문제 해결

문제 해결

Security Analytics and Logging(온프레미스**)** 일반 문제 해결

관리자의 다음 로그 파일에는 Security Analytics and Logging(온프레미스)와 관련된 문제 해결 정보가 포함되어 있습니다.

- `/lancope/var/logs/containers/sal.log` - 일반 애플리케이션 로깅 정보(관리자 전용 구축 전용)
- `/lancope/var/logs/sal_preinstall.log` - 애플리케이션 설치 프로세스와 관련된 정보

플로우 컬렉터에서 다음 로그 파일에는 Security Analytics and Logging(온프레미스) 데이터 저장소 구축과 관련된 문제 해결 정보가 포함되어 있습니다.

- `lancope/var/sw/today/logs/sw.log` - 텔레메트리 로깅 관련 정보
- `/lancope/var/logs/containers/svc-db-ingest.log` - 이벤트 수집 및 데이터베이스 관련 정보

플로우 컬렉터 고급 설정을 사용하는 **Security Analytics and Logging(**온프레미스**)** 구성**(**데이터 저장소에만 해당**)**

최초 설정 중에 방화벽 로그를 저장하지 않도록 플로우 컬렉터를 구성한 경우, 플로우 컬렉터 고급 설정 페이지를 사용하여 수집 설정을 업데이트할 수 있습니다. 고급 설정에 액세스하려면 다음과 같이 합니다.

1. 플로우 컬렉터(이전의 어플라이언스 관리(Admin) 인터페이스)에 로그인합니다.
2. 지원 > 고급 설정을 클릭합니다.
3. 방화벽 이벤트 로그 수집을 활성화하려면 **enable_sal** 필드에 1을 입력합니다.
4. 방화벽 로그에 대한 포트를 변경하려면 **sal_syslog_port** 필드에 새 값을 입력합니다(기본 포트는 8514).
5. 적용 을 클릭한 다음 확인을 클릭합니다.

문제 해결

관리자 전용 구축 시 **Security Analytics and Logging**(온프레미스) 앱 설치 실패

독립형 어플라이언스(관리자 전용)인 관리자에 또는 플로우 컬렉터 및 데이터 노드(데이터 저장소)를 관리하는 관리자에 애플리케이션 설치를 지원합니다. 하나 이상의 플로우 컬렉터를 관리하고 데이터 저장소를 관리하지 않는 경우 관리자에 앱을 설치할 수 없습니다. 이 상황에서 앱을 설치하려고 하면 설치에 실패합니다. 이것이 원인인지 확인하려면 `/lancope/var/logs/sal_preinstall.log`에서 로그 파일을 검토합니다. 다음 메시지 또는 이와 유사한 메시지가 표시되면 설치에서 관리되는 플로우 컬렉터를 탐지한 것입니다.

```
Checking flow collectors...
1 Flow Collector(s) detected
Flow Collector(s) are present in inventory -- aborting installation.
```

앱을 설치하려면 Central 관리자 어플라이언스 인벤토리에서 관리되는 플로우 컬렉터를 모두 제거한 다음 다시 시도하십시오.

⚠

주의 관리자 전용 구축이 있는 경우 Security Analytics and Logging(온프레미스) 앱을 제거하면 관리자에서 이벤트 데이터를 비롯한 모든 관련 정보가 삭제되고 독립형 관리자 제한이 제거됩니다. Security Analytics and Logging(온프레미스) 애플리케이션을 제거한 후에는 트래픽을 검사하기 위해 기존 Secure Network Analytics 구축의 일부로 관리자을(를) 사용하여 하나 이상의 플로우 컬렉터를 관리할 수 있습니다.

Security Analytics and Logging(온프레미스) 앱 삭제 이벤트

앱은 다음과 같은 상황에서 이벤트를 삭제할 수 있습니다.

- 연결, 파일, 악성코드 및 침입 이벤트만이 아니라 모든 이벤트 유형을 시스템 로그로 내보냅니다.
- EPS(average events per second) 수집 속도 또는 버스트 EPS 수집 속도가 Secure Network Analytics 리소스 할당 섹션의 권장 사양을 초과합니다.

관리자 전용 구축의 경우 관리자에서 `/lancope/var/logs/containers/sal.log` 로그 파일의 정보를 검토하여 앱이 이벤트를 삭제하는지 확인합니다. "`events_dropped:`"를 포함하는 항목에 대한 파일을 검색합니다.

데이터 저장소 구축의 경우 플로우 컬렉터에서 `lancope/var/sw/today/logs/sw.log` 로그 파일의 정보를 검토하여 애플리케이션이 이벤트를 삭제하는지 확인합니다. 파일에서 "`sal_event`"를 포함하는 항목을 검색합니다.

이러한 작동이 계속될 경우 Cisco 지원팀에 문의하십시오.

Security Analytics and Logging(온프레미스) 앱 충돌

Security Analytics and Logging(온프레미스) 앱이 충돌하는 경우(예: 과도한 수집 속도로 인해) 관리자을(를) 다시 시작합니다. 이렇게 하면 앱도 다시 시작됩니다.

⚠

주의 앱을 제거하지 마십시오. 관리자 전용 구축이 있는 경우 Security Analytics and Logging(온프레미스) 앱을 제거하면 이벤트 데이터를 비롯한 모든 관련 정보가 관리자에서 삭제됩니다.