

Ricerca di eventi unificati FMC non riuscita con i nomi degli oggetti di rete in Firepower 7.7

Problema

Quando si utilizza Cisco Secure Firewall Management Center (FMC) versione 7.7.10.1, gli oggetti di rete e i gruppi di oggetti non possono essere utilizzati come criteri di ricerca nella pagina Eventi unificati. Quando si tenta di cercare eventi utilizzando nomi di oggetti o gruppi specifici nell'indirizzo IP di origine in Ricerca eventi unificata, il CCP non restituisce alcun risultato o visualizza un messaggio di errore:

The query contains an invalid constraint on the provided field: "Source IP" with value "\${000_ALL-USER_

Gli oggetti sono visibili e utilizzabili in Gestione oggetti e le ricerche in base all'indirizzo IP non elaborato funzionano come previsto. Questo comportamento ha effetto sia sugli oggetti di rete esistenti che su quelli appena creati, rendendo difficile la ricerca di eventi utilizzando nomi di oggetti o di gruppi nell'interfaccia Eventi unificati.

Ambiente

- Cisco Secure Firewall Management Center per VMware (FMCv)
- Versione del software: 7.7.10.1
- Tecnologia: Cisco Secure Firewall Firepower - 7.7
- Sottotecnologia: Cisco Secure Firewall - Monitoraggio / Eventi / Registrazione - 7.7
- Implementazione: Configurazione FMC autonoma
- FMC contiene oltre 1000 oggetti di rete
- L'ambiente include la cronologia delle migrazioni dal CCP locale al CdFMC e viceversa

Risoluzione

Questo problema è causato da un difetto software noto e non può essere risolto completamente tramite modifiche alla configurazione della versione software corrente. Si raccomanda di attuare questo approccio alla risoluzione.

Soluzione immediata

Utilizzare i campi dell'indirizzo IP nelle ricerche degli eventi unificati anziché i nomi o i gruppi di oggetti come soluzione provvisoria. Durante l'analisi degli eventi correlati agli oggetti o ai gruppi interessati:

1. Passare ad Analisi > Eventi unificati.
2. Nei criteri di ricerca, utilizzare gli indirizzi IP effettivi anziché i nomi degli oggetti.
3. Immettere l'indirizzo IP o l'intervallo IP specifico nei campi IP origine o IP destinazione.
4. Eseguire la ricerca per recuperare gli eventi desiderati.

Soluzione a lungo termine

La correzione permanente richiede l'aggiornamento a una versione futura del software FMC che includa la risoluzione per Cisco Bug ID CSCws52418. Attenersi alla seguente procedura:

1. Iscriviti alle notifiche difettose CSCws52418 per ricevere avvisi quando diventano disponibili versioni FMC fisse.
2. Monitorare lo stato del bug per verificare la disponibilità degli aggiornamenti sulla correzione, provvisoriamente programmata per maggio 2026.
3. Pianificare una finestra di manutenzione per aggiornare FMC e i dispositivi gestiti a una versione che includa la correzione per CSCws52418 una volta pubblicata.

Prevenzione e raccomandazioni

Fino al completamento dell'aggiornamento del software:

- Utilizzare i criteri di ricerca basati su IP negli eventi unificati (IP di origine/destinazione)

quando si esaminano gli eventi correlati agli oggetti o ai gruppi interessati.

- Quando si creano nuovi flussi di lavoro operativi, evitare di basarsi esclusivamente sulle ricerche dei nomi degli oggetti negli eventi unificati per i processi operativi o di controllo di questa versione.
- Documentare i nomi degli oggetti interessati e gli indirizzi IP corrispondenti come riferimento durante la risoluzione dei problemi.

Causa

Il comportamento è causato dall'ID bug Cisco CSCws52418, in cui la gestione interna delle ricerche di oggetti per le ricerche di eventi è limitata da un limite interno di circa 1000 voci di oggetti. Gli oggetti al di fuori di questo limite non vengono indicizzati correttamente o restituiti nelle ricerche di eventi unificati in base al nome, con risultati mancanti o errori di vincolo non valido. La ricostruzione del database degli eventi monetdb non risolve questo comportamento in quanto si tratta di una limitazione software codificata e non di un problema di danneggiamento del database.

Contenuto correlato

- Cisco Bug ID CSCws52418 - Alcuni oggetti non sono disponibili per la selezione nei filtri di ricerca degli eventi
- Cisco ID bug CSCwt05296 - Impossibile utilizzare l'oggetto IPv4-Private-All-RFC1918 appena creato o definito dal sistema come filtro negli eventi
- [Supporto tecnico Cisco e download](#)

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).