AMP를 사용하는 ESA의 "Upload Limit Reached" 경고 이해

목차

[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[사용되는 구성 요소](#)
[배경 정보](#)
["업로드 제한 도달" 경고 이해](#)
[지난 24시간 동안 ESA에서 업로드한 샘플 수를 어떻게 확인할 수 있습니까?](#)
[업로드 제한을 어떻게 연장할 수 있습니까?](#)
[관련 정보](#)

소개

이 문서에서는 AMP(Advanced Malware Protection) 기능으로 이메일을 스캔하도록 구성된 경우 ESA(Email Security Appliance)가 보내는 "업로드 제한에 도달함" 알림에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Email Security Appliance
- 지능형 악성코드 차단

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- ESA(Email Security Appliance)에서 소프트웨어 12.x 실행

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

ESA(Email Security Appliance)는 두 가지 주요 기능이 포함된 AMP(Advanced Malware Protection) 기능을 사용합니다.

- 파일 평판

- 파일 분석

File Analysis(파일 분석)는 샌드박스 분석을 위한 메시지 첨부 파일을 ThreatGrid Cloud 서버에 업로드합니다.

"업로드 제한 도달" 경고 이해

메시지 추적은 이메일이 업로드 제한에 도달했기 때문에 AMP(Advanced Malware Protection)에서 스캔하지 않은 것으로 표시할 수 있습니다.

예:

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

새로운 ThreatGrid 샘플 제한 모델에서 이러한 제한은 조직 단위로 파일 분석을 위해 디바이스가 업로드할 수 있는 샘플 수입니다. 모든 통합 디바이스(WSA, ESA, CES, FMC 등)와 AMP for Endpoints는 디바이스 수에 관계없이 매일 200개의 샘플을 사용할 수 있습니다.

이는 공유 제한(디바이스당 제한 없음)이며 2017년 12월 1일 이후에 구매한 라이센스에 적용됩니다.

> **참고:** 이 카운터는 매일 재설정되는 것이 아니라 24시간 롤오버 기간으로 작동합니다.

예:

샘플 업로드 제한이 200개인 4개의 ESA로 구성된 클러스터에서 ESA1이 오늘 10시에 80개의 샘플을 업로드하는 경우, 오늘 10시1분부터 처음 80개의 슬롯이 릴리스되는 내일 10시까지 4개의 ESA(공유 제한) 중 120개의 샘플만 더 업로드할 수 있습니다.

지난 24시간 동안 ESA에서 업로드한 샘플 수를 어떻게 확인할 수 있습니까?

ESA: Monitor(모니터링) > AMP File Analysis(AMP 파일 분석) 보고서로 이동하고 Files Uploaded for Analysis(분석을 **위해 업로드된 파일) 섹션을** 확인합니다.

SMA: Email(**이메일) > Reporting(보고) > AMP File Analysis(AMP 파일 분석) 보고서**로 이동하여 Files Uploaded for Analysis(분석을 위해 **업로드된 파일) 섹션을** 확인합니다.

> **참고:** AMP File Analysis(AMP 파일 분석) 보고서에 정확한 데이터가 표시되지 않으면 사용 설명서의 File Analysis Details in the Cloud Is Incomplete(클라우드에서 파일 분석 세부사항) 섹션을 검토합니다.

> **경고:** 자세한 내용은 결함 CSCvm10813을 참조하십시오.

또는 CLI에서 **grep** 명령을 실행하여 업로드된 파일 수를 계산할 수 있습니다.

이는 각 어플라이언스에서 수행해야 합니다.

예:

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

PCRE 정규식을 사용하여 날짜 및 시간을 일치시킬 수 있습니다.

업로드 제한을 어떻게 연장할 수 있습니까?

Cisco의 어카운트 매니저 또는 세일즈 엔지니어에게 문의하십시오.

관련 정보

- AMP 및 Threat Grid와 Cisco Email Security의 통합에 대한 심층적인 분석
- ESA에서 파일 분석 업로드 확인
- 기술 지원 및 문서 – Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.