De waarschuwing "Upload Limit Reach" op een ESA met AMP begrijpen

Inhoud

Inleiding

In dit document wordt de waarschuwing "Upload Limit Reach" beschreven die de E-mail security applicatie (ESA) werpt wanneer deze geconfigureerd is om e-mails te scannen met de Advanced Malware Protection (AMP)-functie.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- E-mail security applicatie
- Advanced Malware Protection

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- E-mail security applicatie (ESA) met software 12.x

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.

Achtergrondinformatie

De e-mail security applicatie (ESA) gebruikt de Advanced Malware Protection (AMP) functie die twee hoofdfuncties bevat:

- Bestandsreputatie
- Bestandsanalyse

Bestandsanalyse uploadt berichtbijlagen voor zandbakanalyse naar ThreatGrid Cloud-servers.

De melding "Uploadlimiet bereikt" begrijpen

Berichttracering kan tonen dat e-mails niet zijn gescand door Advanced Malware Protection (AMP) omdat ze de uploadlimiet hebben bereikt.

Voorbeeld:

```
02 Dec 2019 14:11:36 (GMT +01:00) Message 12345 is unscannable by Advanced Malware Protection engine. Reason: Upload Limit Reached
```

In het nieuwe ThreatGrid-model zijn deze limieten het aantal monsters dat apparaten mogen uploaden voor bestandsanalyse per organisatie. Alle geïntegreerde apparaten (WSA, ESA, CES, FMC, enz.) en AMP voor endpoints hebben recht op 200 monsters per dag, ongeacht het aantal apparaten.

Dit is een gedeelde limiet (geen limiet per apparaat), en dit geldt voor licenties die na 12-1-2017 zijn gekocht.

> **Opmerking:** Deze teller wordt niet elke dag gereset, in plaats daarvan, dit werkt als een 24 uur rolperiode.

Voorbeeld:

Als de ESA1 vandaag om 10:00 uur 80 monsters uploadt, kunnen er in een cluster van 4 ESA's met een uploadlimiet van 200 monsters van vandaag om 10:01 uur tot morgen om 10:00 uur, wanneer de eerste 80 slots worden vrijgegeven, nog slechts 120 monsters worden geüpload tussen de 4 ESA's (gedeelde limiet).

Hoe kunt u het aantal monsters controleren dat uw ESA's de afgelopen 24 uur hebben geüpload?

ESA: Navigeer naar **Monitor > AMP File Analysis** report en controleer de sectie **Bestanden uploaden voor analyse**.

SMA: Navigeer naar **E-mail > Rapportage > AMP File Analysis** report en controleer de sectie **Bestanden geüpload voor analyse**.

> **Opmerking:** Als het AMP File Analysis-rapport geen nauwkeurige gegevens weergeeft, raadpleegt u de sectie File Analysis Details in the Cloud Are Incomplete in de Gebruikershandleiding.

> **Waarschuwing**: Raadpleeg het defect CSCvm10813 voor de aanvullende informatie.

U kunt ook een **grep**-opdracht uitvoeren vanuit de CLI om het aantal geüploade bestanden te tellen.

Dit moet op elk apparaat gebeuren.

Voorbeeld:

```
grep "Dec 20.*File uploaded for analysis" amp -c
grep "Dec 21.*File uploaded for analysis" amp -c
```

U kunt reguliere PCRE-expressies gebruiken om de datum en tijd aan te passen.

Hoe kunt u de uploadlimiet verlengen?

Neem binnen Cisco contact op met uw accountmanager of Sales Engineer.

Gerelateerde informatie

- Diepe omleiding naar AMP en Threat Grid-integratie met Cisco Email Security
- Uploads van bestandsanalyse op ESA verifiëren
- Technische ondersteuning en documentatie – Cisco Systems

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.