ESR configureren om onbekende MIME-bestanden te uploaden naar File Analysis Server

Inhoud

Inleiding

Dit document beschrijft de stappen om onbekende MIME-type bestanden (Application/Octet-stream) naar File Analysis Server in Cisco ESA te uploaden.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Hoe Advanced Malware Protection (AMP) in ESA werkt.
- Basiskennis van MIME-typen bestanden.

Cisco raadt u aan het volgende te doen:

- Fysieke of virtuele ESA geïnstalleerd.
- Licentie geactiveerd of geïnstalleerd.
- De setup-wizard is voltooid.

- Administratieve toegang tot de ESA Command Line Interface (CLI).

Gebruikte componenten

Dit document is van toepassing op AsyncOS 15.5.1, 15.0.2 en latere releases.

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.

MIME-typen

Een mediatype, ook wel MIME-type (Multipurpose Internet Mail Extensions) genoemd, dient om het karakter en de structuur van een document, bestand of verzameling bytes te identificeren. De specificaties voor MIME-typen worden in de Internet Engineering Task Force (IETF) RFC 6838 vastgesteld en uniform gemaakt.

Niet-herkende subtypen van "tekst" moeten als "gewoon" subtype worden behandeld zolang de MIME-implementatie weet hoe de tekenset moet worden verwerkt. Niet-herkende subtypen die ook een niet-herkende tekenset specificeren, moeten worden behandeld als "application/octet-stream".

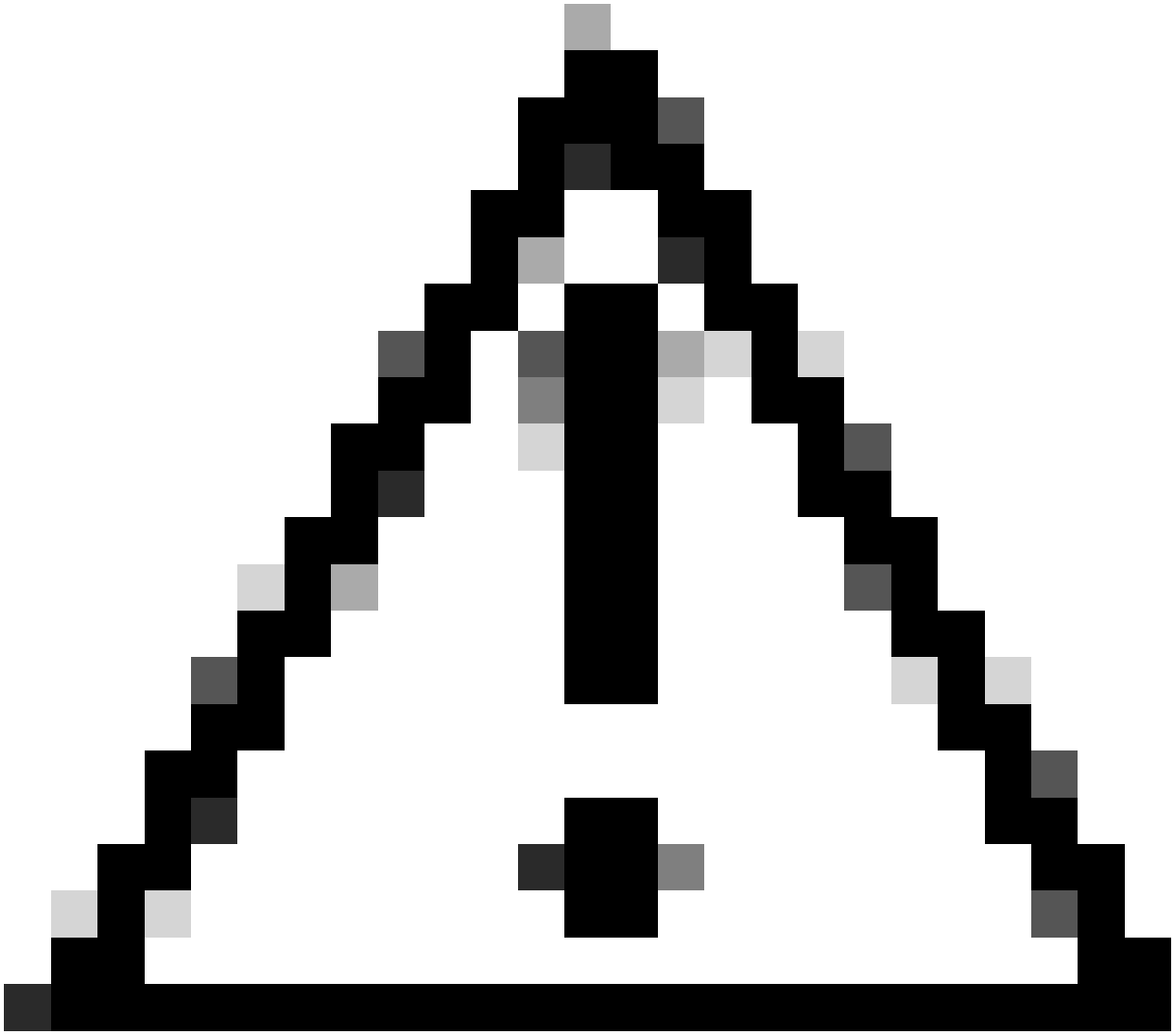
Raadpleeg voor meer informatie RFC 2046 - Multipurpose Internet Mail Extensions (MIME), deel twee: Mediatypen

ESA-applicatie heeft de uploadlimiet overschreden

Als u de service Bestandsanalyse hebt ingeschakeld en de reputatieservice geen informatie over het bestand heeft, en het bestand voldoet aan de criteria voor bestanden die kunnen worden geanalyseerd, dan kan het bericht in quarantaine worden geplaatst en kan het bestand voor analyse worden verzonden. Als u het apparaat niet hebt geconfigureerd voor quarantaineberichten wanneer bijlagen voor analyse worden verzonden, of als het bestand niet voor analyse wordt verzonden, wordt het bericht aan de gebruiker vrijgegeven.

Verwijs voor meer informatie naar de gebruikershandleiding. Gebruikershandleiding voor AsyncOS 15.0 voor Cisco Secure Email Gateway - GD (Algemene implementatie) - Filtering van bestandsnaam en bestandsanalyse [Cisco Secure Email Gateway] - Cisco

We hebben een nieuwe CLI-opdracht geïntroduceerd om het probleem aan te pakken van apparaten met beperkte quota voor het indienen van bestanden die voortijdig de maximale uploadcapaciteit bereiken doordat de ESA excessieve bestanden ter inspectie voorlegt, . Deze verbetering is geïmplementeerd vanaf versie 15.5.1 en wordt ook opgenomen in de 15.0.2 Onderhoudsrelease (MR) en daaropvolgende versies.



Waarschuwing: voor verbeterde beveiliging raden we u sterk aan alle bestanden te uploaden zoals aanbevolen. Als u het echter van essentieel belang acht om deze stap voor specifieke bestandstypen te omzeilen, stelt de geboden opdracht de optie in staat om dit naar eigen goeddunken te doen. We verzoeken u voorzichtig te zijn en de mogelijke risico's te begrijpen.

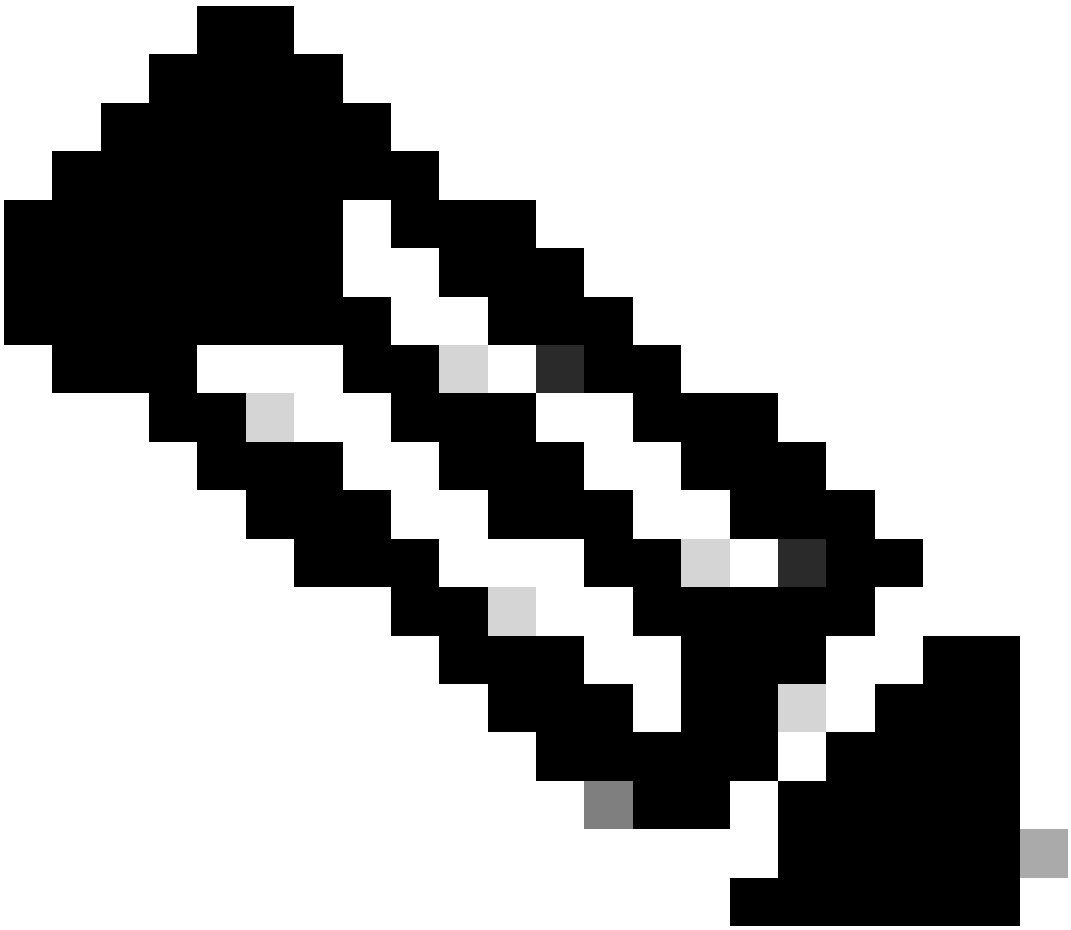
Uitsluiten van toepassing/octet-stream MIME-typen voor uploaden naar bestandsanalyse

Gebruik de volgende stappen om de MIME-typen van de toepassing/octet-stream uit te sluiten voor het uploaden naar de server voor bestandsanalyse:

Stap 1. Log in op CLI.

Stap 2. Start de opdracht ampconfig

Stap 3. Type onbekend mimeoverride en druk op ENTER



Opmerking: unknownmimeoverride is een verborgen opdracht.

Stap 4. Type N in antwoord op "Wilt u onbekende mime voor analyse alleen sturen als hun extensies zijn geselecteerd? [N]> "

Stap 5. Druk op ENTER om de wizard te verlaten.

Stap 6. Wijzigingen vastleggen

```
ESA_CLI> ampconfig

File Reputation: Enabled
File Analysis: Enabled
Appliance Group ID/Name: Not part of any group yet
```

```
Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- SETGROUP - Add this appliance to the group of appliances that can share File Analysis reporting
details.
- CACHESETTINGS - Configure the cache settings for AMP.
[]> unknownmimeoverride

Do you want to send unknown mime for analysis only if their extensions are selected? [Y]> N

ESA_CLI>  commit
```

Gekoppelde defecten en verbeteringen

Deze nieuwe functie wordt geïntroduceerd vanwege deze Functieaanvragen en -defecten:

- Gedragsverandering in HTML en Octet-stream bestanden uploaden naar File Analysis verwart klanten. Cisco bug-id CSCwh61317
- p7s-bestanden worden geüpload naar File Analysis, zelfs als het bestandstype niet is geselecteerd. Cisco bug-id CSCwh70476

Referenties

Gebruikershandleiding voor AsyncOS 15.0 voor Cisco Secure Email Gateway - GD (Algemene implementatie) - Filtering van bestandsnaam en bestandsanalyse [Cisco Secure Email Gateway] - Cisco

RFC 2046 - Multipurpose Internet Mail Extensions (MIME), deel twee: mediatypen

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.