

A pesquisa de eventos unificados do FMC falha com nomes de objetos de rede no Firepower 7.7

Problema

Ao usar o Cisco Secure Firewall Management Center (FMC) versão 7.7.10.1, objetos de rede e grupos de objetos não podem ser usados como critérios de pesquisa na página Eventos unificados. Ao tentar procurar eventos usando nomes de objetos ou grupos específicos em Source IP na pesquisa Unified Event, o FMC não retorna nenhum resultado ou exibe uma mensagem de erro:

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

Os objetos são visíveis e utilizáveis no Gerenciamento de objetos, e as pesquisas por endereço IP bruto funcionam conforme esperado. Esse comportamento afeta objetos de rede existentes e recém-criados, dificultando a pesquisa de eventos usando nomes de objetos ou nomes de grupos na interface de Eventos unificados.

Ambiente

- Cisco Secure Firewall Management Center para VMware (FMCv)
- Versão de software: 7.7.10.1
- Tecnologia: Cisco Secure Firewall Firepower - 7,7
- Subtecnologia: Cisco Secure Firewall - Monitoramento / Eventos / Registros - 7.7
- Implantação: Configuração do CVP autônomo
- O FMC contém mais de 1000 objetos de rede
- O ambiente inclui o histórico de migração do FMC local para o cdFMC e de volta para o local

Resolução

Esse problema é causado por um defeito de software conhecido e não pode ser totalmente resolvido por meio de alterações de configuração na versão de software atual. Recomenda-se a implementação desta abordagem de resolução.

Solução imediata

Use campos de endereço IP em pesquisas de Unified Event em vez de nomes de objetos ou grupos como uma solução temporária. Ao investigar eventos relacionados a objetos ou grupos afetados:

1. Navegue até **Análise > Eventos unificados**.
2. Nos critérios de pesquisa, use os endereços IP reais em vez dos nomes de objeto.
3. Insira o endereço IP específico ou o intervalo de IPs nos campos **Source IP** (IP de origem) ou **Destination IP** (IP de destino).
4. Execute a pesquisa para recuperar os eventos desejados.

Solução de longo prazo

A correção permanente requer a atualização para uma versão futura do software FMC que inclua a resolução do ID de bug Cisco CSCws52418. Siga estas etapas:

1. Inscreva-se para remover as notificações do CSCws52418 para receber alertas quando versões fixas do FMC estiverem disponíveis.
2. Monitore o status do bug para obter atualizações sobre a disponibilidade da correção, provisoriamente agendada para maio de 2026.
3. Planeje uma janela de manutenção para atualizar o FMC e os dispositivos gerenciados para uma versão que inclua a correção para o CSCws52418 depois de publicada.

Prevenção e recomendações

Até que o upgrade do software seja concluído:

- Use critérios de pesquisa baseados em IP em Eventos Unificados (IP de Origem/Destino) ao investigar eventos relacionados a objetos ou grupos afetados.
- Ao criar novos fluxos de trabalho operacionais, evite depender exclusivamente de pesquisas de nome de objeto em Eventos unificados para processos operacionais ou de auditoria nesta versão.
- Documente os nomes de objetos afetados e seus endereços IP correspondentes para referência durante a solução de problemas.

Causa

O comportamento é causado pela identificação de bug Cisco CSCws52418, onde o tratamento interno de pesquisas de objetos para pesquisas de eventos é restringido por um limite interno de aproximadamente 1000 entradas de objetos. Objetos fora desse limite não são indexados corretamente ou retornados em pesquisas de evento unificado por nome, resultando em resultados ausentes ou erros de "restrição inválida". A reconstrução do banco de dados de eventos monetdb não resolve esse comportamento, pois é uma limitação de software codificada, em vez de um problema de corrupção do banco de dados.

Conteúdo relacionado

- ID de bug Cisco CSCws52418 - Alguns objetos não estão disponíveis para seleção em Event Search Filters
- Cisco Bug ID CSCwt05296 - Não é possível usar o objeto recém-criado ou definido pelo sistema IPv4-Private-All-RFC1918 como um filtro em eventos
- [Suporte técnico e downloads da Cisco](#)

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.