ThreatGrid Appliance는 버전 3.0을 설치하기 전에 필요한 재설정을 완료해야 한다고 조언합니다.

목차

소개

ThreatGrid Appliance 3.0 릴리스를 준비하려면 릴리스에 필요한 낮은 수준의 디스크 포맷을 수행하여 디바이스의 모든 데이터를 파기하려면 특정 어플라이언스를 재설정해야 합니다.

기고자: T.J. Bush, Cisco TAC 엔지니어

사전 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco ThreatGrid 어플라이언스

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

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

문제

ThreatGrid Appliance에 대한 알림을 받았습니다.

```
This appliance was initially installed with a software release prior to 2.7.0, and has not had
its datastore reset
after 2.7.0 or later was installed.

The 3.0 software release only supports the new storage format introduced with 2.7.0, and cannot
be installed without first
performing a data reset (which will delete all content and recreate the datastore in the new
format).

This can be done at any time before the appliance 3.0 release is installed.
```

```
A data reset will be required before the appliance 3.0 release can be installed.
Be sure the backup system has been running for 48 hours without any failure reports before
performing this reset,
and that you have downloaded your backup encryption key.

Contact customer support for any question
```

솔루션

> **참고:**디바이스에서 destroy data 명령이 실행되고 프로세스가 시작될 때까지 디바이스에 대한 운영 영향/데이터 손실 위험이 없습니다.

ThreatGrid Appliance 3.0 릴리스를 준비하려면 릴리스에 필요한 낮은 수준의 디스크 포맷을 수행하여 디바이스의 모든 데이터를 파기하려면 특정 어플라이언스를 재설정해야 합니다.디바이스에 대한 데이터 손실을 방지하려면 TGA를 구성하여 NFS 공유에 백업한 다음 포맷이 완료되면 데이터를 복원해야 합니다.이 작업을 완료하려면 백업이 48시간 이상 성공적으로 실행되도록 하는 것이 중요합니다.또한 데이터를 복원하려면 암호화 키를 TGA로 가져와야 하므로 백업해야 합니다.

> **주의:"데이터 제거"를 수행하면 모든 소프트웨어 컨피그레이션이 재설정됩니다.CIMC 컨피그레이션은 수정되지 않지만 Admin, Clean, Dirty 인터페이스 컨피그레이션의 컨피그레이션이 제거됩니다.따라서 CIMC 인터페이스가 비활성화된 M5 ThreatGrid 디바이스를 사용하여 키보드와 모니터를 사용하여 어플라이언스에 대한 물리적 액세스 권한을 가지고 이 단계를 시도하기 전에 인터페이스 설정 및 IP 주소를 다시 구성해야 합니다.**

> **주의**: 암호화 키는 시스템에서 생성된 후에는 검색할 수 없습니다.데이터 손실을 방지하기 위해 키를 안전한 위치에 백업해야 합니다.