Entender o alerta "Limite de carregamento atingido" no ESA com AMP

Contents

Introduction

Este documento descreve o alerta "Limite de carregamento atingido" que o Email Security Appliance (ESA) emite quando configurado para verificar e-mails com o recurso Advanced Malware Protection (AMP).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Dispositivo de segurança de e-mail
- Proteção avançada contra malware

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Email Security Appliance (ESA) executando software 12.x

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O Email Security Appliance (ESA) usa o recurso Advanced Malware Protection (AMP), que contém duas funções principais:

- Reputação do arquivo
- Análise de arquivo

A análise de arquivos carrega anexos de mensagens para análise de sandbox em servidores ThreatGrid Cloud.

Entender o alerta "Limite de upload atingido"

O Rastreamento de mensagens pode mostrar que os e-mails não foram verificados pela Proteção avançada contra malware (AMP) porque atingiram o limite de carregamento.

Exemplo:

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

No novo modelo de limites de amostra do ThreatGrid, esses limites são o número de amostras que os dispositivos podem carregar para análise de arquivos por organização. Todos os dispositivos integrados (WSA, ESA, CES, FMC, etc.) e o AMP for Endpoints têm direito a 200 amostras por dia, independentemente do número de dispositivos.

Esse é um limite compartilhado (não um limite por dispositivo) e se aplica a licenças compradas após 12/1/2017.

> **Note**: Esse contador não é reiniciado todos os dias; em vez disso, ele funciona como um período de renovação de 24 horas.

Exemplo:

Em um cluster de 4 ESAs com um limite de carregamento de 200 amostras, se o ESA1 carregar 80 amostras às 10:00 hoje, apenas 120 amostras adicionais poderão ser carregadas entre os 4 ESAs (limite compartilhado) de hoje às 10:01 até amanhã às 10:00, quando os primeiros 80 slots forem liberados.

Como você pode verificar o número de amostras que seus ESAs carregaram nas últimas 24 horas?

ESA: Navegue para **Monitor > AMP File Analysis** e verifique a seção **Arquivos carregados para análise**.

SMA: Navegue até **E-mail > Relatórios > Análise de arquivo AMP** e verifique a seção **Arquivos carregados para análise**.

> **Note**: Se o relatório de análise de arquivo do AMP não mostrar dados precisos, consulte a seção Detalhes da análise de arquivo na nuvem estão incompletos no Guia do usuário.

> **aviso:** Consulte o defeito CSCvm10813 para obter informações adicionais.

Como alternativa, você pode executar um comando **grep** na CLI para contar o número de arquivos carregados.

Isso deve ser feito em cada dispositivo.

Exemplo:

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

Você pode usar as expressões regulares do PCRE para corresponder a data e a hora.

Como você pode estender o limite de upload?

Entre em contato com seu gerente de contas ou engenheiro de vendas na Cisco.

Informações Relacionadas

- Mergulhe fundo na integração do AMP e do Threat Grid com o Cisco Email Security
- Verificação dos carregamentos de análise de arquivo no ESA
- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.