

Comprender la alerta "Límite de carga alcanzado" en ESA con AMP

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Comprender la alerta de "Límite de carga alcanzado"](#)

[¿Cómo puede comprobar el número de muestras que sus ESA han cargado en las últimas 24 horas?](#)

[¿Cómo puede ampliar el límite de carga?](#)

[Información Relacionada](#)

Introducción

Este documento describe la alerta "Límite de carga alcanzado" que el dispositivo de seguridad de correo electrónico (ESA) lanza cuando se configura para escanear correos electrónicos con la función de protección frente a malware avanzado (AMP).

prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Aplicación de seguridad de correo electrónico
- Protección frente a malware avanzado

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Dispositivo de seguridad de correo electrónico (ESA) que ejecuta el software 12.x

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

El dispositivo de seguridad Email Security Appliance (ESA) utiliza la función de protección frente a malware avanzado (AMP), que contiene dos funciones principales:

- [Reputación de archivos](#)
- [Análisis de archivos](#)

Análisis de archivos carga los archivos adjuntos a los mensajes para el análisis de sandbox en los servidores de la nube de ThreatGrid.

Comprender la alerta de "Límite de carga alcanzado"

El seguimiento de mensajes puede mostrar que la protección frente a malware avanzado (AMP) no ha analizado los correos electrónicos porque han alcanzado el límite de carga.

Ejemplo:

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

En el nuevo modelo de límites de ejemplo de ThreatGrid, estos límites son el número de muestras que los dispositivos pueden cargar para el análisis de archivos por organización. Todos los dispositivos integrados (WSA, ESA, CES, FMC, etc.), así como AMP para terminales, tienen derecho a 200 muestras al día, independientemente del número de dispositivos.

Se trata de un límite compartido (no un límite por dispositivo) y se aplica a las licencias compradas después del 12/1/2017.

Nota: Este contador no se reinicia todos los días, en su lugar, funciona como un período de 24 horas.

Ejemplo:

En un clúster de 4 ESA con un límite de 200 muestras de carga, si el ESA1 carga 80 muestras a las 10:00 hoy, sólo se pueden cargar 120 muestras más entre los 4 ESA (límite compartido) desde hoy a las 10:01 hasta mañana a las 10:00, cuando se liberan las primeras 80 ranuras.

¿Cómo puede comprobar el número de muestras que sus ESA han cargado en las últimas 24 horas?

ESA: Navegue hasta **Supervisar > informe AMP File Analysis** y verifique la **sección Archivos Cargados para Análisis**.

SMA: Navegue hasta el informe **Correo electrónico > Informes > Análisis de archivos AMP** y verifique la **sección Archivos cargados para análisis**.

Nota: Si el informe Análisis de archivos de AMP no muestra datos precisos, revise la sección [Detalles del análisis de archivos en la nube son incompletos](#) de la guía del usuario.

Advertencia: Consulte el defecto [CSCvm10813](#) para obtener información adicional.

Como alternativa, puede ejecutar un comando **grep** desde la CLI para contar el número de archivos cargados.

Esto debe hacerse en cada dispositivo.

Ejemplo:

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

Puede utilizar [expresiones regulares PCRE](#) para coincidir con la fecha y la hora.

¿Cómo puede ampliar el límite de carga?

Póngase en contacto con su comercial o ingeniero de ventas de Cisco.

Información Relacionada

- [Perspectiva en la integración de AMP y Threat Grid con Cisco Email Security](#)
- [Verificación de las Cargas de Análisis de Archivos en ESA](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)