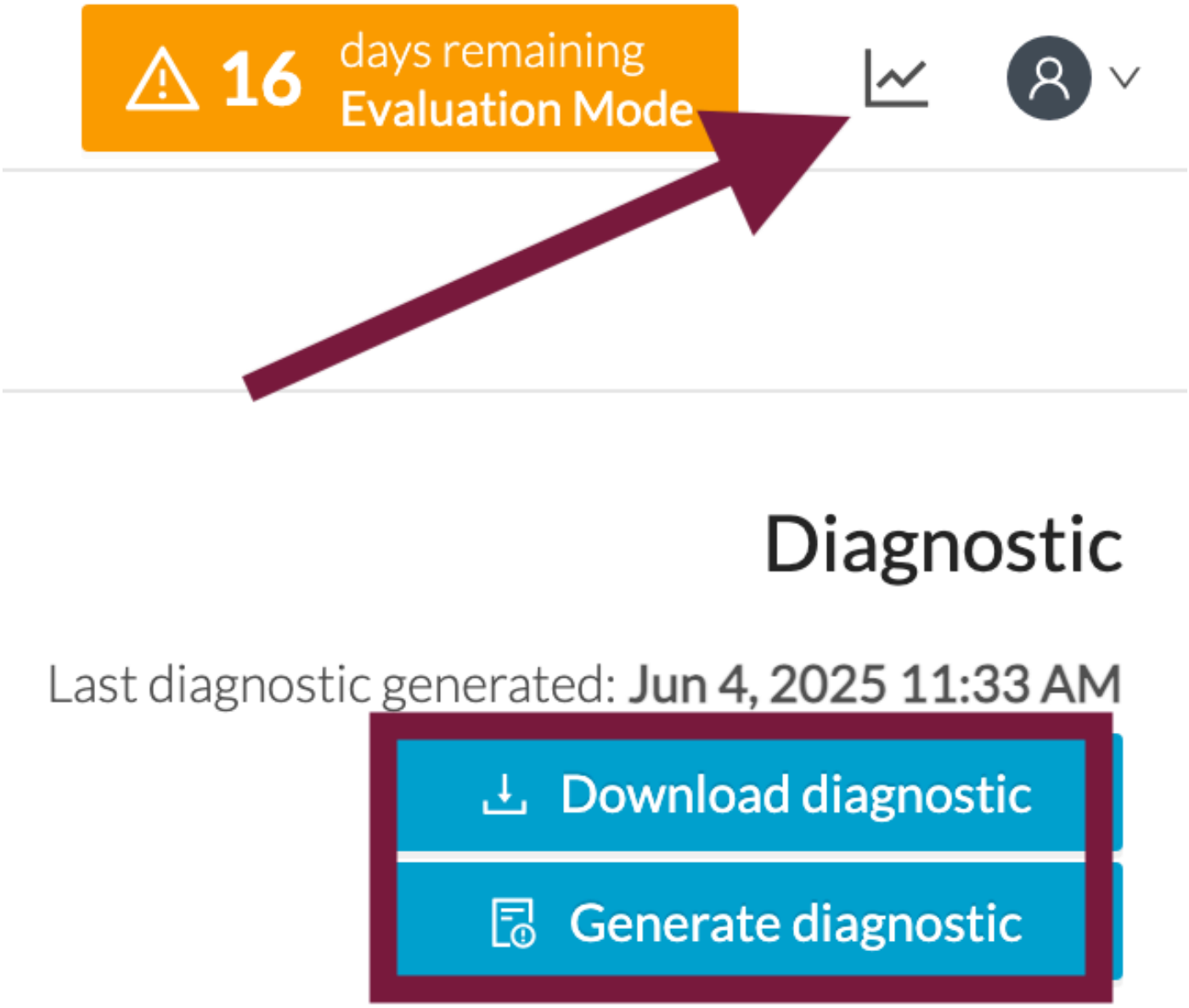
Verifique los procesos del sistema mediante el comando systemctl —failed. Este comando se usa comúnmente para solucionar problemas e identificar servicios o unidades que no se iniciaron o detuvieron inesperadamente.

Registros del sistema

Hay varios registros disponibles en la plataforma:

Desde la interfaz de usuario:

Genere un archivo de diagnóstico. Vaya a Estadísticas del sistema (centro o sensores) y haga clic en Generar diagnóstico.



Desde la CLI:

Utilice el comando sudo -i para acceder al modo de usuario raíz

Utilice los comandos journaltcl para realizar un seguimiento de los registros del sistema.

journalctl -r (-r ✳ inversa)

journalctl —desde "2015-01-10" o —hasta "2015-01-11 03:00"

journalctl -u <process name>

journalctl -f (-f ✳ siguiente)

journalctl -p err (errors on system)

Además, el paquete de diagnóstico se puede iniciar mediante el comando sbs-diag

Registros avanzados

Los registros avanzados se pueden activar desde CLI para estos servicios:

sbs-backend

sbs-burrow

sbs-marmotd

sbs-lsyncd-collect

sbs-lsynd-communication

sbs-gsyncd

sbs-nad

sbs-aspic

pxgrid-agent

Utilice el comando sudo -i para acceder al modo de usuario raíz

Estos registros avanzados realmente pueden inundar el sistema con mensajes, por lo tanto, solo se deben usar cuando se trabaja con el equipo del TAC.

Espacio en disco

- Todos los datos que entran y analizan los sensores se almacenan en la base de datos.
- Supervise el espacio disponible en la partición /data mediante el comando df -h.
- Limpie las capturas de red en /data/tmp/captures/. Utilice el comando rm -rf /data/tmp/captures/* para eliminar todas las capturas si ya no son necesarias.
- Elimine todos los archivos de diagnóstico antiguos.
- Purgue los datos antiguos y no deseados de la base de datos mediante el comando sbs-db purge-xxxxx.

Validación de tráfico

Uso de iptables y TCPdump para seguir el flujo de tráfico.

Seguimiento de firewall

El firewall Iptables está activado en el servidor. Los paquetes descartados se registran como "DropInput and DropForward".

Verifique los contadores de iptables para verificar los paquetes descartados en él (iptables -L -n -v | grep Chain).

Busque paquetes perdidos en el registro (journalctl | grep Drop).

herramienta TCPdump

Se puede utilizar para observar y solucionar problemas del tráfico en la interfaz de red del servidor.

Si el tráfico se inunda, presione ctrl+c para detener la captura.

Examples

Para supervisar flujos NTP (UDP/TCP 123): tcpdump -i [ethX] port 123 :

Para supervisar el tráfico entrante/saliente desde un host específico: tcpdump -i [ethX] host 1.2.3.4

Para guardar la captura en un archivo pcap:

tcpdump -i [ethX] host 1.2.3.4 -r /data/tmp/your_file.pcap

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).