보안

Data Infrastructure Insights

NetApp
February 11, 2026

목차

보안

Data Infrastructure Insights 보안

NetApp 에서는 제품 및 고객 데이터 보안이 무엇보다 중요합니다. Data Infrastructure Insights 릴리스 수명 주기 전반에 걸쳐 보안 모범 사례를 준수하여 고객 정보와 데이터가 최상의 방식으로 보호되도록 합니다.

보안 개요

물리적 보안

Data Infrastructure Insights 프로덕션 인프라는 Amazon Web Services(AWS)에서 호스팅됩니다. 건물은 물론 문에 사용되는 잠금장치나 열쇠를 포함한 Data Infrastructure Insights 프로덕션 서버에 대한 물리적, 환경적 보안 관련 제어는 AWS에서 관리합니다. AWS에 따르면 "전문 보안 직원이 비디오 감시, 침입 탐지 시스템 및 기타 전자 수단을 활용하여 경계와 건물 진입 지점 모두에서 물리적 접근을 통제합니다. 권한이 있는 직원은 다중 인증 메커니즘을 활용하여 데이터 센터 바닥에 접근합니다."

Data Infrastructure Insights 다음의 모범 사례를 따릅니다."공유 책임 모델" AWS에서 설명했습니다.

제품 보안

Data Infrastructure Insights Agile 원칙에 따라 개발 수명 주기를 따르므로, 더 긴 릴리스 주기를 갖는 개발 방법론에 비해 보안 지향적인 소프트웨어 결함을 더 신속하게 해결할 수 있습니다. 지속적인 통합 방법론을 사용하면 기능적 변화와 보안적 변화에 신속하게 대응할 수 있습니다. 변경 관리 절차와 정책은 변경이 언제, 어떻게 발생하는지 정의하고 프로덕션 환경의 안정성을 유지하는 데 도움이 됩니다. 영향을 미치는 모든 변경 사항은 프로덕션 환경에 출시되기 전에 공식적으로 전달, 조정, 적절한 검토 및 승인을 거칩니다.

네트워크 보안

Data Infrastructure Insights 환경의 리소스에 대한 네트워크 액세스는 호스트 기반 방화벽에 의해 제어됩니다. 각 리소스(예: 부하 분산 장치 또는 가상 머신 인스턴스)에는 해당 리소스가 기능을 수행하는 데 필요한 포트로만 인바운드 트래픽을 제한하는 호스트 기반 방화벽이 있습니다.

Data Infrastructure Insights 침입 탐지 서비스를 포함한 다양한 메커니즘을 사용하여 보안 이상이 있는지 프로덕션 환경을 모니터링합니다.

위험 평가

Data Infrastructure Insights 팀은 공식화된 위험 평가 프로세스를 따라 체계적이고 반복 가능한 방식으로 위험을 식별하고 평가하여 위험 처리 계획을 통해 적절하게 관리할 수 있도록 합니다.

데이터 보호

Data Infrastructure Insights 프로덕션 환경은 모든 서비스와 구성 요소에 대해 여러 가용성 영역을 활용하는 고도로 중복된 인프라에 설정됩니다. 가용성이 높고 중복성이 높은 컴퓨팅 인프라를 활용하는 것과 더불어, 중요 데이터는 정기적으로 백업되고 복원은 주기적으로 테스트됩니다. 공식적인 백업 정책과 절차는 비즈니스 활동 중단으로 인한 영향을 최소화하고, 정보 시스템 장애나 재해의 영향으로부터 비즈니스 프로세스를 보호하며, 시기적절하고 적절하게 재개되도록 보장합니다.

인증 및 액세스 관리

모든 고객이 Data Infrastructure Insights 에 접근하는 것은 https를 통한 브라우저 UI 상호작용을 통해 이루어집니다. 인증은 제3자 서비스인 Auth0를 통해 수행됩니다. NetApp 이를 모든 클라우드 데이터 서비스의 인증 계층으로 중앙화했습니다.

Data Infrastructure Insights Data Infrastructure Insights 프로덕션 환경에 대한 논리적 액세스를 중심으로 "최소 권한" 및 "역할 기반 액세스 제어"를 포함한 업계 모범 사례를 따릅니다. 접근은 엄격한 필요성에 따라 통제되며 다중 인증 메커니즘을 사용하는 일부 승인된 직원에게만 허가됩니다.

고객 데이터 수집 및 보호

모든 고객 데이터는 공용 네트워크를 통해 전송될 때 암호화되고, 저장될 때도 암호화됩니다. Data Infrastructure Insights TLS(전송 계층 보안) 및 업계 표준 AES-256 알고리즘을 포함한 기술을 사용하여 시스템의 다양한 지점에서 암호화를 활용하여 고객 데이터를 보호합니다.

고객 프로비저닝 해제

다양한 간격으로 이메일 알림이 발송되어 고객에게 구독 만료를 알립니다. 구독이 만료되면 UI가 제한되고 데이터 수집을 위한 유예 기간이 시작됩니다. 그런 다음 고객에게 이메일을 통해 알림이 전달됩니다. 체험 구독에는 14일의 유예 기간이 적용되고, 유료 구독 계정에는 28일의 유예 기간이 적용됩니다. 유예 기간이 만료되면 고객에게 2일 후에 계정이 삭제된다는 내용의 이메일 알림이 전송됩니다. 유료 고객은 서비스 이용 중단을 직접 요청할 수도 있습니다.

만료된 테넌트와 관련된 모든 고객 데이터는 유예 기간이 끝나거나 고객의 계정 종료 요청이 확인되면 SRE(Data Infrastructure Insights 운영) 팀에서 삭제합니다. 어느 경우든 SRE 팀은 API 호출을 실행하여 계정을 삭제합니다. API 호출은 테넌트 인스턴스와 모든 고객 데이터를 삭제합니다. 고객 삭제는 동일한 API를 호출하고 고객 테넌트 상태가 "삭제됨"인지 확인하여 검증합니다.

보안 사고 관리

Data Infrastructure Insights NetApp의 제품 보안 사고 대응 팀(PSIRT) 프로세스와 통합되어 알려진 취약점을 찾고, 평가하고, 해결합니다. PSIRT는 고객 보고서, 내부 엔지니어링, CVE 데이터베이스와 같은 널리 알려진 출처를 포함한 여러 채널에서 취약성 정보를 수집합니다.

Data Infrastructure Insights 엔지니어링 팀에서 문제가 감지되면 해당 팀은 PSIRT 프로세스를 시작하고 문제를 평가하며 잠재적으로 해결합니다.

또한 Data Infrastructure Insights 고객이나 연구원이 Data Infrastructure Insights 제품의 보안 문제를 발견하고 기술 지원팀이나 NetApp 사고 대응팀에 직접 보고할 수도 있습니다. 이런 경우, Data Infrastructure Insights 팀은 PSIRT 프로세스를 시작하고 문제를 평가하며 잠재적으로 해결합니다.

취약점 및 침투 테스트

Data Infrastructure Insights 업계 모범 사례를 따르고 내부 및 외부 보안 전문가와 회사를 활용하여 정기적으로 취약성 및 침투 테스트를 수행합니다.

보안 인식 교육

모든 Data Infrastructure Insights 직원은 개별 역할에 맞게 개발된 보안 교육을 받으며, 이를 통해 각 직원이 해당 역할의 특정 보안 관련 과제를 처리할 수 있도록 준비합니다.

규정 준수

Data Infrastructure Insights 보안, 프로세스 및 서비스에 대한 외부 공인 회계사 회사의 독립적인 제3자 감사 및 검증을 수행하며, 여기에는 SOC 2 감사 완료도 포함됩니다.

NetApp 보안 권고

NetApp의 사용 가능한 보안 권고 사항을 볼 수 있습니다."여기" .

정보 및 지역

NetApp 고객 정보의 보안을 매우 중요하게 생각합니다. Data Infrastructure Insights 정보를 저장하는 방법과 위치는 다음과 같습니다.

Data Infrastructure Insights 어떤 정보를 저장합니까?

Data Infrastructure Insights 다음 정보를 저장합니다.

- 성능 데이터

  성능 데이터는 모니터링되는 장치/소스의 성능에 대한 정보를 제공하는 시계열 데이터입니다. 예를 들어, 여기에는 스토리지 시스템에서 전달된 IO 수, 파이버채널 포트의 처리량, 웹 서버에서 전달된 페이지 수, 데이터베이스의 응답 시간 등이 포함됩니다.

- 재고 데이터

  인벤토리 데이터는 모니터링되는 장치/소스와 해당 장치/소스의 구성 방법을 설명하는 메타데이터로 구성됩니다. 여기에는 설치된 하드웨어 및 소프트웨어 버전, 스토리지 시스템의 디스크 및 LUN, CPU 코어, 가상 머신의 RAM 및 디스크, 데이터베이스의 테이블스페이스, SAN 스위치의 포트 수 및 유형, 디렉토리/파일 이름(스토리지 워크로드 보안이 활성화된 경우) 등이 포함됩니다.

- 구성 데이터

  여기에는 고객 인벤토리와 운영을 관리하는 데 사용되는 고객이 제공한 구성 데이터(예: 모니터링되는 장치의 호스트 이름 또는 IP 주소, 폴링 간격, 시간 초과 값 등)가 요약되어 있습니다.

- 기미

  비밀은 Data Infrastructure Insights 인수 부서에서 고객 기기와 서비스에 액세스하는 데 사용하는 자격 증명으로 구성됩니다. 이러한 자격 증명은 강력한 비대칭 암호화를 사용하여 암호화되며, 개인 키는 인수 단위에만 저장되고 고객 환경 외부로 절대 유출되지 않습니다. 이러한 설계로 인해 권한이 있는 Data Infrastructure Insights SRE조차도 일반 텍스트 형태의 고객 비밀에 액세스할 수 없습니다.

- 기능적 데이터

  이는 NetApp 이 클라우드 데이터 서비스를 제공함으로써 생성된 데이터로, NetApp 클라우드 데이터 서비스를 개발, 배포, 운영, 유지관리 및 보안하는 데 필요한 정보를 제공합니다. 기능적 데이터에는 고객 정보나 개인 정보가 포함되지 않습니다.

- 사용자 액세스 데이터

NetApp Console 지역별 Data Infrastructure Insights 사이트와 통신할 수 있도록 하는 인증 및 액세스 정보(사용자 권한 부여와 관련된 데이터 포함)입니다.

- 스토리지 워크로드 보안 사용자 디렉토리 데이터

  워크로드 보안 기능이 활성화되어 있고 고객이 사용자 디렉터리 수집기를 활성화하기로 선택한 경우, 시스템은 Active Directory에서 수집된 사용자 표시 이름, 회사 이메일 주소 및 기타 정보를 저장합니다.

> ⓘ 사용자 디렉토리 데이터는 Workload Security 사용자 디렉토리 데이터 수집기가 수집한 사용자 디렉토리 정보를 의미하며, Data Infrastructure Insights/Workload Security 사용자에 대한 데이터는 아닙니다.

인프라 및 서비스 리소스에서 명시적인 개인 데이터는 수집되지 않습니다. 수집된 정보는 NetApp 자동 지원 및 ActiveIQ를 포함한 많은 공급업체의 전화 상담 서비스와 마찬가지로 성능 측정 항목, 구성 정보 및 인프라 메타데이터로만 구성됩니다. 그러나 고객의 명명 규칙에 따라 공유, 볼륨, VM, Q트리, 애플리케이션 등의 데이터에는 개인 식별 정보가 포함될 수 있습니다.

워크로드 보안이 활성화된 경우 시스템은 개인 식별 정보가 포함되어 있을 수 있는 SMB 또는 기타 공유의 파일 및 디렉터리 이름도 추가로 살펴봅니다. 고객이 Workload Security User Directory Collector(기본적으로 Active Directory를 통해 Windows SID를 사용자 이름에 매핑)를 활성화하는 경우, 표시 이름, 회사 이메일 주소 및 선택한 추가 속성은 Data Infrastructure Insights 에서 수집하여 저장합니다.

또한, Data Infrastructure Insights 에 대한 액세스 로그가 유지 관리되며, 이 로그에는 서비스에 로그인하는 데 사용된 사용자의 IP 및 이메일 주소가 포함됩니다.

내 정보는 어디에 저장되나요?

Data Infrastructure Insights 환경이 생성된 지역에 따라 정보를 저장합니다.

다음 정보는 호스트 지역에 저장됩니다.

- 카운터 및 성능 측정 항목을 포함한 원격 측정 및 자산/객체 정보
- 인수 단위 정보
- 기능적 데이터
- Data Infrastructure Insights 내 사용자 활동에 대한 감사 정보
- 워크로드 보안 Active Directory 정보
- 워크로드 보안 감사 정보

다음 정보는 Data Infrastructure Insights 환경을 호스팅하는 지역과 관계없이 미국에 보관됩니다.

- 사이트/계정 소유자와 같은 환경 사이트(때때로 "테넌트"라고 함) 정보입니다.
- NetApp Console 지역별 Data Infrastructure Insights 사이트와 통신할 수 있도록 하는 정보로, 사용자 권한 부여와 관련된 모든 정보가 포함됩니다.
- Data Infrastructure Insights 사용자와 테넌트 간의 관계에 대한 정보입니다.

호스트 지역

호스트 지역은 다음과 같습니다.

- 미국: us-east-1
- EMEA: eu-central-1
- 아시아 태평양: ap-southeast-2

추가 정보

다음 링크에서 NetApp의 개인정보 보호 및 보안에 대해 자세히 알아볼 수 있습니다.

- "신뢰 센터"
- "국경 간 데이터 전송"
- "구속력 있는 기업 규칙"
- "제3자 데이터 요청에 응답"
- "NetApp 개인정보 보호 원칙"

보안 관리 도구

Data Infrastructure Insights 향상된 보안으로 환경을 운영할 수 있는 보안 기능이 포함되어 있습니다. 이러한 기능에는 암호화, 비밀번호 해싱, 내부 사용자 비밀번호 변경 기능, 비밀번호를 암호화하고 복호화하는 키 쌍의 개선 사항이 포함됩니다.

민감한 데이터를 보호하기 위해 NetApp 설치 또는 업그레이드 후 기본 키와 *Acquisition* 사용자 비밀번호를 변경하는 것을 권장합니다.

데이터 소스 암호화된 비밀번호는 Data Infrastructure Insights 에 저장되며, 사용자가 데이터 수집기 구성 페이지에 비밀번호를 입력하면 공개 키를 사용하여 비밀번호를 암호화합니다. Data Infrastructure Insights 데이터 수집기 비밀번호를 해독하는 데 필요한 개인 키가 없습니다. 데이터 수집기 비밀번호를 해독하는 데 필요한 데이터 수집기 개인 키는 인수 단위(AU)에만 있습니다.

업그레이드 및 설치 고려 사항

Insight 시스템에 기본이 아닌 보안 구성이 포함된 경우(즉, 비밀번호를 다시 입력한 경우) 보안 구성을 백업해야 합니다. 새로운 소프트웨어를 설치하거나, 어떤 경우에는 소프트웨어를 업그레이드하면 시스템이 기본 보안 구성으로 돌아갑니다. 시스템이 기본 구성으로 되돌아가면 시스템이 올바르게 작동하려면 기본이 아닌 구성을 복원해야 합니다.

인수 단위의 보안 관리

SecurityAdmin 도구를 사용하면 Data Infrastructure Insights 의 보안 옵션을 관리할 수 있으며, 인수 단위 시스템에서 실행됩니다. 보안 관리에는 키와 비밀번호 관리, 사용자가 만든 보안 구성의 저장 및 복원, 구성을 기본 설정으로 복원하는 작업이 포함됩니다.

시작하기 전에

- Acquisition Unit 소프트웨어(SecurityAdmin 도구 포함)를 설치하려면 AU 시스템에 대한 관리자 권한이 있어야 합니다.
- 나중에 SecurityAdmin 도구에 액세스해야 하는 관리자가 아닌 사용자가 있는 경우 해당 사용자를 *cisys* 그룹에 추가해야 합니다. *cisys* 그룹은 AU 설치 중에 생성됩니다.

AU 설치 후, SecurityAdmin 도구는 다음 위치 중 하나에 있는 인수 유닛 시스템에서 찾을 수 있습니다.

```
Windows - <install_path>\Cloud Insights\Acquisition
Unit\acq\securityadmin\bin\securityadmin.bat
Linux - /bin/oci-securityadmin.sh
```

SecurityAdmin 도구 사용

SecurityAdmin 도구를 대화형 모드(-i)로 시작합니다.

명령줄에서 비밀을 전달하여 로그에 기록될 수 있는 상황을 방지하기 위해 SecurityAdmin 도구를 대화형 모드로 사용하는 것이 좋습니다.

다음 옵션이 표시됩니다.

[SecurityAdmin 도구 옵션(Linux)]

1. 지원

   모든 비밀번호와 키를 포함하는 볼트의 백업 zip 파일을 만들고 해당 파일을 사용자가 지정한 위치나 다음 기본 위치에 저장합니다.

   ```
   Windows - <install_path>\Cloud Insights\Acquisition
   Unit\acq\securityadmin\backup\vault
   Linux - /var/log/netapp/oci/backup/vault
   ```

   볼트 백업에는 민감한 정보가 포함되어 있으므로 안전하게 보관하는 것이 좋습니다.

2. 복원하다

   생성된 볼트의 zip 백업을 복원합니다. 복원되면 모든 비밀번호와 키는 백업 생성 시점의 값으로 되돌아갑니다.

   복원을 사용하면 여러 서버의 비밀번호와 키를 동기화할 수 있습니다. 예를 들어 다음 단계를 따르세요. 1) AU에서 암호화 키를 변경합니다. 2) 볼트의 백업을 만듭니다. 3) 각 AU에 볼트 백업을 복원합니다.

3. 외부 키 검색 스크립트 등록/업데이트

   외부 스크립트를 사용하여 장치 비밀번호를 암호화하거나 암호 해독하는 데 사용되는 AU 암호화 키를 등록하거나 변경합니다.

   암호화 키를 변경하는 경우 업그레이드나 설치 후 복원할 수 있도록 새로운 보안 구성을 백업해야 합니다.

   이 옵션은 Linux에서만 사용할 수 있습니다.

   SecurityAdmin 도구와 함께 자체 키 검색 스크립트를 사용할 때 다음 사항에 유의하세요.

   - 현재 지원되는 알고리즘은 최소 2048비트의 RSA입니다.

- 스크립트는 개인 키와 공개 키를 일반 텍스트로 반환해야 합니다. 스크립트는 암호화된 개인 키와 공개 키를 반환해서는 안 됩니다.
- 스크립트는 원시 인코딩된 콘텐츠(PEM 형식만 해당)를 반환해야 합니다.
- 외부 스크립트에는 실행 권한이 있어야 합니다.

4. 암호화 키 회전

   암호화 키를 순환합니다(현재 키의 등록을 취소하고 새 키를 등록합니다). 외부 키 관리 시스템의 키를 사용하려면 공개 키 ID와 개인 키 ID를 지정해야 합니다.

5. 기본 키로 재설정

   수집 사용자 비밀번호와 수집 사용자 암호화 키를 기본값으로 재설정합니다. 기본값은 설치 중에 제공된 값입니다.

6. 신탁 저장소 비밀번호 변경

   신뢰 저장소의 비밀번호를 변경합니다.

7. 키스토어 비밀번호 변경

   키스토어의 비밀번호를 변경합니다.

8. 수집기 비밀번호 암호화

   데이터 수집기 비밀번호를 암호화합니다.

9. 출구

   SecurityAdmin 도구를 종료합니다.

구성하려는 옵션을 선택하고 화면의 지시를 따르세요.

도구를 실행할 사용자 지정

통제되고 보안을 중시하는 환경에 있는 경우 *cisys* 그룹이 없더라도 특정 사용자가 SecurityAdmin 도구를 실행하도록 할 수 있습니다.

AU 소프트웨어를 수동으로 설치하고 액세스하려는 사용자/그룹을 지정하면 됩니다.

- API를 사용하여 CI 설치 프로그램을 AU 시스템에 다운로드하고 압축을 풉니다.
  - 일회용 승인 토큰이 필요합니다. API Swagger 설명서(관리자 > *API* 액세스_에서 *_API* 설명서 링크 선택)를 보고 *GET /au/oneTimeToken* API 섹션을 찾으세요.
  - 토큰을 받으면 *GET /au/installers/{platform}/{version}* API를 사용하여 설치 프로그램 파일을 다운로드합니다. 플랫폼(Linux 또는 Windows)과 설치 프로그램 버전을 제공해야 합니다.
- 다운로드한 설치 프로그램 파일을 AU 시스템에 복사하고 압축을 풉니다.
- 파일이 있는 폴더로 이동한 후 사용자와 그룹을 지정하여 루트로 설치 프로그램을 실행합니다.

```
./cloudinsights-install.sh <User> <Group>
```

지정된 사용자 및/또는 그룹이 존재하지 않으면 생성됩니다. 사용자는 SecurityAdmin 도구에 액세스할 수 있습니다.

프록시 업데이트 또는 제거

SecurityAdmin 도구는 *-pr* 매개변수와 함께 실행하여 획득 단위에 대한 프록시 정보를 설정하거나 제거하는 데 사용할 수 있습니다.

```
[root@ci-eng-linau bin]# ./securityadmin -pr
usage: securityadmin -pr -ap <arg> | -h | -rp | -upr <arg>

The purpose of this tool is to enable reconfiguration of security aspects
of the Acquisition Unit such as encryption keys, and proxy configuration,
etc. For more information about this tool, please check the Data
Infrastructure Insights
Documentation.

-ap,--add-proxy <arg>        add a proxy server.  Arguments: ip=ip
                              port=port user=user password=password
                              domain=domain
                              (Note: Always use double quote(") or single
                              quote(') around user and password to escape
                              any special characters, e.g., <, >, ~, `, ^,
                              !
                              For example: user="test" password="t'!<@1"
                              Note: domain is required if the proxy auth
                              scheme is NTLM.)
-h,--help
-rp,--remove-proxy           remove proxy server
-upr,--update-proxy <arg>    update a proxy.  Arguments: ip=ip port=port
                              user=user password=password domain=domain
                              (Note: Always use double quote(") or single
                              quote(') around user and password to escape
                              any special characters, e.g., <, >, ~, `, ^,
                              !
                              For example: user="test" password="t'!<@1"
                              Note: domain is required if the proxy auth
                              scheme is NTLM.)
```

예를 들어, 프록시를 제거하려면 다음 명령을 실행합니다.

```
 [root@ci-eng-linau bin]# ./securityadmin -pr -rp
명령을 실행한 후에는 수집 장치를 다시 시작해야 합니다.
```

프록시를 업데이트하려면 다음 명령을 사용합니다.

```
./securityadmin -pr -upr <arg>
```

외부 키 검색

UNIX 셸 스크립트를 제공하면 수집 장치에서 이를 실행하여 키 관리 시스템에서 *개인 키*와 *공개 키*를 검색할 수 있습니다.

키를 검색하기 위해 Data Infrastructure Insights 스크립트를 실행하고 _키 ID_와 _키 유형_이라는 두 개의 매개변수를 전달합니다. _키 ID_는 키 관리 시스템에서 키를 식별하는 데 사용할 수 있습니다. _키 유형_은 "공개" 또는 "비공개 "입니다. 키 유형이 "공개"인 경우 스크립트는 공개 키를 반환해야 합니다. 키 유형이 "개인"인 경우 개인 키를 반환해야 합니다.

키를 수집 장치로 다시 보내려면 스크립트가 키를 표준 출력에 인쇄해야 합니다. 스크립트는 키만 표준 출력에 인쇄해야 합니다. 다른 텍스트는 표준 출력에 인쇄하면 안 됩니다. 요청된 키가 표준 출력에 인쇄되면 스크립트는 종료 코드 0으로 종료되어야 합니다. 다른 반환 코드는 오류로 간주됩니다.

스크립트는 SecurityAdmin 도구를 사용하여 수집 단위에 등록되어야 하며, 이 도구는 수집 단위와 함께 스크립트를 실행합니다. 스크립트에는 루트 및 "cisys" 사용자에 대한 읽기 및 실행 권한이 있어야 합니다. 등록 후 쉘 스크립트가 수정된 경우, 수정된 쉘 스크립트를 수집 단위에 다시 등록해야 합니다.

입력 매개변수: 키 ID	고객의 키 관리 시스템에서 키를 식별하는 데 사용되는 키 식별자입니다.
입력 매개변수: 키 유형	공공 또는 민간.
산출	요청된 키는 표준 출력에 인쇄되어야 합니다. 현재 2048비트 RSA 키가 지원됩니다. 키는 다음 형식으로 인코딩 및 인쇄되어야 합니다. 개인 키 형식 - PEM, DER 인코딩 PKCS8 PrivateKeyInfo RFC 5958 공개 키 형식 - PEM, DER 인코딩 X.509 SubjectPublicKeyInfo RFC 5280
종료 코드	성공 시 종료 코드는 0입니다. 다른 모든 종료 값은 실패로 간주됩니다.
스크립트 권한	스크립트에는 루트 및 "cisys" 사용자에 대한 읽기 및 실행 권한이 있어야 합니다.
통나무	스크립트 실행이 기록됩니다. 로그는 다음에서 찾을 수 있습니다. - /var/log/netapp/cloudinsights/securityadmin/securityadmin.log /var/log/netapp/cloudinsights/acq/acq.log

API에서 사용할 비밀번호 암호화

옵션 8을 사용하면 비밀번호를 암호화한 후 API를 통해 데이터 수집기에 전달할 수 있습니다.

대화형 모드에서 SecurityAdmin 도구를 시작하고 옵션 8: _비밀번호 암호화_를 선택합니다.

```
 securityadmin.sh -i
암호화하려는 비밀번호를 입력하라는 메시지가 표시됩니다.  입력한 문자는 화면에 표시되지 않습니다.  메시지가 나타나면 비밀번호를 다시 입력하세요.
```

또는 스크립트에서 명령을 사용할 경우 명령줄에서 "-enc" 매개변수와 함께 _securityadmin.sh_를 사용하고 암호화되지 않은 비밀번호를 전달합니다.

```
 securityadmin -enc mypassword
image:SecurityAdmin_Encrypt_Key_API_CLI_Example.png["CLI 예제"]
```

암호화된 비밀번호가 화면에 표시됩니다. 앞뒤 기호를 포함한 전체 문자열을 복사합니다.

[대화형 모드 비밀번호 암호화, 너비=640]

암호화된 비밀번호를 데이터 수집기에 보내려면 데이터 수집 API를 사용할 수 있습니다. 이 API에 대한 자세한 내용은 *관리 > API 액세스*에서 확인할 수 있으며, "API 문서" 링크를 클릭하세요. "데이터 수집" API 유형을 선택하세요. *data_collection.data_collector* 제목 아래에서 이 예제에 대한 */collector/datasources* POST API를 선택합니다.

[데이터 수집을 위한 API]

preEncrypted 옵션을 _True_로 설정하면 API 명령을 통해 전달되는 모든 비밀번호는 이미 암호화된 것으로 처리됩니다. API는 비밀번호를 다시 암호화하지 않습니다. API를 빌드할 때 이전에 암호화된 비밀번호를 적절한 위치에 붙여넣기만 하면 됩니다.

[API 예제, 너비=600]