Risoluzione dei problemi e gestione di un server Cyber Vision Center

Sommario

Introduzione

Questo documento descrive i vari passaggi che è possibile eseguire per mantenere, risolvere i problemi e monitorare un Cisco Cyber Vision Server.

Cisco Cyber Vision offre una vista approfondita della postura di sicurezza della tecnologia operativa (OT). Cyber Vision fornisce agli strumenti di sicurezza IT informazioni sugli asset e gli eventi OT, semplificando la gestione dei rischi e l'applicazione di policy di sicurezza in tutta la rete.

Aggiornamenti server

Mantenere aggiornato il server per le correzioni di vulnerabilità, bug e nuove funzionalità che vengono integrate nel software in base agli scenari di distribuzione.

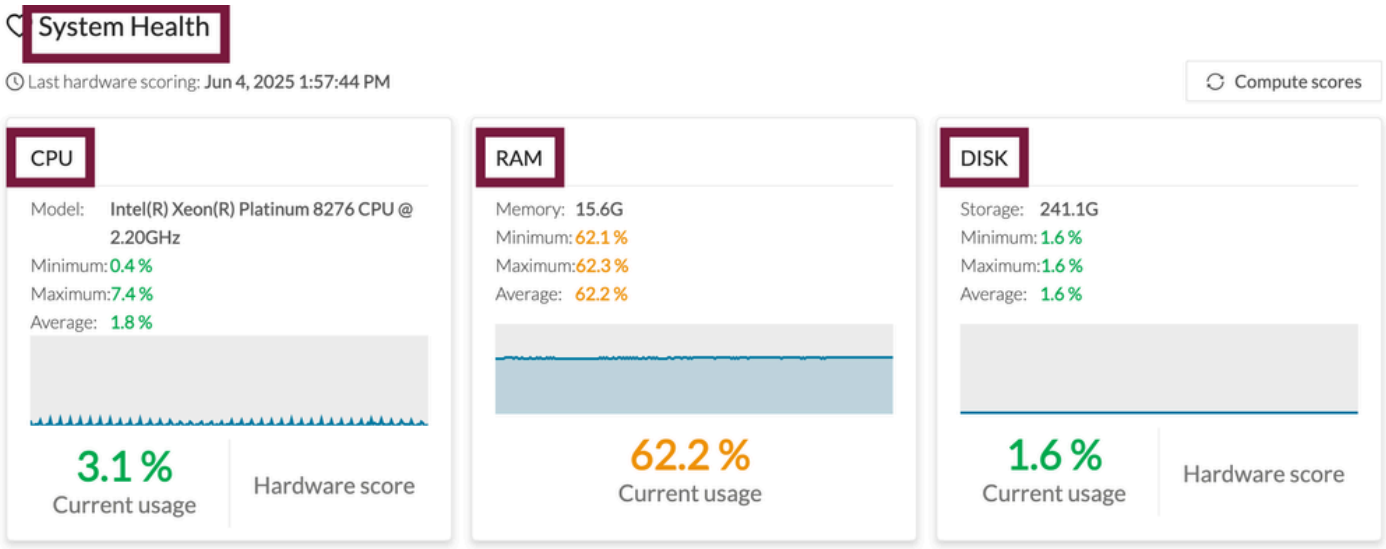
Integrità del sistema

- Configurare i trap SNMPv3 per l'invio di avvisi sullo stato del sistema

Dall'interfaccia utente (per controllare il valore storico):

Passare a Statistiche di sistema (centro o sensori) e verificare l'utilizzo della CPU e della RAM.

- Ci si aspetta che i sensori circa il 600% della RAM e la CPU il 40% siano in condizioni normali.
- Si prevede che circa l'80% della RAM e il 50% della CPU siano in condizioni normali.



Si tratta di valori utilizzati come riferimento. Queste risorse possono raggiungere percentuali molto elevate, ma si prevede che tornino dopo il completamento di un'attività specifica, ma non vi rimangano.

Dalla CLI (controllo in tempo reale):

Utilizzare il comando top per verificare l'utilizzo della CPU e della RAM e individuare i processi che utilizzano le risorse.

È possibile verificarlo con il comando:

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

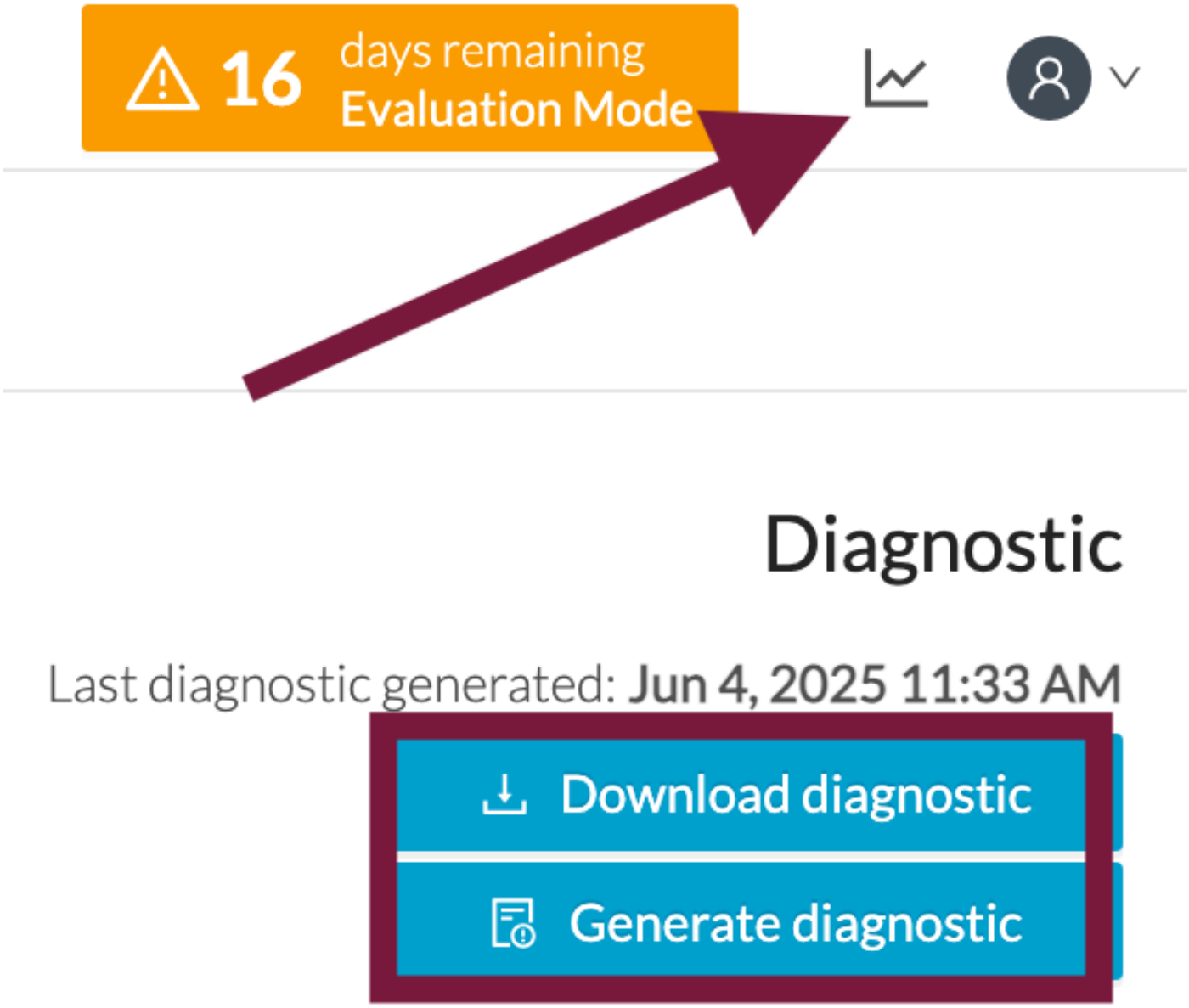
Verificare i processi di sistema utilizzando il comando systemctl —failed. Questo comando viene in genere utilizzato a scopo di risoluzione dei problemi per identificare servizi o unità che non sono stati avviati o arrestati in modo imprevisto.

Log di sistema

Sulla piattaforma sono disponibili diversi log:

Dalla UI:

Generare un file di diagnostica. Andare su Statistiche di sistema (Centro o Sensori) e fare clic su Genera diagnostica.



Dalla CLI:

Utilizzare il comando sudo -i per accedere alla modalità utente root

Utilizzare i comandi journal per tenere traccia dei registri di sistema.

journalctl -r (-r ✳ inverso)

journalctl —da "2015-01-10"o —fino a "2015-01-11 03:00"

journalctl -u <nome processo>

journalctl -f (-f ✳ seguire)

journalctl -p err (errori di sistema)

Inoltre, il pacchetto di diagnostica può essere avviato usando il comando sbs-diag

Log avanzati

I registri avanzati possono essere attivati dalla CLI per i seguenti servizi:

sbs-backend

sbs-burrow

sbs-marmotd

sbs-lsyncd-gather

comunicazione sbs-lsynd

sbs-gsyncd

sbs-nad

sbs-aspic

pxgrid-agent

Utilizzare il comando sudo -i per accedere alla modalità utente root

Questi registri avanzati possono inondare il sistema di messaggi, quindi devono essere utilizzati solo se si collabora con il team TAC.

Spazio su disco

- Tutti i dati in entrata e analizzati da Sensor vengono memorizzati nel database.
- Monitorare lo spazio disponibile nella partizione /data utilizzando il comando df -h.
- Pulire le acquisizioni di rete in /data/tmp/capture/. Utilizzare il comando rm -rf /data/tmp/capture/* per eliminare tutte le acquisizioni se non sono più necessarie.
- Elimina tutti i file di diagnostica meno recenti.
- Eliminare i dati obsoleti e indesiderati nel database utilizzando il comando sbs-db purge-xxxxx.

Convalida traffico

Uso di iptables e TCPdump per seguire il flusso del traffico.

Tracciamento firewall

Firewall iptables abilitato sul server. I pacchetti ignorati vengono registrati come "DropInput e DropForward".

Verificare i contatori iptables per controllare i pacchetti ignorati (iptables -L -n -v | grep Chain).

Cerca pacchetti ignorati nel registro (journalctl) | grep (calo).

Strumento TCPdump

Può essere utilizzato per l'osservazione e la risoluzione dei problemi di traffico sull'interfaccia di rete del server.

Se il traffico viene inondato, premere ctrl+c per interrompere la cattura.

Esempi

Per monitorare i flussi NTP (UDP/TCP 123): tcpdump -i [ethX] porta 123 :

Per monitorare il traffico in entrata/in uscita da un host specifico: tcpdump -i [ethX] host 1.2.3.4

Per salvare l'acquisizione in un file pcap:

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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).