Dépannage et gestion d'un serveur Cyber Vision Center

Table des matières

Introduction

Ce document décrit les différentes étapes qui peuvent être prises pour maintenir, dépanner et surveiller un serveur Cisco Cyber Vision.

Cisco Cyber Vision vous offre une vue détaillée de votre stratégie de sécurité des technologies opérationnelles. Cyber Vision alimente vos outils de sécurité informatique avec des informations sur les ressources et les événements des technologies opérationnelles, ce qui facilite la gestion des risques et l'application des politiques de sécurité sur l'ensemble de votre réseau.

Mises à jour serveur

Tenez le serveur à jour pour obtenir les correctifs de vulnérabilité, les correctifs de bogues et les nouvelles fonctionnalités qui s'intègrent au logiciel en fonction des scénarios de déploiement.

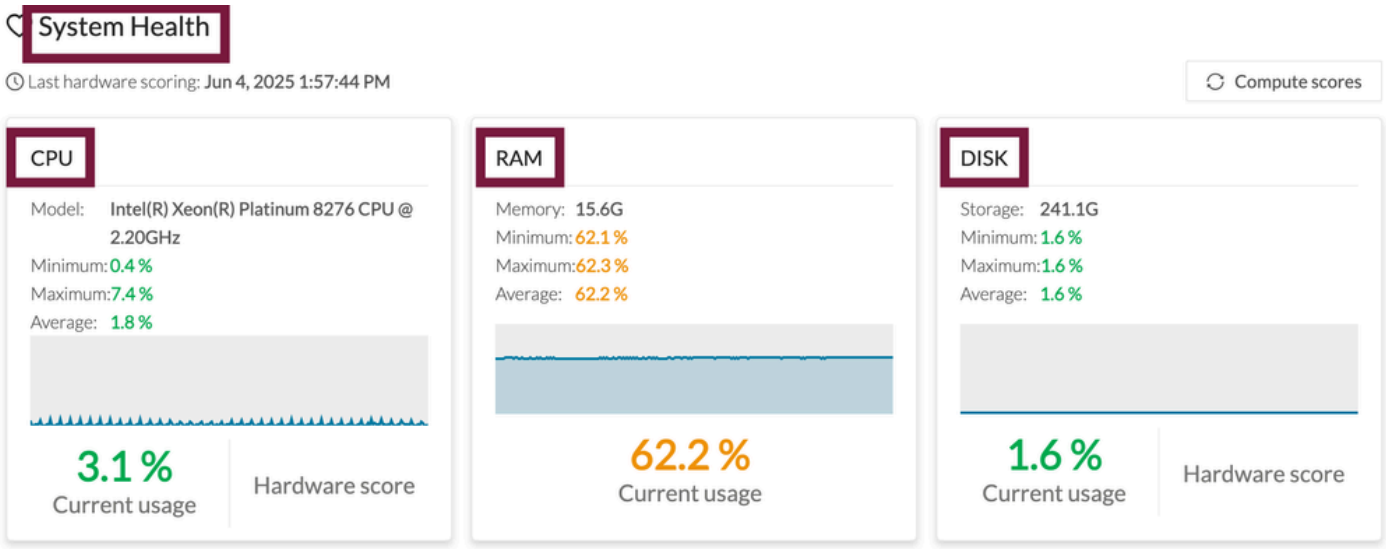
État du système

- Configurer les déroutements SNMPv3 pour envoyer des alertes d'intégrité système

À partir de l'interface utilisateur (pour vérifier la valeur historique) :

Accédez à System Statistics (Center ou Sensors) et vérifiez l'utilisation du processeur et de la mémoire vive.

- Les capteurs d'environ 600 % de RAM et 40 % de CPU devraient être dans un état normal.
- Centralise environ 80 % de RAM et 50 % de CPU dans des conditions normales.



Il s'agit de valeurs utilisées comme référence. Ces ressources peuvent atteindre des pourcentages très élevés, mais on s'attend à ce qu'elles reviennent après l'achèvement d'une tâche précise, mais elles ne resteront pas là.

À partir de l'interface de ligne de commande (vérification en temps réel) :

Utilisez la commande top pour vérifier l'utilisation du processeur et de la mémoire vive afin de déterminer quels processus utilisent les ressources.

Elle peut être vérifiée à l’aide de la commande :

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

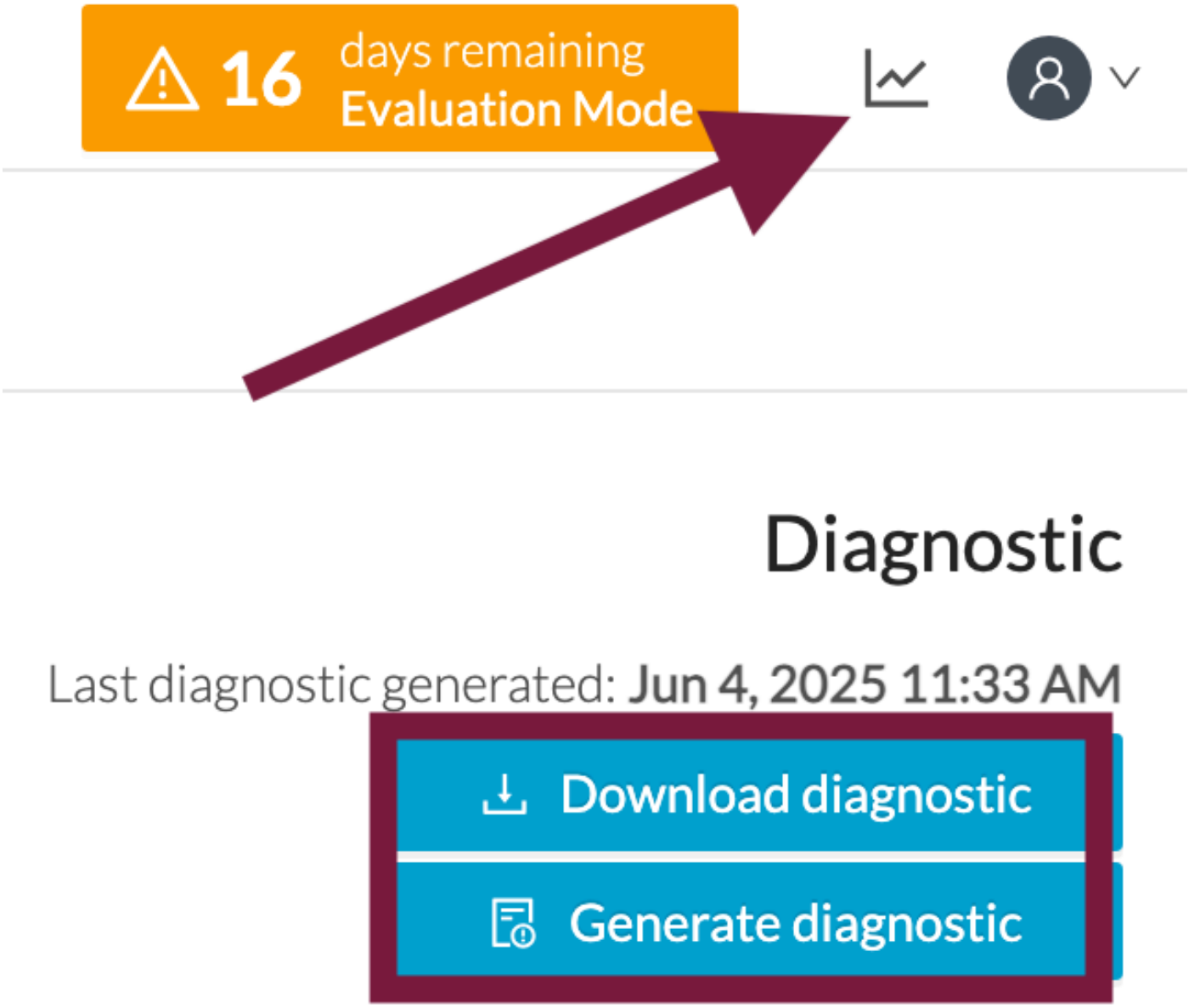
Vérifiez les processus système à l'aide de la commande systemctl —failed. Cette commande est généralement utilisée à des fins de dépannage pour identifier les services ou les unités qui n'ont pas démarré ou qui ne se sont pas arrêtés de manière inattendue.

Journaux du système

Plusieurs journaux sont disponibles sur la plate-forme :

Dans l'interface utilisateur :

Générez un fichier de diagnostic. Accédez à Statistiques système (Centre ou Capteurs) et cliquez sur Générer un diagnostic.



À partir de la CLI :

Utiliser la commande sudo -i pour accéder au mode utilisateur racine

Utilisez les commandes journalcl pour suivre les journaux système.

journalctl -r (-r ✳ inverse)

journalctl —depuis "2015-01-10" ou —jusqu'à "2015-01-11 03:00"

journalctl -u <nom du processus>

journalctl -f (-f ✳ suivre)

journalctl -p err (erreurs sur le système)

Vous pouvez également lancer l'ensemble de diagnostics à l'aide de la commande sbs-diag

Journaux avancés

Les journaux avancés peuvent être activés à partir de la CLI pour les services suivants :

sbs-backend

sous-terrier

sbs-marmotd

sbs-lsyncd-collect

sbs-lsynd-communiquer

sbs-gsyncd

sbs-nad

sbs-aspic

pxgrid-agent

Utiliser la commande sudo -i pour accéder au mode utilisateur racine

Ces journaux avancés peuvent véritablement inonder le système de messages. Par conséquent, ils ne doivent être utilisés qu'en collaboration avec l'équipe du centre d'assistance technique.

Espace disque

- Toutes les données entrantes et analysées par les capteurs sont stockées dans la base de données.
- Surveillez l'espace disponible dans la partition /data à l'aide de la commande df -h.
- Nettoyez vos captures réseau sous /data/tmp/captures/. Utilisez la commande rm -rf /data/tmp/captures/* pour supprimer toutes les captures si elles ne sont plus nécessaires.
- Supprimez tous les anciens fichiers de diagnostic.
- Purgez les données anciennes et indésirables dans la base de données à l'aide de la commande sbs-db purge-xxxxx.

Validation du trafic

Utiliser iptables et TCPdump pour suivre votre flux de trafic.

Suivi du pare-feu

Le pare-feu Iptables est activé sur le serveur. Les paquets abandonnés sont consignés en tant que « DropInput and DropForward ».

Vérifier les compteurs iptables pour vérifier les paquets abandonnés (iptables -L -n -v | chaîne

grep).

Recherchez les paquets abandonnés dans le journal (journalctl | grep Drop).

outil TCPdump

Il peut être utilisé pour observer et dépanner le trafic sur l'interface réseau du serveur.

Si le trafic est inondé, appuyez sur ctrl+c pour arrêter la capture.

Exemples

Pour surveiller les flux NTP (UDP/TCP 123) : tcpdump -i [ethX] port 123 :

Pour surveiller le trafic entrant/sortant d'un hôte spécifique : tcpdump -i [ethX] hôte 1.2.3.4

Pour enregistrer la capture dans un fichier pcap :

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

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.