

Configuration de l'intégration et du dépannage de SD-WAN Advanced Malware Protection (AMP)

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Présentation de la solution](#)

[Composants](#)

[Flux de fonctionnalités](#)

[Configuration de l'intégration SD-WAN AMP](#)

[Configurer la stratégie de sécurité à partir de vManage](#)

[Vérifier](#)

[Dépannage](#)

[Flux de dépannage général](#)

[Problèmes de diffusion de stratégie sur vManage](#)

[Intégration AMP sur routeur de périphérie Cisco](#)

[Vérifier l'intégrité du conteneur UTD](#)

Introduction

Ce document décrit comment configurer et dépanner l'intégration de Cisco SD-WAN Advanced Malware Protection (AMP) sur un routeur Cisco IOS® XE SD-WAN.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Advanced Malware Protection (AMP)
- Réseau étendu défini par logiciel Cisco (SD-WAN)

Composants utilisés

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.

Présentation de la solution

Composants

L'intégration AMP SD-WAN fait partie intégrante de la solution de sécurité de périphérie SD-WAN qui vise à offrir visibilité et protection aux utilisateurs d'une filiale contre les programmes malveillants.

Il se compose des composants suivants :

- Routeur de périphérie WAN au niveau d'une filiale. Il s'agit d'un routeur Cisco IOS® XE en mode contrôleur avec des fonctions de sécurité dans un conteneur UTD
- Cloud AMP. L'infrastructure cloud AMP répond aux requêtes de hachage de fichiers avec une disposition
- ThreatGrid. Infrastructure cloud capable de tester un fichier à la recherche de programmes malveillants potentiels dans un environnement sandbox

Ces composants fonctionnent ensemble pour fournir ces fonctionnalités clés pour AMP :

- Évaluation de la réputation des fichiers

Processus de hachage SHA256 utilisé pour comparer le fichier au serveur cloud AMP (Advanced Malware Protection) et accéder à ses informations sur les menaces. La réponse peut être Propre, Inconnu ou Malveillant. Si la réponse est Inconnu et si l'analyse de fichier est configurée, le fichier est automatiquement soumis pour analyse ultérieure.

- Analyse de fichiers

Un fichier inconnu est envoyé au cloud ThreatGrid (TG) pour détonation dans un environnement de sandbox. Pendant la détonation, le bac à sable capture les artefacts et observe les comportements du fichier, puis attribue au fichier une note globale. Sur la base des observations et du score, Threat Grid peut modifier la réponse aux menaces en choisissant Nettoyer ou Malveillant. Les résultats de ThreatGrid sont signalés au cloud AMP afin que tous les utilisateurs AMP soient protégés contre les programmes malveillants nouvellement découverts.

- Contrôle A Posteriori

Il conserve des informations sur les fichiers même après leur téléchargement, nous pouvons signaler les fichiers qui ont été déterminés comme malveillants après leur téléchargement. La disposition des fichiers peut changer en fonction des nouvelles informations sur les menaces collectées par le cloud AMP. Ce reclassement génère des notifications rétrospectives automatiques.

Actuellement, SD-WAN avec intégration AMP prend en charge l'inspection des fichiers pour les protocoles :

- HTTP
- SMTP

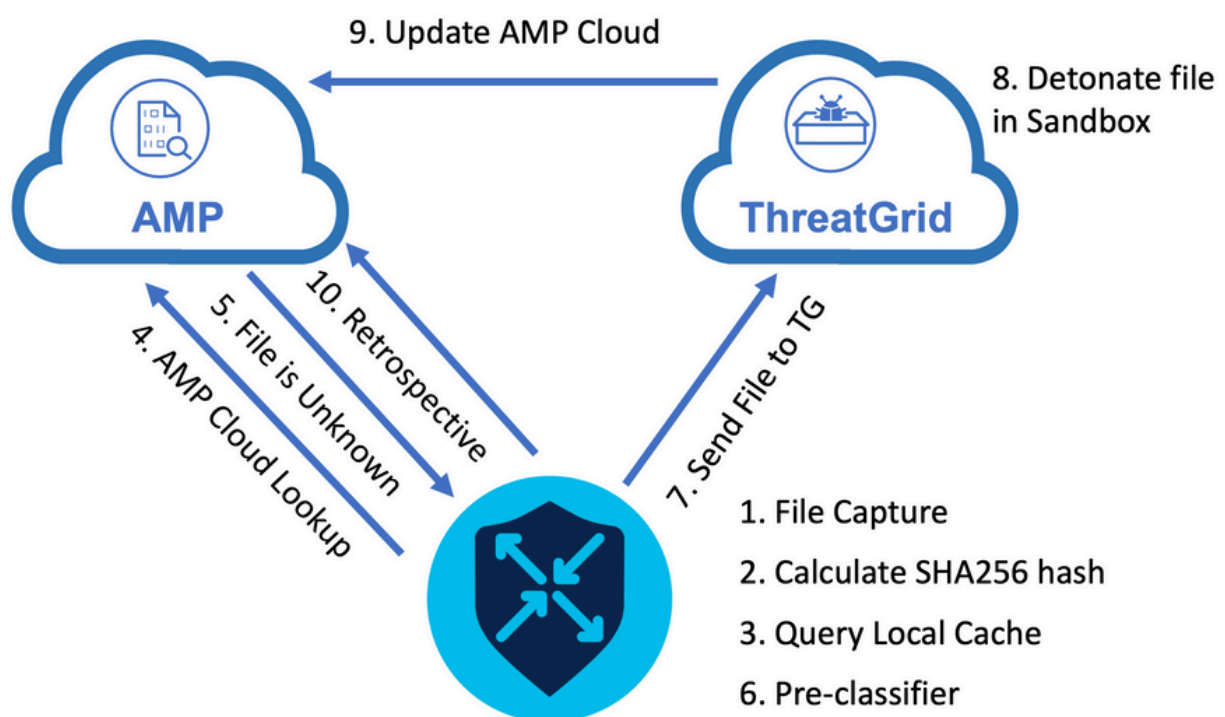
- IMAP
- POP3
- FTP
- PME

Remarque : le transfert de fichiers sur HTTPS est uniquement pris en charge avec le [proxy SSL/TLS](#).

Remarque : l'analyse de fichier ne peut être effectuée que sur un fichier complet, et non sur un fichier divisé en contenu partiel. Par exemple, quand un client HTTP demande un contenu partiel avec l'en-tête Range et récupère le contenu partiel HTTP/1.1 206. Dans ce cas, comme le hachage du fichier partiel est sensiblement différent du fichier complet, Snort ignore l'inspection du fichier pour le contenu partiel.

Flux de fonctionnalités

L'image représente le flux de haut niveau pour l'intégration SD-WAN AMP lorsqu'un fichier doit être soumis à ThreatGrid pour analyse.





Pour le flux illustré :

1. Le transfert de fichiers pour les protocoles pris en charge par AMP est capturé par le conteneur UTD.
2. Le hachage SHA256 du fichier est calculé.
3. Le hachage SHA256 calculé est interrogé sur le système de cache local dans UTD pour voir si la disposition est déjà connue et si la durée de vie du cache n'a pas expiré.

4. S'il n'y a aucune correspondance avec le cache local, le hachage SHA256 est recherché dans le cloud AMP pour une action de disposition et de retour.
5. Si la disposition est UNKNOWN et que l'action de réponse est ACTION_SEND, le fichier est exécuté via le système de préclassification dans UTD.
6. Le pré-classifieur détermine le type de fichier et vérifie également si le fichier contient du contenu actif.
7. Si les deux conditions sont remplies, le fichier est envoyé à ThreatGrid.
8. ThreatGrid fait exploser le fichier dans un sandbox et lui attribue un score de menace.
9. ThreatGrid met à jour le cloud AMP en fonction de l'évaluation des menaces.
10. Le périphérique de périphérie interroge le cloud AMP à la recherche de données rétrospectives en fonction de l'intervalle de pulsation de 30 minutes.

Configuration de l'intégration SD-WAN AMP

 Remarque : une image virtuelle de sécurité doit être téléchargée vers vManage avant la configuration de la fonctionnalité AMP. Pour plus d'informations, accédez à [Image virtuelle de sécurité](#) .

 Remarque : consultez ce document pour connaître les exigences réseau pour que la connectivité AMP/ThreatGrid fonctionne correctement : [Adresses IP/Noms d'hôte requis par AMP/TG](#)

Configurer la stratégie de sécurité à partir de vManage

Pour activer AMP, accédez à Configuration -> Security -> Add Security Policy. Sélectionnez Accès Internet direct et Continuer comme indiqué dans l'image.

Add Security Policy ✕

Choose a scenario that fits your use-case. Click Proceed to continue building your desired policies.

- Compliance**
Application Firewall | Intrusion Prevention | TLS/SSL Decryption
- Guest Access**
Application Firewall | URL Filtering | TLS/SSL Decryption
- Direct Cloud Access**
Application Firewall | Intrusion Prevention | Advanced Malware Protection | DNS Security | TLS/SSL Decryption
- Direct Internet Access**
Application Firewall | Intrusion Prevention | URL Filtering | **Advanced Malware Protection** | DNS Security | TLS/SSL Decryption
- Custom**
Build your ala carte policy by combining a variety of security policy blocks

Proceed Cancel

Configurez les fonctions de sécurité comme vous le souhaitez jusqu'à ce qu'il accède à la fonction Advanced Malware Protection. Ajoutez une nouvelle stratégie de protection avancée contre les programmes malveillants.

Cisco vManage

CONFIGURATION Security > Add Security Policy

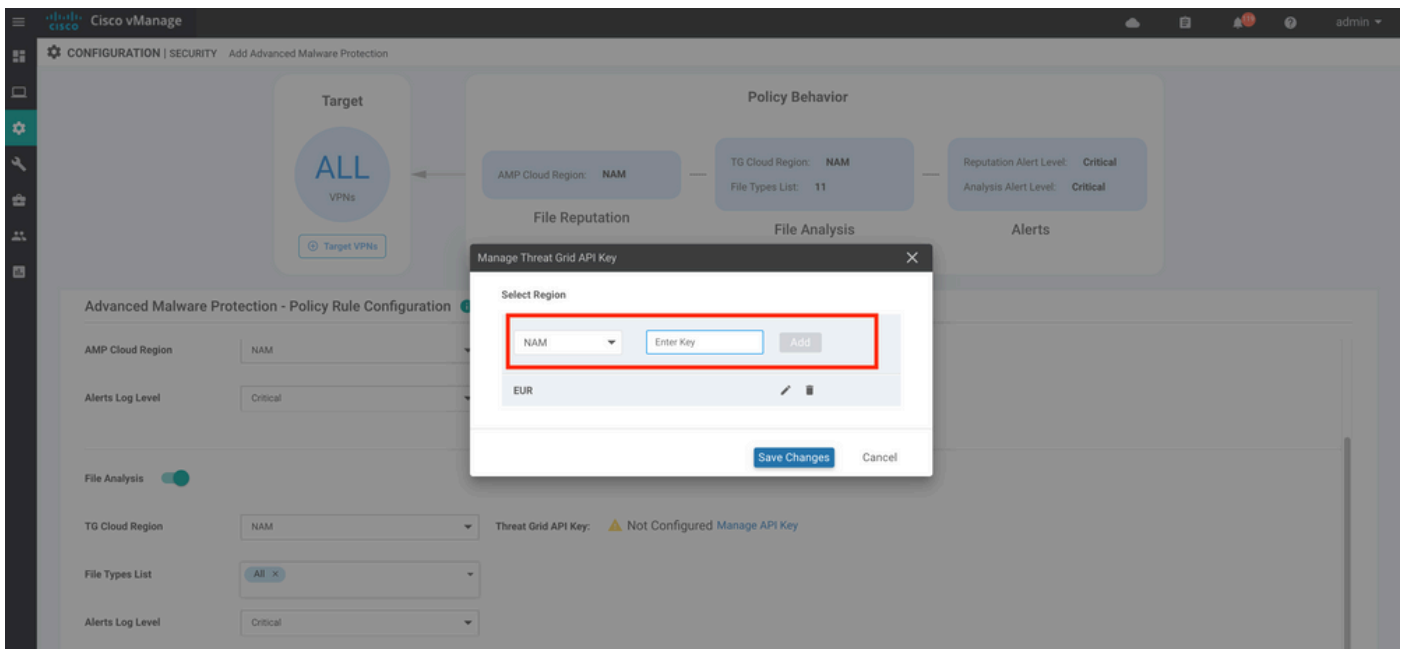
Firewall | Intrusion Prevention | URL Filtering | **Advanced Malware Protection** | DNS Security | TLS/SSL Decryption | Policy Summary

Activate File Reputation and File Analysis to escalate malware protection.

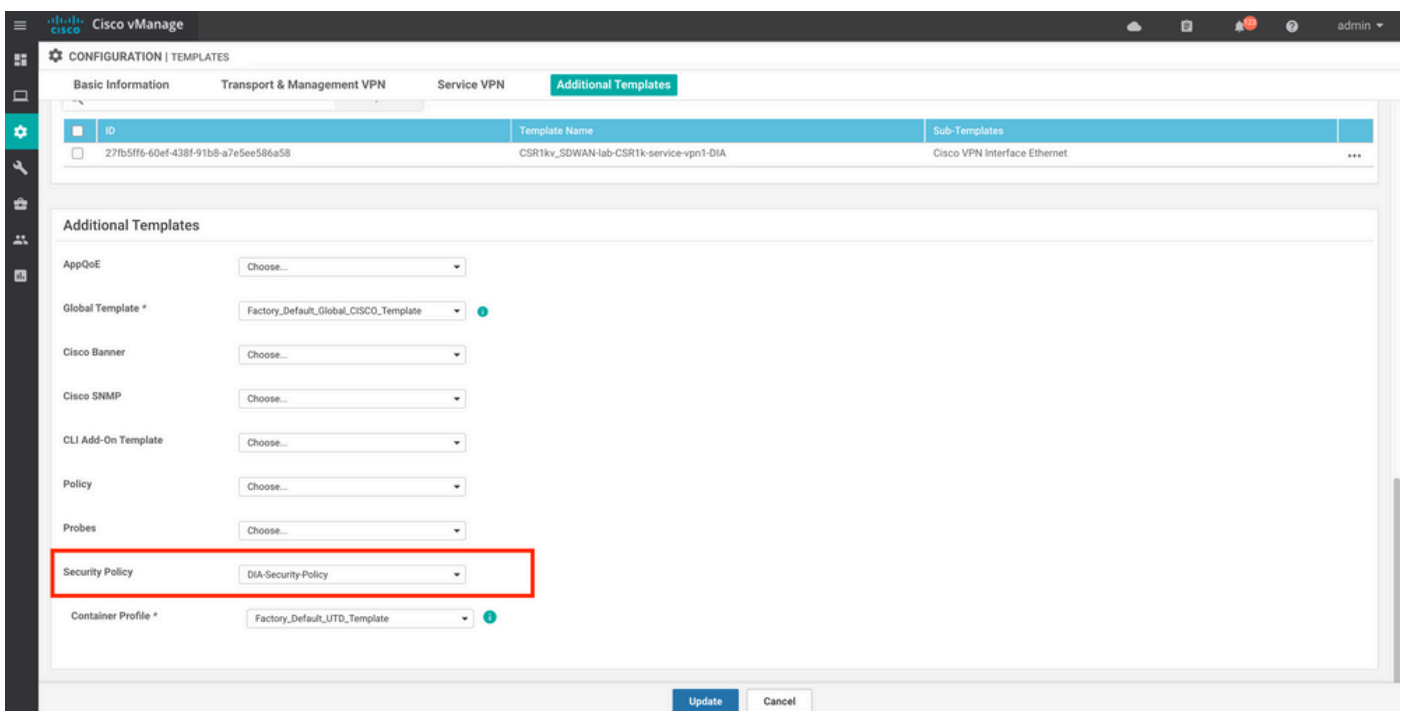
Add Advanced Malware Protection Policy

- Create New
- Copy from Existing

Fournissez un nom de stratégie. Sélectionnez l'une des régions globales du cloud AMP et activez l'analyse des fichiers. Pour l'analyse des fichiers avec ThreatGrid utilisé, choisissez l'une des régions de cloud TG, et entrez la clé API ThreatGrid, qui peut être obtenue à partir du portail ThreatGrid sous Mon compte ThreatGrid.



Une fois cela fait, enregistrez la stratégie et ajoutez cette stratégie de sécurité au modèle de périphérique sous Modèles supplémentaires -> Stratégie de sécurité comme indiqué dans l'image.



Configurez le périphérique avec le modèle de périphérique mis à jour.

Vérifier

Une fois que le modèle de périphérique a été correctement transmis au périphérique de périphérie, la configuration AMP peut être vérifiée à partir de l'interface de ligne de commande du routeur de périphérie :

<#root>

```
branch1-edge1#show sdwan running-config | section utd
app-hosting appid utd
  app-resource package-profile cloud-low
  app-vnic gateway0 virtualportgroup 0 guest-interface 0
    guest-ipaddress 192.168.1.2 netmask 255.255.255.252
  !
app-vnic gateway1 virtualportgroup 1 guest-interface 1
  guest-ipaddress 192.0.2.2 netmask 255.255.255.252
  !
  start
  utd multi-tenancy
  utd engine standard multi-tenancy
  threat-inspection profile IPS_Policy_copy
  threat detection
  policy balanced
  logging level notice
  !
  utd global

  file-reputation

    cloud-server cloud-isr-asn.amp.cisco.com
    est-server cloud-isr-est.amp.cisco.com
  !

  file-analysis

    cloud-server isr.api.threatgrid.com
    apikey 0 <redacted>
  !
  !

  file-analysis profile AMP-Policy-fa-profile

  file-types
  pdf
  ms-exe
  new-office
  rtf
  mdb
  mscab
  mssole2
  wri
  xlw
  flv
  swf
  !
  alert level critical
  !

  file-reputation profile AMP-Policy-fr-profile

  alert level critical
  !

  file-inspection profile AMP-Policy-fi-profile

  analysis profile AMP-Policy-fa-profile
```

```
reputation profile AMP-Policy-fr-profile

!
policy utd-policy-vrf-1
  all-interfaces

  file-inspection profile AMP-Policy-fi-profile

vrf 1
  threat-inspection profile IPS_Policy_copy
exit
policy utd-policy-vrf-global
  all-interfaces

  file-inspection profile AMP-Policy-fi-profile

vrf global
exit
no shutdown
```

Dépannage

L'intégration SD-WAN AMP implique de nombreux composants comme décrit. En matière de dépannage, il est donc essentiel de pouvoir établir des points de démarcation clés pour limiter le problème aux composants du flux de fonctionnalités :

1. vManage. Le vManage peut-il envoyer avec succès la stratégie de sécurité avec la stratégie AMP vers le périphérique de périphérie ?
2. Bord. Une fois que la stratégie de sécurité a été correctement mise en périphérie, le routeur capture-t-il le fichier soumis à l'inspection AMP et l'envoie-t-il au cloud AMP/TG ?
3. Cloud AMP/TG. Si la périphérie a envoyé le fichier à AMP ou à TG, obtient-elle la réponse dont elle a besoin pour prendre une décision d'autorisation ou d'abandon ?

Cet article porte sur le périphérique de périphérie (2) et les divers outils de plan de données disponibles pour aider à résoudre les problèmes d'intégration AMP sur le routeur de périphérie WAN.

Flux de dépannage général

Utilisez ce workflow de haut niveau pour dépanner rapidement les différents composants impliqués dans l'intégration d'AMP, avec pour objectif principal d'établir le point de démarcation du problème entre le périphérique de périphérie et le cloud AMP/TG.

1. La stratégie AMP est-elle correctement appliquée au périphérique de périphérie ?
2. Vérifiez l'état général du conteneur UTD.
3. Vérifiez la réputation des fichiers et analysez l'état du client sur la périphérie.
4. Vérifiez si le transfert de fichiers est transféré vers le conteneur. Cela peut être fait avec le

suivi de paquets Cisco IOS® XE.

5. Vérifiez que la périphérie communique correctement avec le cloud AMP/TG. Cela peut être fait avec des outils comme EPC ou packet-trace.
6. Assurez-vous que UTD crée un cache local basé sur la réponse AMP.

Ces étapes de dépannage sont examinées en détail dans ce document.

Problèmes de diffusion de stratégie sur vManage

Comme l'illustre la configuration de la stratégie AMP, la stratégie AMP est assez simple, sans beaucoup d'options de configuration. Voici quelques points communs à prendre en compte :

1. vManage doit être en mesure de résoudre les noms DNS pour AMP et le cloud ThreatGrid pour l'accès aux API. Si la configuration du périphérique échoue sur vManage après l'ajout de la stratégie AMP, vérifiez le `/var/log/nms/vmanage-server.log` pour les erreurs.
2. Comme indiqué dans le guide de configuration, le niveau du journal des alertes a laissé le niveau critique par défaut, ou Avertissement si nécessaire. La journalisation au niveau des informations doit être évitée car elle peut avoir un impact négatif sur les performances.

Pour vérifier, accédez à la base de données neo4j et affichez le contenu de la table `vmanagedbAPIKEYNODE`.

```
neo4j@neo4j> match (n:vmanagedbAPIKEYNODE) return n; +-----+
+-----+
+-----+ | n | +-----+
+-----+ | (:vmanagedbAPIKEYNODE {_rid:
"0:ApiKeyNode:1621022413389:153", keyServerHostName: "isr.api.threatgrid.com", feature: "Amp", apiKey:
"$CRYPT_CLUSTER$IbGLEMGIYMNRy1s9P+WcfA==$dozo7tmRP1+HrvEnXQr4x1VxSViYkKwQ4HBAIhXWOtQ=", deviceID: "CSR-
07B6865F-7FE7-BA0D-7240-1BDA16328455"}) | +-----+
+-----+
```

Intégration AMP sur routeur de périphérie Cisco

Vérifier l'intégrité du conteneur UTD

Utilisez les commandes `show utd` pour vérifier l'intégrité globale du conteneur UTD :

```
show utd engine standard config
show utd engine standard status
show platform hardware qfp active feature utd config
show platform hardware qfp active feature utd stats
show app-hosting detail appid utd
show sdwan virtual-application utd
```

Vérifier l'état UTD AMP

Assurez-vous que l'inspection des fichiers est activée :

```
<#root>
```

```
branch1-edge1#show sdwan utd dataplane config
utd-dp config context 0
context-flag 25427969
engine Standard
state enabled
sn-redirect fail-open
redirect-type divert
threat-inspection not-enabled
defense-mode not-enabled
domain-filtering not-enabled
url-filtering not-enabled
all-interface enabled

file-inspection enabled
```

```
utd-dp config context 1
context-flag 25559041
engine Standard
state enabled
sn-redirect fail-open
redirect-type divert
threat-inspection enabled
defense-mode IDS
domain-filtering not-enabled
url-filtering not-enabled
all-interface enabled

file-inspection enabled
```

Vérifiez que la connexion au cloud AMP est active :

```
<#root>
```

```
branch1-edge1#show utd engine standard status file-reputation
File Reputation Status:
  Process:
```

```
Running
```

```
Last known status: 2021-06-17 16:14:20.357884-0400 [info] AMP module version 1.12.4.999
```

```
<#root>
```

```
branch1-edge1#show sdwan utd file reputation
utd-oper-data utd-file-reputation-status version 1.12.4.999

utd-oper-data utd-file-reputation-status status utd-file-repu-stat-connected
```

```
utd-oper-data utd-file-reputation-status message "Connected to AMP Cloud!"
```

Vérifiez que la connexion à ThreatGrid est active :

```
<#root>
```

```
branch1-edge1#show utd engine standard status file-analysis
```

```
File Analysis Status:
```

```
Process:
```

```
Running
```

```
Last Upload Status: No upload since process init
```

```
<#root>
```

```
branch1-edge1#show sdwan utd file analysis
```

```
utd-oper-data utd-file-analysis-status status tg-client-stat-up
```

```
utd-oper-data utd-file-analysis-status backoff-interval 0
```

```
utd-oper-data utd-file-analysis-status message "TG Process Up"
```

Si le processus ThreatGrid n'affiche pas l'état Démarré, une nouvelle clé d'API est utile. Pour déclencher une nouvelle clé d'API, accédez à Maintenance -> Security :

Hostname	System IP	Chassis Number	Device Model	Virtual Image State	Virtual Image Version
branch1-cedge1	6.1.1.11	CSR-07B6865F-7FE7-BA0D-7240-...	CSR1000v	RUNNING	1.0.6_SV2.9.13.0_XE17.3

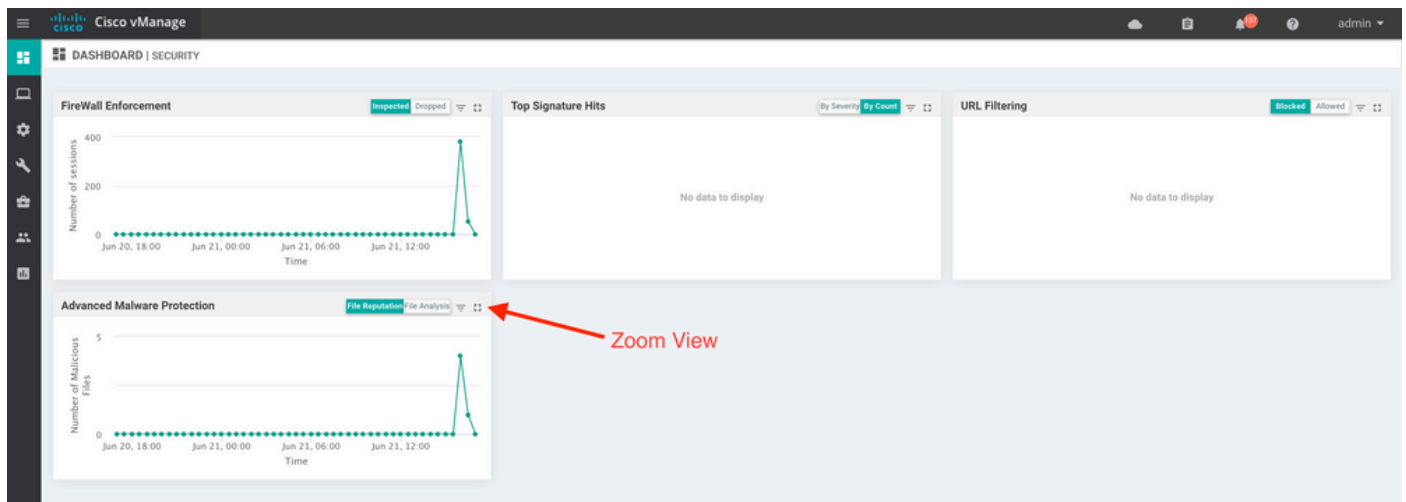
Remarque : une nouvelle clé API déclenche une diffusion de modèle vers le périphérique.

Surveillance de l'activité AMP sur un routeur de périphérie WAN

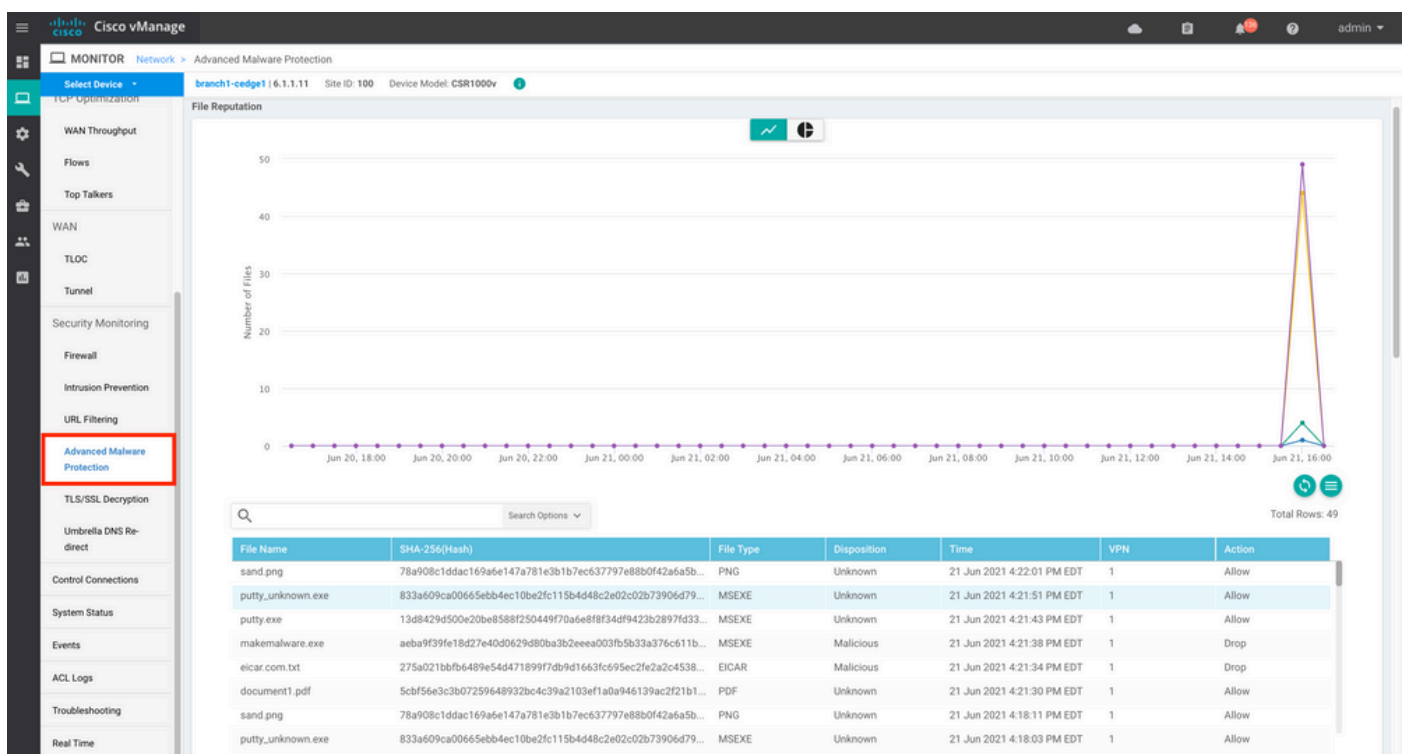
vManage

À partir de vManage, les activités des fichiers AMP peuvent être surveillées à partir du tableau de bord de sécurité ou de Device View.

Tableau de bord :



Vue du périphérique :



CLI

Vérifier les statistiques de réputation des fichiers :

```
branch1-edge1#show utd engine standard statistics file-reputation
File Reputation Statistics
```

```
-----
File Reputation Clean Count:           1
File Reputation Malicious Count:       4
File Reputation Unknown Count:         44
File Reputation Requests Error:        0
File Reputation File Block:            4
File Reputation File Log:              45
```

Vérifier les statistiques d'analyse de fichier :

```
branch1-edge1#show utd engine standard statistics file-analysis
File Analysis Statistics
-----
File Analysis Request Received:      2
File Analysis Success Submissions:   2
File Analysis File Not Interesting:   0
File Analysis File Whitelisted:      0
File Analysis File Not Supported:    0
File Analysis Limit Exceeding:       0
File Analysis Failed Submissions:    0
File Analysis System Errors:         0
```

Remarque : vous pouvez obtenir des statistiques internes supplémentaires à l'aide de la commande `show utd engine standard statistics file-reputation vrf global internal`.

Comportement du plan de données

Le trafic du plan de données soumis à l'inspection de fichier sur la base de la stratégie AMP configurée est transféré vers le conteneur UTD pour traitement. Ceci peut être confirmé avec un suivi de paquet utilisé. Si le trafic n'est pas correctement transféré vers le conteneur, aucune des actions d'inspection de fichier suivantes ne peut se produire.

Cache de fichiers local AMP

Le conteneur UTD dispose d'un cache local de hachage SHA256, de type de fichier, de disposition et d'action en fonction des résultats de la recherche AMP dans le cloud. Le conteneur ne demande une disposition du cloud AMP que si le hachage du fichier ne se trouve pas dans le cache local. La durée de vie du cache local est de 2 heures avant sa suppression.

```
branch1-edge1#show utd engine standard cache file-inspection
Total number of cache entries: 6
File Name|          SHA256|          File Type|          Disposition|          action|
-----|-----|-----|-----|-----|
sand.png          78A908C1DDAC169A          69          1          1
putty.exe         13D8429D500E20BE          21          1          2
makemalware.exe  AEBA9F39FE18D27E          21          3          2
putty_unknown.exe 833A609CA00665EB          21          1          2
document1.pdf     5CBF56E3C3B07259          285         1          1
eicar.com.txt     275A021BBFB6489E          273         3          2
```

Code disposition AMP :

- 0 NONE
- 1 UNKNOWN
- 2 CLEAN
- 3 MALICIOUS

Code action AMP :

- 0 UNKNOWN
- 1 ALLOW
- 2 DROP

Afin d'obtenir le hachage SHA256 complet pour les fichiers, ce qui est très important afin de dépanner un verdict de fichier spécifique, utilisez l'option detail de la commande :

```
branch1-edge1#show utd engine standard cache file-inspection detail
SHA256: 78A908C1DDAC169A6E147A781E3B1B7EC637797E88B0F42A6A5B59810B8E7EE5
amp verdict: unknown
amp action: 1
amp disposition: 1
reputation score: 0
retrospective disposition: 0
amp malware name:
file verdict: 1
TG status: 0
file name: sand.png
filetype: 69
create_ts: 2021-06-21 16:58:1624309104
sig_state: 3
```

```
-----
SHA256: 13D8429D500E20BE8588F250449F70A6E8F8F34DF9423B2897FD33BBB8712C5F
amp verdict: unknown
amp action: 2
amp disposition: 1
reputation score: 0
retrospective disposition: 0
amp malware name:
file verdict: 1
TG status: 7
file name: putty.exe
filetype: 21
create_ts: 2021-06-21 16:58:1624309107
sig_state: 3
```

```
-----
SHA256: AEBA9F39FE18D27E40D0629D80BA3B2EEEEA003FB5B33A376C611BB4D8FFD03A6
amp verdict: malicious
amp action: 2
amp disposition: 3
reputation score: 95
retrospective disposition: 0
amp malware name: W32.AEBA9F39FE-95.SBX.TG
file verdict: 1
TG status: 0
file name: makemalware.exe
```

```
filetype: 21
create_ts: 2021-06-21 16:58:1624309101
sig_state: 3
<SNIP>
```

Afin de supprimer les entrées du cache local du moteur UTD, utilisez la commande suivante :

```
clear utd engine standard cache file-inspection
```

Exécuter les débogages UTD

Les débogages utd peuvent être activés pour résoudre les problèmes AMP :


```
debug utd engine standard file-reputation level info
debug utd engine standard file-analysis level info
debug utd engine standard climgr level info
```

Le résultat du débogage peut être récupéré directement à partir de l'interpréteur de commandes du système à l'adresse /tmp/rp/trace/vman_utd_R0-0.bin, ou copiez le fichier de trace dans le système de fichiers du routeur en procédant comme suit :

```
branch1-edge1#app-hosting move appid utd log to bootflash:
Successfully moved tracelog to bootflash:/iox_utd_R0-0_R0-0.5113_0.20210622110241.bin.gz
branch1-edge1#
```

Pour afficher le journal de suivi UTD :

```
branch1-edge1#more /compressed bootflash:/iox_utd_R0-0_R0-0.5113_0.20210622110241.bin.gz
<snip>
2021-06-22 10:35:04.265:(#1):SPP-FILE-INSPECTION File signature query: sig_state = 3
2021-06-22 10:35:04.266:(#1):SPP-FILE-INSPECTION start_time : 1624372489, current_time : 1624372504,Dif
2021-06-22 10:35:04.266:(#1):SPP-FILE-INSPECTION amp_cache_node_exists:: Entry
2021-06-22 10:35:04.266:(#1):SPP-FILE-INSPECTION Signature not found in cache
2021-06-22 10:35:04.266:(#1):SPP-FILE-INSPECTION file_type_id = 21
2021-06-22 10:35:04.266:(#1):SPP-FILE-INSPECTION Write to cbuffer
2021-06-22 10:35:04.266:(#1):SPP-FILE-INSPECTION Sent signature lookup query to Beaker
2021-06-22 10:35:04.266:(#1):SPP-FILE-INSPECTION File Name = /putty_unknown.exe, file_name = /putty_unkn
2021-06-22 10:35:04.266:(#1):SPP-FILE-INSPECTION amp_extract_filename :: Extracted filename 'putty_unkn
2021-06-22 10:35:04.266:(#1):SPP-FILE-INSPECTION amp_cache_add:: Entry
2021-06-22 10:35:04.266:(#1):SPP-FILE-INSPECTION amp_cache_allocate:: Entry
2021-06-22 10:35:04.266:(#1):SPP-FILE-INSPECTION Return FILE_VERDICT_PENDING
<SNIP>
```

 Note : Dans les versions 20.6.1 et ultérieures, la façon de récupérer et d'afficher les tracelogs utd est conforme au workflow de trace standard avec la commande show logging process vman module utd ...

Vérification de la communication entre la périphérie et le cloud

Pour vérifier que le périphérique de périphérie communique avec le cloud AMP/TG, l'EPC du routeur de périphérie WAN peut être utilisé pour confirmer la communication bidirectionnelle vers/depuis les services cloud :

```
branch1-edge1#show monitor capture amp parameter
monitor capture amp interface GigabitEthernet1 BOTH
monitor capture amp access-list amp-cloud
monitor capture amp buffer size 10
monitor capture amp limit pps 1000
```

Problèmes liés à AMP et TG Cloud

Une fois qu'il a été confirmé que le périphérique de périphérie capture correctement le fichier et l'envoi à AMP/TG pour analyse, mais que le verdict est incorrect, il nécessite le dépannage AMP ou le cloud Threatgrid, ce qui sort du cadre de ce document. Les informations sont importantes lorsque des problèmes d'intégration sont présentés :

- Compte ThreatGrid Organisation
- Horodatage
- ID d'analyse de périphérie (par exemple, CSR-07B6865F-7FE7-BA0D-7240-1BDA16328455), il s'agit du numéro de châssis du routeur de périphérie WAN.
- Hachage SHA256 complet pour le fichier en question

Informations connexes

- [Guide de configuration de la sécurité SD-WAN](#)
- [Portail ThreatGrid](#)
- [Assistance et documentation techniques - Cisco Systems](#)

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.