Vérification de l'intégrité d'un cluster de charge de travail sécurisé (tétration)

Table des matières

Introduction

Ce document décrit les étapes de vérification de l'intégrité d'un cluster de charge de travail sécurisé et met en évidence les aspects clés à examiner lors du processus de vérification de l'intégrité.

Informations générales

Elle met l'accent sur la vérification de la santé; toutefois, si vous remarquez des problèmes ou un comportement anormal, vous devez collecter un instantané et contacter l'équipe d'assistance TAC de Cisco Tetration Solution Support pour obtenir de l'aide. Le cluster de charge de travail sécurisé est constitué de centaines de processus répartis sur plusieurs machines virtuelles sur plusieurs serveurs UCS C220.

Les deux principaux outils d'évaluation de l'état du cluster sont les pages État du cluster et État du service, qui sont toutes deux expliquées dans ce document. L'utilisation de ces pages est généralement le moyen le plus efficace de confirmer l'état de santé global de la grappe.

Quand vérifier l'intégrité du cluster

La plupart du temps, il n'est pas nécessaire de vérifier l'intégrité de votre cluster. Cependant, il y a certaines situations où c'est une bonne idée :

· Si vous remarquez quelque chose d'inhabituel ou d'inattendu dans l'interface utilisateur, d'après votre expérience du fonctionnement normal des choses. Certains exemples courants sont répertoriés dans la section Paramètres d'affichage opérationnels.

· Si vous vous attendez à voir certaines données (comme les données de flux provenant de

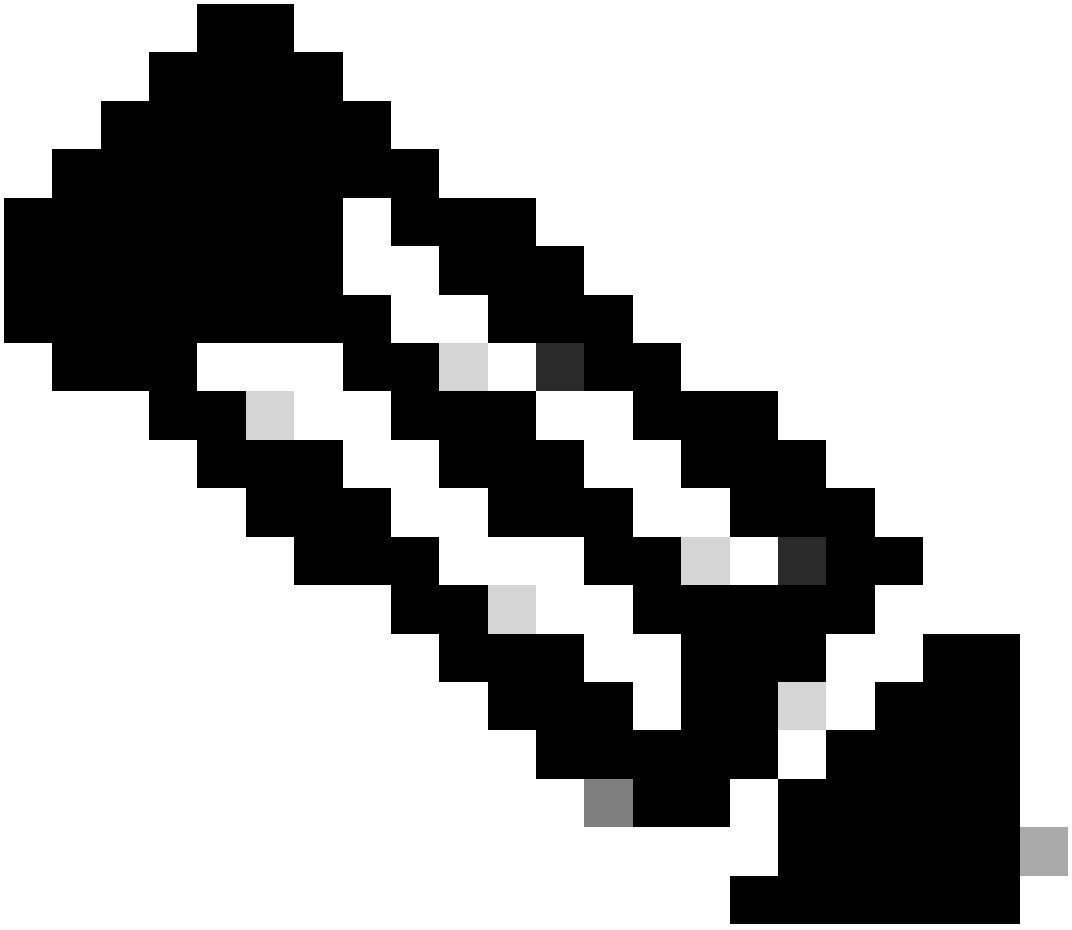
capteurs logiciels ou matériels) dans l'interface utilisateur, mais qu'elles sont manquantes même si vous avez sélectionné la portée et la plage temporelle appropriées.

· Avant et après toute maintenance planifiée, toute mise à niveau ou toute modification importante du cluster. Il est recommandé de prendre un instantané de l'état du cluster avant et après ces activités. Si vous avez besoin de contacter l'assistance du TAC, ces instantanés peuvent vous aider à identifier rapidement ce qui a changé.

Différentes options Vous devez vérifier l'intégrité du cluster de charge globale sécurisée

État du cluster

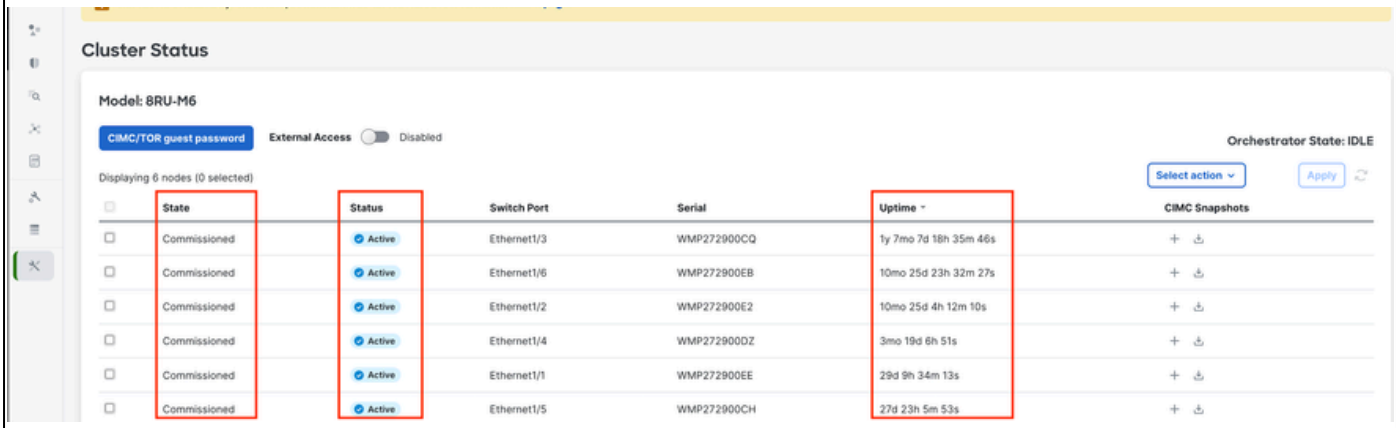
Un cluster de charge de travail sécurisé se compose de 6 serveurs (8RU) ou de 36 serveurs (39RU), selon le type de cluster. La page Cluster Status indique l'état des serveurs, ainsi que des informations sur les serveurs sans système d'exploitation.

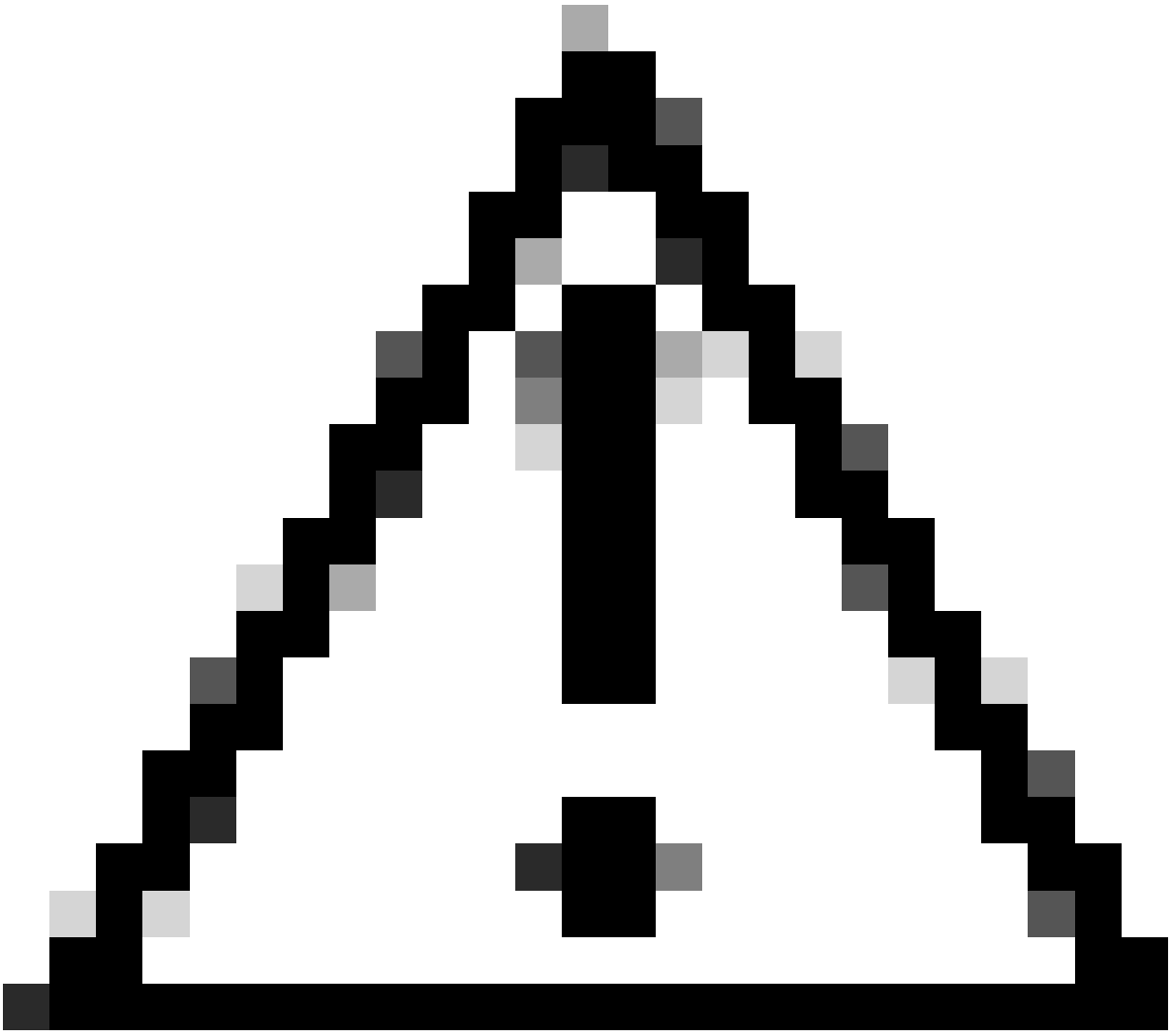


Remarque : La page État du cluster est accessible aux utilisateurs ayant des rôles d'administrateur de site ou d'assistance à la clientèle pour les clusters physiques. Les deux rôles peuvent afficher et effectuer des actions sur la page État du cluster.

Dans le volet de navigation, choisissez Troubleshoot > Cluster Status.

L'état du cluster indique l'état de tous les serveurs dans le rack Cisco Secure Workload. Un serveur en fonctionnement peut afficher l'état Commandé et l'état Actif, comme indiqué ici.





Mise en garde : Si vous remarquez un noeud marqué comme inactif sur la page d'état du cluster, générez un instantané CIMC et soulevez un cas TAC, y compris l'instantané.

Si l'état est Inactif, cela signifie généralement que le serveur est éteint ou peut être arrêté en raison d'un problème matériel, de câble ou de connectivité.

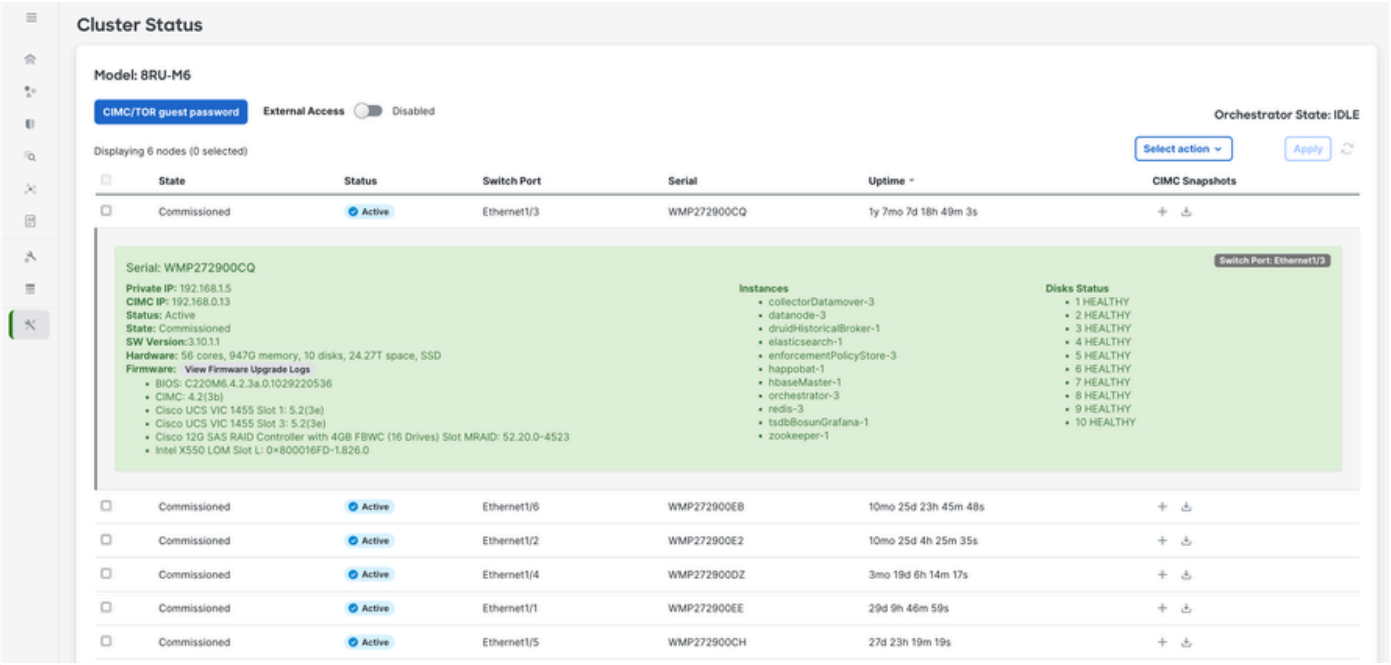
Lorsque vous cliquez sur un serveur dans la liste, vous voyez plus de détails, tels que

· Les machines virtuelles (instances) exécutées sur ce serveur physique

· Adresse IP privée du serveur au sein du cluster

· L’adresse IP CIMC (de gestion)

· Versions actuelles du microprogramme pour le BIOS, CIMC, la carte VIC, la carte LOM et le contrôleur RAID

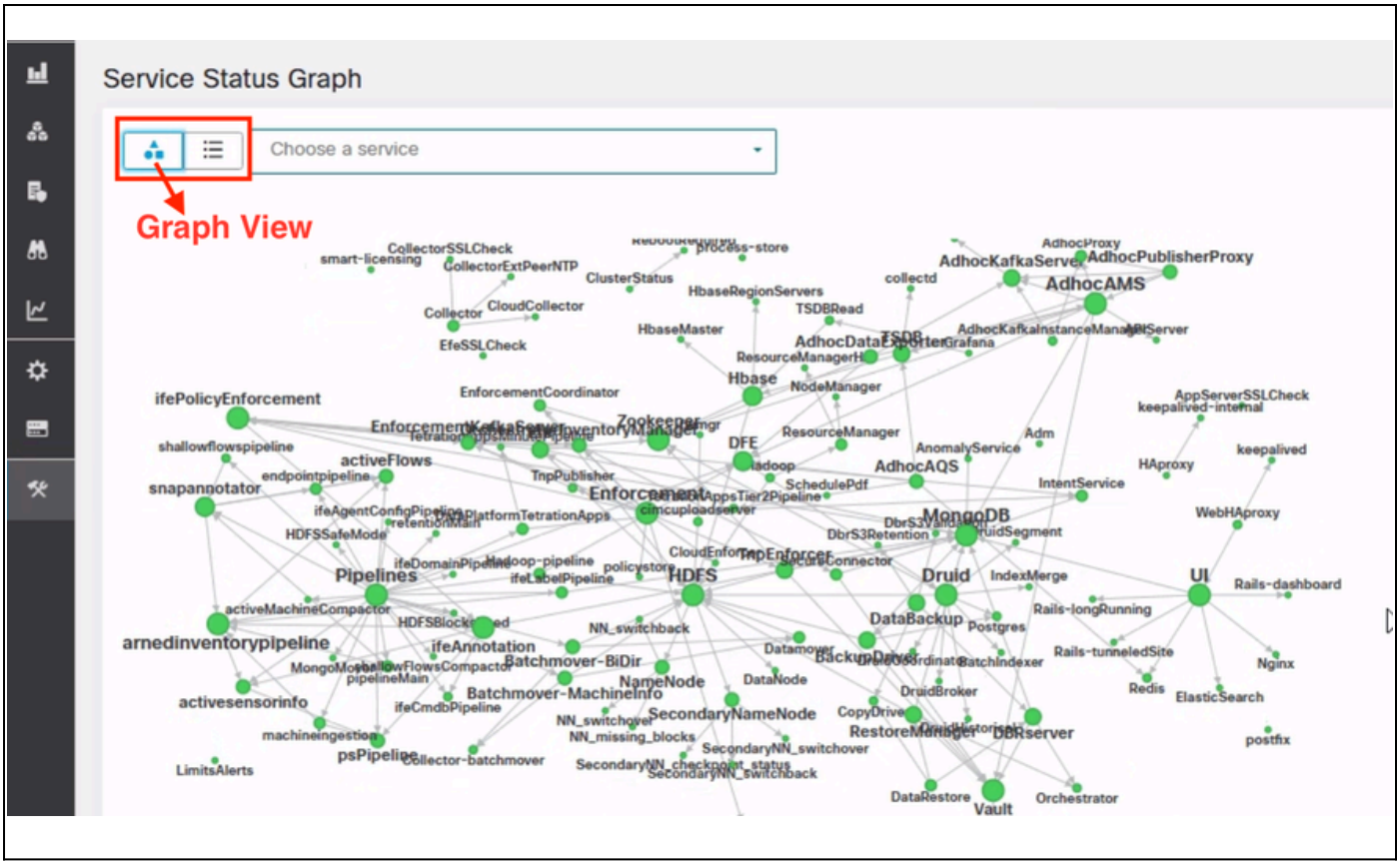


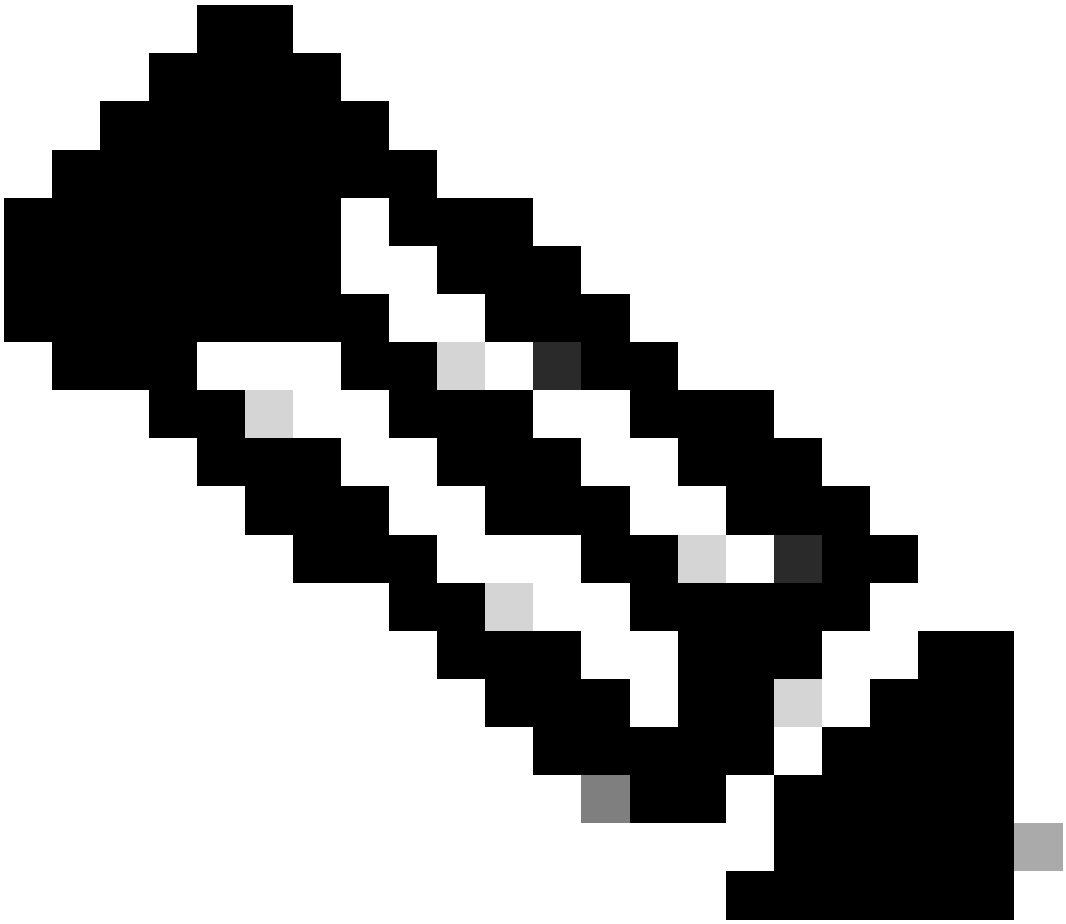
État du service

La page État du service se trouve dans le volet de navigation de gauche sous Dépannage > État du service.

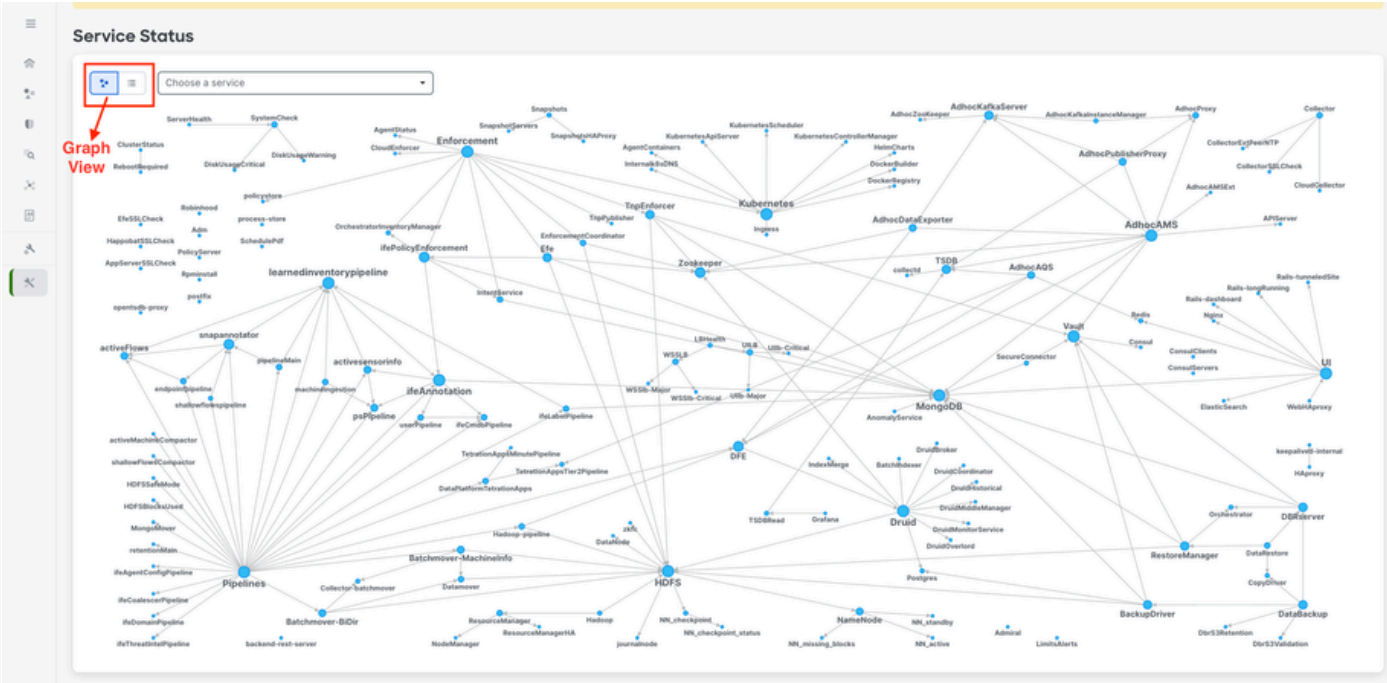
La page État du service affiche l'état de tous les services utilisés dans votre cluster de charge de travail CiscoSecure, ainsi que leurs dépendances.

La vue du graphique montre l'intégrité du service, chaque noeud du graphique montre l'intégrité du service et une périphérie représente la dépendance par rapport aux autres services. Les services défectueux sont marqués en rouge lorsque le service n'est pas disponible et en orange lorsque le service est dégradé mais disponible. Une couleur verte ou bleu ciel indique que le service est sain. Pour plus d'informations sur le débogage de ces noeuds, utilisez l'arborescence qui contient le bouton Développer tout pour afficher tous les noeuds enfants dans l'arborescence des dépendances. Down, indique que le service n'est pas fonctionnel, et Unhealth, indique que le service n'est pas entièrement fonctionnel.


Service Status Graph
Choose a service
Graph View
AdhocKafkaServer
AdhocPublisherProxy
AdhocAMS
collectd
HbaseRegionServers
TSDBRead
HbaseMaster
AdhocDataExporter
Grafana
ResourceManagerHA
Hbase
NodeManager
EnforcementCoordinator
ifePolicyEnforcement
Zookeeper
ResourceManager
DFE
AnomalyService
Adm
AdhocAQS
IntentService
SchedulePdf
shallowflowspipeline
activeFlows
endpointpipeline
snapannotator
TnpPublisher
Enforcement
MongoDB
DruidSegment
DbrS3Retention
HDFSSafeMode
TnpEnforcer
Pipelines
HDFS
Druid
IndexMerge
UI
Rails-dashboard
activeMachineCompactor
DataBackup
Postgres
Rails-longRunning
arnedinventorypipeline
ifeAnnotation
NN_switchback
Batchmover-BiDir
Datamover
BackupDevice
BatchIndexer
Rails-tunneledSite
Nginx
NameNode
DataNode
DruidBroker
Redis
ElasticSearch
activesensorinfo
Batchmover-MachineInfo
ifeCmdbPipeline
SecondaryNameNode
CopyDrive
RestoreManager
DBRserver
machineingestion
NN_switchover
NN_missing_blocks
SecondaryNN_switchover
psPipeline
postfix
LimitsAlerts
DataRestore
Vault
Orchestrator
AppServerSSLCheck
keepalived-internal
keepalived
HAproxy
WebHAproxy
CollectorSSLCheck
smart-licensing
CollectorExtPeerNTP
ClusterStatus
Collector
CloudCollector
EfeSSLCheck
process-store

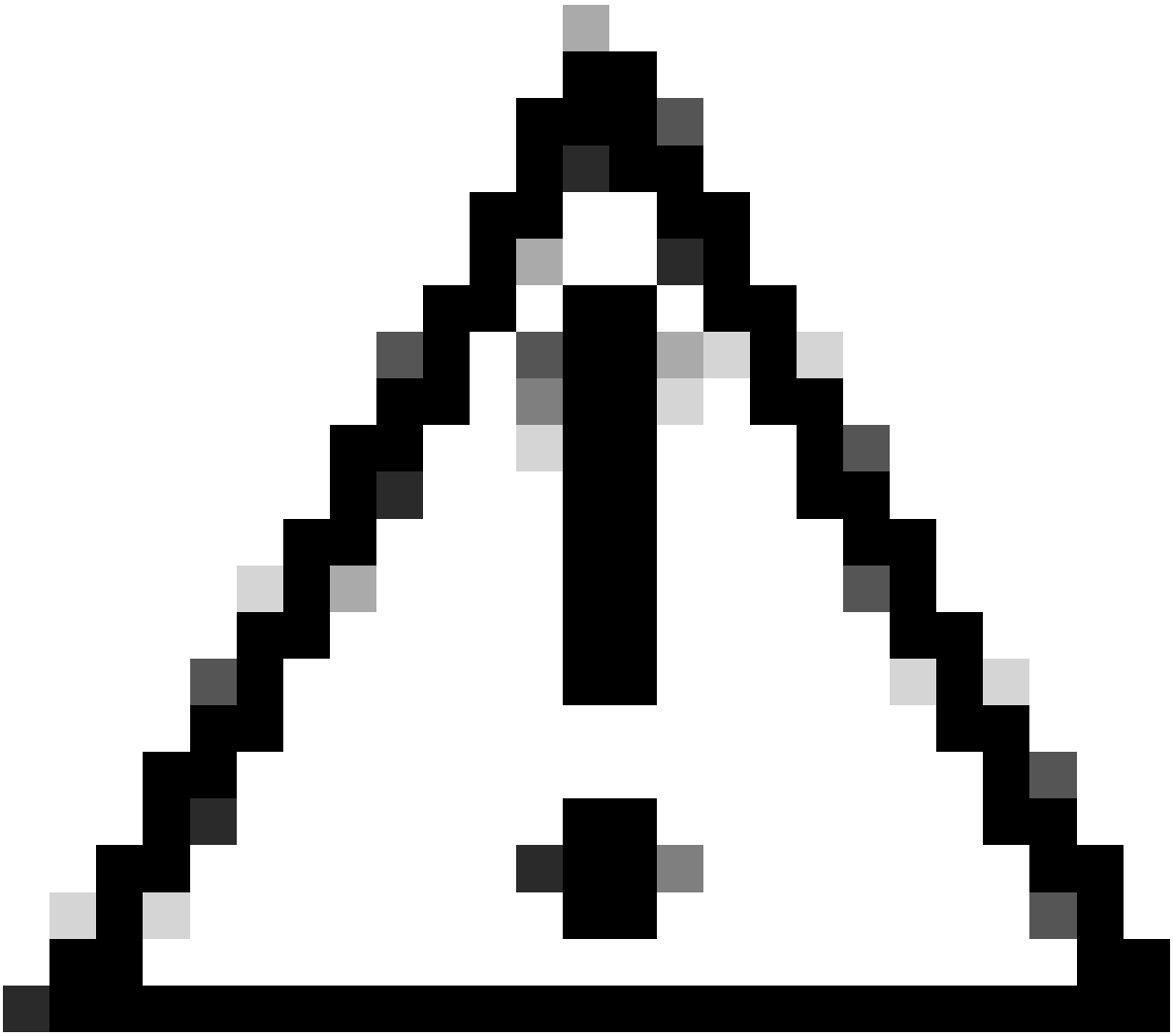


Remarque : À partir de la version 3.10.2.11 du correctif, la page d'état du service s'affiche en bleu ciel. Une couleur verte ou bleu ciel indique que le service est sain.

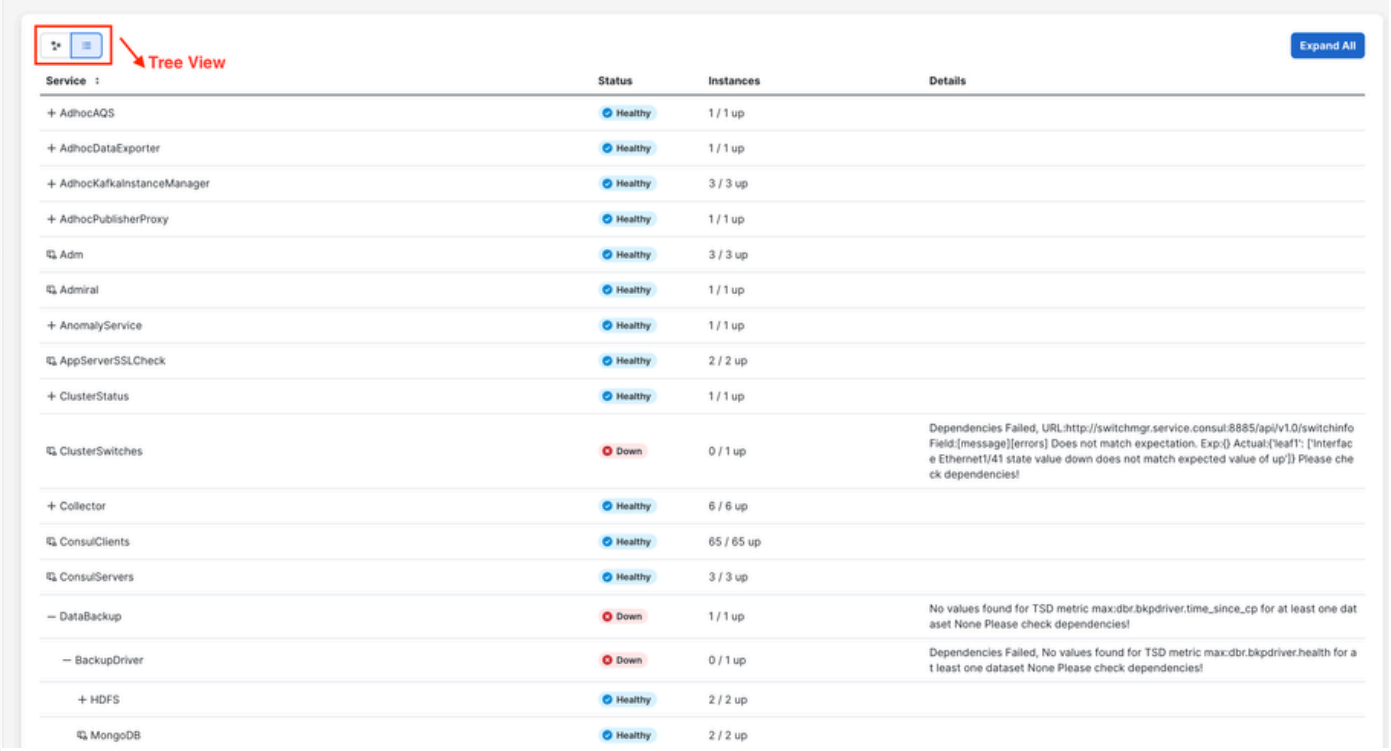


Par défaut, la page État du service affiche les fonctions et les dépendances du cluster dans une vue graphique. Si les icônes sont toutes vertes ou bleu ciel, aucune erreur n'est détectée.

Si un service s'affiche en rouge ou en orange, l'arborescence affiche la liste des services et vous permet d'effectuer une hiérarchisation vers le bas sur les dépendances du service ainsi que sur d'autres détails détectés par la fonction État du service. Ces informations d'erreur de dépendance sont particulièrement importantes à noter et à capturer lors de l'ouverture d'un dossier auprès du TAC.



Mise en garde : Si vous constatez que l'un des services n'est pas sain et s'affiche en rouge, contactez le centre d'assistance technique (TAC) pour obtenir de l'aide afin de résoudre ces problèmes. Un engagement rapide auprès du TAC peut aider à restaurer toutes les fonctionnalités.

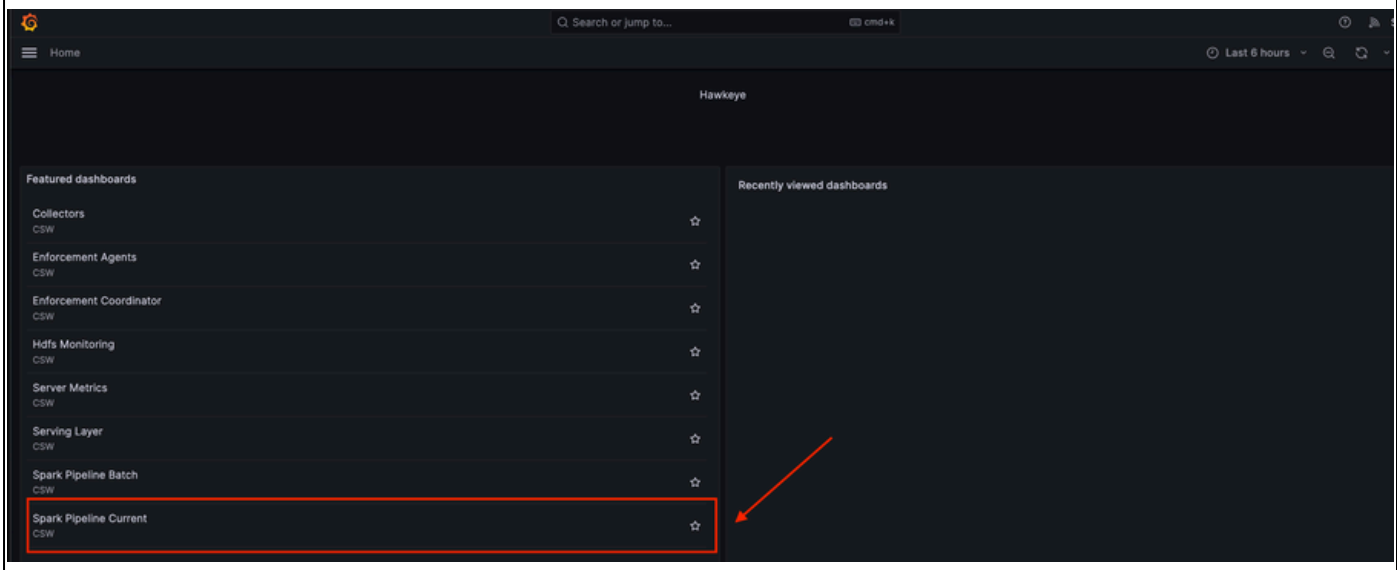


Hawkeye (Graphiques)

Les tableaux de bord Hawkeye offrent une visibilité sur l'intégrité du cluster de charge de travail sécurisé, ainsi que des indicateurs et des informations pour faciliter le dépannage

La page Hawkeye (Graphiques) se trouve dans le volet de navigation de gauche, sous Dépannage > Hawkeye (Graphiques).

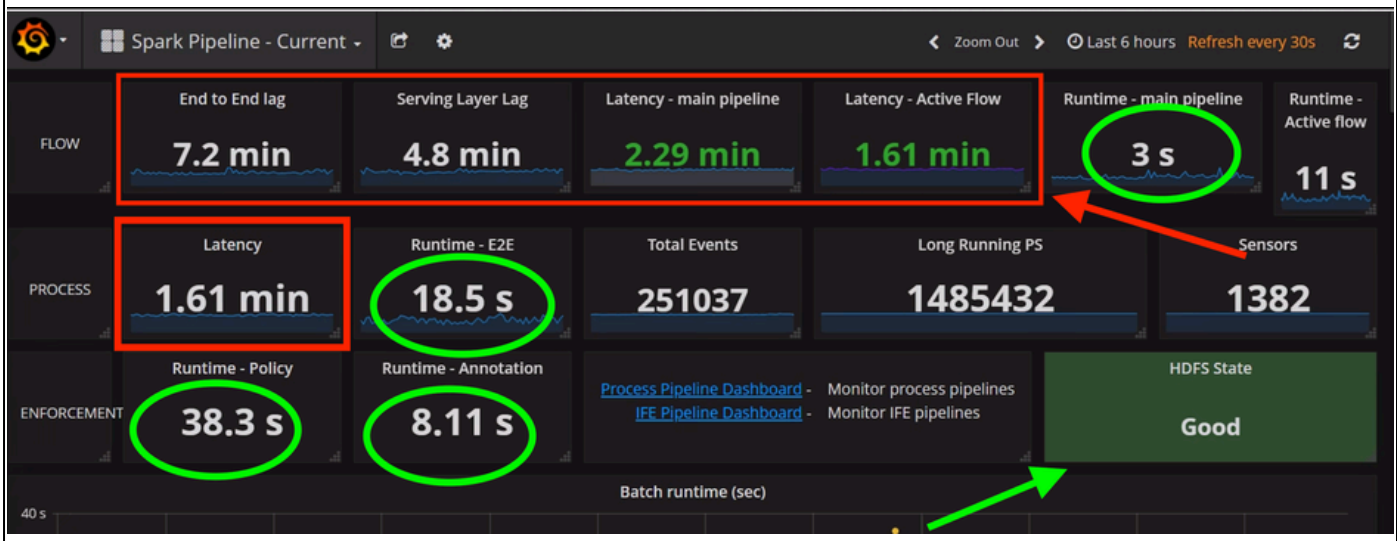
Lorsque vous cliquez sur Hawkeye (Graphiques), un nouvel onglet de navigateur s'ouvre automatiquement et affiche le tableau de bord Hawkeye comme illustré ici.

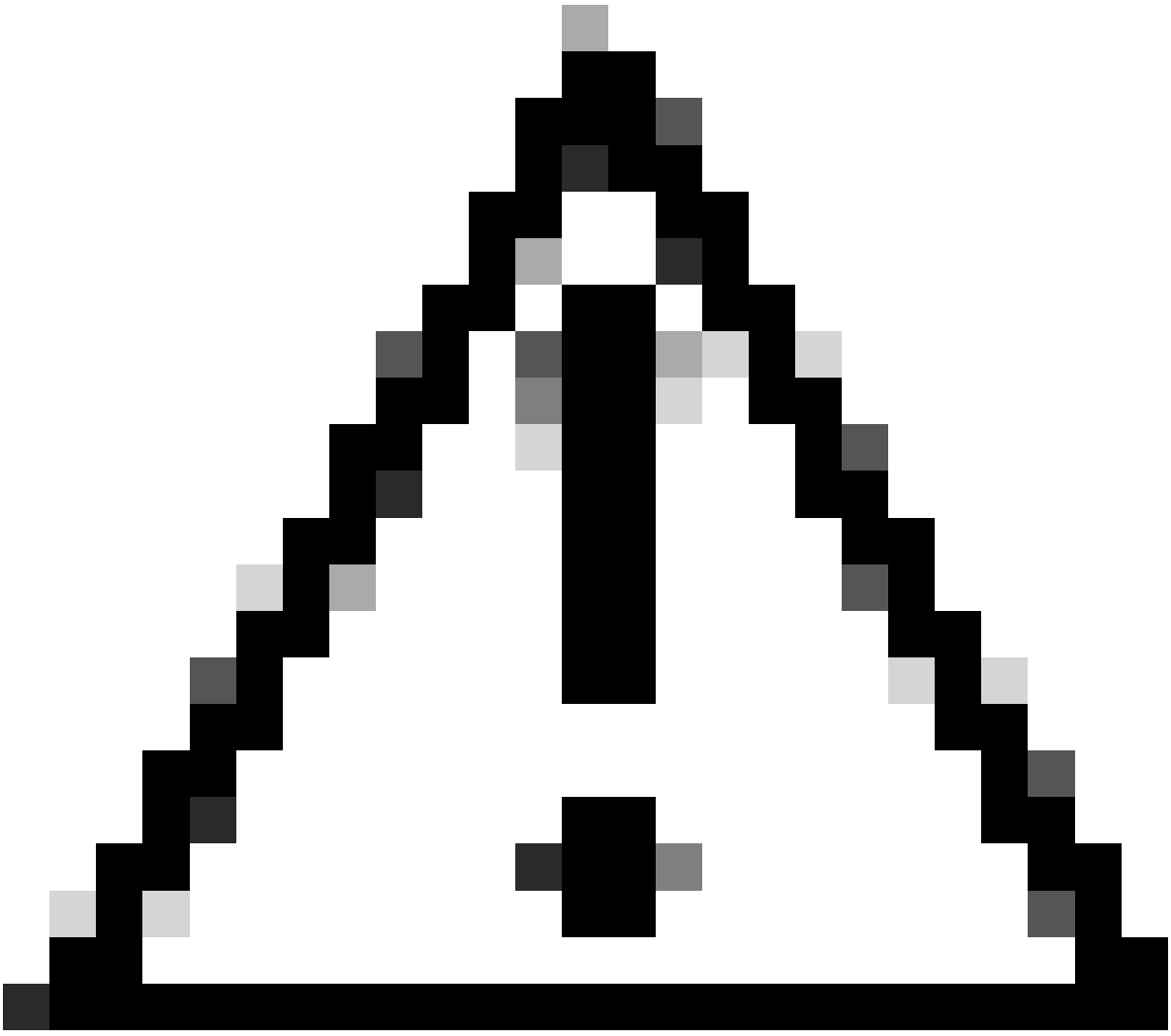


Dans le tableau de bord Hawkeye, cliquez sur l'onglet Spark Pipeline Current pour surveiller l'état du cluster de charge globale sécurisée.

Sur la page Spark Pipeline Current, vérifiez que les valeurs de latence de bout en bout, de latence de couche de desserte, de latence de pipeline principal et de latence de flux active sont toutes inférieures à 10 minutes.

Vérifiez également que les valeurs d'exécution sont inférieures à 1 minute et qu'elles sont présentées en secondes et que l'état HDFS est Bon, comme illustré ci-dessous.





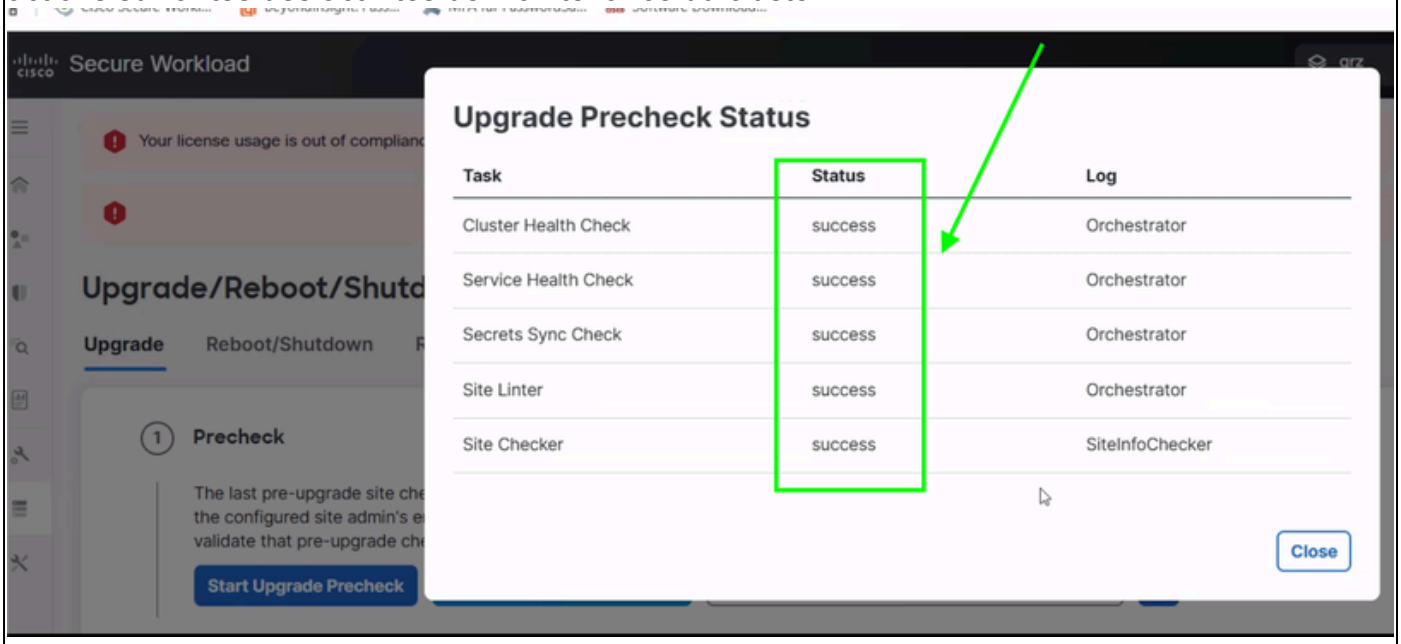
Mise en garde : Si vous observez des valeurs de latence, y compris un décalage de bout en bout ou un décalage de la couche de service, dépassant 6 heures sans montrer de diminution progressive, veuillez contacter le Centre d'assistance technique (TAC).

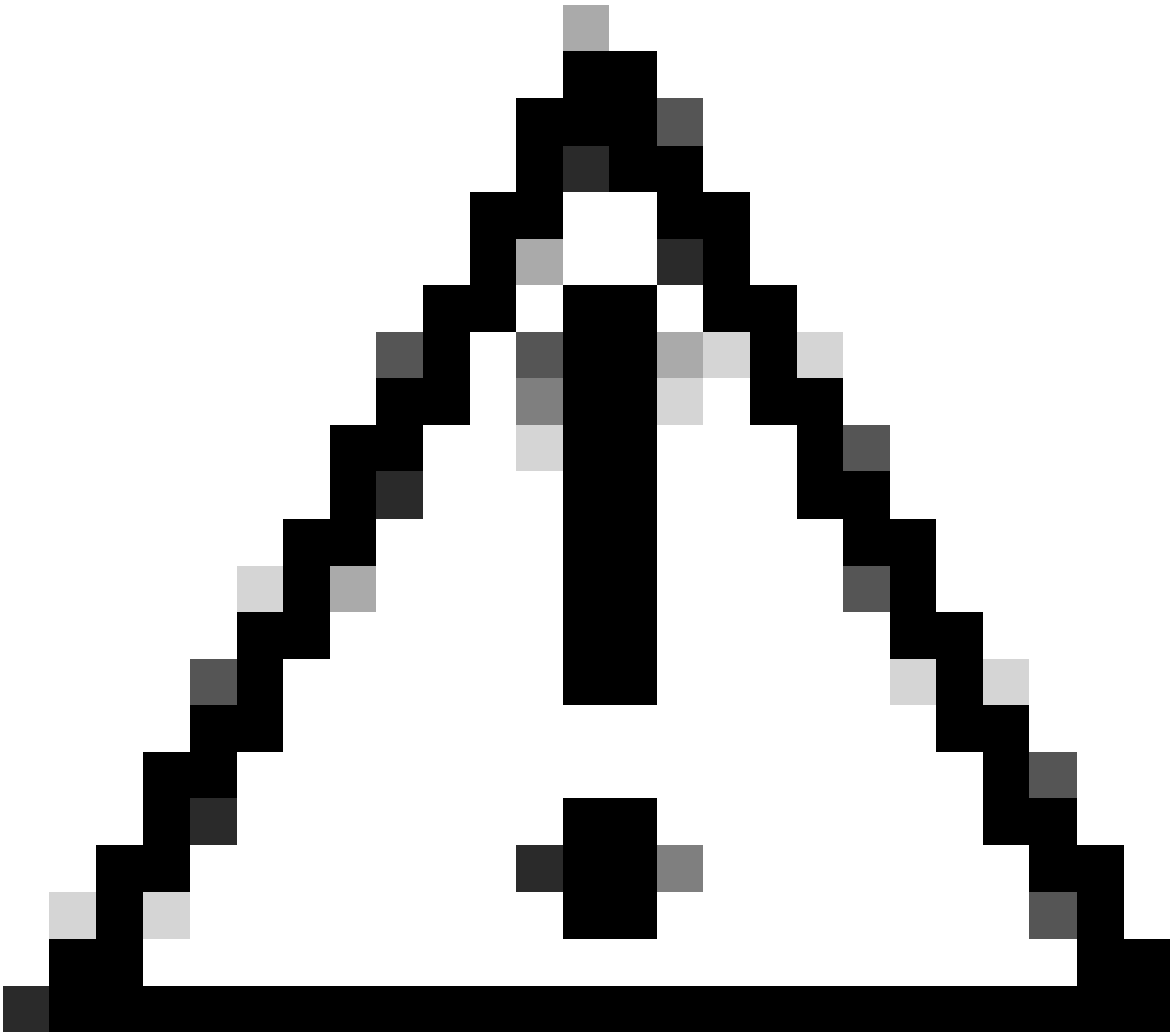
Prévérifications de mise à niveau

Avant et après les tâches de maintenance, utilisez la vérification préalable de la mise à niveau pour exécuter des vérifications de l'intégrité du cluster ; ce processus garantit que les services, les configurations et les composants matériels sont tous en bon état de fonctionnement

1. Accédez à Upgrade Precheck.
   Accédez à l'interface utilisateur TetrationUI et procédez comme suit :
   - Cliquez sur Plate-forme.
   - Sélectionnez Mise à niveau/Redémarrage/Arrêt.
   - Cliquez sur Start Upgrade Precheck.

Patientez quelques minutes pour le résultat des vérifications préalables de la mise à niveau. Si tout fonctionne correctement, comme illustré dans cette image, vous pouvez poursuivre les actions suivantes des activités de maintenance du cluster.





Mise en garde : En cas d'échec de la vérification préalable de la mise à niveau, contactez le centre d'assistance technique (TAC) pour obtenir de l'aide.

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.