Verificare l'integrità di un cluster Tetration Analytics

Sommario

Introduzione

In questo documento viene descritto come verificare lo stato di un cluster Tetration Analytics.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Accesso a un cluster
- Funzionalità dell'interfaccia utente di base

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Versione 2.2.1.x
- Cluster 39RU Tetration Analytics

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali

conseguenze derivanti dall'uso dei comandi.

Premesse

Un cluster Tetration è costituito da centinaia di processi (programmi) in esecuzione su più VM [Virtual Machine] su più server UCS C220-M4. Sono disponibili diversi servizi e funzionalità che consentono di monitorare le operazioni del cluster e avvisare l'amministratore quando il cluster potrebbe non funzionare correttamente.

In questo documento viene illustrato ciò che è necessario verificare durante la verifica dello stato del cluster. Anche se l'ambito di questo documento include la verifica dello stato, se sono necessarie azioni per risolvere problemi che sembrano non funzionare correttamente, raccogliere un'istantanea e aprire una richiesta di assistenza in collaborazione con il team TAC di supporto della soluzione Cisco Tetration.

Due strumenti comuni utilizzati per verificare l'integrità del cluster sono le pagine **Stato cluster** e **Stato servizio** descritte in questo documento insieme a un paio di altri strumenti di sistema. Sebbene gli avvisi e-mail **critici di** Bosun siano spesso una delle prime indicazioni per un amministratore che qualcosa potrebbe accadere nel cluster, la verifica dello stato del cluster viene in genere eseguita in modo ottimale tramite le pagine **Stato cluster** e **Stato servizio**.

Mentre gli allarmi Boson forniscono funzionalità simili al syslog, in alcune versioni di Tetration, alcuni allarmi Bosun critici sono stati attivati in un cluster normalmente funzionante. Una ricerca con la parola chiave metric nello strumento di ricerca dei bug di cisco.com per il prodotto **Tetration** aiuterà a identificare i possibili problemi per una metrica specifica.

Quando verificare lo stato del cluster:

In genere, l'amministratore del cluster non dovrà verificare la funzionalità del cluster. Vi sono tuttavia dei momenti in cui potrebbe essere necessario. Di seguito sono riportati alcuni esempi:

1. Quando l'utente rileva un comportamento imprevisto nell'interfaccia utente. Questa procedura si basa in parte sulle conoscenze e sull'esperienza dell'utente relativamente al funzionamento del cluster, ma alcuni esempi sono illustrati in questa sezione **Parametri di visualizzazione operativa**.

2. Quando si prevede che alcuni dati vengano visualizzati ma non visualizzati nell'interfaccia utente. Ad esempio, i dati di flusso provenienti da un agente software o hardware (sensore) quando si visualizzano l'ambito e l'intervallo di tempo appropriati in cui si prevede di visualizzare i dati.

3. Prima e dopo qualsiasi servizio pianificato, aggiornamento o azione principale del cluster. È buona norma raccogliere un'istantanea prima e un'altra istantanea dopo qualsiasi manutenzione e renderla disponibile nel caso in cui venga aperta una richiesta TAC. Questo consente a TAC di isolare il problema cercando le modifiche apportate durante la manutenzione.

   Nota: Alcune interruzioni del servizio sono normali per un periodo di tempo immediatamente successivo alla manutenzione del sistema nel cluster. Il periodo di tempo può essere fino a

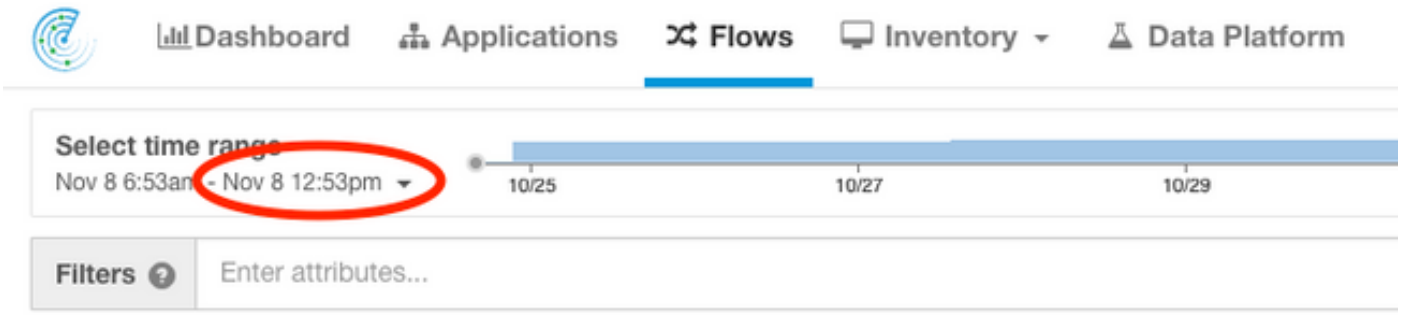
24 ore nell'esempio di sostituzione di un server in cui una VM in modalità dati viene eseguita su tale server. La normale ridondanza del sistema nel cluster in genere riduce gli effetti negativi della sostituzione di un singolo server.

Diversi modi per verificare lo stato operativo di un cluster di Tetration

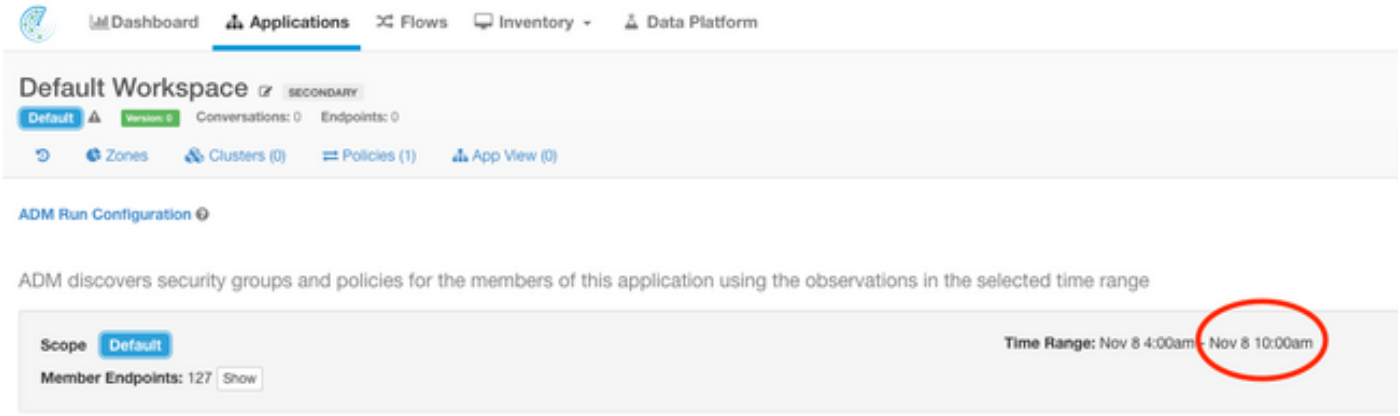
Parametri di visualizzazione operativi

Un amministratore con conoscenze ed esperienza del funzionamento del cluster è in grado di riconoscere l'aspetto del normale funzionamento del cluster nel relativo ambiente. Di seguito sono riportati alcuni esempi di elementi da cercare per verificare se il cluster funziona correttamente.

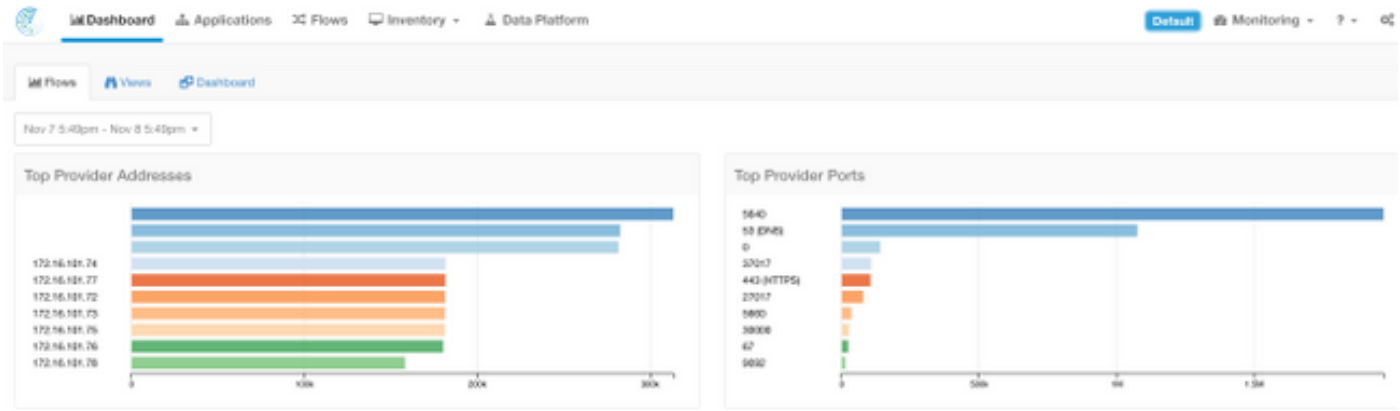
Esempio 1: L'ultimo tempo di flusso disponibile è entro 10 minuti dall'ora corrente



Esempio 2: L'ultima ora disponibile per l'area di lavoro dell'applicazione è entro 10 ore dall'ora corrente:



Esempio 3: Il contenuto del dashboard è popolato.

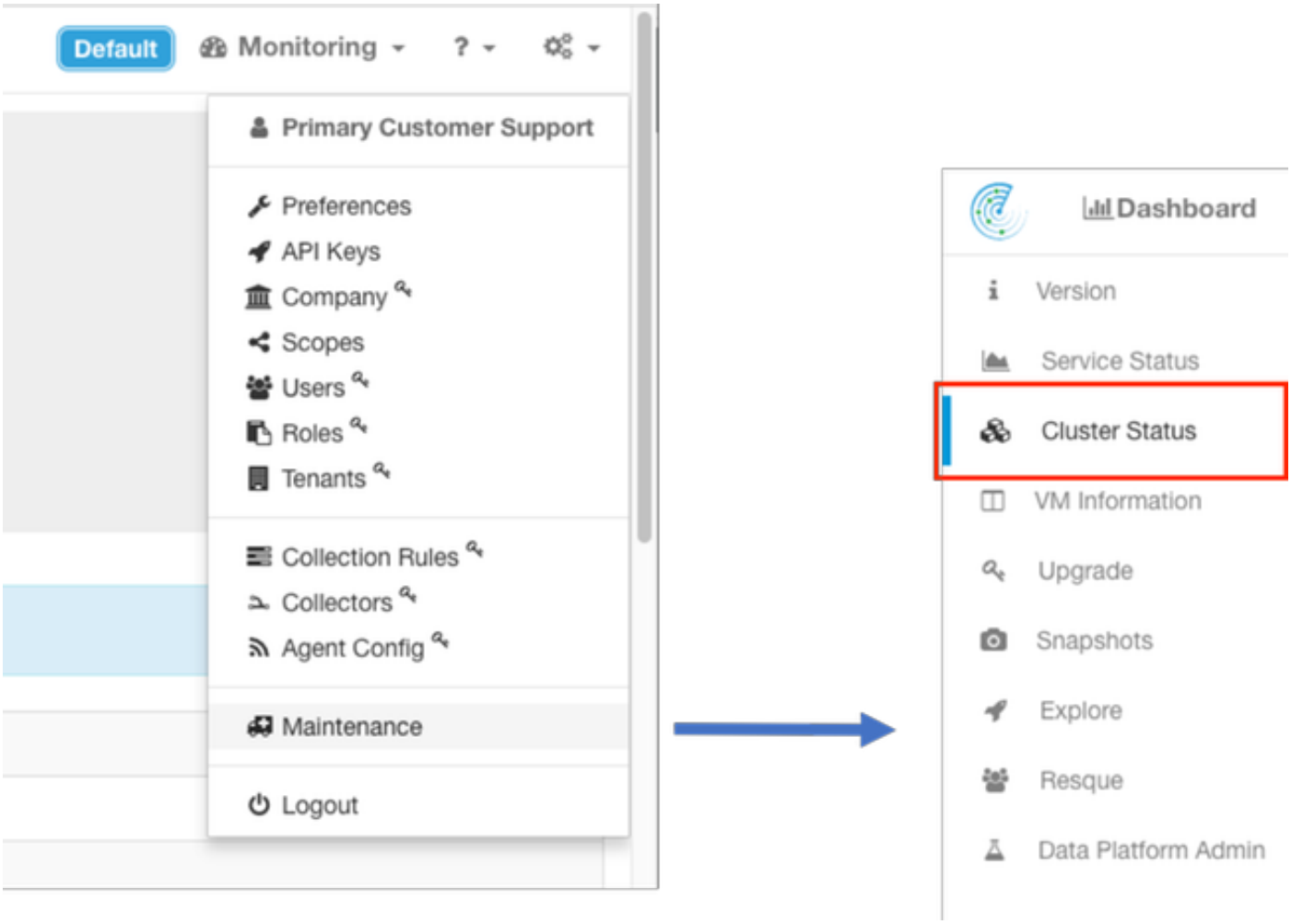


Stato cluster

Un cluster Tetration Analytics è costituito da 6 (8RU) o 36 (39RU) server a seconda del tipo di cluster. La pagina Stato cluster fornisce lo stato dei server e altre informazioni sul server bare metal.

La pagina Stato cluster si trova nel menu Manutenzione disponibile dall'elenco a discesa Impostazioni (**Impostazioni > Manutenzione**; Stato cluster nella colonna sinistra.)

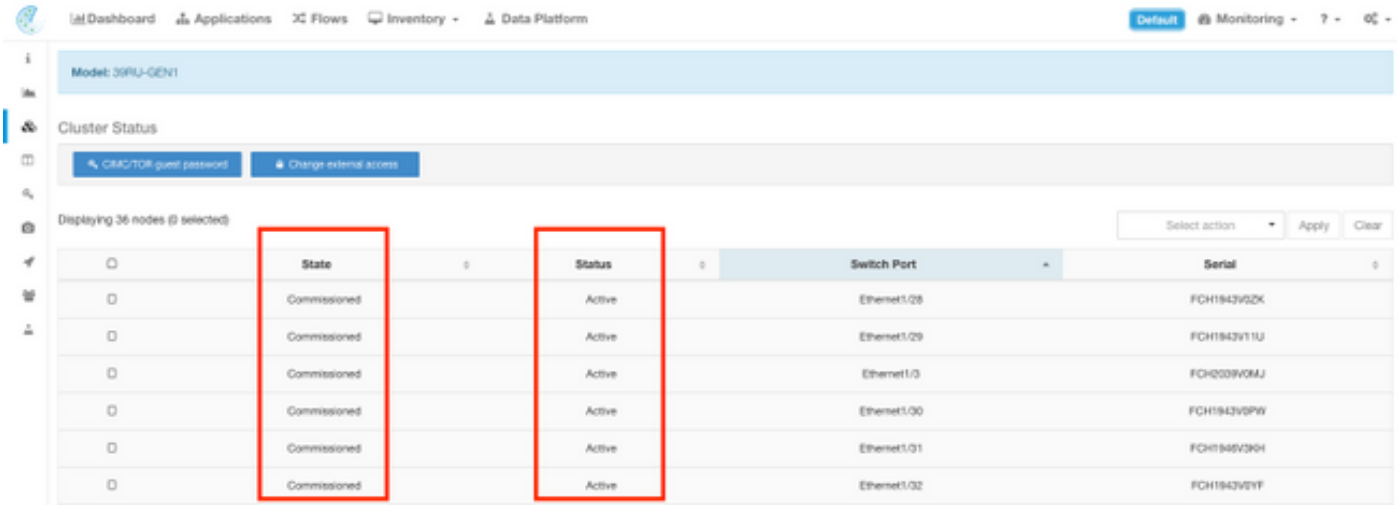
> **Nota:** Solo l'icona è visibile fino a quando non si fa clic sulla colonna sinistra.



Nella pagina Stato cluster di un cluster viene visualizzata una lista di tutti i server del cluster. Un server funzionante deve visualizzare **lo stato** di **commissionato** e lo **stato** di **attivo**, come illustrato

di seguito.

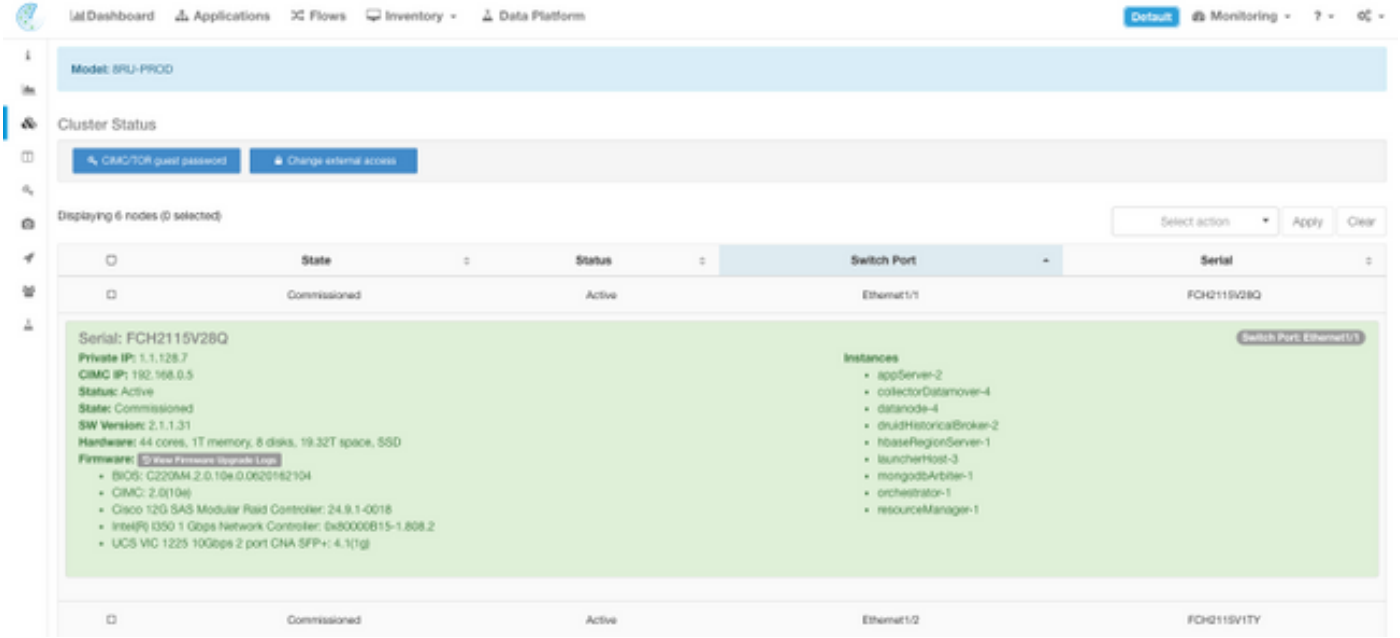
Nota: L'immagine viene troncata ai primi 6 dei 36 server (cluster 39RU).



Se lo stato è Inattivo, in genere si tratta di un server che non è acceso o che potrebbe presentare problemi di connettività o di cavi.

Quando si fa clic su un server nell'elenco, vengono visualizzate ulteriori informazioni sul server specifico, tra cui:

1. Istanze (macchine virtuali) in esecuzione sul server bare metal.
2. Indirizzo IP privato nel cluster.
3. Indirizzo IP CIMC nel cluster.
4. Versioni del firmware (BIOS, CIMC, controller RAID) in esecuzione sul server.



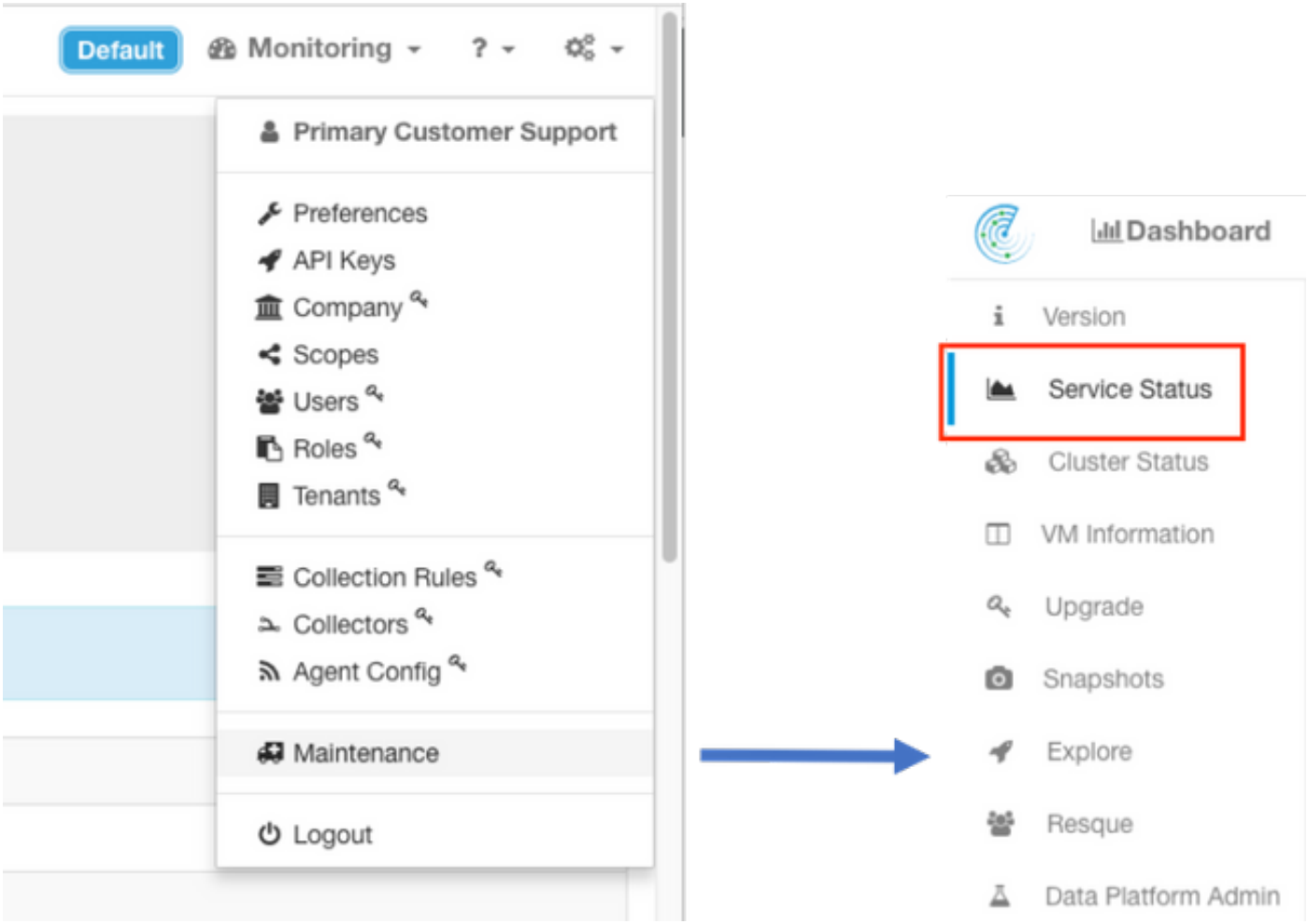
Stato del servizio

OSPF (Open Shortest Path First) ServizioStato pagina visualizza tutto servizios utilizzati nel cluster Cisco Tetration Analytics con le relative dipendenze e integrità stato.

La pagina Stato del servizio si trova nel menu Manutenzione disponibile dall'elenco a discesa delle

impostazioni. (**Impostazioni > Manutenzione**; Stato del servizio nella colonna sinistra.)

Nota: Solo l'icona è visibile fino a quando non si fa clic sulla colonna sinistra.

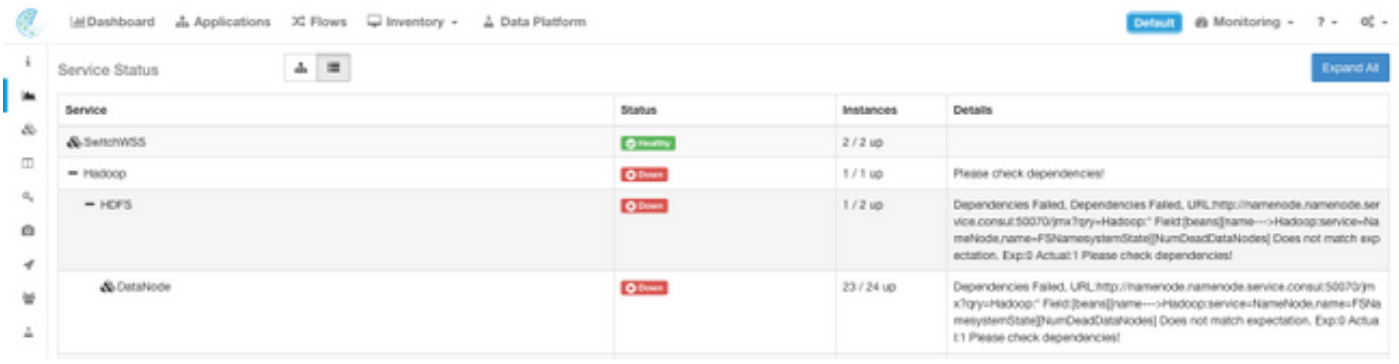


Per impostazione predefinita, la pagina Stato del servizio mostra le funzioni cluster e le dipendenze in una visualizzazione grafica. Se le icone sono tutte verdi, non viene rilevato alcun errore.

Se un servizio è visualizzato in rosso o in arancione, nella struttura verrà visualizzato l'elenco dei servizi e sarà possibile 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.

Ad esempio, di seguito viene illustrato l'aspetto dell'elenco quando una delle macchine virtuali DataNode HDFS nel cluster è inattiva

Nota: L'impatto sul cluster potrebbe non essere visibile a causa della ridondanza progettata nel cluster Tetration.



Nota: Dopo l'esecuzione della manutenzione, alcuni servizi potrebbero tornare in uno stato di funzionamento in ritardo. Ad esempio, un server su cui è in esecuzione un'istanza della

macchina virtuale DataNode che viene rimossa e riassegnata per la manutenzione RMA può impiegare fino a 24 ore prima che il problema rilevato venga risolto.

Anche se i dettagli in Stato del servizio indicano cosa potrebbe accadere in caso di problemi rilevati, si consiglia di aprire una richiesta TAC in caso di domande sul significato e/o sulle potenziali azioni da intraprendere per risolverli.

Avvisi Bosun

Bosun è un sistema di monitoraggio e avviso open source utilizzato nel cluster Tetration Analytics per monitorare varie metriche dei servizi (un programma che viene avviato all'avvio) in esecuzione nel cluster. Quando un servizio viene eseguito normalmente, le relative metriche vengono popolate in openTSDB. Il programma Bosun esamina le metriche di un servizio in openTSDB e applica le regole bosun per determinare se inviare o meno un avviso sulle metriche correnti. Gli avvisi Bosun possono essere visualizzati localmente nell'interfaccia utente del cluster in **Monitoraggio > Sentinel** [Avvisi].

Bosun utilizza la posta elettronica (inviata al sito di configurazione del cluster site_bosun_email) per avvisare l'amministratore del cluster di una potenziale condizione **critica** quando viene superata una soglia per quella metrica. Bosun genera 3 tipi di e-mail:

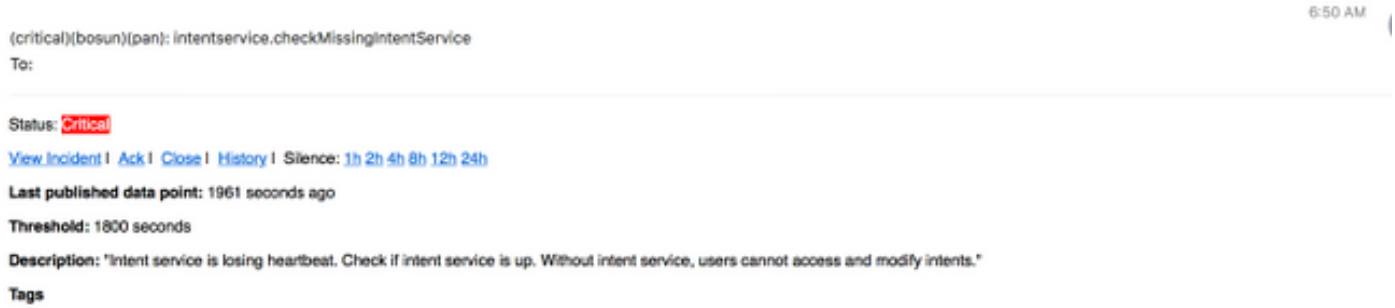
Critico: quando una metrica per una regola di avviso Bosun supera la soglia configurata

Normale: Segue un messaggio e-mail "critico" quando la metrica rientra nella soglia

Riepilogo: Generalmente inviato ogni 6 ore e mostra un riepilogo degli avvisi durante il periodo di 6 ore

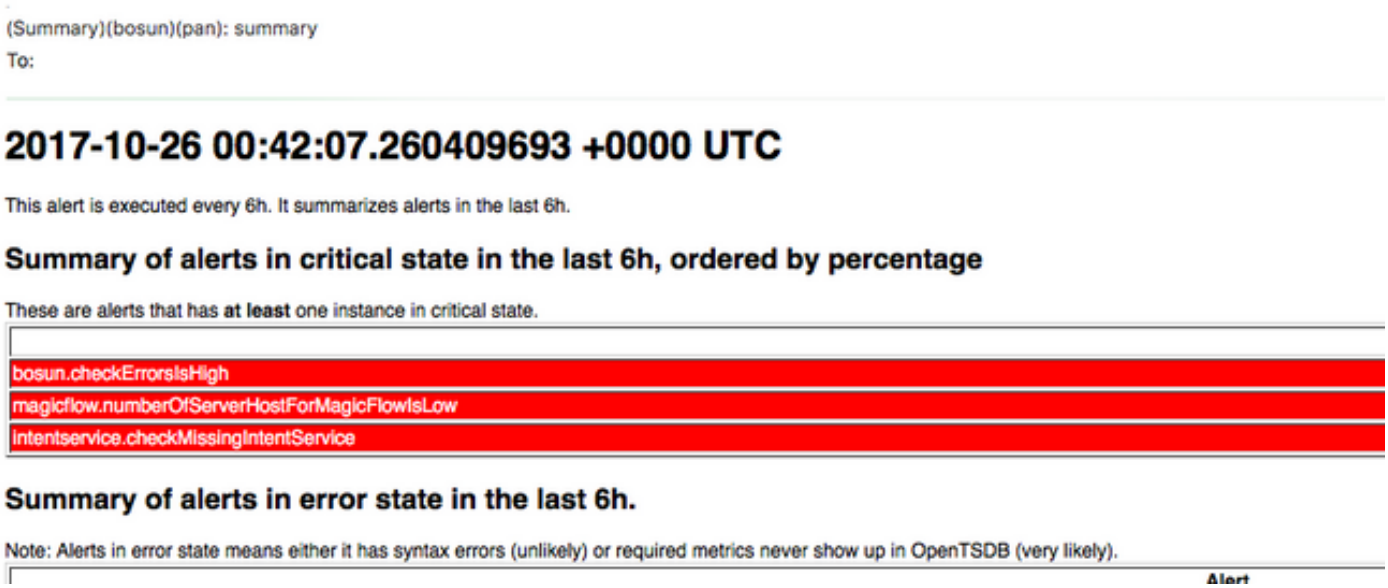
Esempi di avvisi e-mail:

Critico (per la metrica intenservice.checkMissingIntentService) **:**



Normale:

Riepilogo:



Gli alert critici contengono informazioni su quali metriche, quando, la soglia, il punto dati misurato e una descrizione del problema. Ad esempio, l'avviso potrebbe essere generato quando il servizio non funziona correttamente e non fornisce più le relative metriche a openTSDB. Il significato e il potenziale impatto dell'allarme critico di Bosun può richiedere l'apertura di una richiesta TAC per comprendere meglio il contesto e spiegare il significato dell'allarme.

Raccogli snapshot e apri richiesta TAC

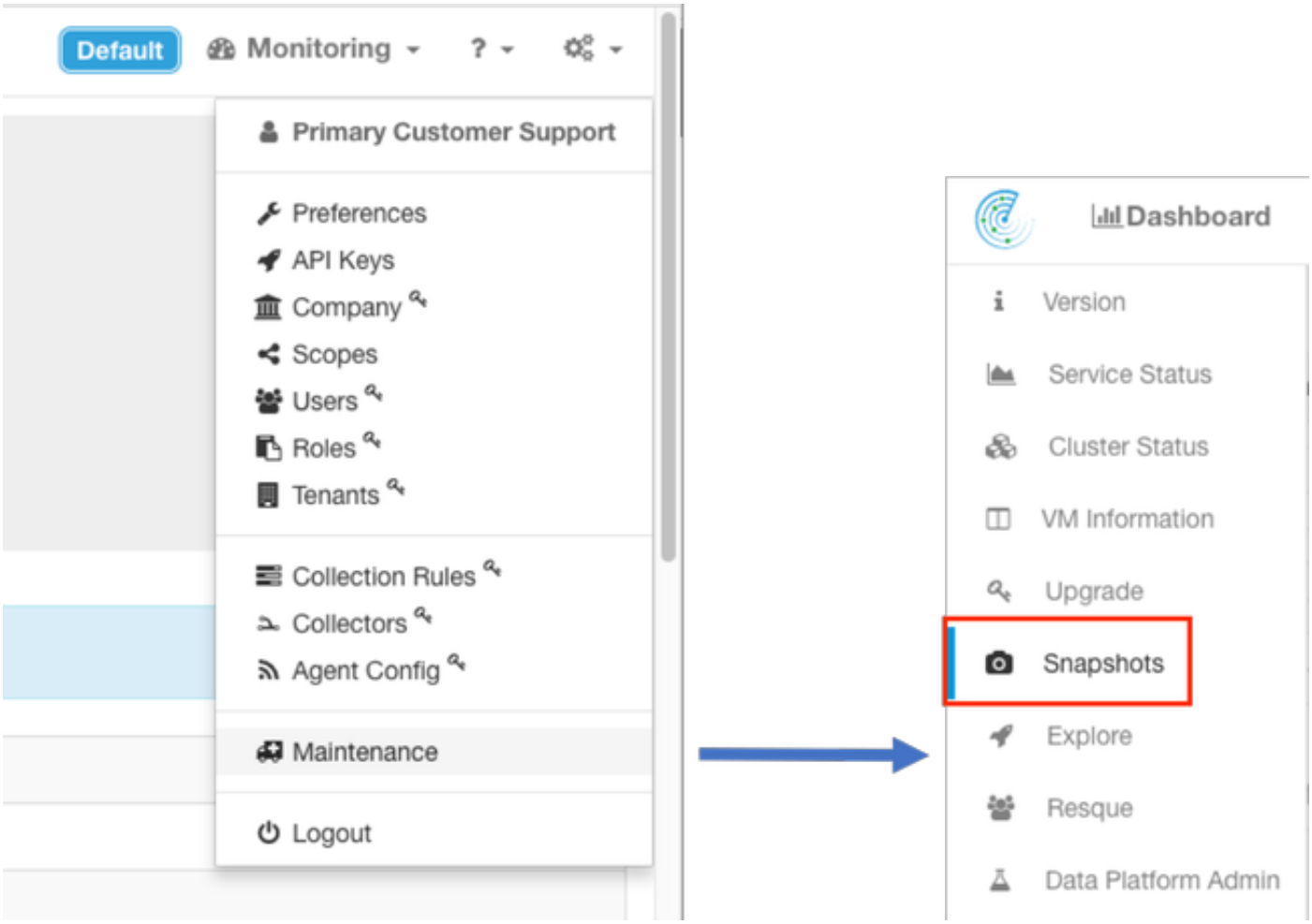
Il team Cisco Tetration Solution è specializzato e supporta i clienti Tetration Analytics. Uno degli elementi più comuni a disposizione dei tecnici TAC per il processo di risoluzione dei problemi è una raccolta di snapshot dei log del cluster. A volte, solo le informazioni contenute nei file di log delle copie istantanee sono sufficienti per comprendere il problema. In caso contrario, in molti casi una copia istantanea costituisce il punto di partenza del processo di risoluzione dei problemi.

Una copia istantanea in un cluster Tetration è simile al supporto tecnico di altri prodotti Cisco. Si tratta di un file tarball compresso o file di log di tutti i server e le macchine virtuali e include:

- Log
- Stato dell'applicazione Hadoop/YARN e dei registri
- Cronologia avvisi
- Numerose statistiche TSDB

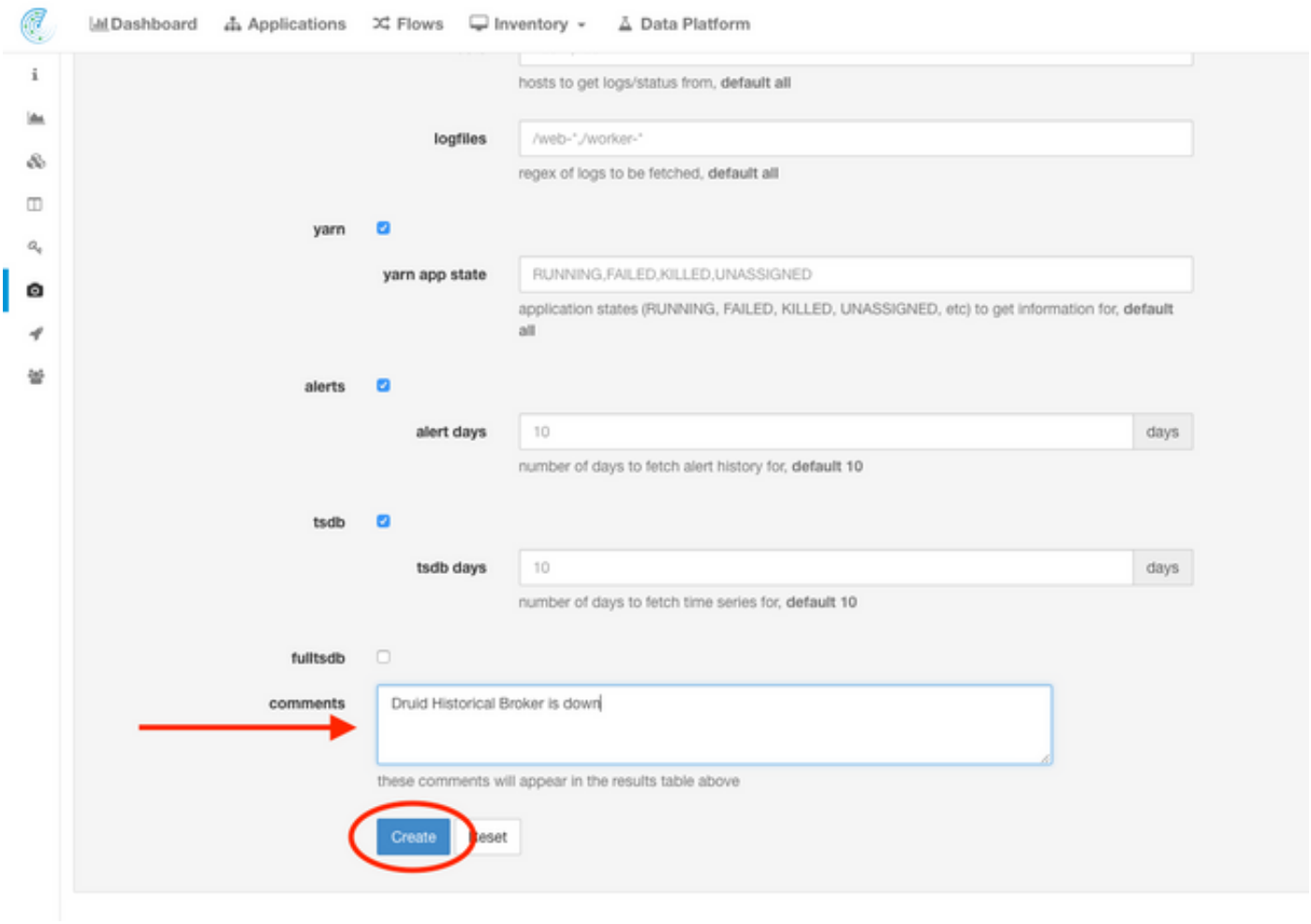
La pagina della copia istantanea si trova nel menu Manutenzione disponibile dal menu a discesa delle impostazioni. (**Impostazioni > Manutenzione**; Istantanee nella colonna sinistra.)

> **Nota:** Solo l'icona è visibile fino a quando non si fa clic sulla colonna sinistra.



La pagina della copia istantanea offre diverse opzioni da selezionare ma, a meno che non sia richiesto da un tecnico TAC, è possibile utilizzare i valori predefiniti per raccogliere la copia istantanea.

Un'area importante da modificare è **Commenti**. I commenti devono fornire informazioni che indichino il motivo per cui lo snapshot è stato raccolto quando sono presenti più snapshot raccolti dal cluster e i commenti aggiunti sono disponibili anche all'interno dello snapshot durante l'analisi da parte di Cisco TAC.



Quando si fa clic sul pulsante **Crea**, viene avviato il processo di copia istantanea. È possibile creare una sola istantanea alla volta e il completamento del processo richiede alcuni minuti. Nella parte superiore della pagina dello snapshot viene visualizzata una barra di avanzamento per la raccolta di snapshot.

La copia istantanea può quindi essere scaricata sul sistema locale dell'utente facendo clic sul collegamento Download appropriato nella pagina della copia istantanea, come mostrato nell'immagine:

> **Nota:** Le dimensioni del file snapshot possono essere di diverse centinaia di megabyte. Il file può quindi essere caricato nella richiesta TAC aperta.

Informazioni correlate

- Supporto Cisco Tetration Analytics
- Documentazione e supporto tecnico – Cisco Systems