Anzeige "Upload-Grenze erreicht" auf ESA mit AMP verstehen

Inhalt

Einleitung

In diesem Dokument wird die Warnung "Upload Limit Reached" (Upload-Grenze erreicht) beschrieben, die die E-Mail-Security-Appliance (ESA) ausgibt, wenn sie für das Scannen von E-Mails mit der Advanced Malware Protection-Funktion (AMP) konfiguriert ist.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- E-Mail Security Appliance
- Advanced Malware Protection

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Email Security Appliance (ESA) mit Software 12.x

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

Die E-Mail Security Appliance (ESA) verwendet die Advanced Malware Protection-Funktion (AMP), die zwei Hauptfunktionen umfasst:

- Dateireputation
- Dateianalyse

Die Dateianalyse lädt Nachrichtenanhänge zur Sandbox-Analyse auf die ThreatGrid Cloud-Server hoch.

Warnung "Upload-Grenzwert erreicht" verstehen

Mit der Nachrichtenverfolgung kann angezeigt werden, dass E-Mails von Advanced Malware Protection (AMP) nicht gescannt wurden, weil sie die Uploadgrenze erreicht haben.

Beispiel:

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

Im neuen ThreatGrid-Modell für Stichprobenlimits sind diese Limits die Anzahl von Stichproben, die Geräte für Dateianalysen pro Organisation hochladen dürfen. Alle integrierten Geräte (WSA, ESA, CES, FMC usw.) sowie AMP für Endgeräte haben Anspruch auf 200 Stichproben pro Tag, unabhängig von der Anzahl der Geräte.

Dies ist ein gemeinsam genutztes Limit (kein Limit pro Gerät), und dies gilt für Lizenzen, die nach dem 12.1.2017 erworben wurden.

> **Anmerkung:** Dieser Zähler wird nicht jeden Tag zurückgesetzt, sondern dies funktioniert als 24 Stunden Roll-over-Zeitraum.

Beispiel:

Wenn die ESA1 heute um 10:00 Uhr 80 Samples hochlädt, können in einem Cluster von 4 ESAs mit einem Grenzwert von 200 Upload-Samples von heute um 10:01 Uhr bis morgen um 10:00 Uhr, wenn die ersten 80 Slots freigegeben werden, nur 120 weitere Samples von den 4 ESAs hochgeladen werden.

Wie können Sie überprüfen, wie viele Stichproben Ihre ESA in den letzten 24 Stunden hochgeladen haben?

ESA: Navigieren Sie zu **Monitor > AMP File Analysis (Überwachung > AMP-Dateianalyse)**, und überprüfen Sie den Abschnitt "**Zur Analyse hochgeladene Dateien**".

SMA: Navigieren Sie zu **E-Mail > Reporting > AMP File Analysis (**Bericht über **AMP-Dateianalyse)**, und überprüfen Sie den Abschnitt **Files Uploaded for Analysis (Zur Analyse hochgeladene Dateien)**.

> **Anmerkung:** Wenn der AMP-Dateianalysebericht keine genauen Daten zeigt, lesen Sie den Abschnitt Details zur Dateianalyse im Abschnitt Cloud sind unvollständig im Benutzerhandbuch.

Warnung: Weitere Informationen finden Sie im Defekt CSCvm10813.

Alternativ können Sie einen Befehl **grep** aus der CLI ausführen, um die Anzahl der hochgeladenen Dateien zu zählen.

Dies muss auf jeder Appliance geschehen.

Beispiel:

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

Sie können reguläre PCRE-Ausdrücke verwenden, um Datum und Uhrzeit abzugleichen.

Wie können Sie das Upload-Limit verlängern?

Wenden Sie sich an Ihren Account Manager oder Vertriebstechniker bei Cisco.

Zugehörige Informationen

- Umfassende Informationen zur Integration von AMP und Threat Grid mit Cisco Email Security
- Uploads der Dateianalyse auf die ESA überprüfen
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.