Verificar a Integridade de um Cluster de Carga de Trabalho Seguro (Tetration)

Contents

Introdução

Este documento descreve as etapas para verificar a integridade de um cluster de carga de trabalho segura e destaca os principais aspectos a serem revisados durante o processo de verificação de integridade.

Informações de Apoio

O seu principal objetivo é a verificação da saúde; no entanto, se você notar algum problema ou comportamento anormal, será necessário coletar um instantâneo e entrar em contato com a equipe de TAC do Cisco Tetration Solution Support para obter assistência. O cluster de carga de trabalho seguro é composto de centenas de processos distribuídos em várias máquinas virtuais em vários servidores UCS C220.

As duas principais ferramentas para avaliar a integridade do cluster são as páginas Status do cluster e Status do serviço, ambas explicadas neste documento. O uso dessas páginas geralmente é a maneira mais eficaz de confirmar a integridade geral do cluster.

Quando verificar a integridade do cluster

Na maioria das vezes, não é necessário verificar a integridade do cluster. No entanto, há certas situações em que é uma boa ideia:

· Se você observar algo incomum ou inesperado na interface do usuário (IU), com base na sua experiência com o funcionamento normal das coisas. Alguns exemplos comuns são listados na seção Parâmetros de exibição operacional.

· Se você espera ver determinados dados (como dados de fluxo de sensores de software ou

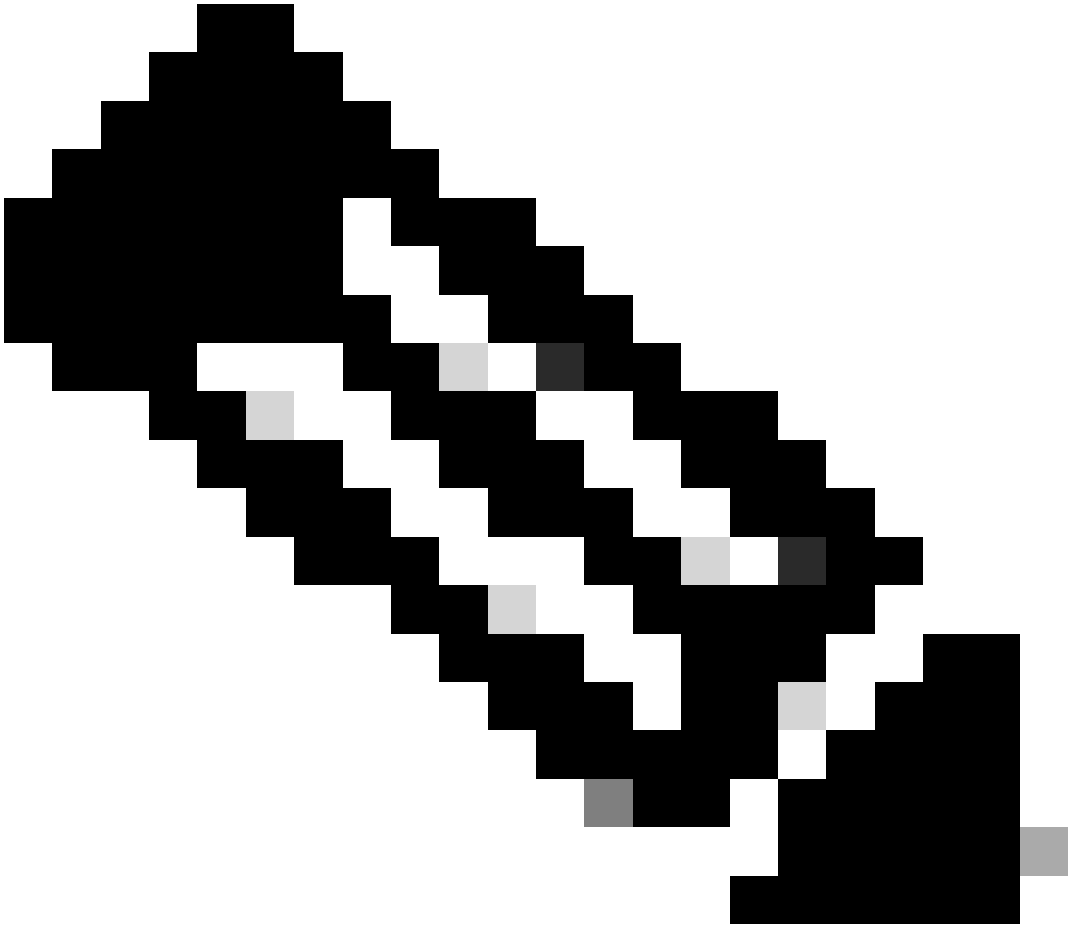
hardware) na interface do usuário, mas eles estão ausentes, mesmo que você tenha selecionado o escopo e o intervalo de tempo corretos.

· Antes e depois de qualquer manutenção programada, atualizações ou grandes alterações no cluster. É uma prática recomendada tirar um instantâneo do estado do cluster antes e depois dessas atividades. Se você precisar entrar em contato com o suporte do TAC, ter esses instantâneos pode ajudar a identificar rapidamente o que mudou.

Opções diferentes Você precisa verificar a integridade do cluster de carga de trabalho segura

Status do cluster

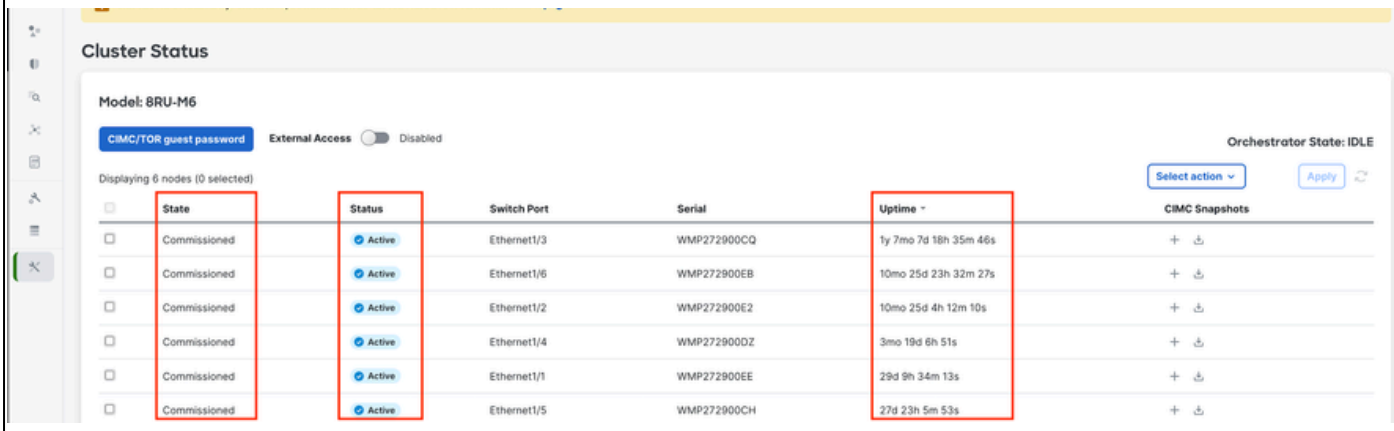
Um cluster de carga de trabalho seguro consiste em 6 servidores (8RU) ou 36 servidores (39RU), dependendo do tipo de cluster. A página Status do Cluster fornece o estado dos servidores, bem como informações do servidor bare-metal.

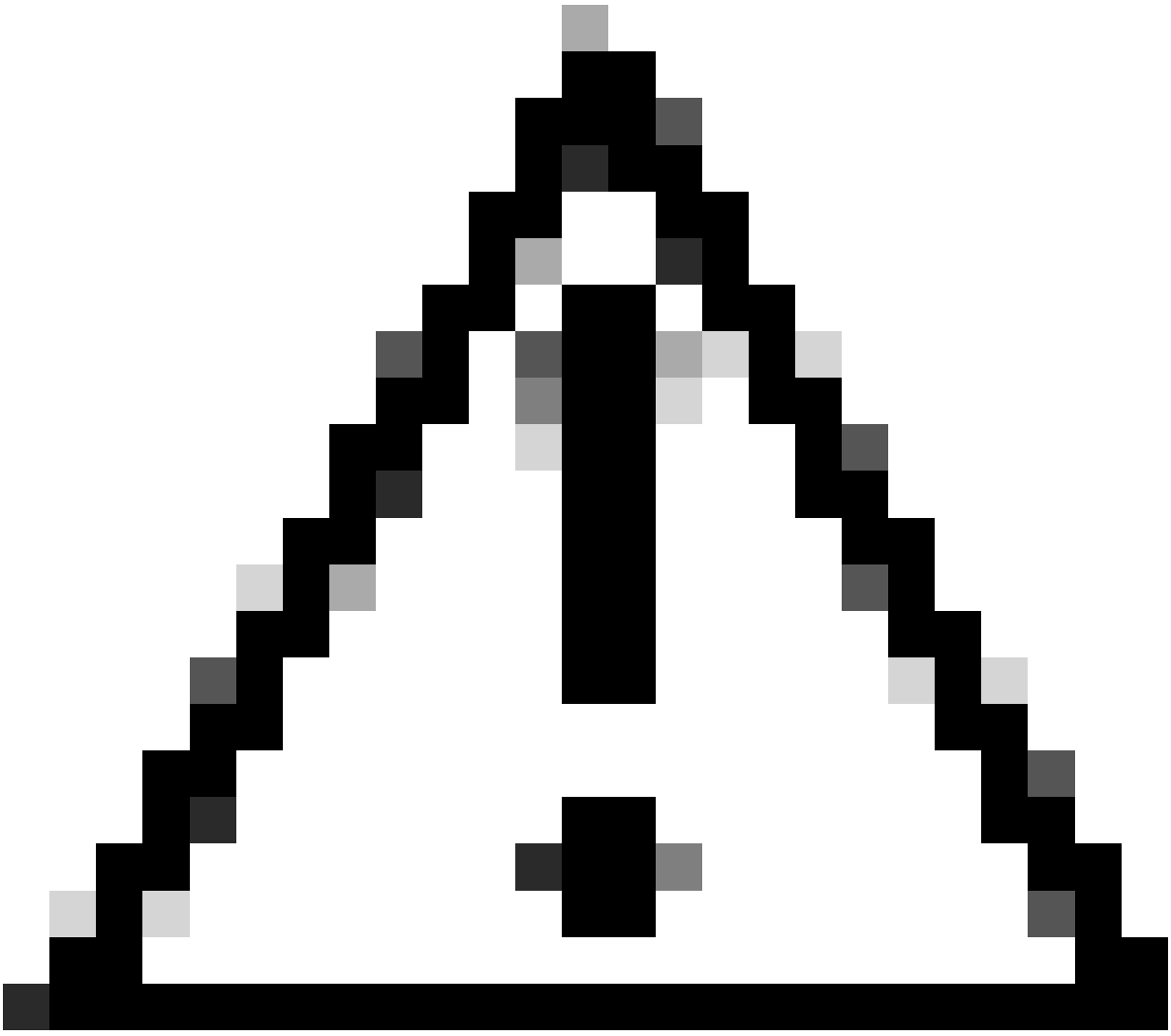


Note: A página Status do cluster pode ser acessada por usuários com as funções Administrador do site ou Suporte ao cliente para clusters físicos. Ambas as funções podem exibir e executar ações na página Status do Cluster.

No painel de navegação, escolha Solução de problemas > Status do cluster.

O status do cluster mostra o status de todos os servidores no rack Cisco Secure Workload. Um servidor em funcionamento pode exibir um Estado de Comissionado e um Status de Ativo, como mostrado aqui.





Caution: Se você observar qualquer nó marcado como inativo na página de status do cluster, gere um instantâneo do CIMC e gere um caso de TAC, incluindo o instantâneo.

Se o status for exibido como Inativo, isso geralmente significa que o servidor está desligado ou pode estar inativo devido a um problema de hardware, cabo ou conectividade.

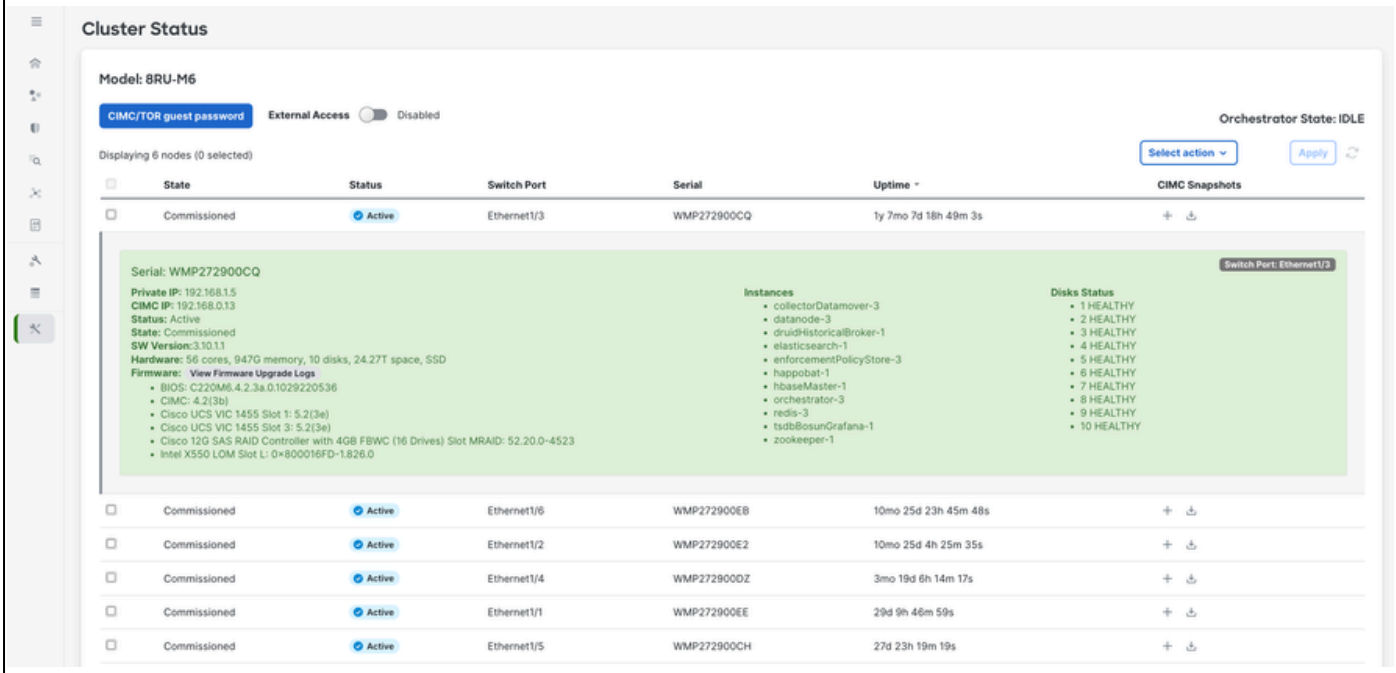
Ao clicar em um servidor na lista, você verá mais detalhes, como

· As máquinas virtuais (instâncias) em execução nesse servidor físico

· O endereço IP privado do servidor dentro do cluster

· O endereço IP do CIMC (gerenciamento)

· As versões atuais de firmware para o BIOS, CIMC, placa VIC, placa LOM e controlador RAID

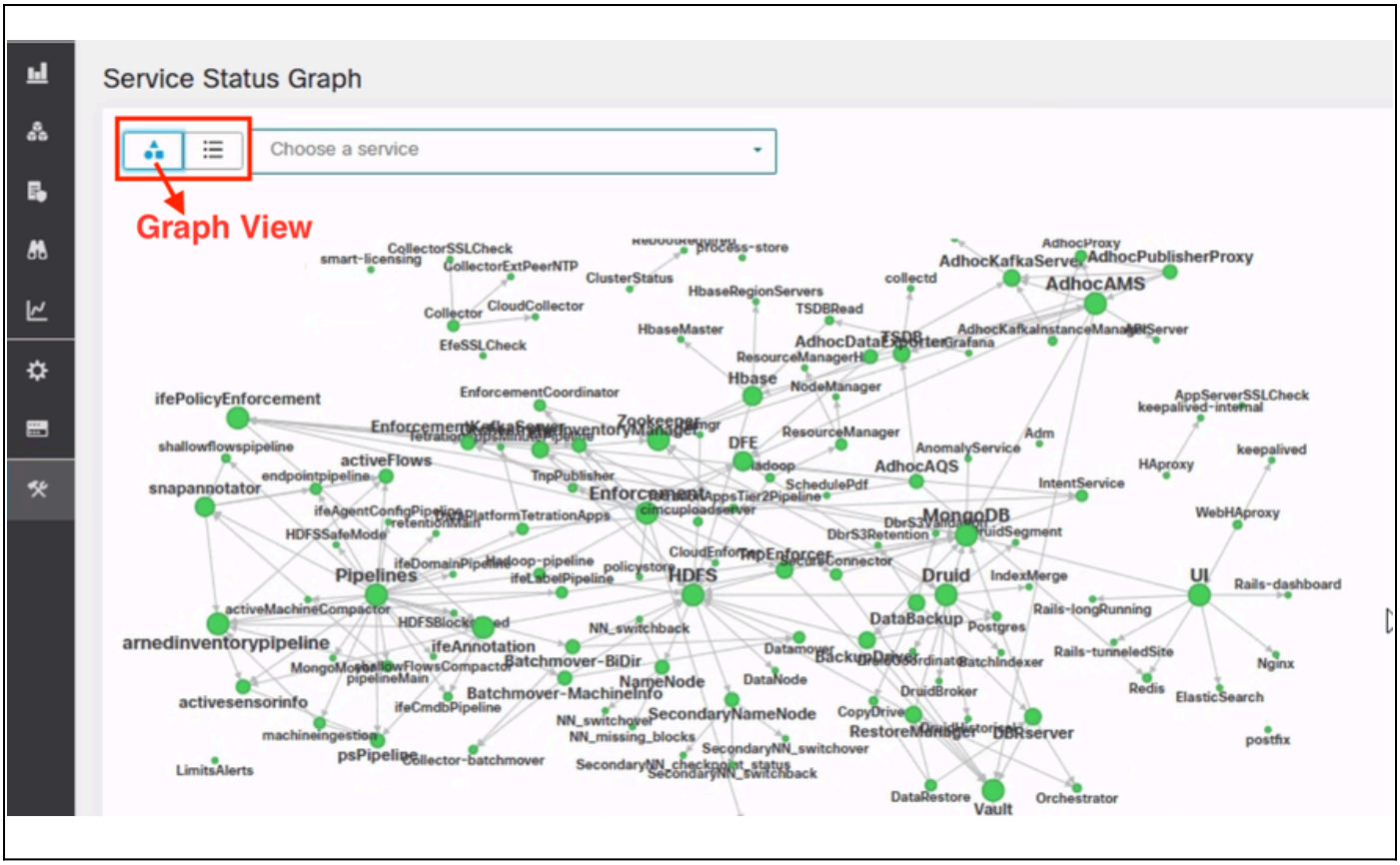


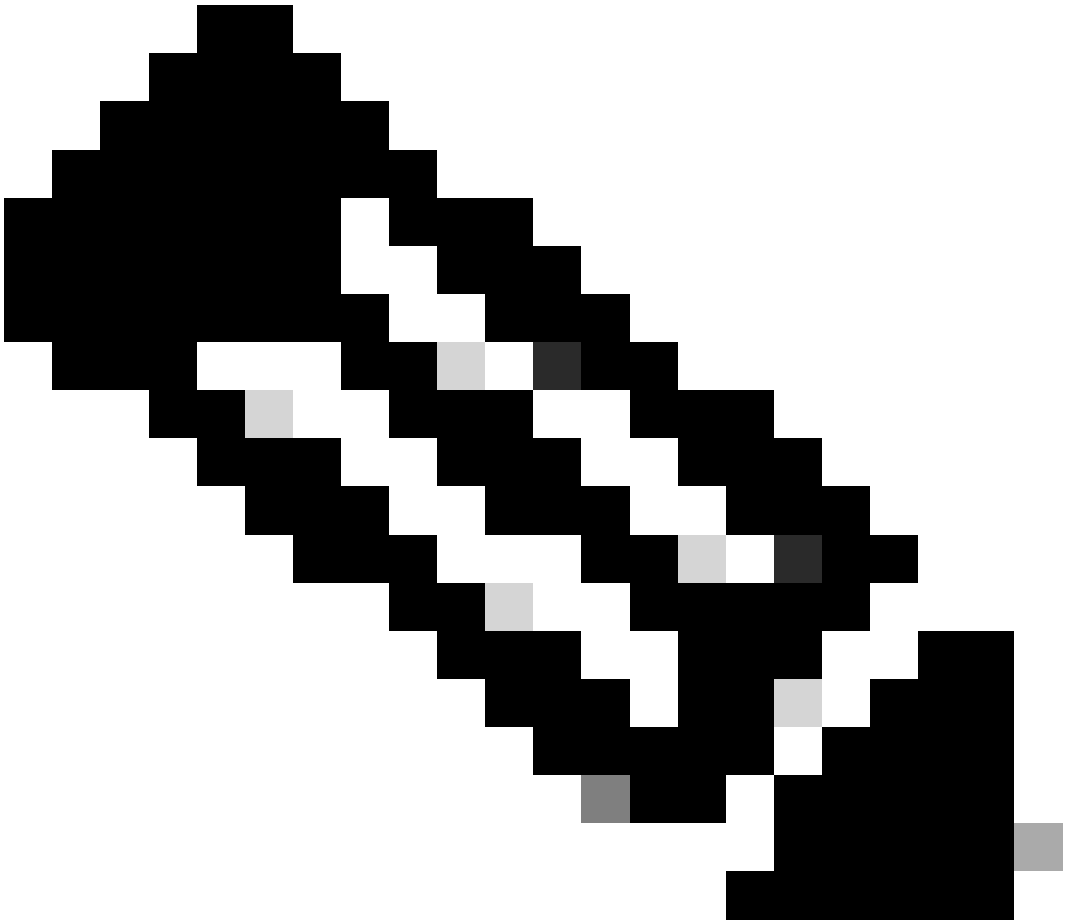
Status do serviço

A página Status do serviço está localizada no painel de navegação esquerdo em Solução de problemas > Status do serviço.

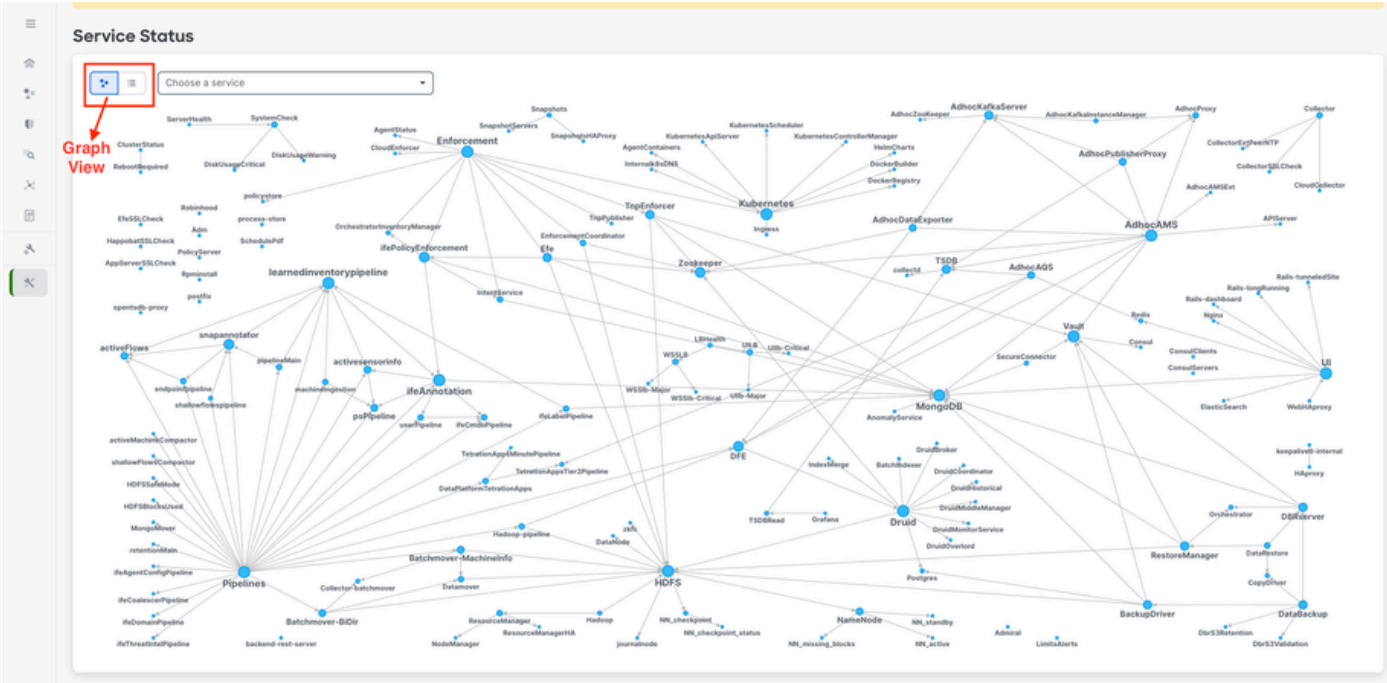
A página Status do Serviço exibe a integridade de todos os serviços usados no cluster de carga de trabalho do CiscoSecure junto com suas dependências.

A exibição de gráfico mostra a integridade do serviço, cada nó no gráfico mostra a integridade do serviço e uma borda representa a dependência de outros serviços. Serviços não íntegros são marcados em vermelho quando o serviço não está disponível e em laranja quando o serviço está degradado, mas disponível. Uma cor verde ou azul celeste indica que o serviço está íntegro. Para obter mais informações de depuração sobre esses nós, use a exibição de árvore que tem o botão Expandir Tudo para mostrar todos os nós filho na árvore de dependência. Inativo, indica que o serviço não está funcionando, e Não íntegro, indica que o serviço não está totalmente funcional.


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

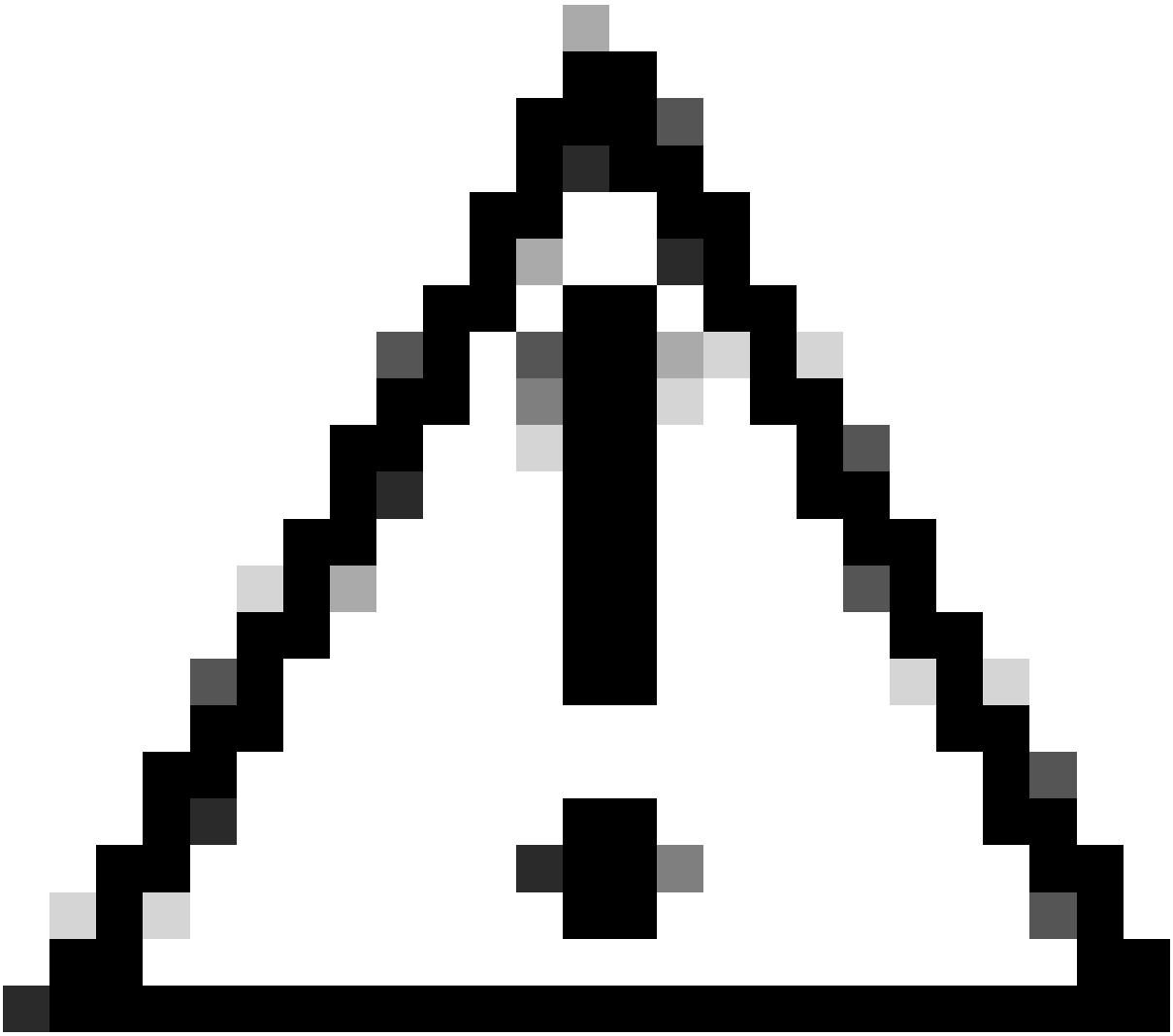


Note: Começando com a versão do patch 3.10.2.11, a página de status do serviço aparece em azul-celeste. Uma cor verde ou azul celeste indica que o serviço está íntegro.

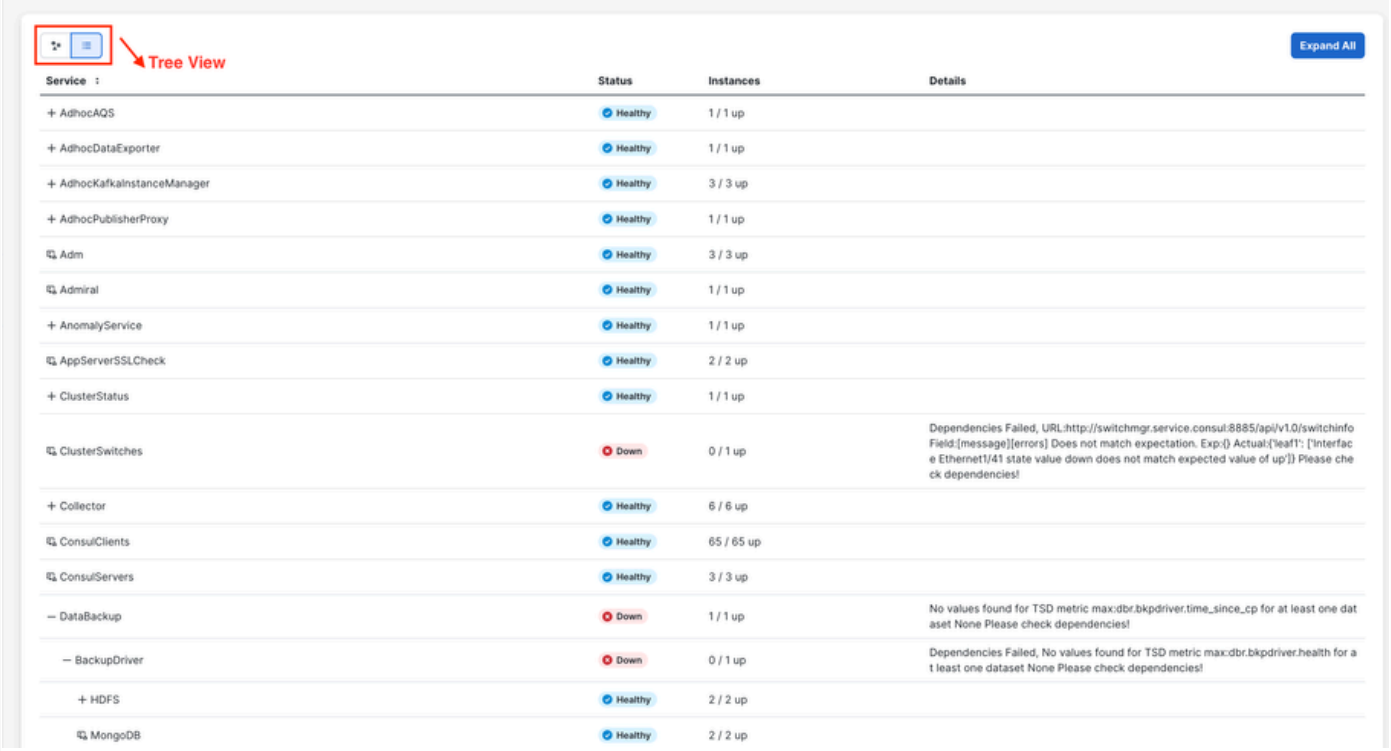


Por padrão, a página Status do serviço mostra as funções e dependências do cluster em uma exibição gráfica. Se os ícones estiverem todos verdes ou azuis, nenhum erro será detectado.

Se houver um serviço exibido em vermelho ou laranja, a exibição em árvore mostrará a lista de serviços e permitirá que você se aprofunde nas dependências do serviço, bem como em outros detalhes detectados pela função Status do serviço. Essas informações de erro de dependência são particularmente importantes para observar e capturar ao abrir um caso no TAC.



Caution: Se você perceber que algum dos serviços não está íntegro e está vermelho, entre em contato com o Centro de Assistência Técnica (TAC) para obter suporte para resolver esses problemas. O rápido envolvimento com o TAC pode ajudar a restaurar a funcionalidade completa.

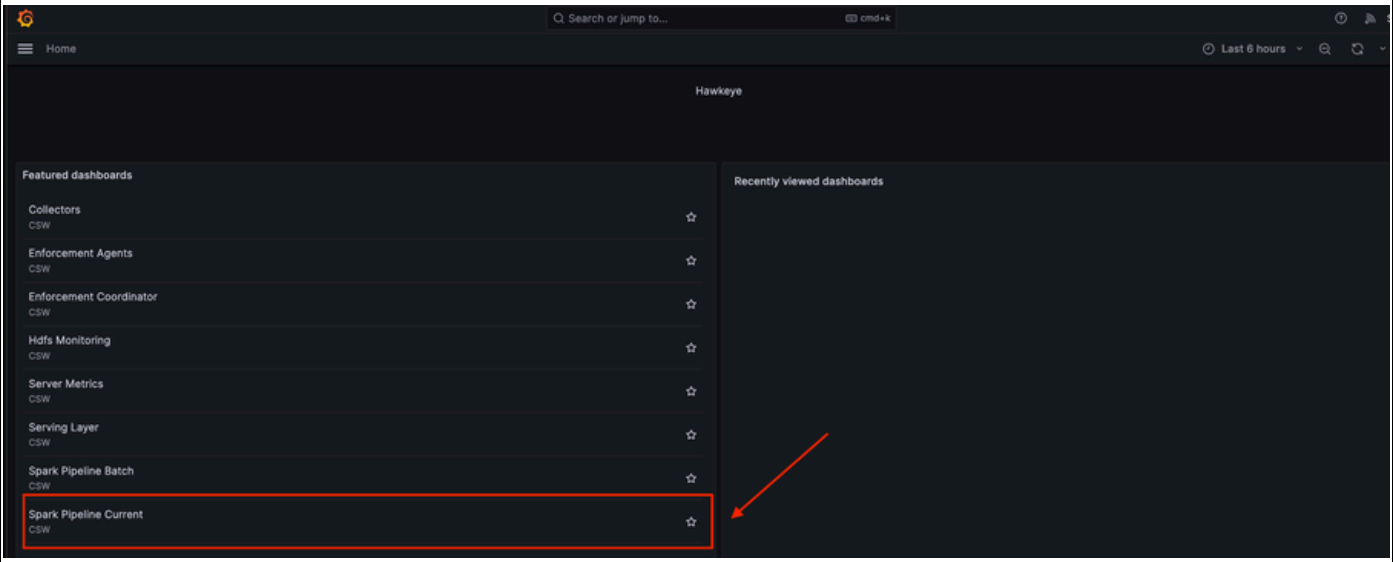


Gavião Arqueiro (Gráficos)

Os painéis Hawkeye oferecem visibilidade sobre a integridade do cluster de carga de trabalho segura, bem como métricas e percepções para ajudar na solução de problemas

A página Hawkeye (Charts) está localizada no painel de navegação à esquerda em Troubleshoot > Hawkeye (Charts).

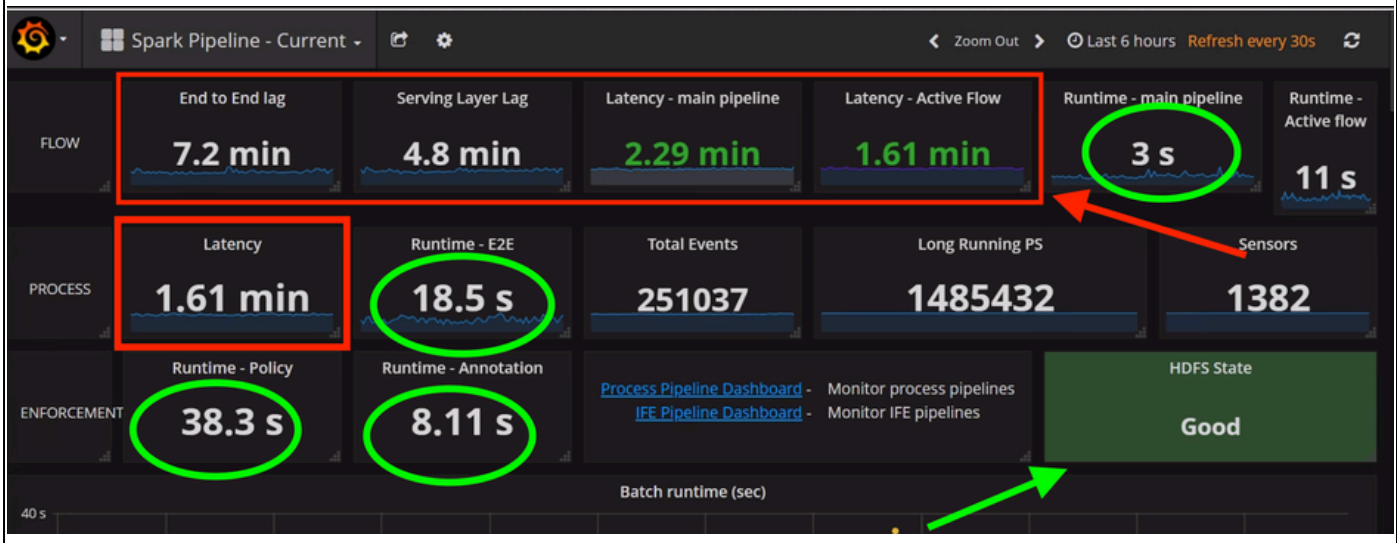
Quando você clica em Hawkeye (Gráficos), uma nova guia do navegador é aberta automaticamente, exibindo o painel Hawkeye, como mostrado aqui.

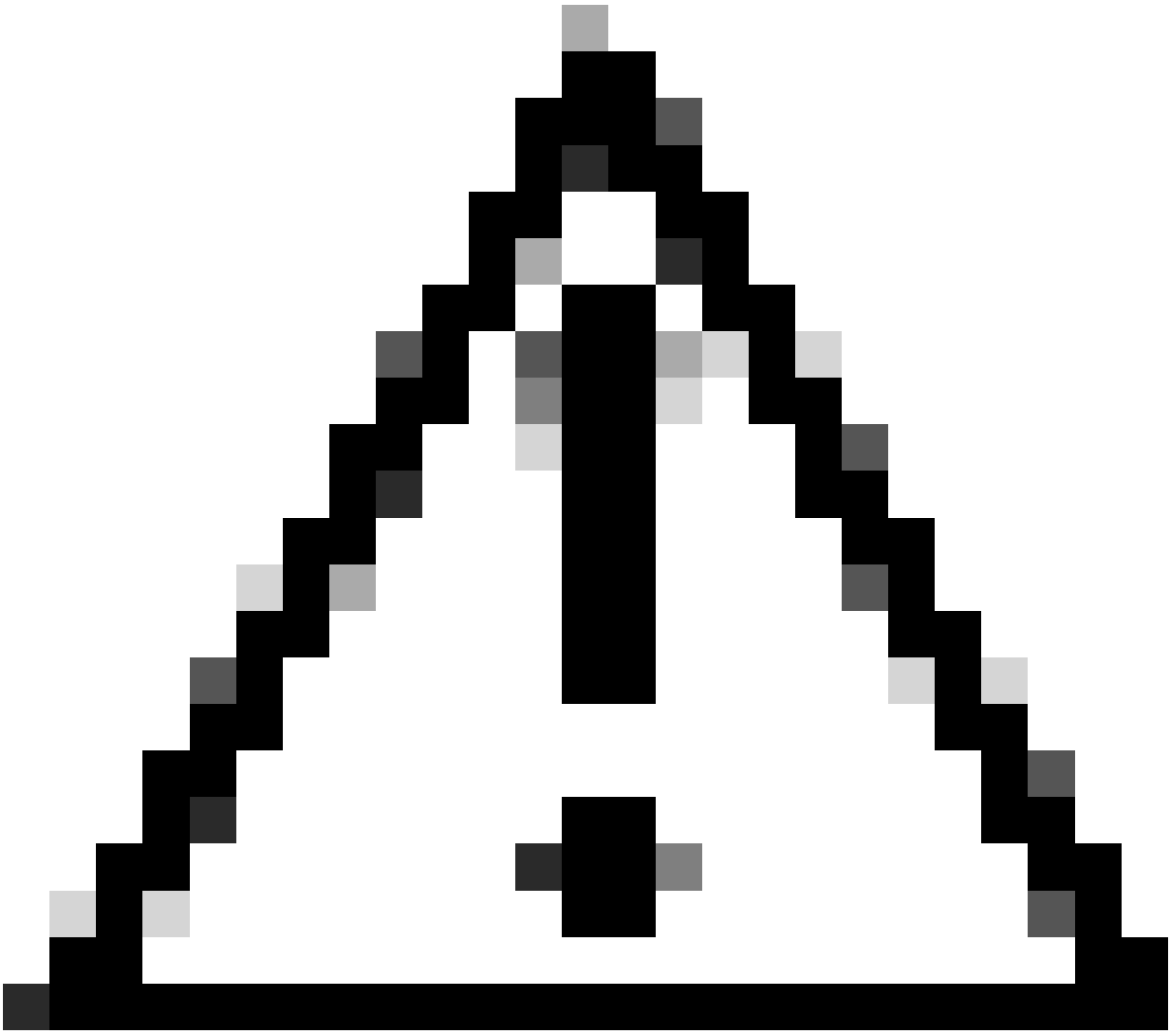


No painel Hawkeye, clique na guia Atual do Pipeline Spark para monitorar a integridade do cluster de carga de trabalho seguro.

Na página Atual do Pipeline Spark, verifique se os valores de Lag Fim-a-Fim, Lag da Camada de Serviço, Latência do Pipeline Principal e Latência do Fluxo Ativo estão abaixo de 10 minutos.

Além disso, confirme se os valores de tempo de execução são inferiores a 1 minuto e são apresentados em segundos e se o estado do HDFS é Bom, como ilustrado a seguir.





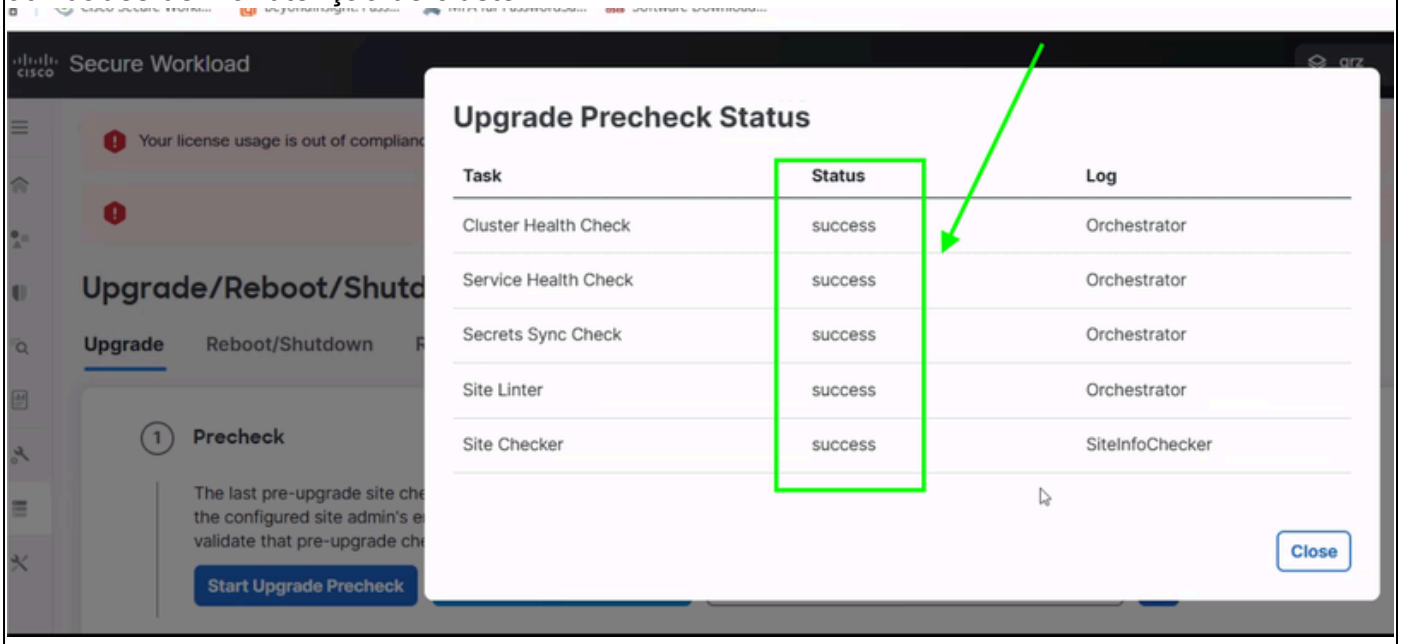
Caution: Se você observar valores de latência, incluindo atraso de ponta a ponta ou atraso da camada de serviço, que excedam 6 horas sem mostrar uma redução gradual, entre em contato com o Centro de Assistência Técnica (TAC).

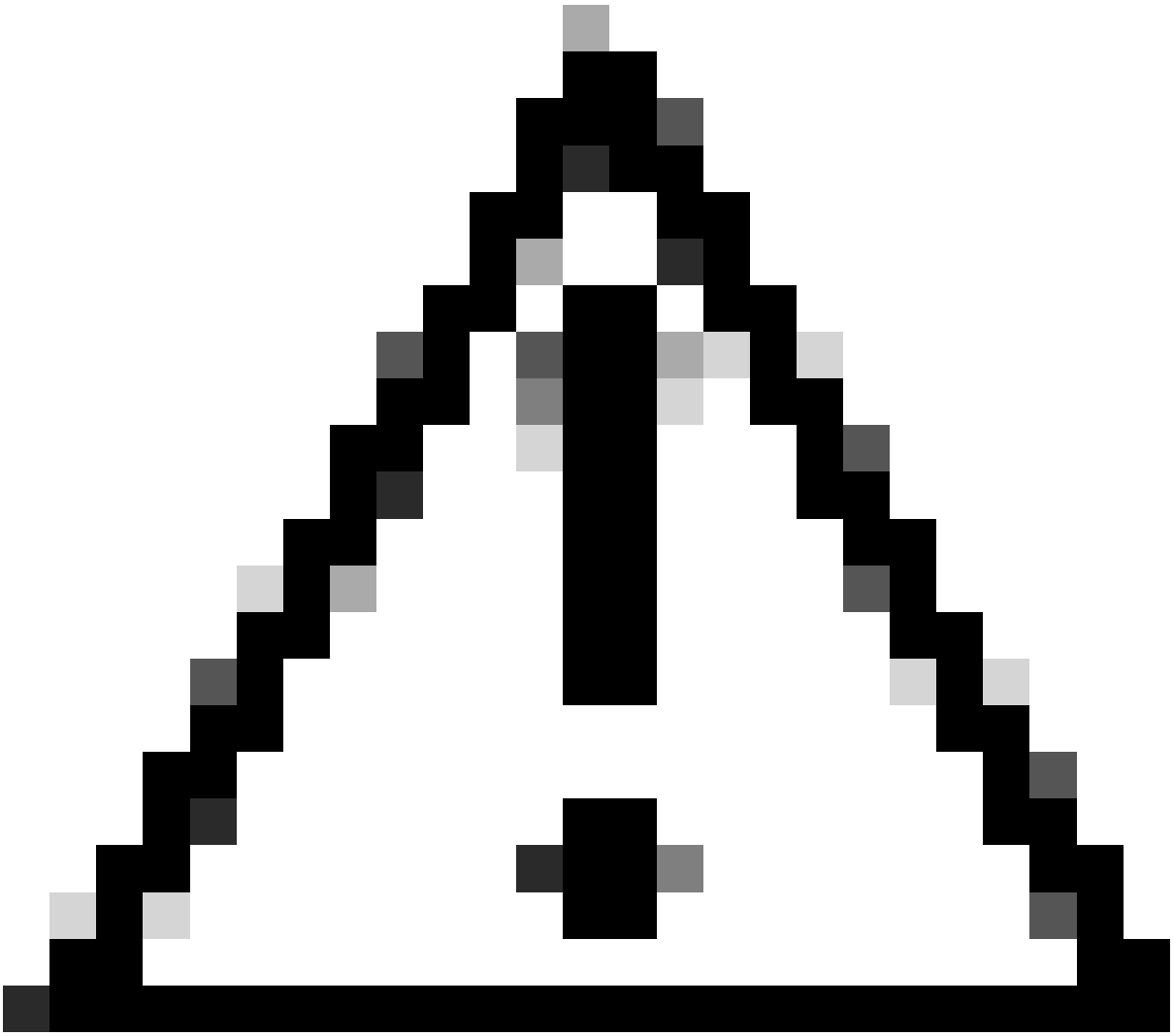
Pré-verificações de Atualização

Antes e depois das tarefas de manutenção, use a pré-verificação de atualização para executar verificações de integridade do cluster; esse processo garante que os serviços, as configurações e os componentes de hardware estejam todos em ordem de funcionamento adequada

1. Navegue paraVerificação prévia de atualização.
   Navegue até aIUtetraçãoE siga estas etapas:
   - Clique em Platform.
   - Selecione Upgrade/Reboot/Shutdown.
   - Clique em Start Upgrade Precheck.

Aguarde alguns minutos pela saída das pré-verificações de atualização. Se tudo for bem-sucedido como mostrado nesta imagem, você poderá prosseguir com as próximas ações das atividades de manutenção de cluster.





Caution: Se alguma pré-verificação de atualização não for bem-sucedida, entre em contato com o Centro de Assistência Técnica (TAC) para obter assistência.

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.