Verifica dello stato di un cluster con carico di lavoro protetto (Tetration)

Sommario

Introduzione

In questo documento vengono descritti i passaggi per verificare lo stato di un cluster con carico di lavoro protetto e vengono evidenziati gli aspetti chiave da esaminare durante il processo di verifica dello stato.

Premesse

Il suo obiettivo principale è la verifica della salute; tuttavia, in caso di problemi o comportamenti anomali, è necessario raccogliere un'istantanea e contattare il team TAC di supporto della soluzione Cisco Tetration per assistenza. Il cluster con carico di lavoro sicuro è costituito da centinaia di processi distribuiti su più macchine virtuali su diversi server UCS C220.

I due strumenti principali per la valutazione dello stato di integrità del cluster sono le pagine Stato cluster e Stato servizio, illustrate in questo documento. L'utilizzo di queste pagine rappresenta in genere il modo più efficace per verificare lo stato complessivo del cluster.

Quando verificare lo stato del cluster

Nella maggior parte dei casi non è necessario verificare l'integrità del cluster. Tuttavia, ci sono alcune situazioni in cui è una buona idea:

· Se nell'interfaccia utente (UI) si nota qualcosa di insolito o imprevisto, in base all'esperienza acquisita con il funzionamento normale. Alcuni esempi comuni sono elencati nella sezione Parametri di visualizzazione operativi.

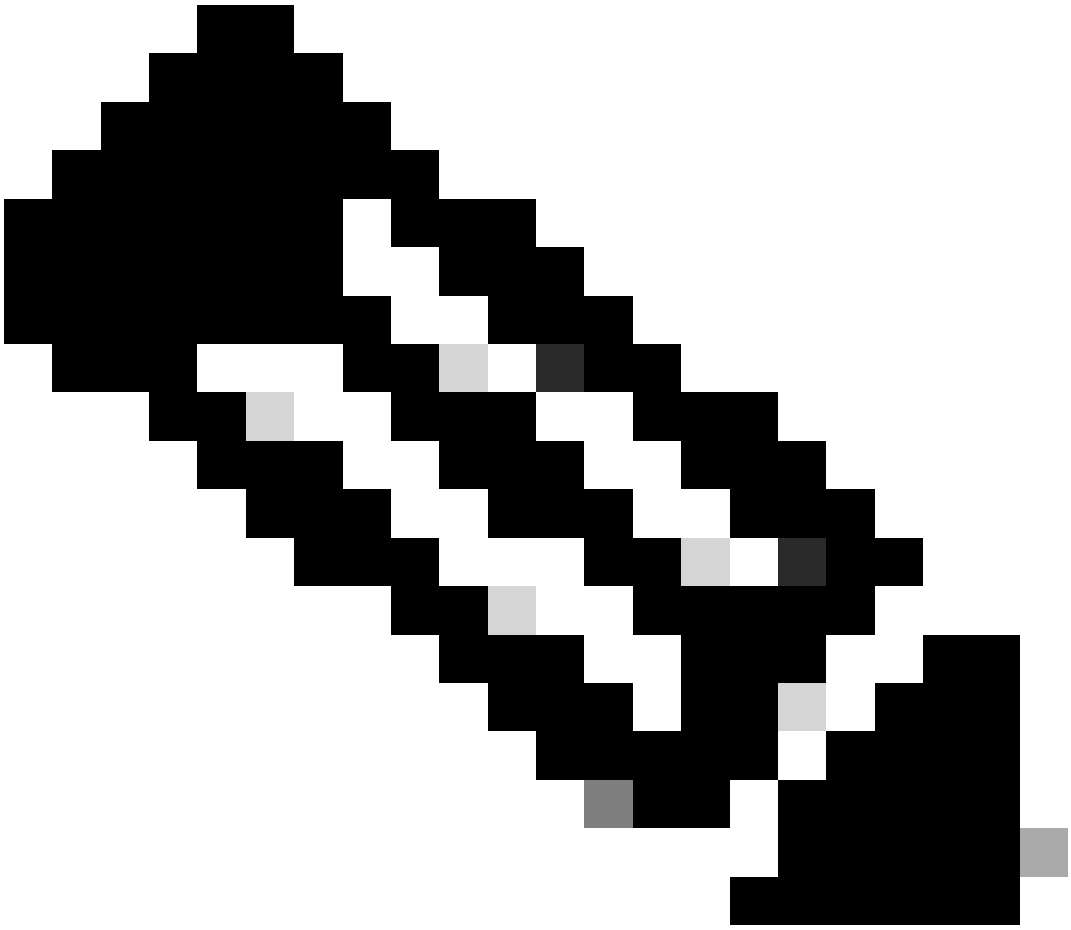
· Se si prevede di visualizzare determinati dati (come i dati di flusso provenienti da sensori software o hardware) nell'interfaccia utente, ma questi mancano anche se è stato selezionato l'ambito e l'intervallo di tempo corretti.

· Prima e dopo qualsiasi manutenzione pianificata, upgrade o modifiche importanti al cluster. È consigliabile eseguire un'istantanea dello stato del cluster prima e dopo queste attività. Se avete bisogno di contattare il supporto TAC, la disponibilità di queste istantanee può aiutare a individuare rapidamente ciò che è cambiato.

Opzioni diverse per verificare lo stato del cluster del carico di lavoro protetto

Stato cluster

Un cluster con carico di lavoro sicuro è costituito da 6 server (8RU) o da 36 server (39RU), a seconda del tipo di cluster. La pagina Stato cluster fornisce lo stato dei server e le informazioni sul server bare metal.

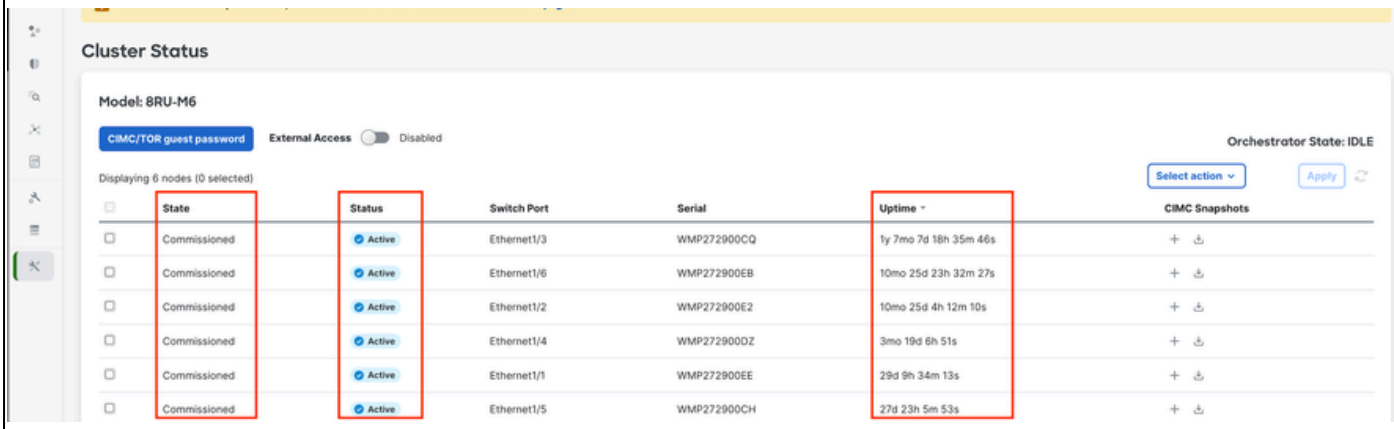


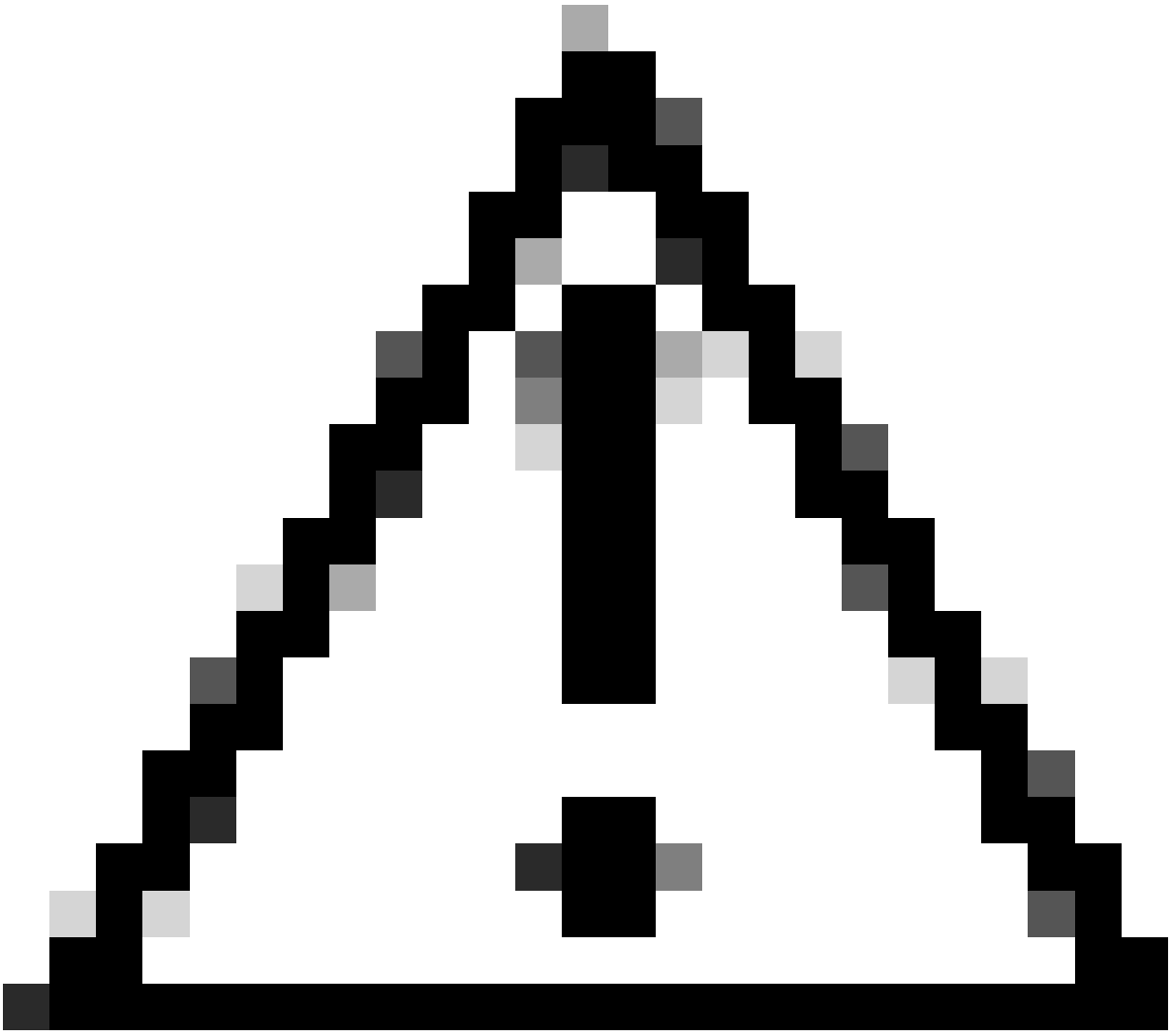
Nota: La pagina Stato cluster è accessibile agli utenti con ruoli di amministratore del sito o di supporto tecnico per i cluster fisici. Entrambi i ruoli sono in grado di visualizzare ed

eseguire azioni nella pagina Stato cluster.

Nel riquadro di navigazione, scegliere Risoluzione dei problemi > Stato cluster.

Lo stato del cluster mostra lo stato di tutti i server nel rack Cisco Secure Workload. Un server funzionante può visualizzare lo stato Commissionato e lo stato Attivo, come mostrato di seguito.





Attenzione: Se si nota un nodo contrassegnato come inattivo nella pagina dello stato del cluster, generare uno snapshot CIMC e sollevare una richiesta TAC, inclusa la snapshot.

Se lo stato è Inattivo, significa in genere che il server è spento o può essere inattivo a causa di un problema di hardware, cavo o connettività.

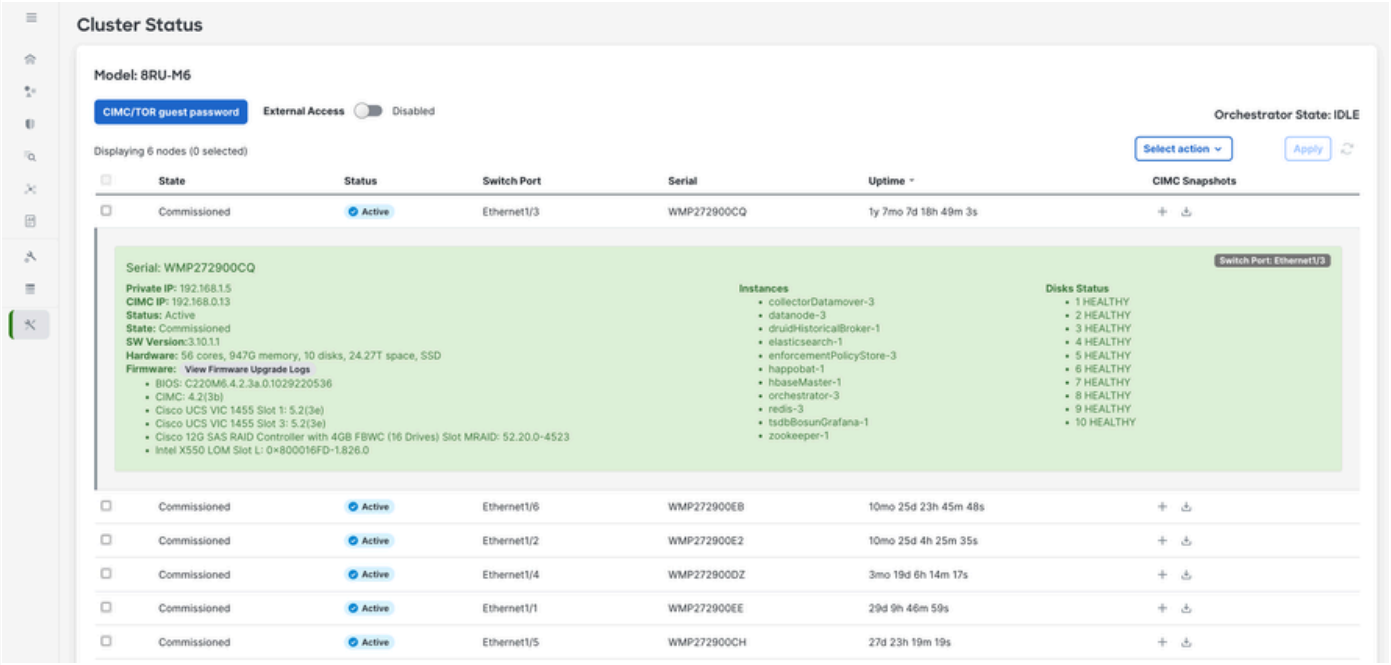
Quando si fa clic su un server nell'elenco, vengono visualizzati ulteriori dettagli, ad esempio

· Le macchine virtuali (istanze) in esecuzione sul server fisico

· Indirizzo IP privato del server nel cluster

· Indirizzo IP CIMC (gestione)

· Versioni correnti del firmware per BIOS, CIMC, scheda VIC, scheda LOM e controller RAID

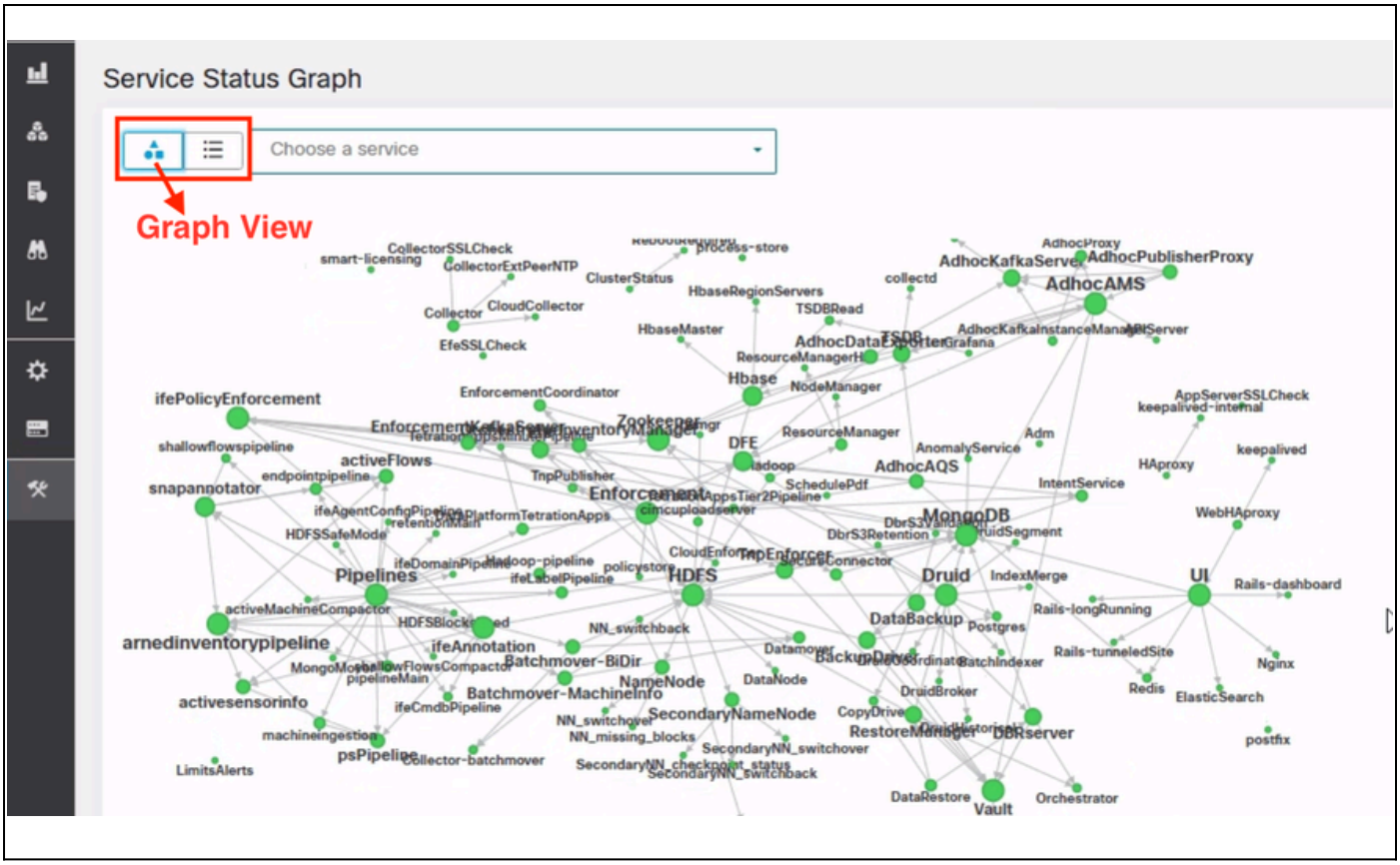


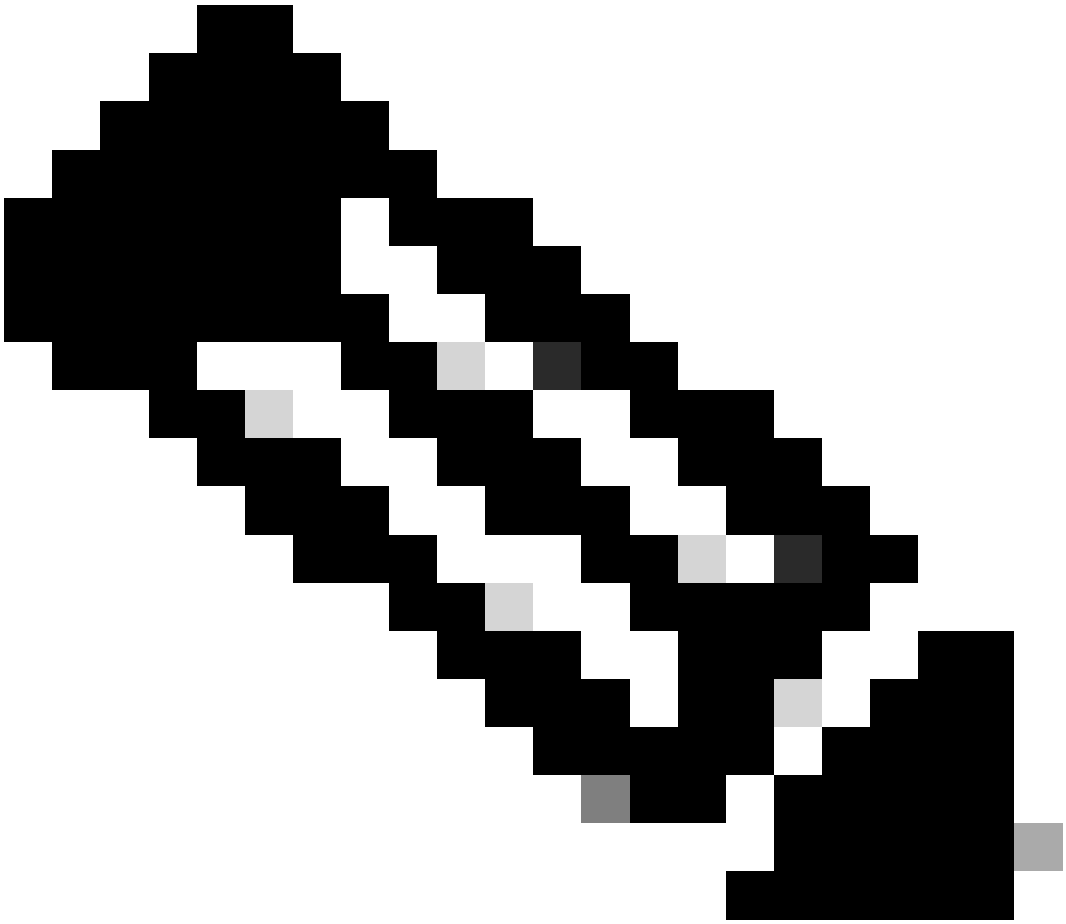
Stato del servizio

La pagina Stato del servizio si trova nel pannello di navigazione a sinistra in Risoluzione dei problemi > Stato del servizio.

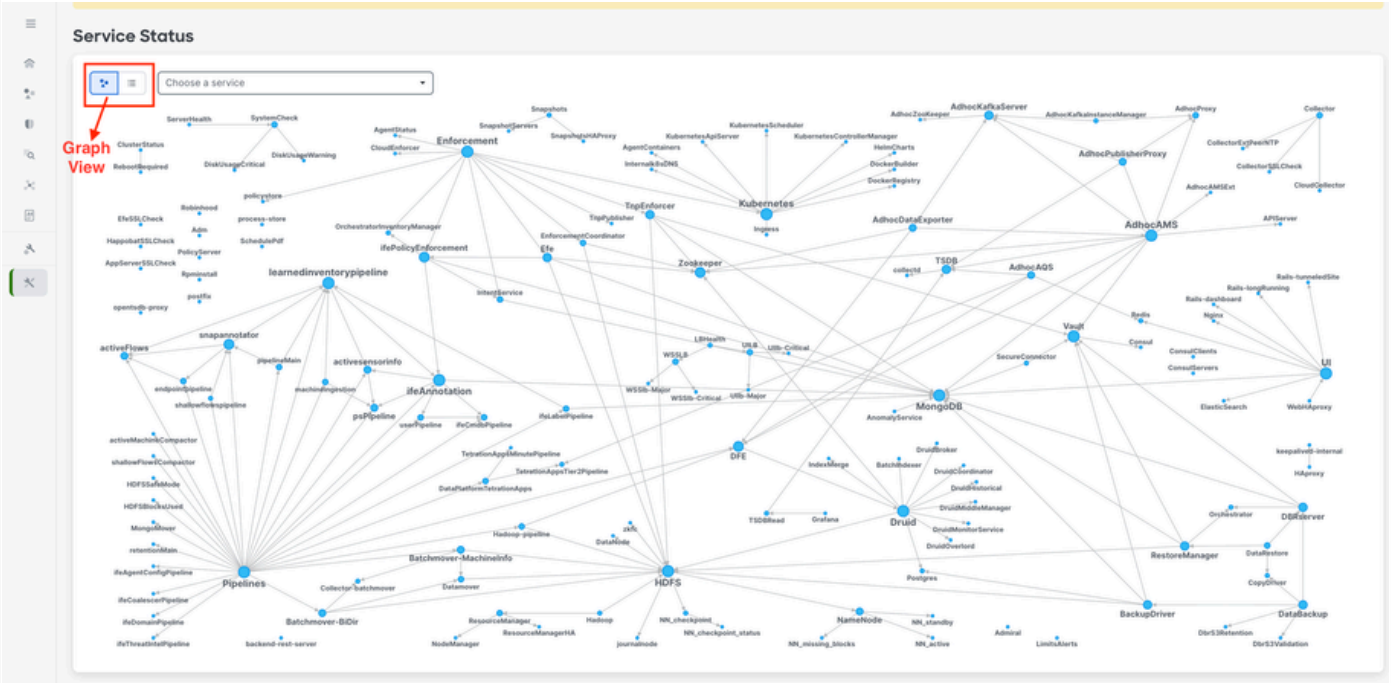
La pagina Stato del servizio visualizza lo stato di tutti i servizi utilizzati nel cluster di carico di lavoro CiscoSecure con le relative dipendenze.

La vista del grafico mostra lo stato del servizio, ogni nodo del grafico mostra lo stato del servizio e un bordo rappresenta la dipendenza da altri servizi. I servizi non integri vengono contrassegnati in rosso quando il servizio non è disponibile e in arancione quando il servizio è danneggiato ma disponibile. Il colore verde o il colore blu cielo indicano che il servizio è integro. Per ulteriori informazioni di debug su questi nodi, utilizzare la visualizzazione struttura con il pulsante Espandi tutto per visualizzare tutti i nodi figlio nella struttura delle dipendenze. Inattivo indica che il servizio non è funzionante e Non integro indica che il servizio non è completamente funzionante.


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

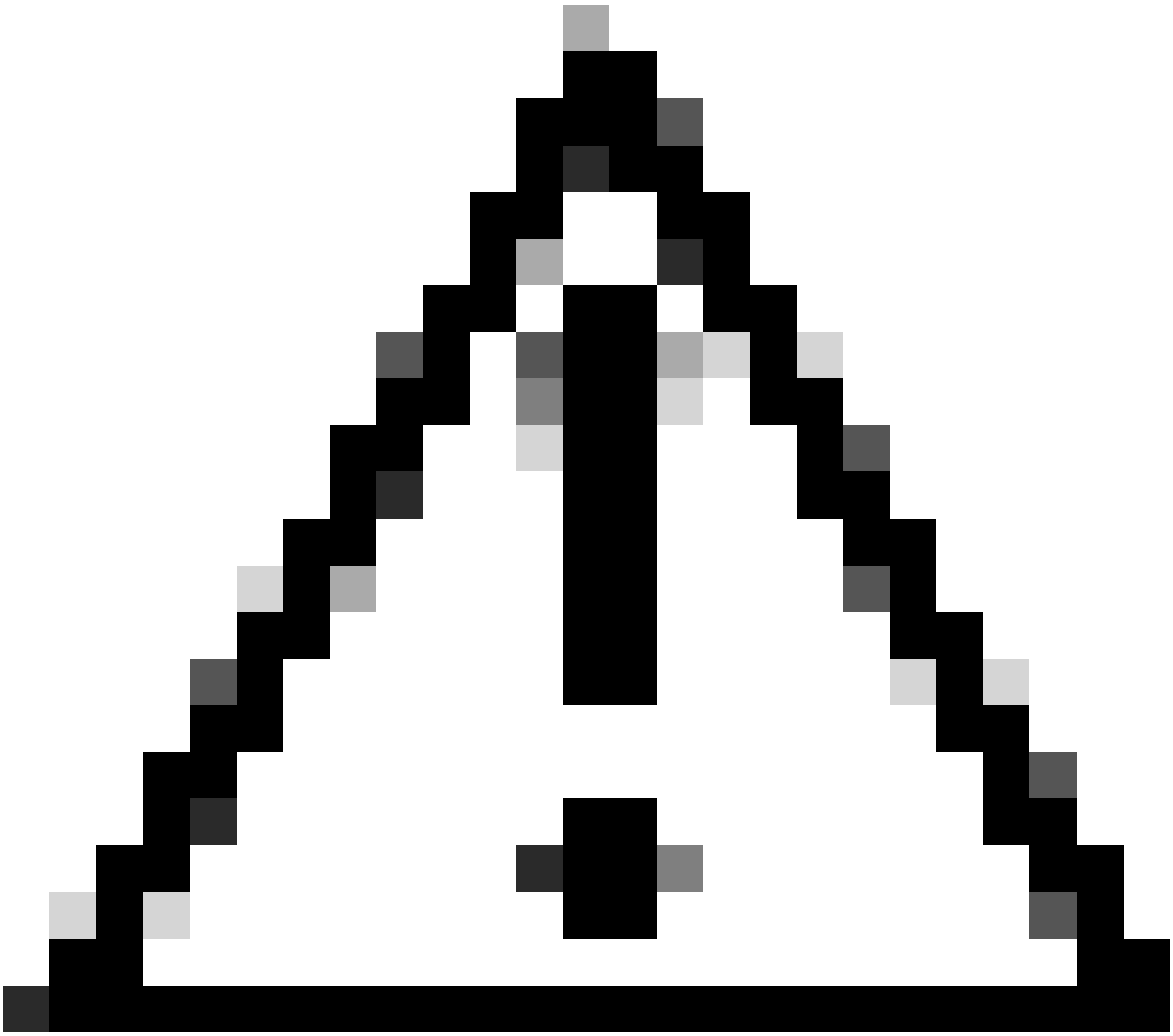


Nota: A partire dalla versione 3.10.2.11 della patch, la pagina relativa allo stato del servizio viene visualizzata in blu cielo. Il colore verde o il colore blu cielo indicano che il servizio è integro.

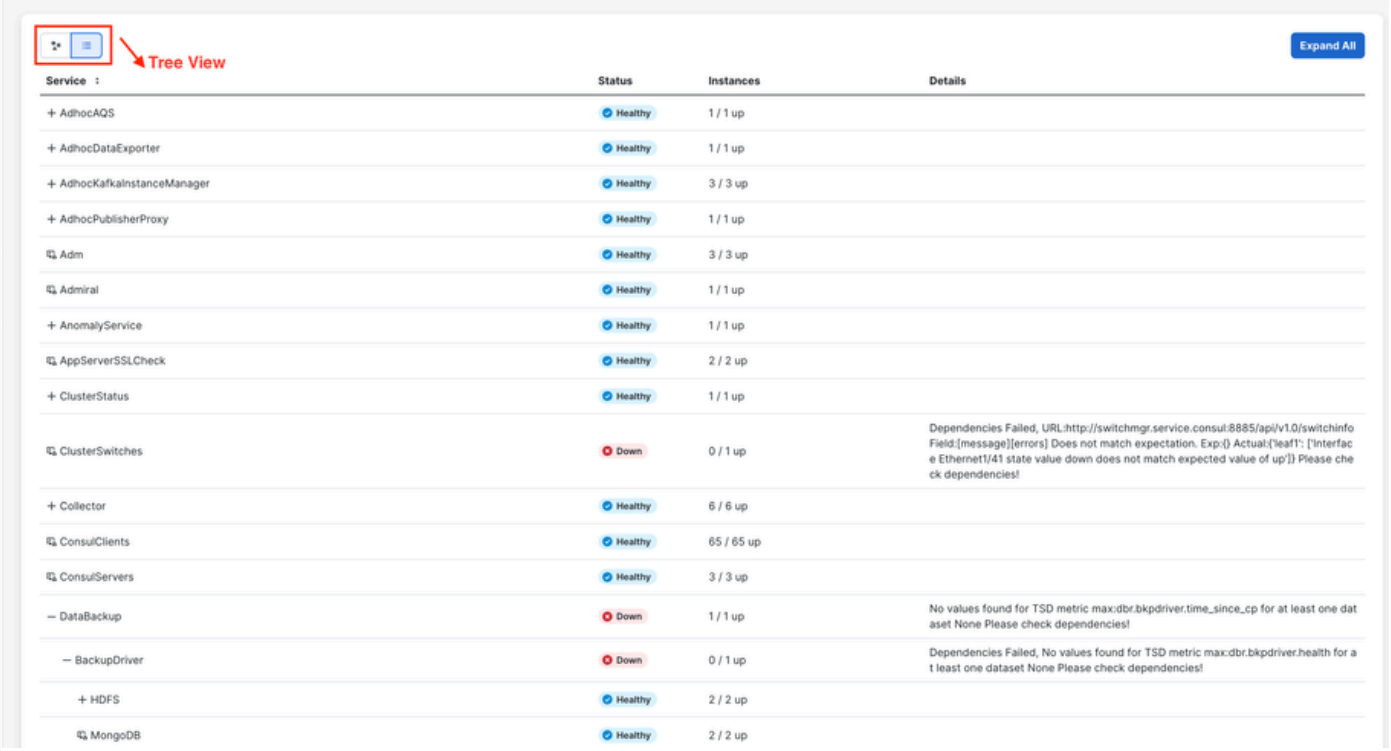


Per impostazione predefinita, la pagina Stato del servizio mostra le funzioni cluster e le dipendenze in una visualizzazione grafica. Se le icone sono tutte di colore verde o azzurro, non viene rilevato alcun errore.

Se un servizio è visualizzato in rosso o in arancione, la struttura mostra l'elenco dei servizi e consente di espandere le dipendenze del servizio e altri dettagli rilevati dalla funzione Stato del servizio. Queste informazioni sull'errore di dipendenza sono particolarmente importanti da rilevare e acquisire quando si apre una richiesta con il TAC.



Attenzione: Se uno dei servizi non è integro e di colore rosso, contattare il Technical Assistance Center (TAC) per assistenza nella risoluzione dei problemi. La collaborazione rapida con TAC consente di ripristinare la piena funzionalità.

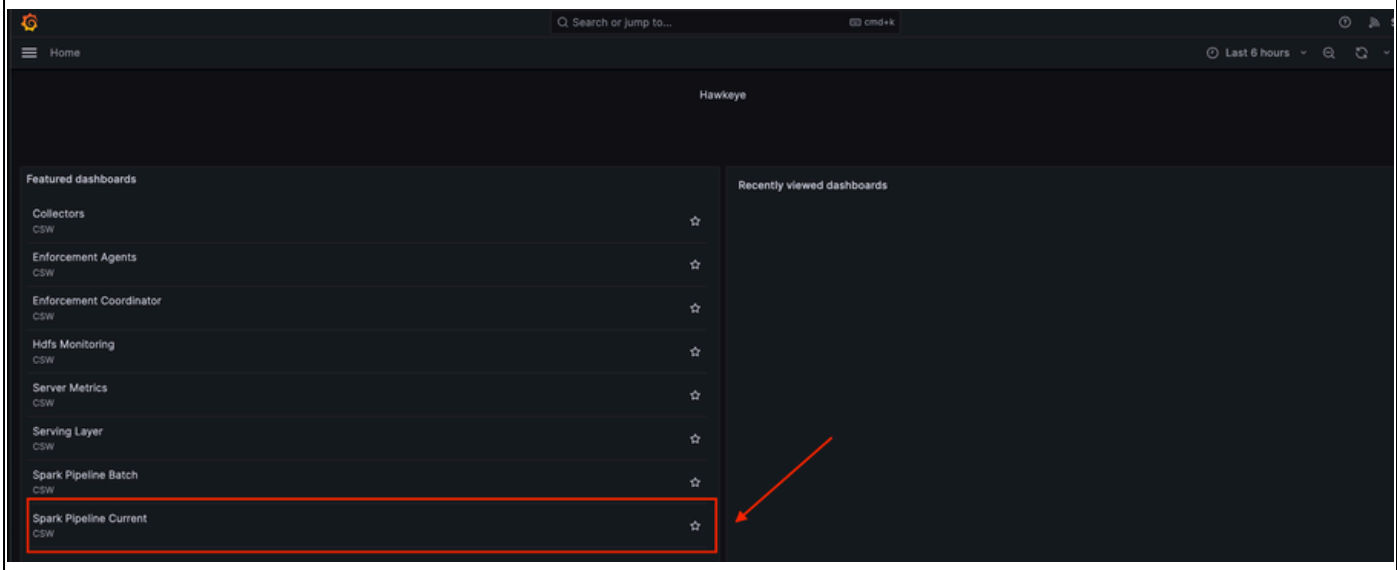


Occhi di falco (grafici)

I dashboard hawkeye offrono visibilità sullo stato del cluster del carico di lavoro sicuro, nonché metriche e informazioni dettagliate per la risoluzione dei problemi

La pagina Chiave di attivazione (Grafici) si trova nel riquadro di navigazione a sinistra sotto Risoluzione dei problemi > Chiave di attivazione (Grafici).

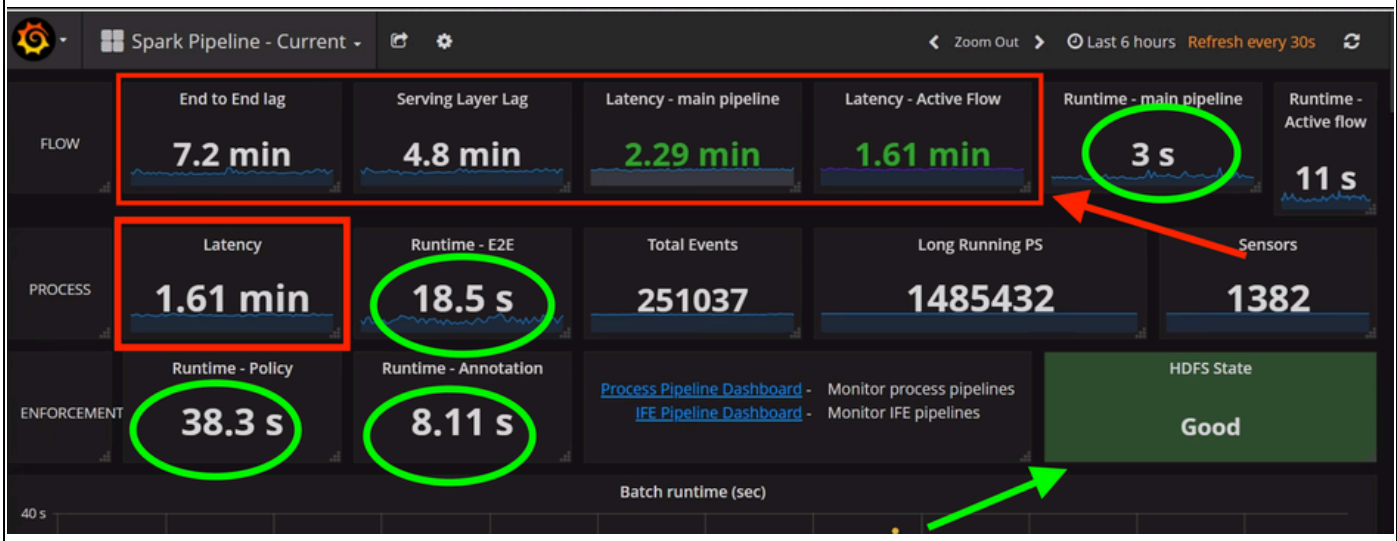
Quando si fa clic su Chiave hawkey (Grafici), viene visualizzata automaticamente una nuova scheda del browser che mostra il quadro comandi di Chiave hawkey come mostrato di seguito.

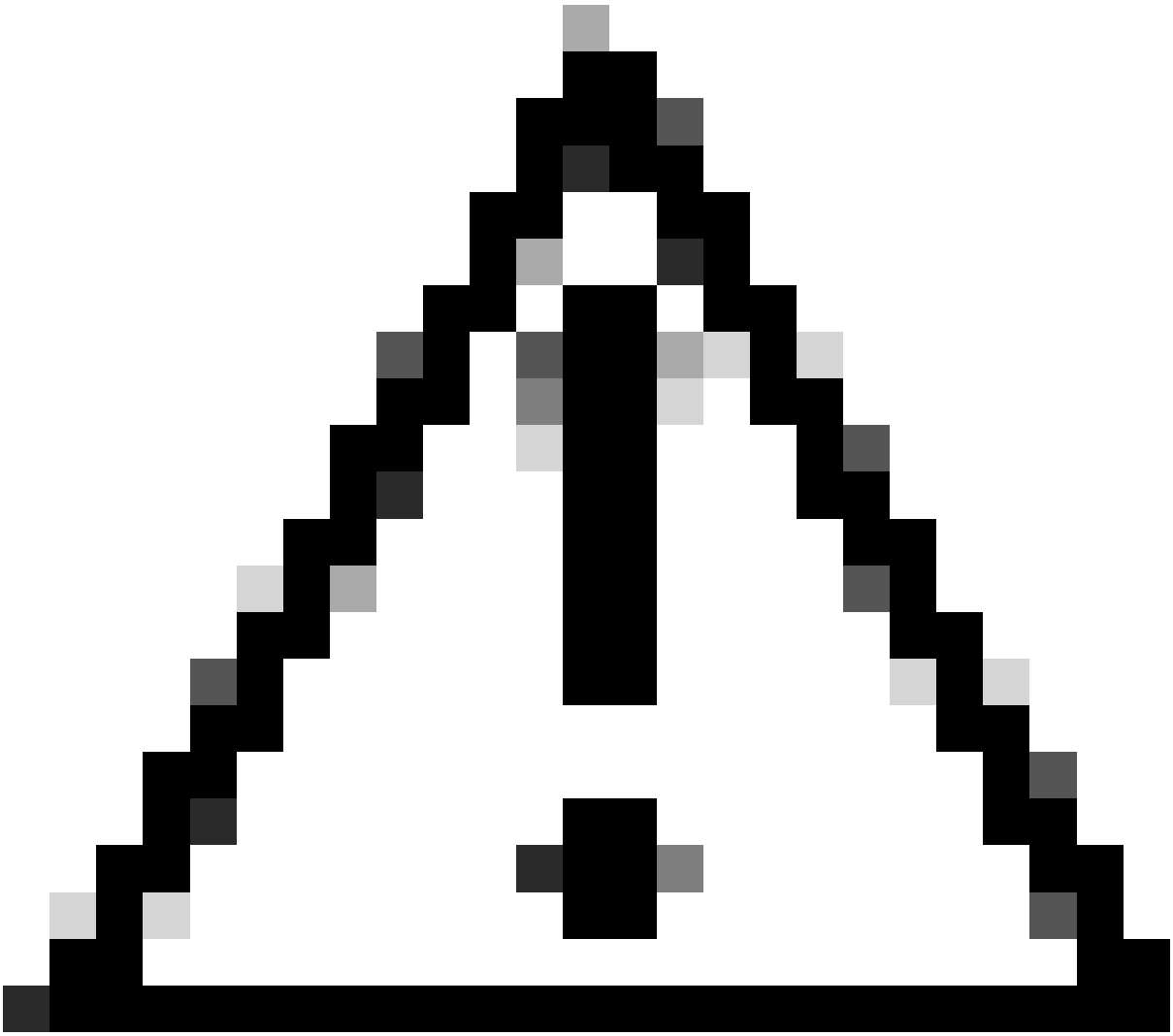


Dal dashboard di Hawkeye, fare clic sulla scheda Corrente Pipeline Spark per monitorare lo stato del cluster del carico di lavoro sicuro.

Nella pagina Corrente tubazione di spark verificare che i valori di Ritardo estremità-estremità, Ritardo livello di servizio, Latenza tubazione principale e Latenza flusso attivo siano inferiori a 10 minuti.

Inoltre, verificate che i valori di runtime siano inferiori a 1 minuto e che vengano visualizzati in secondi e che lo stato di HDFS sia Buono, come illustrato di seguito.





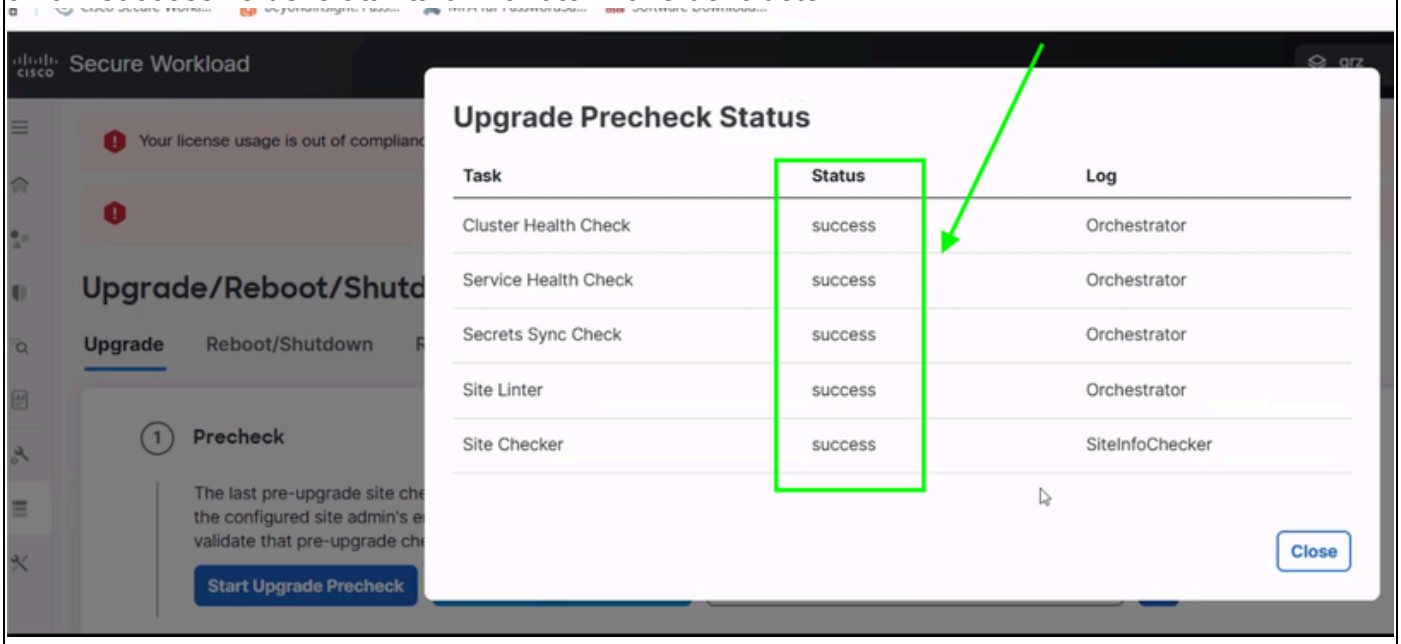
Attenzione: Se si osservano valori di latenza, incluso il ritardo end-to-end o il ritardo del livello di servizio, superiori a 6 ore senza mostrare una riduzione graduale, contattare il Technical Assistance Center (TAC).

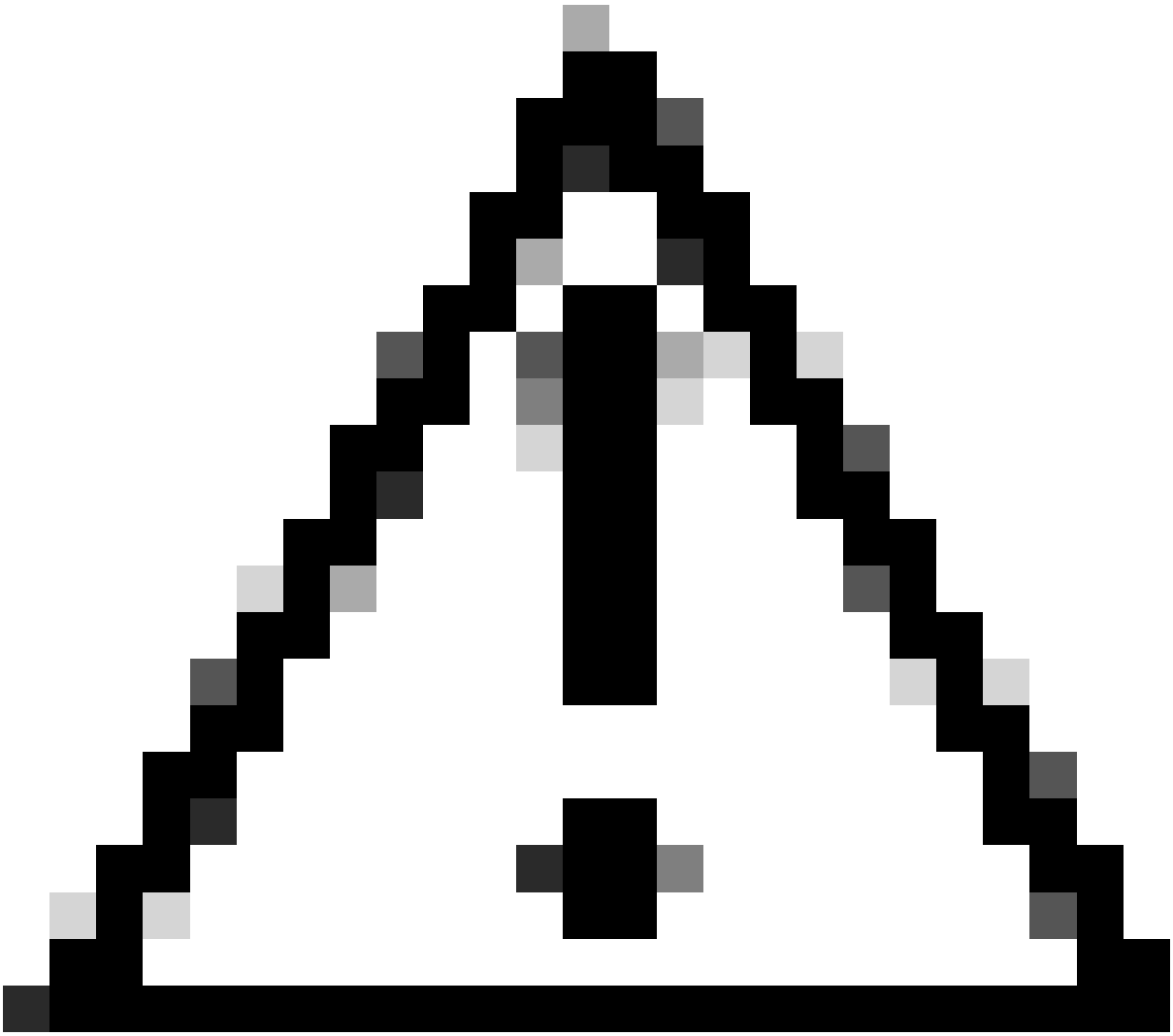
Aggiorna controlli preliminari

Prima e dopo le attività di manutenzione, utilizzare la verifica preliminare di aggiornamento per eseguire i controlli di integrità del cluster. questo processo garantisce che i servizi, le configurazioni e i componenti hardware funzionino correttamente

1. Passare a Preselezione aggiornamento.
   Passare a TetrationUI e attenersi alla procedura seguente:
   - Fare clic su Piattaforma.
   - Selezionare Upgrade/Reboot/Shutdown (Aggiorna/Riavvia/Arresta).
   - Fare clic su Avvia pre-aggiornamento.

Attendere alcuni minuti per l'output dei controlli preliminari di aggiornamento. Se tutte le operazioni hanno esito positivo, come illustrato in questa immagine, è possibile procedere con le azioni successive delle attività di manutenzione del cluster.





Attenzione: Se i controlli preliminari dell'aggiornamento non hanno esito positivo, contattare il Technical Assistance Center (TAC) per assistenza.

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).