Bestanden herstellen die door Secure Endpoint zijn gekwantificeerd

Inhoud

Inleiding

Dit document beschrijft hoe u bestanden kunt herstellen die in quarantaine zijn geplaatst door de connector voor Secure Endpoint vanaf de console Secure Endpoint.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Secure Endpoint-console

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende softwareversies:

- Secure Endpoint console v5.4.2025030619

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

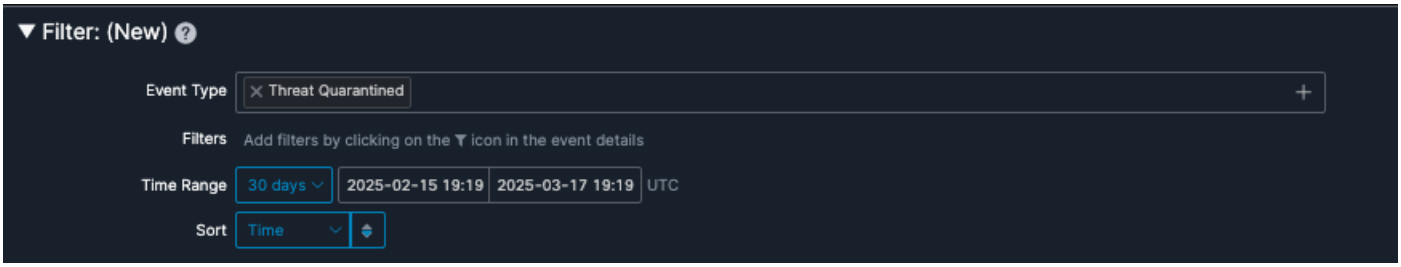
Probleem

Bestanden die door de Secure Endpoint (SE)-connector in quarantaine zijn geplaatst, kunnen worden hersteld voor bestandsanalyse, valse positieve inzendingen of herstel wanneer bekend is dat het bestand veilig is. Beheerders kunnen deze actie rechtstreeks uitvoeren vanuit de Secure Endpoint Console.

Oplossing

1. Ga naar de pagina Evenementen op uw SE-console.

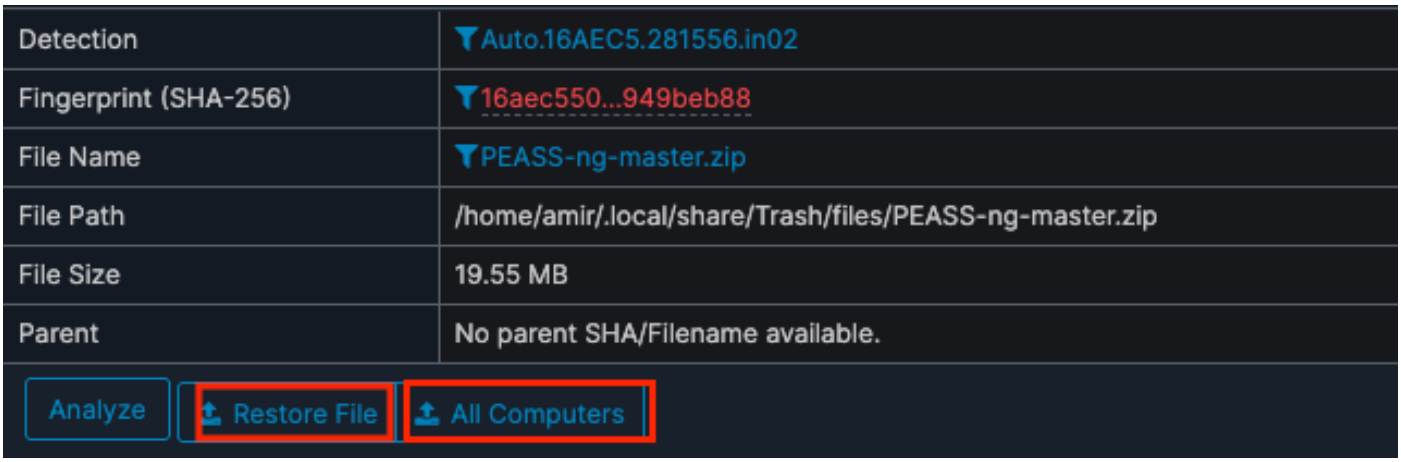
2. Filter de gebeurtenissen om alle succesvolle quarantaine te tonen door het filter Event Type = Threat Quarantined te selecteren.



Type bedreigingsgekwantificeerde gebeurtenis

3. Identificeer de detectiegebeurtenis die is gekoppeld aan het bestand dat u wilt herstellen.

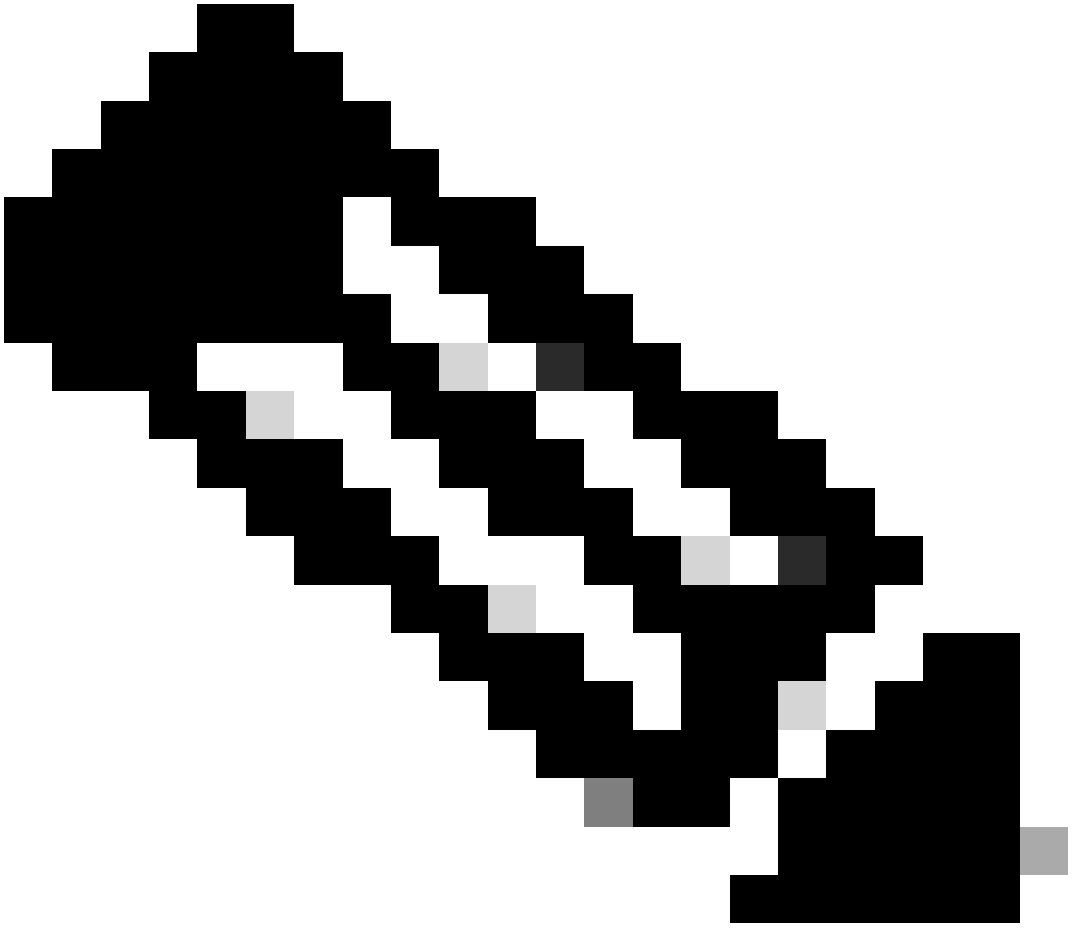
4. Vouw de gebeurtenisgegevens uit om toegang te krijgen tot de optie Terugzetbestand. Als u Terugzetbestand selecteert, wordt het bestand op het betreffende systeem hersteld. Door All Computers te selecteren wordt het bestand hersteld op alle machines waar het in quarantaine is geplaatst.



Bestandsopties terugzetten

5. Het hartslaginterval is de frequentie waarmee de connector naar huis belt om te zien of er bestanden zijn die door de beheerder moeten worden hersteld. Bestanden worden hersteld zodra de betrokken computers online zijn of wanneer het volgende hartslaginterval optreedt.

6. Als het bestand vertrouwd is, kunt u het toevoegen aan een lijst Toestaan om te voorkomen dat het opnieuw in quarantaine wordt geplaatst.



Opmerking: Bestanden blijven 30 dagen in quarantaine of wanneer de quarantainemap 100 MB bereikt en de oudste bestanden worden gewist. Quarantined-bestanden kunnen niet meer worden hersteld nadat ze zijn gewist.

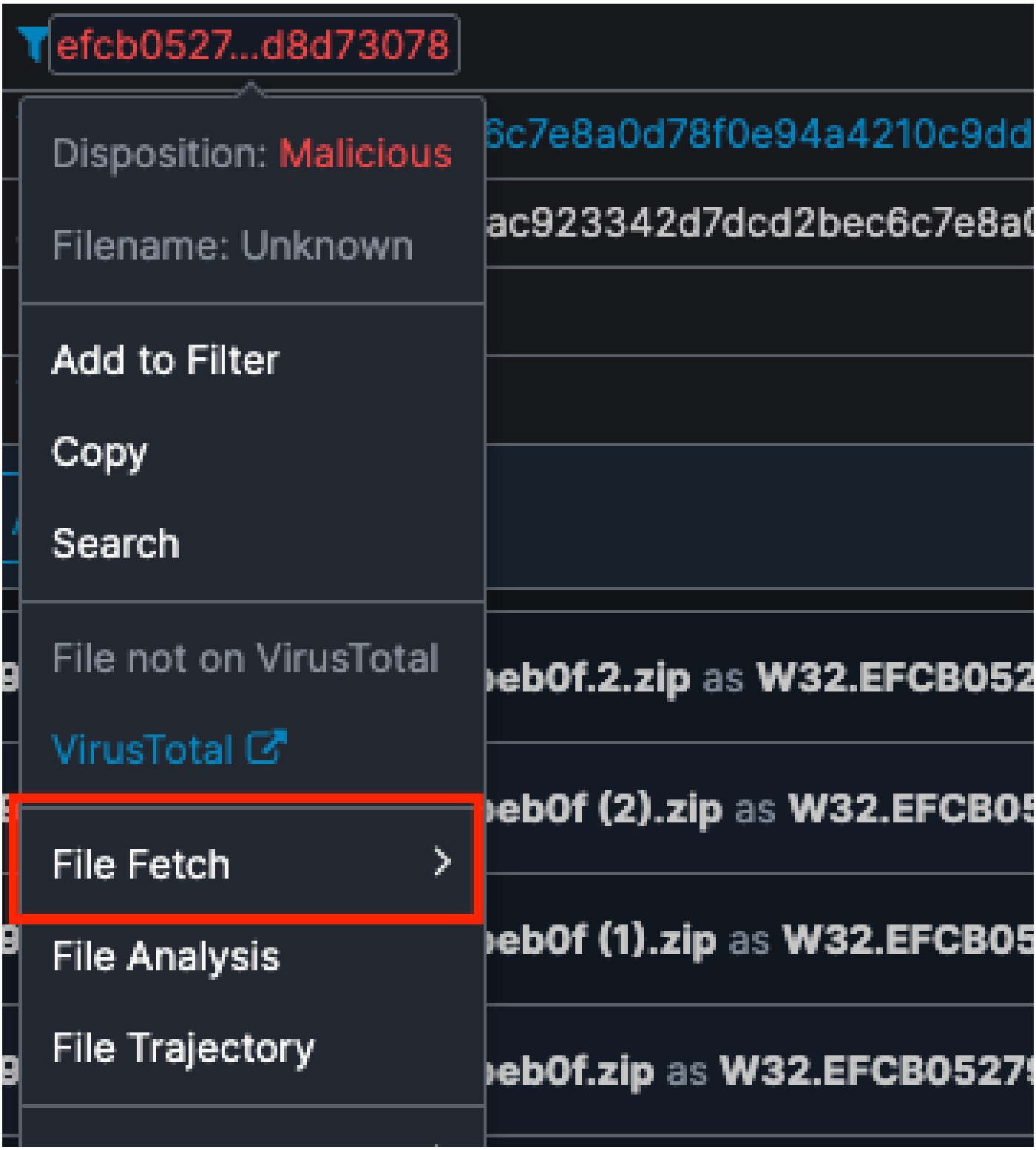
Als u eenvoudig een quarantaine bestand voor bedreigingsanalyse of valse positieve inzendingen moet downloaden zonder het te herstellen naar uw omgeving, kunt u de functie File Fetch gebruiken.

1. Ga naar de pagina Evenementen op uw SE-console.

2. Filter de gebeurtenissen om alle succesvolle quarantaine te tonen door het filter Event Type = Threat Quarantined te selecteren.

3. Identificeer de detectiegebeurtenis die is gekoppeld aan het bestand dat u wilt downloaden.

4. Klik op de SHA-256-waarde van het gequaranteerde bestand om de optie File Fetch te openen.



Bestanden ophalen

Dit geeft de status van de bestandsophaal, de optie om de ophaal te starten, en toegang om het bestand in de File Repository te bekijken.

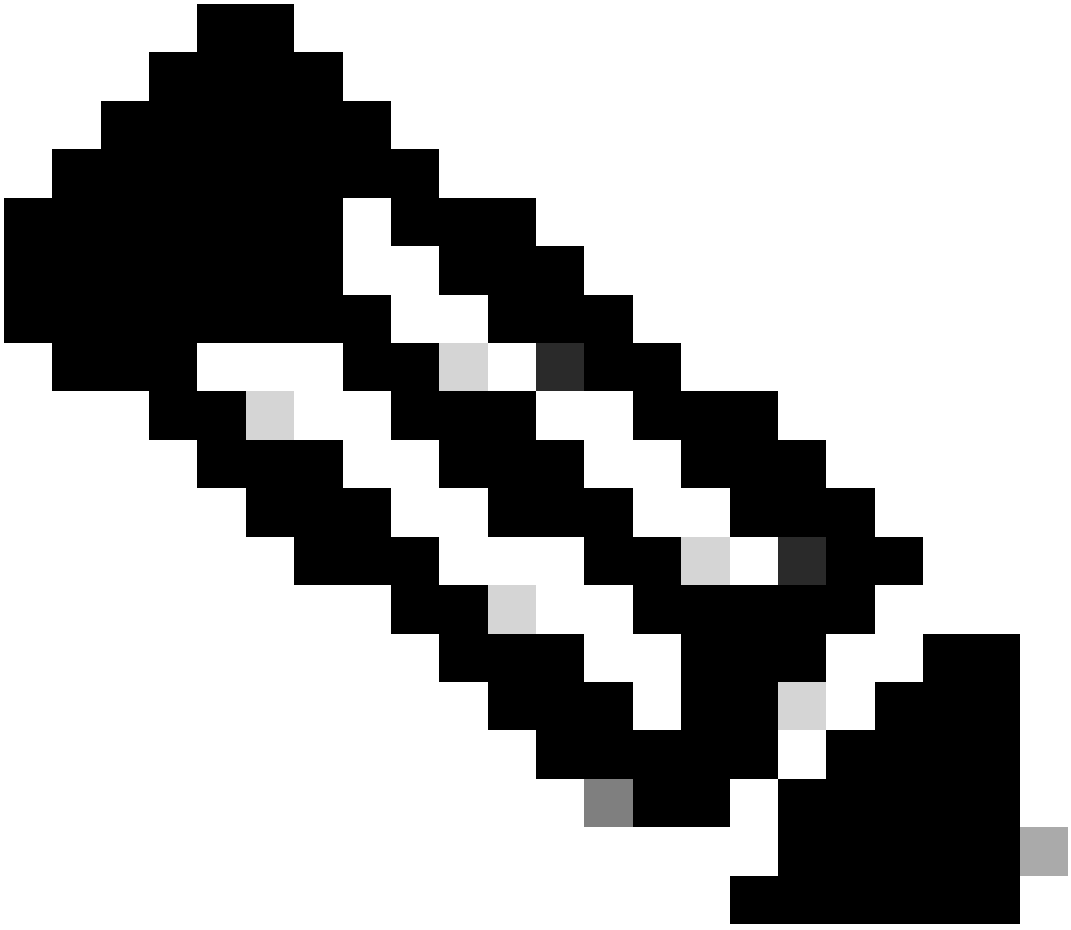
5. Klik op Fetch File, selecteer de computer waarvan u het bestand wilt ophalen en bevestig door op Fetch te klikken.

6. Een e-mailbericht wordt verzonden zodra het bestand is geüpload naar de File Repository.

7. Zodra het bestand beschikbaar is, kunt u het bestand en de optie om het te downloaden in Analysis> File Repository zien.

Downloadbestand

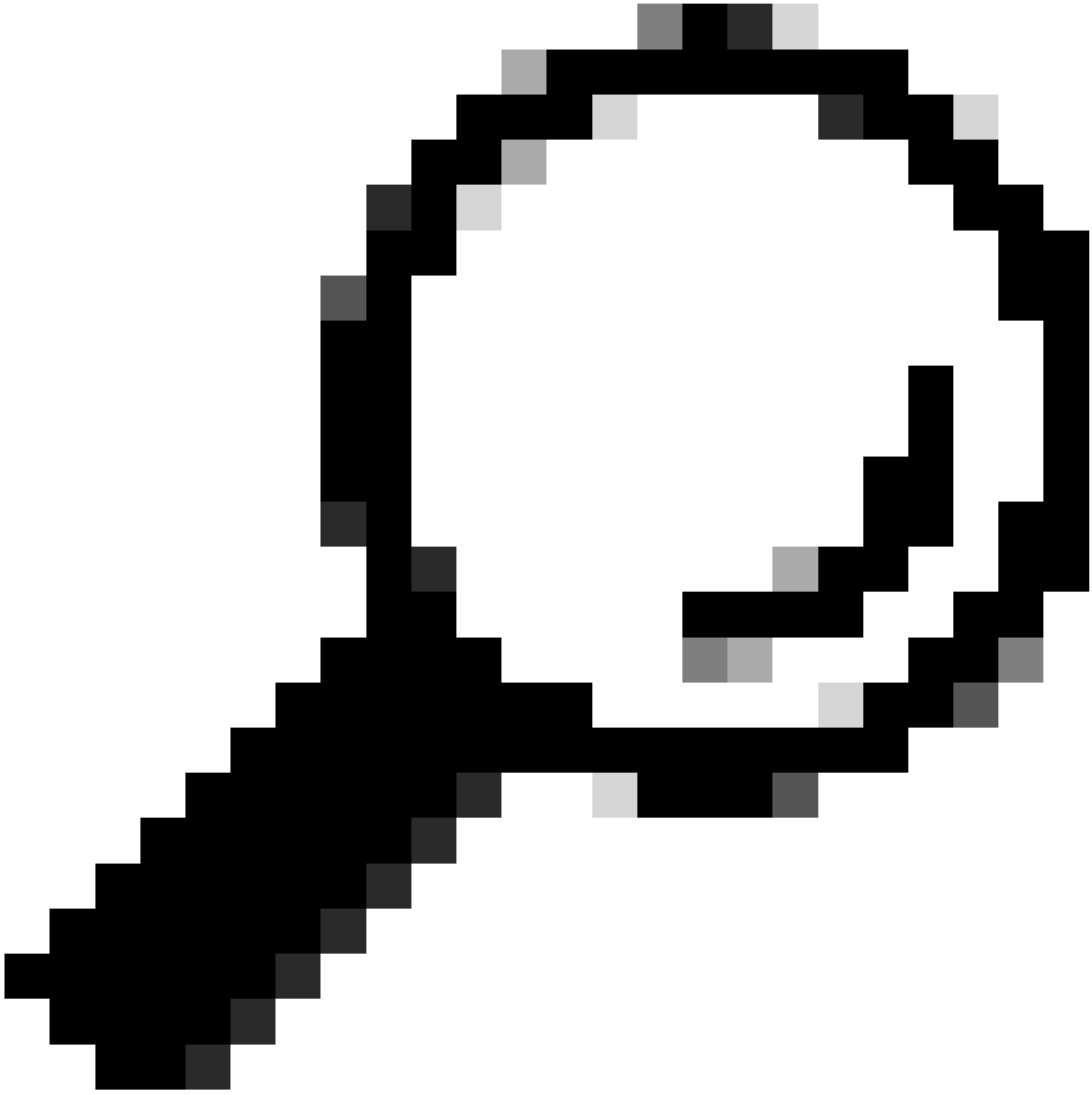
Alle bestanden die zijn gedownload vanuit de File Repository worden gezipt en met een wachtwoord beveiligd.



Opmerking: Om File Fetch goed te laten functioneren, moet het netwerkverkeer worden toegestaan om de juiste File Fetch-server op basis van uw cloudregio: Europa: rff.eu.amp.cisco.com Noord-Amerika: rff.amp.cisco.com APJC rff.apjc.amp.cisco.com. Zorg er bovendien voor dat Two-Factor Authentication (2FA) is ingeschakeld voor de Administrator-account, omdat het nodig is om met succes een verzoek voor het ophalen

---

van bestanden te starten.



Tip: U kunt gebeurtenissen filteren met behulp van Event Type = Quarantined Restore Failure en Event Type = File Fetch Mislukkingen identificeren en de corresponderende redenen voor respectievelijk Terugzetten en File Fetch-bewerkingen bekijken.

Als u het bestand niet kunt herstellen met de beschreven stappen, neemt u contact op met Cisco TAC en specificeert u het .qrt-bestand in de map C:\Program Files\Cisco\AMP\Quarantine.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.