



보안

Data Infrastructure Insights

NetApp
January 10, 2025

목차

보안.....	1
Data Infrastructure Insights 보안	1
정보 및 지역.....	3
SecurityAdmin 도구	5

보안

Data Infrastructure Insights 보안

NetApp에게 제품 및 고객 데이터 보안은 무엇보다도 중요합니다. Data Infrastructure Insights는 릴리스 라이프사이클 전반에 걸쳐 보안 모범 사례를 준수하여 고객 정보와 데이터를 최상의 방법으로 보호합니다.

보안 개요

물리적 보안

Data Infrastructure Insights 운영 인프라는 AWS(Amazon Web Services)에서 호스팅됩니다. 건물, 문에 사용되는 잠금 또는 키를 비롯한 Data Infrastructure Insights 프로덕션 서버에 대한 물리적 및 환경적 보안 관련 제어가 AWS에서 관리됩니다. AWS에 따라: “물리적 액세스는 비디오 감시, 침입 탐지 시스템 및 기타 전자 수단을 활용하는 전문 보안 직원이 경계와 건물 진입점에서 모두 제어합니다. 공인 직원은 다중 요소 인증 메커니즘을 사용하여 데이터 센터 바닥에 액세스합니다.”

Data Infrastructure Insights는 "공유 책임 모델" AWS에서 설명한 의 모범 사례를 따릅니다.

제품 보안

Data Infrastructure Insights는 애자일 원칙에 따라 개발 라이프사이클을 따르므로 릴리스 주기 개발 방법론에 비해 보안 지향 소프트웨어 결함을 보다 신속하게 해결할 수 있습니다. 지속적인 통합 방법을 사용하여 기능 및 보안 변경 사항에 신속하게 대응할 수 있습니다. 변경 관리 절차 및 정책은 변경 발생 시기와 방법을 정의하고 운영 환경의 안정성을 유지하는 데 도움이 됩니다. 영향력 있는 변경 사항은 생산 환경에 배포하기 전에 공식적으로 전달, 조정, 적절하게 검토 및 승인됩니다.

네트워크 보안

Data Infrastructure Insights 환경의 리소스에 대한 네트워크 액세스는 호스트 기반 방화벽으로 제어됩니다. 각 리소스(예: 로드 밸런서 또는 가상 머신 인스턴스)에는 인바운드 트래픽을 해당 리소스가 기능을 수행하는 데 필요한 포트만 제한하는 호스트 기반 방화벽이 있습니다.

Data Infrastructure Insights는 침입 감지 서비스를 비롯한 다양한 메커니즘을 사용하여 프로덕션 환경의 보안 이상 징후를 모니터링합니다.

위험 평가

Data Infrastructure Insights 팀은 위험 치료 계획을 통해 적절히 관리할 수 있도록 위험을 식별하고 평가하는 체계적이고 반복 가능한 방법을 제공하는 공식화된 위험 평가 프로세스를 따릅니다.

데이터 보호

Data Infrastructure Insights 운영 환경은 모든 서비스 및 구성 요소에 대해 여러 가용 영역을 사용하는 매우 이중화된 인프라에 설정됩니다. 가용성이 높고 이중화된 컴퓨팅 인프라를 활용하는 동시에 중요한 데이터가 정기적으로 백업되고 복원이 정기적으로 테스트됩니다. 공식적인 백업 정책 및 절차는 비즈니스 활동 중단에 영향을 최소화하고 정보 시스템 또는 재해의 실패로부터 비즈니스 프로세스를 보호하며 시기 적절하고 적절한 재개를 보장합니다.

인증 및 액세스 관리

Data Infrastructure Insights에 대한 모든 고객은 https를 통한 브라우저 UI 상호 작용을 통해 액세스할 수 있습니다. 인증은 타사 서비스인 Auth0을 통해 수행됩니다. NetApp은 이를 모든 클라우드 데이터 서비스의 인증 계층으로 중앙 집중화하고 있습니다.

Data Infrastructure Insights는 Data Infrastructure Insights 운영 환경에 대한 논리적 액세스와 관련하여 "최소 권한" 및 "역할 기반 액세스 제어"를 비롯한 업계 모범 사례를 따릅니다. 액세스 권한은 엄격한 요구 사항에 따라 제어되며 다중 요소 인증 메커니즘을 사용하는 권한이 있는 일부 직원에게만 부여됩니다.

고객 데이터의 수집 및 보호

모든 고객 데이터는 공용 네트워크를 통해 전송 중에 암호화되고 저장된 데이터는 암호화됩니다. Data Infrastructure Insights는 TLS(전송 계층 보안) 및 업계 표준 AES-256 알고리즘을 포함한 기술을 사용하여 시스템의 다양한 지점에서 암호화를 활용하여 고객 데이터를 보호합니다.

고객 프로비저닝 해제

이메일 알림은 고객에게 구독이 만료됨을 알리기 위해 다양한 간격으로 발송됩니다. 구독이 만료되면 UI가 제한되고 데이터 수집을 위한 유예 기간이 시작됩니다. 그러면 고객에게 이메일을 통해 알립니다. 평가판 구독의 경우 14일의 유예 기간이 있으며 유료 구독 계정의 유예 기간은 28일입니다. 유예 기간이 만료된 후 고객은 이메일을 통해 계정을 2일 이내에 삭제할 것이라는 알림을 받습니다. 유료 고객은 서비스 종료 요청을 직접 할 수도 있습니다.

만료된 테넌트 및 모든 관련 고객 데이터는 유예 기간이 끝났거나 고객의 계정 종료 요청이 확인된 경우 Data Infrastructure Insights Operations(SRE) 팀에서 삭제합니다. 두 경우 모두 SRE 팀은 API 호출을 실행하여 계정을 삭제합니다. API 호출은 테넌트 인스턴스와 모든 고객 데이터를 삭제합니다. 동일한 API를 호출하고 고객 테넌트 상태를 "삭제됨"인지 확인하여 고객 삭제를 확인합니다.

보안 사고 관리

Data Infrastructure Insights는 NetApp의 제품 보안 사고 대응 팀(PSIRT) 프로세스와 통합되어 알려진 취약점을 찾고, 평가하고, 해결합니다. PSIRT는 고객 보고서, 내부 엔지니어링 및 CVE 데이터베이스와 같이 널리 알려진 소스를 비롯한 여러 채널의 취약점 정보를 포함합니다.

Data Infrastructure Insights 엔지니어링 팀에서 문제를 감지한 경우 팀은 PSIRT 프로세스를 시작하고 문제를 평가 및 잠재적으로 해결합니다.

또한 Data Infrastructure Insights 고객 또는 연구자가 Data Infrastructure Insights 제품의 보안 문제를 식별하고 이 문제를 기술 지원팀에 보고하거나 NetApp의 사고 대응 팀에 직접 보고할 수도 있습니다. 이 경우 Data Infrastructure Insights 팀은 PSIRT 프로세스를 시작하고 문제를 평가 및 잠재적으로 해결합니다.

취약점 및 침투 테스트

Data Infrastructure Insights는 업계 모범 사례를 따르며 내부 및 외부 보안 전문가와 회사를 통해 정기적인 취약성 및 모의 해킹 테스트를 수행합니다.

보안 인식 교육

모든 Data Infrastructure Insights 직원은 각 직원이 각자의 역할에 맞는 특정 보안 관련 과제를 처리할 수 있도록 개별 역할에 맞게 개발된 보안 교육을 이수해야 합니다.

규정 준수

Data Infrastructure Insights는 외부의 인가된 CPA 회사를 통해 SOC 2 감사 완료와 더불어 보안성, 프로세스 및 서비스에 대한 독립된 제3자 감사 및 검증을 수행합니다.

NetApp 보안 권고

NetApp에서 제공하는 보안 권고를 볼 수 ["여기"](#) 있습니다.

정보 및 지역

NetApp은 고객 정보의 보안을 매우 중요하게 생각합니다. Data Infrastructure Insights에서 정보를 저장하는 방법과 위치를 확인하십시오.

Data Infrastructure Insights는 어떤 정보를 저장합니까?

Data Infrastructure Insights는 다음 정보를 저장합니다.

- 성능 데이터

성능 데이터는 모니터링되는 장치/소스의 성능에 대한 정보를 제공하는 시계열 데이터입니다. 예를 들어, 스토리지 시스템에서 제공되는 입출력 수, FiberChannel 포트의 처리량, 웹 서버에서 제공하는 페이지 수, 데이터베이스의 응답 시간 등이 여기에 포함됩니다.

- 재고 데이터

인벤토리 데이터는 모니터링되는 디바이스/소스와 해당 소스 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 수와 유형, 디렉토리/파일 이름(스토리지 워크로드 보안이 설정된 경우) 등이 포함됩니다.

- 구성 데이터

이 요약에는 모니터링된 장치의 호스트 이름 또는 IP 주소, 폴링 간격, 시간 초과 값 등 고객 인벤토리 및 작업을 관리하는 데 사용되는 고객이 제공한 구성 데이터가 요약되어 있습니다.

- 비밀

비밀은 Data Infrastructure Insights Acquisition Unit에서 고객 장치 및 서비스에 액세스하는 데 사용하는 자격 증명으로 구성됩니다. 이러한 자격 증명은 강력한 비대칭 암호화를 사용하여 암호화되며 개인 키는 획득 장치에만 저장되며 고객 환경을 떠나지 않습니다. 권한 있는 Data Infrastructure Insights SRE도 이 설계 때문에 일반 텍스트로 고객 비밀에 액세스할 수 없습니다.

- 기능 데이터

이 데이터는 NetApp에서 클라우드 데이터 서비스를 제공하여 생성되는 것으로, 클라우드 데이터 서비스의 개발, 구축, 운영, 유지보수, 보안에 대해 NetApp에 알려줍니다. 기능 데이터에는 고객 정보 또는 개인 정보가 포함되어 있지 않습니다.

- 사용자 액세스 데이터

사용자 권한 부여와 관련된 데이터를 포함하여 NetApp BlueXP 이 지역 데이터 인프라 인사이트 사이트와 통신할 수 있도록 하는 인증 및 액세스 정보입니다.

- 스토리지 워크로드 보안 사용자 디렉토리 데이터

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



사용자 디렉토리 데이터는 Data Infrastructure Insights/Workload Security 자체의 사용자에게 대한 데이터가 아니라 워크로드 보안 사용자 디렉토리 데이터 수집기에서 수집한 사용자 디렉토리 정보를 말합니다.

- 인프라 및 서비스 리소스에서 명시적 개인 데이터 * 가 수집되지 않습니다. 수집된 정보는 성능 메트릭, 구성 정보 및 인프라 메타데이터로만 구성되며, NetApp의 자동 지원 및 ActiveIQ를 비롯한 수많은 공급업체 Phone-Home과 매우 유사합니다. 그러나 고객의 명명 규칙에 따라 공유, 볼륨, VM, qtree, 응용 프로그램 등에 개인 식별 정보가 포함될 수 있습니다.

워크로드 보안이 설정된 경우 시스템은 SMB 또는 기타 공유에서 파일 및 디렉토리 이름을 추가로 확인합니다. 여기에는 개인 식별 정보가 포함될 수 있습니다. 고객이 워크로드 보안 사용자 디렉토리 수집기를 활성화하면(기본적으로 Active Directory를 통해 Windows SID를 사용자 이름에 매핑), 표시 이름, 회사 이메일 주소 및 선택된 추가 속성이 Data Infrastructure Insights에 의해 수집되고 저장됩니다.

또한 Data Infrastructure Insights에 대한 액세스 로그는 유지 관리되며 서비스에 로그인하는 데 사용되는 사용자의 IP 및 이메일 주소를 포함합니다.

내 정보는 어디에 저장되니까?

Data Infrastructure Insights는 환경이 생성되는 지역에 따라 정보를 저장합니다.

다음 정보는 호스트 영역에 저장됩니다.

- 카운터 및 성능 메트릭을 포함한 원격 측정 및 자산/객체 정보
- 획득 장치 정보
- 기능 데이터
- Data Infrastructure Insights 내의 사용자 활동에 대한 정보 감사
- 워크로드 보안 Active Directory 정보
- 워크로드 보안 감사 정보

다음 정보는 Data Infrastructure Insights 환경을 호스팅하는 지역에 상관없이 미국에 있습니다.

- 사이트/계정 소유자와 같은 환경 사이트("테넌트"라고도 함) 정보
- 사용자 승인과 관련된 모든 작업을 포함하여 NetApp BlueXP 이 지역별 데이터 인프라 인사이트 사이트와 통신할 수 있도록 하는 정보.
- Data Infrastructure Insights 사용자와 테넌트 간의 관계와 관련된 정보입니다.

호스트 영역

호스트 영역은 다음과 같습니다.

- 미국: 동쪽편 - 1
- EMEA: EU-CENTRAL-1
- APAC: AP-남동-2

추가 정보

다음 링크에서 NetApp의 개인 정보 보호 및 보안에 대해 자세히 확인할 수 있습니다.

- ["보안 센터"](#)
- ["국가 간 데이터 전송"](#)
- ["기업 규칙을 구속하는 중입니다"](#)
- ["타사 데이터 요청에 대한 응답"](#)
- ["NetApp 개인 정보 보호 원칙"](#)

SecurityAdmin 도구

Data Infrastructure Insights에는 환경을 향상된 보안으로 운영할 수 있는 보안 기능이 포함되어 있습니다. 암호화, 암호 해싱의 개선, 내부 사용자 암호 변경 기능, 암호 암호화 및 암호 해독을 위한 키 쌍 등의 기능이 있습니다.

중요한 데이터를 보호하려면 설치 또는 업그레이드 후에 기본 키와 `_Acquisition_user` 암호를 변경하는 것이 좋습니다.

데이터 소스의 암호화된 암호는 사용자가 데이터 수집기 구성 페이지에 입력할 때 공개 키를 사용하여 암호를 암호화하는 Data Infrastructure Insights에 저장됩니다. Data Infrastructure Insights에는 데이터 수집기 암호를 해독하는 데 필요한 개인 키가 없습니다. AUS(Acquisition Unit)에만 데이터 수집기 암호를 해독하는 데 필요한 데이터 수집기 개인 키가 있습니다.

업그레이드 및 설치 고려 사항

Insight 시스템에 기본이 아닌 보안 구성(예: 암호 키 다시 입력)이 포함된 경우 보안 구성을 백업해야 합니다. 새 소프트웨어를 설치하거나 소프트웨어를 업그레이드하는 경우 시스템을 기본 보안 구성으로 되돌립니다. 시스템이 기본 구성으로 복원되면 시스템이 올바르게 작동하려면 기본이 아닌 구성을 복원해야 합니다.

획득 장치의 보안 관리

SecurityAdmin 도구를 사용하면 Data Infrastructure Insights의 보안 옵션을 관리할 수 있으며 획득 장치 시스템에서 실행됩니다. 보안 관리에는 키 및 암호 관리, 사용자가 만들고 복원한 보안 구성을 기본 설정으로 저장 및 복원하는 작업이 포함됩니다.

시작하기 전에

- 획득 장치 소프트웨어(SecurityAdmin 도구 포함)를 설치하려면 AU 시스템에 대한 관리자 권한이 있어야 합니다.
- 나중에 SecurityAdmin 도구에 액세스해야 하는 관리자가 아닌 사용자가 있는 경우 `_cisys_group`에 추가해야 합니다. AU 설치 중에 `_cisys_group`이 생성됩니다.

AU 설치 후 다음 위치 중 하나에 있는 획득 장치 시스템에서 SecurityAdmin 도구를 찾을 수 있습니다.

```
Windows - C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat
Linux - /bin/oci-securityadmin.sh
```

SecurityAdmin 도구 사용

대화형 모드(-i)에서 SecurityAdmin 도구를 시작합니다.



명령줄에서 암호를 전달하지 않도록 대화형 모드에서 SecurityAdmin 도구를 사용하는 것이 좋습니다. 이 도구는 로그에 캡처될 수 있습니다.

다음 옵션이 표시됩니다.

```
[root@ci-qa-xitij-cis2-28594linau bin]# ./securityadmin -i
Select Action:

1 - Backup
2 - Restore
3 - Register / Update External Key Retrieval Script
4 - Rotate Encryption Keys
5 - Reset to Default Keys
6 - Change Truststore Password
7 - Change Keystore Password
8 - Encrypt Collector Password
9 - Exit

Enter your choice: █
```

1. * 백업 *

모든 암호 및 키가 포함된 볼트의 백업 zip 파일을 작성하고 사용자가 지정한 위치 또는 다음 기본 위치에 파일을 배치합니다.

```
Windows - C:\Program Files\SANscreen\backup\vault
Linux - /var/log/netapp/oci/backup/vault
```

볼트 백업은 중요한 정보를 포함하기 때문에 안전하게 유지하는 것이 좋습니다.

2. * 복원 *

작성된 볼트의 zip 백업을 복원합니다. 복원되면 모든 암호와 키는 백업 생성 시 기존 값으로 되돌려집니다.

복원은 여러 서버의 암호 및 키를 동기화하는 데 사용할 수 있습니다. 예를 들어 다음 단계를 사용합니다. 1) AU의 암호화 키 변경 2) 볼트 백업을 작성합니다. AUS 각각에 볼트 백업을 복원합니다.

3. * 외부 키 검색 스크립트 등록/업데이트 *

외부 스크립트를 사용하여 장치 암호를 암호화 또는 해독하는 데 사용되는 AU 암호화 키를 등록하거나 변경합니다.

암호화 키를 변경할 때는 업그레이드 또는 설치 후 복원할 수 있도록 새 보안 구성을 백업해야 합니다.

참고 이 옵션은 Linux에서만 사용할 수 있습니다.

SecurityAdmin 도구와 함께 사용자 고유의 키 검색 스크립트를 사용하는 경우 다음 사항을 염두에 두십시오.

- 현재 지원되는 알고리즘은 최소 2048비트의 RSA입니다.
- 스크립트는 개인 키와 공개 키를 일반 텍스트로 반환해야 합니다. 스크립트는 암호화된 개인 키와 공개 키를 반환하지 않아야 합니다.
- 스크립트는 원시 인코딩된 내용을 반환해야 합니다(PEM 형식만 해당).
- 외부 스크립트에는 `_execute_permissions` 가 있어야 합니다.

4. * 암호화 키 회전 *

암호화 키를 회전합니다(현재 키 등록 취소 및 새 키 등록). 외부 키 관리 시스템의 키를 사용하려면 공개 키 ID와 개인 키 ID를 지정해야 합니다

5. * 기본 키로 재설정 *

획득 사용자 암호 및 획득 사용자 암호화 키를 기본값으로 재설정합니다. 기본값은 설치 중에 제공되는 값입니다.

6. * truststore 암호 변경 *

truststore의 암호를 변경합니다.

7. * Keystore 암호 변경 *

키 저장소의 암호를 변경합니다.

8. * Collector 암호 암호화 *

데이터 수집기 암호를 암호화합니다.

9. * 종료 *

SecurityAdmin 도구를 종료합니다.

구성할 옵션을 선택하고 화면의 지시를 따릅니다.

도구를 실행할 사용자 지정

보안을 중요시하는 통제된 환경에서 `_cisys_group`이 없지만 특정 사용자가 SecurityAdmin 도구를 실행하기를 원할 수

있습니다.

수동으로 AU 소프트웨어를 설치하고 액세스할 사용자/그룹을 지정하면 이 작업을 수행할 수 있습니다.

- API를 사용하여 CI 설치 프로그램을 AU 시스템에 다운로드하고 압축을 풉니다.
 - 1회 인증 토큰이 필요합니다. API Swagger 설명서(_Admin > API Access _ 및 _API Documentation_link 선택)를 참조하여 _get/au/oneTimeToken_API 섹션을 찾습니다.
 - 토큰이 있으면 _get/au/installers/{platform}/{version}_API를 사용하여 설치 관리자 파일을 다운로드합니다. 설치 프로그램 버전과 함께 플랫폼(Linux 또는 Windows)을 제공해야 합니다.
- 다운로드한 설치 관리자 파일을 AU 시스템에 복사하고 압축을 풉니다.
- 파일이 포함된 폴더로 이동하고 설치 관리자를 루트로 실행하고 사용자 및 그룹을 지정합니다.

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

지정된 사용자 및/또는 그룹이 없으면 해당 사용자 및/또는 그룹이 생성됩니다. 사용자는 SecurityAdmin 도구에 액세스할 수 있습니다.

프록시를 업데이트 또는 제거하는 중입니다

SecurityAdmin 도구는 _-pr_parameter로 도구를 실행하여 획득 장치에 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 후 획득 장치를 다시 시작해야 합니다.
```

프록시를 업데이트하려면 명령은 입니다

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

외부 키 검색

UNIX 셸 스크립트를 제공할 경우 획득 장치에서 이를 실행하여 키 관리 시스템에서 * 개인 키 * 및 * 공개 키 * 를 검색할

수 있습니다.

키를 검색하기 위해 Data Infrastructure Insights에서 스크립트를 실행하고 두 가지 매개 변수(*key id_and_key type*)를 전달합니다. `_Key id_`를 사용하여 키 관리 시스템의 키를 식별할 수 있습니다. `_키 유형_`은(는) "public" 또는 "private"입니다. 키 유형이 "public"인 경우 스크립트는 공개 키를 반환해야 합니다. 키 유형이 "private"인 경우 개인 키를 반환해야 합니다.

키를 다시 획득 장치로 보내려면 스크립트는 키를 표준 출력으로 인쇄해야 합니다. 스크립트는 `PRINT_ONLY_THE` 키를 표준 출력으로 가져와야 합니다. 다른 텍스트는 표준 출력으로 인쇄해서는 안 됩니다. 요청된 키가 표준 출력으로 인쇄되면 스크립트는 종료 코드가 0인 상태에서 종료되어야 합니다. 다른 반환 코드는 오류로 간주됩니다.

이 스크립트는 획득 장치와 함께 스크립트를 실행하는 SecurityAdmin 도구를 사용하여 획득 장치에 등록해야 합니다. 스크립트에는 root 및 "cisys" 사용자에게 대해 `_READ_AND_EXECUTE_` 권한이 있어야 합니다. 등록 후 셸 스크립트가 수정되면 수정된 셸 스크립트를 획득 장치에 다시 등록해야 합니다.

입력 매개 변수: 키 ID	고객 키 관리 시스템에서 키를 식별하는 데 사용되는 키 식별자입니다.
입력 매개 변수: 키 유형	퍼블릭 또는 프라이빗.
출력	요청된 키를 표준 출력으로 인쇄해야 합니다. 현재 2048비트 RSA 키가 지원됩니다. 키는 PEM, DER로 인코딩된 PKCS8 PrivateKeyInfo RFC 5958 공개 키 형식(PEM, DER로 인코딩된 X.509 SubjectPublicKeyInfo RFC 5280)으로 인코딩 및 인쇄되어야 합니다
종료 코드	종료 코드 0을(를) 성공했습니다. 다른 모든 종료 값은 실패로 간주됩니다.
스크립트 권한	스크립트에는 루트 및 "cisys" 사용자에게 대한 읽기 및 실행 권한이 있어야 합니다.
로그	스크립트 실행이 기록됩니다. 로그는 - /var/log/NetApp/cloudinsights/SecurityAdmin/securityadmin.log /var/log/NetApp/cloudinsights/acq/acq.log 에서 확인할 수 있습니다

API에서 사용하기 위한 암호 암호화

옵션 8에서는 암호를 암호화하고 API를 통해 데이터 수집기로 전달할 수 있습니다.

대화형 모드에서 SecurityAdmin 도구를 시작하고 옵션 8: `_Encrypt Password_` 를 선택합니다.

```
securityadmin.sh -i
```

암호화할 암호를 입력하라는 메시지가 표시됩니다. 입력한 문자는 화면에 표시되지 않습니다. 메시지가 나타나면 암호를 다시 입력합니다.

또는 스크립트에서 명령을 사용할 경우 명령줄에서 "-enc" 매개 변수와 함께 `_SecurityAdmin.sh_`를 사용하여 암호화되지 않은 암호를 전달합니다.

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

암호화된 암호가 화면에 표시됩니다. 선행 또는 후행 기호를 포함하여 전체 문자열을 복사합니다.

```
[root@ci-eng-srivardh-learn bin]# securityadmin.sh -i
Select Action:

1 - Backup
2 - Restore
3 - Change Encryption Keys
4 - Reset to Default Keys
5 - Check for Default Encryption Keys
6 - Change Truststore Password
7 - Change Keystore Password
8 - Encrypt Password
9 - Exit

Enter your choice: 8
Please enter your password to encrypt:
Please confirm your password to encrypt:

Your Encrypted Password below

ciYJAMpdEncBsLQwF2gobbiERL4Jrwb7tLW0fYhu0dERGZU3L+uWfcCXdNSXTWr6SFuumwsWVFib3h78vnM0s6vM7G/2k1Bd8ggJiQ+tS/LZkmJ6XKgTdcf3LGN8UqzQy
Rn0v5jJBGip6nCysrt9dapsEiRVHrMJVr8btGYbb4Zoz62qudMfW9uQdm3qyzSKbIY0L0An89yDPC0kDkaXreyLfpju0G5UmeZz1KGCT0aBTggri/JIYyyr4w2ZLnG0w21
LGm59vor70GU0iKZYablD+7LpsdCCBi1eF86BCj2RkxX0of891sHN+E7zTvZEofdGVWepc7b/HNah5XiXgVvk1viCZ/WqkyQ==
```

암호화된 암호를 데이터 수집기에 보내려면 데이터 수집 API를 사용할 수 있습니다. 이 API의 Swagger는 * Admin > API Access * 에서 확인할 수 있으며 "API Documentation" 링크를 클릭하십시오. "데이터 수집" API 유형을 선택합니다. data_collection.data_collector_heading 아래에서 이 예제에 대한 `/collector/datasources_POST` API를 선택합니다.

data_collection.data_collector

POST /collector/datasources Create a data collector

Create a data collector

Parameters Try it out

Name	Description
preEncrypted boolean (query)	Optional, defaults to false. If preEncrypted query parameter set to true, directs server to treat all passed secret values as already encrypted Default value : false

Request body required application/json

Example Value | Schema

```
{
  "acquisitionUnit": {
    "additionalProp1": "string",
    "additionalProp2": "string"
  }
}
```

`_preEncrypted_option`을 `_True_`로 설정하면 API 명령을 통해 전달하는 모든 암호는 * 이미 암호화된 * 로 처리되며

API는 암호를 다시 암호화하지 않습니다. API를 구축할 때 이전에 암호화된 암호를 적절한 위치에 붙여 넣기만 하면 됩니다.

https://<TENANT URL>/rest/v1/collector/datasources?preEncrypted=true

```
{
  "name": "cdot-aaaaa",
  "config": {
    "dsTypeId": "93",
    "vendorModelId": "1",
    "packages": [
      {
        "id": "foundation",
        "displayName": "Inventory",
        "isMandatory": true,
        "attributes": {
          "RELEASESTATUS": "OFFICIAL",
          "enabled": true,
          "ip": "10.62.219.30",
          "user": "admin",
          "password":
            "J8bepjwz9oNknfs6mcqbz3zuEThZQp1VyTk+1wE05gWwmmj1u0CB688nfOnB1xnIBVsAWyLmORxFAw
            vcDCvGbTraqp/+nT0k94LO8Z7Q04I5KqhHfTvINGU54S4IVLWiMIFj8kSU4RhMvNNNq5Tarz0gJZhWR+
            4RoNF+84R/uFFGwKebIrfHxWZZMoW7pEJ2kzLFBtBzx2mUvRP0kn6AFbyS4+DM2YTPQkSk3W2Gzc
            +nfPDDyH8Tq6AM5WsVCKqnZAa2ZIY1FxMkKT7iFt5oiYnl93ka7OrQImM9QAYpoyw/JT0nXHDuf683uE
            K32yn9CgxNGXy5NcNzRurdFNb5w=="
        }
      },
      {
        "id": "storageperformance",
        "displayName": "Array Performance",
        "isMandatory": false,
        "attributes": {
          "password": "this will not be encrypted on the server side"
        }
      }
    ]
  },
  "acquisitionUnit": {
    "id": "1"
  }
}
```

저작권 정보

Copyright © 2025 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이선스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 <http://www.netapp.com/TM>에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.