Solucione problemas e gerencie um servidor Cyber Vision Center

Contents

Introdução

Este documento descreve as várias etapas que podem ser executadas para manter, solucionar problemas e monitorar um Cisco Cyber Vision Server.

O Cisco Cyber Vision oferece uma visão detalhada da postura de segurança da tecnologia operacional (TO). O Cyber Vision alimenta suas ferramentas de segurança de TI com informações sobre ativos e eventos de TO, facilitando o gerenciamento de riscos e a aplicação de políticas de segurança em toda a rede.

Atualizações do servidor

Mantenha o servidor atualizado para correções de vulnerabilidades, correções de bugs e novos recursos que se integram ao software com base em cenários de implantação.

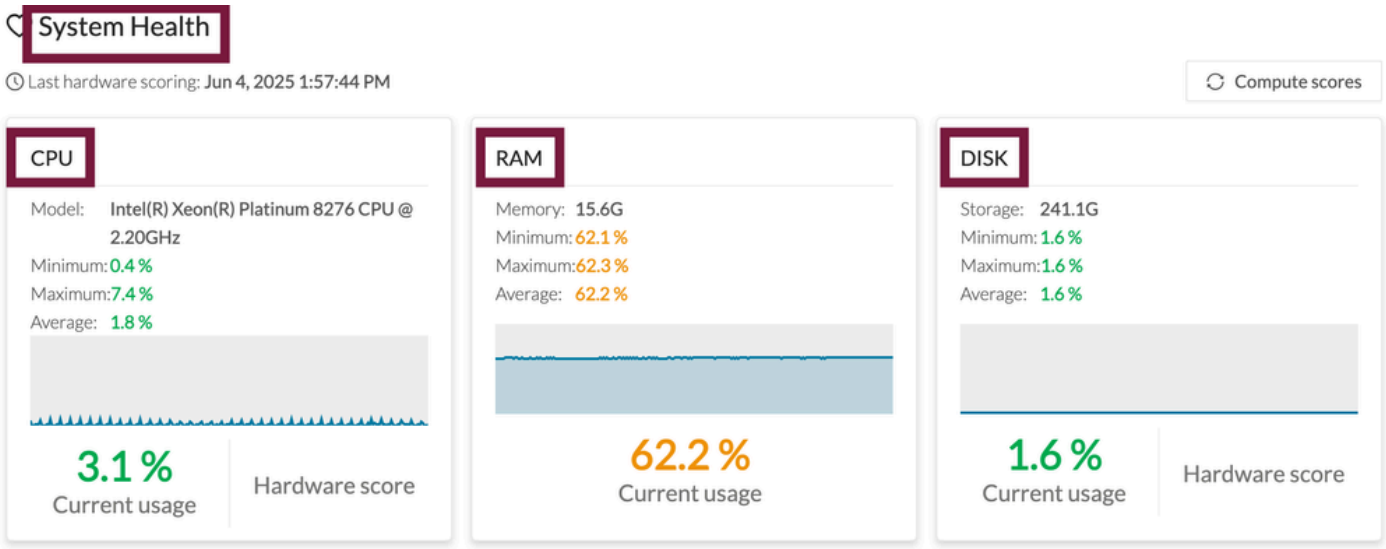
Integridade do Sistema

- Configurar interceptações SNMPv3 para enviar alertas de integridade do sistema

Na interface do usuário (para verificar o valor histórico):

Navegue até System Statistics (Center ou Sensors) (Estatísticas do sistema (Centro ou Sensores)) e verifique a utilização da CPU e da RAM.

- Espera-se que os sensores com cerca de 600% de RAM e 40% de CPU estejam em condições normais.
- Centra cerca de 80% de RAM e CPU 50% devem estar em condição normal.



Esses são valores usados como referência. Esses recursos podem atingir percentuais muito altos, mas espera-se que voltem após a conclusão de uma tarefa específica, mas não permaneçam lá.

Na CLI (verificação em tempo real):

Use o comando top para verificar a utilização da CPU e da RAM e entender quais processos estão consumindo os recursos.

Ele pode ser verificado usando o comando:

'top -n 1 -b' | cabeça -n 5

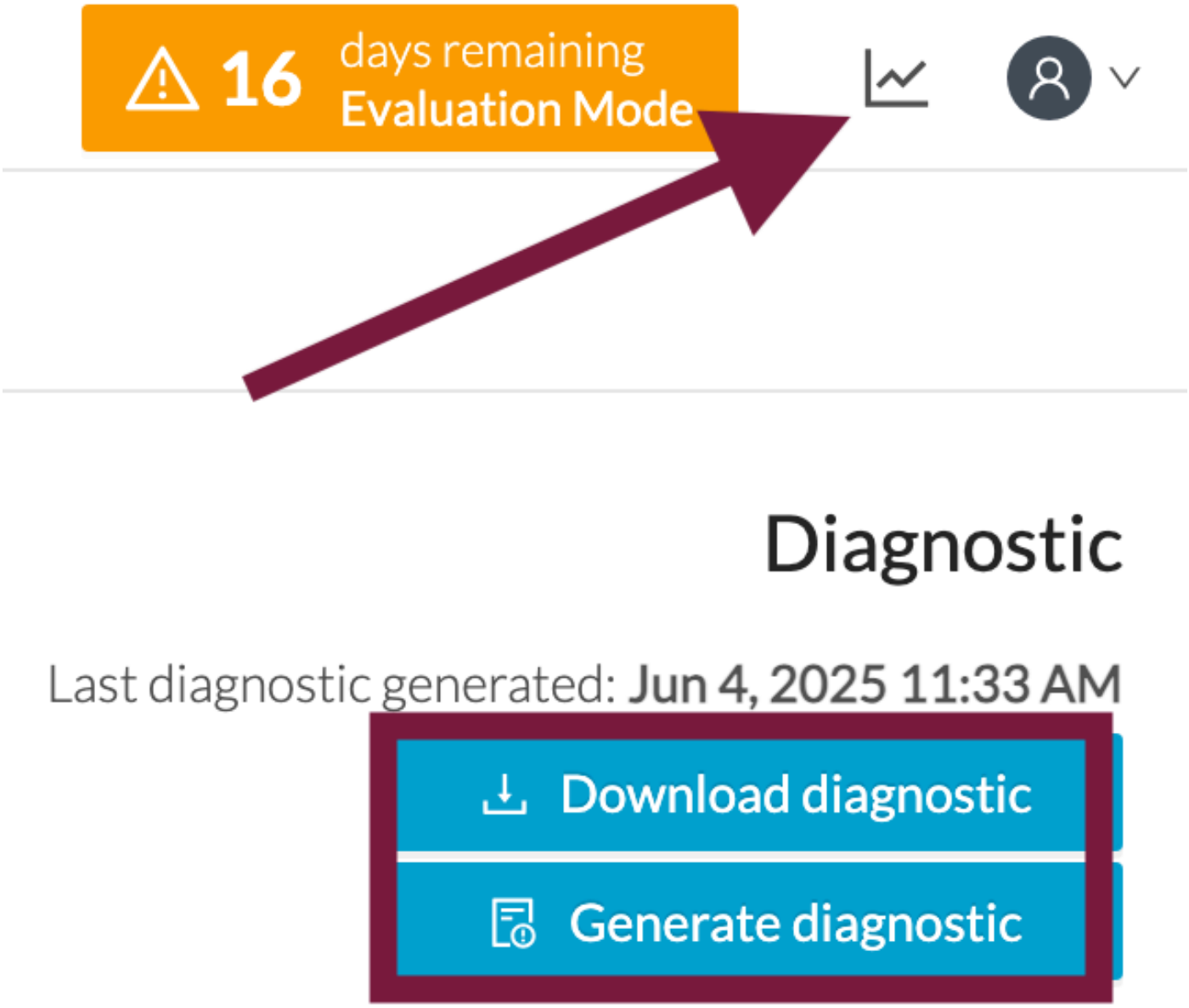
Verifique os processos do sistema usando o comando systemctl —failed. Esse comando é geralmente usado para fins de solução de problemas para identificar serviços ou unidades que não iniciaram ou pararam inesperadamente.

Registros de sistema

Vários registros estão disponíveis na plataforma:

Na interface do usuário:

Gere um arquivo de diagnóstico. Acesse System Statistics (Center ou Sensors) (Estatísticas do sistema (Centro ou Sensores)) e clique em Generate Diagnostic (Gerar diagnóstico).



Na CLI:

Usar o comando sudo -i para acessar o modo de usuário root

Use comandos journaltcl para rastrear logs do sistema.

journalctl -r (-r ✳ reverso)

journalctl —desde "2015-01-10"ou —até "2015-01-11 03:00"

journalctl -u <nome do processo>

journalctl -f (-f ✳ seguir)

journalctl -p err (erros no sistema)

Além disso, o pacote de diagnósticos pode ser iniciado com o comando sbs-diag

Logs avançados

Os logs avançados podem ser ativados pela CLI para estes serviços:

back-end SBS

sbs-burrow

sbs-marmotd

sbs-lsyncd-collect

sbs-lsynd-communication

sbs-gsyncd

sbs-nad

sbs-aspic

pxgrid-agent

Usar o comando sudo -i para acessar o modo de usuário root

Esses registros avançados podem inundar o sistema com mensagens, portanto, devem ser usados somente ao trabalhar com a equipe do TAC.

Espaço em disco

- Todos os dados recebidos e analisados pelos sensores são armazenados no banco de dados.
- Monitore o espaço disponível na partição /data usando o comando df -h.
- Limpe suas capturas de rede em /data/tmp/captures/. Use o comando rm -rf /data/tmp/captures/* para excluir todas as capturas se elas não forem mais necessárias.
- Exclua todos os arquivos de diagnóstico mais antigos.
- Limpe dados antigos e indesejados no banco de dados usando o comando sbs-db purge-xxxxx.

Validação de tráfego

Usando iptables e TCPdump para seguir seu fluxo de tráfego.

Rastreamento de firewall

O firewall Iptables está habilitado no servidor. Os pacotes descartados são registrados como "DropInput e DropForward".

Verifique os contadores iptables para verificar os pacotes descartados (iptables -L -n -v | grep

Chain)

Procure pacotes descartados no registro (journalctl | grep Drop

ferramenta TCPdump

Ele pode ser usado para observar e solucionar problemas de tráfego na interface de rede no servidor.

Se o tráfego ficar inundado, pressione ctrl+c para interromper a captura.

Examples

Para monitorar fluxos de NTP (UDP/TCP 123): tcpdump -i [ethX] porta 123 :

Para monitorar o tráfego de entrada/saída de um host específico: tcpdump -i [ethX] host 1.2.3.4

Para salvar a captura em um arquivo pcap:

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

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.