Récupérer les fichiers mis en quarantaine par Secure Endpoint

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Problème

Solution

Introduction

Ce document décrit comment restaurer des fichiers qui ont été mis en quarantaine par le connecteur Secure Endpoint à partir de la console Secure Endpoint.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Console Cisco Secure Endpoint

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- Console de terminal sécurisé v5.4.2025030619

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

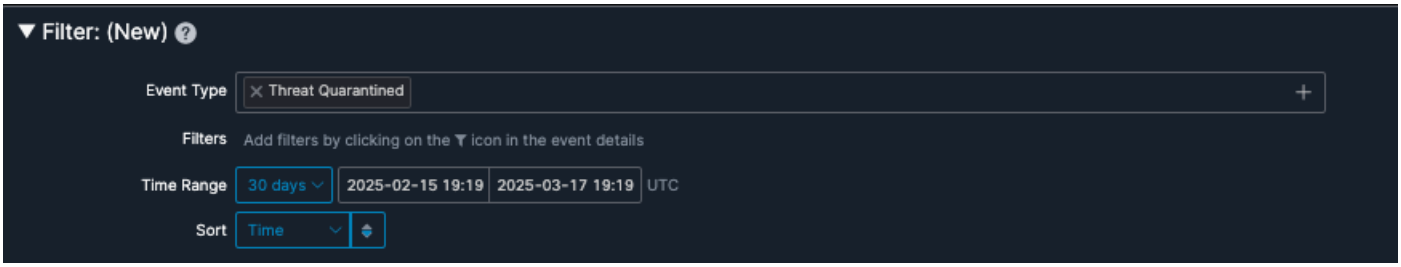
Problème

Les fichiers mis en quarantaine par le connecteur Secure Endpoint (SE) peuvent être récupérés à des fins d'analyse, d'envoi de faux positifs ou de restauration lorsque leur sécurité est reconnue. Les administrateurs peuvent effectuer cette action directement à partir de la console Secure Endpoint.

Solution

1. Accédez à la page Événements sur votre console SE.

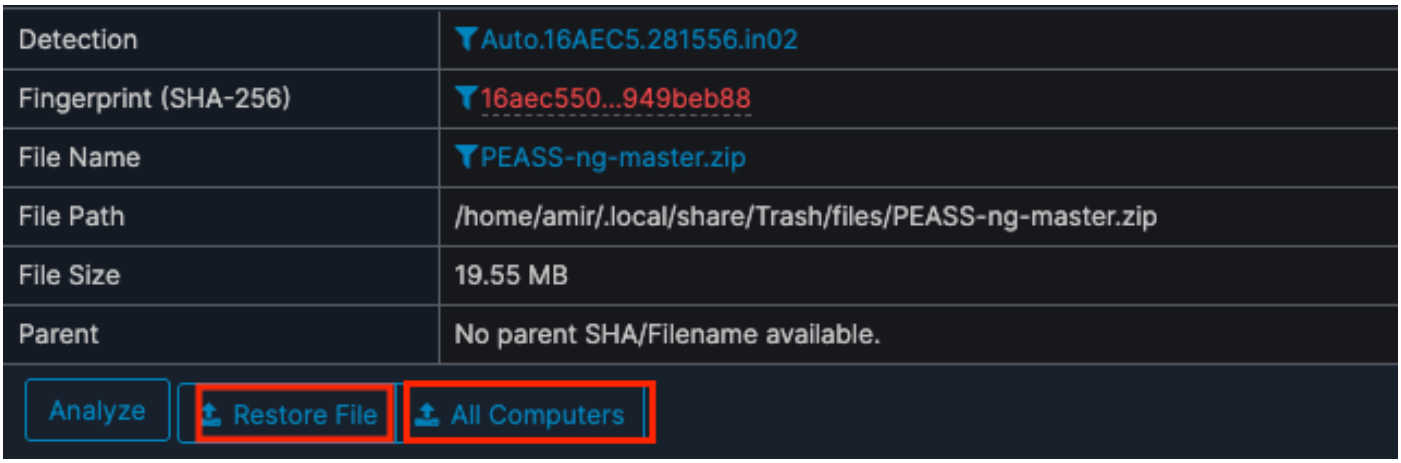
2. Filtrez les événements pour afficher toutes les quarantaines réussies en sélectionnant le filtre Type d'événement = Menace mise en quarantaine.



Type d'événement de menace en quarantaine

3. Identifiez l'événement de détection associé au fichier que vous devez restaurer.

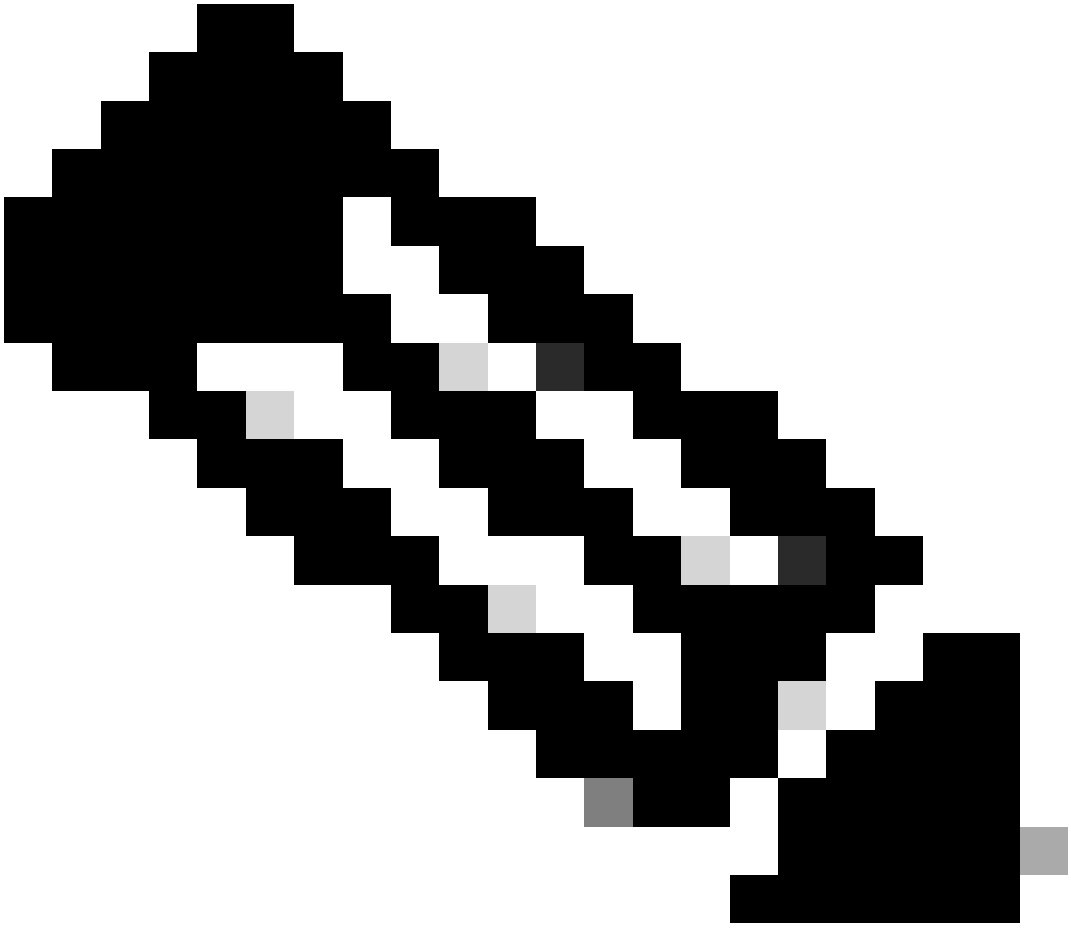
4. Développez les détails de l'événement pour accéder à l'option Restaurer le fichier. Sélectionner Restaurer le fichier restaure le fichier sur l'ordinateur affecté. La sélection de Tous les ordinateurs restaure le fichier sur toutes les machines sur lesquelles il a été mis en quarantaine.



Options de restauration des fichiers

5. L'intervalle de pulsation est la fréquence à laquelle le connecteur appelle son domicile pour voir s'il y a des fichiers à restaurer par l'administrateur. Les fichiers sont restaurés une fois que les ordinateurs concernés sont en ligne ou que l'intervalle de pulsation suivant se produit.

6. Si le fichier est approuvé, ajoutez-le à une liste verte pour l'empêcher d'être à nouveau mis en quarantaine.



Remarque : Les fichiers restent en quarantaine pendant 30 jours ou lorsque le dossier de quarantaine atteint 100 Mo et que les fichiers les plus anciens sont purgés. Les fichiers mis en quarantaine ne peuvent plus être restaurés après leur purge.

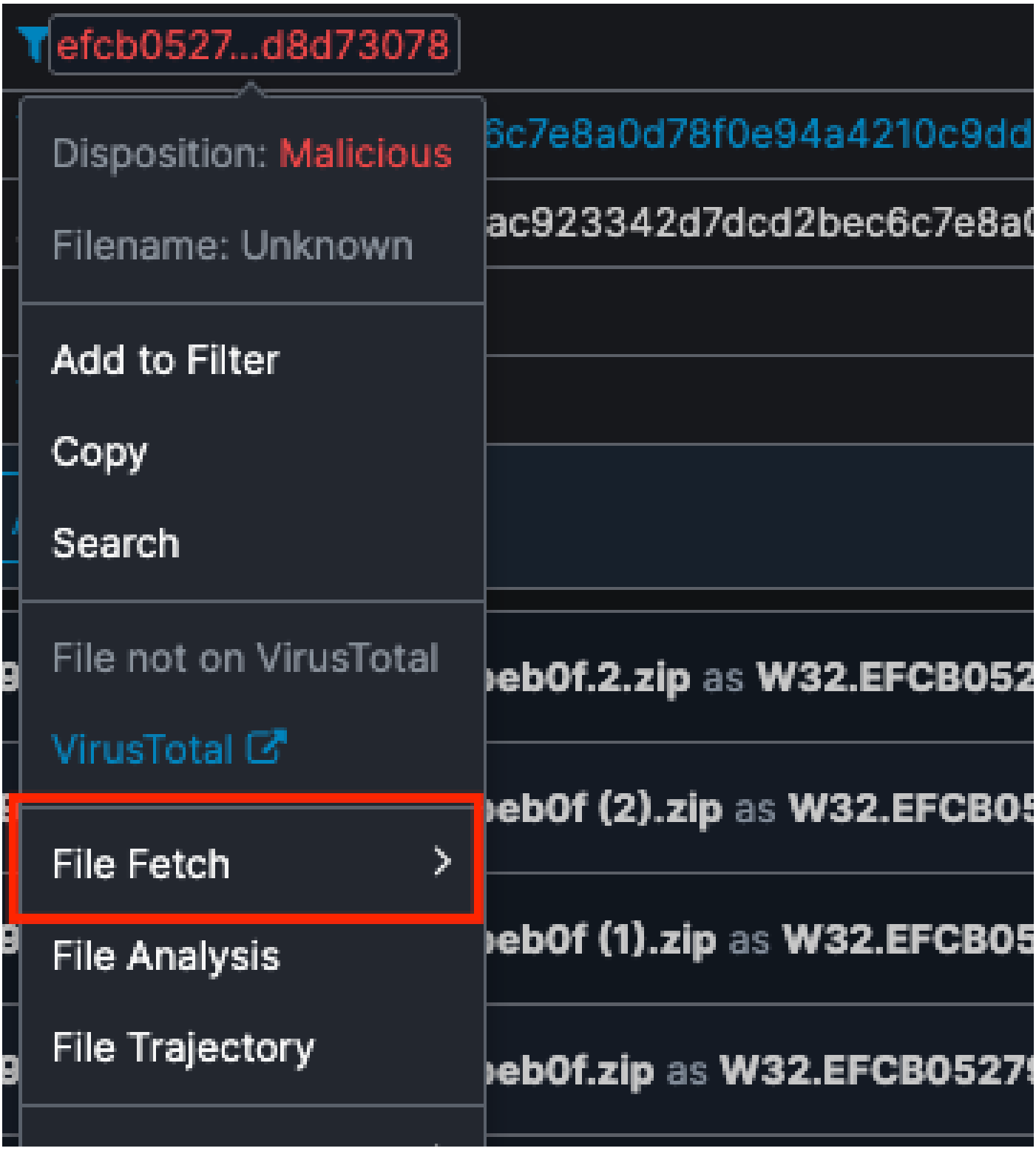
Si vous devez simplement télécharger un fichier mis en quarantaine pour l'analyse des menaces ou les envois de faux positifs sans le restaurer dans votre environnement, vous pouvez utiliser la fonctionnalité File Fetch. Étapes pour télécharger un fichier mis en quarantaine :

1. Accédez à la page Événements sur votre console SE.

2. Filtrez les événements pour afficher toutes les quarantaines réussies en sélectionnant le filtre Type d'événement = Menace mise en quarantaine.

3. Identifiez l'événement de détection associé au fichier que vous devez télécharger.

4. Cliquez sur la valeur SHA-256 du fichier mis en quarantaine pour afficher l'option File Fetch.



Récupération de fichier

Cela indique l'état de la récupération du fichier, l'option permettant de lancer la récupération et l'accès permettant de visualiser le fichier dans le référentiel de fichiers.

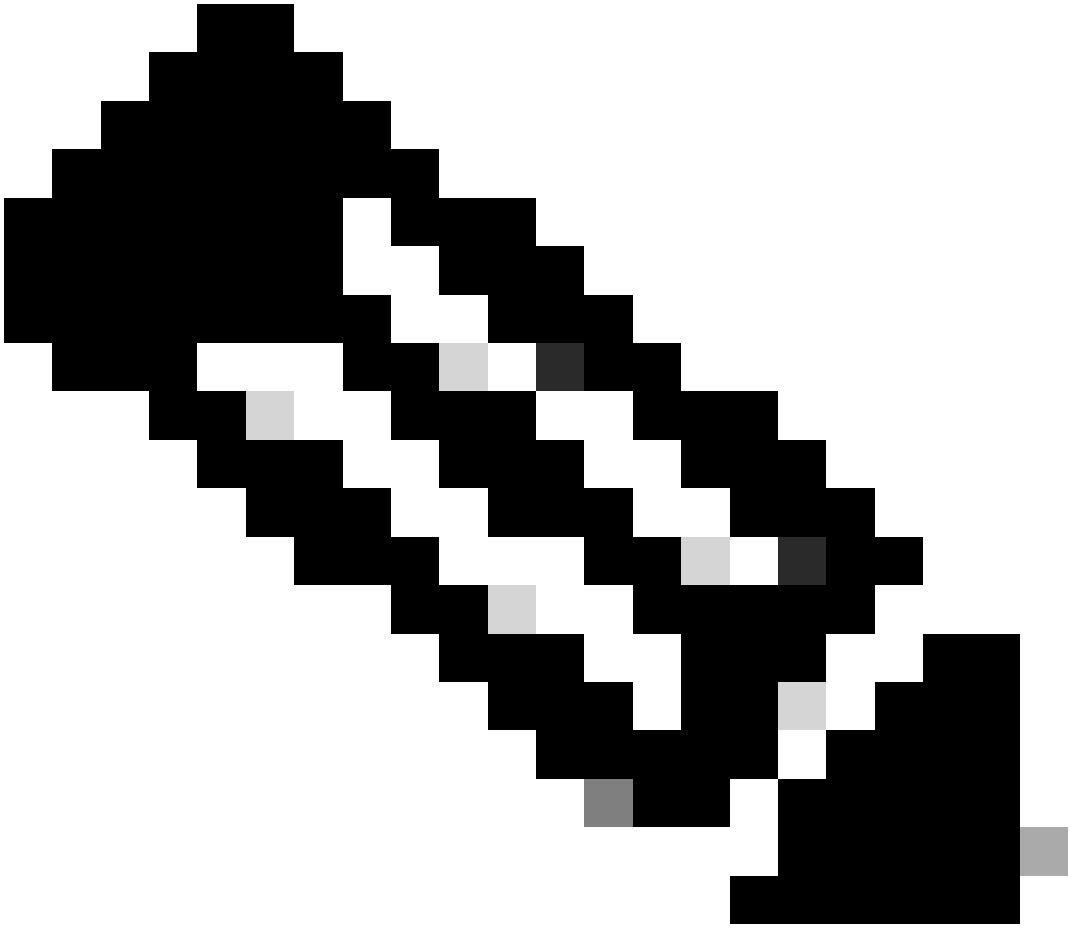
5. Cliquez sur Récupérer le fichier, sélectionnez l'ordinateur à partir duquel vous souhaitez récupérer le fichier et confirmez en cliquant sur Récupérer.

6. Une notification par e-mail est envoyée une fois le fichier téléchargé dans le référentiel de fichiers.

7. Une fois le fichier disponible, vous pouvez le voir et l'option de le télécharger dans Analysis> Référentiel de fichiers.

Télécharger le fichier

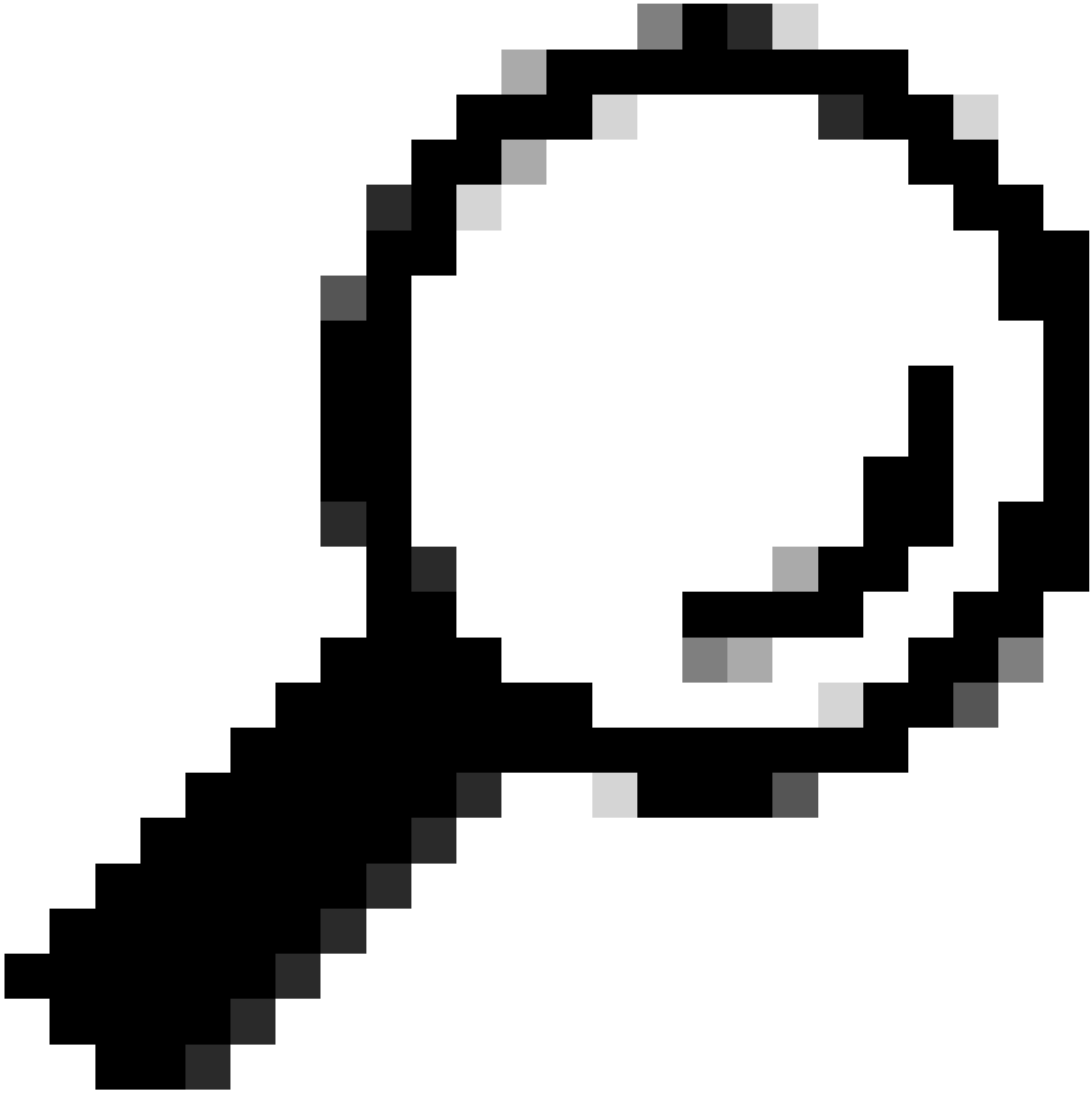
Tous les fichiers téléchargés à partir du référentiel de fichiers sont compressés et protégés par mot de passe.



Remarque : Pour que la fonction File Fetch fonctionne correctement, le trafic réseau doit être autorisé vers le serveur File Fetch approprié en fonction de votre région de cloud : Europe: rff.eu.amp.cisco.com Amérique du Nord : rff.amp.cisco.com APJC : rff.apjc.amp.cisco.com. Assurez-vous également que l'authentification à deux facteurs (2FA) est activée pour le compte Administrateur, car elle est nécessaire pour lancer une

---

demande de récupération de fichier.



Conseil : Vous pouvez filtrer les événements en utilisant Event Type = Quarantined Restore Failed et Event Type = File Fetch Failed pour identifier les échecs et examiner les raisons correspondantes pour les opérations de restauration et de récupération de fichiers, respectivement.

Si vous ne parvenez pas à restaurer le fichier à l'aide des étapes décrites ci-dessus, contactez le centre d'assistance technique Cisco et fournissez le fichier .qrt situé dans le répertoire C:\Program Files\Cisco\AMP\Quarantine.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.