Risoluzione dei problemi relativi all'errore "You have 0 out of xxxxxx FireSIGHT host licenses REMAINING"

Sommario

Problema

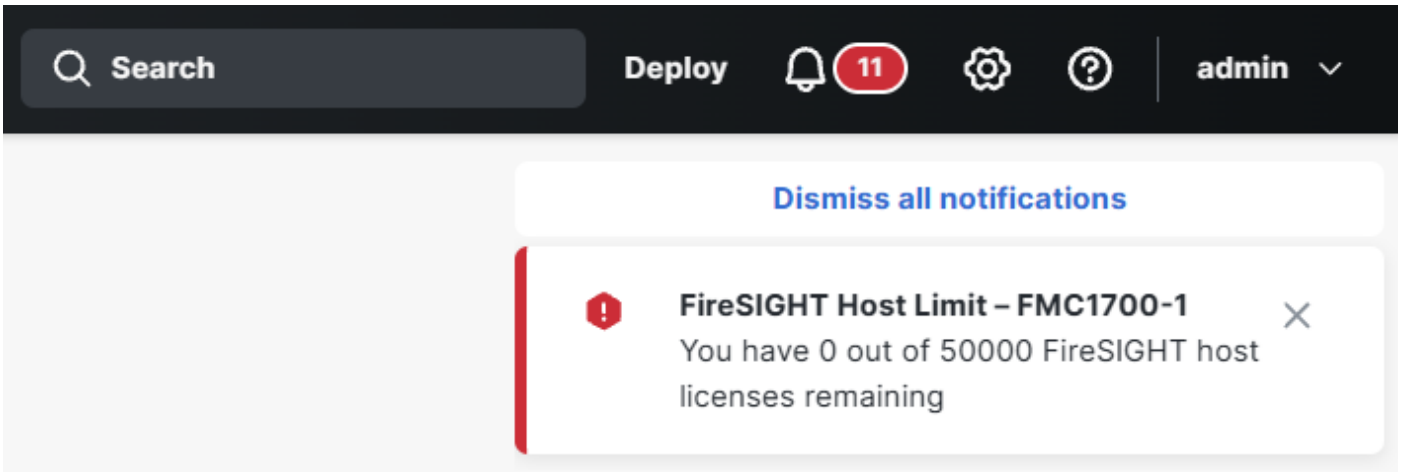
Un centro di gestione dei firewall visualizza un avviso di integrità che indica che è stato raggiunto il limite di licenze host. Il messaggio di errore specifico mostra:

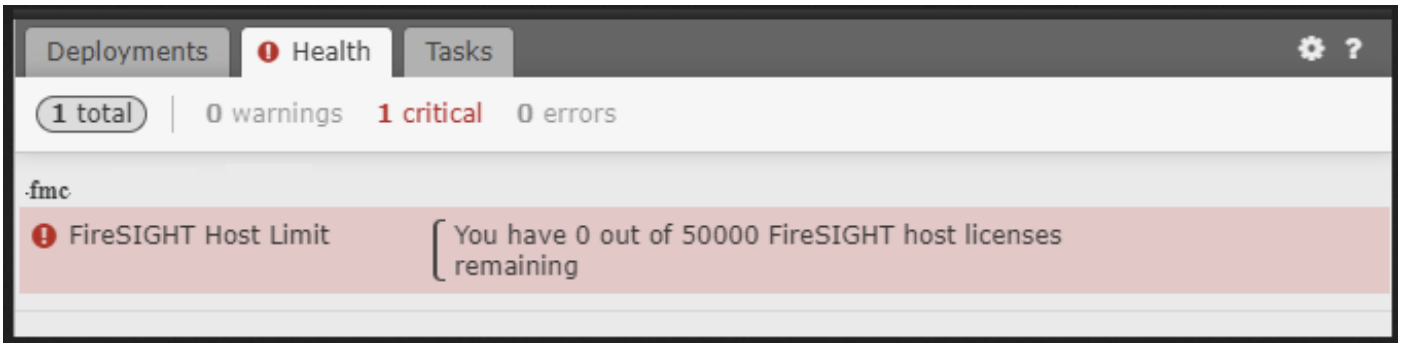
<#root>

FireSIGHT Host Limit – [FMC hostname]

You have 0 out of xxxxxx FireSIGHT host licenses remaining

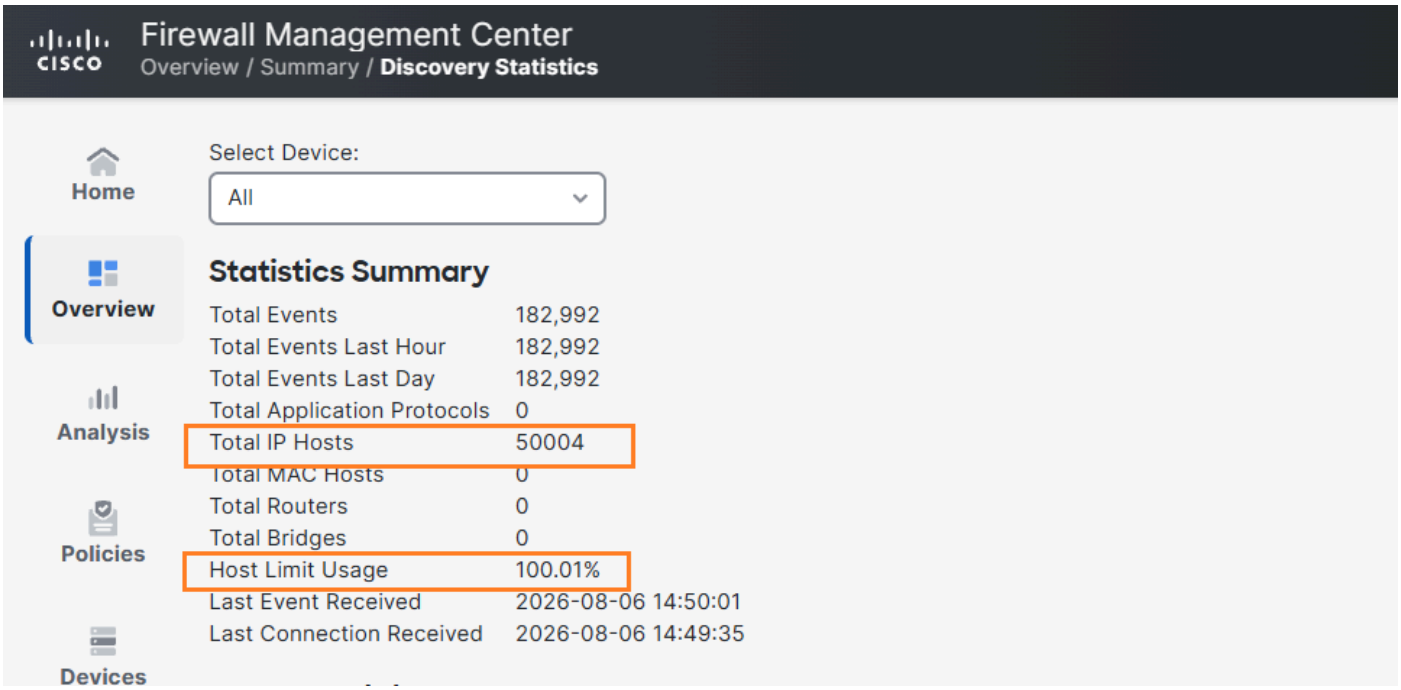
Esempi:





Nota: Il numero totale di licenze host dipende dalla piattaforma FMC.

Inoltre, nella pagina Panoramica > Riepilogo > Statistiche di individuazione viene visualizzato l'utilizzo al 100%:



Ambiente

- FMC 7.7.10. Il problema può riguardare anche altre versioni software.
- Individuazione rete configurata con rilevamento host abilitato.

Risoluzione

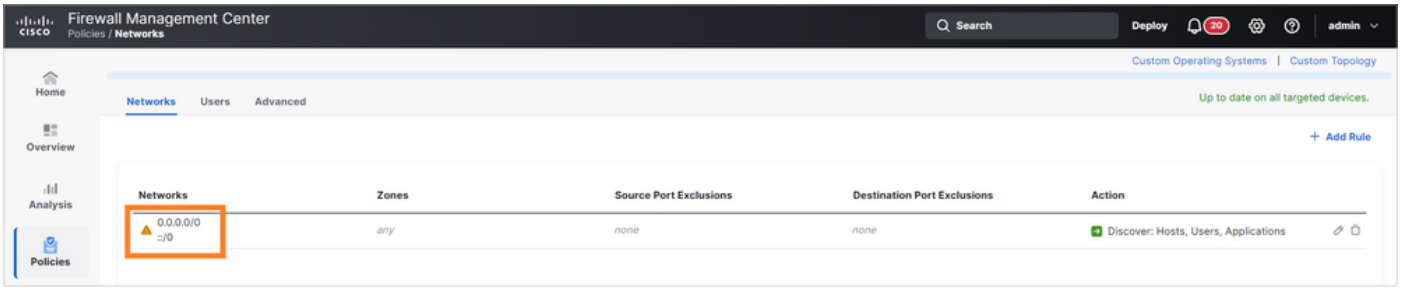
L'avviso relativo al limite host del FMC non causa interruzioni del traffico del firewall. Il controllo e l'ispezione degli accessi continuano a funzionare normalmente. L'impatto principale è sulla visibilità dell'host e sulla tracciabilità del contesto nel FMC.

Questa notifica viene visualizzata quando il CCP ha raggiunto la capacità massima per tenere traccia degli host nella mappa di rete e nel database host.

Verifica ambito di individuazione rete

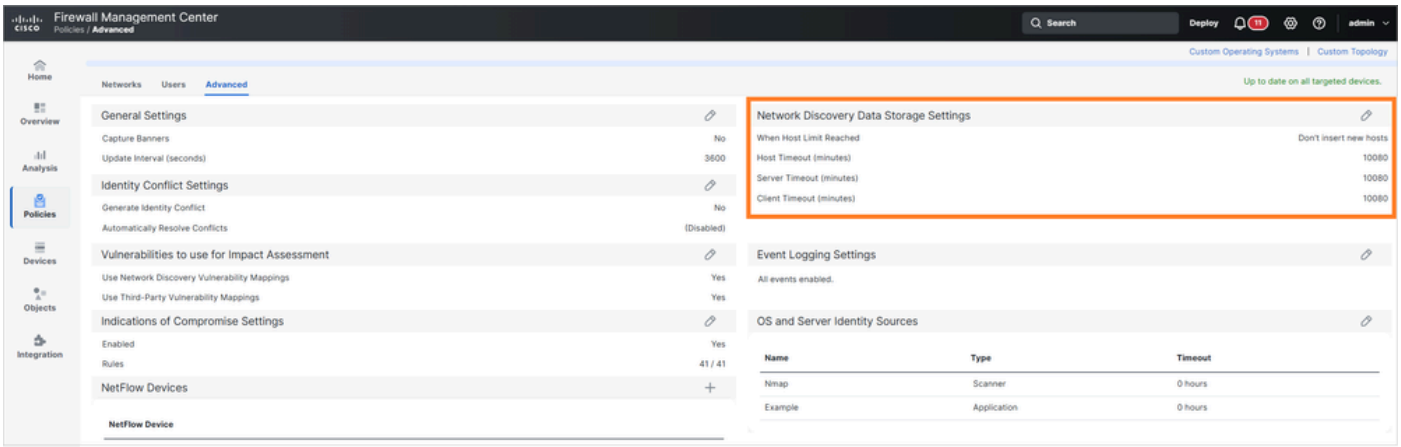
Assicurarsi che il rilevamento sia limitato alle reti interne necessarie. Evitare di individuare intervalli di indirizzi pubblici, NAT, guest, di bilanciamento del carico o transitori non necessari, a meno che non sia necessario per la visibilità della sicurezza.

In questo caso, è necessario modificare la configurazione di individuazione della rete e specificare solo le reti interne che si desidera monitorare. In caso contrario, gli host esterni (Internet) possono riempire il database di individuazione:



Analisi della configurazione corrente

Controllare il limite dell'host corrente esaminando le impostazioni di individuazione della rete in Criteri > Individuazione rete > Avanzate > Impostazioni di archiviazione dati individuazione rete:



La configurazione in genere mostra:

- Al raggiungimento del limite host: Non inserire nuovi host
- Timeout host: 10080 minuti / 7 giorni
- Timeout server: 10080 minuti / 7 giorni
- Timeout client: 10080 minuti / 7 giorni

Con l'impostazione corrente Non inserire nuovi host e il database host pieno, FMC non aggiunge i nuovi host rilevati fino a quando il numero di host non scende al di sotto del limite, causando una visibilità incompleta dell'host.

Modifica della configurazione opzionale

È possibile modificare il comportamento del limite host per consentire il rilevamento continuo degli host attivi:

Passaggio 1: Passare a Criteri > Individuazione rete.

Passaggio 2: Fare clic sulla scheda Avanzate.

Passaggio 3: In Impostazioni archiviazione dati individuazione rete fare clic su Modifica.

Passaggio 4: Cambia quando il limite dell'host raggiunge da Non inserire nuovi host a Elimina

host.

Passaggio 5: Salvare le modifiche.

Passaggio 6: distribuire la configurazione per applicare le modifiche.

Impatto e comportamento previsti

Con l'impostazione "Drop hosts" abilitata:

- Non è prevista alcuna interruzione del traffico del firewall.
- Il controllo e l'ispezione dell'accesso continuano normalmente.
- Quando si aggiungono nuovi host individuati, FMC rimuove l'host con il periodo di inattività più lungo dalla mappa di rete.
- Viene mantenuta la registrazione continua degli host attualmente attivi.
- Il contesto host cronologico per gli host eliminati non può più essere visibile fino a quando tali host non sono nuovamente attivi.

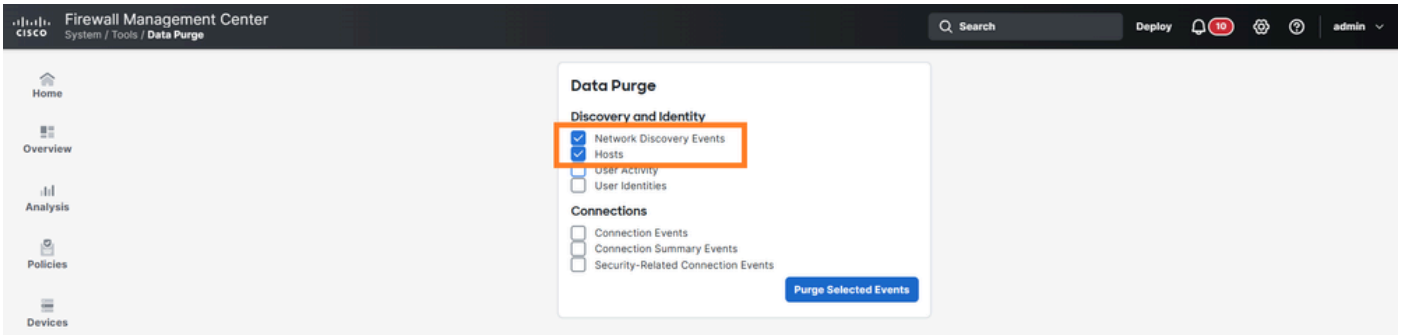
Revisione timeout host

I valori di timeout predefiniti, pari a 10080 minuti (7 giorni), sono in genere appropriati. Prendere in considerazione l'opportunità di effettuare modifiche solo se gli host inattivi vengono conservati troppo a lungo.

Pulizia manuale dell'host (se necessario)

Se è necessaria una riduzione immediata del numero di host, è possibile eliminare gli host non più validi da Analisi > Host > Vista tabella degli host. Si noti che si tratta solo di un'azione di pulizia. Se l'ambito di individuazione rimane troppo ampio, FMC esegue nuovamente il rilevamento degli stessi host.

In alternativa, è possibile rimuovere tutti gli host dal database di ricerca da Sistema > Strumenti > Rimozione dati:



Causa

Il limite di licenze host FireSIGHT viene raggiunto quando il FMC rileva e tiene traccia del numero massimo di host nella mappa di rete e nel database host. I fattori comuni comprendono:

- Ambito di individuazione della rete configurato in modo troppo ampio, inclusi intervalli di indirizzi esterni o pubblici non necessari.
- Individuazione di NAT, load balancer o indirizzi temporanei che utilizzano licenze host.
- Impostazioni di timeout host che mantengono gli host inattivi per periodi estesi.
- La crescita naturale della rete raggiunge il limite di capacità host FMC.

Contenuto correlato

- Guida alla configurazione dei dispositivi di Cisco Secure Firewall Management Center - Criteri di individuazione della rete
- 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).