Ripristino dei file messi in quarantena dall'endpoint protetto

Sommario

Introduzione

In questo documento viene descritto come ripristinare i file messi in quarantena dal connettore Secure Endpoint dalla console Secure Endpoint.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Secure Endpoint console

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software:

- Secure Endpoint Console v5.4.2025030619

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

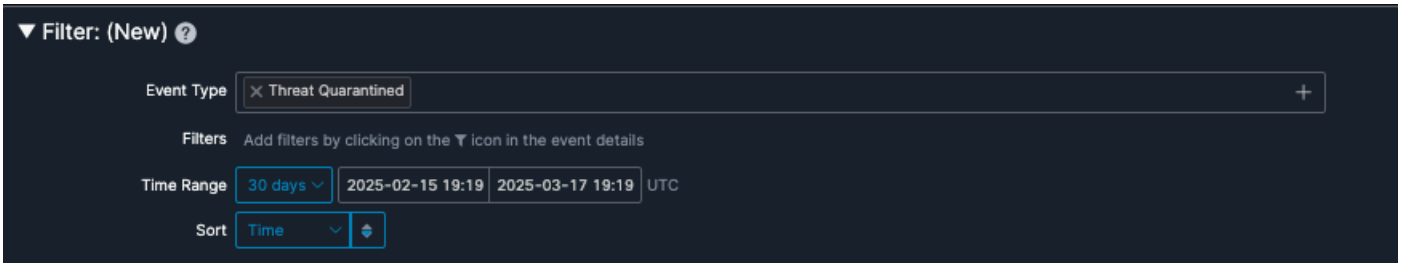
Problema

I file messi in quarantena dal connettore Secure Endpoint (SE) possono essere recuperati per l'analisi, l'invio di falsi positivi o il ripristino quando il file è sicuramente sicuro. Gli amministratori possono eseguire questa azione direttamente da Secure Endpoint Console.

Soluzione

1. Passare alla pagina Eventi sulla console SE.

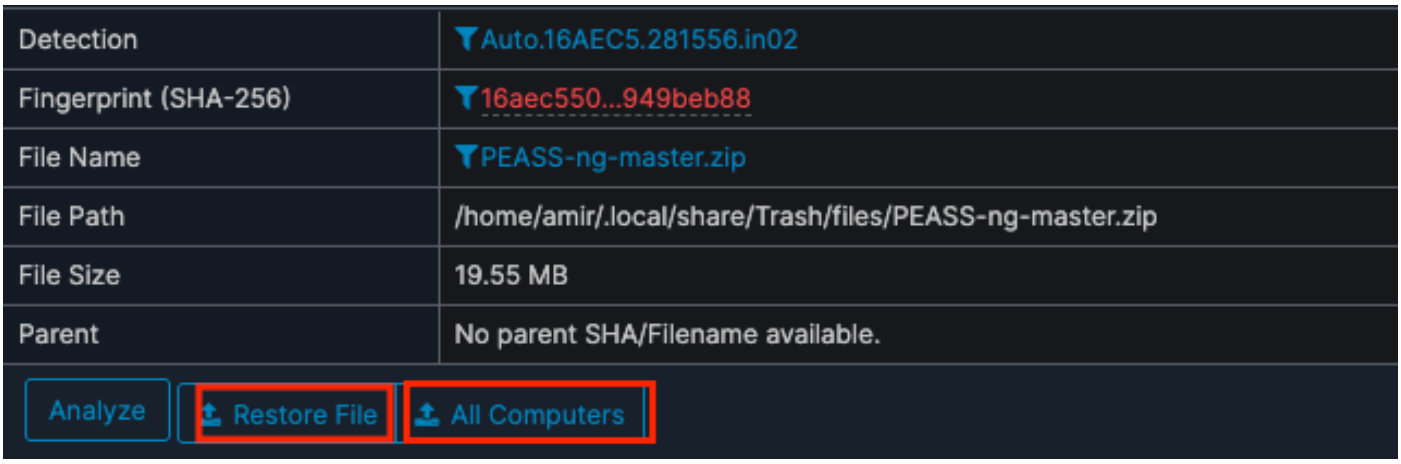
2. Filtrare gli eventi per visualizzare tutte le quarantene riuscite selezionando il filtro Tipo evento = Minaccia in quarantena.



Tipo di evento in quarantena minaccia

3. Identificare l'evento di rilevamento associato al file da ripristinare.

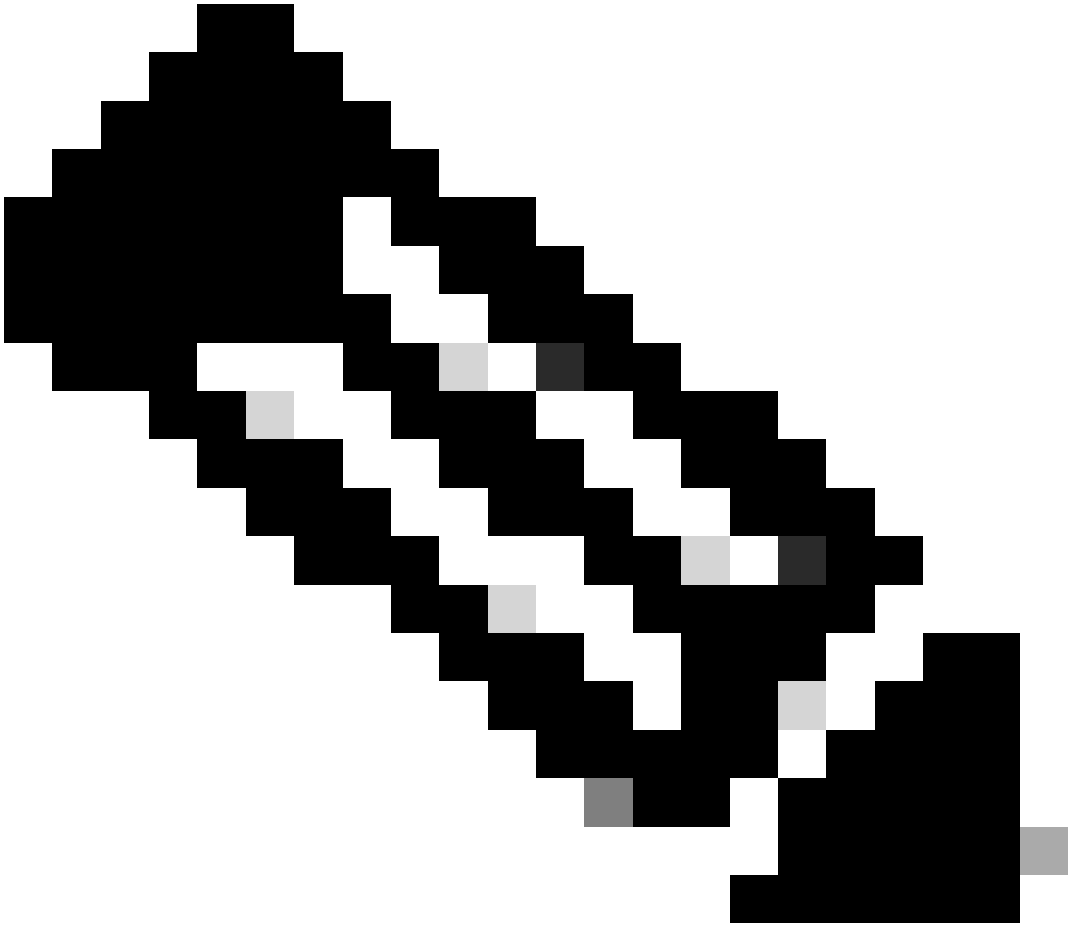
4. Espandere i dettagli dell'evento per accedere all'opzione Ripristina file. Selezionando Ripristina file il file verrà ripristinato nel computer interessato. Selezionando Tutti i computer il file viene ripristinato in tutti i computer in cui è stato messo in quarantena.



Opzioni per il ripristino dei file

5. L'intervallo di heartbeat è la frequenza con cui il connettore chiama la home per vedere se ci sono file da ripristinare da parte dell'amministratore. I file vengono ripristinati quando i computer interessati sono in linea o si verifica l'intervallo di heartbeat successivo.

6. Se il file è attendibile, aggiungerlo a un elenco degli oggetti autorizzati per evitare che venga nuovamente messo in quarantena.



Nota: I file rimangono in quarantena per 30 giorni o quando la cartella di quarantena raggiunge i 100 MB e i file meno recenti vengono eliminati. I file in quarantena non possono più essere ripristinati dopo essere stati eliminati.

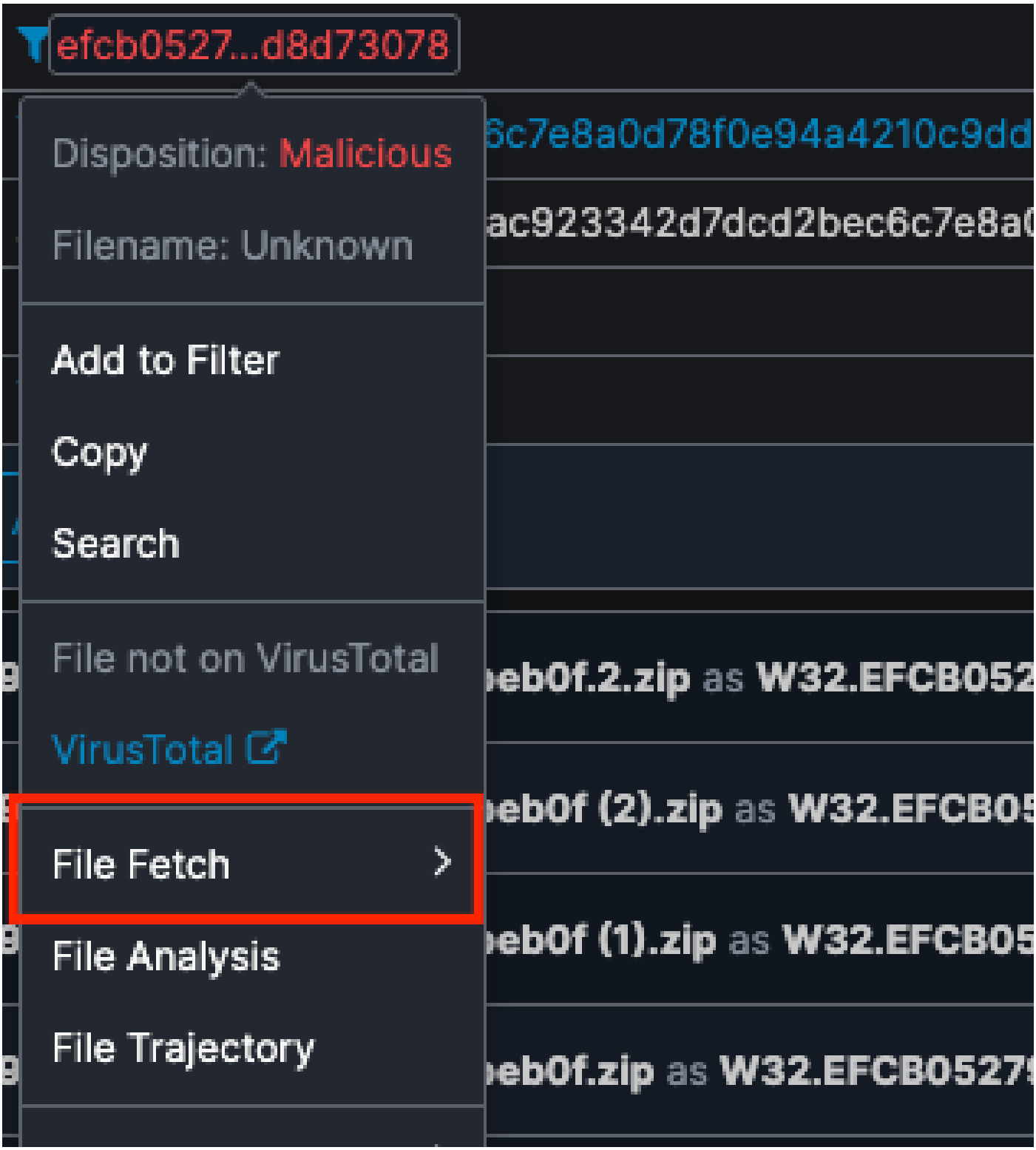
Se è sufficiente scaricare un file in quarantena per l'analisi delle minacce o per invii di falsi positivi senza ripristinarlo nell'ambiente in uso, è possibile utilizzare la funzionalità Recupero file.

1. Passare alla pagina Eventi sulla console SE.

2. Filtrare gli eventi per visualizzare tutte le quarantene riuscite selezionando il filtro Tipo evento = Minaccia in quarantena.

3. Identificare l'evento di rilevamento associato al file da scaricare.

4. Fare clic sul valore SHA-256 del file in quarantena per visualizzare l'opzione File Fetch.



Recupero file

Fornisce lo stato del recupero del file, l'opzione per avviare il recupero e l'accesso per visualizzare il file nel repository dei file.

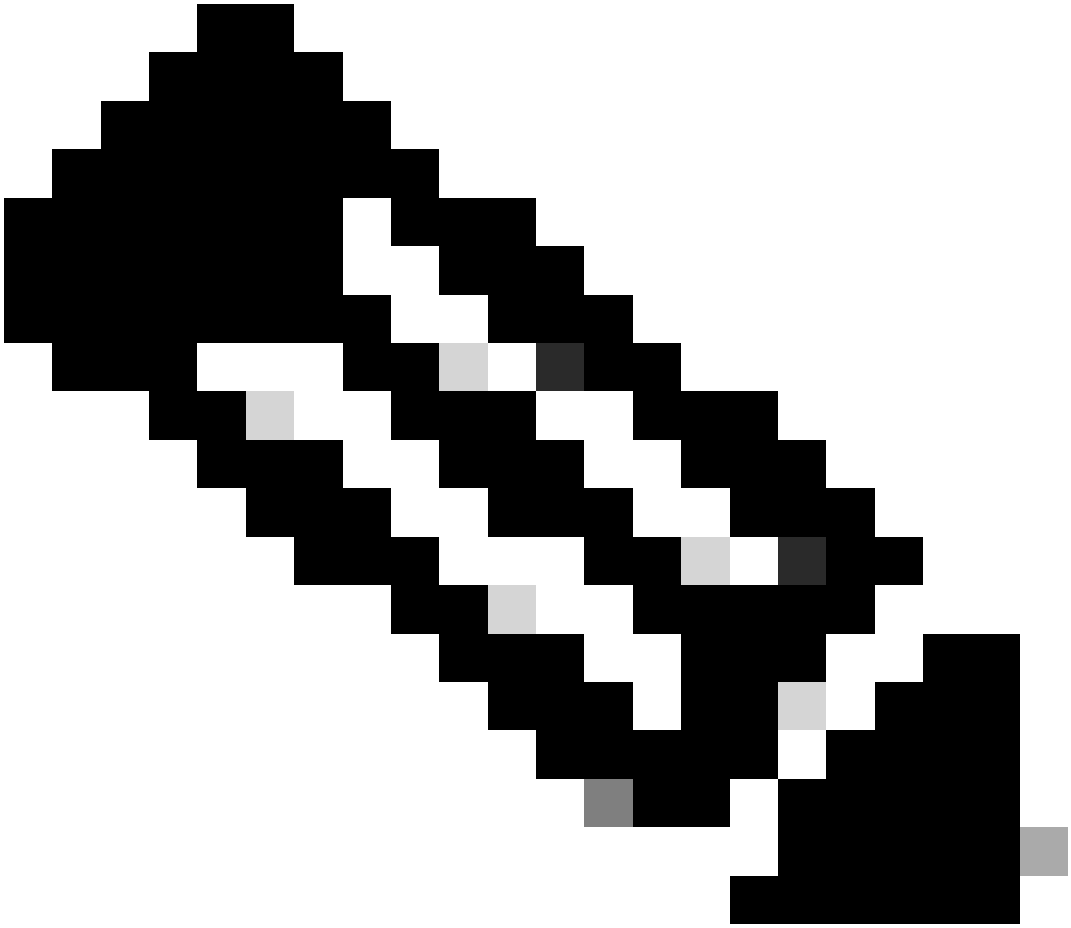
5. Fare clic su Recupera file, selezionare il computer da cui si desidera recuperare il file e confermare facendo clic su Recupera.

6. Una volta caricato il file nel repository, viene inviata una notifica e-mail.

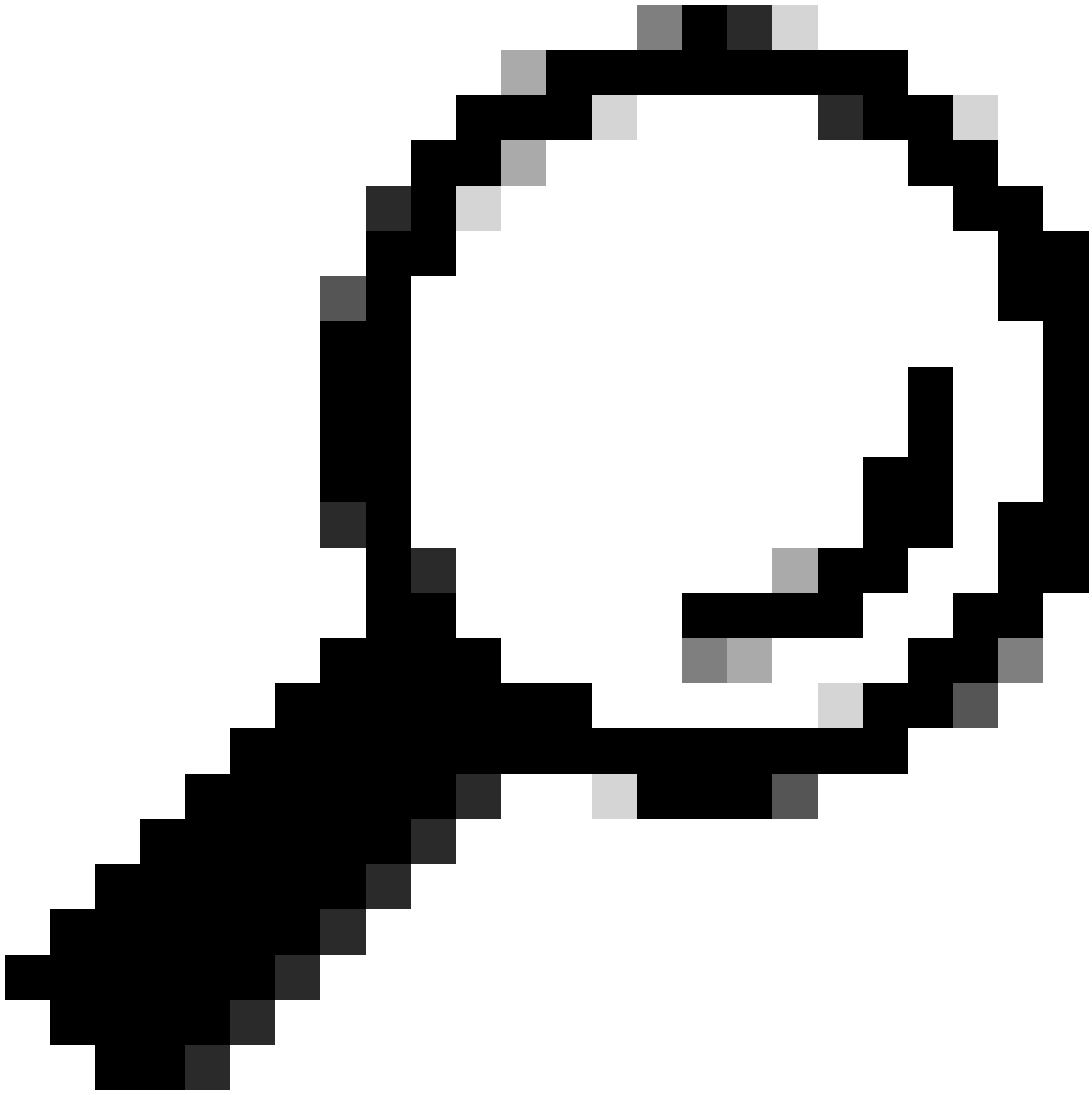
7. Una volta che il file è disponibile, è possibile visualizzarlo e l'opzione per scaricarlo in Analysis> File Repository.

Scarica il file

Tutti i file scaricati dal repository dei file vengono compressi e protetti da password.



Nota: Per il corretto funzionamento del recupero file, è necessario consentire il traffico di rete al server di recupero file appropriato in base all'area del cloud: Europa: rff.eu.amp.cisco.com Nord America: rff.amp.cisco.com APJC: rff.apjc.amp.cisco.com. Verificare inoltre che l'autenticazione a due fattori (2FA) sia abilitata per l'account Administrator, in quanto è necessaria per avviare correttamente una richiesta di recupero file.



Suggerimento: È possibile filtrare gli eventi utilizzando Tipo di evento = Ripristino in quarantena non riuscito e Tipo di evento = Recupero file non riuscito per identificare gli errori e rivedere i motivi corrispondenti per le operazioni di ripristino e recupero file, rispettivamente.

Se non è possibile ripristinare il file seguendo la procedura descritta, contattare Cisco TAC e specificare il file .qrt nella directory C:\Program Files\Cisco\AMP\Quarantine.

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).