

Solucione problemas e ative o NVM para a análise XDR

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Fluxos NVM do XDR Analytics](#)

[Fluxos de dados NVM - Análise XDR](#)

[Status do sensor NVM](#)

[ID da Org. NVM](#)

[Status de provisionamento do NVM Data Lake](#)

[Depuração](#)

[Observações e alertas](#)

[Alertas de NVM](#)

[Configurações de alerta NVM](#)

[Observações do NVM](#)

[Avisos de detecção de NVM](#)

[Conclusão](#)

Introdução

Este documento descreve como solucionar problemas do Cisco XDR Analytics para Cisco eXtended Detection and Response (XDR) / Network Visibility Module (NVM)

Pré-requisitos

Portal Ative XDR Analytics com integração XDR

Requisitos

Conta de análise XDR em execução com integração XDR única

Componentes Utilizados

- Análise de XDR
- XDR
- Sensor NVM
- Secure Client (Versão 5.0+)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

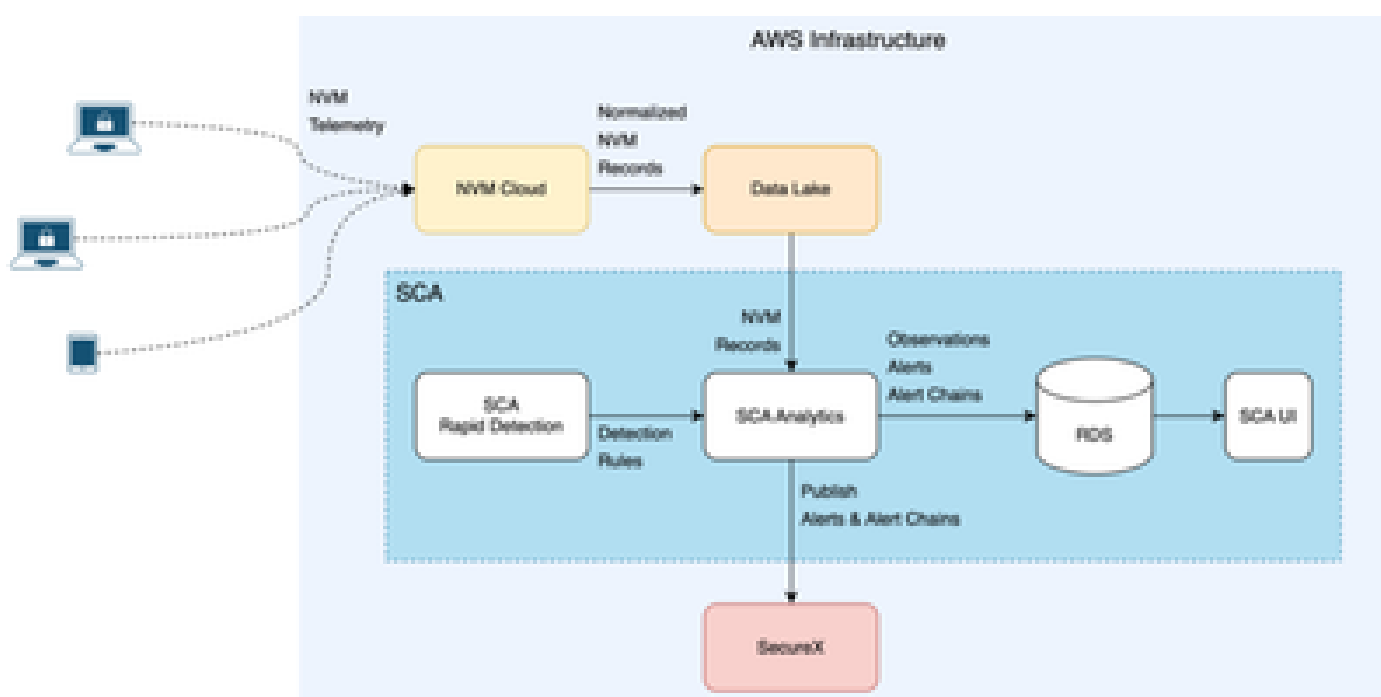
Fluxos NVM do XDR Analytics

A análise XDR agora consome a telemetria NVM
A telemetria é gerada pelo componente NVM no Cisco Secure Client.

O NVM oferece visibilidade de rede aprimorada, incluindo comportamentos de usuário, comunicações de rede e processos, reduzindo assim o tempo de investigação de incidentes e preenchendo lacunas na visibilidade do endpoint

<https://docs.xdr.security.cisco.com/Content/Help-Resources/nvm-resources.htm>

Fluxos de dados NVM - Análise XDR

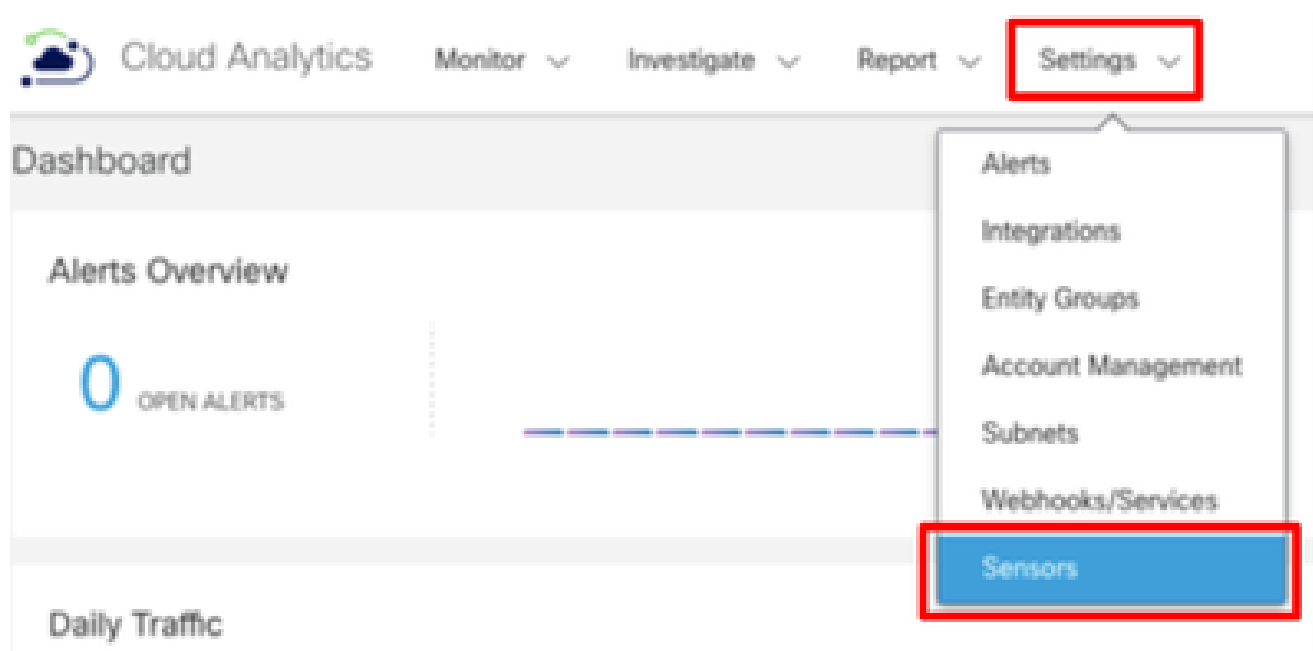


- Recomendamos sempre estar atualizado com suas versões do Secure Client. Esse fluxo de trabalho exige que você use o Secure Client versão 5.0 ou posterior:
https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/Cisco-Secure-Client-5/admin/guide/b-cisco-secure-client-admin-guide-5-0/deploy-anyconnect.html
- Mantenha uma atualização atualizada da versão do Secure Client e do Deployment Profile: <https://docs.xdr.security.cisco.com/Content/Client-Management/client-management.htm>
- O NVM Cloud lida com o volume de telemetria e o disponibiliza para a inclusão. O Data Lake adota a telemetria e a normaliza para um armazenamento eficiente

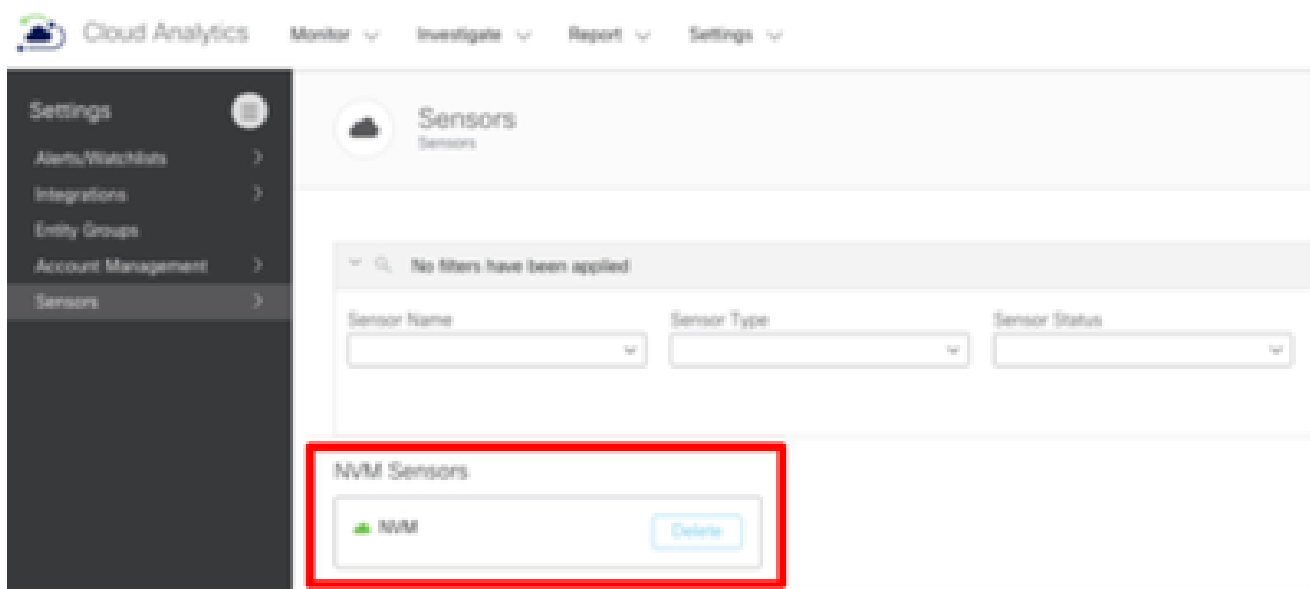
- A análise XDR processa registros NVM em intervalos regulares (10 minutos) para gerar detecções - Observações e alertas
- As detecções rápidas ajudam a adicionar rapidamente observações e alertas simples usando configurações
- O XDR Analytics correlaciona alertas em cadeias de ataque (antigas cadeias de alerta)
- O usuário pode publicar cadeias de alerta e ataque no XDR.

Status do sensor NVM

- Verificando se o sensor NVM foi criado:- No painel de análise XDR, navegue até configurações > Sensores



- Confirme se o sensor NVM está disponível na lista de sensores



aviso: O Portal de Análise XDR deve ter no máximo um único Locatário/Organização XDR associado a ele.

ID da Org. NVM

- Confirme se os clientes NVM têm a mesma exibição de ID da organização no ponto de extremidade da API:

<https://XDR Analytics PORTAL URL/api/v3/integrations/securex/orgs/>

```
pretty print()
{"meta":{"limit":1000,"next":null,"offset":0,"previous":null,"total_count":1},"objects":[{"org_id":"XXXXXXXXXXXXXXXXXXXXXXXXXXXX","org_name":"Cisco"}]}
```

Status de provisionamento do NVM Data Lake

- Os pontos de extremidade da API para garantir que o lago de dados seja integrado corretamente, a associação pode ser confirmada usando esse ponto de extremidade da API: https://XDR Analytics Portal URL/api/v3/integrations/securex/orgs/onboard_datalake/

```
Pretty print()
"Datalake provisioned successfully"
```

- Todos os usuários com acesso concedido por meio do portal podem acessar esses endpoints (administradores do portal, TAC, Engenharia)

Depuração

- Depurando códigos de resposta:

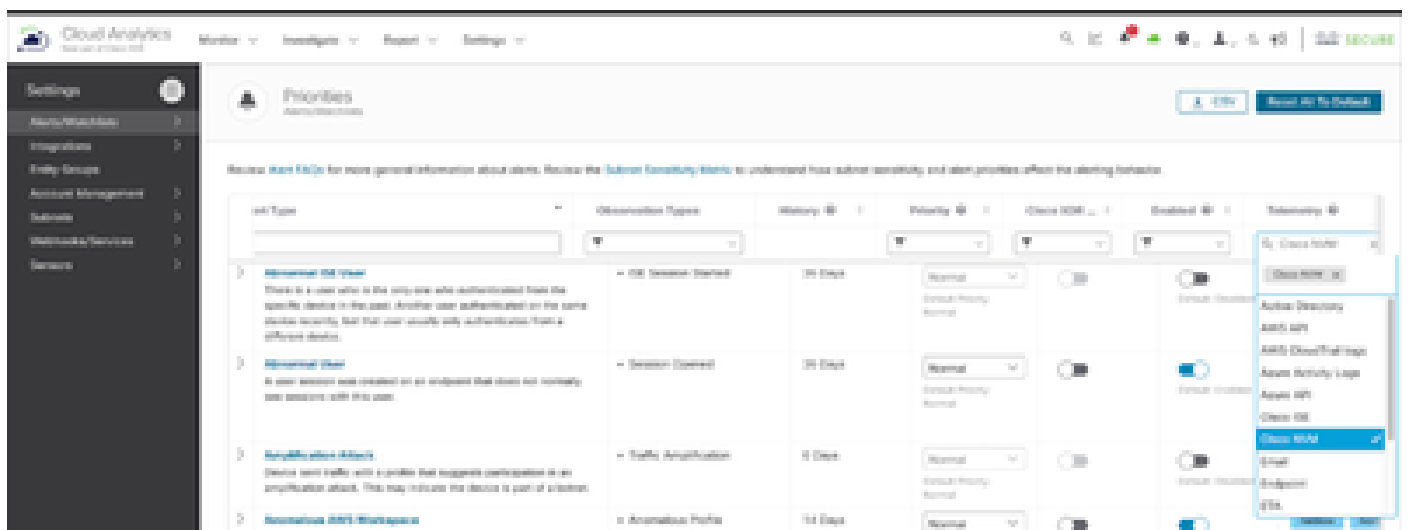
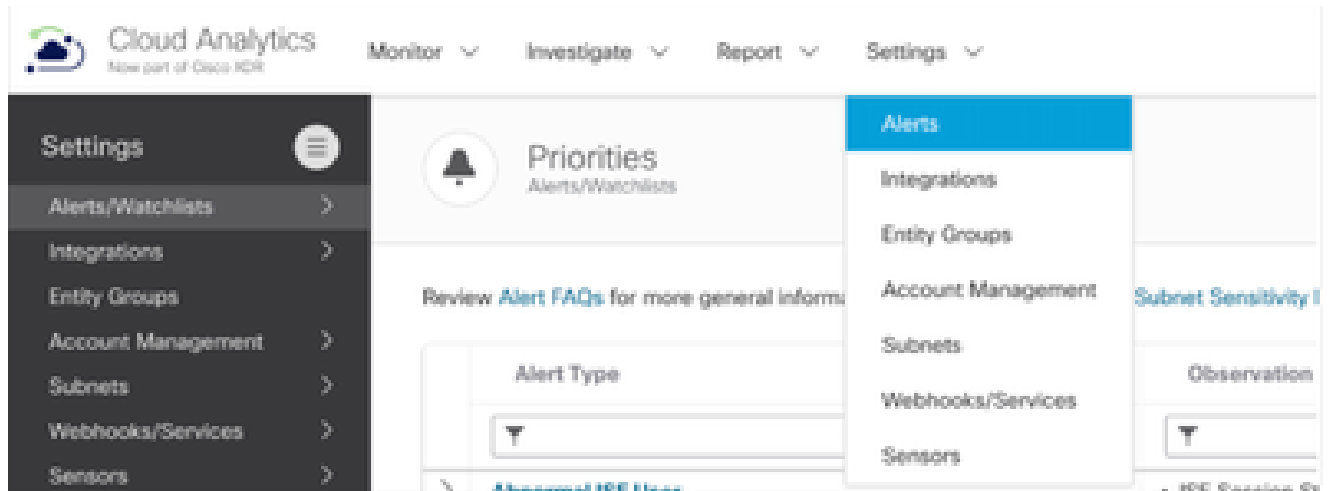
Código de Resposta	Ação exigida
DataLake provisionado com êxito	Validar fluxos NVM via Visualizador de Eventos
Não é possível provisionar lago de dados, nenhuma organização XDR detectada	Use a integração de um clique XDR para conectar análises XDR e XDR
Não é possível provisionar datalake, várias organizações XDR detectadas	Entre em contato com o TAC para obter assistência

- Se qualquer uma dessas etapas falhar, execute o Secure Client Diagnostics And Reporting Tool (DART) na interface do Secure Client para diagnosticar o problema (sempre solicite que o DART seja executado como administrador)
[Coletar pacote DART para cliente seguro](#)

Observações e alertas

Alertas de NVM

- Faça login no portal de análise XDR
- Configurações > Alertas Telemetria > Cisco NVM
- Telemetria > Cisco NVM



Configurações de alerta NVM

Priorities						Clear All	Reset All
Review Alert FAQs for more general information about alerts. Review the Subnet Sensitivity Matrix to understand how subnet sensitivity and alert priorities affect the alerting behavior.							
Alert Type	History	Priority	Enabled	Published to Secured	Subnetting		
LDAP Connection from Suspicious Process This device was detected running a non-standard LDAP process. This might indicate an credential theft attempt.	0 Days	Normal	☒	☐	☐	Close Alert	
Malicious Process Detected A process running has a hash matching one in a list of known malicious process hashes	0 Days	Normal	☒	☐	☐	Close Alert	
Metasploit Executed Execution of the offensive tool Metasploit has been detected in endpoint via endpoint telemetry	0 Days	Normal	☒	☐	☐	Close Alert	
Port 8888 Connections from multiple sources Multiple devices transferred files to a host serving on a busy port. This might indicate an exfiltration attempt.	0 Days	Normal	☒	☐	☐	Close Alert	
Potential Persistence Attempt This device was detected applying known persistence mechanisms like establishing background processes used for network access or running applications from network shares	0 Days	Normal	☒	☐	☐	Close Alert	
Potential System Process Impersonation A process with a name that looks like a common process has been executed indicating process impersonation	0 Days	Normal	☒	☐	☐	Close Alert	
SMB/SMBv2 Connection to multiple destinations The host has transferred files into multiple destination hosts using SMB and connected to those hosts using RDP. This could indicate lateral movement.	1 Day	Normal	☒	☐	☐	Close Alert	
Suspicious Process Path A process was executed on an endpoint from a directory that shouldn't have executables	0 Days	Normal	☒	☐	☐	Close Alert	

Observações do NVM

- Atividade suspeita de endpoint
- Portal de análise XDR
- Monitor > Observações
- Observação selecionada
- Filtrar atividades suspeitas de endpoint

Cloud Analytics
Monitor
Investigate
Report
Settings

Observations

Highlights

Types

By Device

Selected Observation

Selected Observation

Observations

Persistent External Server observation

Observation Type*

Suspi

ISE Suspicious Activity

Suspicious Endpoint Activity

Suspicious Network Activity

Suspicious SMB Activity

Search

Filter by source name, sha1, new

Avisos de detecção de NVM

- O NVM captura apenas processos e dados de fluxo que têm uma conexão de rede associada
- Por padrão, o NVM é configurado para relatar dados de fluxo apenas no final do fluxo

Conclusão

Essas etapas ajudam você a navegar pela Análise XDR para ativar Observações e Alertas usando informações de NVM e solução de problemas do fluxo de trabalho.

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.